

KRİPTO PARALARA EL KOYMA KILAVUZU



KRİPTO PARALARA EL KOYMA KILAVUZU

Sürüm 1.0

Avrupa Konseyi Siber Suçlar Programı Ofisi

10 Şubat 2021

Bu kılavuz,
Güneydoğu Avrupa ve Türkiye proje ülkelerinin / alanlarının girişimiyle
iPROCEEDS-2 çerçevesinde geliştirilmiştir

Funded
by the European Union
and the Council of Europe



Implemented
by the Council of Europe

Teşekkür

Bu Kılavuz, Avrupa Birliği ve Avrupa Konseyi Ortak Projesi [iPROCEEDS-2](#) çerçevesinde hazırlanmıştır ve proje ülkelerindeki / bölgelerindeki yetkililerin siber suçlardan elde edilen gelirleri arama, , el koyma ve bölgedeki internet üzerinden kara para aklama faaliyetlerini önleme ve elektronik kanıtları güvence altına alma kapasitesini daha da güçlendirmeyi amaçlamaktadır.

Bu belge üzerindeki çalışmalar Avrupa Konseyi Siber Suçlar Programı Ofisi (C-PROC) tarafından koordine edilmiştir. İlgili tüm uzmanlar, sanal para birimleriyle ilgili uygulamalı faaliyetlerde dünyanın her yerindeki soruşturma görevlileri için bir yol gösterici olmayı amaçlayan bu kılavuz taslağını hazırlamak için kapsamlı uzmanlıklarını sağlamıştır.

Taslağı Hazırlayanlar:

- Christophe LANDRIES (Belçika)
- Jussi AITTOLA (Finlandiya)
- Gergely VESSZOS (Macaristan)
- Bart DE VLAMINCK (Belçika)

İLETİŞİM

Avrupa Konseyi Siber Suç Programı Ofisi
(C-PROC)

Tel +33-3-9021-4506

E-mail alexander.seger@coe.int

UYARI

Bu teknik rapor, Avrupa Konseyi veya Avrupa Birliği'nin resmi tutumlarını yansıtmamaktadır.

www.coe.int/cybercrime

Funded
by the European Union
and the Council of Europe



Implemented
by the Council of Europe

İçindekiler

1	Giriş	2
1.1	Gerekçe	2
1.2	Kılavuzun Amacı.....	2
1.3	Kılavuz Kimlere Yöneliktir?	3
2	El koymanın arkasındaki teori.....	3
2.1	Tanımlar (FATF/AB)	3
2.1.1	"Sanal Para Birimi", "Kripto Para Birimi" ve "Sanal Varlıkların" Tanımı.....	3
2.1.2	Sanal para birimlerinin sınıflandırılması	6
2.1.3	"SVSS" nin tanımı.....	7
2.1.4	Dağıtık Defterin tanımı	8
2.1.5	Blok zinciri nedir?	8
2.2	Genel konseptler	9
2.2.1	İş ispatı nedir?	9
2.2.2	Hisse ispatı nedir?	9
2.2.3	(Merkezi Olmayan Finansta) Yield Farming nedir?	9
2.2.4	Genel-özel anahtar nedir?	10
2.2.5	Cüzdan nedir?	10
2.2.5.1	Tanım	10
2.2.5.2	Emanetçi olan ve olmayan cüzdan.....	11
2.2.5.3	Çeşitler: masaüstü, mobil, donanım, kağıt, online.....	11
2.2.5.4	Anahtar Kelime	12
2.2.5.5	İşlemler ve işlem ücretleri	12
2.3	Bitcoin	13
2.3.1	Bitcoin nedir?.....	13
2.3.2	Bitcoin tarihi	14
2.3.3	Altcoin (Alternatif Kripto Para) Nedir?	14
2.4	Ethereum	14
2.4.1	Ethereum'un temellerini ve Ethereum tabiatını bilmek neden önemlidir?	14
2.4.2	Ethereum nedir?.....	15
2.4.3	Ether nedir?.....	15
2.4.4	ERC-20 nedir?.....	15
2.4.5	Ethereum akıllı sözleşmeleri nasıl çalışır?	15

2.5	Kripto paraların regülasyonu	15
2.5.1	FATF (Mali Eylem Görev Gücü) seyahat kuralı	15
2.5.2	AMLD5 ve ulusal kanunlardaki uygulamalar	16
2.5.3	AB Dijital Finans Paketi: Kripto varlıklara ilişkin yasal öneriler, fırsatları ele geçirme ve riskleri azaltma 16	
2.5.4	MICA (Kripto Varlıklarda Piyasalar) kılavuzu	17
2.6	Kripto paranın kullanımı aşağıdakileri içerir ancak bunlarla sınırlı değildir	18
2.6.1	Darknet (Karanlık internet) pazarları	18
2.6.2	Fidye Yazılımı	18
2.6.3	Şantaj	19
2.6.4	Hortumlar (dolandırıcılık)	19
2.6.5	Saadet zincirleri	19
3	El koyma ile ilgili pratik kılavuzlar	19
3.1	El koyma/ müsadere nedir?	19
3.1.1	Kripto varlıklar ve normal varlıklar	20
3.2	El koyma öncesi planlama	20
3.2.1	Giriş ve yasal çerçeve	20
3.2.2	Eğitim ve uzmanlık	21
3.2.3	Ne aranıyor?	22
3.2.4	Devlet kontrolündeki cüzdanlar	23
3.2.5	Yetkiler, karar verme yetkisi kimde?	24
3.2.6	Suç ortaklarının farkında olun	24
3.2.7	Strateji ve eylem planı	25
3.3	Masaüstü Cüzdan	26
3.3.1	Giriş	26
3.3.2	Bitcoin Core ve "hafif cüzdan" (light wallet)'lardan farkı	26
3.3.3	Electrum	29
3.3.4	Exodus	45
3.3.5	Ethereum Cüzdanları	49
3.3.5.1	MyCrypto Cüzdanı	49
3.3.5.2	Metamask	53
3.4	Mobil Cüzdan	65
3.4.1	Giriş	65
3.4.2	En iyi uygulamalar ve kılavuzlar	65
3.4.3	MyCeliium	66
3.4.4	Jaxx Liberty	69

3.5	Donanım Cüzdanı	74
3.5.1	Giriş	74
3.5.2	En iyi uygulamalar ve kılavuzlar.....	75
3.5.2.1	Ledger cüzdanı	75
3.6	Kağıt Cüzdan	101
3.6.1	Giriş	101
3.6.2	Şifrelenmiş ve Şifrelenmemiş	105
3.7	Emanetçi ve online web cüzdanları	111
3.7.1	Giriş	111
3.7.2	En iyi uygulamalar ve kılavuzlar.....	114
3.7.3	İki Faktörlü Kimlik Doğrulama (2FA).....	116
3.8	Anahtar Kelimeler.....	116
3.9	Raporlama	117
4	Kapanış.....	118

1 Giriş

Covid-19 salgını nedeniyle birçok işletme ve kurum, faaliyetlerini fiziksel varlıktan çevrimiçi bir ortama dönüştürmüş ve teknolojiye daha da fazla güvenmeye başlamıştır. Suçlular, doğaları gereği bir toplumda devam eden değişikliklere uyum sağlayabildiklerinden, faaliyetlerini çevrimiçi dünyaya da kaydırmış ve dünya çapında artan internet kullanıcılarının peşine düşmüştür.

Failler, vergi kaçakçılığından kara para aklamaya ve uyuşturucu kaçakçılığına kadar çeşitli suç faaliyetlerini yerine getirirken, sağladığı iddia edilen mahremiyet ve anonimlik nedeniyle giderek daha fazla kripto para kullanmaktadır.

Europol'un İnternet Organize Suç Tehdit Değerlendirmesine (IOCTA 2019) göre, *"kripto para birimleri siber suçları kolaylaştırmaya devam etmekte ve bilgisayar korsanları ve dolandırıcılar artık rutin olarak kripto varlıklarını ve işletmelerini hedef almaktadır"*, bu nedenle, *"emniyet kuvvetleri ve yargı, kripto para varlıklarının nasıl tanınacağı, izleneceği, el konulacağı ve kurtarılacağı konusunda bilgi geliştirmeye, paylaşmaya ve yaymaya devam etmelidir."*

Kripto para birimlerinin artık bir yenilik olmadığı gerçeğine rağmen, kullanıcıların kimliğini gizlemek için teknolojiyi kullanması, işlemlerin sınır ötesi doğası, finansal işlemlerle alakalı kimi zaman tutarsız olan düzenlemeler ve yasadışı faaliyetlerle uğraşırken uygulanan ulusal mevzuattaki tutarsızlıklar bu para birimini birçok suçlu için tercih edilir hale getirmiştir.

Sanal para birimlerinin dondurulması ve el konulmasına ilişkin kılavuzlar ulusal düzeyde mevcut olsa da, farklı zorluklara ilişkin en iyi uygulamaları ve çözümleri uluslararası bir bakış açısıyla içeren bir kılavuz, dünyanın dört bir yanındaki ülkelerde görev yapan birçok kamu görevlisi için faydalı olabilir.

Kripto para birimine ele koyma kılavuzu, iPROCEEDS-2 projesi Sonuç 4 kapsamında geliştirilmiştir: *"çevrimiçi suç gelirlerinin aranması, el konulması ve müsadere edilmesinde ve siber suçla mücadelede ve elektronik kanıtların güvence altına alınmasında yetkili soruşturma birimlerinin kapasitelerinin ve mali müfettişler, savcılar, istihbarat temsilcileri ve siber güvenlik uzmanları arasındaki kurumlar arası işbirliğinin daha da güçlendirilmesi."*

1.1 Gerekçe

iPROCEEDS-2 projesinin uygulanmasının ilk yılında, bu konuda kapasite geliştirme ihtiyacı olduğu için sanal para konusu birçok kez gündeme gelmiştir. Kripto para birimlerinin dondurulması ve el konulması için kılavuz ilkeler, konuya ilişkin mevzuat taslağı hazırlama desteğinin yanı sıra birkaç iPROCEEDS-2 proje ülkesi / bölgesi tarafından da talep edilmiştir.

1.2 Kılavuzun Amacı

Konuyla ilgili uluslararası uzmanlar tarafından hazırlanan Kılavuz, kripto para biriminin dondurulması ve el konulması ile ilgili bir dizi genel kuralın yanı sıra en iyi uygulamaları sunmaktadır.

Girişim, ulusal yaklaşımların ötesine geçmekte ve sanal para birimleri içeren suçları hedefleyen dünya çapındaki birçok ülkeye faydalı olacak uluslararası bir bakış açısı sağlamaktadır.

Böyle bir Kılavuz geliştirmenin beklenen sonucu, mali bir yönü olan ancak bunlarla sınırlı olmayan suçları hedefleyen tüm devlet kurumlarının kabiliyetlerinin artırılmasıdır.

1.3 Kılavuz Kimlere Yöneliktir?

Bu Kılavuz, emniyet kuvvetlerini, savcılar, hakimleri, Mali İstihbarat Birimlerini, Mali Soruşturma Birimlerini, adli bilişim uzmanlarını ve / veya eğitim kurumlarını desteklemeyi amaçlamaktadır.

Başlangıçtan itibaren bu Kılavuz, sanal para ile uğraşırken yerel makamlara adım adım direktifler sağlama ve bu tür bir varlıkla karşılaşıldığında farklı durumlarda (ev aramaları, tutuklamalar vb.) tüm soruşturma yetkilileri için bir araç olma amacını taşımaktadır.

2 El koymanın arkasındaki teori

2.1 Tanımlar (FATF/AB)

Bitcoin'in ortaya çıkışından bu yana, sanal para birimi ve blok zinciri teknolojisi için çeşitli tanımlamalar yapılmıştır. Bu konu, Avrupa Birliği düzeyinde ve uluslararası düzeyde, Uluslararası Para Fonu, Uluslararası Uzlaşma Bankası ve Mali Eylem Görev Gücü gibi çok sayıda politika yapıcı tarafından incelenmiştir. Bu politika yapıcılarının her biri konuya farklı bir şekilde değinmiştir, ancak Mali Eylem Görev Gücü'nün açıklaması dışında, bu terimlerin uluslararası kabul görmüş tanımları yoktur.

Farklı ulusal düzenlemelerin çeşitliliğini ve bu kılavuzun ulusal yaklaşımları aşan uluslararası bir kapsama sahip olacağını göz önünde bulundurarak, terimler için Mali Eylem Görev Gücü'nün ve Avrupa Birliği'nin tanımı kullanılacaktır.

2.1.1 "Sanal Para Birimi", "Kripto Para Birimi" ve "Sanal Varlıkların" Tanımı

I. Mali Eylem Görev Gücü

Mali Eylem Görev Gücü (FATF) Haziran 2014'te sanal para birimi raporunu yayınlamıştır.¹

Rapor, sanal para birimini itibari para biriminden ayırmıştır. İtibari para birimi, yasal olarak belirlenen ve düzenleyen bir ülkede bir değişim aracı olarak kabul edilen ve o ülkenin madeni parası ve kağıt parası olarak tanımlanan en çok kullanılan para türüdür.

Rapor ayrıca sanal para birimini, itibari para birimi cinsinden değeri elektronik olarak aktarmak için kullanılan ve dolayısıyla itibari para biriminin dijital bir temsili olan e-paradan ayırmaktadır. E-para, itibari para birimi için dijital bir transfer mekanizmasıdır - yani yasal değere sahip meblağı elektronik olarak transfer eder.

Sanal Para Birimi

- bir değişim aracının dijital bir temsilidir
- ve/veya bir hesap birimidir
- ve/veya bir tasarruf aracıdır
- ancak yasal para statüsüne sahip değildir
- basılmaz veya herhangi bir yargı makamınca garanti edilmez
- ve yukarıdaki işlevleri yalnızca sanal para biriminin kullanıcıları arasındaki anlaşmalar yoluyla yerine getirmez

¹ <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>

Kripto Para Birimi

- matematik tabanlıdır
- merkezi olmayan dönüştürülebilir bir sanal para birimidir
- kriptografi ile korunmaktadır
- değeri bir kişiden (birey veya kuruluş) diğerine aktarmak için genel ve özel şifrelere güvenir
- her aktarıldığında kriptografik olarak imzalanmalıdır

Rapor, çoğu Bitcoin'den türetilen yüzlerce (günümüzde on binlerce) kripto para birimi şartnamesinin tanımlandığını belirtmektedir.

FATF Tavsiyeleri, 2015 yılında buna sanal varlık tanımını da dahil etmiştir.²

Sanal Varlık

- değerini dijital bir temsilidir
- dijital olarak alınıp satılabilir veya transfer edilebilir ve ödeme veya yatırım amacıyla kullanılabilir.

FATF Tavsiyeleri, sanal varlıkların itibari para birimlerinin, menkul kıymetlerin ve diğer finansal varlıkların dijital temsillerini içermediğinin altını çizmektedir.

II. AB Kurumları

AB kurumları tarafından yapılan tanımlar, bazı küçük farklılıklar dışında, çoğunlukla FATF tanımlarına benzemektedir.

Avrupa Birliği Adalet Divanı, 22 Ekim 2015³ tarihinde Bitcoin'in varlık olarak değil, özel bir ödeme olarak kullanıldığını belirten bir ön karar vermiştir. Bu nedenle, bitcoin sanal para birimleri "yasal para birimleri olarak kullanılan döviz, banknot ve madeni paralarla" alakalı işlemlere ilişkin hüküm kapsamındaki KDV'den muaftır.

Avrupa Merkez Bankası (ECB), Şubat 2015⁴ tarihli analizinde tanımlandığı üzere sanal para birimlerini tam bir 'para' biçimi olarak görmemektedir. ECB, sanal para birimlerinin ekonomik veya yasal 'para' veya 'para birimi' tanımına uymadığını açıklamış ve kamuoyunda düşük düzeyde kabul gördüklerini kaydetmiştir.

ECB'nin raporuna göre,

Sanal para birimi

- değerini dijital bir temsilidir,
- bir merkez bankası, kredi kurumu veya e-para kurumu tarafından düzenlenmemiştir,
- bazı durumlarda paraya alternatif olarak kullanılır.

² <https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>

³ Case C-264/14, <http://curia.europa.eu/juris/liste.jsf?num=C-264/14>

⁴ <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>

Avrupa Bankacılık Otoritesinin (EBA) Ocak 2019⁵ tarihli kripto varlıklar hakkındaki raporu, 'kripto varlık' kategorisini oluşturan biraz farklı bir tanım sağlamaktadır.

EBA'nın raporuna göre,

Kripto varlık şu özelliklere sahip bir varlık anlamına gelir:

1. algılanan veya doğal değerinin bir parçası olarak öncelikle kriptografiye ve dağıtık hesap defteri teknolojisine (DLT) veya benzer bir teknolojiye bağlıdır,
2. bir merkez bankası veya kamu otoritesi tarafından basılmaz veya garanti edilmez ve
3. takas aracı olarak ve / veya yatırım amacıyla ve / veya bir mal veya hizmete erişmek için kullanılabilir.

EBA'nın tanımları, 'kripto varlık' terimi altındaki sanal para birimlerini ve madeni paraları içermektedir.

Avrupa Parlamentosu'nun "Kripto para birimleri ve blok zinciri" adlı çalışması, sanal para birimlerini kripto para birimleri olarak tanımlamaktadır.⁶

Avrupa Parlamentosu'nun araştırmasına göre,

Kripto para birimleri;

1. değer dijital bir temsildir
2. merkezi değildir, yani bir merkez bankası veya bir kamu otoritesi tarafından basılmaz veya garanti edilmez
3. yasal olarak belirlenmiş bir para birimine bağlı değildir
4. yasal kur veya para statüsüne sahip değildir
5. elektronik olarak devredilebilir, depolanabilir ve ticareti yapılabilir

Beşinci Kara Para Aklamanın Önlenmesi Yönergesinde (Gerekçe 10)⁷ Avrupa Komisyonu, direktifin kapsamına sanal para platformlarını ve cüzdan sağlayıcılarını dahil etmiş ve sanal para birimlerinin tanımını oluşturmuştur.

Beşinci AML Direktifine göre,

Sanal para birimleri

- değer dijital bir temsildir
- bir merkez bankası veya bir kamu kurumu tarafından basılmaz veya garanti edilmez, yasal olarak belirlenmiş bir para birimine bağlı değildir ve yasal bir kur veya para statüsüne sahip değildir
- ancak gerçek veya tüzel kişiler tarafından bir değişim aracı olarak kabul edilir ve elektronik ortamda devredilebilir, depolanabilir ve ticareti yapılabilir.

⁵ <https://eba.europa.eu/sites/default/documents/files/documents/10180/2545547/67493daa-85a8-4429-aa91-e9a5ed880684/EBA%20Report%20on%20crypto%20assets.pdf?retry=1>

⁶

<https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf>

⁷ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843>

Beşinci AML direktifi, sanal para birimlerinin AB Elektronik Para Direktifi (2009/110 / EU) kapsamında elektronik para ve İkinci AB Ödeme Hizmetleri Direktifinde (2015/2366 / EU) tanımlanan daha geniş fon kavramı ile karıştırılmaması gerektiğini de vurgulamaktadır.

Özet

Yukarıdaki tanımlara göre, **sanal para birimi**:

- itibari para biriminden (yani gerçek para birimi, gerçek para veya ulusal para birimi) farklıdır
- e-paradan farklıdır
- dijital para biriminin bir alt kategorisidir

FATF, AB tanımlarına dayalı olarak sanal para birimi ve kripto para birimi terimleri arasında bir ayrım yapmış olsa da, "kripto para birimi" terimiyle "sanal para birimi" çoğunlukla birbirinin yerine kullanılmaktadır.

Bununla birlikte, 'kripto varlık' terimi ile ilgili olarak, AB organları FATF tanımlarını kullanmaktadır. Avrupa Parlamentosu ve Konseyinin "Kripto Varlık Piyasaları Hakkında Yönetmelik" için mevcut teklifi, EBA'nın çalışmasına atıfta bulunmakla birlikte 'kripto varlıkların'⁸ herhangi bir tanımının, FATF'nin tavsiyelerinde verilen sanal varlıkların tanımına karşılık gelmesi gerektiğini ve kripto varlık hizmetlerinin herhangi bir listesinin, kara para aklama endişelerini artırma ihtimali olan ve FATF tarafından bu şekilde tanımlanan sanal varlık hizmetlerini de kapsamaması gerektiğini belirtmektedir.

2.1.2 Sanal para birimlerinin sınıflandırılması

"Sanal para birimi" teriminden ilk defa 2009 yılında bir CNN makalesinde bahsedildi ve bu terim hi5 jetonları ve "Second Life" Linden Doları veya "World of Warcraft" altınları gibi oyun para birimleri için kullanıldı.⁹ Bitcoin ağı Ocak 2009'da ortaya çıkmasına rağmen söz konusu makale bundan bahsetmemiştir.

Çeşitli çalışmalar, Avrupa Merkez Bankası'nın 2012¹⁰ bildirisi veya 2016'daki¹¹ IMF Tartışma Notu dahil olmak üzere sanal para birimlerini kategorize etmiş ancak FATF'nin sınıflandırması uluslararası düzeyde kabul edilmiştir.

Sanal para birimleri hakkındaki söz konusu FATF raporu, aşağıdakiler arasında ayrım yapar:

- Dönüştürülebilir sanal para birimleri,
- Dönüştürülemeyen sanal para birimleri,
- Merkezi sanal para birimleri,
- Merkezi olmayan sanal para birimleri.

Dönüştürülebilir (veya açık) sanal para birimi,

- Gerçek para birimi cinsinden eşdeğer bir değere sahiptir ve,
- Gerçek para birimi ile karşılıklı olarak değiştirilebilir.

Çalışma, bazı dönüştürülebilir sanal para birimlerinin doğrudan veren yönetici aracılığıyla takas edilebileceğinin, diğerlerinin ise sanal bir para birimi değiştiricisi aracılığıyla takas edilmesi gerektiğinin altını çizmektedir. Bitcoin, Litecoin, Ether, Second Life Linden Doları dönüştürülebilir sanal para birimleridir.

⁸ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593>

⁹ http://edition.cnn.com/2009/TECH/05/18/online.currency/index.html?eref=rss_tech

¹⁰ <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>

¹¹ <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>

Dönüştürülemez (veya kapalı) sanal para birimi

- belirli bir sanal etki alanına veya dünyaya özgü olması amaçlanmıştır,
- sadece bu sanal ortamda bir değeri vardır,
- belirli sanal alan veya dünya dışındaki itibari para birimi ile değiştirilemez.

Bu özel sanal dünya, Devasa Çok Oyunculu Çevrimiçi Rol Yapma Oyunu (MMORPG) veya çevrimiçi bir alışveriş sitesi (örneğin: Amazon Paraları için Amazon.com) olabilir.

Resmi olmayan, ikincil bir piyasanın, 'dönüştürülemeyen sanal para birimini' itibari para birimi veya başka bir varlık ile takas etme fırsatı sağlayabileceğini, ancak ilgili şirketlerin ortak uygulamaları ve bu ikincil piyasalara karşı yazılı yasaklayıcı önlemleri olduğunu belirtmekte fayda var.

Merkezi sanal para birimleri

- sistemi kontrol eden
- bir yöneticiye sahiptir

Bu yönetici para birimini çıkarır, kullanımı için kuralları belirler, merkezi bir ödeme defteri tutar ve para birimini dolaşımdan çekme yetkisine sahiptir.

Second Life Linden doları, World of Warcraft altını ve kötü şöhretli OneCoin, merkezi sanal para birimleridir.

Merkezi olmayan sanal para birimleri

- dağıtılmıştır
- açık kaynaktır
- matematik tabanlı uçtan uca sanal para birimleridir
- merkezi yönetim yetkisi yoktur

Bitcoin, Ether ve Litecoin, merkezi olmayan sanal para birimlerine örnektir.

Saadet zinciri gibi bazı dolandırıcılık sistemlerinin operatörleri, müşteri çekmek için madeni paralarını merkezi olmayan sanal para birimleri olarak tanıtmaktadırlar, ancak aslında sistemleri merkezi bir sistemdir.

2.1.3 "SVSS" nin tanımı

FATF Tavsiyeleri, 2015 yılında sanal varlık servis sağlayıcısı tanımını da kapsamına dahil etmiştir¹².

Tavsiyelere dayalı olarak, sanal varlık servis sağlayıcısı, bir işletme olarak başka bir gerçek veya tüzel kişi adına aşağıdaki faaliyet veya işlemlerden birini veya birkaçını gerçekleştiren herhangi bir gerçek veya tüzel kişi anlamına gelmektedir:

- sanal varlıklar ve itibari para birimleri arasında değiş tokuş yapan
- bir veya daha fazla sanal varlık birimi arasında değiş tokuş yapan
- sanal varlıkları aktaran
- sanal varlıkların veya araçların güvenliğini ve / veya yönetimini yapan
- sanal varlıklar üzerinde kontrol sağlayan

¹² <https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>

- bir sanal varlığın teklifi ve / veya satışı ile ilgili finansal hizmetlerin sağlanmasına katkı sunan

Bölüm 1.1.2'de bahsedildiği gibi, AB kurumları "sanal varlık" yerine "kripto varlık" terimini kullanmaktadır.

Avrupa Parlamentosu ve Konseyinin "Kripto Varlık Piyasaları Hakkında Yönetmelik" için mevcut teklifi (MiCA), kripto varlık için yeni bir tanım ve kripto varlık servis sağlayıcıları için yeni bir kategori oluşturmakla birlikte bunlar da daha önce atıfta bulunulan FATF Tavsiyelerinin tanımlarına dayanmaktadır.

2.1.4 Dağıtık Defterin tanımı

Dağıtık Defter Teknolojisi (DLT), iyi bilinen ve yaygın olarak kullanılan bir teknolojidir. Ancak, Avrupa Komisyonu'nun Ortak Araştırma Merkezi (JRC), Avrupa Merkez Bankası (ECB) gibi uluslararası kuruluşların terimle ilgili farklı bir tanımı vardır.

JRC'nin 2019'daki çalışmasına göre, DLT'ler verilerin kaydedildiği, paylaşıldığı ve dağıtılmış bir bilgisayar veya katılımcı ağı üzerinden senkronize edildiği belirli veritabanı türleridir.¹³

ECB'nin araştırma belgesine göre¹⁴dağıtık defter, bir ağ üzerinde paylaşılan bir bilgi kaydı veya veritabanıdır ve en iyi bilinen dağıtık defter türü "blok zinciridir". Araştırmaya göre, bu isim, bazı Dağıtık Defter Teknolojisi çözümlerinin tüm bireysel işlemleri, bir zincir oluşturmak üzere kronolojik sırayla birbirine bağlı gruplar veya bloklar halinde depolaması gerçeğinden gelmektedir. Bu uzun zincir, verilerin güvenliğini ve bütünlüğünü sağlayan karmaşık bir algoritma kullanılarak bir araya getirilmektedir.

ECB'nin raporu, dağıtık bir deftere erişimin sınırsız olabileceğinin altını çizmektedir yani, herhangi bir taraf katılımcı olabilmekte veya defter belirli bir kullanıcı grubuyla sınırlandırılabilir. Bu, ağ üyelerinin tüm deftere veya sadece bir kısmına erişebileceği anlamına gelmektedir. İzin haklarına bağlı olarak, üyeler daha sonra ağın diğer üyelerine dağıtılmak üzere veriler ekleyebilmektedir. Yalnızca yetkili kuruluşların güncelleme yapmasına izin vermek, ağ kötü niyetli kullanıcılardan veya işleyişini bozmaya çalışan harici saldırganlardan korumanın yararlı bir yolu olabilir.

2.1.5 Blok zinciri nedir?

JRC'nin çalışmasına bakıldığında, blok zinciri, DLT'lerin daha geniş anlamının bir parçasıdır. Blok zinciri teknolojisi, blok zincirlerindeki verileri kaydetmek ve senkronize etmek için kriptografik teknikler kullanmaktadır. Aradaki fark, verilerin dağıtılma, doğrulanma ve kaydedilme biçimiyle ilgilidir. Tüm blok zinciri türleri DLT'dir, ancak tüm DLT'ler blok zinciri değildir.

2017'deki Küresel Blok Zinciri Karşılaştırma Çalışmasına dayalı olarak, blok zinciri, uçtan uca (P2P) bir ağ üzerinden çoğaltılan bir veritabanı türüdür. Blok zinciri özeldir, çünkü birden fazla tarafın veritabanını paylaşmasına ve birbirlerine güvenmeseler bile güvenli bir şekilde değişiklik yapmalarına olanak tanıyan yeni bir veritabanı türüdür.¹⁵

Bitcoin blok zinciri, kronolojik sırayla Bitcoin işlemlerinin halka açık bir kayıdır. Bu blok zinciri daha sonra tüm Bitcoin kullanıcıları arasında paylaşılmaktadır. Bu sistem Bitcoin işlemlerini doğrulamak ve mükerrer harcamayı önlemek için kullanılmaktadır.

¹³ <https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/blockchain-now-and-tomorrow>

¹⁴ <https://www.ecb.europa.eu/pub/annual/special-features/2016/html/index.en.html>

¹⁵ Dr Garrick Hileman & Michel Rauchs tarafından hazırlanan Küresel Blok Zinciri Karşılaştırma Çalışması 2017, s. 13.

Birçok farklı web sitesinde ele alınabilir; örneğin: <https://explorer.bitcoin.com/btc>

2.2 Genel konseptler

2.2.1 İş ispatı nedir?

Bitcoin Wiki'ye göre, bir iş ispatı, (madenciler tarafından) üretilmesi zor (maliyetli, zaman alıcı) ancak başkaları tarafından doğrulanması kolay ve belirli gereksinimleri karşılayan bir veri parçasıdır.

Bir madencinin amacı, SHA-256 hashing ile önceden tanımlanmış bir dizine (bir dizi önde gelen sıfır) karşılık gelen rastgele bir sayı (yalnızca bir kez kullanılan bir sayı olarak adlandırılır) bulmaktır.

Bir madenci bir eşleşme bulursa, bloğunu Bitcoin ağına gönderir, böylece hashing (kriptografik özet) işleminin diziyi takip ettiğine dair her düğüm kendi çalışmasını kontrol edebilir. Bloğu bulmak zordur, doğrulamak nispeten kolaydır.

Örneğin:

Gerekli dizin: 9 önde gelen sıfır

Madenci tarafından kullanılan tek kullanımlık sayı: 2831785

Kriptografik işlemden sonra ortaya çıkan karma: 00000000a0e06c78b106b48d30b55bd2e5076aa13619072161145855b2eb93c

URL: <https://live.blockcypher.com/btc/block/00000000a0e06c78b106b48d30b55bd2e5076aa13619072161145855b2eb93c/>

Bitcoin ağı madenci bloğunu kabul ettiğinde, bu madenci yeni oluşturulan bitcoinlerle ödüllendirmektedir. Dolayısıyla, madencilik, blok başlığında tekrar tekrar hashing yapma ve istenen çıktıya bir eşleşme olana kadar bir parametreyi değiştirme işlemidir.

Önceki bloğun hashing değeri kriptografik fonksiyonda da kullanıldığından, her blok bir öncekine bağlanır. Bitcoin'de yaklaşık her 10 dakikada bir yeni bir blok çıkarılır ve bu blokların her biri, işlemlerin bellek havuzundan seçilen ve genellikle ücret adı verilen bir teşvikle yönlendirilen ve daha sonra madencinin de ödüllendirildiği bu zaman dilimine ait Bitcoin işlemlerini içermektedir.

Dizin her 14 günde bir (veya 2016 blokta) değişmektedir. Baştaki sıfırların sayısı, ağda mevcut olan hashing gücüne bağlıdır.

2.2.2 Hisse ispatı nedir?

Bu fikir birliği mekanizmasında, kullanıcıların bir işlem bloğunu doğrulamak için ağ tarafından seçilme şansına sahip olmak için bir miktar para veya madeni para yatırması gerekir. İş kanıtında olduğu gibi, seçilen hisse adresi yeni paralarla ödüllendirilmektedir dolayısıyla bu sistemin de bir teşviki vardır.

Bir kullanıcı cüzdanına ne kadar çok madeni para koyarsa, seçilme ve yeni para alma şansı o kadar artar.

Hisse ispatı, iş ispatına göre çok daha çevre dostu bir alternatif olarak kabul edilmektedir.

2.2.3 (Merkezi Olmayan Finansta) Yield Farming nedir?

Yield farming Ethereum ağında popüler bir uygulamadır ve bir şekilde bahis yapmaya benzer. Yield farming kullanıcıları tokenlarını (jetonlarını) merkeziyetsiz bir finans uygulamasında (DeFi) hisseler ya da kitlerler. Bunun karşılığında, bu DeFi uygulamasının yerel tokenını (jetonunu) ve işletim ücretlerinden bir pay alırlar. Her şey, yield farming kullanıcısının nasıl ödüllendirileceğine ilişkin DeFi uygulamasının türüne bağlıdır.

2.2.4 Genel-özel anahtar nedir?

Bitcoin gibi büyük kripto para birimleri, genel / özel anahtar çiftlerini kullanan asimetrik kriptografi üzerine kuruludur: genel anahtarlar herkese açıktır ve özel anahtarlar gizli tutulur.

Bitcoin için, genel anahtar, (eliptik eğri çarpımı olarak bilinen) tek yönlü bir kriptografik işlev aracılığıyla özel anahtardan türetilir. Bitcoin adresi, tek yönlü bir kriptografik karma işlevi aracılığıyla ortak anahtardan oluşturulur (aşağıya bakınız).

Özel anahtar sadece rastgele oluşturulmuş bir sayıdır. Özel anahtar üzerindeki kontrol, ilgili adresle ilişkili tüm fonlara erişim sağlar. Bitcoinleri harcamak için özel bir anahtar gereklidir.

Ancak, el koyma için özel anahtar(lar)ın üstünde bir şifre ya da PIN kodu gerekecektir (aşağıya bakınız).

2.2.5 Cüzdan nedir?

2.2.5.1 Tanım

Bir kripto para cüzdanı, genel ve özel anahtarları depolayan fiziksel bir donanım aygıtı, bir program veya bir hizmet olabilir. Kullanıcının parasına erişimi kontrol eden bir kullanıcı arayüzü olarak düşünülebilir.

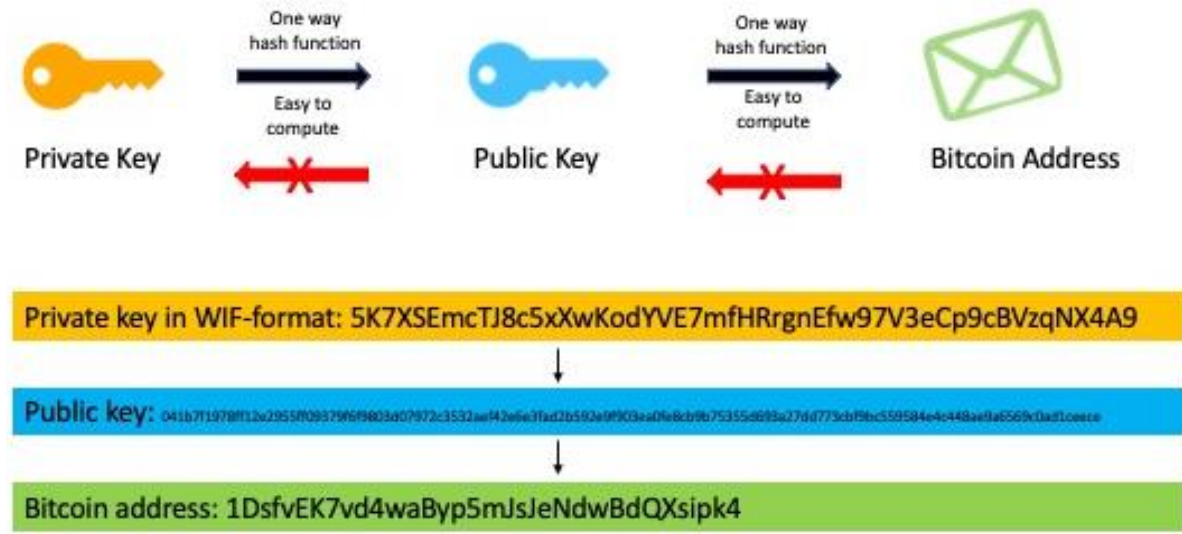
Günümüzde çoğu cüzdan, tüm anahtarların tohum (seed) olarak bilinen tek bir anahtardan ağaç benzeri hiyerarşik bir yapıdan türetildiği deterministik (ya da HD) cüzdanlardır.



Yukarıdaki ekran görüntüsü HD simgesini göstermektedir, Bitcoin Core (v0.20.1) cüzdanından alınmıştır. 2009'da başlayan Bitcoin'in ilk günlerinde mevcut olan tek cüzdan buydu ancak o zamanlar HD değildi (ve Bitcoin-Qt olarak adlandırılıyordu). Kullanıcıların bu cüzdanı çok sık yedekleme zorunluluğu vardır. HD cüzdanlar bu tür bir bakıma ihtiyaç duymazlar.

Kripto cüzdanlarının kripto para birimleri içerdiği konusunda bazen bir yanlış anlama vardır. Kripto cüzdanlar yalnızca kullanıcının kripto para birimlerini ilgili genel anahtarla harcamasına izin veren özel anahtarlar içerir.

Örneğin: Bitcoin Core'daki özel bir anahtar, kriptografik olarak bir genel anahtarla bağlantılıdır. Buna karşılık, bu genel anahtar, kriptografik olarak belirli bir bitcoin adresine bağlıdır. Özel anahtar, bitcoinleri bitcoin adresinde kontrol edebilir.



2.2.5.2 Emanetçi olan ve olmayan cüzdan

Emanetçi bir cüzdanda özel anahtarlar üçüncü bir tarafça tutulur. Bu, bir finans kurumu veya kripto para değişim platformu olabilir. Kendi kendine tutulan ya da saklanan kripto cüzdanı olarak da bilinen emanetçi olmayan bir cüzdan, kişilerin özel anahtarlarını/ kripto paralarını depolamalarına ve kullanmalarına izin veren cüzdan türüdür. Electrum, Ledger cüzdanı ve Jaxx Liberty emanetçi olmayan cüzdan türünün örnekleridir.

2.2.5.3 Çeşitler: masaüstü, mobil, donanım, kağıt, online

Kripto para birimi kullanımınıza bağlı olarak, birden fazla farklı cüzdan türüne sahip olabilir veya kullanabilirsiniz.

Masaüstü cüzdanlar, bunları genellikle günlük olarak kullanmayanlar tarafından bir bilgisayarda yerel depolama alanı olarak kullanılır.

Bunlar, genellikle bu cüzdanları tehlikeye atmak için özel olarak tasarlanmış farklı kötü amaçlı yazılım türleri nedeniyle daha az güvenli bulunan online (sıcak) cüzdanlardır.

Bu tür kötü amaçlı yazılımlara bir örnek Coinbitclip olarak adlandırılır. Bu kötü amaçlı yazılım, bir kullanıcı bitcoin gönderirken genel anahtarı değiştirmek için tasarlanmıştır. Truvalı, bitcoinlerin kötü amaçlı yazılımın bitcoin adresine gönderilmesiyle sonuçlanan çok benzer görünümlü bir Bitcoin adresi kullanır.

Bu masaüstü cüzdanlar müşterek bir cüzdan olarak da kullanılabilir. Örneğin, masaüstü cüzdanınızı cep telefonu uygulamanızda aynı anahtar kelimeyle kurarak kullanabilirsiniz.

Exodus cüzdan hem masaüstünde hem de mobil cihazda kullanılabilecek iyi bir cüzdan örneğidir. Yükleme işlemi sırasında, cüzdanı başka bir cihazda aynı anahtar kelimelerle geri yüklersiniz ya da bir mobil cihaz ile QR kodunu tarayabilirsiniz, böylece iki cüzdan da senkronize edilecektir.

Mobil cihaz cüzdanları günlük kullanım durumunda daha fazla kullanılır. Bir kripto para büfesine (ATM'ye) gittiğinizde, istediğiniz adrese kripto para yatırmak için mobil cihazınızdaki QR kodu büfeye okutunuz. Ters durumda, cüzdandan kripto para satmak istiyorsanız, büfe tarafından verilen belirli bir miktarı büfe tarafından gönderilen adrese göndermek için büfenin verdiği QR kodu okutunuz.

Kağıt cüzdanlar, Bitcoin kullanıcılarının genellikle kullanmaya başladığı ilk cüzdan türüdür. Bu cüzdanlar genelde kağıda basılır ya da dijital olarak bir PDF dosyasında tutulurdu. Normal bir kağıt cüzdanda bir genel ve bir özel anahtarınız bulunur. Kağıt cüzdanla ilgili sorun, özel anahtar kısmen ya da tamamen yok edildiğinde kişinin tüm kripto paralara erişimini kaybetmesi ve böylece bu varlıkları korumanın güvenli bir yolu olmamalarıdır.

Kağıt cüzdanlar zaman zaman şüphelilerin evlerinde, ya bir QR kod ve ilişkili genel-özel anahtar çifti ile ya da basit bir metin biçiminde bulunabilir. Bunların her iki biçimde de tanınması çok önemlidir. Bir kağıt cüzdan kurma işlemi bu kılavuzun sonraki kısımlarında açıklanmaktadır.

Donanım cüzdanları, son zamanlarda bireysel kullanım için endüstri standardı haline geldi. Bu cüzdanlar, donanım düzeyinde şifreleme ve birçok farklı kripto para birimini depolamak için çok güvenli bir yöntem sağlarlar. Ledger donanım cüzdanının nasıl kurulduğu kılavuzun ilerleyen bölümlerinde açıklanmaktadır. Ledger veya Trezor gibi bir donanım cüzdanı kullanırken en önemli şey anahtar kelimelerini korumaktır. Anahtar kelimeleri yanlış girmek cüzdanınızı tehlikeye atar.

