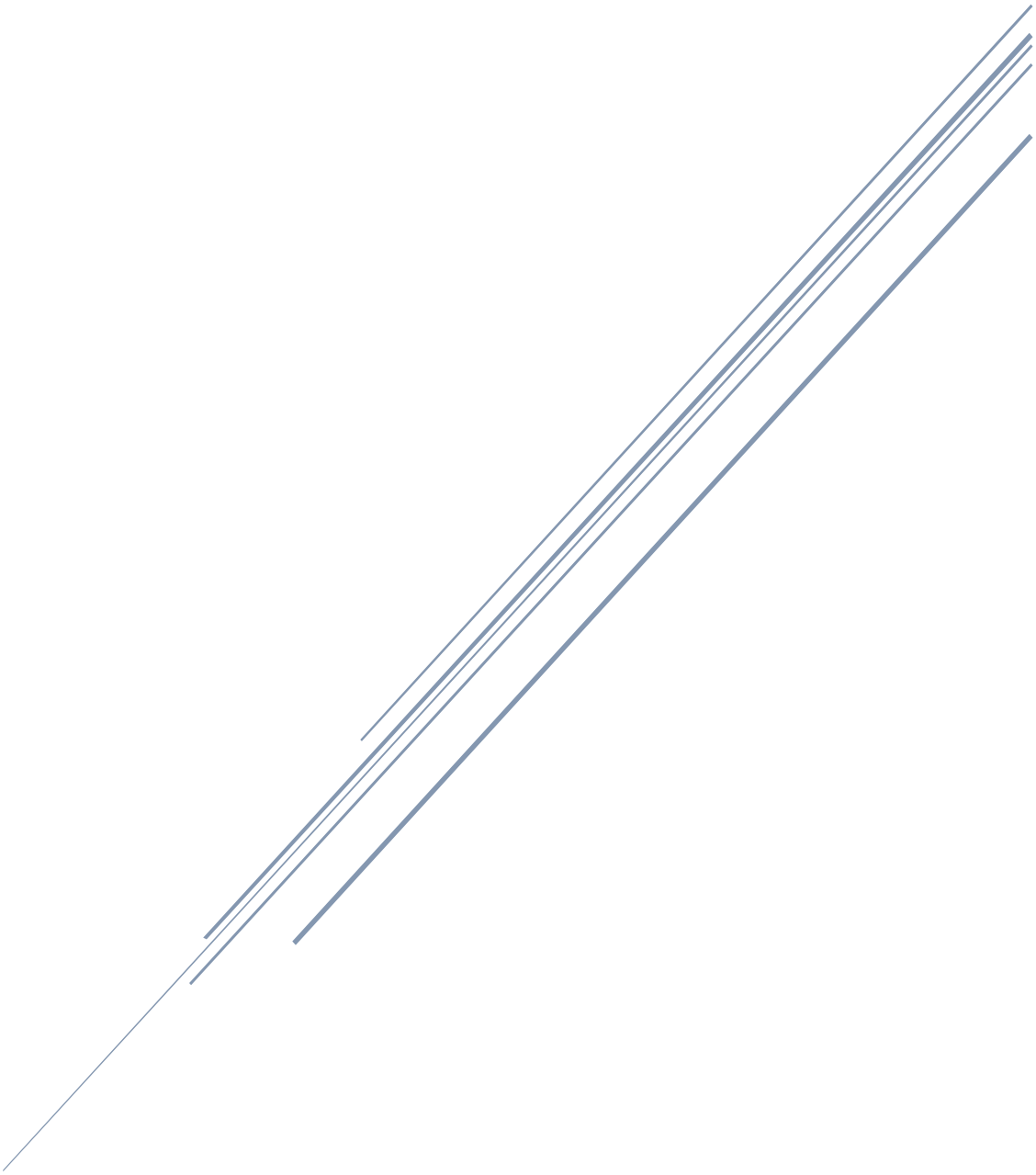
KRİPTO VARLIKLARA İLİŞKİN TEMEL KAVRAMLAR

denetci.org



18 Mayıs
2025

İÇİNDEKİLER

1. KRİPTO VARLIK HİZMET SAĞLAYICILARINA İLİŞKİN TEMEL KAVRAMLAR

1.1. AÇIK ANAHTAR

Dağıtık defter ağı (1.14) üzerinden bir cüzdandan (1.8) diğer bir cüzdana kripto varlık (1.34) gönderilebilmesi için cüzdanı eşsiz bir şekilde belirleyen hesap adreslerinin (1.2) oluşturulması, gerçekleştirilen kripto varlık transfer işlemlerinin doğrulanması ve benzeri amaçlarla kullanılan anahtarıdır.

1.2. ADRES

Dağıtık defter ağındaki (1.14), kripto varlık hesaplarını (1.34) ve akıllı sözleşmeleri (1.4) tekil olarak tanımlayan karakter dizisidir.

1.3. AĞLAR ARASI GEÇİŞ SİSTEMLERİ (CROSS DOMAİN SOLUTİONS)

Soğuk cüzdanın (1.42) izole edilmiş bileşenlerinin bulunduğu ağ ile internete bağlı bileşenlerin yer aldığı ağ arasında, sadece belirli verilerin geçişini sağlamak amacıyla elektronik yöntemlerle veri iletim kontrolü sağlayan sistem ve süreçleridir (teknik hava boşluğu (1.28) olarak da değerlendirilebilir).

1.4. AKILLI KONTRAT / SÖZLEŞME

Dağıtık defter teknolojisi (1.14) üzerinde çalışan, önceden belirlenmiş koşulların gerçekleşmesiyle otomatik olarak yürütülen ve düğümler (1.18) tarafından doğrulanan yazılım kodudur.

1.5. AKTİF-OLMAYAN SOĞUK CÜZDAN

İlklendirilen (1.33) ve cüzdan (1.8) adresleri (1.2) oluşturulan ancak bu adreslerdeki kripto varlıkların (1.34.) transfer edilebilmesi için cüzdanı işleten KVHS'nin (1.35) belirlediği ek işlemlerin, şartların ve prosedürlerin yerine getirilmesi gereken soğuk cüzdanlardır (1.42).

1.6. ANA ANAHTAR (MASTER KEY)

İlklendirmede (1.33) güvenli donanım modülü kullanılarak oluşturulan, güvenli donanım modülünde tutulan ve diğer tüm anahtarların (1.1) (1.40) güvenliğini sağlayan anahtardır.

1.7. AYRIK HESAP (SEGREGATED ACCOUNT)

Yalnızca bir müşteri için oluşturulan ve sadece o müşteriye ait kripto varlıkların (1.34) saklandığı hesap türüdür.

1.8. CÜZDAN (WALLET)

Kripto varlıkların (1.34) transfer edilebilmesini ve bu varlıklara ilişkin özel (1.40) ve açık anahtarların (1.1) çevrim içi veya çevrim dışı olarak depolanmasını sağlayan yazılım, donanım, sistem ya da uygulamalardır.

1.9. CÜZDAN ERİŞİM DENETİMİ

Transfer emirlerinin yetkili kullanıcılar tarafından verildiğinin ve onaylandığının doğrulanması ile sürecin Sermaye Piyasası Kurulunun düzenlemelerine, kripto varlık hizmet sağlayıcılarının (1.35) belirlediği politikalara ve Tebliğ'in 31 inci maddesi uyarınca imzalanan saklama sözleşmesine uygun olarak yürütüldüğüne ilişkin kontrollerin tamamıdır.

1.10. ÇATALLANMA

Kripto varlık (1.34) ağında, geçici olarak birden fazla geçerli blok üretilmesi veya ağındaki protokol kurallarının değiştirilmesi sonucu, bazı düğümlerin (1.18) güncellenmiş kurallarla devam ederken bazılarının eski kurallarla işlemeye devam etmesiyle ağın kalıcı olarak ayrışmasıdır.