Son olarak, online veya sözde web cüzdanları bulunmaktadır. Bu kripto cüzdanları bir web tarayıcısında çalıştırılabilir. Bununla birlikte, bu cüzdanlar siber saldırılara veya (örneğin Coinbitclip trojan gibi) hırsızlıklara açık olduğundan burada büyük güvenlik endişesi vardır. Block.io ve blockchain.com bu web cüzdanlarına örnektir.

2.2.5.4 Anahtar Kelime

Bugünkü cüzdanlar, BİTCOİN İyileştirme Önerileri BIP0032 ve BIP0044 tarafından tanımlanan hemen hemen tüm hiyerarşik deterministik cüzdanlar (veya HD cüzdanlar)dır.

Bu HD cüzdanlar bir anımsatıcı oluşturan İngilizce kelime listesinden kurulan bir anahtar kelimeyi kullanırlar. Anımsatıcı, bir kripto para cüzdanının kurtarılması için gereken tüm bilgileri depolayan 12 ila 36 kelimelik bir dizidir.

HD cüzdanı ilk kez oluştururken, kullanıcıya 12 veya bazı durumlarda bu anahtar kelimeyi yaratacak 24 İngilizce kelime gösterilecektir.

Cüzdanın oluşturulduğu anda (anımsatıcının) tek bir yedeklemesi yeterlidir, çünkü anahtar kelime (anımsatıcı aracılığıyla) cüzdanın tüm özel anahtarlarını yeniden oluşturabilir.

İngilizce kelimeler ve anımsatıcılar BIP0039 standardının bir parçasıdır ve tam liste şu adreste mevcuttur: <https://github.com/bitcoin/bips/blob/master/bip-0039/english.txt>

Aşağıdaki kelime dizisi bir anımsatıcı örneğidir ve <https://iancoleman.io/bip39/#english> sitesinde oluşturulmuştur:

hurt toss large spider review donate execute coconut torch place small foil

Tüm Bitcoin İyileştirmek Önerileri (BIP)'nin listesini <https://github.com/bitcoin/bips> adresinde bulabilirsiniz.

2.2.5.5 İşlemler ve işlem ücretleri

Bir işlem, bir blok zincirinde kaydedilecek olan kripto para ekosistemindeki katılımcılar (veya cüzdanlar) arasında bir değer aktarımıdır. Örneğin, A bitcoin adresindeki (gönderen) 1 bitcoinin B bitcoin adresine (alıcı) gönderilmesidir. İşlem ücreti madenciler için finansal bir teşvik olarak kabul edilebilir.

Bununla birlikte, işlemlerin tüm ayrıntılarını (kelimenin tam anlamıyla) açıklamak bu kılavuzun amacı değildir. Sadece, bir işlemin şunlardan oluştuğunu hatırlatalım:

1. Bir işlem kimliği (kriptografik özet)
2. Gönderilen bitcoinlerin sayısı
3. İşlem ücreti
4. Gönderenin bir veya daha fazla işlem girdisi (UTXO'LAR)¹⁶ veya adres(ler)i
5. Bir veya daha fazla işlem çıktısı (bir veya daha fazla alıcı adresi ve muhtemelen bir veya daha fazla değişiklik adresi)

İki girdi ve iki çıktılı blockchain.com¹⁷ adresindeki örneğe bakınız. Bir çıktı ödeme olarak, diğeri değişim olarak kabul edilir:

Hash	3f8a389b807382e2ab85590a77df7de0de8de9bce05fdffcdc40...	2020-12-16 13:56
	bc1q3pzfmq0cvgdptnm0ur4dqwr5ymsnv6nn4... 0.00556857 BTC	bc1q3pzfmq0cvgdptnm0ur4dqwr5ymsnv6nn4... 0.02074681 BTC
	bc1q3pzfmq0cvgdptnm0ur4dqwr5ymsnv6nn4... 1.43478000 BTC	14ZyyYUBBfTD1BxaK4LHteYm28nm6onsH1 1.41947201 BTC
Fee	0.00012975 BTC (34.693 sat/B - 15.355 sat/WU - 374 bytes)	1.44021882 BTC UNCONFIRMED

2.3 Bitcoin

2.3.1 Bitcoin nedir?

Bitcoin 2009 yılında Satoshi Nakamoto tarafından oluşturulan, anlık ödemeler için kullanılabilen, bilinmeyen mucit veya Bitcoin mucitleri için bir takma ad olan bir varlık, protokol ve eşler arası bir ağıdır. Satoshi Nakamoto, merkezi bir banka veya devlet hazinesine başvurmadan işlemleri doğrulamak ve güvence altına almak amacıyla bilgisayar kodunu kullanmak için 2008'te bir atılım yapmıştır.

Bitcoin tanıtım kılavuzu 31 Ekin 2008'de yayınlandı, kılavuzu şu adresten indirebilirsiniz: <https://bitcoin.org/bitcoin.pdf>.

Bitcoin ağındaki işlemler bankalar veya devletler gibi aracılar olmadan yapılır ya da Nakamoto'nun özetlediği gibi; "elektronik paranın tamamen eşler arası versiyonu", "online ödemelerin bir finansal kurumdan geçmeden doğrudan bir taraftan diğerine gönderilmesine" izin vermektedir.

Her bitcoin adresinin bakiyesi, herkesin erişebileceği bir kayıt defteri olan Bitcoin blok zincirinde tutulur.

Bitcoin protokolü, para birimlerinin üretimini düzenlemek ve para transferini doğrulamak için çeşitli şifreleme teknikleri kullanır.

Bitcoin açık bir kaynaktır ve bu nedenle kodu kamu alanının bir parçasıdır. Hiç kimse bitcoine sahip değildir veya kontrol etmez ve eşler arası teknolojisi sayesinde herkes buna katılabilir.

Büyük harfle başlayan "Bitcoin", Bitcoin kavramını veya tüm ağı tanımlarken kullanılır. Küçük harfle başlayan "bitcoin" bitcoinleri bir hesap birimi olarak tanımlamak için kullanılır.

¹⁶ UTXO: *Unspent Transaction Output*. More info at: https://en.wikipedia.org/wiki/Unspent_transaction_output

¹⁷ <https://www.blockchain.com/btc/tx/3f8a389b807382e2ab85590a77df7de0de8de9bce05fdffcdc40df99cbfc5092>

2.3.2 Bitcoin tarihi

Bitcoin başlangıcından önce var olan kavramları ve teknolojileri kullanır. Örneğin, çalışma ispatı ve bir blok zincirinin (kayıt defteri) arkasındaki fikirler zaten mevcuttu. Zaman damgalarının ve hesaba dayalı bulmacaların kullanımı da yeni değildi. Bitcoin'in yaratıcısı Satoshi Nakamoto, zaten mevcut olan bu teknolojilere başvurdu. Dağıtılmış kayıt defteri konseptini önemli bir son dokunuş olarak ekledi ve Bitcoin'i bugünkü haline getirdi.

2.3.3 Altcoin (Alternatif Kripto Para) Nedir?

Altcoinler veya alternatif kripto paralar, Bitcoin olmayan diğer tüm kripto para birimleridir. Kripto para piyasasında binlerce altcoin vardır, <https://coinmarketcap.com/> gibi web sitelerinden bu alternatif kripto paraları görüntüleyebilirsiniz.

Ethereum, Litecoin, Monero vb. altcoin örnekleridir.

2.4 Ethereum

2.4.1 Ethereum'un temellerini ve Ethereum tabiatını bilmek neden önemlidir?

Ethereum ilk olarak 2013'te tanıtıldı ve Ethereum blok zinciri 2015'te yayınlandı. Bitcoin ile karşılaştırıldığında, Ethereum sadece bir kripto para birimi değildir. Ethereum platformu, her yerde ve Bitcoin'de olduğu gibi yürütülebilen kod ve bilgisayar programlarını saklamak için yapılmış merkezi olmayan bir blok zinciridir; merkezi olmayan yapısından dolayı kapatılamaz.

Ethereum, Turing-complete komut dizisini çalıştırabilen ve merkezi olmayan uygulamaları çalıştırabilen Ethereum Virtual Machine (EVM) adı verilen merkezi olmayan bir çoğaltılmış sanal makineye sahiptir.

Ethereum, Coinmarketcap.com'a göre piyasadaki en popüler ikinci kripto para birimidir. Şimdiye kadar yayınlanmış tüm verileri farklı proje ve kodlarda depolayacak bir Ethereum arşiv düğümü çalıştırabilir, ancak bu yaklaşık 4 ila 5 terabayt depolama alanını kaplayacaktır. Ethereum blok zincirinin kendisi hâlâ 200 gigabayttan daha azdır, ancak bunlar sadece doğrudan blok zincirinde saklanan işlemlerdir.

Akıllı Sözleşmeler

Akıllı sözleşmeler, iki taraf arasındaki hüküm ve koşulların kodun kendisinde yazıldığı kendiliğinden uygulanan sözleşmelerdir. Ethereum blok zincirinin akıllı bir sözleşme ile kullanımı şöyle açıklanabilir: bir araba satın almak istediğinizi ve ödeme planının Ethereum sözleşmesinde tutulduğunu hayal edin. Son ödemeyi yaptıktan sonra, sözleşmeyi kapatmak için aracınızın belgelerini Gönderen son adımı sözleşme kendi kendine yürütür.

Öncü Koin Arzı (ICO)

Ayrıca, birkaç yıl önce, Ethereum ağı, öncü halka arzın (IPO) dijital eşdeğeri olan öncü koin arzı platformu olarak kullanılmaya başlandı. Sadece birkaç ay içinde, birçok farklı proje, herkesin ethereum veya hatta bitcoin ile satın alabileceği kendi yerel tokenlarını (jetonlarını) (ERC-20 tipi tokenlar) yarattı.

Hesaplar ve işlemler

Ethereum ve Bitcoin arasındaki temel fark, hesabın "durum değişikliğini" başlatan bir Ethereum işlemi için, yalnızca bu durum değişikliğini yaratan veya başlatan tam ethereum miktarını göndermesi gerektiğidir. Bitcoin'de olduğu gibi fazla bir değişiklik (adres değişikliği) oluşturulmaz, çünkü sadece

gerekli miktar gönderilecektir. Ayrıca, bitcoin işlemlerine kıyasla işlem kilobitlerinden de tasarruf sağlar. Bir işlemden sonra, değer ether hesabınızdan (genel-özel anahtarları da kullanan hesaplardan) düşülür.

2.4.2 Ethereum nedir?

Basit bir ifadeyle, Ethereum, eter (ETH) ve birçok farklı Ethereum tokenının (jetonunun) bir ödeme aracı olarak kullanıldığı veya akıllı bir sözleşmede uygulandığı açık kaynaklı bir blok zinciri platformudur.

2.4.3 Ether nedir?

Ether, Ethereum'un yerel kripto para birimidir. Bitcoin'de olduğu gibi değer depolar, ancak sadece ether cüzdanınızın durumu değiştiğinden transferleri daha "ekonomik"tir.

2.4.4 ERC-20 nedir?

ERC-20, tüm ERC-20 tokenlarının (jetonlarının) bulunduğu Ethereum blok zincirindeki akıllı sözleşmeler için bir Ethereum standardıdır. ERC-20 tokenlarının (jetonlarının) tam listesine şu adresten erişebilirsiniz: <https://etherscan.io/tokens>.

Bu tokenları (jetonları) göndermek için, cüzdanda az miktarda ethereum (ETC) olması gerekir.

2.4.5 Ethereum akıllı sözleşmeleri nasıl çalışır?

Yukarıda açıklandığı üzere, akıllı bir sözleşme, belirli koşullar yerine getirildiğinde önceden belirlenmiş bir eylemi kendi kendine gerçekleştiren güvenilir bir programdır. Örneğin, bu "eylem", bir veya daha fazla çalışana aylık ödeme yapan veya bir şirketin tedarik zincirindeki bir adımı güncelleyen bir Ethereum işlemi olacaktır.

2.5 Kripto paraların regülasyonu

2.5.1 FATF (Mali Eylem Görev Gücü) seyahat kuralı

2019'te FATF, FATF gereksinimlerinin Sanal Varlıklar ve Sanal Varlık Servis Sağlayıcıları ile ilgili olarak nasıl uygulanması gerektiğini daha da açıklığa kavuşturmak için Interpretive Note to Recommendation 15'i kabul etti. Haziran 2020'de, FATF sanal varlıklar ve sanal varlık servis sağlayıcıları için revize edilmiş FATF standartlarının 12 aylık bir incelemesini kabul etti (VASP'ler)¹⁸.

Bu belgelerde FATF, sanal varlıklardan kaynaklanan riskleri yönetmek ve azaltmak için, ülkelerin sanal varlık servis sağlayıcılarının AML/CFT amaçları doğrultusunda düzenlenmesini ve lisanslı veya kayıtlı olmasını ve FATF Tavsiyelerinde belirtilen ilgili önlemlerin izlenmesi ve uygunluğunun sağlanması için etkili sistemlere tabi olmasını sağlaması gerektiğini belirtmektedir.

Önleyici tedbirlerle ilgili olarak, sanal varlık servis sağlayıcılar (VASP'ler) aşağıdaki niteliklere tabidir:

- VASP'lerin müşteri durum tespiti yapmak için gerekli olduğu eşiğin üzerinde belirlenen ara sıra işlemler 1.000 USD / EUR'dur
- Ülkeler, kaynak VASP'lerin gerekli ve doğru kaynak bilgilerini ve sanal varlık transferlerine ilişkin gerekli yararlanıcı bilgilerini alıp tutmasını sağlamalı ve talep edildiği takdirde, bunları uygun yetkililere sunmalıdır.

¹⁸ <http://www.fatf-gafi.org/media/fatf/documents/recommendations/12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf>

2.5.2 AMLD5 ve ulusal kanunlardaki uygulamalar

Beşinci Kara Para Aklama Direktifi'nde (5th AMLD), Avrupa Komisyonu, direktifin kapsamını sanal para birimi platformlarına ve cüzdan sağlayıcılarına kadar genişletti ve sanal para birimlerinin AB Elektronik Para Direktifi (2009/110/AB) kapsamında elektronik para veya revize edilmiş İkinci AB Ödeme Hizmetleri Direktifi (2015/2366/AB) kapsamında daha büyük fon kavramı ile karıştırılmaması gerektiğini belirtmektedir.

Komisyon, inovasyona izin vermek, ancak finansal istikrarı muhafaza etmek ve yatırımcıları korumak için kripto varlıklar hakkında bir çerçeve önermektedir çünkü kripto varlıkları bir hizmete erişim anahtarı olarak hizmet edebilir, ödemeleri kolaylaştırabilir veya finansal araçlar olarak tasarlanabilir.¹⁹

Komisyon, halihazırda AB Mevzuatı tarafından yönetilen kripto varlıkları ile piyasa katılımcılarının ve düzenleyicilerin DLTs borsalarının kullanımıyla deneyim kazanmalarını sağlayacak diğer kripto varlıkları arasında ayırım yapmaktadır. Komisyon, kripto varlık formunda finansal araçlardaki işlemlerde ticaret yapmaya ve işlemleri çözümlemeye çalışmak isteyen piyasa altyapıları için bir pilot rejim önermektedir.

2.5.3 AB Dijital Finans Paketi: Kripto varlıklara ilişkin yasal öneriler, fırsatları ele geçirme ve riskleri azaltma

Dijital Finans Paketi

24 Eylül 2020'de, Avrupa Komisyonu Dijital Finans Paketi'ni kabul etti. Teklifin amacı, AB finans sektörü için yeni bir dijital finans stratejisinin temellerini atmaktır ve temel hedefi, AB'nin dijital devrimi benimsemesini ve dijital finansın faydalarını Avrupalı tüketiciler ve işletmeler için erişilebilir hale getirerek yenilikçi Avrupalı firmalarla birlikte yönlendirmesini sağlamaktır. Komisyon, dijital dostu kurallar koyup bunları tüketiciler için güvenli hale getirerek, ilgili riskleri ele alırken yüksek yenilikçi girişimler ile finans sektöründeki müesses firmalar arasındaki sinerjiden yararlanmayı amaçlamaktadır.

Bu teklifin, Avrupa Birliği'ndeki tamamen sanal para birimi ile ilgili ilk düzenleyici teklif olduğunu belirtmek gerekir.

Kripto varlıklara ilişkin yasal öneriler

Komisyon, inovasyona izin vermek, ancak finansal istikrarı muhafaza etmek ve yatırımcıları korumak için kripto varlıklar hakkında bir çerçeve önermektedir çünkü kripto varlıkları bir hizmete erişim anahtarı olarak hizmet edebilir, ödemeleri kolaylaştırabilir veya finansal araçlar olarak tasarlanabilir.²⁰

Komisyon, halihazırda AB Mevzuatı tarafından yönetilen kripto varlıkları ile piyasa katılımcılarının ve düzenleyicilerin DLTs borsalarının kullanımıyla deneyim kazanmalarını sağlayacak diğer kripto varlıkları arasında ayırım yapmaktadır. Komisyon, kripto varlık formunda finansal araçlardaki işlemlerde ticaret yapmaya ve işlemleri çözümlemeye çalışmak isteyen piyasa altyapıları için bir pilot rejim önermektedir.

Komisyon, inovasyona izin vermek, ancak finansal istikrarı muhafaza etmek ve yatırımcıları korumak için kripto varlıklar hakkında bir çerçeve önermektedir çünkü kripto varlıkları bir hizmete erişim anahtarı olarak hizmet edebilir, ödemeleri kolaylaştırabilir veya finansal araçlar olarak tasarlanabilir.²¹

Komisyon, halihazırda AB Mevzuatı tarafından yönetilen kripto varlıkları ile piyasa katılımcılarının ve düzenleyicilerin DLTs borsalarının kullanımıyla deneyim kazanmalarını sağlayacak diğer kripto varlıkları

¹⁹ https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en

²⁰ https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en

²¹ https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en

arasında ayırım yapmaktadır. Komisyon, kripto varlık formunda finansal araçlardaki işlemlerde ticaret yapmaya ve işlemleri çözümlemeye çalışmak isteyen piyasa altyapıları için bir pilot rejim önermektedir.

2.5.4 MiCA (Kripto Varlıklarda Piyasalar) kılavuzu

Komisyon, Dijital Finans Paketi'nin bir parçası olarak, Kripto Varlıklarda Piyasalar (MiCA) ile ilgili önerisini yayınladı. Teklif, **kripto varlıklarının** ihracı ve **kripto varlık servis sağlayıcılarının** sağlanmasına odaklanmaktadır.²²

MiCA'nın hedefleri, kripto varlık endüstrisine daha geniş bir uygulama alanı sağlamak için tek tip gereksinimler oluşturmaktır.

Bu gereksinimler şunlardır:

- şeffaflık ve açıklama
- yetkilendirme ve denetim
- operasyon, organizasyon ve yönetim
- tüketicinin korunması
- piyasanın kötüye kullanımının önlenmesi

Teklif göre,

kripto varlık

- değer ya da hakların dijital bir temsilidir
- elektronik olarak transfer edilebilir ve saklanabilir
- dağıtılmış kayıt defteri ya da benzer bir teknolojiyi kullanır

Teklif şu araçların **kripto varlık olmadığı** altını çizer:

- MiFID II finansal araçları
- EMD2 elektronik para
- depozitolar
- yapısal depozitolar
- seküritizasyon

Teklif **stabil kriptoparalar** arasında ayırım yapar ve iki yeni kategori yaratır:

- varlık referanslı tokenlar (jetonlar)
- elektronik para tokenları (jetonları)

Tüm kripto varlıkları için çok sayıda hüküm geçerlidir. Varlık referanslı tokenlar veya e-para tokenları olarak kategorize edilen sabit kripto paralar için daha katı gereksinimler geçerlidir. En katı gereklilikler, Avrupa Bankacılık Otoritesi tarafından önemli olarak belirlenen stabil kripto paralar için geçerlidir.

Teklif ayrıca **kripto varlık ihraççıları** için şunları belirtmektedir:

- tüzel kişilik olarak dahil edilmeleri
- herhangi bir ihraçtan önce, bir tanıtım belgesi yazıp yayınlamaları
- ve pazarlama standartlarına uyum sağlamaları

²² <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593>

MİCA ayrıca, tanıtım belgelerinin öngörülen minimum bilgileri içermesi gerektiğini, ancak varlık referanslı tokenlar (jetonlar) veya e-para tokenları (jetonları) ile ilgili olmadıkça herhangi bir kurum tarafından önceden onaylanması gerekmediğini belirtti. Bununla birlikte, varlık referanslı tokenlar ve e-para tokenlarının ihraççıların bir düzenleyici tarafından yetkilendirilmesi gerekecektir.

Teklifeye dayanarak, listelenen hizmetler servis sağlayıcı olarak MİCA altında düzenlenecektir.

Tanımdaki kripto varlık hizmet sağlayıcıları şunlardan sorumludur:

- kripto varlıkların gözetimi ve yönetimi
- kripto varlıklar için bir ticaret platformunun işletilmesi
- fiat para birimi için kripto varlıklarının değişimi
- diğer kripto varlıkları için kripto varlıklarının değişimi
- üçüncü taraflar adına kripto varlıklar için emirlerin yerine getirilmesi
- kripto varlıkların yerleştirilmesi
- kripto varlıklar için siparişlerin alınması ve iletilmesi; ve kripto varlıklarla ilgili tavsiyeler

MİCA kripto varlık servis sağlayıcılarının tüzel kişiler olarak kurulması ve yetkilendirilmesi gereken faaliyet kümelerini tanımladı; bu şirketler, müşteri varlıklarının korunması, piyasa kötüye kullanımı ve ihtiyati gereklilikler gibi düzenleyici hükümlere uymak zorundadır.

2.6 Kripto paranın kullanımı aşağıdakileri içerir ancak bunlarla sınırlı değildir

2.6.1 Darknet (Karanlık internet) pazarları

Darknet pazarları, Bitcoin ve diğer kripto paraların ilk gerçek kullanımlarını almış olabileceği yerlerdir. Ünlü İpek Yolu 2011'de başladı ve tamamen yeni bir suç kategorisinin başlangıcı oldu. Bazıları, İpek Yolu'nun kurulmasının aslında Bitcoin'e ve daha sonra diğer kripto paralara ilk değeri verdiğini söylemekte. Aklınıza gelebilecek her şeyi darknet pazarlarından satın alabilirsiniz (uyuşturucu, gerçek/sahte pasaportlar ve ehliyetler, sahte para, kredi kartı bilgileri vb. gibi çoğunlukla yasadışı mal ve hizmetler). Bu pazarlara erişmek için, genellikle şifreleme yoluyla kullanıcıyı anonim ve görünmez kılan Tor veya I2P gibi özel anonimleştirme yazılımı yüklemeniz gerekir. Darknet pazarları, genellikle, pazar sahibinin emanet hesaplarında bulunan tüm fonlarla kaçtığı çıkış dolandırıcılıklarında bir veba yaşıyor. Son emniyet işlemleri, yöneticileri tutuklayıp suçlayarak ve kripto paralarına el koyarak bu pazarları aşağı çekti.

Bu işlemlere rağmen, Dark Web'de hâlâ (artan) sayıda darknet pazarı var. Bu pazarların çoğu Bitcoin'i kabul ederken, daha fazla gizlilik/güvenlik odaklı bazı pazarlar sadece Monero'yu kabul ediyor.

2.6.2 Fidyeye Yazılımı

2020, fidye yazılımının yılı olarak adlandırılmakta. Fidyeye yazılımı ödemelerinin %50'den fazla arttığı ve kampanyaların daha fazla hedeflendiği tahmin edildi. Fidyeye yazılımı mağdurun bilgisayar veya ağını şifreler ve bitcoin şeklinde bir fidye ister. Bu fidye talepleri yüzlerce dolar ile milyonlarca arasında olabilir. Temmuz 2020'de, Garmin, NetWalker adında bir fidye yazılımından zarar gördü ve talebin 11 milyon dolar olduğu tahmin edildi. Bu aktörlerden bazıları yaptırımları atlatmak için devlet aktörleri ve gasp mağdurları olabilir (DPRK). Şirket veya birey, bu aktörlere ödeme yaparak çeşitli kripto para adreslerini ve aktörlerini aktif olarak kara listeye alan OFAC tarafından belirlenen yaptırımları ihlal edebilir.

2.6.3 Şantaj

Son birkaç yılda, mevcut veri ihlallerinin toplam miktarı nedeniyle birçok farklı kripto para şantajına şahit olduk. Tipik şantajlar, esasen kişinin mağdurun gerçek adını ve bir ihlalde bulunan gerçek bir şifreyi belirten bir e-mail alması şeklinde gerçekleşir. E-mail şantajcının mağdurun bazı videolarını ele geçirdiğini söyler ve bu verileri akrabalarına, iş yerine iletmemek ve sosyal medyada yayınlamamak için birkaç yüz dolar bitcoin ister. Bunların çoğunun gerçek olduğuna dair bir kanıt yoktur; ancak bazı durumlarda, web kameraları önünde uygunsuz şeyler yaptıkları görülen bazı mağdurların hacklenmiş Wİ-Fİ ağları aracılığıyla tehlikeye atıldığı fark edildi. Fakat bu "gerçek" olaylar çok nadiren gerçekleşti.

2.6.4 Hortumlar (dolandırıcılık)

Hortumlar genel olarak, halk tarafından tanınan kişiler tarafından bile reklamı yapılan, kripto ile ilgili yatırım fırsatları veya "sahte" öncü koin arzlarıdır (ICO'lar). 2019'da, PlusToken adlı en büyük hortumlardan biri tahmini 6 milyar dolarlık kazanç elde ettiği kaydedildi. PlusToken hortumu tedavüldeki tüm bitcoinlerin %1.1'inden fazlasını kontrol etti. Bu hortumlar, çoğunlukla fintech yatırımcılarını ya da sadece FinTech dalgasını sürmek isteyen ve açgözlülükle beslenen sıradan insanları hedef almakta. Ayrıca, ünlülerin ve hatta kraliyet ailesinden isimlerin bu yatırım fırsatlarını teşvik etmek için sahte kampanyalarda kullanıldığı görülmüştür.

2.6.5 Saadet zincirleri

Bitcoin aldatmacası, yeni hortum tiplerini örneğin OneCoin gibi "bitcoin görünümlü" saadet zincirleri yarattı. OneCoin'ler Çok Katmanlı Pazarlama sistemiyle çalıştırılır. Pop-up'lar, YouTube videoları ve Facebook grupları ile reklamları yapıldı ve ayda % 15-25 gibi gerçekçi olmayan bir getiri vaat ettiler. Bu pazarlama materyallerinde OneCoin ile Bitcoin karşılaştırıldı ve yeni bir blok zinciri teknolojisi kullanıldığı belirtildi. OneCoin müşterileri çekmek için merkezi olmayan bir sanal para birimi olarak tanıtılırken; sistem aslında madeni parayı tedavüle çıkaran, ağ kurallarını belirleyen ve para birimini tedavülden çekme yetkisine sahip olan merkezi bir yönetim ekibi ile merkezileştirildi. OneCoin 4 milyar dolar kazanç getirmeyi başardı ve Times dergisi tarafından "tarihin en büyük dolandırıcılıklarından biri" olarak seçildi.²³

3 El koyma ile ilgili pratik kılavuzlar

Genel olarak, herhangi bir sanal paranın ele geçirilmesi veya müsadere edilmesi durumunda, aşağıdaki adımları belirleyebiliriz:

- El koyma öncesi planlama
- Bilgi toplama ve/veya sanal paranın izini sürmek
- Sanal paraların kontrolünü ele geçirmek
- Güvenli sanal paraların yönetimi ve elden çıkarılması

3.1 El koyma/ müsadere nedir?

El koyma veya müsadere, bir suç mahallinde bulunan kanıtlara el konması gibi, suçla ilgili varlık veya kanıtların yasal süreçle veya zorla alınması eylemidir.

Avrupa Birliği'nde, AB'deki suç araçlarının ve gelirlerinin bloke edilmesi ve müsadere edilmesine ilişkin 2014/42 /EU Yönergesi, suç gelirlerinin izlenmesi, bloke edilmesi, yönetilmesi ve müsadere edilmesi için emniyet kuvvetlerinin kapsamını genişletmektedir. Yönerge, Üye Devletlerin, gıyaben yapılan işlemlerden de kaynaklanabilecek bir suç için nihai bir mahkumiyete tabi olarak, bu tür araçlara veya

²³ <https://www.thetimes.co.uk/article/the-4bn-onecoin-scam-how-crypto-queen-dr-ruja-ignatova-duped-ordinary-people-out-of-billions-then-went-missing-trqr52pq>

gelirlere karşılık gelen araç ve gelirlere veya mülklere el konulmasını sağlamak için gerekli önlemleri almaları gerektiğinin altını çizmektedir.²⁴

3.1.1 Kripto varlıklar ve normal varlıklar

Kripto varlıkları ile normal varlıklar arasındaki temel fark, –özellikle merkezi olmayan sanal para birimlerinde– sistemde genellikle merkezi olmayan bir otorite bulunmamasıdır ve işlemlerin geleneksel olarak izlenmesi bir seçenek değildir.

Bu, şüphelinin finansal kayıtlarını kullanamayacağımız anlamına gelmez: çok sayıda finansal kurum (örneğin, bankalar) sanal para ile ilgili işlemleri listeledi ve bu bilgi bazen, şüphelinin tercih edilen kripto değişimini tanımlamak için bir yol olabilir.

Fakat, el koyma, bloke etme ya da müsadere normal hallerden oldukça farklıdır.

3.2 El koyma öncesi planlama

3.2.1 Giriş ve yasal çerçeve

Kripto para ekosistemi küreseldir ve farklı ulusal düzenlemelerle sınırsızdır. Bu ağın dünyada ne kadar yaygın olduğunu gösteren Bitcoin ağı görseline <https://bitnodes.io> sitesinden erişebilirsiniz.

El koyma işlemi yapılırken, öncelikle kripto paraları ele geçirmek için belirli bir ülkede uygulanan geçerli yasalar olup olmadığını bilmek önemlidir. Sanal paralara el koymak için dünya çapında standartlar olmasına rağmen, idari uygulama ve mevcut içtihat hukuku her ülkede, hatta Avrupa Birliği Üye Devletlerinde bile farklıdır.

Muhtemelen dünyadaki bazı ülkelerde kripto paralara el konulmasıyla ilgili hiçbir yasa veya yasal çerçeve olmayacak. Diğer ülkelerde, ceza davalarında varlıklara (örneğin paraya) el koyma yasaları kripto paralar için de geçerli olacaktır.

Herhangi bir yasadışı davranışın (örneğin yasa dışı yollarla kanıt elde etme) ve prosedür hatalarının önüne geçmek için, kripto paralara el konulmasına yönelik geçerli yasal çerçeve ve prosedürleri anlamak önemlidir.

El koymanın geçerliliği her zaman aklınızda olsun. Mal varlığı geri alımının motivasyonu, dolandırıcılık ve hacklenme mağdurları için gelir elde etmek veya çeşitli suçlar yoluyla elde edilen yasadışı gelirleri suçlulardan almak gibi çeşitli şekillerde olabilir. Yasadışı gelirlere el konulmasının (miktarla bağlı olarak) bazı suçlular için hapis cezasından çok daha ağır bir ceza olabileceğini unutmayın. Bu son yorumla, suçlulardan gelen varlıklara el koymanın önemini vurgulamak niyetindeyiz. Genel olarak, emniyet kuvvetleri ve diğer ilgili hizmetler, suçlulardan yasadışı gelir elde etmek için daha fazla çaba ve zaman harcamalıdır. Başarı oranını artırmak için iyi bir hazırlık şarttır.

Özel (bir) anahtar(lar) ya da anahtar kelime aracılığıyla kripto paralara erişim örneğin masaüstü bir bilgisayarda (yani Electrum gibi emanetçi olmayan bir cüzdanda) kendi yerinde bulunabilir ya da aynı veya başka bir yargı alanındaki emanetçi bir cüzdanda online olarak saklanabilir.

Aslında, kripto paralar çeşitli şekillerde saklanabilir. Emanetçi cüzdanlara el koyma tekniklerinin emanetçi olmayan cüzdanlardan nasıl farklılaştığını daha sonra göreceksiniz.

²⁴ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0042>

Emanetçi olmayan cüzdanlardaki paralara el koymak çok daha zor olabilir, çünkü bu fonlar bir şüpheli ve nihayetinde onun suç ortakları tarafından kontrol edilecektir. Bu nedenle, emanetçi cüzdanlardaki sürece nazaran, fonlara el koymak için kontrolü ele almak çok daha zor olabilir. Tabii ki, SVSS'in (örneğin borsa) emniyet kuvvetleri ile işbirliği yaptığı göz önüne alındığında.

Bu nedenle, bir ele koyma işleminin başarılı bir sonuç vermesi için iyi bir hazırlık ve strateji uygun olacaktır.

Aşağıda, el koyma öncesi planlama aşamasında dikkate alınması gereken konuların ve en iyi uygulamaların kapsamlı olmayan bir özeti yer almaktadır.

3.2.2 Eğitim ve uzmanlık

Kripto para gelirlerine el koymak çok zor olabilir ve belirli bir düşünce yapısı gerektirir. Bu karmaşık yapısından dolayı, kripto paralara el koyma işleminin yetkili emniyet kuvvetleri tarafından ve mümkünse kripto paralara el koyma konusunda deneyimli (uzman) emniyet kuvvetleri tarafından yapılması tavsiye edilir.

Gerekli beceriler eğitim ve pratik yoluyla kazanılabilir. Ne kadar çok eğitim alınıp pratik yapılırsa o kadar iyidir.

Kripto paraları ele geçirmeyi kapsayan çeşitli eğitimler geliştirilmiştir. Bunlardan biri, 2019/2020 yılında EMPACT çerçevesinde geliştirilen eğitimidir. Bu "Cryptocurrency and Dark Web Investigations" yerinde eğitim paketi, Belçika, Avusturya, Norveç ve İspanyol polisinin yanı sıra EUROPOL, INTERPOL, SELEC, UNODC, ECTEG ve AGİT gibi çeşitli emniyet kuvvetleri ve uluslararası kuruluşlar tarafından geliştirilmiştir. Bu eğitim kapsamındaki derslerden birisi (Bitcoin Testnet vs. kullanarak) kripto paralara el koymayla ilgilidir. Bu eğitim paketi ECTEG'in malıdır ve emniyet teşkilatları aracılığıyla ECTEG'den talep edilebilir. Bugünlerde, Chainalysis gibi kripto paralar için izleme ve takip etme çözümleri sunan birçok özel şirket, kripto para temellerinden özel araştırma eğitimlerine kadar sertifikalı eğitim paketleri de sunmaktadır.

(Hem cezai hem de cezai olmayan davalarda) Kripto paranın artan kullanımı ve küresel kabulü nedeniyle, kripto paraya el konulmasıyla potansiyel olarak karşı karşıya kalabilecek emniyet kuvvetleri, kripto paranın kullanımıyla ilgili en azından en alakalı izleri tanıyabilmelidir. Daha yaygın kavramlar ve bu yeni teknolojilerin emniyet kuvvetleri içinde kullanımı konusunda farkındalık yaratmak önemlidir. Örneğin, emniyet yetkilileri QR kodları, anahtar cümleleri, genel ve özel anahtarları, kripto para adres formatlarını, cüzdanları vs. tanıyabilmelidirler.

El koyma amaçları bakımından, kripto paraların farklı adres formatlarının tanınması ayrıca önem arz eder. Bir emniyet görevlisi hangi kripto paranın kullanıldığını anlayamadığında, el koyma işlemi bu kripto paraları doğru adres formatına ve ilgili devlet kontrolündeki cüzdana aktarmak için bir sorun haline gelebilir. Örneğin, Bitcoin (1,3 ya da bc1 ile başlayan) bir Bitcoin adresine ve Ethereum (0x ile başlayan) bir Ethereum adresine gönderilmelidir.

Bilinmeyen bir adres formatı bulurken, hangi kripto paranın kullanıldığını bulmak için yararlı olabilecek araçlar (örneğin internette) vardır. Bazı kripto paraların çok sınırlı bir kullanım alanı vardır ve bunlara el koymak çok daha zordur.

El koyma işlemi gerçekleştirirken, kripto para cüzdanları ve farklı cüzdan türleri (mobil, emanetçi, masaüstü, donanım, kağıt) hakkında iyi bilgi sahibi olmak önemlidir. Bu kılavuzun ilerleyen kısımlarında, her bir cüzdan türü için el koyma işleminin nasıl gerçekleştirilebileceği ayrıntılı olarak ele alınacaktır. Bazı cüzdanlar sadece bir kripto para birimini desteklerken (ör. Bitcoin Core), bazıları da birden çok kripto para birimini destekler (ör. Exodus).

3.2.3 Ne aranıyor?

Kripto paralara el konulmasıyla karşılaşıldığında, birkaç özel şey aramak uygun olabilir. Örneğin;

- Kripto para adresleri/ genel anahtarlar
- Özel anahtarlar ve anahtar kelime listeleri
- QR kodlar
- PIN kodları
- Cüzdanlar
- Şifreler
- Madencilik ekipmanı
- vb.

Kripto parayla ilgili bu şeyler, örneğin bir ev araması esnasında bir binada ya da tutuklama sırasında şüphelinin üstünde bulunabilir. Birçok durumda, kripto paraların bulunma şansının yüksek olduğu önceden bilinecektir; fakat bazen kripto paraların varlığı beklenmedik şekilde ortaya çıkacaktır. Örneğin, kenevir tarlası bulmayı uman birisi bunun yerine bir madencilik çiftliği bulmuştu.

Yukarıda bahsedilen şeylerin çoğunun saklanması veya yok edilmesinin çok kolay olduğunu unutmayın.

Örneğin, nakit bir milyon Euro ile özel bir anahtar veya basit bir nottaki 12 kelimelik bir anahtarla erişilebilen aynı miktardaki bitcoin eşdeğeri arasındaki farkı düşünün.

Bir kapıyı çalmadan ya da bir zile basmadan önce bunu göz önüne almak önemlidir. Duruma bağlı olarak, belirli (hazırlık) önlemleri ve/veya taktikler gerekli olabilir (aşağıya bakınız - eylem planı).

Mümkünse, el koyma işlemini önceden hazırlamak ve şüphelinin hangi kripto paraları ve cüzdanlarını kullanabileceğini anlamaya çalışmak iyi bir uygulamadır. Bazen, önceden başlatılan bir soruşturma yoluyla, şüphelinin hangi kripto paraları kullandığına dair göstergelere ulaşılabilir. Örneğin, bir darknet satıcısı sahte ürünler satıyor ve bunların Bitcoin ile ödenmesi gerekmekte.

Genelde, Bitcoin'in ceza davasında kullanılması kuvvetle muhtemeldir. Ancak son zamanlarda, Monero ve Zcash gibi özel koinlerin kullanımı artmaktadır. Örneğin bazı darknet pazarları, sadece White House Market (Beyaz Saray Pazarı) gibi Monero gibi koinleri kabul etmekte.

Ayrıca, birçok durumda, kripto para cüzdanlarına erişimin şifreler veya PIN kodlarıyla korunacağı ihtimalinin yüksek olduğunu unutmayın. Bir cüzdana erişim açık ve kilitsiz olsa da, para transferi için bir şifre veya PIN'in gerekli olması muhtemeldir. Daha da önemlisi, kripto paralara el koymak ve bunları devlet kontrolündeki bir cüzdana göndermek için muhtemelen bir şifre veya PIN kodu gerekecektir. Bu nedenle, şifreleri ya da PIN kodlarını aramak gerekli olabilir. Şifre ya da PIN kodları, klavyenin altı, post-itler, ajanda gibi birçok yerde olabilir. Şifreler bazen bellek analizi gibi özel araştırma teknikleriyle de elde edilebilir. Donanım ve mobil cüzdanlar bir PIN koduyla korunabilir.

Yasal çerçeveye bağlı olarak bazı ülkelerde, bir şüpheliden kendi kendini suçlamaktan bahsetmeden şifre sormak mümkün olacaktır. Hatta bazı yargı bölgelerinde, şüpheli emniyet kuvvetleriyle işbirliği yaparsa cezai indirim bile alabilir.

Aynı durum anahtar cümleler için de geçerlidir. Bir anahtar ifade ile bir şifre (veya PIN) gereksiniminin atlanabileceğini bilmek çok önemlidir (aşağıya bakınız).

Bundan sonra, kripto parayla ilgili aranacak bazı şeylere dair genel bir bakış bulabilirsiniz.

İsim	Bitcoin	Ethereum	Ripple	Litecoin	Dash	Monero	Zcash
Kısaltma	BTC	ETH	XRP	LTC	DASH	XMR	ZEC
Adresin ne ile başladığı	1, 3, bc1	0x	r	L	X	4	t1, t3, z1, z3
Adres uzunluğu	26-35	42 hex	34	34	34	95	35 or 96
Özel anahtarın ne ile başladığı	5, L, K	rastgele	s, p	6, T	7, X	rastgele	K, L
Özel anahtar uzunluğu	51/52	64 hex	51/52	51/52	51/52	64 hex	51/52

3.2.4 Devlet kontrolündeki cüzdanlar

Bir hükümet ya da devlet kontrolü altında olan cüzdanlardır. Yasal çerçeveye bağlı olarak daha özel anlamda, bu cüzdan emniyet kuvvetleri, mahkeme, (soruşturma) yargıç, cumhuriyet savcısı, bir müsadere organı, varlık yönetimi ile uğraşan özel bir şirket veya hatta bir müzayede evinin kontrolü altında olabilir.