1.11. ÇOK TARAFLI EŞİK KRİPTOGRAFİSİ

Kripto varlığın (1.34) kontrolünü sağlayan özel anahtarın (1.40) kriptografik yöntemler kullanılarak birden fazla taraf arasında paylaştırılmasını sağlayan, belirlenmiş sayıda tarafın işlem yapması ile kripto varlık transferinin imzalaması ve sair faaliyetlerin gerçekleşebildiği tekniklerdir.

1.12. ÇOKLU İMZA (MULTİ-SİGNATURE)

Kripto varlık (1.34) transferlerinin geçerli sayılabilmesi için birden fazla yetkilinin özel anahtarlarıyla (1.40) imza atmasının mümkün olduğu ve birden fazla imza atıldığının dağıtık defter (1.15) düğümlerinde (1.18) kontrol edildiği tek bir kişinin işlem yapmasını engelleyen güvenlik mekanizmasıdır (kripto varlığın dağıtık defter dışı mekanizmalarla birden fazla yetkili tarafından imzalanmasına müsaade eden yöntemler için çok taraflı eşik kriptografisi (1.11) tanımına bakınız).

1.13. DAĞITIK DEFTER AĞI

İşlemlerin bir uzlaşma mekanizmasıyla doğrulanarak kaydedildiği ve bu kayıtların düğümler (1.18) arasında senkronize şekilde tutulduğu, merkezi olmayan bilgi işlem yapısıdır.

1.14. DAĞITIK DEFTER ENTEGRASYONU

Kripto varlık hizmet sağlayıcı (1.35) kuruluşların müşterilerine sundukları kripto varlık hizmetleri kapsamında, kuruluşa ait bilgi sistemlerinin kripto varlıkların (1.34) dağıtık defter ağları (1.13) ile etkileşmelerini sağlayan entegrasyonlarıdır (Bu entegrasyon kapsamında; işlem emirlerinin ağlara gönderilmesini, operasyonel süreçlerin daha güvenli yürütülebilmesi için

ağların çatallanma (1.10) vb. durumları hakkında bilgi sahibi olmalarını, transfer ücretlerini hesaplamalarını, işlemleri gerçek zamanlı olarak izlemelerini ve doğrulama yapmalarıdır).

1.15. DAĞITIK DEFTER TEKNOLOJİSİ

İşlem kayıtlarının ve durum verilerinin, dağıtık işleme ve depolama olanağı sağlanarak merkezi bir otoriteye ihtiyaç duyulmaksızın; eş katılımcıların işlettiği düğümlerden (1.18) oluşan bir ağ tarafından mutabakatla doğrulandıktan sonra yine düğümlerde kopyalarının tutulduğu teknolojidir.

1.16. DİJİTAL İMZALAMA ÖZEL ANAHTARI

Kripto varlık hizmet sağlayıcı (1.35) kuruluş yetkililerinin kimliklerini doğrulamak üzere kullandıkları mobil cihaz, akıllı kart ve benzeri ekipmanlarda üretilen, tutulan ve kullanılan imza anahtarıdır.

1.17. DİJİTAL İMZALAMA SERTİFİKASI

Kripto varlık hizmet sağlayıcı (1.35) kuruluş yetkililerinin kimliklerini doğrulamak amacıyla kullanılan dijital imzalama özel anahtarına karşılık gelen açık anahtarın, açık anahtar altyapısı (Bu amaçla anahtarlar, örneğin X509 v3 formatına uygun olarak sertifikalandırılıp ISO/IEC 27099'e uygun olarak yönetilebilir) kapsamında sertifikalandırılmasıdır.

1.18. DÜĞÜM (NODE)

Dağıtık defter ağına (1.13) katılan, dağıtık defterin (1.15) tamamını veya bir kısmını saklayan ve işlemleri doğrulayan bağımsız bir yazılım veya cihazıdır.