Yasal çerçeveye ve bir ülkenin geçerli el koyma prosedürlerine bağlı olarak, devlet kontrolündeki cüzdanların görünümü çeşitli biçimlerde olabilir. Örneğin, bir donanım cüzdanı, kağıt cüzdan, çoklu imza cüzdanı şeklinde olabilir veya varlık yönetimi, özel bir şirket veya müzayede evi gibi üçüncü bir tarafın kontrolü altında olabilir.

Bahsedildiği üzere, kripto paralara el konulurken, devlet kontrolündeki uygun bir cüzdanın uygun adresine gönderilmeleri gerekir. Örneğin, bitcoinlerin bir bitcoin adresine, Monero'nun bir Monero adresine gönderilmesi gerekir. Bazı cüzdanlar tek kripto parayı desteklerken, bazıları birden çok kripto para birimini destekler (yukarıya bakınız).

Mümkünse (yani, ilgili yasal çerçeveyi ve el koyma prosedürlerini dikkate alarak), bir kripto paraya el koyma durumuyla karşı karşıya kalındığı anda, uygun el koyma adres(ler)ini ve devlet kontrolündeki cüzdan(lar)ı önceden hazırlamak iyi olacaktır.

Not: el koyma adresi, ele geçirilen kripto paraların gönderileceği adrestir.

Hangi kripto paraların bulunacağına bağlı olarak; biri Bitcoin için, diğeri Monero için vb. gibi devlet kontrolünde birkaç cüzdan hazırlamak gerekebilir veya bu farklı cüzdanlar yerine çok para birimli bir cüzdan kullanılabilir. Bu cüzdan hazırlama süreci ülkeden ülkeye değişkenlik gösterir.

Bu nedenle, mümkünse, bu adreslerin/cüzdanların oluşturulması güvenli bir bilgisayar ortamında yapılmalıdır ve iç kuralların bir izdüşümü olarak yazılı bir adım adım kılavuza sahip olmanızı şiddetle tavsiye ederiz.

Şüpheli her bir el koyma veya müsadere için tek bir adres kullanılması tavsiye edilir.

Devlet kontrolünde bir cüzdanın oluşturulması

Bazı ülkelerde, el koyma adres(ler)i bir el koyma yetkilisi tarafından sağlanacak veya (varlık yönetiminden sorumlu) özel bir şirketin veya müzayede evinin web arayüzü aracılığıyla alınacaktır. Böyle durumlarda, el koyma amaçlı cüzdanlar oluşturmak için emniyet kuvvetlerine ihtiyaç olmayacaktır.

Diğer ülkelerde, bu tür cüzdanların oluşturulması ve güvenli varlık yönetimi, emniyet kuvvetlerinin kontrolü ve sorumluluğu altında olacaktır.

3.2.5 Yetkiler, karar verme yetkisi kimde?

Geçerli yasal çerçeveye göre, kripto para ele geçirilmesinden sorumlu olan kolluk kuvvetleri, doğru yetkilere sahip olmalıdır. Ayrıca bazı yargı bölgelerinde, kimin el koymaya karar verme yetkisine sahip olduğunu bilmek önemlidir.

Bu noktada sorulacak ilgili sorular şunlardır: bir el koyma işlemi için hangi yetkiler/mahkeme kararları gerekir? El koyma işlemine karar verme gücü kimdedir? vs.

Örneğin (yazılım cüzdanı içeren) bir bilgisayarın, donanım cüzdan cihazının ve bir kağıt cüzdana el konulmasının yeterli olmadığını anlamak da önemlidir. Ayrıca, (cüzdan içeren) bir DAT dosyası da yeterli olmayacaktır. Bir bilgisayara ya da donanım cüzdanına vs. el koymak kripto paralara el koymakla eşdeğer değildir.

Bu kılavuzda birkaç kez ifade edildiği gibi, **kripto paralara etkili şekilde el koymak için devlet kontrolündeki bir cüzdana işlem/transfer yapmak gerekli olacaktır.**

Ayrıca, bazı yargı bölgelerinde arama ve el koyma emrinin yanı sıra, ek yetkiler/mahkeme emirleri gerekebilir. Örneğin, el koyma amacıyla bir transfer yapılmasına izin veren bir mahkeme emri gerekebilir.

3.2.6 Suç ortaklarının farkında olun

Belirtildiği gibi, kripto paralara el konulurken, şüphelinin cüzdan(lar)ının bir veya daha fazla yedeklemesi (örneğin özel anahtarlar, anahtar cümleler) olabileceğinden, eylem hızı çok önemli olabilir ve suç ortaklarına, şüpheli aleyhine bir kanun yaptırımı eylemiyle karşı karşıya kaldıkları anda fonları devlet kontrolü dışındaki bir cüzdana transfer etmeleri talimatı verilebilir.

Bu nedenle, örneğin bir ev araması esnasında, şüpheliyi (ve akrabalarını) cep telefonu gibi herhangi bir iletişim cihazından derhal ayırmak ve şüpheliyi (ve akrabalarını) hiçbir kanıtın ortadan kaldıramayacağı veya dış dünyayla herhangi bir etkileşimin mümkün olmayacağı şekilde kontrol etmek önemlidir (aşağıya bakınız).

3.2.7 Strateji ve eylem planı

Stratejiler ve eylem planına ilişkin ipuçları daha önce açıklanmıştı.

Bu nedenler, kripto paralara el konulurken, neyin aranacağını anlamak ve el koymayla ilgili temel kavramlar hakkında iyi bilgi sahibi olmak önemlidir. Eğitim ve uygulama yoluyla bu bilgiler edinilebilir. Ayrıca, ülkeden ülkeye değişiklik gösteren uygulanabilir yasal çerçeveyi ve el koyma prosedürlerini iyi anlamak esastır. Kripto paralara el koymayla ilgili sonraki adım, mümkünse, el koyma için doğru yetkilere/mahkeme kararlarına karar verme ve bertaraf etme yetkisinin kimde olduğunu bilin.

El koyma öncesi planlamayla ilgili diğer bir önemli adım, ne aranacağını ve eylem planının nasıl olacağını açıklayabileceğiniz kısa toplantılar düzenlemektir.

Uygun ekipmanı hazırladığınızdan ve ekipte doğru yetenekli (uzman) meslektaşlarınız olduğundan emin olun.

Yine belirtmek gerek ki, el koyma işlemleri zaman ve planlama gerektirir. Bu yüzden, kapıyı tekmelemeden önce bununla bekleme.

El koyma işlemi farklı durumlarda gerçekleşebilir. Bazı durumlarda, iyi bir hazırlık yapma imkanı olur fakat bazen, kripto para bulunması beklenmeyen bir ev aranırken durum böyle olmaz.

Bu nedenle, mümkün olduğunca, müdahale için etkili bir strateji ve eylem planı belirlenmesi tavsiye edilir. Şüphelinin cüzdan(lar)ı erişilemez hale getirmesini veya kanıtları yok etmesini önleyecek bir müdahale şekli gereklidir. Örneğin, şüpheli bulunduğu yerde bir polis müdahalesinden endişe duyduğunda, şifreli bilgisayarı kapatabilir, akıllı telefon ve/veya cüzdan mobil uygulamasını kilitleyebilir veya emniyet kuvvetlerinden önce fonları transfer edebilecek bir suç ortağını uyarabilir.

Kolluk kuvvetleri bazı durumlarda, şüpheliyi rahatsız etmek için tuzak kurabilir.

Polis müdahalesi ideal olarak, şüphelinin herhangi bir manipülasyon yapmak için hiçbir yolu olmayacak şekilde yapılmalıdır.

Kripto paralara el konulurken zaman çok önemlidir. Mümkünse derhal harekete geçiniz. Devlet kontrolündeki bir cüzdana aktarıldıktan sonra kripto paralara etkin bir şekilde el konulacaktır.

Kripto para birimleri ve cüzdan tipinin (örneğin emanetçi cüzdan olup olmamasına) kullanıldığına bağlı olarak, el koyma işlemleri değişiklik gösterebilir ve farklı bir yaklaşım ile eylem planı gerektirebilir.

Notlar

Bazen, kripto paraların varlığı ve kullanımı sonradan, şüphelinin ofisinde cihazları adli tıp analizinden geçirilirken tespit edilecektir. Kripto paralar o an henüz transfer edilmediyse, bunlara el koymak hâlâ mümkün olacaktır.

Bazen, ekipman, uzman memur, yetki eksikliği vb. nedeniyle yerinde bir el koyma işlemi gerçekleştirmek mümkün olmayabilir. Bunu aklınızda tutun ve bu durumlardan kaçının.

Devlet kontrolündeki hangi cüzdanın ve/veya prosedürlerin kullanılacağına bağlı olarak, yazım hatalarını önlemek için el koyma adresini önceden QR kod şeklinde hazırlamak bir seçenek olabilir. El koyma işleminden hemen önce, adresin doğru olup olmadığını görmek için bu el koyma adresi çifte kontrol

edilmelidir. Burada sunulacak bir öneri de, dört gözün yakalama adresini kontrol edebileceği ve dolayısıyla varlıklara el koyan kişileri koruyabileceği dört göz ilkesini kullanmaktır.

Geçerli yasa ve prosedürler şüphelinin cihazlarının el koyma için kullanılmasına izin verildiğinde, bazı durumlarda cihazın ilk önce parmak izleri, DNA ve kan izleri gibi diğer izler için kontrol edilmesi gerektiğini göz önünde bulundurun. Bu, soruşturulacak duruma bağlı olacaktır.

El koyma işlemi öncesi bir diğer iyi uygulama cüzdan bakiyesini kontrol etmektir. Bakiye sıfırsa el konulacak bir şey yok demektir.

3.3 Masaüstü Cüzdan

3.3.1 Giriş

Masaüstü veya yazılım cüzdanları bir bilgisayara yüklenir ve kullanıcılara genel ve özel anahtarların ve dolayısıyla fonların tam kontrolünü sağlar. Bitcoin Core, Electrum, Exodus, Coinomi, Jaxx Liberty, Atomic and birçok kripto para bu cüzdanlara örnektir. Bu cüzdanların bazıları mobil sürümleriyle eşleştirilebilir.

3.3.2 Bitcoin Core ve "hafif cüzdan" (light wallet)'lerden farkı

Bitcoin Core orijinal Bitcoin cüzdanıdır ve bitcoinleri saklamak için hâlâ en güvenli yerlerden biridir.

Bitcoin ağının neredeyse %99'u Bitcoin Core düğümlerinden meydana gelir (<https://coin.dance/nodes>).

Diğer cüzdanlardan en büyük farkı, Bitcoin Core'un tüm bitcoin işlemlerinin (blok zinciri) tam geçmişini indirmesidir ve bu nedenle, cüzdan, adreslerin bakiyesini sorgulamak için üçüncü taraf düğümlerine bağlı kalmak zorunda değildir. Öte yandan, (Electrum, Ledger, Jaxx, vb.) gibi hafif bir düğüm, blok zinciri ile etkileşim kurmak için (Bitcoin Core gibi) tam bir düğüme bağlanmalıdır. Bir başka ifadeyle, hafif bir istemci başladığında, (Bitcoin ağında bir yerde olan) tam bir düğüme bağlanır ve Bitcoin adreslerinin bakiyesini sorar.

Bitcoin Core'un bir dezavantajı, özellikle kullanıcının yerel depolamada tam bir blok zincirine (+300 Gb) ihtiyacı varsa, fazladan hard disk alanına ihtiyaç duymasıdır. İsteğe bağlı olarak, Bitcoin Core kullanıcıları "Pruning"i etkinleştirebilir ve böylece tam blok zincirinin daha küçük bir sürümünü kullanabilir. Cüzdan bunu, en son blok zincirini indirirken artık ihtiyaç duymadığı eski verileri silerek yapar.

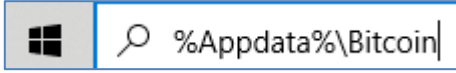
Wallet.dat

Bitcoin Core'un gerçek cüzdan dosyası, önceden tanımlanmış ismi olan wallet.dat'dur. Bu dosya, özel anahtarları, genel anahtarları, (adreslere karşılık gelen) komut dizilerini, anahtar meta verilerini (örneğin, etiketler) ve cüzdanınızla ilgili işlemleri içerir. wallet.dat'ın önceden tanımlanmış isim olduğunu unutmayın. Kullanıcılar isterlerse bunu, örneğin "recipes.txt". vb. şeklinde değiştirebilirler.

Cüzdan dosyasının varsayılan konumları:

Windows

Başlat -> Çalıştır'a gidin (veya WinKey+R yapın) ve çalıştırın: %APPDATA%\Bitcoin



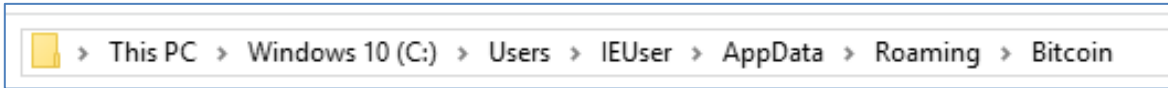
Bitcoin'in data dosyası açılacak:

Name	Date modified	Type	Size
blocks	09/12/2019 15:54	File folder	
chainstate	09/12/2019 15:55	File folder	
wallets	09/12/2019 15:55	File folder	
.lock	18/07/2019 10:09	LOCK File	0 KB
banlist.dat	18/07/2019 10:09	DAT File	1 KB
debug.log	09/12/2019 15:55	Text Document	11.667 KB
fee_estimates.dat	09/12/2019 15:55	DAT File	243 KB
mempool.dat	09/12/2019 15:55	DAT File	1 KB
peers.dat	09/12/2019 15:55	DAT File	2.125 KB

Birçok kullanıcı için, bunlar aşağıdaki konumlardır:

C:\Documents and Settings\YourUserName\Application data\Bitcoin (Windows XP)

C:\Users\YourUserName\AppData\Roaming\Bitcoin (Windows Vista, 7 and 10)



"AppData" and "Application data" varsayılan olarak gizlidir. Bitcoin data dosyaları herhangi bir başka sürücüde veya klasörde saklanabilir.

Linux

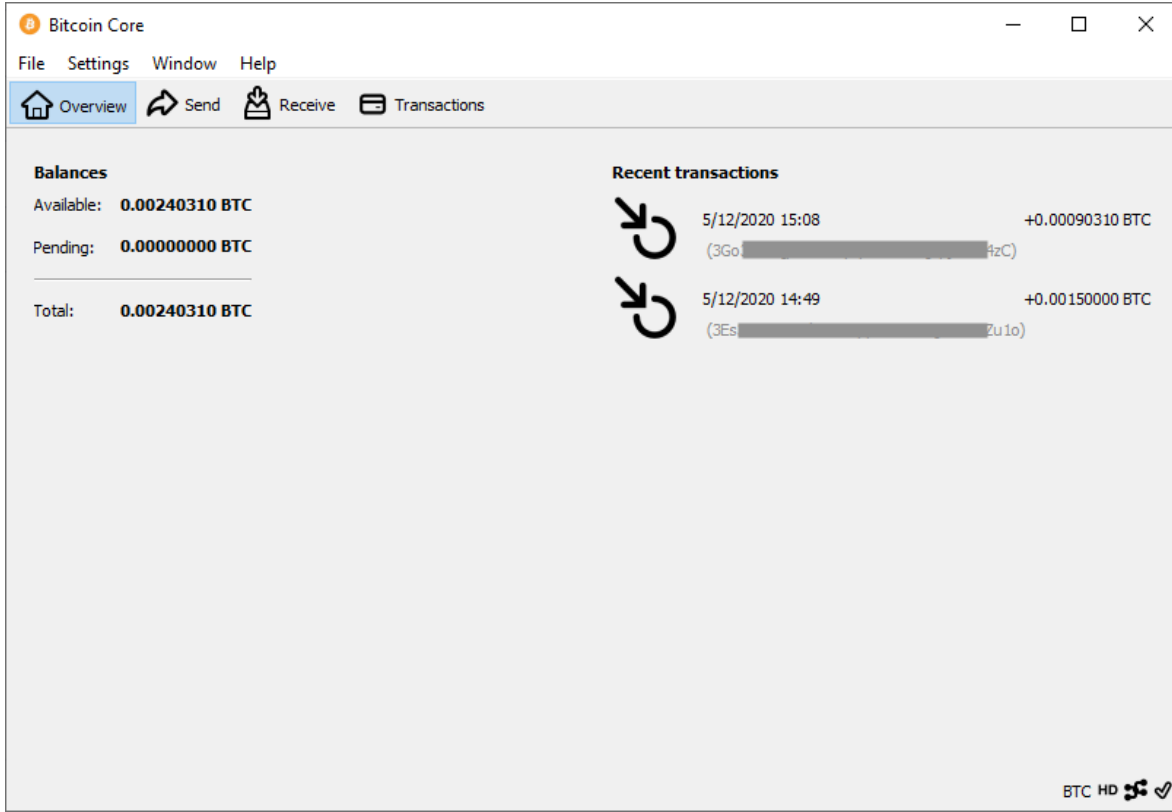
Bitcoin, datalarını varsayılan olarak şuraya koyacaktır: ~/.bitcoin/

Nokta ile başlayan dizinleri görmek için "ls -a" yapmanız gerekir.

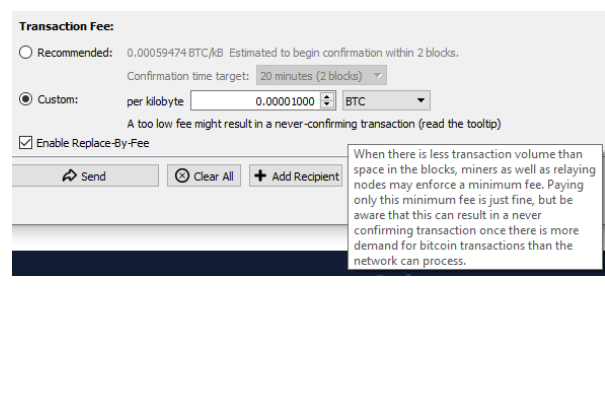
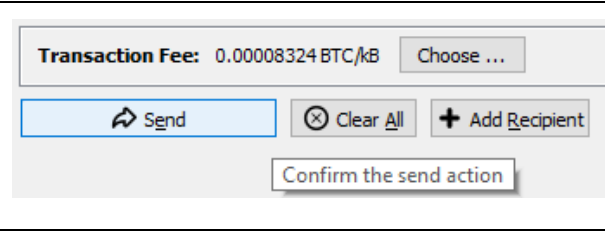
Mac

Bitcoin, datalarını varsayılan olarak şuraya koyacaktır: ~/Library/Application Support/Bitcoin/

Bitcoin Core'da El Koyma İşlemi



	Şifreli bir cüzdanın (dosyanın) sağ alt köşesinde bir asma kilit vardır. Şifreyi bilmiyorsanız, başka bir işlem yapamazsınız.
	Cüzdan şifrelenmemişse veya şifreyi biliyorsanız, bitcoinlere el koymak için "Gönder"e tıklayın.
	"Ödeme Yap" alanına el koyma adresini yapıştırın ve "Ücreti hesaptan çıkar" seçeneğini işaretleyin. Bu ücret gönderilen tutardan düşülecektir.
	Tüm bitcoinleri devlet kontrolündeki adrese göndermek için "Mevcut bakiyeyi kullan"a tıklayın.

	Hızlı bir işlem gerekiyorsa, "Özel"e tıklayarak daha yüksek bir işlem ücreti kullanın. Zaman ve imkanınız varsa, tahmini ücretler için şu adresi ziyaret edin: https://www.buybitcoinworldwide.com/fee-calculator
	El koymak için "Gönder"e tıklayın.

3.3.3 Electrum

- Kullandığı anahtar kelime: İsteğe bağlı BIP39 uzantılı zorunlu 12 kelimelik anahtar ifade
- Kullandığı şifre: İsteğe bağlı

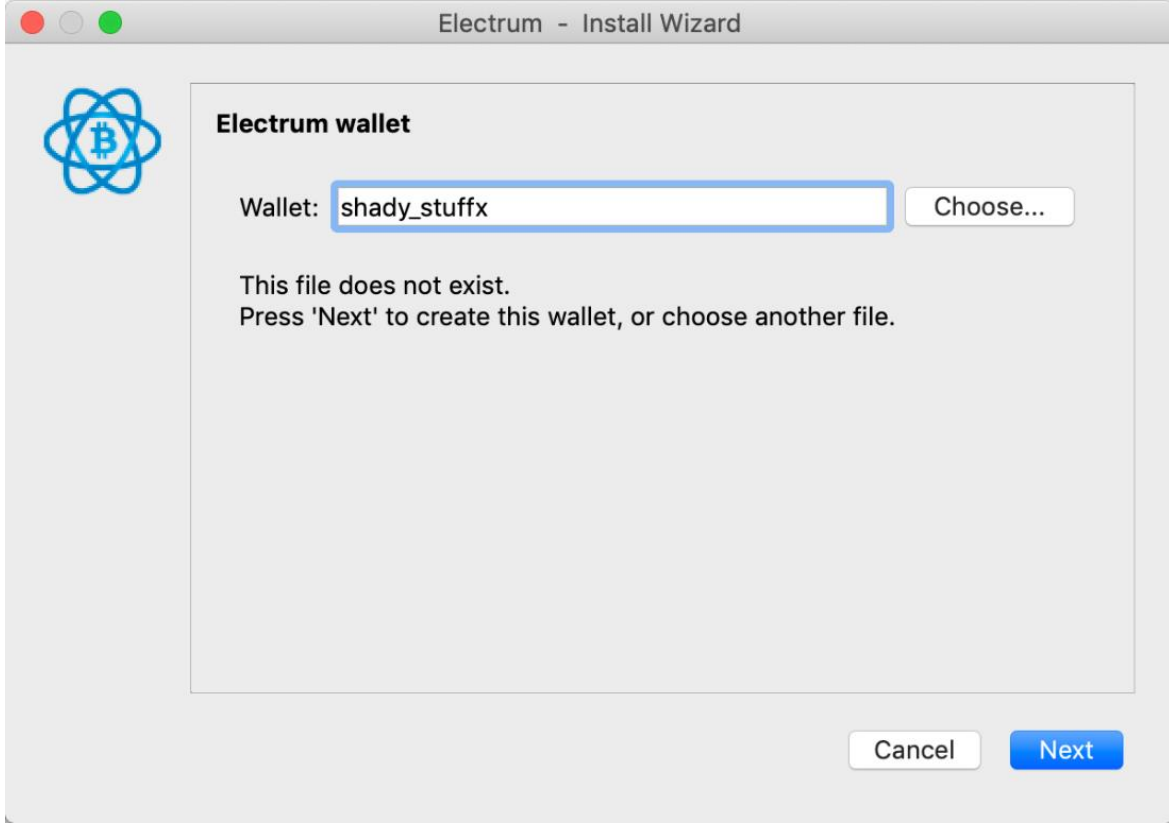
Electrum cüzdanının kurulumu oldukça basittir. Mobil uygulama (Android) ve çeşitli platformlar için masaüstü cüzdan olarak kullanılabilir (aşağıdaki resme bakın). (Daha sonra açıklanacak olan) Electrum ve Exodus cüzdanları çok popülerdir.

Sources and Binaries		
 Python (3.6.1 and higher)	Electrum-4.0.6.tar.gz	signature
 Linux	Appimage	signature
 Windows (7 and higher)	Standalone Executable	signature
	Windows Installer	signature
	Portable version (security advice)	signature
 OSX (10.13 and higher)	Executable for OS X	signature
 Android (5.0 and higher) (available on Google Play)	64 bit	signature
	32 bit	signature

İpucu: Bir Electrum cüzdanını kurarken ve güncellerken, örneğin kötü amaçlı yazılım içeren sahte bir sürümü yüklediğinizden emin olmak için GPG imzalarını doğrulamak iyi olacaktır. Bunun nasıl yapılacağı <https://electrum.org/#download> adresinde şu başlıkta bulunabilir: "GPG imzaları nasıl doğrulanır".

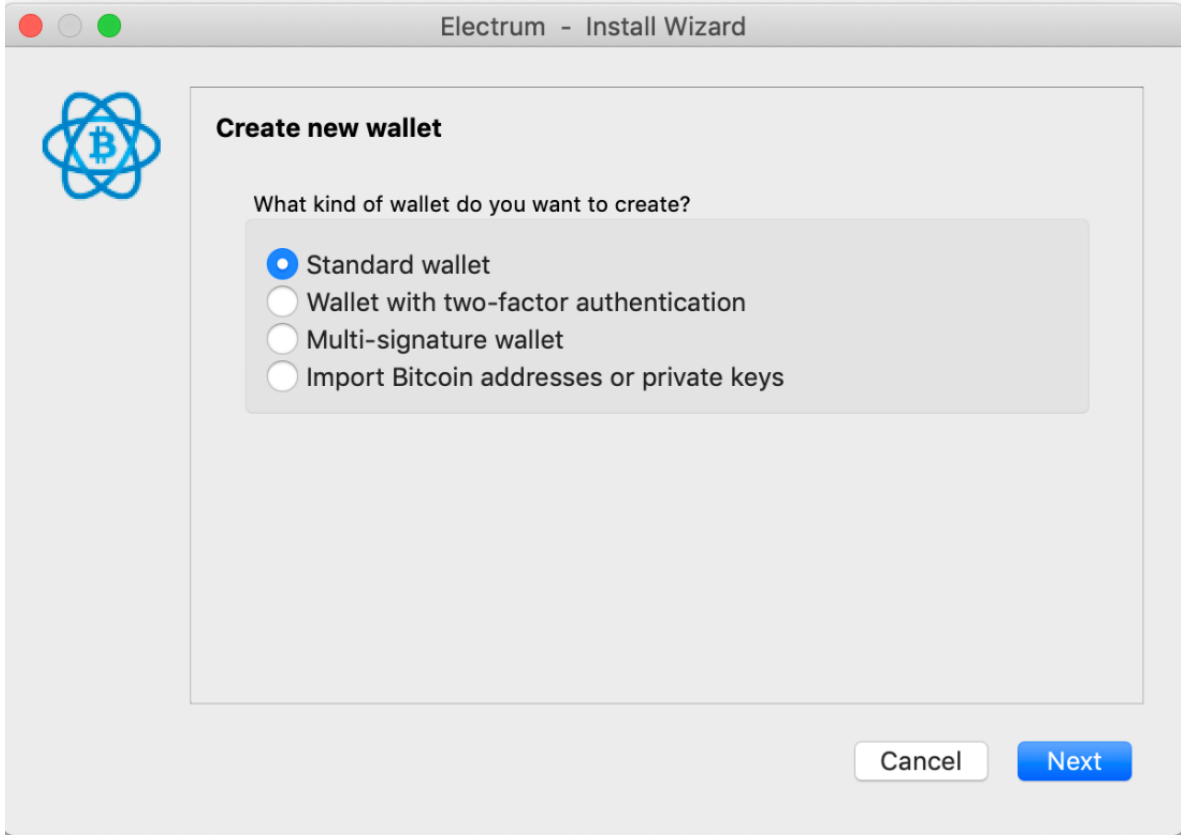
Electrum'un resmi web sitesinde, Electrum'un 3.3.4'ten daha eski sürümlerinin kimlik avına açık olduğu, Electrum'un electrum.org dışındaki bir kaynaktan indirilmemesi ve GPG imzalarının nasıl doğrulanacağını öğrenilmesi konusunda kullanıcılar için bir uyarı mevcuttur.

Electrum'u kurarken, aşağıda gösterildiği gibi bir cüzdan adı istenecektir. "default_wallet" olarak isimlendirilmesi şart değildir, herhangi bir isim verilebileceğinin farkında olun. Örneğin aşağıda ekran görüntüsü olan cüzdanın adı "shady_stuffx"dir.



Yükleme işlemi sırasında, şu cüzdan türleri oluşturulabilir: standart cüzdan, iki faktörlü kimlik doğrulamalı cüzdan, çoklu imza cüzdanı veya aşağıda gösterildiği gibi Bitcoin adreslerini veya özel anahtarları içe aktarma seçeneği.

Açıklama: Bu Electrum bölümünde (el koyma örneği dahil olmak üzere) sadece bir Electrum standart cüzdanının kullanımını, cüzdana el konulması ve kurtarılmasını kapsıyoruz. İki faktörlü kimlik doğrulamalı cüzdanlar ve çoklu imza cüzdanları için diğer gereksinimler geçerlidir. Bunlar hakkında daha fazla bilgi için resmi Electrum web sitesine bakın. İki faktörlü kimlik doğrulama (2FA) kılavuzun ilerleyen bölümlerinde ele alınmıştır.



“Standart cüzdan” seçeneğini seçtikten sonra, aşağıda gösterildiği gibi, yeni bir anahtar ifade oluşturabilir, mevcut bir cüzdanı bir anahtar ifadeden geri yükleyebilir (aşağıya bakınız), bir anahtar kullanabilir veya Electrum'u bir donanım aygıtına bağlayabilirsiniz.

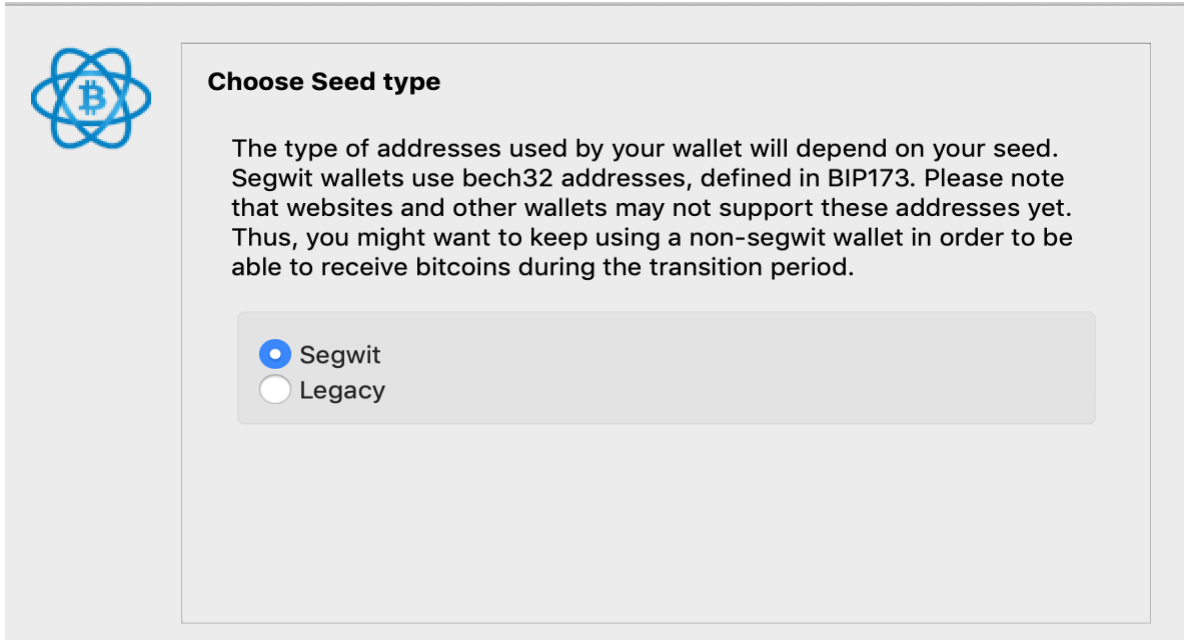
Bu aşamada mevcut bir cüzdanı anahtar kelimelerden yeniden yüklemek için “Bir anahtarım var” seçeneğini seçip bulduğunuz kelimeleri girmeniz gerekir.



“Yeni anahtar oluřtur” seeneęini setikten sonra, iki anahtar eřidinden birini seebilirsiniz: “SegWit” ya da “Legacy”. Electrum iinde, SegWit cüzdanları “bc1” ile bařlayan bech32 adreslerini kullanır ve eski cüzdan adresleri 1 ile bařlar.

Ařaęıdaki ekran görüntüsünde belirtildięi gibi, bazı web siteleri ve cüzdanların bu bech32 adreslerini henüz desteklemeyebileceęini ve SegWit olmayan bir cüzdan kullanmaya devam edebileceęinizi lütfen unutmayın.

Daha sonra ele alınacak olan Jaxx Liberty, bu cüzdanın bir örneğidir.



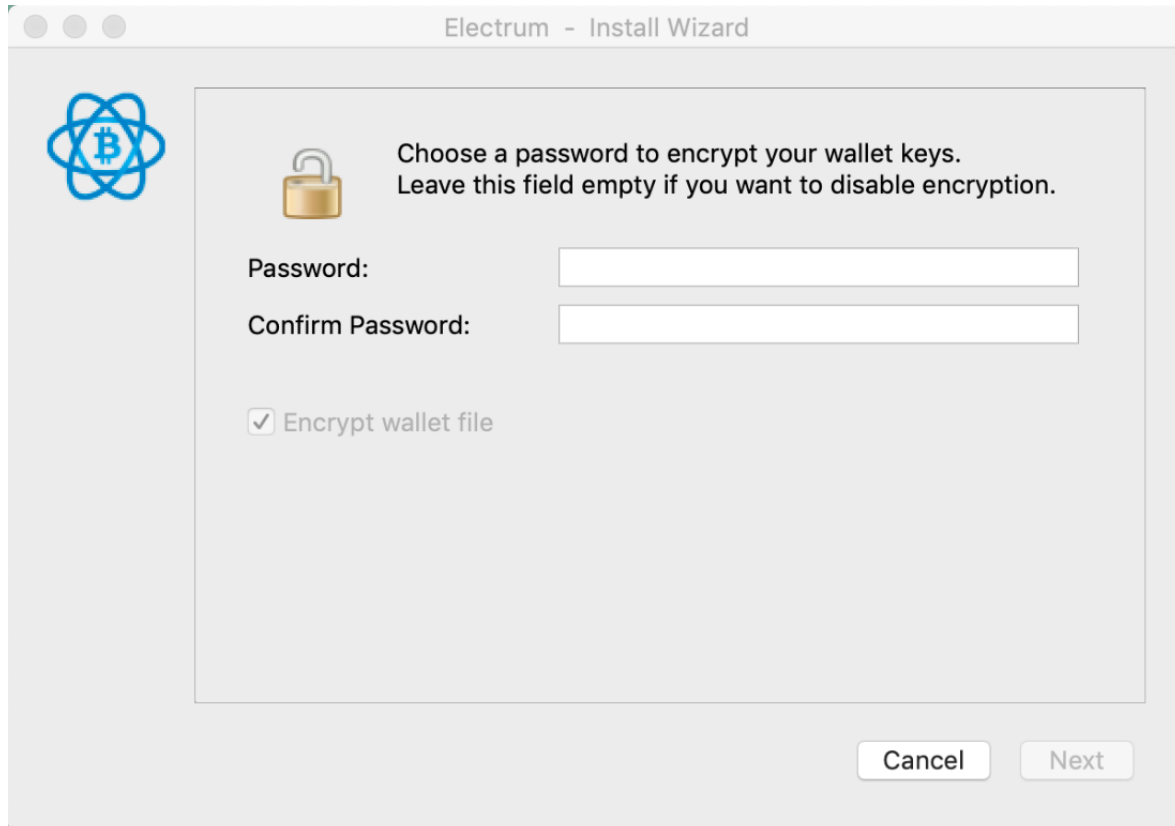
Choose Seed type

The type of addresses used by your wallet will depend on your seed. Segwit wallets use bech32 addresses, defined in BIP173. Please note that websites and other wallets may not support these addresses yet. Thus, you might want to keep using a non-segwit wallet in order to be able to receive bitcoins during the transition period.

☒ Segwit
☐ Legacy

Şimdi, yeni bir cüzdan oluştururken, yeni bir anahtar ifade alacaksınız. Electrum genellikle bazı özel kelimelerle genişletilebilen 12 kelime kullanır. Bu örnekteki anahtar kelime listesi "havaalanı cins önde ayak karışımı fikir içi boş davul keskin pazarlık ikinci harika"dır.

Son olarak, kullanıcı aşağıda gösterildiği gibi, cüzdana bir şifre ekleyebilecektir. Bir şifre eklendiğinde, cüzdan dosyası şifrelenecektir.



Electrum - Install Wizard



 Choose a password to encrypt your wallet keys.
Leave this field empty if you want to disable encryption.

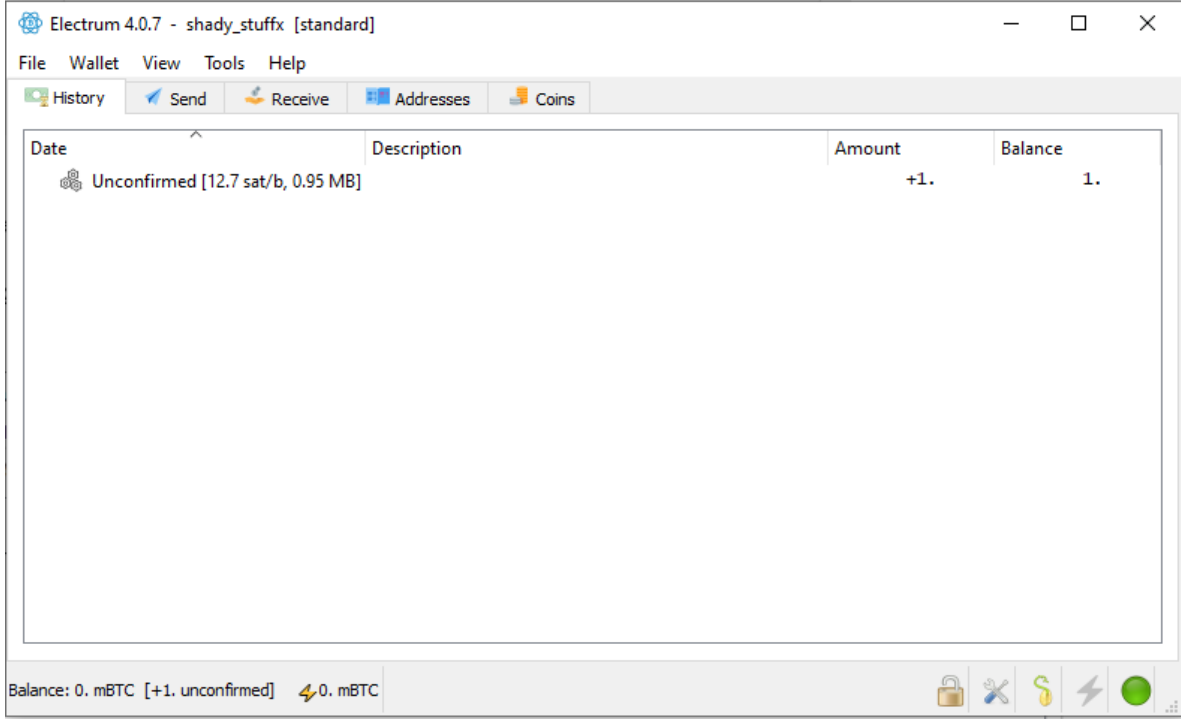
Password:

Confirm Password:

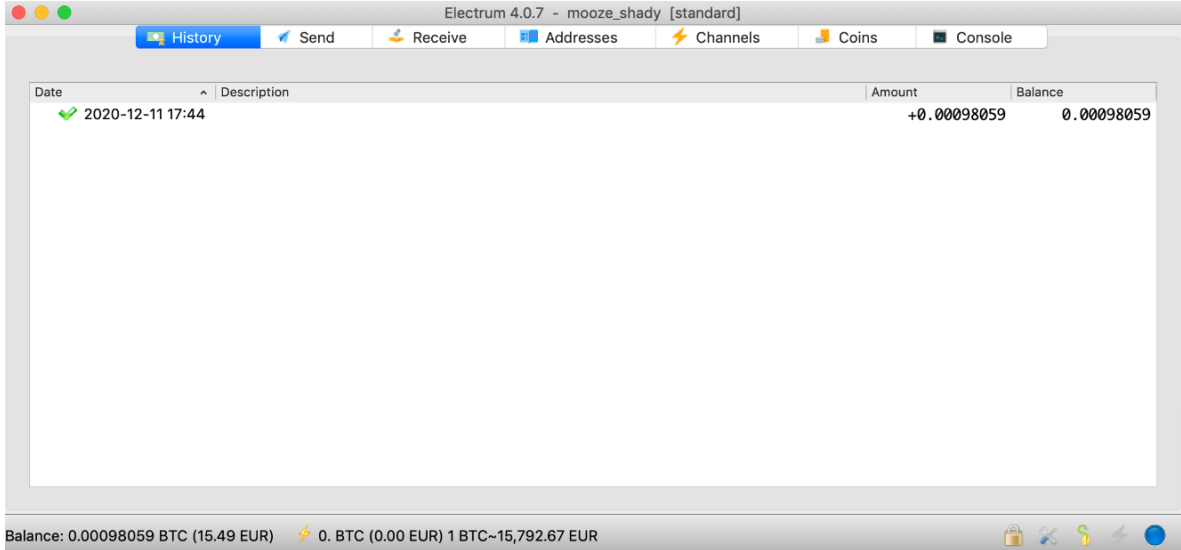
☒ Encrypt wallet file

Cancel Next

Electrum cüzdanının aşağıda gösterilen ana sayfasından, "shady_stuffx" cüzdan adını, sürümünü, işlem geçmişini ve bakiyesini görebilirsiniz (bu örnekte doğrulanmamış gözüküyor, yani cüzdan bekleyen bir işlem alıyor).



Bu nedenle, Electrum masaüstünde çalışırken aşağıdaki ekran görüntüsündeki gibi görünür; Mac ve Windows sürümü kozmetik olarak biraz farklı görünse bile, tüm işlevler aynı şekilde yapılır. Mevcut bakiyeyi ve gerçekleşen işlemleri hemen fark edersiniz (bu örnek durumda, yalnızca gelen bir işlem var).



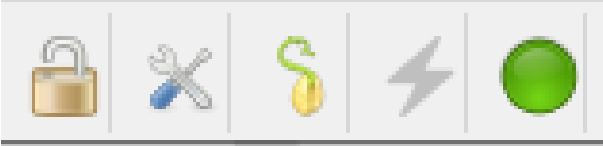
Cüzdanın sağ alt köşesinde bir asma kilit (simge) olduğundan emin olun. Asma kilit kapatıldığında, cüzdan şifre ile korunup şifrelenir ve para transferi/el koyma işlemi için bir şifre gerekir. Özel anahtarları çıkarmak veya bu cüzdandan anahtar ifadeyi almak için de bir şifre de gerekecektir.

Asma kilit açıksa, cüzdan (şifre) korumalı değildir. Şifre olmadan paraya el konulabilir.

Aşağıda asma kilidin yakınlaştırıldığı iki (Mac ve Windows) ekran görüntüsü yer almaktadır. Asma kilit simgesinin yanında "Tercihler" simgesi, ardından "Anahtar", "Şimşek Ağı" ve "Ağ" simgeleri bulunur. (Cüzdan şifrelenmişse) "Anahtar" simgesine tıklandığında, anahtar ifadeyi almak için bir şifre istenecektir.



Şifrelenmiş cüzdan = kapalı asma kilit (Mac)



Şifrelenmemiş cüzdan = açık asma kilit (Windows)

Yukarıda gösterilen cüzdanda sadece bir gelen işlem ve ekran görüntüsü alındığı esnada 0,00098059 EURO'yu temsil eden 15,49 BTC'luk toplam bakiye bulunmakta. "Bakiye" altta ve cüzdanın adı yukarıda bulunabilir, bu durumda cüzdanın adının "mooze_shady" olduğu görülmekte. Cüzdanın sürümü 4.0.7'dir.

Cüzdan adının altında, şu sekmeleri bulabilirsiniz:

- Geçmiş
- Gönder
- Al
- Adresler
- ...

"Geçmiş" sekmesi işlemlerin bir özetini içerir (yukarı bakınız). Bu işlemlerin genel özeti, (blok zinciri analizi gibi) daha fazla araştırma yapmak için çok uygun olabilir. Ayrıca bir işleme sağ tıkladığınızda, işlem hakkında daha fazla ayrıntı elde edilebilir. Ancak blok zinciri analizi bu kılavuzun kapsamı dışındadır.

"Gönder" sekmesi bitcoin göndermek ve bitcoine el koymak için kullanılacaktır. "Al" sekmesi ise bitcoin almak için kullanılırken, "Adresler" sekmesi, bu cüzdana ait bitcoin adreslerinin listesini içerir.

Electrum 4.0.7 - mooze_shady [standard]

History Send Receive Addresses Channels Coins Console

Type	Address	Label	Balance	Tx
receiving	bc1qetnvgdrdsscrzreks9y7x0962zuk8fhn7szpkw		0.00098059	1
receiving	bc1q3rt0peag2f6s3yphmv2y9tdjgmkdwkfd0ca4yn		0.	0
receiving	bc1q8pqdq4v94ahne15a158dnzhmjsur1hmvprnr3q		0.	0
receiving	bc1qh65p7m0g9f3ku3yqshzf8frvacs4u0x9gjqso0v		0.	0
receiving	bc1q9dct9h1nt18pwd6mc8jt3qqa65y2pppy4eyc7c		0.	0
receiving	bc1q7jvs0dka2p89tz22q4y40cm0xqem675jl3ycg8		0.	0
receiving	bc1qfv9jh65nx56scgt8nyzj6r9d6t339e0mvx45y3		0.	0
receiving	bc1qsf4f4q2h2853k27dme9n7jm67s42x5ftvpjze		0.	0
receiving	bc1qu7rzhv5vpm5swj9yc3qh59dal13k9a6pef0dxv		0.	0
receiving	bc1qjdftwzdsghgd9znk8wszjzkptns85wvd9sr17		0.	0
receiving	bc1qqw4nhuexeu23zjmj2fu2yrnczs2ghf2aq0lxzz		0.	0
receiving	bc1qe0gg8kvzykm0xwmu3874dt95phr384ym69k7		0.	0
receiving	bc1qfut2vmjpmwmc7z2t7kxxfsus18hj2xt3f5t6		0.	0
receiving	bc1qmqfwLakaxd0u7r5y5m663jzpgs8dw5au89sxc		0.	0
receiving	bc1qplwdewr6zxqvyLudt5dtycamgqg27kqlnqycsx		0.	0
receiving	bc1q5xgxn96rhmd2avpawd52392q9mqzlcwg3susjqz		0.	0
receiving	bc1qu7fve0ft7z4w3z7l6x8dwt53vv7auwkeakqzle		0.	0
receiving	bc1av9un7w9zmtmhv5z7aa88snfk4a8aa1w9aada2		0.	0

Balance: 0.00098059 BTC (15.54 EUR) 0. BTC (0.00 EUR) 1 BTC~15,843.61 EUR

Yukarıda: bir Mac bilgisayarındaki adreslerin ekran görüntüsü.

Electrum 4.0.7 - shady_stuffx [standard]

File Wallet View Tools Help

History Send Receive Addresses Coins

Type	Address	Label	Balance	Tx
receiving	bc1qpjddq5xx0xnszmcdxh9p1939r24m3dwwh92uyra		1.	1
receiving	bc1q233ctrdjk492yz20428ggjwwxwef89wcecr4g		0.	0
receiving	bc1qdp70qqrsns779wnr97ee23ygkdxtyrtv6744m		0.	0
receiving	bc1q22t0anx5a0xu5ynm10mq7lzneqcnxkfed5xs4e		0.	0
receiving	bc1q3rcwjpgwfevfy7jhu3e0pz0r7c29l9gmsmczv4c5		0.	0
receiving	bc1qmvmd28t09k8n28q2f4t64wqsj30nyzhse7umx		0.	0
receiving	bc1qeh9mk42vaummuag3cqfmggwwad0k65rc8xqu8g		0.	0
receiving	bc1qzvcuh476z39pncqt6avcqqg977gjj2lmcjfngeu		0.	0
receiving	bc1qk5sg7tad1xxhqf1lwwgt7w63nm3cjsq7q0e		0.	0
receiving	bc1qpkv4fe7rawakpdkrmvhgj0d3gpyg6svv1uffwm		0.	0
receiving	bc1qqd6j2r4cp7e53zmqum8mj1025j7py0fnfyqasdd		0.	0
receiving	bc1qn1jete8n2mdetjtf4xz9r6k447kt8h959vtwm6		0.	0
receiving	bc1qw963rdvrpun75f36z5qlxrkyxtea7xjtfkrn1a		0.	0
receiving	bc1q25x6en4lxxmv8esgcsr5sny86v02u89v8gmga		0.	0
receiving	bc1qkzc5xcqcmgrca8svgf4yuxd5nuytd6s20hdrh		0.	0
receiving	bc1qfaxzfnmfgxly0y5gmhx5yhf5476rkwahsvmhck		0.	0
receiving	bc1qs5quqmmjhr70e4wunhfy9t7hu397s357tu7ke		0.	0
receiving	bc1q1pg32z1v368x0rndqnx2ve8km6e1dcdeqhz44u		0.	0
receiving	bc1qzsnskd5s9th6awewmmkgs2wpewp9pvzz34dqk		0.	0

Balance: 0. mBTC [+1. unconfirmed] 0. mBTC

Yukarıda: bir Windows bilgisayarındaki adreslerin ekran görüntüsü.

Bu durumda, Mac ekran görüntüsünde, sadece "bc1qetnvgdrdsscrzreks9y7x0962zuk8fhn7szpkw"²⁵ bitcoin adresinin bakiyesi var. Windows ekran görüntüsünde, sadece "bc1qpjddq5xx0xnszmcdxh9p1939r24m3dwwh92uyra" adresinin onaylanmamış bakiyesi bulunmaktadır; ancak yakından bakıldığında, Windows cüzdanı mBTC olarak ayarlanırken, Mac cüzdanı BTC şeklindedir. Bu cüzdanlar eğitim amaçlı oluşturulmuşlardır ve bu nedenle yalnızca bir kez kullanılmış adresleri vardır. Çoğu zaman, birkaç bitcoin adresi alttaki bakiye toplamında toplanacak bir bakiyeye sahip olacaktır.

²⁵ Yani, Segwit cüzdanı, BIP173'TE tanımlanan bech32 adresini kullanır.

(Mac'te, Windows için benzer) El koyma işlemi örneği

(Mac'te, Windows için benzer) El koyma işlemi örneği

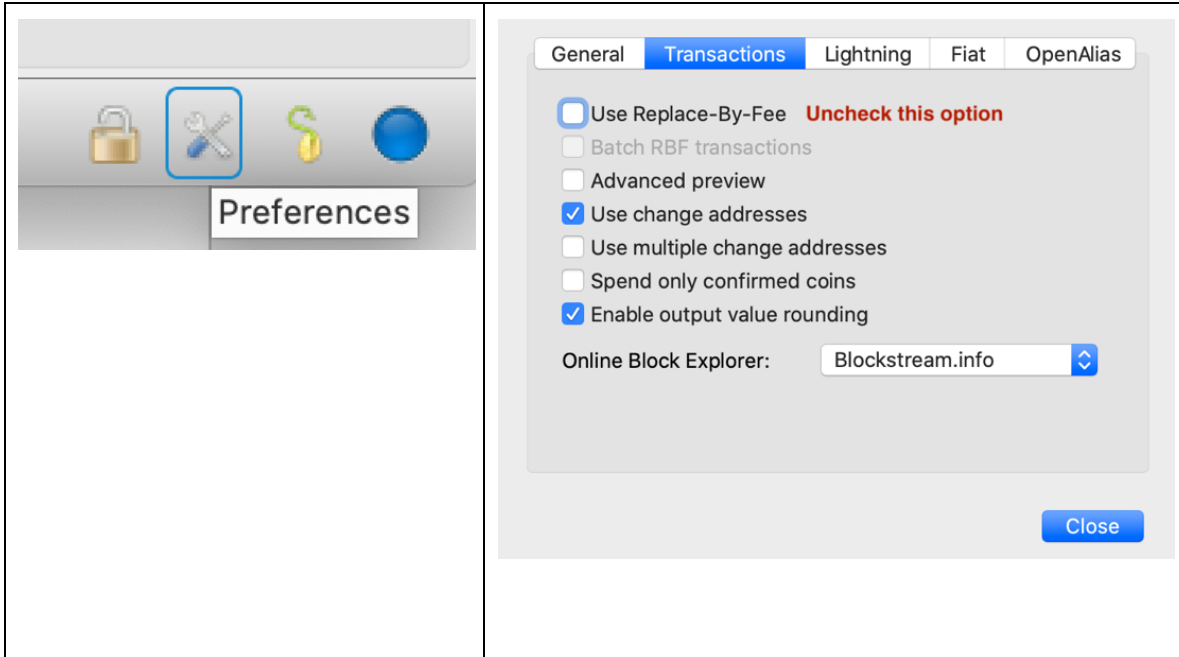
DİKKAT: **Uncheck** "Use Replace-By-Fee" (Ücret Değiştirme Kullanın) seçeneğinin **işaretini kaldırın!**

Electrum 4.0.4 sürümünden bu yana, Ücret Değişimi (Replace-By-Fee) seçeneği cüzdanlarında aktif olması koşuluyla (işlem ağa iletilmeden önce), kullanıcılar Bitcoin işlemini onaylanmadan önce iptal edebilirler.

Fakat, bir işlemin iptal edilebilmesi için kullanıcının cüzdanında yeterli bakiye olmalıdır.

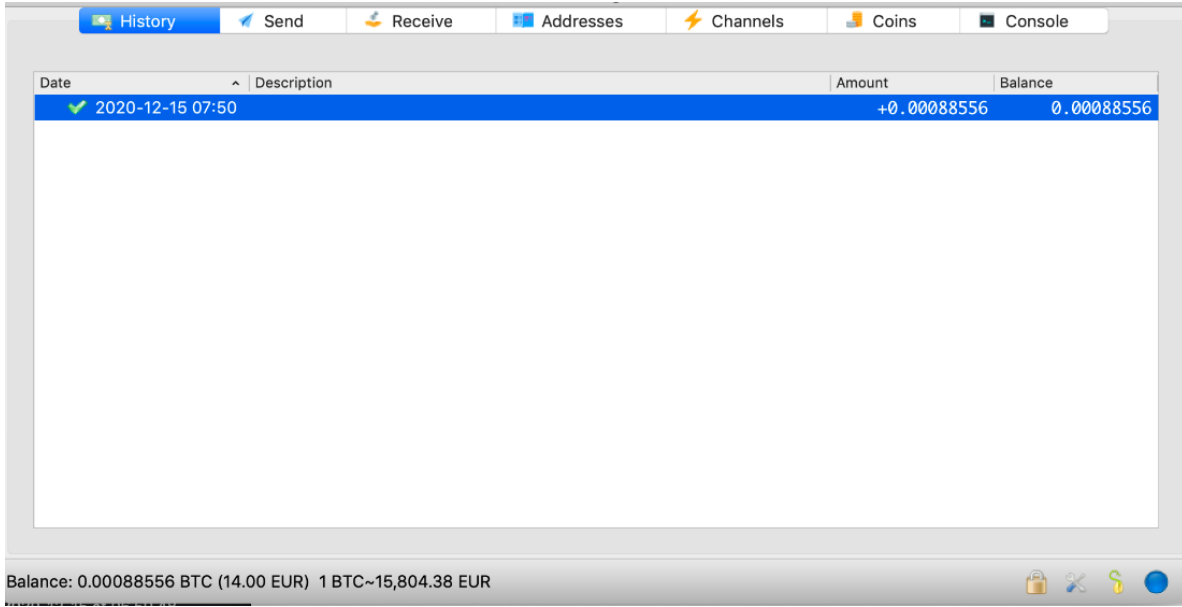
Açıklama: Ücret Değişimi (Replace-By-Fee) seçeneği varsayılan olarak etkinleştirilir.

Olası tüm risklere engel olmak için, "Use Replace-By-Fee" (Ücret Değiştirme Kullanın) seçeneğinin işaretini aşağıdaki gibi kaldırmak iyi olacaktır:



Devre dışı bırakıldığında, el koyma işlemine devam edebilirsiniz.

Aşağıda, (14,00 Euro'ya eşdeğer) 0.00088556 BTC içeren (4.0.7 sürüm) bir Electrum cüzdanından adım adım el koyma işlemi örneği bulabilirsiniz.



Aşağıda gösterilen “Gönder” sekmesinde, bu cüzdandaki bitcoinlerin (yani, 0,00088556 BTC) hükümet kontrolündeki bir cüzdana nasıl transfer edileceği ve el konulacağı gösterilmiştir.

“Öde”nin yanında, elle ya da kopyala-yapıştır yaparak el koyma adresini doldurmanız gerekir. Fakat yazım hataları için çok dikkatli olun.

Adresi yazarken not defteri dosyası oluşturup boşaltmak ve not defterinde adresi en az 2 veya 3 farklı kişinin yazmasını sağlamak iyi bir uygulamadır. Ayrıca, daha önce yazılanları başkalarının görmediğinden emin olun. 2 ya da 3 kişi not defterinin farklı sayfalarına adresi yazdıktan sonra bu 2-3 yazıyı karşılaştırın; hepsi eşleştğinde, herkesin bitcoinlerin gönderileceği adresi kabul ettiğinden emin olabilirsiniz.

Bu “Öde” veri giriş alanının en sağında iki seçenek daha vardır: “QR kodunu oku” ve “Dosyayı oku”. QR kodu seçeneği ile QR kod olarak temsil edilen bir bitcoin adresi okunabilir. (El koyma adresini temsil eden) Bu QR kod önceden basılabilir veya akıllı telefon gibi bir mobil cihazda saklanabilir.

Hangi seçeneği seçerseniz seçin, el koyma işleminden önce el koyma adresinin doğruluğunu her zaman iki kez kontrol edin; el koyma öncesi planlama bölümünde daha önce belirtildiği gibi, dört göz prensibine uyulması önerilir.

El koyma işlemine yerel bir açıklama (örneğin alıcı adı, dosya numarası) eklenebilir. Tüm cüzdana el koymak için miktar “Max” olarak ayarlanmalıdır (bu, cüzdandaki tüm fonların muhtemelen farklı bitcoin adreslerinde bulunduğu anlamına gelir).

History Send Receive Addresses Channels Coins Console

Pay to: 1E6ZBvcgtqZHTP4eqrFPiF1gQknMC1qYRf

Description: Target X seizing

Amount: 0.00083122 BTC 13.14 EUR Max

Clear Save Pay...

Balance: 0.00088556 BTC (14.00 EUR) 1 BTC~15,806.43 EUR

Daha sonra, özel örneğimizde "Öde"ye tıkladıktan sonra, pencere aşağıda gösterildiği gibi görünür.

Ücret tahmin algoritmaları (ETA, Static veya Mempool) ve ücret oranı kaydırıcısı ayarı, Electrum cüzdanının şüphelinin bilgisayarındaki önceki (gönderme) işlemler(in)de nasıl kullanıldığına bağlı olarak farklı görünebilir.

Örneğimizde ("Öde"ye tıkladıktan sonra...) ücret hesaplama algoritması Electrum tarafından "ETA" olarak ayarlanır ve kaydırıcı, Electrum tarafından en sağdaki (maksimum) olarak ayarlanır. Ücret tahmin algoritmaları ve ücret oranı kaydırıcı ayarı ayarlanabilir (aşağıya bakınız).

Amount to be sent: 0.00073158 BTC (11.56 EUR) Advanced

Mining fee: 0.00015398 BTC (2.43 EUR)

Fee rate: ETA

Warning: The fee for this transaction seems unusual (21.05% of amount)

Target: In the next block
Current rate: 80.2 sat/byte

Password

Cancel Send

Ücretin işlem baytlarına bağlı olduğunu unutmayın (bitcoin fiyatı değil ancak haliyle doğal olarak ilişkilidir), bir girdi ve bir çıktı, blok zincirindeki bitcoin bloğundan en az bayt miktarını kullandığı için gönderilmesi en ucuz olandır. Ağ tıkanmasına bağlı olarak, bu örnekte olduğu gibi oldukça pahalı olabilir. Ücret genelde birkaç dolar sentidir. Ancak işlemin baytları ile daha fazla ilgisi olduğundan, ücret çok

değişebilir. İşlem yapmadan önce işlem ücretini bir Bitcoin ücret hesaplayıcısından (kılavuzda daha sonra açıklanmıştır) hesaplamanız önerilir.

Yukarıdaki ekran görüntüsünde, bu işlem için ücretin alışılmadık derecede yüksek görüldüğü konusunda bir uyarı var (ücretin %21.05'i!)

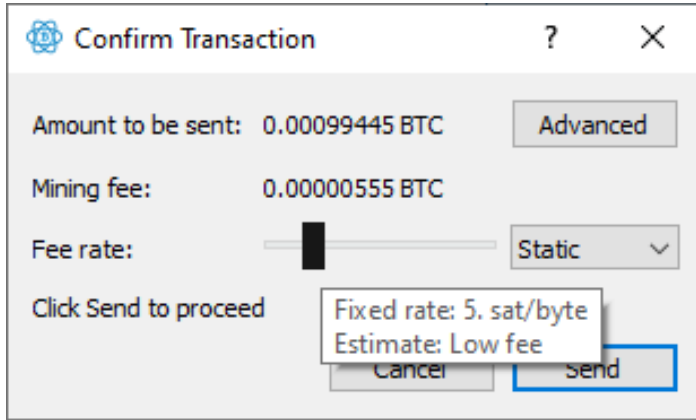
Aslında, bu gerçek ücret ayarlarıyla, örnek el koyma işlemimizin blok zincirinin bir sonraki bloğuna eklenmesi hedeflenmektedir.

Daha önce belirtildiği gibi, işlem ücretleri madencilere ödenen tutarlardır.

Bunun, durumla ilgili belirli (taktiksel) kriterlere ve geçerli yasal çerçeve ve el koyma prosedürleri gibi diğer ilgili unsurlara bağlı olarak ayarlanabilen çok yüksek bir ücret olduğunu unutmayın. Bir el koyma işleminden önce düşünülmesi gereken işlem ücretleriyle ilgili bazı ilgili sorular şunlardır:

- Bu ücreti kim ödeyecek? (Şüpheli mi? Hükümet mi?)
- Fonların şüpheli için daha sonraki bir aşamada geri ödenmesinin gerekmesi riski varsa, o zaman bu masrafları kim kendi hesabına alacak? Ve bu ikinci durumda, şüpheliye ne kadar para ödenmesi gerekiyor?
- Oyunda herhangi bir suç ortağı var mı (bundan sonra bakınız)?
- ...

Örneğin, ilgili (taktiksel) kriterlerle ilgili olarak, bir polis müdahalesi sırasında bir suç ortağının veya belirli bir süre sonra (örneğin, bir ev aramasından kısa bir süre sonra) bir şüphelinin hedeflenen cüzdana (örneğin, özel anahtar(ler) veya anahtar ifade aracılığıyla) erişme riski ne zaman yüksek olursa, bu işlemin hangi blokta hedeflenebileceğine karar vermek için (sonraki blok, 5 blok içinde vb.) bir risk analizi (maliyet-fayda analizi) yapılmalıdır. Ayrıca, yukarıda belirtildiği üzere, geçerli yasal çerçeve ve el koyma prosedürlerine bağlı olarak, daha sonra herhangi bir tartışmayı önlemek için işlem ücretlerinin kimin hesabından tahsil edileceğini kontrol edin.

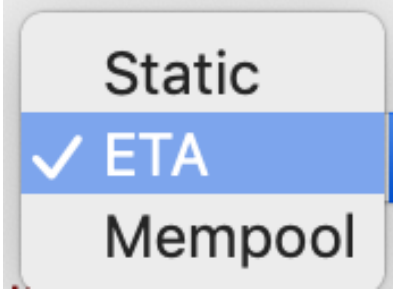


İşlem göndermeyle ilgili bir başka örnek, sabit (statik) bir ücret ayarlamaktır ve yukarıdaki ekran görüntüsünde, bayt başına 5 satoshi'lik bir işlem belirlenmiştir ve işlem, mevcut ağ trafiğine bağlı olarak saatler içinde devam etmelidir.

Daha önce bahsedildiği ve aşağıda gösterildiği gibi, kaydırıcının yanındaki seçim listesinde birkaç ücret tahmin algoritması vardır: Static, ETA ve Mempool. Statik sabit bir orandır ve piyasa koşullarını dikkate almaz. ETA ve Mempool, ücret piyasası koşullarına göre uygun ücretler önermektedir. ETA durumunda, imlecı ücret kaydırıcısının üzerinde duraklatırken, işlemin kaç blok içinde onaylanacağını gösteren bir

araç ipucu alırsınız. Ortalama olarak, bir bloğun mayınlanması 10 dakika sürer. Mempool durumunda, bu, daha fazla ödeme yapan doğrulanmamış işlemlerin boyutu olacaktır.

Daha fazla bilgi için: <https://bitcoinelectrum.com/how-to-manually-set-transaction-fees/>



Her ücret tahmin algoritması seçeneği için, ücret kaydırıcısı ayarlanabilir. Aşağıda, "ETA" seçeneği için başka bir örnek olarak, ücret kaydırıcısı (az çok yarıya kadar) sola taşınır. Bu durumda, el koyma işlemini blok zincirindeki 5 blok içinde onaylamak ve kaydetmek hedeflenmiştir ve maliyet şimdi miktarın %6,54'üdür. Bitcoin fiyatındaki rekor yükseklikler nedeniyle yazım esnasında ağ çok sıkışık olduğundan yüzdenin yüksek görüldüğünü yine unutmayın. Ayrıca, kaydırıcıyı ne kadar sola sürüklerseniz, ücret o kadar düşük olur, ancak işlemin onaylanması da bir o kadar uzun sürer. Bunun tersi de sağ taraf için geçerlidir.

Amount to be sent: 0.00083122 BTC (13.14 EUR)

Advanced

Mining fee: 0.00005434 BTC (0.86 EUR)

Fee rate: ETA

Warning: The fee for this transaction (6.54% of amount)

Target: Within 5 blocks
Current rate: 28.3 sat/byte

Password

Cancel Send

Cüzdan şifre korumalı ve şifrelenmişse, paralara etkili bir şekilde el koymak için bir şifre gerekecektir. Şifreyi girdikten sonra "Gönder" i tıklayın, ödeme aşağıda gösterildiği gibi gönderilecektir.



Yukarıdaki ekran görüntüsündeki alfanumerik sayı, bu el koyma işleminin kriptografik özetini veya "İşlem Kimliğini" ifade eder. Bu numarayı kullanarak işlemin durumu bir blok zinciri gezgini aracılığıyla blok zinciri içinde kontrol edilebilir, örneğin:

<https://www.blockchain.com/btc/tx/d00b510ab0dd7ae2ee51976937ff93de3f9a1b7688cf53ea691379a954b631ff>

Bu el koyma işleminden hemen sonra, el konulan cüzdanımızın işlem geçmişi aşağıdaki gibidir:

Date	Description	Amount	Balance
Unconfirmed [rbf, 53.8 sat/b, 0.37 MB]	Seizure Target X	-0.00088556	0.
2020-12-15 07:50		+0.00088556	0.00088556

Balance: 0.00088556 BTC (13.99 EUR) [-0.00088556 unconfirmed] 1 BTC~15,798.65 EUR

Gördüğünüz üzere, el koyma işlemi henüz doğrulanmamış durumda.

Bazı önemli açıklamalar

- Gerçek el koymadan önce yapılan herhangi bir test işlemi olamaz. Suçlular paylaşılan bir cüzdan kullanıyorsa, yetkisiz bir işlem fark edilirse, yerinde güvenlik önlemleri olabilir.
- El koyma zaman açısından kritiktir ve el koyma işlemi tek bir işlemde ve nispeten yüksek bir ücretle yapılmalıdır, böylece diğerleri Mempool'da işlenmeyi beklerken (yeni bir bloğa mayınlı) işlemin yerini alamaz.
- Electrum bir bilgisayarda açık olduğunda, (yasalar ve geçerli prosedürler izin verirse) aynı bilgisayarda başka mevcut Electrum cüzdanları olup olmadığını kontrol etmek iyi bir uygulamadır. Aşağıdaki örnekte gösterildiği gibi, Electrum menüsünden "Dosya" > "Son zamanlarda açılanlar" seçeneğini seçerken, bu bilgisayarın en az 5 farklı Electrum cüzdanı içerdiğini göreceksiniz.

File	Wallet	View	Tools	Help
Recently open				
Open		⌘O		default_wallet ⌘1
New/Restore		⌘N		mooze_shady ⌘2
Save backup		⇧⌘S		shady_stuff ⌘3
Delete				shady_stuffx ⌘4
				wallet_1 ⌘5

Hatta daha da iyisi, "Aç"a tıkladığınızda, örneğimizde sekiz Electrum cüzdanı içeren bir "cüzdanlar" klasörüne yönlendirileceksiniz. Bu cüzdanlardan biri "wallet_test1" olarak adlandırılır (bu cüzdan yukarıda gösterildiği gibi "Son zamanlarda açılanlar" altında listelenmez) ve aşağıdaki ekran görüntüsünde görebileceğiniz üzere, şifreyle korunmaktadır. Bir cüzdan şifreyle korunup şifrelendiğinde yalnızca bir işlemi yürütmek için değil, bu cüzdanı açmak için de bir şifre gerekir.

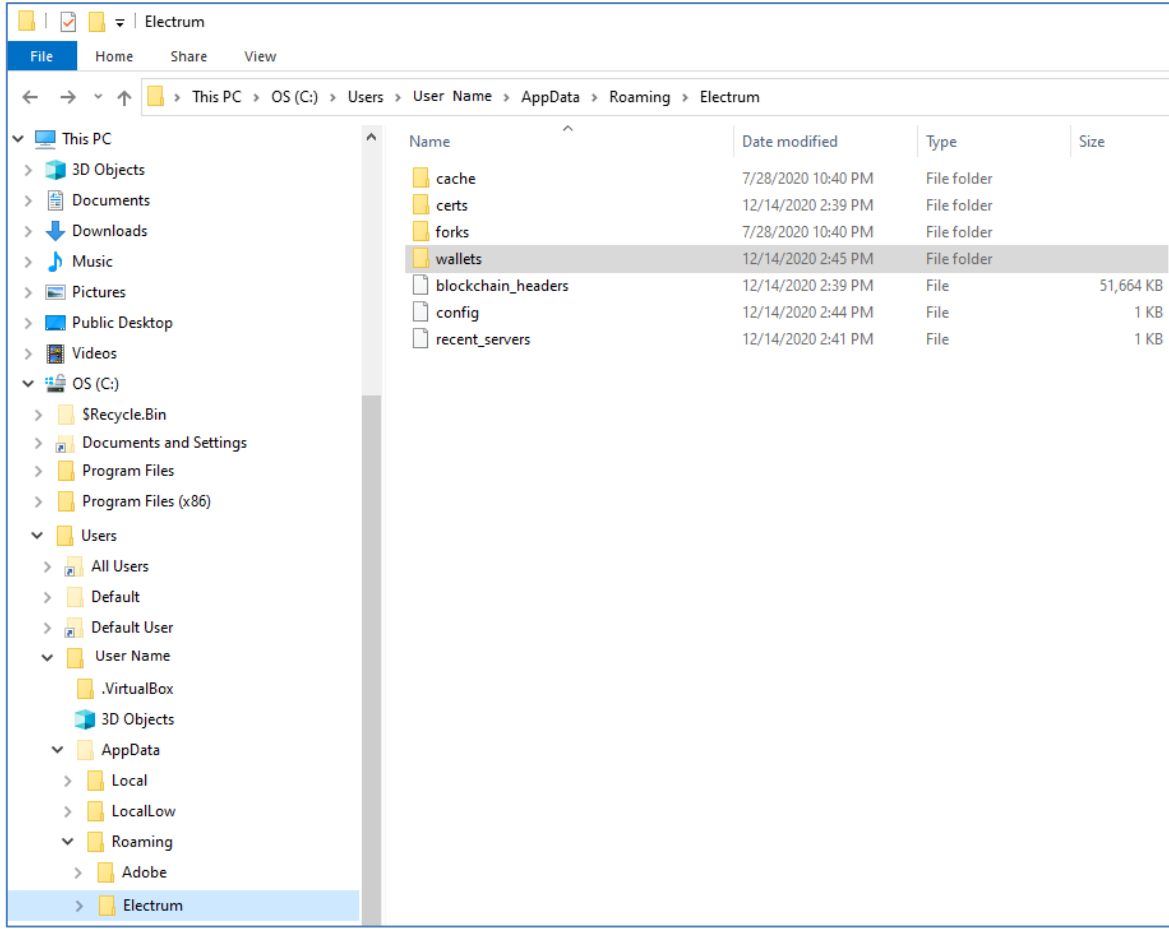


Şüphelinin Electrum cüzdanlarını bilgisayarındaki herhangi bir yerde saklayabileceğini unutmayın. Ayrıca, bir bilgisayar farklı cüzdan yazılımları içerebilir. Ülkenizdeki yasalar ve geçerli prosedürler izin veriyorsa, çalışan işlemler bir Windows bilgisayarında örneğin Görev Yöneticisi kullanılarak kontrol edilebilir(CTRL+ALT+DEL). Ayrıca, cüzdan yazılımının olup olmadığını anlamak için bilgisayarı (örneğin masaüstündeki) simgeleri vb. aracılığıyla kontrol edebilirsiniz.

Cüzdan dosya(lar)ının varsayılan yerleri:

Windows

- Gizlenen dosyaları göster (yukarıya bakınız)
- Gözet: Users\YourUserName\AppData\Roaming\Electrum\wallets



Linux

Bitcoin datasını varsayılan olarak şuraya koyacaktır: ~/.electrum

Nokta ile başlayan dizinleri görmek için bir "ls-a" yapmanız gerekir.

Mac

- Bulucuyu aç
- Dosyaya git (shift+command+G) ve ~/.electrum çeşidi

Şifre korumalı ve şifrelenmiş standart bir Electrum cüzdanı, ilgili anahtar ifadesini bulurken atlanabilir. Bu cüzdan daha sonra Electrum kurulum sihirbazı aracılığıyla geri yüklenebilir ve sihirbaz "Yeni bir anahtar oluşturmak mı yoksa mevcut anahtarı kullanarak cüzdanı geri yüklemek mi istiyorsunuz?" diye sorduğunda, daha sonra (aşağıda gösterildiği gibi) "Zaten bir anahtarım var" seçeneği seçilmelidir ve bulunan anahtar ifade bir sonraki adımda girilebilir. Bundan sonra, bu cüzdan anahtar ifadesiyle yeniden yüklenecektir. İsteğe bağlı olarak, bu geri yüklenen cüzdan için yeni bir şifre seçilebilir. Yeni yüklenen bu cüzdandan bir el koyma işlemi yapılabilir.



3.3.4 Exodus

- Anahtar kullanımı: 12 kelimelik bir anahtar ifade kullanılabilir (MetaMask, Jaxx Liberty ve daha fazlasıyla uyumlu)
- Şifre kullanımı: var (sadece cüzdana erişmek için)
- Değişim işlevi: var



Exodus, 120'den fazla kripto para ve tokenı (jetonu) destekleyen popüler bir çoklu para birimi cüzdanıdır. Kullanıcılar, cüzdanın kendisindeki diğer kripto para ile para alışverişi yapabilirler.

(Bir şifre ile erişildikten sonra) bu cüzdanın "otomatik kilit"e gidebileceğini unutmayın. Kullanıcı bunu ayarlarda tanımlayabilir ve 5 dakika ile 2 saat arasında yapılandırılabilir (veya hiç yapılandırılmayabilir).

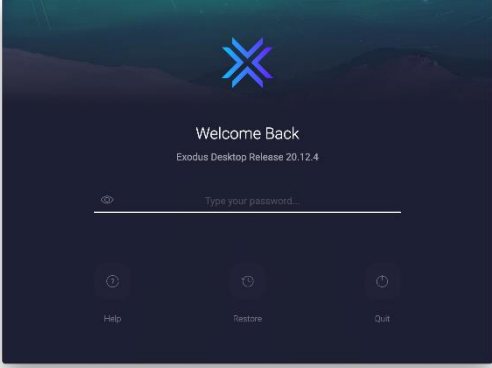
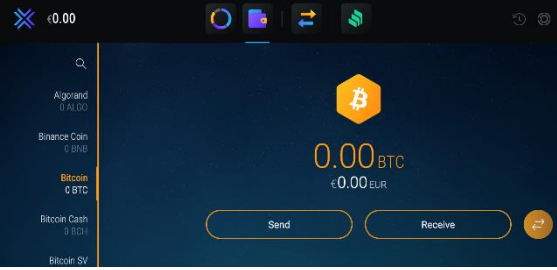
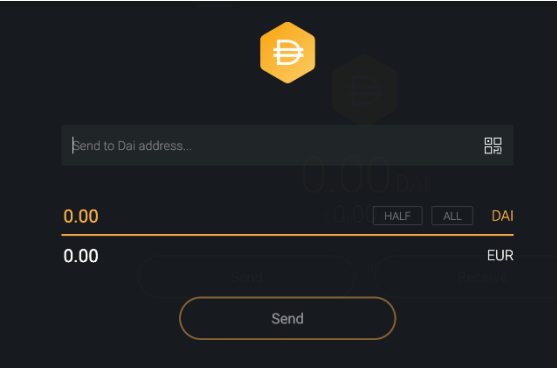
Masaüstü cüzdanı bir mobil sürümle eşleştirebilir ve kullanıcılar bir Trezor donanım cihazıyla bile eşleştirebilir. Trezor (T veya One model) ekstra güvenlik için özel anahtarlarını çevrimdışı tutacaktır.

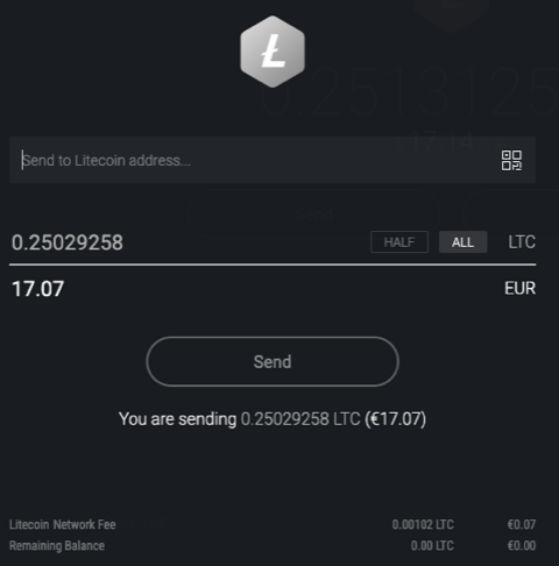
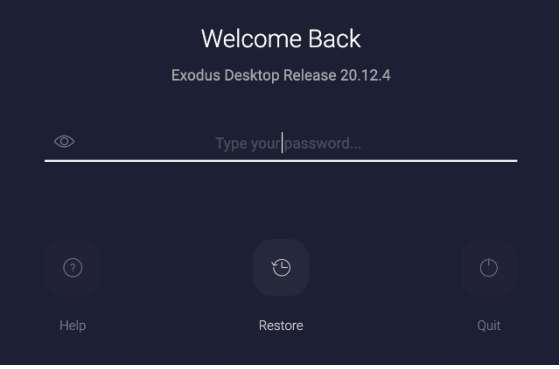
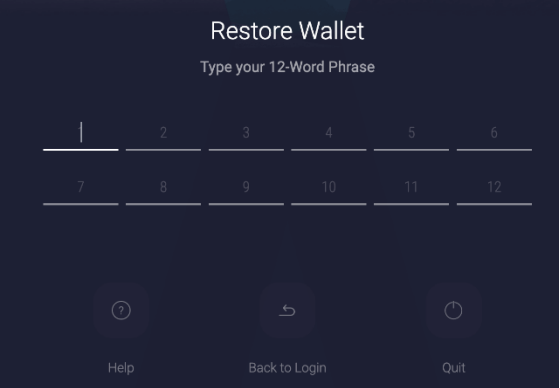
Sıfır bakiyesi olmayan varlıklar gizlenemez (ancak bu Jaxx Liberty'de yapılabilir).

Diğer kripto paraları cüzdanda takas ederken, dalgalı minimumlar ve maksimumlar olduğunu unutmayın²⁶.

²⁶ Daha fazla bilgi için lütfen şu adresi ziyaret edin: <https://support.exodus.io/article/787-how-do-i-exchange-assets-in-exodus#>

Exodus'da El Koyma İşlemi (Masaüstü sürümü)

	Exodus'u başlatırken, cüzdana erişmek için bir şifre gereklidir. Hiçbir şifre bulunmadığında (veya şüpheli işbirliği yapmazsa), paralara el koymanın başka bir yolu yoktur. Tek yol anahtar ifadeyi, bulmak ve cüzdanı bununla yeniden yüklemektir.
	Cüzdana erişildiğinde, fonları olan kripto paralardan birine tıklayın. Çok para birimli bir cüzdanda, her kripto para birimi ayrı ayrı ele geçirilmelidir. Ethereum tokenları (jetonları) için, önce tokenları sonra Ether'in kendisini (ETH) gönderin.
	Örneğin: DAI DAI, Ethereum ağında \$ 1.00 USD değerini korumaya çalışan istikrarlı bir coindir. Bu, DAI tokenlarına (jetonlarına) el koymak için bir Ethereum adresine ihtiyacınız olduğu anlamına gelir. Yine, Ethereum tokenları ile uğraşırken, önce tokenları sonra Ether'i (ETH) gönderin.

	Bu ekran görüntüsü cüzdandaki bazı Litecoinleri göstermektedir. Mevcut maksimum göndermek için "Tümü"ne tıklayın. İşlem maliyetleri uygulamanın alt kısmında gösterilir. Bilginize: Tabii ki, el koymanın bu kısmı bir Litecoin adresine ihtiyaç duyacaktır. Eski Litecoin adres formatı 3 ile başlarken (ki bu, bir Bitcoin adresi için çok kafa karıştırıcıydı), yeni Litecoin adres formatları M, LTC1 (bech32) ile başlar. Litecoin'i cüzdanınızda Bitcoin ile değiştirmek isterseniz, lütfen ülkenizdeki yasaların buna izin verip vermediğini kontrol edin ve bu takaslarda minimum ve maksimumlar olduğunu unutmayın.
	Bir anahtarın bulunması durumunda; Bir anahtar bulunduğunda, cüzdanı yeniden yüklemek için anahtarı kullanabilirsiniz.
	12 kelimelik gizli ifadeyi büyük harf olmadan sırayla yazın. İşiniz bittiğinde sağdaki oku tıklayın. Birkaç saniye sonra, Exodus "Hepsi tamam!" diyen bir pop-up ile açılacaktır. Tamam'a tıklayın ve Exodus blok zincirlerini yeniden tararken ve bakiyeleri gösterirken birkaç dakika bekleyin.