1.19. DÜĞÜM HİZMET SAĞLAYICI

İşlemlerin dağıtık defter ağına (1.13) gönderilmesi, sonuçlarının takibi, ağ ücretlerinin hesaplanması ve benzeri hizmetleri sunmak amacıyla, dağıtık defterin (1.15) tamamını veya bir kısmını farklı roller veya doğrulama düzeylerinde işleyerek veya depolayarak ağdaki düğümlere kesintisiz erişim hizmeti sağlayan aracı kuruluşlarıdır.

1.20. FPT_EMS (PROTECTİON AGAİNST ELECTROMAGNETİC EMANATİON)

Ortak kriterler standardı (ISO/IEC 15408) kapsamında; güvenli donanım modülünde işlenen kripto varlık (1.34) özel anahtarı (1.40), ana anahtar (1.6) ve benzeri gizli verilerin güvenliğine yönelik; elektromanyetik yayılım, basit güç analizi, diferansiyel güç analizi, zamanlama ve benzeri dışarıdan gözlemlenebilir fiziksel olaylara dayalı saldırılara karşı alınan önlemlerin yeterliliğinin değerlendirilmesidir.

1.21. EAL4 (EVALUATİON ASSURANCE LEVEL)

Ortak kriterler değerlendirmesi kapsamında EAL1-EAL7 seviyelerinden dördüncüsü olan EAL4 değerlendirme güvence seviyesi, ortak kriterler değerlendirmesine tabi ürünün metodik olarak tasarlandığı, test edildiği ve gözden geçirildiğidir.

1.22. EN 419221-5

Kripto varlık hizmet sağlayıcılar (1.34) tarafından kullanılacak güvenli donanım modüllerinin sağlaması gereken koruma profilidir.

1.23. EŞİK KRİPTOGRAFİSİ

İmzalama, yedekten kurtarma ve benzeri işlemlerin, önceden belirlenmiş asgari sayıda (veya daha fazla) katılımcının işlem yapmasıyla ortaklaşa gerçekleştirilmesini sağlayan kriptografik mekanizmalarıdır.

1.24. FIPS 140-3

Amerika Birleşik Devletleri Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından yayımlanan ve ISO/IEC 19790'ı temel alarak kriptografik modüllerin güvenlik gereksinimlerini içeren standardıdır.

1.25. GÜVENLİ DONANIM MODÜLÜ (HARDWARE SECURİTY MODULE - HSM)

Kriptografik anahtarların üretiminden kullanımdan kaldırılmasına kadar yaşam döngüsü boyunca korunması, özel anahtarların (1.40) harici veri tabanında saklanması için şifrelenmesi ve yedeklenmesi gibi işlemlerin; güvenli başlatma, kurcalama ve yetkisiz erişim gibi tehditlere karşı fiziksel ve teknik önlemlerle güçlendirilmiş yazılım ve donanım bileşenleriyle oluşturulan güvenli bir ortamda yapıldığı modülüdür.

1.26. GÜVENLİ ORTAM (SECURE ENCLAVE)

Aynı işlemci ve ortak hafıza kaynaklarını kullanan yazılımlar arasında kritik verilerin güvenli işlenmesi ve saklanmasını sağlamak amacıyla fiziksel ve/veya mantıksal güvenlik mekanizmaları kullanılarak oluşturulan izole ortamdır.

1.27. GÜVENLİK SINIRI

Cüzdan (1.8) bileşenlerinin, kripto varlık hizmet sağlayıcının (1.35) idari, teknik ve fiziksel bilgi güvenliği kontrolleriyle korunduğu ve bu bileşenlerin dış bileşen ve sistemlerle iletişiminin, güvenli protokoller veya güvenliği test edilmiş mekanizmalarla sağlandığı fiziksel/mantıksal bölge sınırlarıdır.