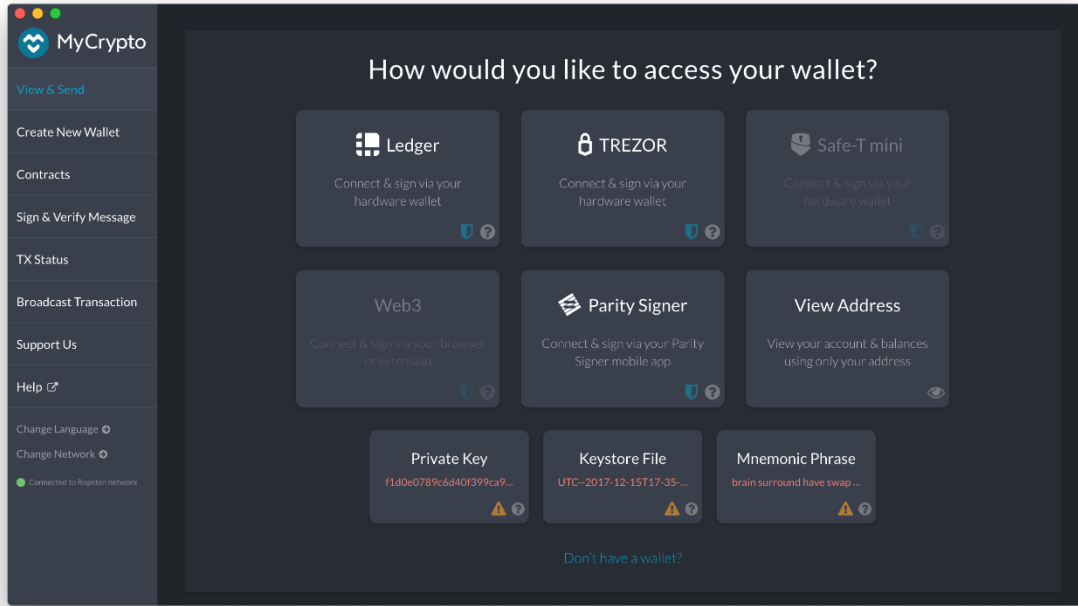
Bu nedenle, ele konulacak her kripto para için, hantal olabilecek ve devlet kontrolünde bulunan ilişkin bir el koyma adresine ihtiyaç duyulacaktır.

Örneğin, bitcoinler için Bitcoin adresi, litecoinler için bir Litecoin adresi gerekmektedir.

3.3.5 Ethereum Cüzdanları

3.3.5.1 MyCrypto Cüzdanı

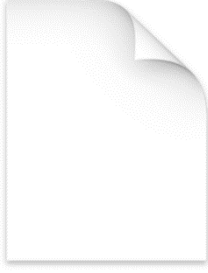
- Anahtar kullanımı: 12 kelimelik bir anahtar kullanılabilir (MetaMask, Jaxx ve daha fazlasıyla uyumlu)
- Şifre kullanımı: var
- Cüzdan dosyası kullanımı: isteğe bağlı, KeyStore dosyası olarak adlandırılır



MyCrypto cüzdanına (yanı sıra MyEtherWallet'a) birçok şekilde erişilebilir. Örneğin, bir Ledger veya Trezor donanım cüzdanı ile birlikte kullanabilirsiniz, ancak kullanıcılar Mycrypto'nun kendisinde yeni bir cüzdan dosyası da oluşturabilirler ("Yeni cüzdan oluştur").

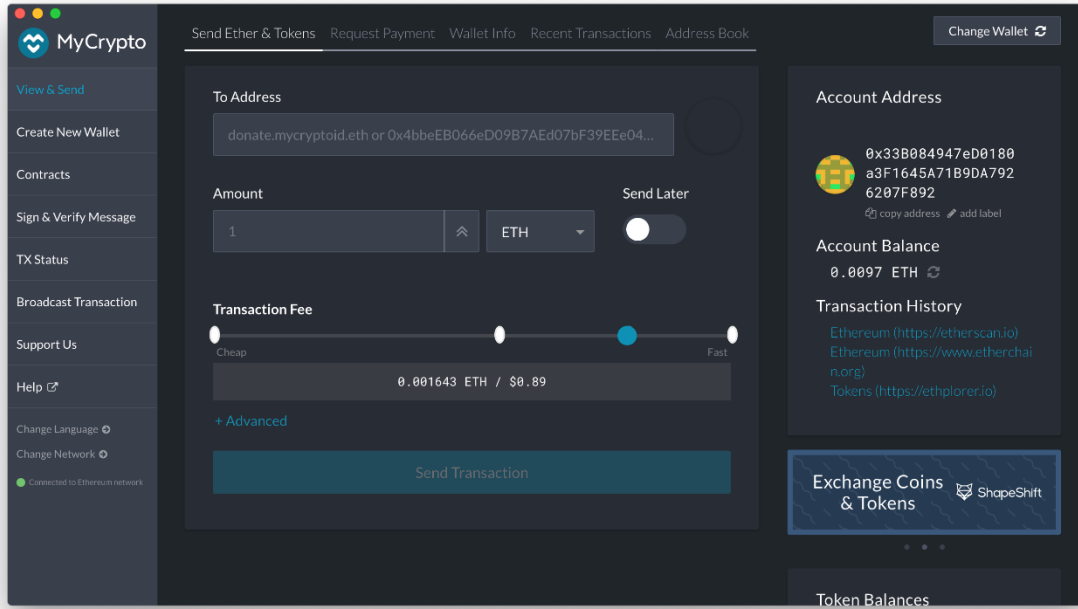
Şüphelinin makinesinde bu cüzdana erişirken, önce "KeyStore Dosyası" düğmesine tıklamanız önerilir, çünkü varsayılan olarak (bir KeyStore Dosyası oluşturulduğu sürece), sizi bu dosyanın bulunduğu doğru klasöre götürecektir. Uyarı: Bu dosya şifre korumalı!

Bir KeyStore dosyası (örneğin aşağıdaki ekran görüntüsü) işlemleri imzalamak için kullanılan özgün bir Ethereum özel anahtarının şifrelenmiş bir sürümüdür. (Kullanıcı dosyayı yeniden adlandırmadıysa) Varsayılan olarak, UTC-- ve bir zaman damgası ile başlar:



UTC--2020-03-09T11-4
7-05.877Z-...18facbb021

Document - 489 bytes



MyCrypto (ve diğer Ethereum cüzdanları) can store both Ethereum (ETH) and Ethereum tokens.

MyCrypto'da El Koyma İşlemi

Bu cüzdana çeşitli yollarla erişim sağlanabilir:

- KeyStore dosyası ve şifresi
- Özel bir anahtar ve şifresi
- Bir anahtar (hatırlatıcı ifade)
- Bir donanım aygıtı (Ledger veya Trezor) bulundu ve PIN kodu bilinmekte. Bu durumda, Ledger ve Trezor'a özgü uygulamaları kullanmak daha iyidir.

Linke tıklayarak Etherscan.io adresindeki Ethereum adresini kontrol edin ve ERC-20 token (jeton) stokunu genişletin. Bu şekilde tam bakiyeyi ve bu adrese bağlı olan tüm ERC-20 tokenlarını görebilirsiniz. Bir Ethereum adresinde çok sayıda ERC-20 tokenı olabilir.

Transaction History

Ethereum (<https://etherscan.io>)

Ether Value: \$5.24 (@ \$540.33/ETH)

Token: \$0.00 2

View expanded ERC-20 token holding

MyCrypto'ya dönünce, "Tokenlar için Tara" ya tıklayın (sağ altı).

Token Balances

No tokens found

Add Custom Token

Scan For Tokens

MyCrypto'ya özel bir token eklemek

Etherscan web sitesi ERC-20 tokenlarını gösterdiğinde ve MyCrypto göstermediğinde, "Özel Token Ekle"yi tıklayarak bunları Mycrypto'ya ekleyebilirsiniz.

Sonra, Etherscan'da, MyCrypto'ya eklemek istediğiniz tokenın adına tıklayın (bu durumda, "Training Token").

Training Tok... TT 55,000

0x54658e84a78d78a39e87...

Ve Training Token'ın sözleşme adresini kopyalayın.

Profile Summary [Edit]

Contract: 0x54658e84a78d78a39e872f74d79bae1cb29fad70

Copy address

Ardından, "Özel Token Ekle" yi tıklayarak bu adresi Mycrypto'ya yapıştırın, tüm alanlar otomatik olarak doldurulacaktır ve Kaydet'i tıklayın.

Token Balances

No tokens found

Address

039e872f74d79bae1cb29fad70d

Decimals

18

Token Symbol

TT

Balance

55000000000000000000000000000000

Need help? [Learn how to add custom tokens.](#)

Cancel

Save

El koyma işlemi devam etti

The screenshot shows the MetaMask wallet interface. At the top, there are tabs: 'Send Ether & Tokens', 'Request Payment', 'Wallet Info', 'Recent Transactions', and 'Address Book'. A 'Change Wallet' button is in the top right. The main area is divided into two columns. The left column contains the 'To Address' field with the address '0x5C04BE4Ec4052393C17B674833a1440c610b7c2b', an 'Amount' field set to '1', a 'Send Entire Balance' button, a 'Send Later' toggle, a 'Transaction Fee' slider set to 'Cheap' with a value of '0.00028 ETH / \$0.15', and a 'Send Transaction' button. The right column shows the 'Account Address' as '0x33B084947eD0180a3F1645A71B9DA7926207F892', the 'Account Balance' as '0.0097 ETH', and a 'Transaction History' section with links to 'Ethereum (https://etherscan.io)', 'Ethereum (https://www.etherchain.org)', and 'Tokens (https://ethplorer.io)'. At the bottom right, there is a 'Buy ETH with Credit Card' button with a 'simplex' logo.

Bir Ethereum cüzdanında el konulması gereken ilk varlıklar Ethereum tokenlarıdır. Bunun nedeni, cüzdandaki Ether (ETH)'in de gaz (işlem) fiyatını ödemek için kullanılacak olmasıdır.

"Adres" bölümünde, devlet tarafından kontrol edilen Ethereum adresini doldurun (Bu adres 0x ile başlar).

Tüm tokenlar (jetonlar) Ethereum el koyma adresine gönderildikten sonra, Ether'in kendisine (ETH) de el konulabilir. Token(lar)a el koymak için kullandığınız Ethereum adresini kullanın.

El koyma adımları

- Seçim listesine tıklayın ("Miktar" ın sağında) ve el konulması gereken tokenları seçin.
- "Tüm Bakiyeyi Gönder" i tıklayın, böylece tüm tokenlara el konulacaktır (örnekte, tüm TT tokenları)
- Daha hızlı (ancak daha pahalı) işlemler için "İşlem Ücreti" kaydırıcısını sağa kaydırın
- İşlem Gönder düğmesine basın

Diğer her token için aynı manipölasyonu yapın ve Ethereum (ETH) ile el koymayı bitirin.

3.3.5.2 Metamask

- Anahtar kullanımı: var
- Şifre kullanımı: var
- Swap özelliği: var

Metamask, Ethereum cüzdanı olarak hizmet veren bir tarayıcı uzantısı (Tilki simgesi) olarak kullanılabilir²⁷. Bir mobil uygulama olarak da mevcuttur, ancak bu kılavuz sadece tarayıcı uzantısını kapsayacaktır.

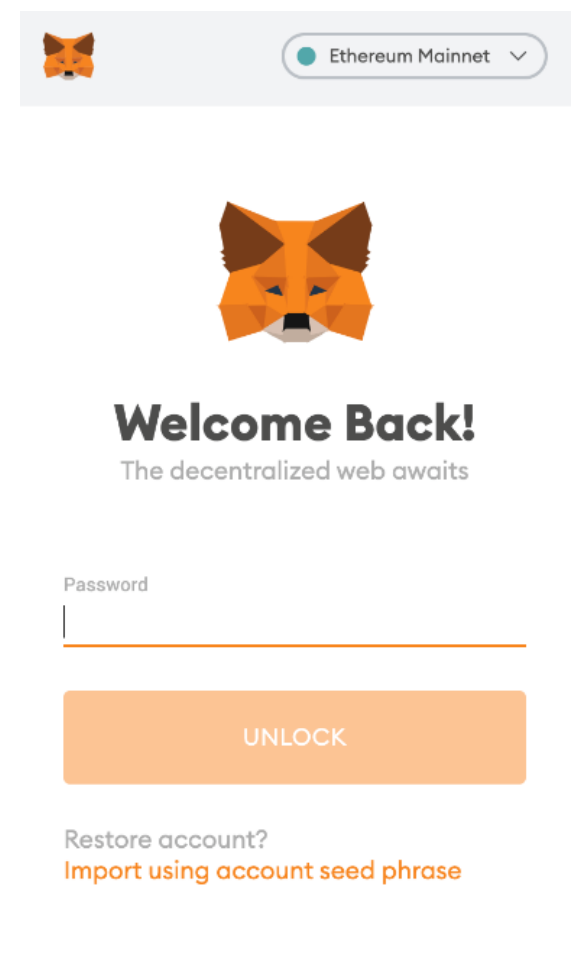


Diğer Ethereum cüzdanlarında olduğu gibi, kullanıcılar Ethereum tokenlarının yanı sıra eter (ETH) depolayabilirler.

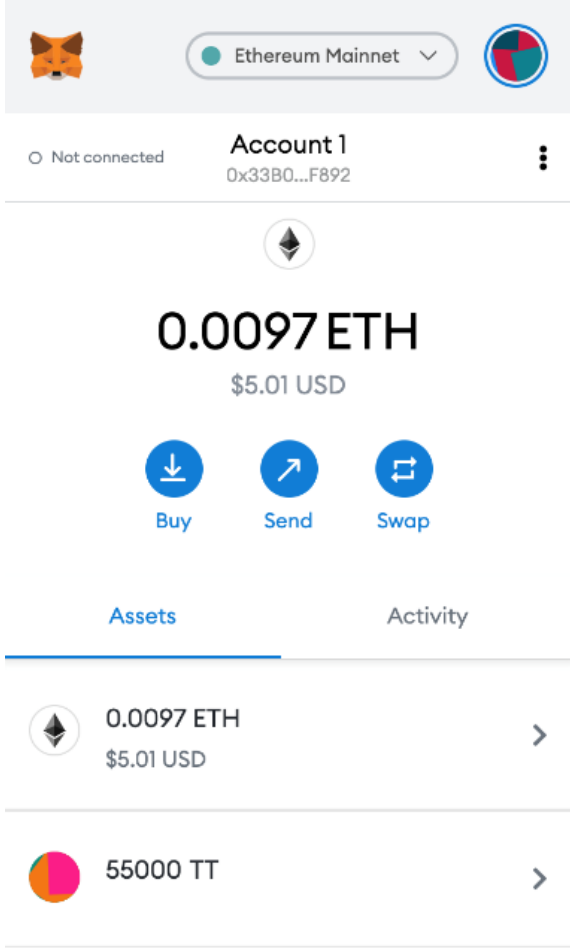
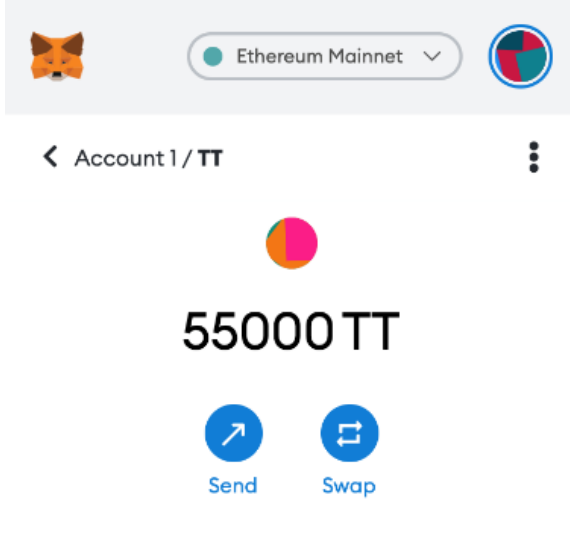
Cüzdan ayrıca merkezi olmayan uygulamalarla (dApps), örneğin Uniswap (merkezi bir değişim) ya da Compound (a DeFi uygulaması) etkileşime girebilir.

Metamask'da El Koyma İşlemi

1. Seçenek: şifre bulunduğunda

 The image shows the Metamask login interface. At the top, there is a small fox icon and a dropdown menu set to 'Ethereum Mainnet'. Below this is a large orange fox head icon. The text 'Welcome Back!' is prominently displayed, followed by 'The decentralized web awaits'. There is a 'Password' label and a text input field. Below the input field is an orange 'UNLOCK' button. At the bottom, there is a link that says 'Restore account? Import using account seed phrase'.	Bu cüzdana erişebilmek için bir şifreye ihtiyacınız var. Tipik bir Metamask şifresi en az 8 karakterden oluşur. Alternatif olarak, bir anahtar ifade bulduysanız ancak şifre yoksa, "Hesap anahtar ifadesini kullanarak içe aktar"ı tıklayın.
---	---

²⁷ Metamask ile ilgili daha bilgi için: <https://docs.metamask.io/guide/>

	Şifreyi kullanarak, burada gösterilene benzer bir ekran göreceksiniz. Burada, bu cüzdandaki varlıklara ilişkin genel bir bakış elde edersiniz. Fark ettiğiniz üzere, bu cüzdanda 0.0097 ETH ve 55000 TT tokenlar var. Bu cüzdanın cüzdan adresi, varsayılan bir ad olan "Account 1"ın altında belirtilmiştir. Gerekirse, sadece üzerine tıklayarak kopyalanabilir. Hesabın (Account) yanındaki Menü simgesine tıklayın (3 puan) ve el koymak için herhangi bir önemli tokenı kaçırmadığınızdan emin olmak için "Etherscan'da Görüntüle" ye tıklayın.
	Cüzdanda herhangi bir token (jeton) görürseniz, önce tokena tıklayarak onlara el koyun ve bunları devlet tarafından kontrol edilen el koyma adresine göndermek için "Gönder" e basın. İşlem ücretinin yanındaki "Hızlı"yı (Fast) tıklayın. Hızlı, "daha fazla işlem maliyeti" anlamına gelir, ancak işleminiz daha hızlı onaylanır.

Send Tokens

Cancel

Seizina Address

0x5c04be4ec4052393c17b674833a1440c610b7c2b

Asset:

TT

Balance: 55000 TT

Amount:

0 TT

Max

No Conversion Rate Available

Transaction Fee:

Slow

0.00056 ETH

\$0.29

Average

0.00063 ETH

\$0.33

Fast

0.00081 ETH

\$0.42

Advanced Options

Sonraki'ne tıklayın.

Reject

Confirm

Bu tokena el koymak için Onayla'yı tıklayın.

Devlet kontrolündeki Ethereum adresine el koymak için, cüzdandaki her tokena ayrı ayrı el konulmalıdır.

Şüphelinin, kendisinin kontrol ettiği bir adrese kripto paraları gönderen gizli bir komut dosyası koymuş olabileceğini unutmayın.



Ethereum Mainnet



Send ETH

Cancel

 **Seizing Address**

0x5c04be4ec4052393c17b674833a1440c610b7c2b

Asset:

 **ETH**

Balance: 0.009698 ETH

Amount:

0 ETH

\$0.00 USD

Max

↑↓

Transaction Fee:

Slow	Average	Fast
0.00028 ETH \$0.14	0.0003 ETH \$0.16	0.00041 ETH \$0.21

Advanced Options

Cancel

Next

Son olarak, ETH'ye tıklayın ve maksimum Ethereum miktarını ("Max" e tıklayın) aynı el koyma adresine gönderin.

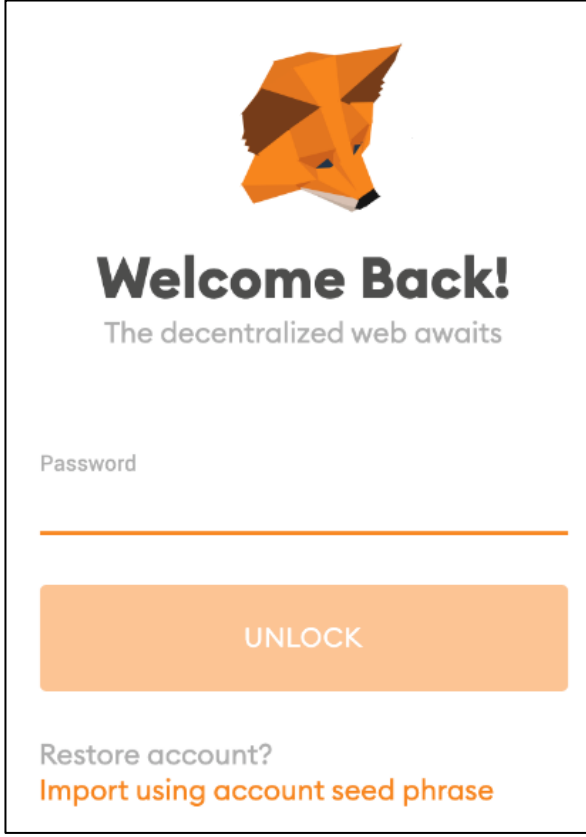
Yine, işlem ücretinin yanındaki "Hızlı'yı tıklayın. Bu biraz daha pahalıdır, ancak el konulan Ether hedef (el koyma) adresinde daha hızlı olacaktır.

Sonraki'ne tıklayın.

Reject

Confirm

Son olarak, el koymak için Onayla'yı tıklayın.

2. Seçenek: sadece anahtar bulunduğunda fakat şifre olmadığında

The image shows the Metamask 'Welcome Back' screen. At the top is the Metamask fox logo. Below it, the text 'Welcome Back!' is displayed in a large, bold font, followed by 'The decentralized web awaits' in a smaller font. A 'Password' label is positioned above a text input field. Below the input field is a large orange button labeled 'UNLOCK'. At the bottom, there is a link that says 'Restore account?' followed by 'Import using account seed phrase' in orange text.

Öncüllerde bir anahtar ifade bulunursa, cüzdanı geri yükleyebilir ve kendi şifrenizi belirleyebilirsiniz. Bir Metamask anahtar ifadesi 12 İngilizce kelimeden oluşur. Anahtar Ledger, Trezor, Jaxx vb. gibi diğer cüzdanlarla uyumludur. Başlamak için, "Hesap anahtar ifadesini kullanarak içe aktar"ı tıklayın.

 METAMASK

Ethereum Mainnet

[< Back](#)

Restore your Account with Seed Phrase

Enter your secret twelve word phrase here to restore your vault.

Wallet Seed

Paste seed phrase from clipboard

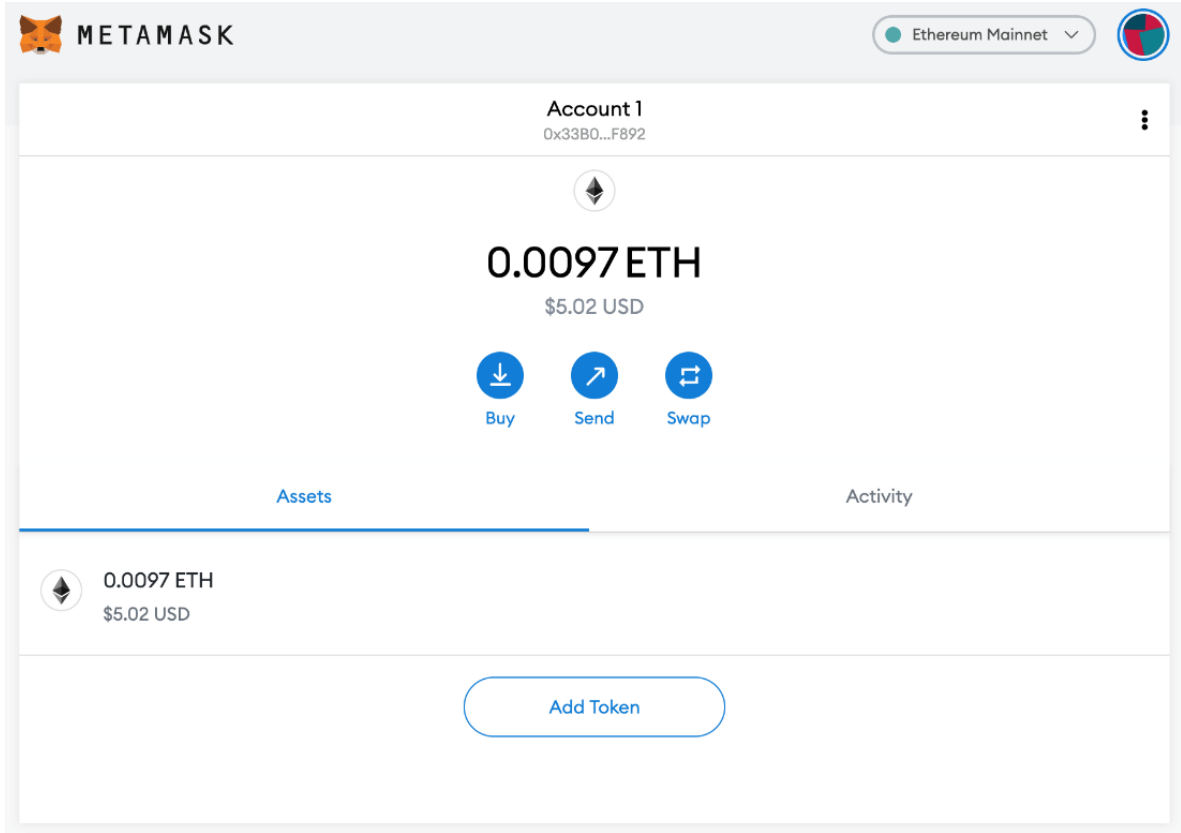
☐ Show seed phrase

New password (min 8 chars)

Confirm password

Restore

Bulunan anahtar ifadeyi yazın, (en az 8 karakterli) yeni bir şifre verin ve onaylayın. Seçilen şifreyi bir kağıda yazın.



Ardından, bir şifre yazmışsınız gibi benzer bir ekran göreceksiniz. El koyma işlemi, yukarıda açıklandığı gibi devam edebilir.

İpucu: Bir anahtar ile geri yükledikten sonra, tüm tokenlar cüzdanda mevcut olmayabilir. Bunu Ethereum blok zincirinde kontrol edebilirsiniz (örn. etherscan.io). Aşağıda, nasıl kontrol edileceği ve cüzdanın Ethereum adresine bağlı olan ancak Metamask'ta görünmeyen bir tokenın (jetonun) nasıl ekleneceği açıklanmaktadır.

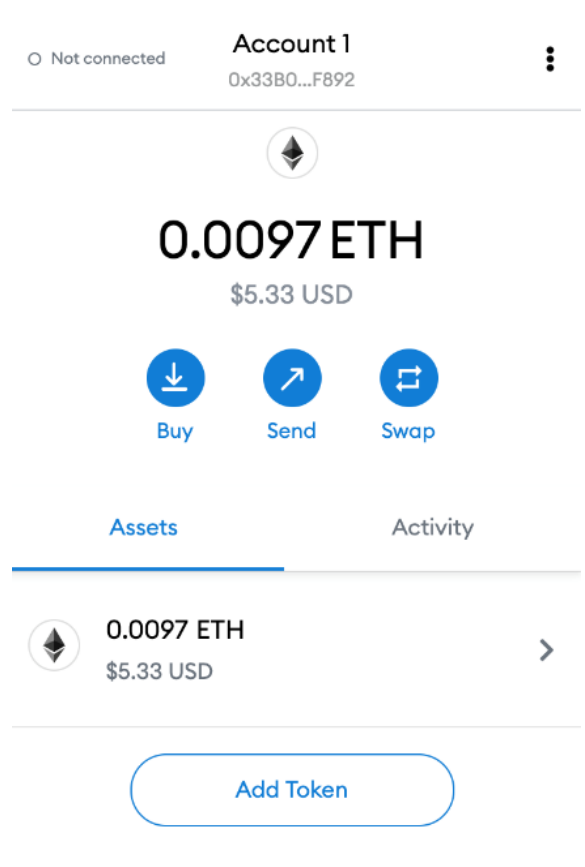
	Hesabın (Account) yanındaki Menü simgesine tıklayın (3 puan) ve el koymak için herhangi bir tokenı kaçırmadığınızdan emin olmak için "Etherscan'da görüntüle"ye tıklayın.
	Erc-20 tokenı tutma görünümünü genişletin ve tokenın adını tıklayın.

	Bu tokenin sözleşme adresini kopyalayın. Token adını tıkladığınızda sayfanın sağ tarafında bunu bulacaksınız (yukarıdaki ekran görüntüsü). Aşağıda açıklandığı gibi devam edin.
---	---

Gördüğünüz gibi, bazen bir tokenin "sözleşme adresini" cüzdana eklemek gerekecektir (bu durumda TT tokeni).

Bilginize: Metamask cüzdanında izlemek için yeni bir token eklerken, form alanlarından biri sizden bir 'Token Sözleşme adresi' ister. Bu, tokenların mantığını yöneten gerçek token sözleşmesinin adres konumunu ifade eder. Kendi kişisel tokenlerinizi tutan adres için bu geçerli değildir²⁸.

Metamask'ta bu nasıl yapılır:

	"Varlıklar" sekmesinde, biraz aşağı kaydırın ve mavi "Token Ekle" düğmesine tıklayın.
--	--

²⁸ <https://metamask.zendesk.com/hc/en-us/articles/360015488811-What-is-a-Token-Contract-Address>

 Ethereum Mainnet  Add Tokens Search Custom Token Token Contract Address 4a78d78a39e872f74d79bae1cb29fad70 Token Symbol TT Edit Decimals of Precision 18 Cancel Next	"Özel Token"ı (sekmeyi) tıklayın. Ekleme istediğiniz tokenın sözleşme adresini yapıştırın. Bu durumda sözleşme adresi şudur: 0x54658e84a78d78a39e872f74d79bae1cb29fad70 Bunu "Token Sözleşme Adresi" alanına yapıştırın. Formun geri kalanı otomatik olarak doldurulacaktır. "Sonraki" ve "Token ekleyin"e tıklayın. Token sözleşme adreslerinin nasıl bulunacağı yukarıdaki tabloda açıklanmıştır. "Sonraki"ne tıklayın.
---	---



Ethereum Mainnet





0.0097 ETH
\$5.33 USD



Buy Send Swap

Assets

Activity



0.0097 ETH
\$5.33 USD



55000 TT

Add Token

Token artık Metamask'ta da görünecektir.

Şimdi şuna tıklayarak bu tokena el koyabilirsiniz:

< Account 1 / TT



55000 TT



Send Swap

Ve sonra, Gönder butonuna tıklayın.

Send TokensCancel ✓ Seizing Address 0x5c04be4ec4052393c17b674833a1440c610b7c2b Asset:  TT Balance: 55000 TT Amount: 55000 TT Max No Conversion Rate Available Transaction Fee: Slow 0.00351 ETH \$1.93 Average 0.00594 ETH \$3.26 Fast 0.00648 ETH \$3.56 Advanced Options Cancel Next	Şimdi, Token Gönder ekranındayız. Devlet kontrolündeki el koyma adresini yapıştırın. "Max"ı tıklayın ve "Hızlı" işlemi seçin "Sonraki"ne tıklayın.
TRANSFER  55000 TT 0 DETAILS DATA GAS FEE 0.006482 \$3.56 AMOUNT + GAS FEE TOTAL 55000 TT + 0.006482 \$3.56 Reject Confirm	Şimdi bir onay ekranı göreceksiniz. Tokenlara el koymak için "Onayla"yı tıklayın. El konulacak başka tokenlar varsa önce bunu yapın. En yüksek bakiyeye sahip jetonlara el koyarak devam etmeniz önerilir. Tüm tokenlara el konulduğunda, Ether'i devlet kontrolündeki aynı Ethereum adresine gönderin.

3.4 Mobil Cüzdan

3.4.1 Giriş

İOS, Android cihazlar ve masaüstü ortamlar için birçok farklı cüzdan türü vardır. Mobil ödemeler ve kullanım kolaylığı, bunu geniş kitlelere yaygın olarak sunduğundan, kripto paraları harcamak ve almak amacıyla QR kodlarını tarayabilmek için bir kripto para uzmanı olmanıza gerek yoktur. Bitcoin.org²⁹'da farklı platformlar için çok sayıda farklı uygulama bulabilirsiniz. Bu bölümde, yaygın olarak kullanılan ve popüler olan birkaç uygulamayı tanıtacağız. Şüphelilerin bilgisayarına veya mobil cihazına eriştiğinizde, bu logolardan birini fark etmek, kripto para kullanımının kesin bir ipucudur.

Operating System

Mobile Desktop

Hardware

User type

Criteria

Features

Below is a list of wallets available for your operating system

Android Wallets

	Control	Validation	Transparency	Environment	Privacy	Fees
Bitcoin Wallet	●	▲	●	▲	▲	●
Bither	●	▲	▲	▲	▲	▲
BitPay	●	▲	▲	▲	▲	▲
BLW	●	▲	▲	▲	▲	▲
BRD	●	▲	▲	▲	▲	●
Eclair Mobile	●	▲	▲	▲	▲	▲
Edge	▲	▲	▲	▲	▲	▲
Electrum	●	▲	▲	▲	▲	●
Mycelium	●	▲	●	▲	▲	▲

● Good ▲ Acceptable ▲ Caution ■ Not applicable

3.4.2 En iyi uygulamalar ve kılavuzlar

Mobil cüzdanlardan el koymak biraz zor olabilir. Devlet kontrolündeki cüzdana erişim için bir QR kodunuz yoksa, bir mobil cihazda yazdığınız göz önüne alındığında, hata yapma konusunda hassas olabilecek adresi elle yazmanız gerekir.

²⁹ <https://bitcoin.org/en/choose-your-wallet>

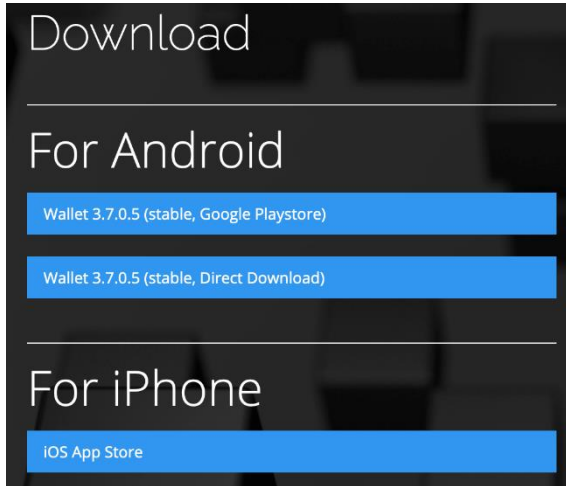
Bununla birlikte, bir QR kodu oluşturmak oldukça kolay olduğundan, bu dönüştürücülerden birinin güvenli bir bilgisayara yüklenmesi önerilir. Tutuklama veya ev aramasına giderken, QR kodunu ve metin dizgisini el koyma işlemi için hazır bulundurmalısınız. Elbette, daha önce hiç duymadığını tamamen yeni kripto paralarla karşılaştığını durumlar olabilir; fakat kripto paralara el konulmasının ve müsadere edilmesinin zaman bakımından ne kadar duyarlı olduğu göz önüne alındığında, çok para birimli bir cüzdana sahip boş bir mobil cihazınızın olması veya hatta -sorumlu kişi tarafından yetkilendirilmişse- bir takas (swap) hizmeti kullanmaya hazır olmanız gerekebilir.

3.4.3 MyCelsius

- 12 kelimelik anahtar ifade kullanır (BIP39 ile uyumlu)
- PIN kodu kullanımı: cüzdan açma ve gönderme için tercihe bağlı
- Bitcoin (BTC) ve ether (ETH) (+ tokenlar) depolayabilir

MyCelsius (Jaxx Liberty ve Exodus'un yanında) en popüler kripto cüzdanlarından biridir ve tıpkı diğerleri gibi, MyCelsius da fonların kaynağını gizlemek için suçlular arasında oldukça popüler hale gelen uygulama içi para değişimi sağlar.

MyCelsius kurulumu, Google hizmetlerine kaydolmadan bir Android telefonda yapılabilir, anonimlik herkes için önemli olduğundan bu kullanışlı olabilir. MyCelsius uygulamasının Android ve iOS'ta doğrudan indirilmesi şu adresten yapılabilir: <https://wallet.mycelsius.com/contact.html>.

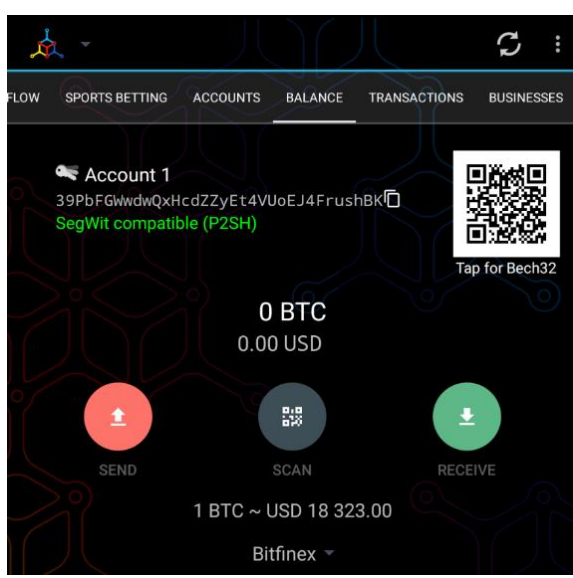


İndirildikten sonra yükleme işlemi oldukça basittir. Önce uygulama dosyasını başlatın ve bu örnekte gösterilen bir Android sürümüdür. Sonra, kabul etmeniz gereken bilinmeyen bir kaynaktan apk dosyasını yüklemek için izin isteyecektir.

Bu cüzdan Tor üzerinden yönlendirilebilir ve Ledger ve Trezor donanım cihazlarıyla uyumludur. Daha fazla bilgi için aşağıdaki web sayfalarını inceleyebilirsiniz:

<https://support.ledger.com/hc/en-us/articles/115005199449-Set-up-Mycelsius-on-Android>
<https://wiki.trezor.io/Apps:MyCelsius>

MyCelsius'da El Koyma İşlemi (araştırmacı tarafından kullanılan ya da bilinen bir PIN kodu yoktur)

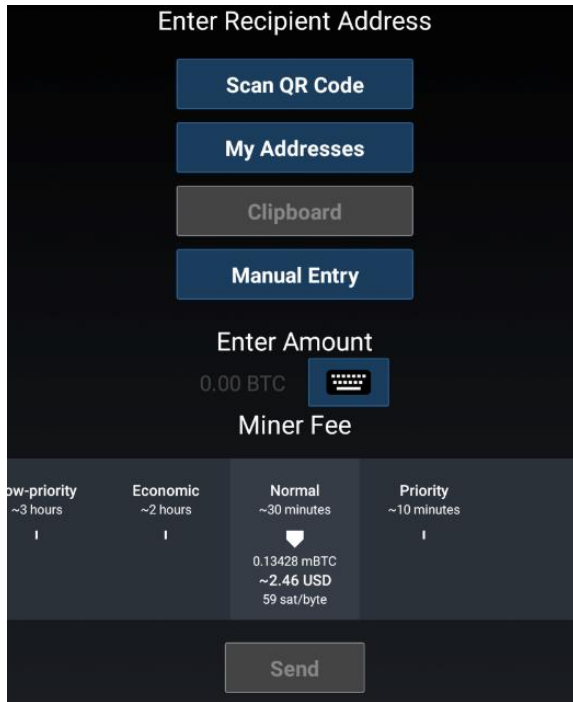


Bakiye ekranında (=ana ekran), cüzdanda ne kadar para olduğunu ve ne tür paralar olduğunu görebiliriz (Bitcoin, Ethereum ya da tokenlar).

Bu ekran görüntüsünde (Bitfinex) aşağıda belirtilenler bizim için geçerli değildir. Bu, bu kullanıcının mevcut Bitcoin fiyatını elde etmek için Bitfinex API'sini seçtiği anlamına gelir.

Bu Bitcoin hesabı (adres 39PbF ile başlar) hiç bitcoin yoktur. Burada el konulacak para yoktur.

Burada biraz para varsa, sadece kırmızı "Gönder" düğmesine tıklayabilirsiniz.



"Gönder"e tıkladıktan sonra, yeni bir ekran çıkacaktır.

(Devlet tarafından kontrol edilen) El koyma adresi, bir QR kodunu tarayarak veya elle buraya girilebilir. Ayrıca, kripto paraları gönderdiğiniz adresi, dört göz kuralını kontrol etmenin güvencelerini de unutmayın.

Elle giriş yapmaktan kaçınılmalıdır çünkü bitcoin adreslerini yazarken kolayca hata yapılabilir.

Bunun yerine kopyala-yapıştır yapmayı deneyin ve adresi iki üç kez kontrole din çünkü adresi değiştirebilecek kötü amaçlı yazılım vardır.

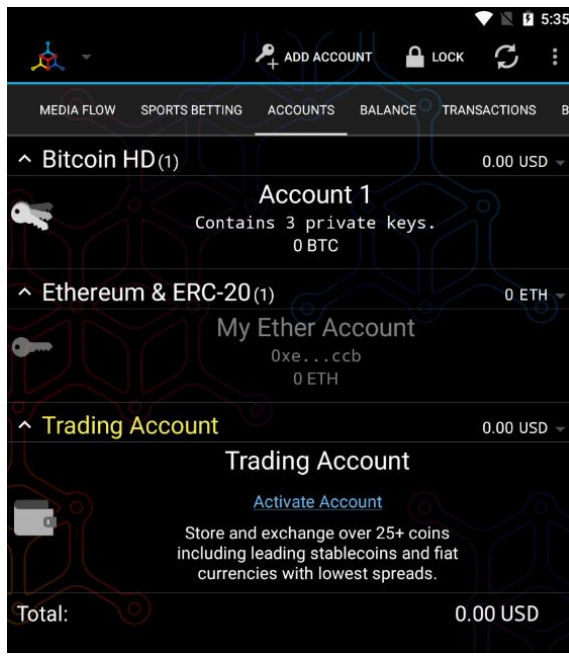
Ardından, toplam tutarı girin veya sadece bitcoinlerin "maximum"u olarak ayarlayın ve bir işlem ücreti seçin. Uygulamada bulunan her hesap için bu işlemi ayrı ayrı yapmanız gerektiğini unutmayın, en büyük bakiyeye sahip olanlarla başlayın.

İşlem maliyeti aşağıda belirtilmiştir ve işlemin Bitcoin ağı tarafından ne kadar hızlı onaylanması gerekiyorsa, ücret o kadar fazla olacaktır.