1.28. HAVA BOŞLUĞU (PHYSİCAL AİRGAP)

Güvenli donanım modül ve modülü yöneten sunucu vb. soğuk cüzdan (1.42) bileşenlerinin bulunduğu ağın, soğuk cüzdanın diğer bileşenlerinin bulunduğu ağlardan fiziksel olarak izole edilerek veri geçişinin kontrollü olarak manuel yöntemlerle sağlandığı süreç ve mekanizmalarıdır.

1.29. HAVUZ HESABI (OMNİBUS)

Birden fazla müşterinin kripto varlıklarının (1.34) ortak bir adreste (1.2) bileşik olarak tutulduğu hesap türüdür.

1.30. İŞLEM EMRİ

Müşteri tarafından ilgili KVHS'ye (1.35) verilen; kripto varlık (1.34) transferi, kripto varlık çekim adres (1.2) değişikliği ve benzeri taleplerdir.

1.31. ISO/TR 23576

ISO tarafından yayımlanan, dağıtık defter teknolojileri (1.15) kapsamındaki dijital varlık saklama kuruluşlarının güvenlik yönetimine ilişkin teknik raporudur.

1.32. KORUMA PROFİLİ

Ortak Kriterler değerlendirmesine tabi tutulacak sıcak/soğuk cüzdan (1.41) (1.42) altyapılarında kullanılan ürünlere yönelik hazırlanacak güvenlik gereksinimlerini tanımlayan dokümandır.

1.33. KRİPTOGRAFİK İLKLENDİRME (KEY CEREMONY)

Kripto varlıklara (1.34) ilişkin özel anahtarlar (1.40) ve bu anahtarların üretiminde kullanılan tohum (1.43) değerlerinin korunmasını sağlayan ana anahtarların (1.6) güvenilir bir ortamda ve yetkililerin gözetimi altında, güvenli bir şekilde kayıt altına alınarak oluşturulması ve yedeklenmesi sürecidir.

1.34. KRİPTO VARLIK

Dağıtık defter teknolojisi (1.15) veya benzer bir teknoloji kullanılarak elektronik olarak oluşturulup saklanabilen, dijital ağlar üzerinden dağıtımı yapılan ve değer veya hak ifade edebilen gayri maddi varlıklardır.

1.35. KRİPTO VARLIK HİZMET SAĞLAYICI (KVHS)

Platformları, kripto varlık (1.34) saklama hizmeti sağlayan kuruluşları ve 6362 sayılı Sermaye Piyasası Kanununa dayanılarak yapılacak düzenlemelerde kripto varlıkların ilk satış ya da dağıtımı dâhil olmak üzere kripto varlıklarla ilgili olarak hizmet sağlamak üzere belirlenmiş diğer kuruluşlardır.

1.36. KRİPTO VARLIK KİLİTLEME (STAKİNG)

Akıllı kontratlar (1.4) veya benzeri teknik mekanizmalar aracılığıyla, müşteri kripto varlıklarının (1.34) belirli bir süre için dağıtık defter ağında (1.13) mislen iade edilmek üzere kilitli tutularak müşteriye fayda sağlayan işlemlerdir.

1.37. KRİPTO VARLIK SAKLAMA HİZMETİ

Platform müşterilerinin kripto varlıklarının (1.34) veya bu varlıklara ilişkin cüzdandan (1.8) transfer hakkı sağlayan özel anahtarların (1.40) saklanmasını, yönetimini veya Sermaye Piyasası Kurulu tarafından belirlenecek diğer saklama hizmetleridir.

1.38. KURUM KAYDİ SİSTEMİ

Dağıtık defter ağına (1.13) işlenmeyen, platformun işlem platformu/işlem defteri/emir defteri ve muhasebe sisteminde yer alan kayıtlardır.

1.39. ONAYLI ADRES LİSTESİ (WHİTELİST)

Sadece belirlenmiş çekim adreslerine (1.2) kripto varlık (1.34) transferine izin veren listedir.