Ücret ne kadar yüksekse, işlem blok zincirinde o kadar hızlı onaylanır ve olasılık o kadar az olur; nihai suç ortakları cihazlarındaki cüzdanın bir kopyasıyla bunu geçersiz kılabilir.

Son olarak, bitcoinlere el koymak için "Gönder"e tıklayın.

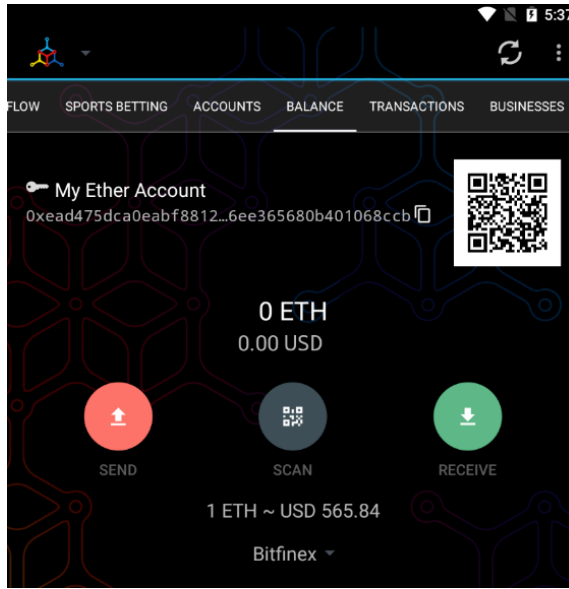
Economic	Normal	Priority	
~2 hours	~30 minutes	~10 minutes	
0.14953 mBTC	0.15701 mBTC	0.16448 mBTC	0.17196 mBTC
~2.74 USD	~2.87 USD	~3.01 USD	~3.15 USD
56 sat/byte	69 sat/byte	73 sat/byte	76 sat/byte



El koyulacak başka kripto paralar olup olmadığını görmek için "Hesaplar"a tıklayın.

Örneğin, bu ekran görüntüsü ayrıca bir Ethereum hesabının olduğunu göstermekte.

"Ethereum & ERC-20"a ve "Bakiye"ye tıklayın.



Şimdi MyCelium'un Ethereum hesabındayız.

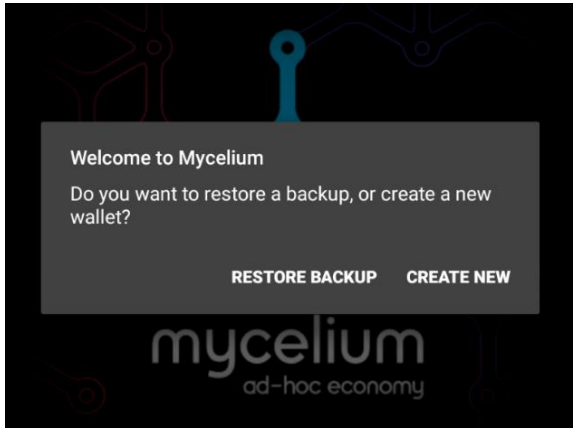
Yukarıda açıklandığı gibi aynı prosedürü izleyin. Herhangi bir ERC-20 tokeni varsa (örneğin, USDC, DAI, BAT, ...) önce onlara el koyun.

Ethereum (ETH) ve tokenlar için aynı Ethereum el koyma adresini kullanın.

Anahtar bulundu

MyCelium, diğer BIP39 uyumlu cüzdanlarla uyumlu olan BIP39 uyumlu 12 kelimelik anımsatıcı bir ifade kullanır³⁰.

³⁰ Uyumlu cüzdanların listesi için şuraya bakınız: <https://www.blockplate.com/blogs/blockplate/list-of-bip39-wallets-mnemonic-seed>

	12 kelimelik anımsatıcı bir ifade bulunduğunda, fonları geri yüklemek için BIP39 uyumlu herhangi bir cüzdan kullanabilirsiniz. Bu ekran görüntüsü MyCelium'un Geri Yükleme ekranını gösterir. Bu 12 kelimeyi yazdıktan sonra, yukarıda açıklandığı gibi Bakiye ekranına ulaşacaksınız.
---	---

3.4.4 Jaxx Liberty

- 12 kelimelik bir anımsatıcı (anahtar ifade) kullanır, ancak varsayılan olarak şifre yoktur.
- Simplex, ShapeShift ve Changelly ile değişimi (swapı) destekler.
- iOS, iPadOS ve Android'deki diğer cihazlar eşleştirilebilir.

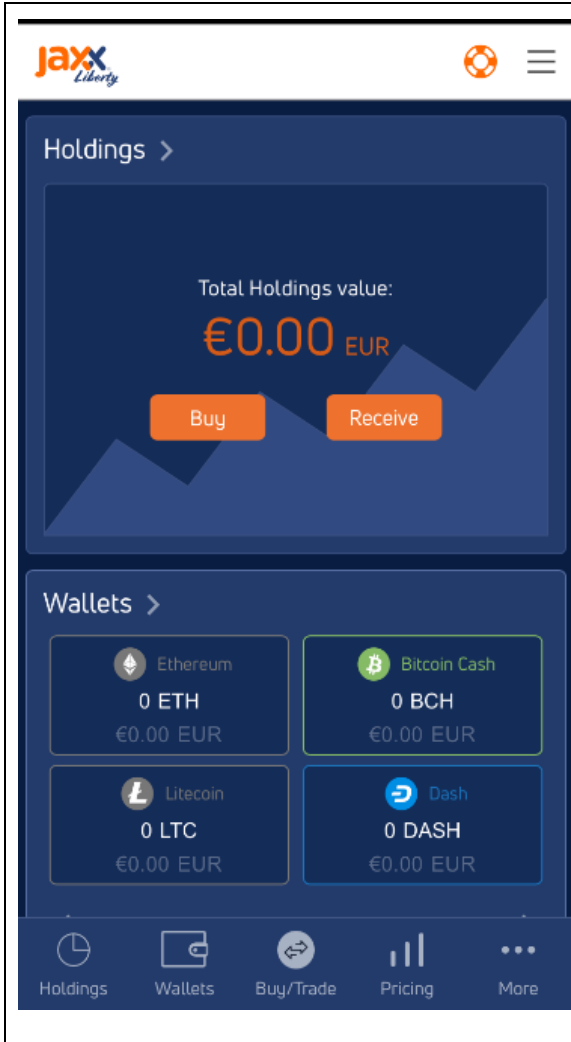
Dikkat:

Bu cüzdandan Bitcoine el koyarken: yerel bir SegWit (Bech32) Bitcoin adresi kullanmayın. Bir Bech32 adresi bc1 ile başlar. Jaxx Liberty (2.4.6 #289 sürümü) bu adreslere gönderemez.

Çözüm: 1 ya da 3 ile başlayan bir Bitcoin el koyma adresi kullanın!

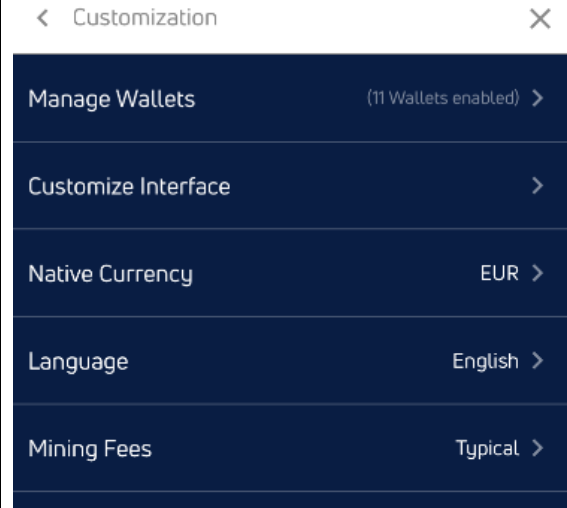
1. Seçenek: şifre bulunduğunda ya da hiç şifre kullanılmadığında

Ön İpucu: kullanıcılar farklı kripto para cüzdanlarını etkinleştirebilir ve devre dışı bırakabilir. Örneğin, kullanıcı Bitcoin varlıklarını Jaxx'te saklamak isterse, cüzdanı devre dışı bırakabilir; böylece "Toplam Tutar değeri" 0 EURO gösterecektir!



Bu olası bir senaryo: cüzdan boş görünüyor, bu yüzden önce devre dışı bırakılmış cüzdanlar olup olmadığını kontrol edelim.

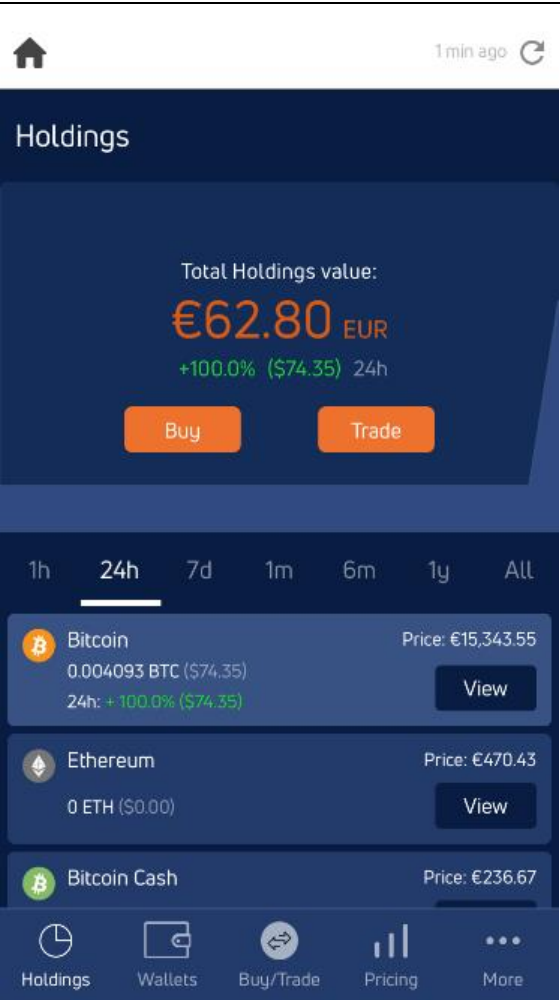
Öğrenmek için sağ üstteki yuvarlak simgeye ve "Cüzdanları Yönet" e tıklayın.





Soldaki ekran görüntüsü Bitcoin cüzdanının devre dışı bırakıldığını göstermekte. Bu cüzdanı etkinleştirmek için anahtarı tıklayın. Ardından, Ana ekrana geri dönün ve "Başlatmak için Tıklayın".





Holdings

1 min ago

Total Holdings value:

€62.80 EUR

+100.0% (\$74.35) 24h

Buy Trade

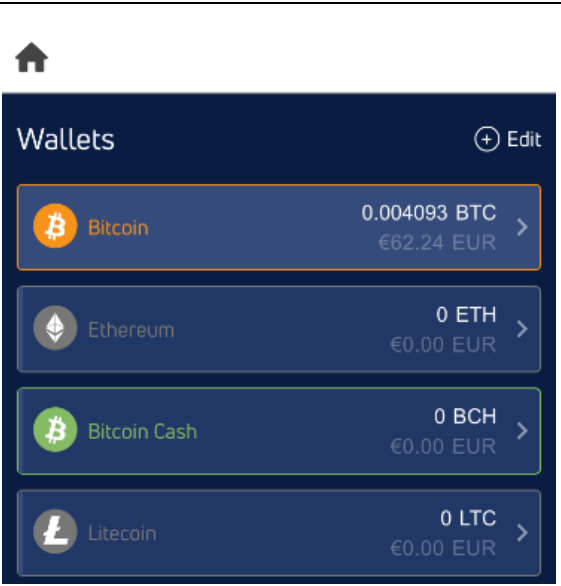
1h 24h 7d 1m 6m 1y All

Bitcoin Price: €15,343.55
0.004093 BTC (\$74.35)
24h: +100.0% (\$74.35) View

Ethereum Price: €470.43
0 ETH (\$0.00) View

Bitcoin Cash Price: €236.67

Holdings Wallets Buy/Trade Pricing More



Wallets

+ Edit

Bitcoin 0.004093 BTC
€62.24 EUR

Ethereum 0 ETH
€0.00 EUR

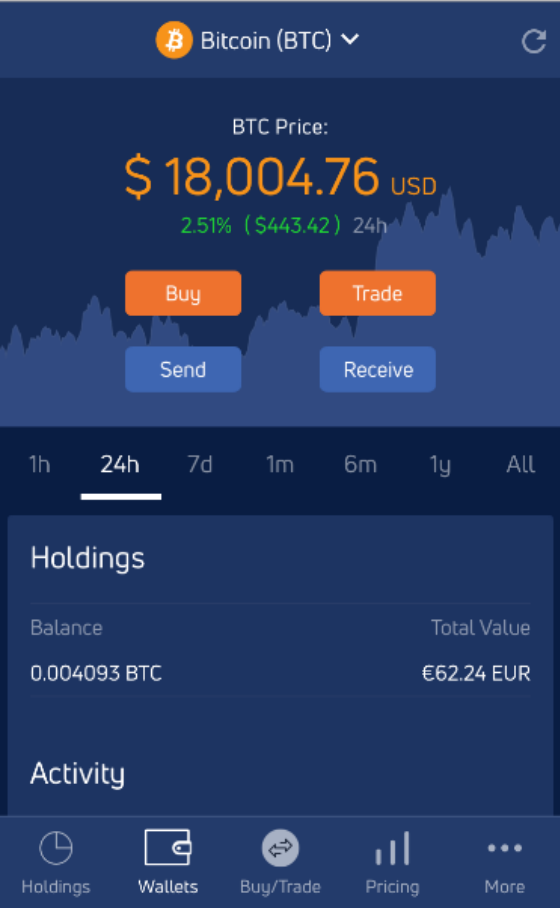
Bitcoin Cash 0 BCH
€0.00 EUR

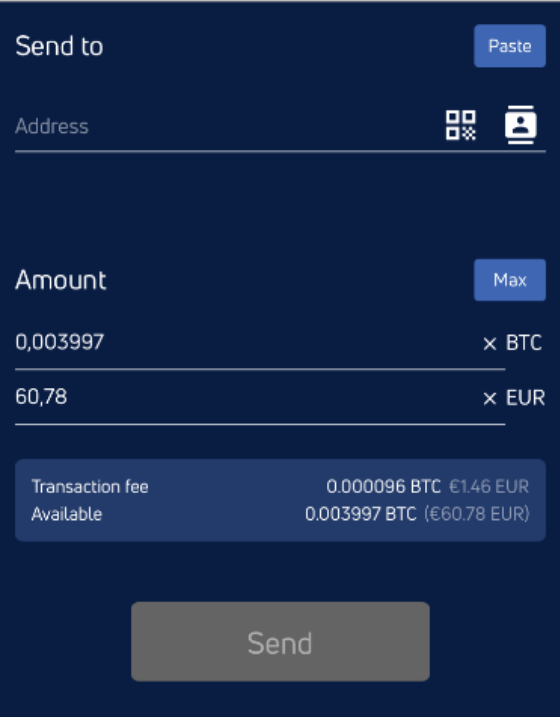
Litecoin 0 LTC
€0.00 EUR

Yalnızca Bitcoin cüzdanında para var.

Paralara el koymak için Bitcoin'e ve tekrar (Cüzdanlar ekranında) Bitcoin'e tıklayın.

El koyma buradan başlayabilir.

	Jaxx Liberty Bitcoin cüzdanında, toplam BTC varlığından bahsediliyor (0.004093 BTC). Bu paralara el koymak için Gönder'e tıklayın.
--	--



Adres'e Bitcoin el koyma adresini kopyalayın.

Tüm miktarı göndermek için "Max"ı tıklayın.

İşlem ücreti aşağıda görünecektir.

El koymak için "Gönder"i tıklayın.

Bu cüzdana başka kripto paralar bulduysanız aynı işlemi yapın.

2. Seçenek: anahtar bulunduğunda

12 kelimelik bir anahtar ifade farklı birkaç cüzdanla kullanılabilir. Şüphelinin cep telefonunda Jaxx varsa, bunun Jaxx için anahtar olma ihtimali vardır. Tüm cüzdanlar aynı türetme yollarını kullanmadığından, farklı cüzdanlara (veya bir araca) sahip bir anahtar kullanmaya çalışın. Bazen, tüm cüzdanlar aynı türetme algoritmasını veya BIP39 standartlarını tam anlamıyla takip etmediklerinden, pozitif bir değer olması gerektiğinde sıfır değeri göstereceklerdir.

3.5 Donanım Cüzdanı

3.5.1 Giriş

Donanım cüzdanları son yıllarda oldukça popüler hale gelmiştir. Bu cüzdanlar birçok farklı kripto para birimi için en iyi ve en güvenli depolama yolu olarak kabul edilmektedir. Ayrıca, belgenin sonunda açıklanan kağıt cüzdandan daha iyi koruma sağladıkları kabul edilmektedir.

Bazı ajanslar için en iyi uygulama, kurcalamaya dayanıklı bir kanıt torbasına konan kağıt cüzdanları kullanmaktır; ancak bazı kolluk kuvvetleri, el konulan varlıklarını korumak için donanım cüzdanları kullanmaktadır. Cihaza sınırlı sayıda kişinin erişimi olduğunda bu sorun olmayabilir. Fakat, PIN kodu her girildiğinde, birisinin ona yetkisiz erişim sağlama ve sonunda cüzdana bulunan sanal paraları çalma riski vardır.

Bu cüzdanların aynı zamanda bir uzlaşma noktası olabilecek tipik anahtar kelime uygulamaları da vardır. Anahtar kelime işlemi ve Ledger cüzdanının nasıl kurulacağı, defter cüzdanının kurulum ve müsadere sürecinde açıklanmıştır.

3.5.2 En iyi uygulamalar ve kılavuzlar

3.5.2.1 Ledger cüzdanı

Son zamanlarda birçok suçlunun, daha güvenli oldukları, birden fazla para birimini depolayabildikleri ve şüphelinin yardımı olmadan açmak veya kaba kuvvet uygulamak çok zor olduğu için donanım cüzdanlarını kullanmaya başladığı görülmüştür.

Bir Ledger cihazı PIN kodu ile korunmaktadır ve 3 yanlış PIN kodu denemesinden sonra kendini temizler/siler; bu da anahtar kelimeler olmadan sanal para verilerinden herhangi birini geri yüklemeyi imkansız kılar. Elinizde birkaç donanım cüzdanı (Ledger, Trezor, KeepKey, vb.) bulundurmanız önerilir, çünkü bazıları aslında onları geri yüklerken farklı özel anahtar kümeleri döndürür ve aynı zamanda oldukça güvenli kabul edilirler. Ayrıca, eğitimlerde bu tür cüzdanların nasıl kurulacağını ve geri yükleneceğini öğrenmek iyidir.

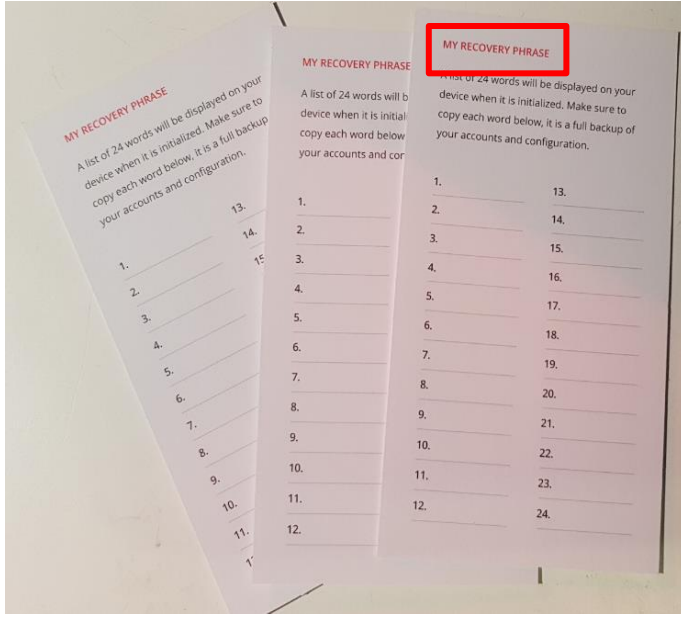
Şimdi bitcoinleri kutudan çıkarmadan ona aktarmaya ve geri yüklemeye kadar temiz bir "Ledger Nano S" cüzdan kurulumunu inceleyeceğiz.



Soldaki resimde ambalajda yeni bir Ledger Nano S gösterilmektedir.

Ekran görüntüsünde görüldüğü üzere, Cihaz normal bir USB cihazına benziyor ve kablo üzerinde ledger logosu bulunan bir mikro USB kablosuyla birlikte geliyor (bu aynı zamanda kripto para kullanımının ya da hatta kutunun kendisinin bir ipucudur).

En önemlisi, bir araştırmacı için Kurtarma sayfası veya KURTARMA İFADEM yazan bir sayfamız var. Bunlar ayrıca soldaki resimlerde gösterilip belirtilmektedir.



Yeni bir cüzdan kurmak için aşağıdaki adımları izleyin.

Bu cüzdanlar daha sonra devlet kontrolündeki cüzdanlar için el koyma olarak kullanılabilir. Varsayılan olarak, bir eylemi onaylamak için, seçiminizi onaylamak amacıyla üstteki her iki düğmeye de basmanız gerekir.

Cihazı mikro USB kablosuyla bilgisayarınızın USB'sine takın. Cihaz hemen devreye girmeli ve başlamak için her iki düğmeye de basmanız



ister (iki düğme cihazın üst kısmında bulunur).

Sağdaki düğmeyi seçin ve yeni bir cihaz olarak yapılandırın.

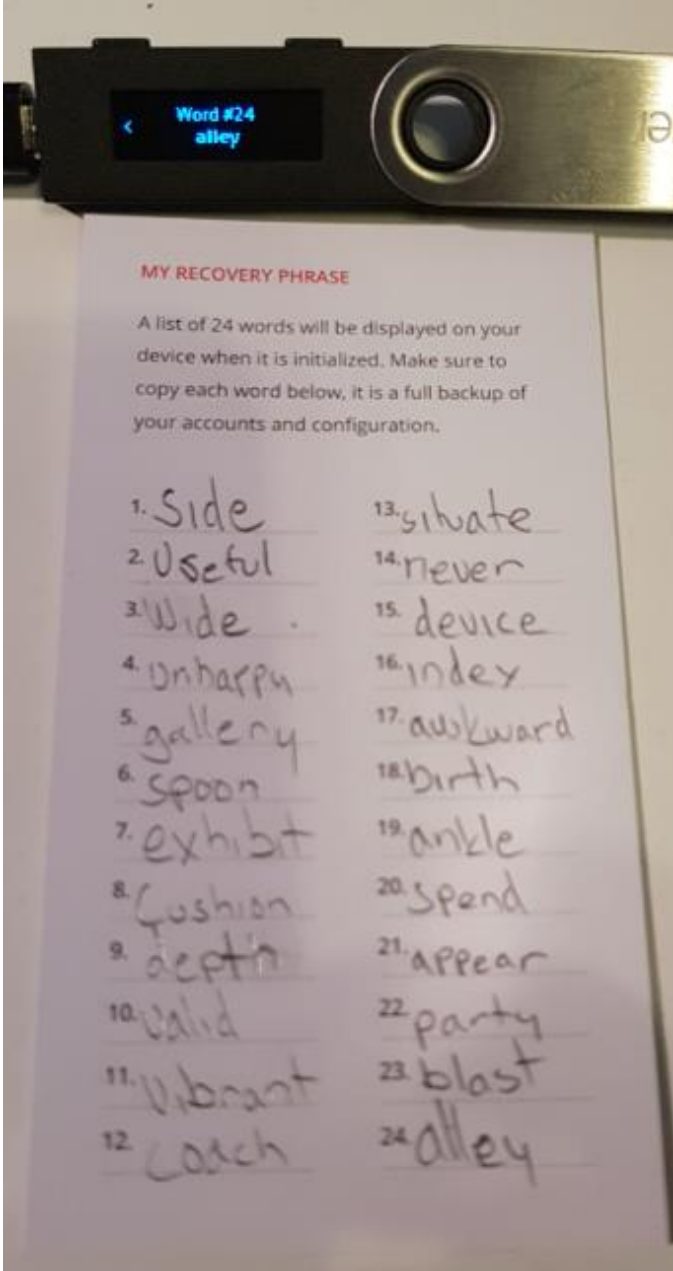
Yeni bir PIN kodu seçin.

Ledger cihazındaki iki düğmeye basarak PIN kodunu onaylayın.

Şimdi, verilen sayfaya yazdığımız 24 anahtar kelimeyi alacağız.

1. Kelime

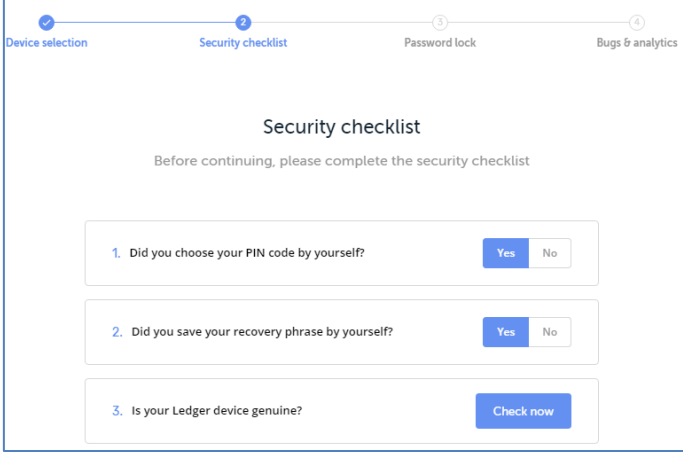
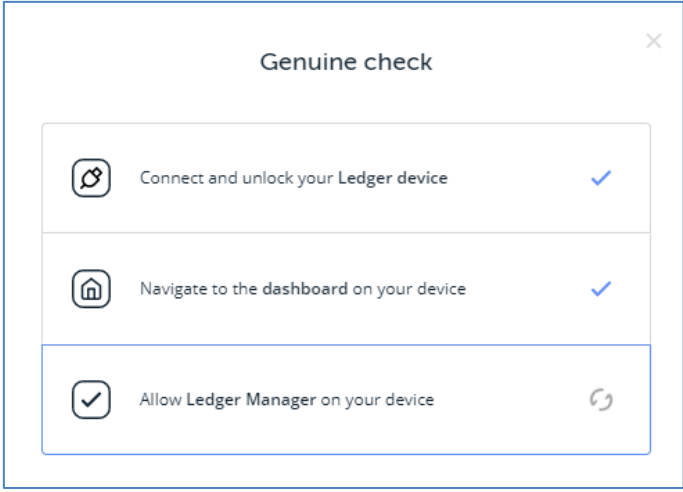
2. Kelime



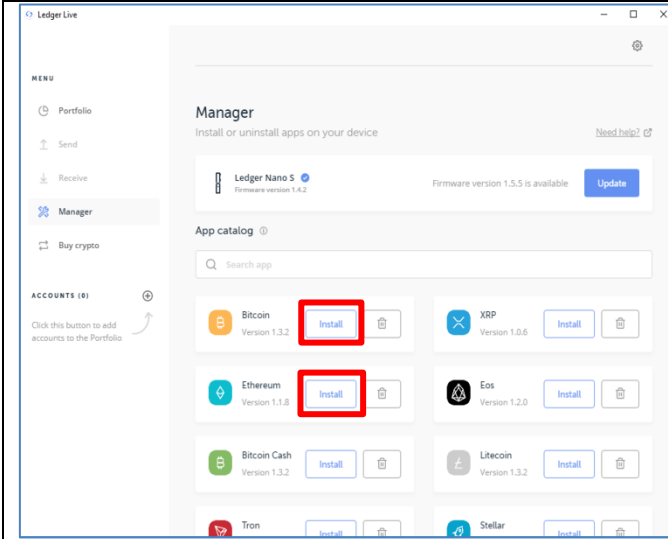
24 Kelime ve tüm anahtar kelime listesi solda gösterilmiştir.

Şimdi, yazdığımız 24 kelimenin hepsini onaylayacağız ve esasen, aynı cüzdanı, uyumlu herhangi bir BIP39/BIP44 cihazına geri yükleyebiliriz.

	Tüm anahtar kelimeleri alıp onayladıktan sonra, cihaz kullanmaya hazırdır.
NOW ON MOBILE Ledger Live Your accounts. All in one place. Everywhere. The perfect companion to your Ledger devices. Download Now Or choose to download for your platform: Mac OS, Windows, Linux, iOS, Android Get started with your Ledger device - Initialize as new device - Restore device from recovery phrase - Use an initialized device - Don't have a Ledger device?	Sonraki adım, kullanmak istediğimiz cihaza sanal para uygulamalarını kurmaktır. Bitcoin uygulamasını Ledger Nano S'ye yüklemek için https://www.ledger.com/pages/ledger-live adresine gidin ve platformunuz için Ledger Live uygulamasını indirip kurun. Önceki örnekte olduğu gibi, başlatma işlemini zaten yaptık, başlatılmış bir cihaz kullanmayı seçebiliriz. Cihazda elle yaptığımız işlemin Live uygulaması aracılığıyla da yapılabileceğini unutmayın.
1 Device selection 2 Security checklist 3 Password lock 4 Bugs & analytics Select your device  Ledger Nano S  Ledger Blue	İnternette satılan bazı kullanılmış ve sahte cihazlar olduğu için birkaç soru çıkacaktır ve cihazı kendileri başlatıp kurmayan kişilerin sanal paraları çalındı. "Gerçekten kendiniz mi kurdunuz?"u seçin.

	"Kurtarma ifadenizi kendiniz mi kaydettiniz?"i seçin.
 	Cihazın "Orijinal Kontrolü" ne gitmek için "Şimdi Kontrol Et" i tıklayın. "Cihazınızda Ledger Manager'a İzin Ver"mek için cihazdaki sağ düğmeyi tıklayın. Ledger şirketine veri ve analiz gönderme izinleri (devre dışı bırak).

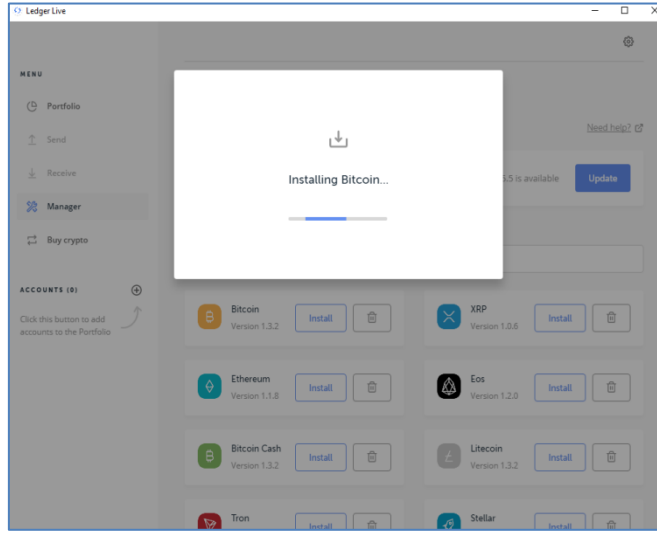
Bugs and analytics Share anonymized data to help improve Ledger security products and services Technical data* Learn more Ledge will automatically collect fully anonymized technical data to help improve user experience. * mandatory Analytics Learn more Enable analytics to help Ledger understand how to improve user experience. Bug reports Automatically send reports to help Ledger fix bugs. Terms * By continuing, you acknowledge that you have read and agree to the Terms of Use and Privacy Policy.	Ve son olarak, Ledger Live uygulamanız için güvenli bir şifre oluşturun. Ledger Live'in temiz bir kurulumu ve farklı bir şifre olsa da, PIN kodu ile cihaza başka bir bilgisayardan erişebileceğinizi unutmayın. Bu, Ledger Live şifresinin yerel olarak kaydedildiği anlamına gelir.
Password lock (optional) Set a password to prevent unauthorized access to Ledger Live data on your computer, including account names, transactions and public addresses New password Confirm password > Make sure to remember your password. Do not share it. > Losing your password requires resetting Ledger Live and re-adding accounts. > Resetting Ledger Live does not affect your crypto assets.	Ayrıca, anahtar kelimeleriniz varsa, cüzdanı herhangi bir bilgisayara geri yükleyebilirsiniz.
Install apps or add accounts Open the Manager to install apps or add accounts if your Ledger device already has apps installed Open Manager Add accounts	Cüzdanı kurduktan sonra, artık (örneğin) Ledger için devlet kontrolünde bir el koyma cüzdanı oluşturabiliriz. Ana pencerede, "Yöneticiyi Aç" ı seçin. Bitcoin uygulamasını yüklemek için "yönetici" yi açın ve Bitcoin kutusunda "yükle" yi seçin.



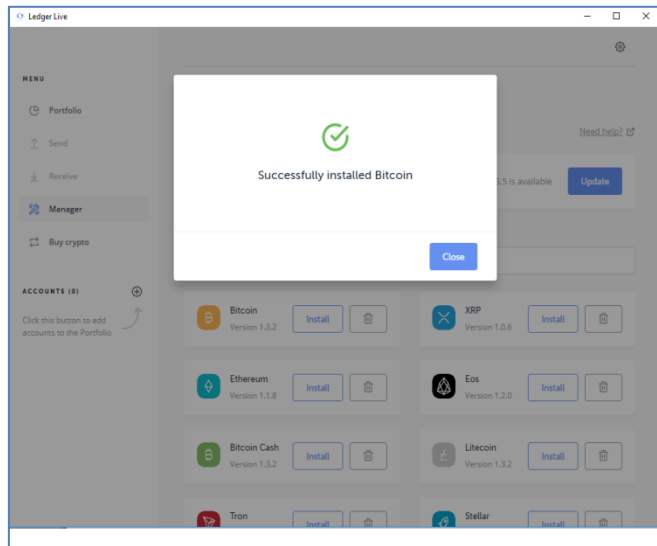
Ethereum için, Ethereum uygulamasının yanındaki "kur"u seçin. Her ikisi de resimde (kırmızı kutu şeklinde) belirtilmiştir.

Bitcoin cüzdanını Ledger Live uygulamasına ve Ledger cihazına yüklemek birkaç dakika sürecektir.

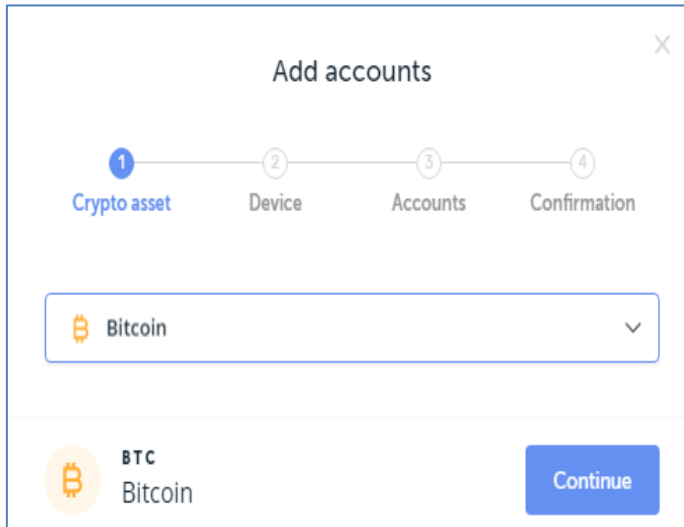
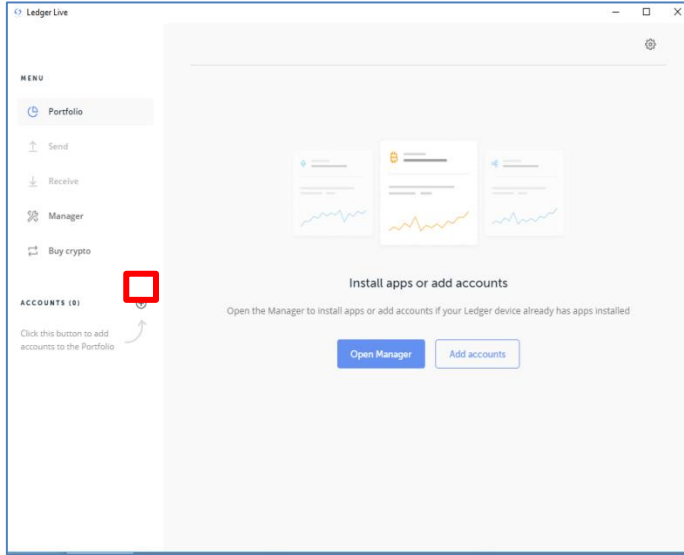
Ayrıca, cihazın üzerindeki her iki düğmeye de basarak (yukarıda belirtildiği gibi) Ledger Yöneticisinin cihaza erişimini onaylamanız gerekir.



Ledger Live, kurulumun başarılı olduğunu gösterdikten sonra, Ledger cihazında da Bitcoin logosuna sahip olmalısınız.



Bitcoin uygulaması, başarılı bir kurulumun ardından Ledger cihazında görüntülenmelidir.



Devlet kontrolünde bir hesap eklemek çok basit bir süreçtir. Ledger cihazında birçok farklı kripto para birimi ve token (jeton) depolanabilir, çünkü daha küçük birimler çoğu durumda kullanışlı ve kolay bir çözüm olabilir.

Resimde "Accounts" (+) (Hesaplar) gösterildikten sonra artı işaretini seçin.

"Hesap ekle"yi ve sanal para birimi türünü seçin.

< Back

Add accounts

1 ☒ Crypto asset 2 ☒ Device 3 ☐ Accounts 4 ☐ Confirmation



Follow the steps below to add **Bitcoin (BTC)** accounts

 Connect and unlock your Ledger device ☒

 Navigate to the Bitcoin app on your device ☒

Continue

< Back

Add accounts

1 ☒ Crypto asset 2 ☒ Device 3 ☒ Accounts 4 ☐ Confirmation

ADD NEW ACCOUNT

 EXAMPLE_TEST_ACCOUNT ☒

 **BTC**
Bitcoin

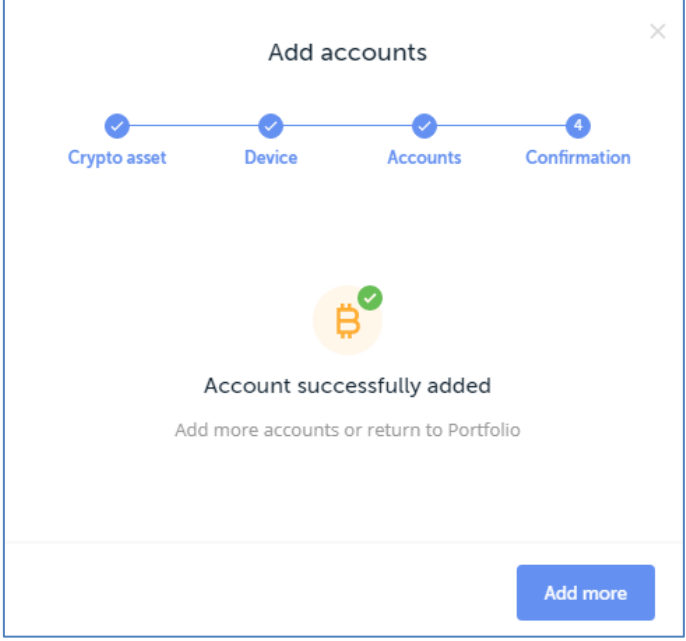
Add account

Ledger cihazını bağlayın ve kilidini açın.

Bitcoin uygulamasını buradan seçin (resimde değil).

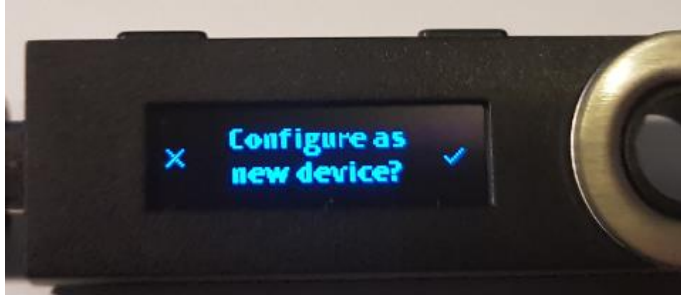
Hesaba istediğiniz ismi verin.

Örn, bir durum adı (örnekte "Example_test_account").

	Bir isim verdikten sonra, bitcoinleri kullanmaya ve göndermeye hazırdır. Litecoin, Ethereum vb.gibi farklı para birimleri için de aynı işlemi takip edebilirsiniz. Bir Ethereum ERC-20 tokenının geri yüklenmesi ve el konulması bu kılavuzda daha sonra ele alınacaktır.
---	--

Ledger cihazını bir anahtar ifadeyle yeniden yükleme

	Bir Ledger cihazını anahtar kelimelerden geri yüklemek doğrudan cihazdan yapılabilir. Bu, kurulum sürecine çok benzer ve cihaz tüm süreç boyunca size rehberlik edecektir. Bu, öğrenilmesi ve uygulanması çok önemli bir süreçtir. Ayrıca, müsadere sahnesinde özgüveninizi artıracaktır. Bu, başkası cüzdanınıza erişmeden önce el koyma işlemi hızlı bir şekilde yapabilmenize neden olur. Genelde, cüzdanlar, anahtar ifade kullanılarak aynı anda başka bir yerde kullanılabilir.
---	--



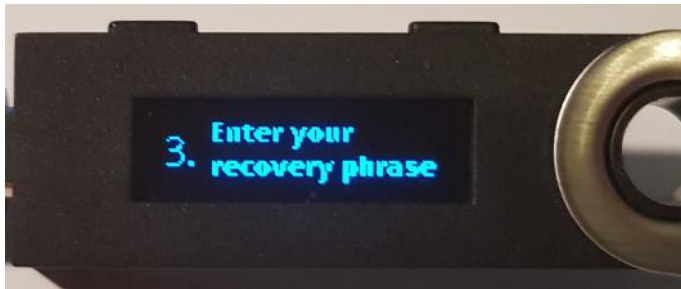
Cihazın üstündeki sol düğmeye basarak "X"i seçin (yeni bir cihaz olarak yapılandırmayın!).