1.40. ÖZEL ANAHTAR

Cüzdanlardan (1.8) transfer hakkı sağlayan, işlemlerin yetkili kişi tarafından verildiğini kriptografik olarak kanıtlayan veya akıllı kontratları (1.4) yönetmek için kullanılabilen gizli anahtarıdır.

1.41. SICAK CÜZDAN

Kripto varlık hizmet sağlayıcıların (1.35), müşterilerinin kripto varlık (1.34) transferlerini karşılamak için kullandıkları, soğuk cüzdanın (1.42) tanımında belirtilen izolasyonun zorunlu tutulmadığı cüzdan (1.8) teknolojisidir.

1.42. SOĞUK CÜZDAN (AKTİF VE AKTİF-OLMAYAN SOĞUK CÜZDAN)

Kripto varlık (1.34) transferinin imzalanması gibi kritik işlemlerin yetkili personel müdahalesi gerektiren fiziksel hava boşluğu ve/veya yetkili müdahalesi gerektirmeyen teknik hava boşlukları (1.3) kullanılarak izole edilmiş ortamlarda yapılmasına olanak sağlayan cüzdan (1.8) teknolojisidir.

1.43. TOHUM (SEED)

Kripto varlık (1.34) özel anahtarlarını (1.40) deterministik olarak türetmek için kullanılan başlangıç anahtarıdır.

2. KRİPTO VARLIKLARA İLİŞKİN TEMEL KAVRAMLAR

2.1. BLOKZİNCİR (BLOCKCHAIN)

Blokzincir, dijital verilerin şeffaf, güvenli ve merkezi olmayan bir şekilde kaydedilmesini sağlayan dağıtık bir veri tabanı teknolojisidir.

Bloklar halinde gruplanmış veriler, kronolojik sırayla birbirine zincirlenir (block + chain), her blok öncekinin kriptografik özetini (hash) (2.39) içerir. Bu yapı, verilerin sonradan değiştirilmesini neredeyse imkânsız hale getirir.

Özellikleri:

- **Dağıtık yapı:** Veriler merkezi bir sunucuda değil, ağdaki tüm katılımcılarda (node) (1.18) tutulur.
- **Değiştirilemezlik:** Bir blok eklendikten sonra geri dönüp değiştirmek teknik olarak çok zordur.
- **Şeffaflık:** Blok zinciri herkese açıktır; işlemler doğrulanabilir.
- **Güvenlik:** Kriptografi ile korunur; sahtecilik önlenir.

2.2. BİTCOİN

Bitcoin, 2008 yılında Satoshi Nakamoto takma adlı kişi veya kişiler tarafından ortaya atılan, merkezi olmayan, dijital bir para birimidir.

2009 yılında açık kaynaklı olarak geliştirilmeye başlanmıştır ve işlemler, herhangi bir banka ya da otoriteye ihtiyaç duymadan, blockchain (blokzinciri) (2.1) adı verilen dağıtık bir defter sistemi (1.15) üzerinde gerçekleştirilir.

Özellikleri:

- **Merkeziyetsizlik:** Hiçbir devlet, banka veya kuruma bağlı değildir.
- **Maksimum arz sınırı:** Toplamda üretilebilecek Bitcoin sayısı 21 milyon ile sınırlıdır.
- **Geri döndürülemezlik:** Onaylanan işlemler blokzincirine kalıcı olarak kaydedilir.
- **Kriptografik güvence:** Sahtecilik ve çift harcama gibi riskler önlenir.

2.3. ALTCOİN

Altcoin yani alternatif coin, Bitcoin (2.2) dışındaki tüm kripto para birimlerini tanımlamak için kullanılır.

Her altcoin, Bitcoin'in ardından geliştirilen farklı blockchain (2.1) teknolojilerine dayanabilir veya Bitcoin'in açık kaynak kodu üzerinden türetilmiş olabilir.