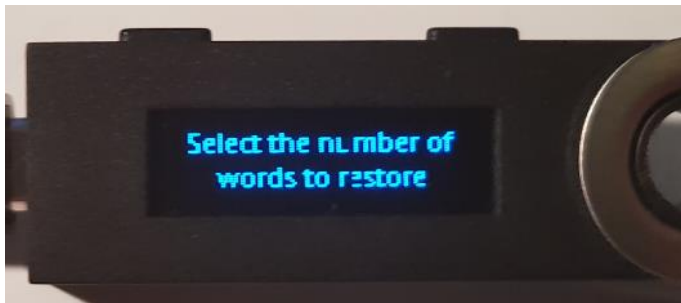
"Yapılandırmayı geri yükle?"yi seçin.



Yeni bir PIN kodu seçin. Bu kodun eski PIN koduyla veya şüphelinin olası PIN koduyla hiçbir ilgisi yoktur.



Anahtar kelimelerden kurtarma ifadesini (anahtarı) girin.





Bu cüzdan aynı zamanda diğer kelime listelerini (uzunlukları) desteklediğinden, herhangi bir 12 - 18 - 24 kaynak kelime listesini geri yükleyebilirsiniz.

MY RECOVERY PHRASE

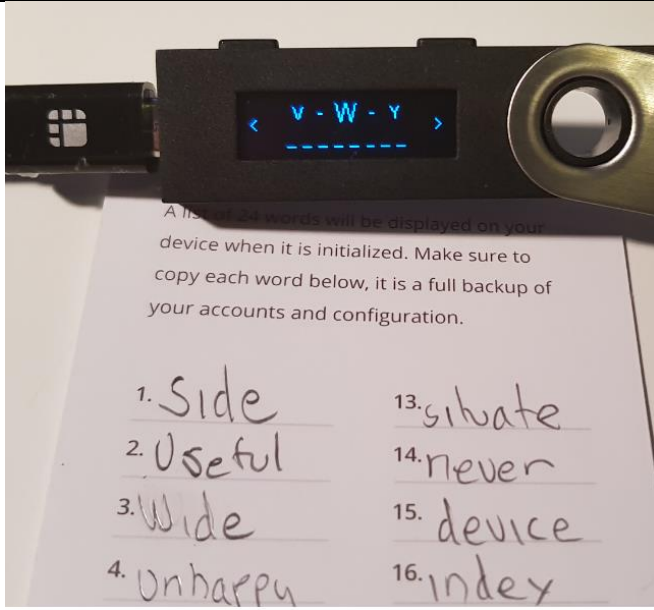
A list of 24 words will be displayed on your device when it is initialized. Make sure to copy each word below, it is a full backup of your accounts and configuration.

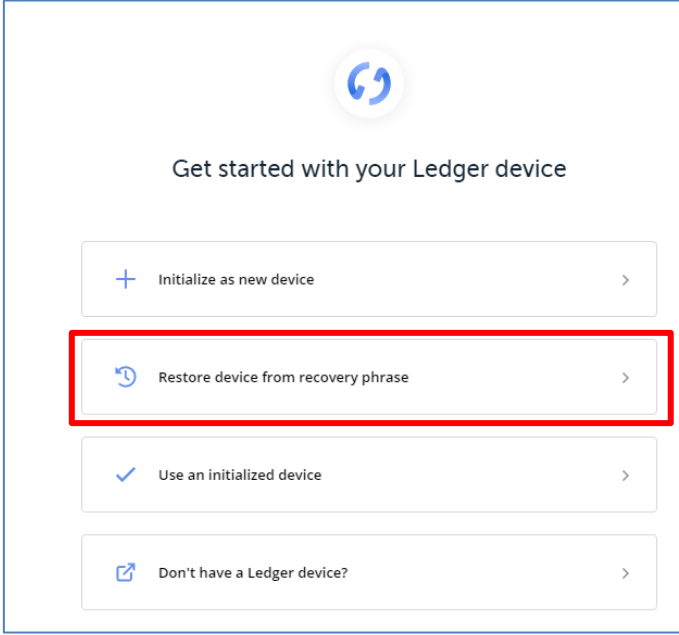
- | | |
|-------------|-------------|
| 1. Side | 13. sivate |
| 2. Useful | 14. never |
| 3. Wide | 15. device |
| 4. unhappy | 16. index |
| 5. gallery | 17. awkward |
| 6. spoon | 18. birth |
| 7. exhibit | 19. ankle |
| 8. Cushion | 20. spend |
| 9. depth | 21. appear |
| 10. valid | 22. party |
| 11. Vibrant | 23. blast |
| 12. Coach | 24. alley |

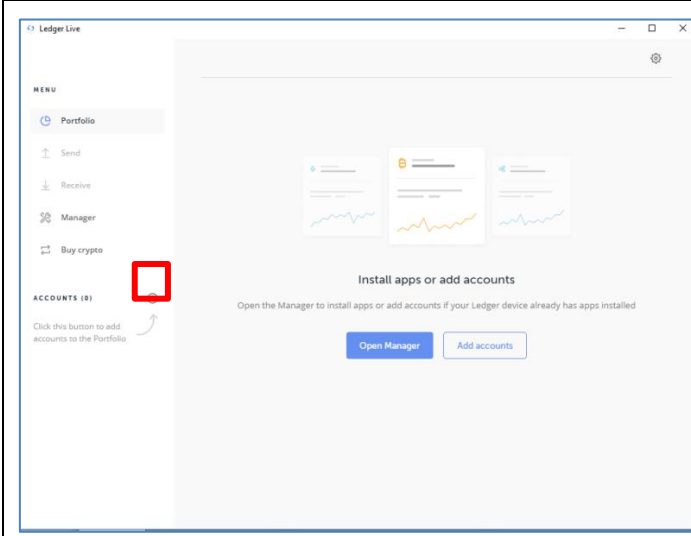
Yeniden yükleme, şüphelimizin evinde bulduğumuz kelime listesindeki ilk kelimeyle başlar.

Yeniden yükleme cümlemizi kullanıyoruz.

İlk kelimenin ilk harfini girin.

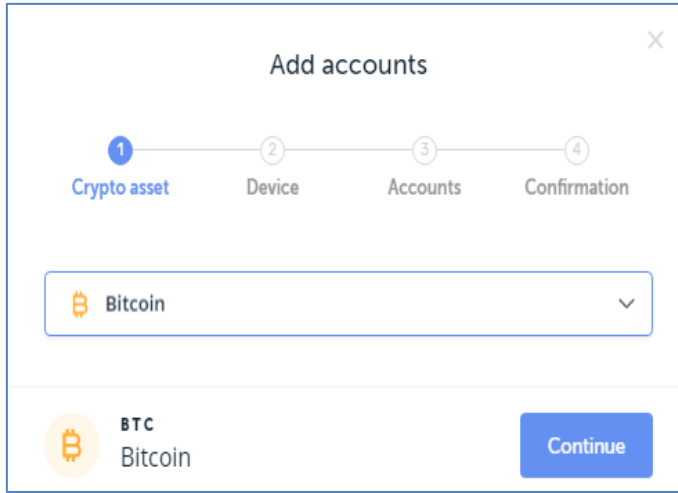


	24. kelimeden sonra, cihaz verilen anahtar kelimeleri işleyecek ve cüzdanın tam bir kopyasını size iade edecektir. Şimdi Ledger Live uygulamasını yüklemeli ve Bitcoin uygulamasını yükleme işlemini tekrarlamalıyız. Diğer sanal para birimlerini bulmanız gerekiyorsa, tüm uygulamaları tek tek yüklemeniz gerektiğini unutmayın. Ayrıca, bu cihazlardaki bellek öbeği çok küçük olduğundan, tüm kripto para uygulamalarını tek seferde yükleyemeyeceğinizi unutmayın. Ledger Live'ı yükledikten sonra, cihazı anahtar ifadeden geri yüklemeyi seçeceğiz (daha önce anlatıldığı gibi, aynı adımlar için kısa bir talimat verecektir.)
---	--



Bitcoin uygulamasını yükledikten sonra, daha önce bir uygulamayı yüklemek için açıklanan adımlarda olduğu gibi, yöneticiyi açıp Bitcoin uygulamasını ledger cihazına yüklememiz gerekir.

(+) tuşuna basarak yeni hesabı kurun.



Ekleme istediğiniz varlığı seçin ve ledger'inizi bağlayıp kilidini açın.

< Back×

Add accounts

✓

Crypto asset

2

Device

3

Accounts

4

Confirmation



Follow the steps below to add **Bitcoin (BTC)** accounts



Connect and unlock your Ledger device

✓



Navigate to the Bitcoin app on your device

✓

Continue

< Back×

Add accounts

✓

Crypto asset

✓

Device

3

Accounts

4

Confirmation

ADD EXISTING ACCOUNT



BTC 0.0029388

✓

ADD NEW ACCOUNT



Bitcoin 2

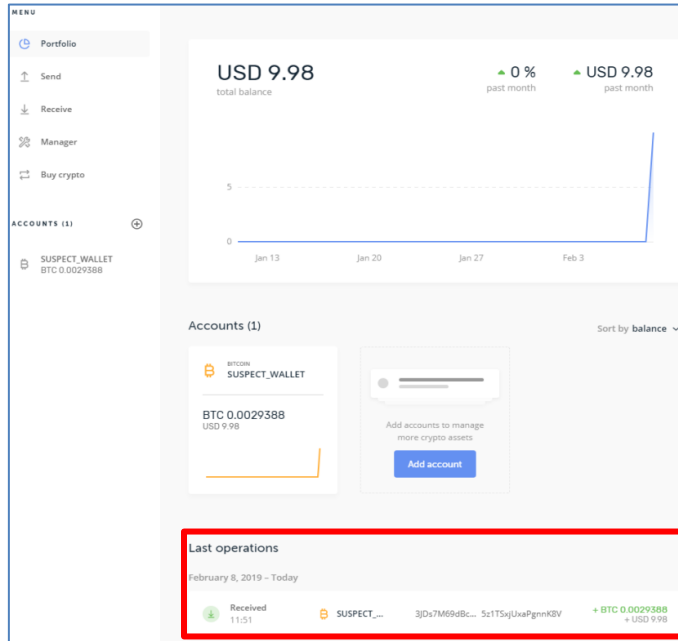
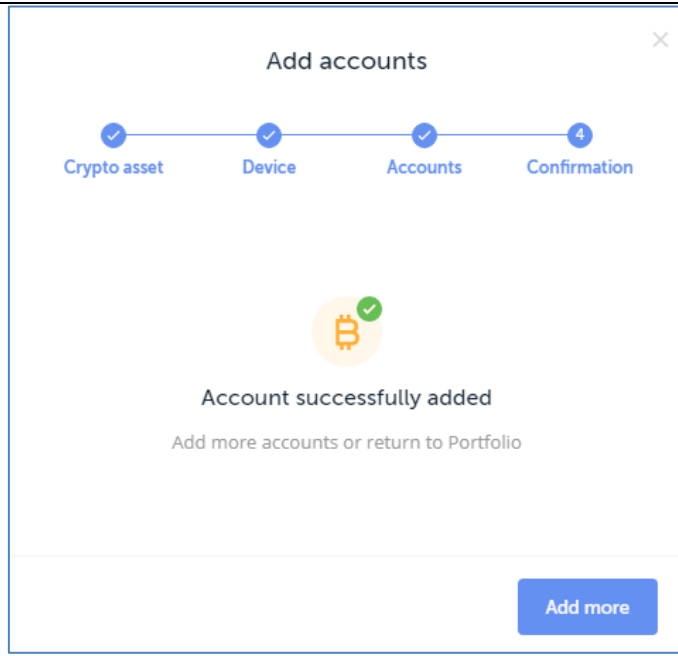
☐



BTC
Bitcoin

Add account

Senkronizasyondan sonra, her şey doğru yapılmışsa ve verilen anahtar kelime kullanılan gerçek anahtar ise şüphelinin Bitcoin hesabı görünmelidir. Hesabı istediğiniz şekilde adlandırabilirsiniz, burada "SUSPECT_WALLET" olarak adlandırılmıştır.

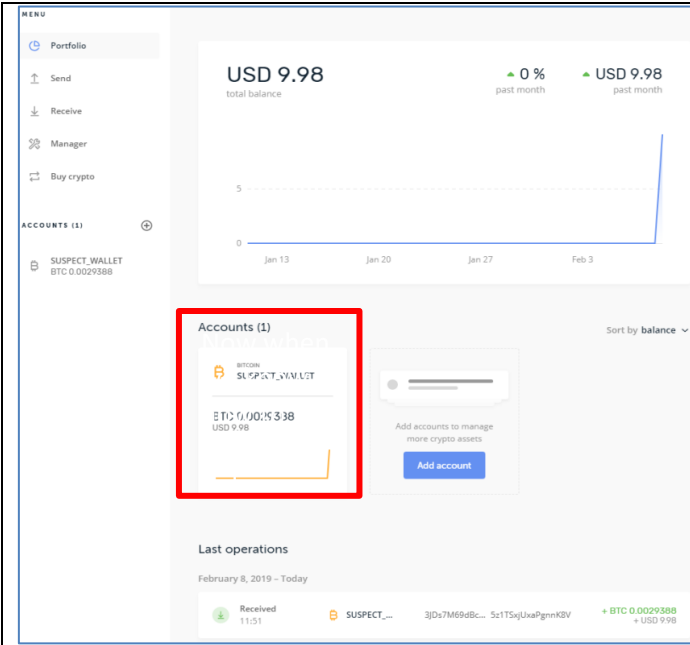


Bitcoin'in kurulumu ve senkronizasyonundan sonra, Bitcoin 1 hesabının paralarına, t retme yolu '0'a eriřimimiz olduėunu fark ettik.

T m t retme yolları i in hesapları tek tek elle eklemeniz gerektiėini belirtmek gerek. T retme yolları bu belgenin ilerleyen kısımlarında ele alınacaktır.

T m paraların g nderilmesi durumunda bile, kanıta dayalı kullanım i in Bitcoin (ve diėerlerinin) adreslerini ve verilerini  ıkarabileceėimiz bir ge miře sahip olunuz.

řimdi, ledger c zdanlarına nasıl eriřeceėimizi bildiėimizde, ondan nasıl el koyma iřlemi yapacaėımızı incelememiz gerekir.



İlk adım, devlet kontrolünde bir cüzdan oluşturmak ve daha önce ele aldığımız Bitcoinlerimizi ona göndermektir.

Ledger yöneticisinden Bitcoin hesabımızı seçip "Gönder"i seçeceğiz.

Burada Bitcoinlerin hedefini isteyecektir, ancak bazı değişikliklerle bunu herhangi bir sanal para biriminde kullanabilirsiniz.

Daha önce bahsedildiği gibi, Bitcoinlere el koyarken yapılacak iyi bir uygulama, alıcı adresini 2 veya 3 ayrı kişi tarafından bir not defterine yazmak ve tüm yazılı adreslerin eşleşip eşleşmediğini kontrol etmek ve ardından adresi alıcı adres sütununa koymaktır. Örnekte Bitcoinleri alındıkları adrese göndereceğim.

El koyma/ müsadere işlemi yaparken çok yüksek bir işlem ücreti kullanmanız tavsiye edilir; özellikle büyük bir meblağ transfer ediyorsanız, onaylanması için bir gece veya birkaç saat beklemek istemezsiniz, bu oldukça sinir bozucu olabilir.

Bayt başına kaç satoshinin, örneğin <https://bitcoinfees.net/> ya da <https://bitcoinfees.earn.com/> 'den ne tür gecikmelerle ilişkili olduğunu kontrol etmek iyi bir uygulamadır.

Resimde bir SegWit işleminde bir girdi ve bir çıktı işlemi 20 dakika içinde 3 satoshis/bayt ücretiyle

Bitcoin Fee Calculator & Estimator

to confirm within: transaction type:

To confirm within 2 blocks (~20 min)	3 satoshis/vbyte
For a standard transaction with 1 inputs	~138 vbytes
and 1 outputs	~414 satoshis
	~0.01 USD

< Back Send X

1 Details 2 Device 3 Verification 4 Confirmation

 Connect and unlock your Ledger device ✓

 Navigate to the Bitcoin app on your device ↻

Continue



onaylanacaktır. Bundan şu anda ağda çok fazla trafik ve gecikme olmadığını tahmin edebilir ve bayt başına oldukça düşük bir 2 satoshi ile devam edebiliriz. Bu, işlemin bir saat içinde ağdan geçmesini sağlayacaktır. Bu bir egzersiz işlemi olduğu için ücret oldukça düşüktür ancak yüz binlerce euro veya dolara el konulduğunda 10 dolar veya euro ücret hiçbir şey değildir.

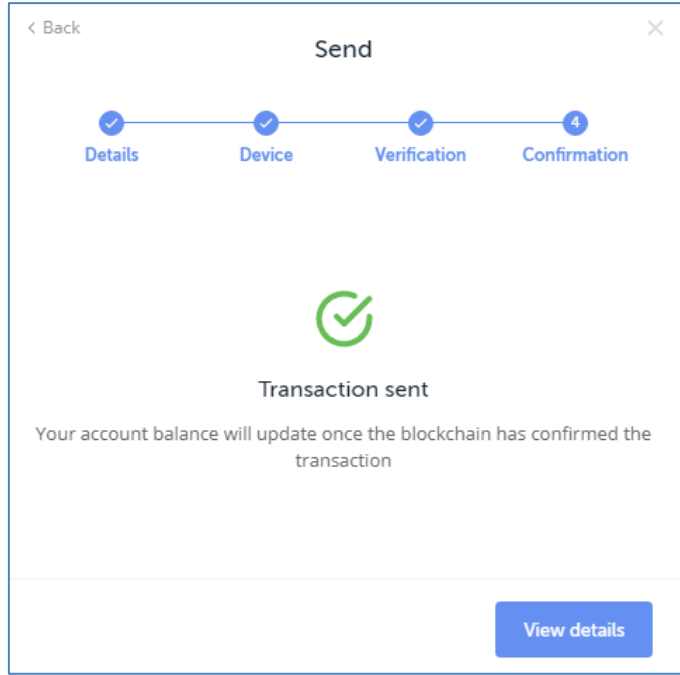
Ücretleri hesaplayıp tahmin ettikten ve işlemi onaylamak için el koyma adresini verdikten sonra, Ledger cihazını tekrar bağlayıp açmanız gerekir.

Her şeyi iki ve üç kez kontrol etmeden önce sağ düğmeye **BASMAYIN**; varış adresini en az iki ayrı kişi tarafından teyit edin ve işleme eklenen tutar ve işlem ücretlerinden emin olun.

Sağ tuşa tıklayarak işlemi onayladıktan hemen sonra, işlem hedef adrese gönderilir.

Her şey tamam. Talimatları izlediyseniz, Bitcoin cüzdanının "şüpheli" donanım/yazılımından Bitcoinslere başarıyla el koydunuz veya müsadere ettiniz.

Hemen hemen her cüzdan yazılımına veya cihazına aynı teknikleri uygulayabilirsiniz. İşlem gönderme ve alma konusunda bilgi sahibi olmak



için Bitcoin Testnet'i denemeniz şiddetle tavsiye edilir.

Ethereum ERC-20 tokenlarına bir ledger cihazından el koyma

Aşağıdaki örnekte, Ethereum cüzdanının GSEnetwork'ün yerel tokenı olan GSE adlı bir ERC-20 tokenı tuttuğunu gördük.^{31,32}

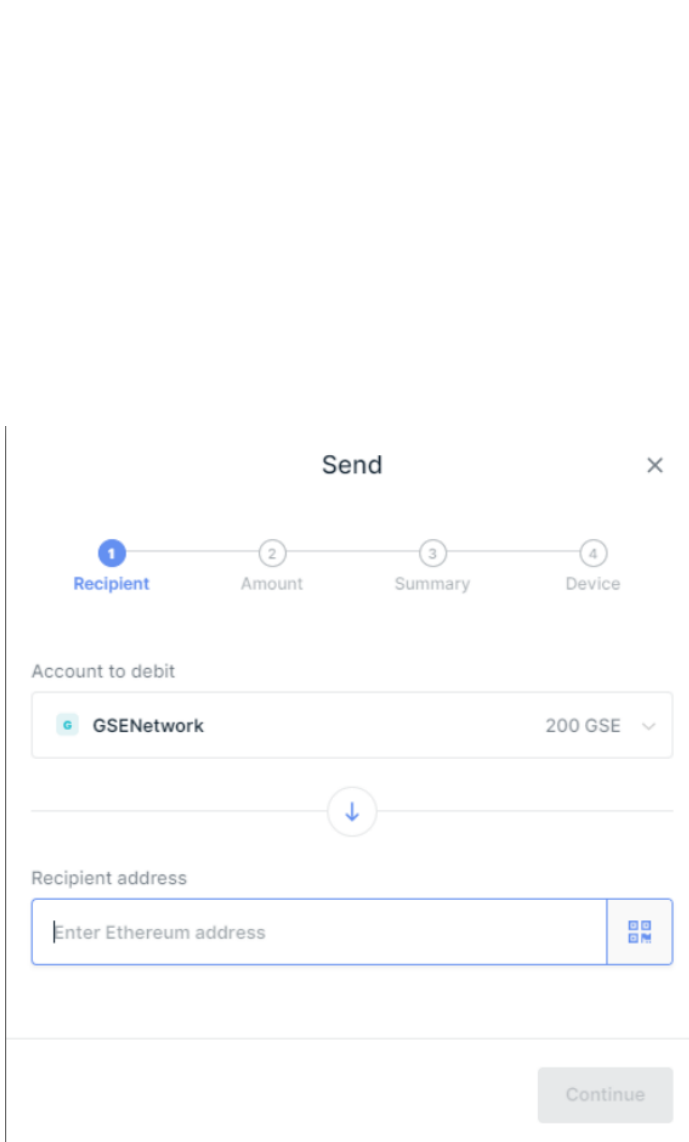
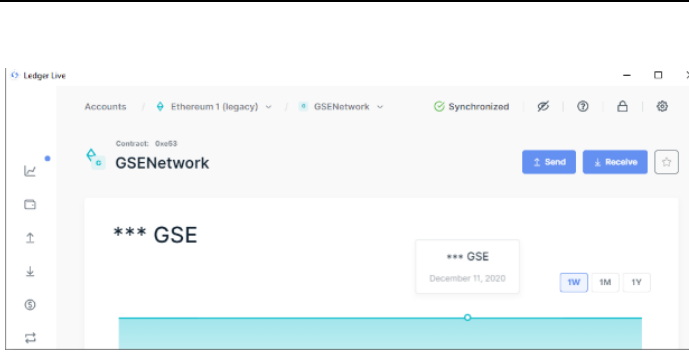
Account Name	Status	Symbol	Balance	Change
BITCOIN Bitcoin 1 (legacy)	✓	*** BTC	€***	+ 0 %
BITCOIN CASH Bitcoin Cash 1 (unsplit)	✓	*** BCH	€***	- 4 %
BITCOIN GOLD Bitcoin Gold 1 (unsplit)	✓	*** BTG	€***	- 2 %
ETHEREUM Ethereum 1 (legacy)	✓	*** ETH	€***	- 2 %

Ethereum uygulamasını kayıt defterine (ledger) yüklediğinizde, örnekte bazı detayların anonim hale getirildiği görülebilir.

ERC-20 tokenlarına el koyma süreci, bazı benzerlikleri olan bitcoinlere el koymaktan biraz farklıdır. Temel fark, ERC-20 tokenlarını bir Ethereum sözleşmesinden aktardığınızda, içeriği / tokenları bir Ethereum sözleşmesinden devlet kontrolünde bir (Ethereum) sözleşmeye

³¹ <https://cryptobriefing.com/what-is-gsenetwork-introduction-to-gse-token/>

³² <https://etherscan.io/token/0xe530441f4f73bdb6dc2fa5af7c3fc5fd551ec838>



göndererek Ethereum ağında aktarmanızdır.

Bir Ethereum adresi birkaç farklı tipte token tutabilir. GSE Token sözleşme adresi, aşağıdaki resimde vurgulanmış kırmızı kutuda görülmektedir.

GSE tokenlarından bir el koyma işlemi gerçekleştirirken, GSE tokenlarının gönderilmesini istediğimiz Ethereum adresini borçlandırmak ve eklemek için resimde belirtilen "Tokenları Göster" kısmından token hesabını seçmeniz gerekir.

Daha önce bahsedildiği gibi, bazı detaylar anonimleştirilmiştir ve bu nedenle Ethereum adresi bu örnekte tam uzunlukta değildir.

Ethereum adresini yapıştırdıktan sonra, transferle ilişkilendirmek istediğimiz Gaz miktarını seçmemiz gerekiyor (Gaz Gwei'dir ve madenciye giden bitcoin işlem ücretine eşdeğerdir; Gwei, Bitcoin'deki Satoshi'si gibi Ether'in bir kısmıdır.). Ayrıca, Ethereum ağı çok daha yavaş ve sıkışık hale geldiğinden işlemler için kullanılacak Gaz / Gwei miktarı arttı.^{33,34}

GSE miktarını belirledikten sonra veya gönderilecek Max Gönder'i seçerek ve hedef Ethereum adresini yeterli miktarda Gaz ile belirleyerek işleme devam edebiliriz. Ledger yazılımı çok faydalıdır ve süreç boyunca size birçok yönden rehberlik eder. Yine de farklı kripto paralar, tokenlar ve diğer işlevlerle farklı işlemleri eğitmeniz önerilir.

³³ <https://ethgas.io/>

³⁴ https://ycharts.com/indicators/ethereum_average_gas_price

Send

×

1

Recipient

2

Amount

3

Summary

4

Device

Account to debit

GSENetwork

200 GSE

▼

↓

Recipient address

0x7E3

QR

QR

Continue

← Back

Send

×

✓

Recipient

2

Amount

3

Summary

4

Device

①

Maximum spendable amount is ~ 200 GSE

[Learn more](#)

Amount

Send Max

☒

200

GSE

↔

0.00

€

Gas price [↗](#)

36 Gwei

Slow

Fast

Gas limit

65138

Network fees

G

0.002345 ETH

Continue

< Back Send X

✓ Recipient ✓ Amount **3 Summary** 4 Device

From
GSENetwork

To
0x7E39

Amount 200 GSE

Network fees 0.002344968 ETH

Continue

< Back Send X

✓ Recipient ✓ Amount ✓ Summary **4 Device**

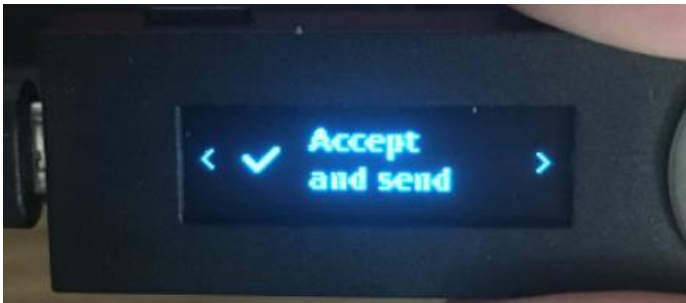
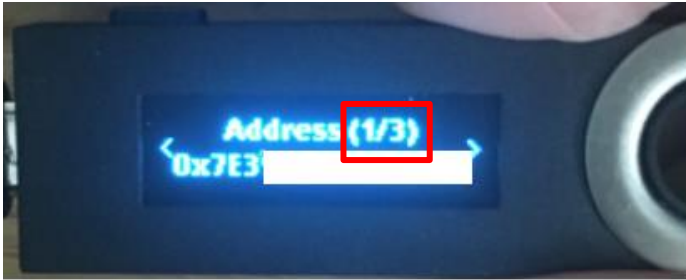
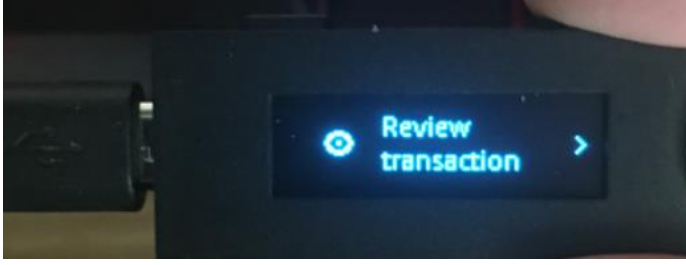


Connect and unlock your device



Ledger, cihazı anahtar kelimelerden geri yüklerken veya kayıt defterine (ledger) doğrudan şüpheli bilgisayardan canlı olarak erişerek veya hatta şüpheliden alınan PIN kodunu ve Ledger'in temiz bir kurulumuyla daha önce girdiğiniz PIN kodunu isteyecektir. Ardından, cihaza yüklediğiniz Ethereum uygulamasına gitmeniz gerekiyor.

Ledger cihazında ve uygulamasında, işlemi manüel olarak doğrulamanız ve gözden geçirmeniz ve her şeyin doğru olup olmadığını iki, hatta üç kez kontrol etmeniz gerekir. Ethereum adresi oldukça uzun olduğundan bunu yapmak biraz zor ve ekranı sola veya sağa kaydırmanız gerek. Bulunduğunuz sayfanın 1 / 3'ü gibi bir gösterge göreceksiniz.



Gözden geçirip her şeyin doğruluğundan emin olduktan ve bir meslektaşınızın da kontrol etmesini sağladıktan sonra, ledger ünitesindeki sol üst düğmeye tıklayarak ve GSE tokenlarına el koyarak işlemi göndermeye devam edebilirsiniz.

3.6 Kağıt Cüzdan

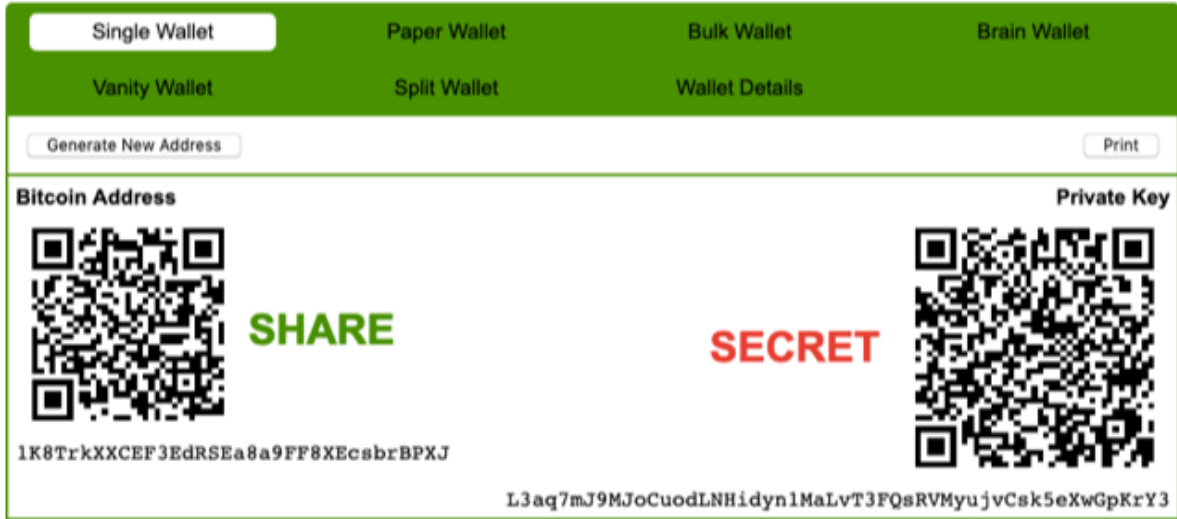
3.6.1 Giriş

Kağıt cüzdanlar Bitcoinin ilk günlerinde "bir şey"di. Çoğunlukla, Trezor ve Ledger gibi şirketlerin yeni kuruldukları veya yeni başladıkları için o zamanlar pek tanınmadığı 2011 ve 2016 yılları arasında kullanıldılar.

Bu, bitcoin kağıt cüzdanlarının bugün kullanımda olmadığı anlamına gelmez, bir çekmecede veya kitap arasında gizlenmiş ve bulunmayı bekliyor olabilirler.

Aşağıda bir bitcoin kağıt cüzdanının ekran görüntüsü bulunmakta. Bu kağıt cüzdanlar www.bitaddress.org adresinden online oluşturulabilirler. Bununla birlikte, web sitesi, oluşturma komut dizisini indirmenizi ve çevrimdışı (tercihen yeni yüklenmiş) bir bilgisayarda bir bitcoin cüzdanı oluşturmaınızı önerir.

Oluşturma komut dizisi GitHub'larından indirilebilir: <https://github.com/pointbiz/bitaddress.org/archive/v3.3.0.zip>.



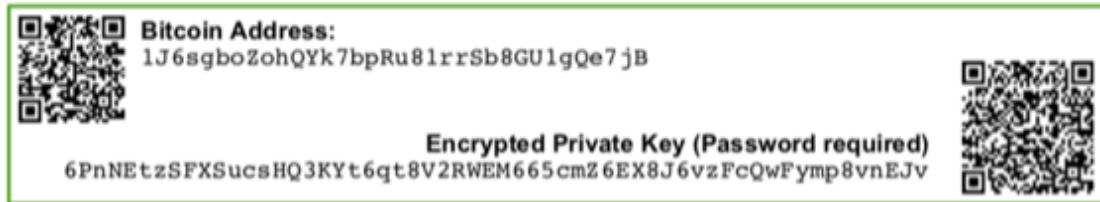
Klasik bir kağıt cüzdanın bir **özel anahtarı** ve bir **bitcoin adresi** vardır.

Kağıt cüzdanlar da şifrelenebilir. Şifrelenmiş özel (bitcoin) anahtar, 6P ile başlar.

Şifrelenmiş bir kağıt cüzdan örneği aşağıda gösterilmiştir.

bitaddress.org

<https://www.bitaddress.org/bitaddress.org-v3.3.0-SHA256-dec1...>



Bu durumda, araştırmacılar sadece şifreyi bildiklerinde paraya el koyabilirler.

Güvenli bir çevrimdışı cüzdan oluşturmanın birçok olası yolu vardır. Bazı ajanslar, sanal bir döviz borsası tarafından kontrol edilen bir hükümet cüzdanına sahip olma yoluna gitmişlerdir, bazılarının (daha önce gösterilen) donanım cüzdanları vardır, bazılarının da çoklu imza anahtarlarına sahip kendi kağıt cüzdanları vardır.

Son gösterge, çoklu imzalı bir çevrimdışı kağıt cüzdanın nasıl oluşturulacağıyla ilgilidir. Bu şekilde, soruşturmanızı dışarıdan bir değişime afişe etmek ya da hackleme olasılığınız minimumdur.

Öncelikle, çalıştırılabilir bir Ubuntu DVD'si oluşturmanız gerek. Ubuntu resmini Ubuntu web sitesinden indirebilirsiniz. İndirdikten sonra, Ubuntu'yu ve indirilen bittaddress.org kopyasının bir suretini DVD'ye yükleyeceksiniz. Çalıştırılabilir DVD değiştirilemediğinden ve içerik bir SHA hesaplamasıyla doğrulanabildiğinden, kurcalamaya karşı oldukça dayanıklı olarak kabul edilebilir. Çevrimdışı bir cüzdan oluştururken en önemli şey gerçekten çevrimdışı olmaktır. Güvenli bir şekilde silinebilen cihazları veya tamamen ayrı bir özel bilgisayar kullanın. Cüzdanın bir gözetim zincirine sahip olması gerekir, çoklu imzalı cüzdanları kullanırken genel anahtarı bir kanıt çantasının üstüne yazdırmak ve özel anahtarı kurcalamaya dayanıklı bir çanta içine yazdırmak bile olası bir çözümdür. Gitmenin birkaç farklı yolu var ve kuruluşun ihtiyaçları da ele alınmalıdır. **El koyma cüzdanları oluştururken, özel anahtarları veya anahtar sözcükleri yazdırmak için asla bir ağ kopyalayıcı veya yazıcı kullanmayın.** Ağ yazıcılarının veya fotokopi makinelerinin çoğunun, yazdırma arabelleğini depolayan bir hard disk vardır ve bu nedenle, normal bakım sırasında bir fotokopi makinesi servisi gelip hard disk değiştirdiğinde kolayca tehlikeye girebilirler.

bitaddress.org çevrimdışı kodda, bir "ana anahtar" ile çoklu imzalı bir cüzdan oluşturma ve bir koruma noktası daha ekleme imkanı da vardır. Tipik bir cüzdanın oluşturulması 1 dakikadan az sürer ve imha edilebilen veya güvenli bir şekilde silinebilen bir yazıcıyla basıldığında, kullanımı biraz güvenlidir. Uzun vadeli depolama için, bir genel- bir özel anahtar kombinasyonuna güvenilmesi önerilmez.

Çoğu zaman, aceleniz varsa ve bitcoinleri yalnızca geçici süreliğine tutmaya ihtiyacınız varsa, bir mobil uygulama süpürme cüzdanı kullanabilir veya birkaç genel - özel anahtar seti oluşturabilirsiniz. Tek bir adres oluşturmak için, DVD'nizdeki Bitaddress html dosyasını açmanız ve sayaç %100'e gelene kadar fareyi hareket ettirmeniz yeterlidir.



% 100'e ulaştığınızda, otomatik olarak size 1 rakamıyla başlayan bir P2KH adresi oluşturacaktır. Hatırlanması gereken çok önemli bir nokta da, çok gizli bir öge olarak kabul edilmesi gereken özel anahtarı da oluşturmaktır. Herhangi biri QR kodunu veya özel anahtarı görebiliyorsa, parayı adresten çekebilir. Ayrıca, genel - özel anahtar çiftini yazdırdıktan sonra, yazıcı belleğini silmeyi veya temizlemeyi unutmayın.



bitaddress.org komut dosyasını kullanarak bölünmüş cüzdan oluşturmak çok kolay bir işlemdir. Birleştirmek için gereken hisse sayısını ve oluşturulacak hisse sayısını seçmek hiç zamanınızı almaz ve artık çoklu imzalı bir cüzdanınız var. Aşağıda, herhangi ikisinin birlikte cüzdan için işlem imzalayabildiği üç hisseden oluşan çevrimdışı bir cüzdan örneği yer alıyor.

Single Wallet	Paper Wallet	Bulk Wallet	Brain Wallet
Vanity Wallet	Split Wallet	Wallet Details	
Minimum share threshold needed to combine 2 Number of shares 3 Generate			
Bitcoin Address 1AuP7uYMYs6P4mtVamsaJyD8mn71PGo7Mx 			
Share 1: 3XxT9p56GGwD3Qkhm3ojwvFNpD1g4LzgeP5KcvzzJGqS6EF 			
Share 2: 3Y2nt6kWiymM73GXmnNTxbMpPVbjnJ7XeZ4ES6EvBbrAJ9i 			
Share 3: 3Y8T5Ti8FVPaXvLNuHBJkxgdDh1aKNLEpmfJRqjjLp8vR8e 			
Enter Available Shares (whitespace separated) 3XxT9p56GGwD3Qkhm3ojwvFNpD1g4LzgeP5KcvzzJGqS6EF 3Y2nt6kWiymM73GXmnNTxbMpPVbjnJ7XeZ4ES6EvBbrAJ9i Combine Shares			
Combined Private Key 5JKRtqFqyzzdsPgsw3ghjABrGZ8a2mgDXzA8jiRPzLmUvJTCX			

3.6.2 Şifrelenmiş ve Şifrelenmemiş

Ek bir güvenlik katmanı oluşturmak için kağıt cüzdanlar da şifrelenebilir. Kuruluşunuza el koyma sürecini oluştururken, kuruluşunuzun kullandığı adrese başka bir güvenlik düzeyi veya katmanı yaratabileceğinden bunu akılda tutmak iyidir. Bununla birlikte, bu ana şifrenin kaybolması durumunda, şifreyi zorlamanın neredeyse imkansız olduğunu göz önünde bulundurmak önemlidir. Bu, şifreleme ana şifresini ve dolayısıyla parasını da kaybetmiş suçlularda bile görülmüştür.

Single Wallet Paper Wallet Bulk Wallet Brain Wallet

Vanity Wallet Split Wallet Wallet Details

Hide Art? ☒ Addresses to generate: 1 Generate Print

BIP38 Encrypt? ☒ Passphrase: ABCDEFGH1234567890 Addresses per page: 7

Bitcoin Address:
1K9xi3GN6A8vreyNd5SFveFycwCUBKfrPU

Encrypted Private Key (Password required)
6PnSrKAB4sz9ndnj98ZEGWTFMGSHuwpHMTTwVoHNniq63njxZqxKi9S

Bunun bir yolu, parolayı hatırlayarak bir Beyin cüzdanı oluşturmaktır, şifreleme size her zaman aynı genel ve özel anahtarı verecektir. Parola cüzdanı oluştururken, bazı yaygın kelimeler için Bitcoin ağını bu kelimeler, kriptografik özetler, genel ve özel anahtarlar için tarayan botların olduğunu bilmekte fayda vardır. Bot, içinde para olan bir cüzdan bulduğunda, cüzdanı hemen süpürüp boşaltır. Bitmex, yaptıkları bir testle ilgili bir rapor yayınlanmış ve yaygın olarak bilinen bir parola kullanılırken cüzdanın boşaltılmasının yaklaşık 0,67 ila 3 saniye sürdüğünü ortaya çıkarmıştır³⁵.

Single Wallet Paper Wallet Bulk Wallet Brain Wallet

Vanity Wallet Split Wallet Wallet Details

Enter Passphrase: 1234567890abcdefg Show? ☒ Print

Algorithm: SHA256(passphrase)

Compressed address? ☐ View

Warning: Choosing a strong passphrase is important to avoid brute force attempts to guess your passphrase and steal your bitcoins.

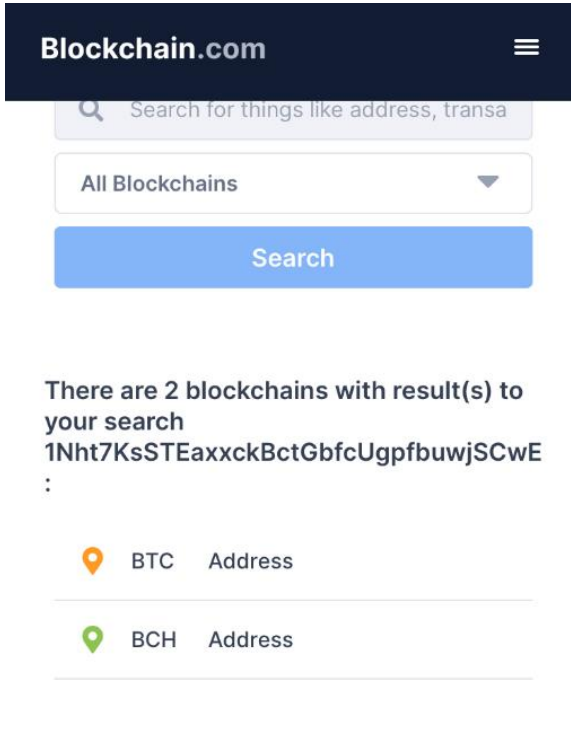
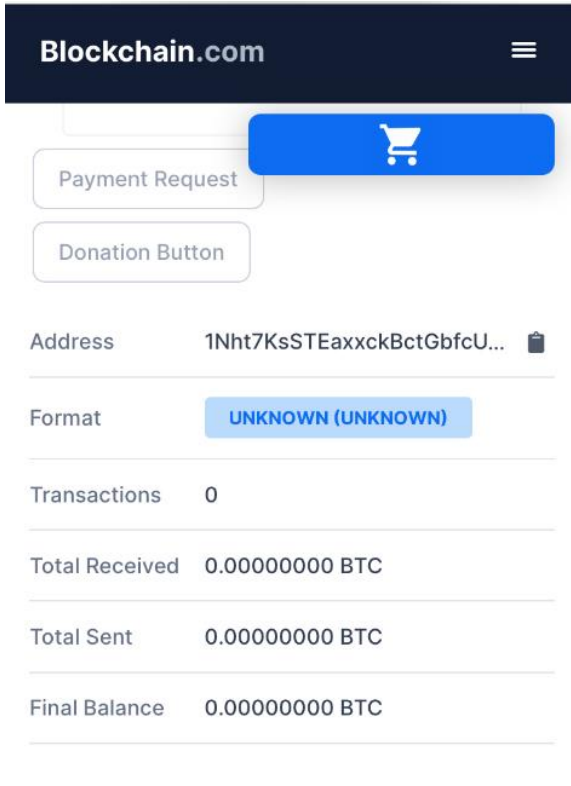
Bitcoin Address:
1Nht7KsTEaxxckBctGbfcUgpfbuwjSCwE

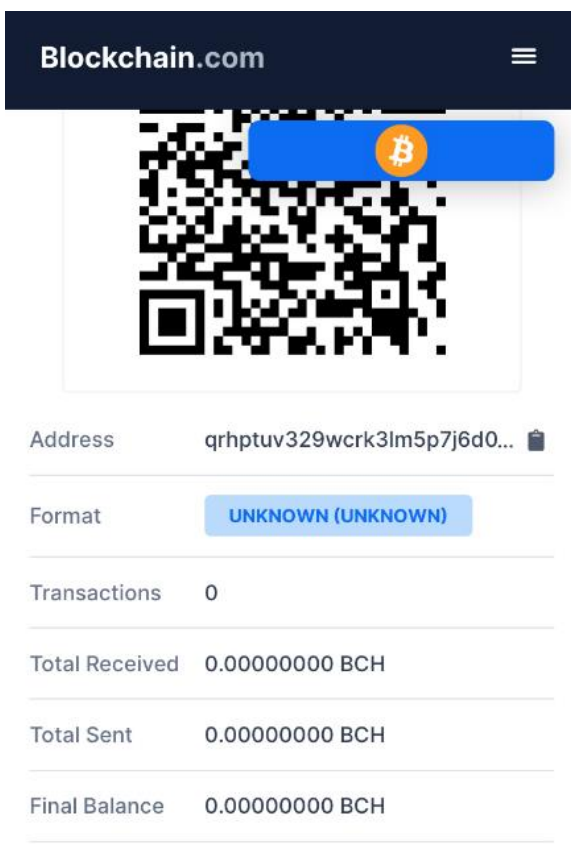
Private Key (Wallet Import Format):
5JrTVMfW87wUJgmA5DF9T3QLMK7koYBqa7ziQwU1N7T7uqAdkQF

Kağıt cüzdana el koyma

İlk adım, el konulacak para olup olmadığını kontrol etmektir. Cep telefonunuzdaki Bitcoin Adresinin yanındaki QR kodu tarayın, kopyalayın ve www.blockchain.com/explorer gibi bir bitcoin blok gezginine göz atın.

³⁵ <https://blog.bitmex.com/call-me-ishmael/> - faiz parçası, beyin cüzdanlarının süpürülmesi üzerine çalışma

	Arama alanına adresi kopyalayın. Olası sonuçları olan iki potansiyel blok zinciri göreceksiniz: Bitcoin (BTC) ve Bitcoin Cash (BCH). Önce tıklayın ve Bitcoin (BTC) blok zincirini kontrol edin. Bitcoin Cash çatallanmasıyla ilgili daha fazla bilgi için: https://en.wikipedia.org/wiki/Bitcoin_Cash Bitcoin çatallanmasıyla ilgili daha fazla bilgi için: https://en.wikipedia.org/wiki/List_of_bitcoin_forks
	Görünüşe göre, bu kağıt cüzdanda hiç bitcoin yok çünkü sıfır işlem ve aynı zamanda sıfır bakiye var. Gezginin önceki sayfasına dönün ve Bitcoin Cash'e (BCH) tıklayın.



The screenshot shows the Blockchain.com interface for a Bitcoin Cash (BCH) address. At the top, there's a dark blue header with 'Blockchain.com' and a menu icon. Below it, a large QR code is displayed. A blue banner with a Bitcoin logo is overlaid on the QR code. Under the QR code, the address 'qrhptuv329wcrk3lm5p7j6d0...' is shown. Below the address, there's a 'Format' dropdown menu set to 'UNKNOWN (UNKNOWN)'. Further down, a table shows transaction details: Transactions: 0, Total Received: 0.00000000 BCH, Total Sent: 0.00000000 BCH, and Final Balance: 0.00000000 BCH.

Bitcoin Cash blok zinciri de herhangi bir para göstermiyor.

Bu, kağıt cüzdanın boş olduğu ve hiç kullanılmadığı anlamına gelir.

Peki cüzdandaki paralar?

Bir kağıt cüzdana bağlı bitcoinleri çekmek veya bunlara el koymanın en iyi yolu (mobil veya masaüstü) bir yazılım cüzdanındaki "süpürme" özelliğini kullanmaktır.

Süpürme

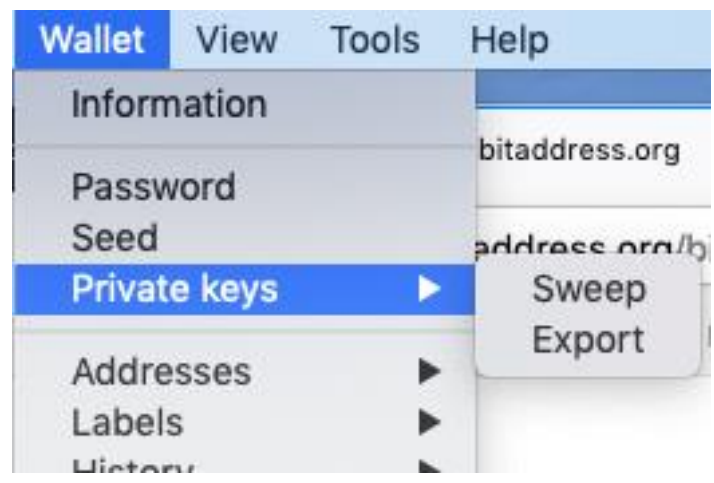
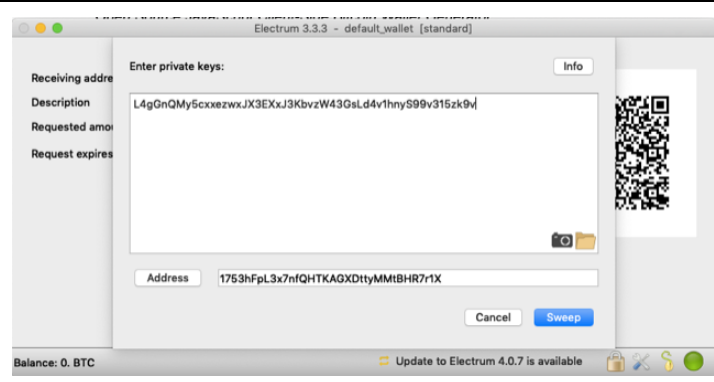
Kağıt cüzdanın özel anahtarını süpürmek, bu cüzdanın tüm bakiyesini devlet (veya araştırmacı) tarafından kullanılan ve kontrol edilen cüzdana gönderecektir.

Başka bir deyişle, kağıt cüzdan adresinin bakiyesi boşaltılacak ve devlet cüzdanına eklenecektir. Bu, standart bir işlem yoluyla gerçekleşir (bu da madenci ücretlerinin ödenmesini gerektirir), bu nedenle cüzdanın çevrimiçi olması gerekir (internet bağlantısı gereklidir).

Bir yazılım cüzdanında "içe aktarma" işlevi de kullanılabilir, fakat bu önerilen bir uygulama değildir çünkü araştırmacının ikinci bir manipülasyon, yani devlet kontrolündeki bir cüzdan adresine bir işlem gerçekleştirmesi gerekir. Ayrıca fazladan zaman alır ve şüphelinin suç ortağı cüzdanın bir kopyasına sahip olduğunda, fiili el koyma gerçekleşmeden önce parayı transfer edebilir.

Özel bir anahtarı süpürmek birkaç cüzdanda yapılabilir. Electrum, Mycelium ve Jaxx Liberty (mobil bir cüzdan) bunları desteklemekte. Jaxx Liberty "kağıt cüzdanın içe aktarılması"ndan bahseder ama emin olun ki cüzdan bir kaydırma yapar.

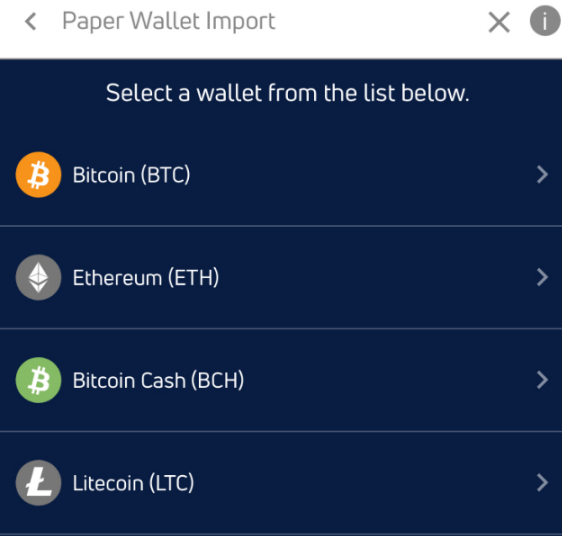
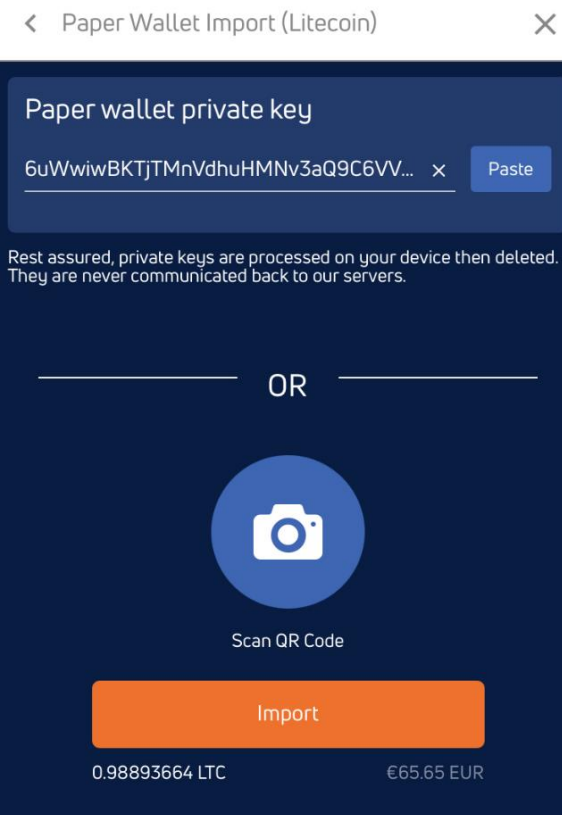
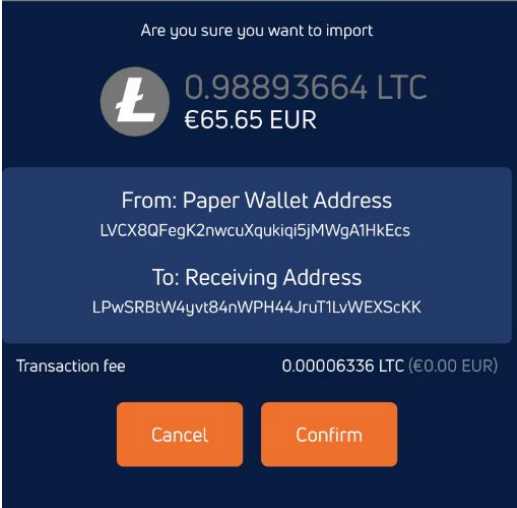
Electrum'da (masaüstü uygulaması) bir bitcoin (BTC) özel anahtarının süpürülmesi

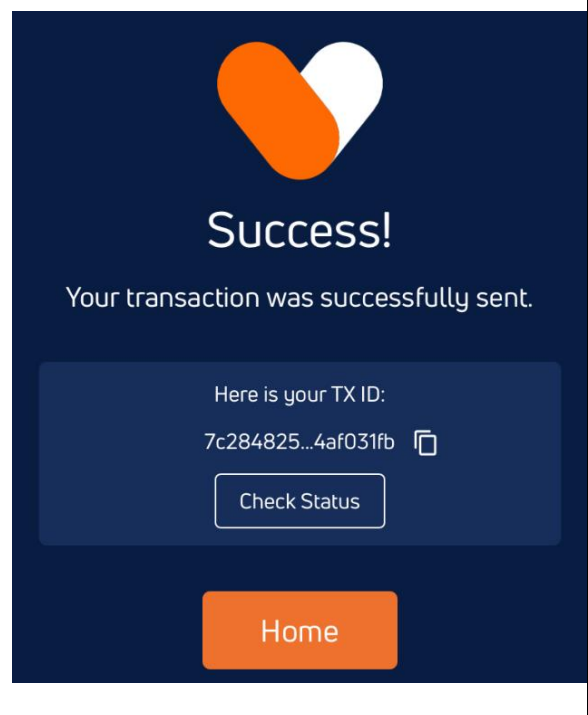
	Örneğin, şifrelenmemiş bir özel anahtarı süpürmek, Electrum gibi bir masaüstü cüzdanında kolayca yapılabilir. İlk önce, kağıt cüzdandaki özel anahtarın QR'ını tarayın. Menü'ye git ve Cüzdan'a tıkla. Sonra sırayla Özel anahtarlar'a ve Süpür'e tıkla.
	Electrum'da yeni bir pencere görünecek. Özel anahtarı bu pencereye kopyalayıp yapıştırın ve Süpür'ü tıklayın. Bir QR kod okuyucuyla kopyalayabilirsiniz. Electrum size paraların gönderileceği adresi gösterecek (Electrum cüzdanında).

Jaxx Liberty'de (mobil uygulama) bir Litecoin (LTC) özel anahtarını süpürme örneği

	Jaxx Liberty'de yuvarlak/tekerlek simgesini (sağ üst) tıklayın.
---	--

Menu ×  Bulletins >  Security >  Tools >  Customization >  About Version 2.4.6 #289 >  Support >	Sonra Araçlar'a tıklayın.
< Tools × Pair/Restore Existing Wallet > Display Private Keys > Third Party Authorization (0 of 1) > Paper Wallet Import > Deep Address Scanner >	Ardından, "Kağıt Cüzdanı İçe Aktar"ı tıklayın. Unutmayın: "İçe aktar" diyor, ancak Jaxx Liberty'nin asıl yaptığı şey özel anahtarın süpürülmesidir.

	Bir sonraki adım, ne tür bir kağıt cüzdanı içe aktarmak istediğinizi seçmektir (süpürme). Litecoin (LTC)'e tıklayın.
	(solda) Özel anahtarı yapıştırın veya özel anahtarın QR kodunu cüzdanda tarayın. (aşağıda) Onayla'yı tıklayın. 

	Başarılı olursa işlem kimliği (transaction ID) görünecektir. Daha sonra raporda kullanmak üzere bunu bir yere kopyalayabilirsiniz.
---	---

3.7 Emanetçi ve online web cüzdanları

3.7.1 Giriş

Emanetçi cüzdan, üçüncü bir tarafın anahtar yönetimini yürüttüğü bir cüzdandır; bu üçüncü taraf çoğu durumda bir SVSS olarak kabul edilecektir (örneğin, Coinbase, Xapo, BitGo).

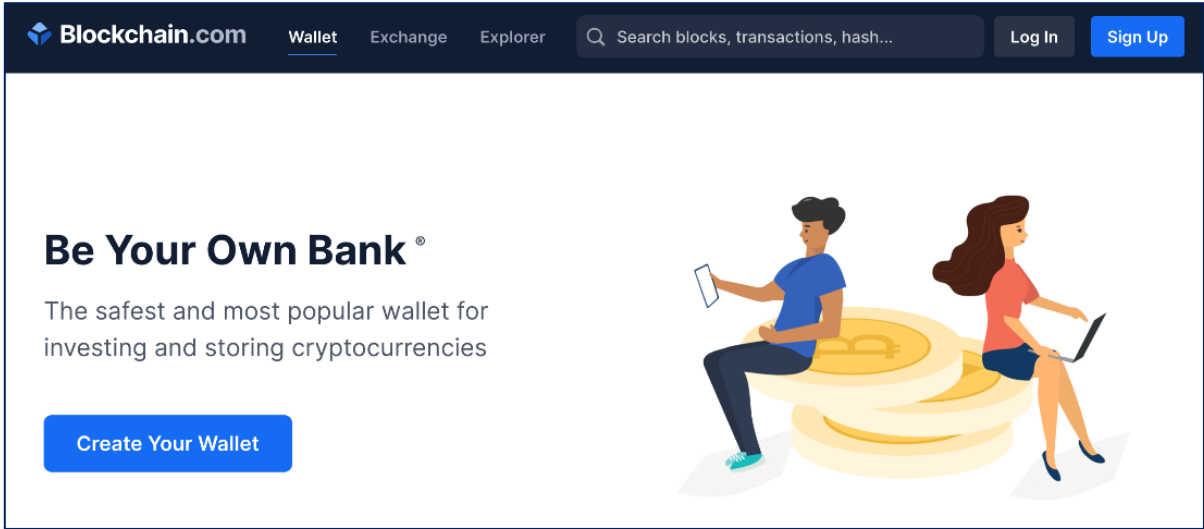
Bankalar, kredi birlikleri, sigorta şirketleri, emeklilik fonları ve koruma fonları gibi kurumsal yatırımcılar da emanetçi hizmetlerden yararlanır.

Bu bağlamda, böyle bir cüzdan online bir cüzdan olarak düşünülebilir, ancak tüm çevrimiçi cüzdanlar emanetçi cüzdanlar değildir. Emanetçi olmayan bu çevrimiçi cüzdanların özel anahtarları, kullanıcının kendisi veya kullanıcı ve cüzdan sağlayıcısı tarafından kontrol edilir. Bu durumda Block.io gibi bir cüzdan var.³⁶

Blockchain.com

Emanetçi olmayan online cüzdanın bir örneği Blockchain.com cüzdanıdır (aynı zamanda mobil uygulaması da vardır).

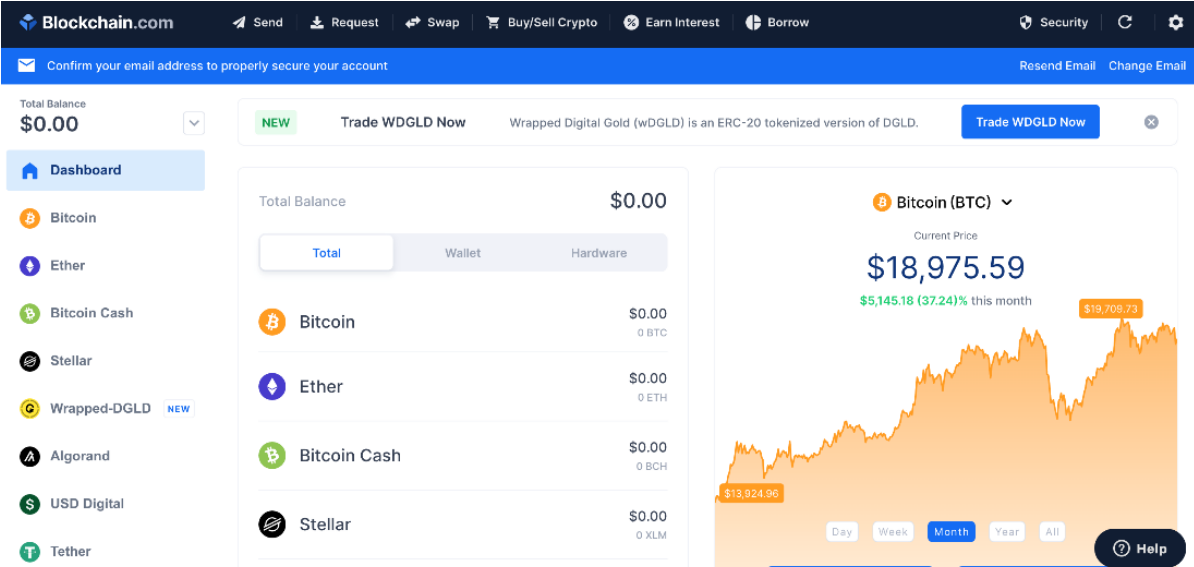
³⁶ Ek bilgi için: <https://block.io/security>



Blockchain.com cüzdanının oturum açmak için bir cüzdan tanımlayıcısı (Cüzdan Kimliği) ve giriş yapmak için şifresi bulunur. Bu cüzdan kimliği 32 alfanumerik karakter ve 4 kısa çizgiden oluşur ve aşağıdaki biçimi alır:

XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX

Kullanıcı bir Blockchain.com cüzdanına kaydolduğunda, cüzdan tanımlayıcısını içeren bir e-posta alır.



Çoğu cüzdan gibi, Blockchain.com cüzdanı da (12 kelimelik) bir anahtar cümleyle çalışır.

El koyma öncesi planlama

Emanetçi bir cüzdanla uğraştığınızı düşündüğünüzde, daha önce açıklandığı gibi el koyma öncesi planlamayı aklınızda bulundurun ve bu kullanıcının hesabını dondurmak için saklayıcıya (platform) başvurun.

Blockchain.com şirketinin, bir emanet hizmeti olmadığı için kullanıcı hesaplarını veya fonlarını dondurmadığını bilmek güzel. Bununla birlikte, diğer SVSS'ler, emniyet kuvvetleri kendilerine bir

mahkeme celbi, emir veya meydana gelen geçerli yasal prosedüre bağlı olarak MLAT gönderirse bunu yapabilir. Genellikle sorunsuz işbirliği için "kolluk kuvvetleri için" alt sayfası vardır.

El koyma

Cüzdanın kendisinden el koymak biraz zor olabilir. Araştırmacılar aşağıdaki noktaları akılda tutmalıdırlar (+ izin veriliyorsa her zaman geçerli yasal çerçevenizi kontrol edin).

- En kolay durum, şüphelinin cüzdanının açık olması veya anahtarın bulunmasıdır (örneğin, bir ev araması sırasında). Bu durumda, araştırmacı paraları devlet kontrolündeki bir cüzdana aktararak varlıkları güvence altına almalıdır.
- Şüphelinin cüzdanı kilitliyse, ancak e-posta hesabına erişilebiliyorsa, cüzdana erişim sağlamak için cüzdanın şifresi değiştirilebilir. Bu durumda, araştırmacının yasal yetkisinin olması şarttır. Çoğu durumda, çevrimiçi bir cüzdan oluştururken, kullanıcıyı doğrulamak ve oturum açma girişimlerine yetki vermek için bir e-posta hesabı gereklidir.
- Cüzdan kimliği, doğrulama e-postasının altında da belirtilecektir.
- Bağlı e-posta hesabına erişmek için (yasal çerçeveye bağlı olarak) sulh hakiminin / hakim / savcının onayı gereklidir.
- Tüm bu bilgilere sahip olan araştırmacı, cüzdanı devralabilir ve sanal paraları devlet kontrolündeki bir cüzdana aktarabilir.

Sonuç: ideal el koyma durumu, cüzdanın açık olduğu veya anahtarın bulunduğu zamandır. Çoğu durumda, anahtar Coinomi gibi diğer BIP44 / BIP39 tipi cüzdanlarla uyumlu olacaktır.

Müşteri bilgilerinizi bilin ve Blockchain.com (Lüksemburg) ile iletişime geçin

Blockchain.com (Blockchain Lüksemburg SA), cüzdanları aracılığıyla kripto paralar arası değişim yapmak veya bedelsiz dağıtımların bir parçası olmak isteyen kullanıcıların kimlik doğrulamasını gerektirir.

Bu, kolluk kuvvetleri bir adres (Bitcoin veya başka bir kripto para birimi) veya bir işlem kriptografik özet değeri bulursa, adres veya kriptografik özet bir swap veya değişim işleminde kullanılmışsa Blockchain Access UK Ltd.'nin bunu kullanıcının profiliyle ilişkilendirebileceği anlamına gelir (çünkü bu eylemler için KYC gerekir). Blockchain.com'un bu yan kuruluşu, takas, kurumsal saklama ve tezgah üstü ticaret hizmetlerini yönetir.

Blockchain Access UK Ltd. bir borsa olarak çalışır ve "Amerika Birleşik Devletleri'nde kayıtlı bir Para Hizmetleri İşletmesidir. Bu nedenle, müşteri bilgilerini, örneğin Amerika Birleşik Devletleri Banka Gizlilik Yasası'nın gerektirdiği risk temelli yaklaşımla tutarlı bir şekilde toplar ve kaydeder."

Yukarıda belirtildiği gibi, Blockchain.com müşterilerinin verilerini saklar ve resmi olarak talep edilmesi durumunda, bu verilerin kanun uygulayıcı yetkililerle paylaşılması gerekir.

Bununla birlikte, web sitelerine göre, Blockchain Luxembourg kendi emanetçi cüzdan kullanıcılarının aşağıdaki bilgilerini bilmiyor.³⁷

- Cüzdan bakiyeleri
- İşlem geçmişi
- Ziyaret edilen web sayfaları
- Yasal isimler
- Posta adresleri

³⁷ Daha fazla bilgi için: <https://www.blockchain.com/legal/law>

- Sosyal güvenlik ya da ulusal kimlik numaraları

AB yönetmeliği olmasına rağmen, Blockchain Lüksemburg'un, bir kullanıcı adına (veya kullanıcının isteklerine karşı) sanal para harcayamayacağını, kanuni yaptırım adına sanal parayı donduramayacağını veya kaybedemeyeceğini veya cüzdanların içeriğini bilemeyeceğini belirttiğini vurgulamakta fayda var.

3.7.2 En iyi uygulamalar ve kılavuzlar

Araştırmacılar, şüphelilerinin tarayıcı geçmişini incelerken ilginç işaretler bulabilirler. İşaretler, örneğin, kara para akladıkları veya yasa dışı gelirlerini depoladıkları Sanal Varlık Hizmet Sağlayıcılarına birden ortaya çıkabilir.

Bir diğer önemli adım da şüpheli akıllı telefonlarda 2FA uygulamalarını kontrol etmektir. Kraken veya diğerleriyle bir Google Authenticator bağlantısı var mı? Eğer öyleyse, muhtemelen bu platformda bir hesap tutuyorlar.

Hemen hemen tüm emanetçi cüzdanların (özellikle kripto para platformları) kullanıcıları hakkında kişisel bilgilere sahip olduğunu bilmek iyidir. En azından, bir e-posta adresini ve IP adresi günlüklerini paylaşabilecekler.

Bireyler belirli bir miktarın üzerinde ticaret yapmak istediklerinde veya itibari parayla ticaret yapmak istediklerinde, iş yaptıkları platformun Müşterini Tanı (KYC) yönetmeliğine uyma ihtimalleri vardır.

Örneğin Kraken^{38,39} 'e bakalım. Kraken'in, kolluk kuvvetleri hizmetlerine ve hizmetlerinden yapılan sanal para işlemlerinin arkasındaki kişileri tanımlamasına yardımcı olabilecek müşteri politikalarını çok iyi bildiği bilinmektedir.

³⁸ <https://support.kraken.com/hc/en-us/articles/360001449826-Deposit-and-withdrawal-limits-by-verification-level>

³⁹ <https://support.kraken.com/hc/en-us/articles/201352206-Verification-level-requirements>

	Daily limits	Monthly limits	Margin	Requirements
Tier 0 Deposits and withdrawals are not available.	Deposit (fiat) \$0.00 Deposit (crypto) \$0.00 Withdraw (fiat) \$0.00 Withdraw (crypto) \$0.00	Deposit (fiat) \$0.00 Deposit (crypto) \$0.00 Withdraw (fiat) \$0.00 Withdraw (crypto) \$0.00		Account signup
Tier 1 You can trade between all currencies, but account funding is limited to digital currencies only.	Deposit (fiat) \$0.00 Deposit (crypto) No limit Withdraw (fiat) \$0.00 Withdraw (crypto) \$2,500.00	Deposit (fiat) \$0.00 Deposit (crypto) No limit Withdraw (fiat) \$0.00 Withdraw (crypto) \$20,000.00	Enabled	• Full name • Date of birth • Country of residence • Phone number
Tier 2*	Deposit (fiat) \$2,000.00 Deposit (crypto) No limit Withdraw (fiat) \$2,000.00 Withdraw (crypto) \$5,000.00	Deposit (fiat) \$10,000.00 Deposit (crypto) No limit Withdraw (fiat) \$10,000.00 Withdraw (crypto) \$50,000.00	Enabled	• All of the above • Address verification
Tier 3	Deposit (fiat) \$25,000.00 Deposit (crypto) No limit Withdraw (fiat) \$25,000.00 Withdraw (crypto) \$50,000.00	Deposit (fiat) \$200,000.00 Deposit (crypto) No limit Withdraw (fiat) \$200,000.00 Withdraw (crypto) \$200,000.00	Enabled	• All of the above • Government issued ID • Verified proof of residence (e.g., utility bill no more than 3 months old) • Social Security number (US only) • ID confirmation photo (see footnote)*
Tier 4 Individual High Value Account or Corporate Account	Deposit (fiat) \$100,000.00 Deposit (crypto) No limit Withdraw (fiat) \$100,000.00 Withdraw (crypto) \$100,000.00	Deposit (fiat) \$500,000.00 Deposit (crypto) No limit Withdraw (fiat) \$500,000.00 Withdraw (crypto) \$500,000.00	Enabled	• If you are interested in a personal or business Tier 4 account, please contact support. • Choose the category "Verification: Tier 4" for your support request.

Uygun bir KYC (Müşterini Tanı), platformun talep üzerine kanun yaptırımı için en azından aşağıdaki belgelere sahip olmasını sağlar:

- Ehliyet veya resmi makamlarca verilmiş fotoğraflı kimlik ile doğrulanmış ad
- Doğrulanmış ikamet kanıtı
- Sosyal güvenlik numarası
- Email adresi, telefon numarası

- IP ve Çerez Bilgileri

Belirli bir kullanıcı hakkında KYC (Müşterini Tanı) bilgilerine sahip olup olmadıklarını öğrenmek için çeşitli kanallar aracılığıyla bir Sanal Varlık Hizmet Sağlayıcısıyla iletişime geçilebilir. İletişime geçmeden önce, Sanal Varlık Hizmet Sağlayıcısının uyumlu olup olmadığını kontrol etmek için LEA topluluğunuzla danışmak iyi olacaktır. KYC (Müşterini Tanı) ve diğer ilgili bilgilere sahiplerse, soruşturmacıların bu bilgileri almak için bir mahkeme celbi veya yargı yetkisine bağlı olarak uygun talep göndermeleri gerekir.

3.7.3 İki Faktörlü Kimlik Doğrulama (2FA)

Kullanıcıların 2FA (İki Faktörlü Kimlik Doğrulama) (Google Authenticator, YubiKey, Authy veya SMS kodları aracılığıyla) kullanmaları önerilir. Çoğu durumda, ekstra bir güvenlik katmanı olarak, kullanıcı oturum açmak istediğinde bağlı e-posta adresine bir link gönderilir. Dolayısıyla, araştırmacının bir şifresi ve kimlik doğrulama uygulamasına erişimi olsa bile, şüphelinin (sulh hakiminin / hakim onayı ile - yukarıya bakın) e-posta hesabına erişim de gerekli olabilir.

3.8 Anahtar Kelimeler

Anahtar kelimeler bu kılavuzda birkaç kez ele alınmıştır, bunlar kripto paraların önemli ve esas parçasıdır. Anahtarla, çok sayıda farklı madeni parayı geri yükleyebilir ve bunlara el koyabilir ve şüphelinin cüzdanının tam olarak aynı kopyasını geri yükleyebilirsiniz.⁴⁰ Fakat, bazı cüzdanların BIP protokollerini aynı şekilde takip etmediğini ve bu nedenle bir cüzdanın size bir sürü para iade edebileceğini, diğerinin ise tamamen boş bir cüzdan açtığını bilmek de önemlidir.

Anahtar kelimeleri araştırmak için, bir kripto para cüzdanı kurmadan bile özel anahtarları belirlemeye yönelik bazı araçlar vardır. Daha önce belirtildiği gibi, BIP32/44/49 cüzdanları aynı adresleri vermelidir, ancak bu her zaman böyle değildir⁴¹. Electrum, Exodus, Mycelium, Copay, Jaxx, Coinomi ve diğer bazı cüzdanlar tamamen farklı bir özel ve genel anahtar seti iade edebilir. Bunun nedeni, farklı yazılım sağlayıcılarının anahtar algoritmalarını biraz farklı kullanmasıdır. Bu nedenle, farklı onarım süreçleri ve araçlarının denenmesi önerilir. Ian Coleman hangi adreslerin anahtar kelimelerle ilişkili olduğunu kontrol etmek için çevrimdışı olarak indirilebilen Mnemonic Code Converter⁴² adlı bir web sitesi oluşturdu; ancak farkı tanıyıp farklı yazılımların hangi anahtarları döndürdüğünü analiz ediyor gibi görünmemekte. Fakat hâlâ çok kullanışlı ve birçok farklı sanal paranın anahtar kelimelerini dönüştürücüde kullanabilirsiniz. Mevcut olan bu türetme araçlarını test edip denemeniz önerilir, ayrıca kurumunuzda bazı özel kolluk kuvvetleri araçları da olabilir.

Bu kılavuzda kullanılan şu anahtar kelimeleri (BIP49) kontrol ederken

“yan kullanışlı geniş mutsuz galeri kaşık sergi yastık derinlik geçerli canlı antrenör durumlar asla cihaz indeks garip doğum ayak bileği harcamalı görünmek parti patlama yolu”

anahtar için şu sonucu alacağız

Türetme yolu m/49'/0'/0'/0/0

Genel anahtar: 3A9XTNSSaQesZjDwEWcP6knKGC9YzFBQHe

Özel anahtar: L2HFbHMB3hZVsaVQDkD7D7VUKg8A96x7mKhazKGQreJLGUfApHhQ

⁴⁰ Daha fazla kaynak için https://en.bitcoin.it/wiki/Seed_phrase

⁴¹ Anahtar kelimelerle ilgili daha fazla kaynak için <https://walletsrecovery.org/>

⁴² <https://iancoleman.io/bip39/>

Doğru. Dolayısıyla, bir bakıma anahtar kelime listesinden doğru özel anahtarları oluşturmak için de bu aracı kullanabilirsiniz. Bu araçlarla pratik yapmanız şiddetle tavsiye edilir. Türetme yolu aşağıdaki gibi oluşturulur⁴³.

m/purpose/coin_type/account/change/address_index

- m: ana anahtardır
- purpose: BIP uygulamasıdır; bu durumda 49, BIP49 anlamına gelir
- coin_type: şu anda Bitcoin için 0, Bitcoin Testnet için 1, Litecoin için 2 ve Ethereum için 60 olacaktır.
- account: alt hesaplar kurma imkanı verir; örneğin 1 dirty coinler için ve 2 karışık mixed coinler içindir ve 3 sadece clean coinler için olabilir vs.
- change: adresi yalnızca bir işlemde değişimi almak için bir adres olarak işaretler
- address_Index ödemeler için numaralandırılmış alıcı adresini temsil eden bir sayıdır
- numbering: 0'dan başlar, bu nedenle 3 değeri ağacın o dalındaki alıcı adres 4 olacaktır.

Ian Colemans türetme yolu aracı gibi bir araç kullanırken, aslında şüphelinin sahip olduğu bilgisayara aynı tür cüzdanı yüklemenize gerek yoktur.

3.9 Raporlama

Kripto paralara el koyulurken bazı bilgilerin belgelendirilmesi ve raporlanması gerekir. Raporun ilgili bilgi ve unsurları, ülkenin geçerli yasal çerçevesine ve raporlama standartlarına bağlıdır.

Bir rapor, el koyma işlemiyle ilgili genelde en azından aşağıdaki bilgileri içerir:

- Kripto paranın adı (ör., Bitcoin, Ethereum)
- Tutar (ör., 0,15 BTC, 1 ETH)
- İşlem ücreti (tutar)
- Tarih, zaman ve zaman dilimi (ör., 25/12/2020 10:00 CET)
- İşlem kimliği (kriptografik özet)
- Göndericinin adres(ler)i
- Alıcı adresi (yani devlet kontrolündeki adres)

Ayrıca ne tür cüzdan(lar) ve cihaz(lar) kullanıldığını, el koyma işleminin hangi koşullarda ve nasıl gerçekleştirildiğini, cihaz(lar) üzerinde yapılan manipülasyonları, el koyma sırasındaki bakiyeyi vs. raporda belirtebilirsiniz.

Bir raporda devlet kontrolündeki bir cüzdanın özel anahtarlarını veya anahtarlarını asla ifşa etmeyin.

Örneğin bitcoine el koyarken, Bitcoin'in sabit blok zinciri, tartışılmaz bir kanıt biçimi işlevi görebilir. İlgili bilgilerle birlikte Bitcoin işlemleri otomatik olarak kaydedilir ve böylece halka açık Bitcoin blok zincirinde belgelenir.

Bir el koyma işleminin ekran görüntülerini ve/veya ekran kaydını (özel anahtarı göstermeden) rapora eklemek iyi bir uygulamadır.

⁴³ Türetme yollarıyla ilgili daha fazla bilgi için: https://en.bitcoin.it/wiki/BIP_0175

4 Kapanış

Bu kılavuz, Avrupa Birliği iPROCEEDS-2 çerçevesinde görevlendirilmiş ve geliştirilmiştir. Araştırmacıya, kripto paraları ele geçirebilmek için pratik deneyim sağlayacak gerekli bazı bilgilerde ve TPP’de ustalaşmak için rehberlik edecektir. Ne yazık ki, bu (el koyma) alanı çok geniş olduğundan tüm konular ele alınamamıştır.

Kılavuz yazılırken tüm yazılım ve teknikler geçerli idi. Buna rağmen, araştırmacıların, kripto para alanının sürekli geliştiğinin ve oldukça hızlı bir şekilde değiştiğinin farkında olmaları gerekir. Bu nedenle, kripto paralara el koymaları gerektiğinin farkına vardıklarında, araştırmacılar ayrıca kendilerini önceden hazırlamak, güncellemek ve eğitim/pratik yapmak için yeterli zamana ihtiyaç duyarlar.

Bazen beklenmedik durumlar ortaya çıkabilir; fakat kılavuzdaki konuları test edip uygulayarak birçok durumda başarılı olmayı sağlayacak büyük bir adım atılmış olacaktır.

Ayrıca aşağıda belirtilen mevcut destekleyici materyallerin kullanılması da önerilmektedir:

- Europol Bitcoin araştırma kılavuzu
- Sanal Varlıklara El Konulmasına İlişkin Kılavuz (Guidelines for the Seizure and Sale of Virtual Assets), INTERPOL (Kasım 2020, sadece resmi kullanımlar için)
- “Kripto Para ve Karanlık Ağ Soruşturmaları” (“Cryptocurrency and Dark Web Investigations”) eğitim paketi
- Nick Furneau Kripto Paraların Araştırılması⁴⁴

Bu kılavuz, yalnızca devlet ve kanun uygulayıcılara dağıtım amaçlı hazırlanmıştır; kılavuzun yetkisiz dağıtımı ve/veya herhangi bir bölümünün kopyalanması kısıtlanmıştır/yasaktır.

⁴⁴ Nick Furneau Investigating cryptocurrencies (Kripto Paraların Araştırılması):
<https://investigatingcryptocurrencies.com/>