2.4. JETON (TOKEN)

Token, bir blokzincir (2.1) platformu üzerinde oluşturulan dijital varlık veya temsil birimidir. Kendi blokzinciri olmayan; bunun yerine genellikle Ethereum, Binance Smart Chain gibi mevcut bir blokzincir üzerinde çalışan kripto varlıklardır (1.34).

2.5. COİN

Kendi blokzincir (2.1) ağı üzerinde çalışan bağımsız bir kripto para (2.40) birimine coin denir. Genellikle ağın yerel dijital varlığıdır ve ağ üzerinde işlem ücreti ödemek, transfer yapmak veya madencilik (2.10) / işlem doğrulama gibi işlevlerde kullanılır.

2.6. MERKEZİ BORSA (CEX)

Kripto varlıkların (1.34) alım-satım, takas ve saklama (1.37) işlemlerinin bir merkezi yapı (bir şirket veya kurum) tarafından yürütüldüğü dijital ticaret platformudur. Bu borsalar, kullanıcıların emirlerini (1.30) eşleştirir, işlem güvenliğini (1.27) (1.9) sağlar ve genellikle kullanıcı varlıklarını kendi cüzdanlarında (1.8) tutar.

2.7. MERKEZİYETSİZ BORSA (DEX)

Kripto varlıkların (1.34) kullanıcılar arasında doğrudan ve aracı olmadan işlem görmesini sağlayan, akıllı sözleşmelerle (1.4) çalışan dijital ticaret platformlarıdır. DEX'ler genellikle bir blokzincir (2.1) üzerinde çalışır ve varlıklar kullanıcı cüzdanları (1.8) arasında doğrudan transfer edilir.

2.8. STABLECOİN

Stablecoin, değerini genellikle bir geleneksel varlığa (örneğin; Türk Lirası, Euro, altın) sabitleyen kripto varlık (1.34) türüdür. Amaç, kripto para (2.40) piyasalarındaki yüksek fiyat oynaklığını azaltmak ve dijital işlemlerde istikrarlı bir değer birimi sağlamaktır.

2.9. MERKEZİYETSİZ FİNANS (DECENTRALİZED FİNANCE – DEFİ)

Merkeziyetsiz Finans (Decentralized Finance – DeFi), geleneksel finansal hizmetlerin (borç verme, alma, takas, sigorta vb.) aracı kurumlar olmadan, blokzincir (2.1) ve akıllı sözleşmeler (1.4) aracılığıyla sunulmasını ifade eder. DeFi sistemlerinde işlemler kullanıcılar arasında doğrudan (2.7) gerçekleşir ve kontrol merkezi bir otoriteye değil, kodlara (akıllı sözleşmelere) aittir.

2.10. MADENCİLİK (MİNİNG)

Madencilik (Mining), blokzinciri (2.1) üzerinde yapılan işlemleri doğrulamak (1.18) ve yeni bloklar oluşturmak için kullanılan süreçtir. Bu işlem, genellikle yüksek işlem gücü gerektiren matematiksel problemleri çözmeyi içerir. Madenciler, bu işlemler karşılığında kripto varlık (1.34) ödülleri alır (örneğin Bitcoin (2.2) ödülü). En yaygın yöntemlerden biri İş İspatı (Proof of Work – PoW) (2.14) mekanizmasıdır.

2.11. STAKİNG

Staking, kripto varlıkların (1.34) bir blokzincir ağı (2.1) üzerinde belirli bir süre kilitlenerek (1.36), ağın güvenliğine ve düğüm işlem doğrulamasına (1.18) katkı sağlanması karşılığında ödül kazanılması sürecidir. Bu yöntem, genellikle Hisse İspatı (Proof of Stake – PoS) (2.15) ve türev konsensüs mekanizmalarında kullanılır.

2.12. DEĞİŞTİRİLEMEZ JETON (NFT)

Değiştirilemez Jeton (NFT - Non-Fungible Token), dijital ortamda benzersiz ve tekil bir varlığı temsil eden, blokzincir (2.1) üzerinde kayıtlı bir kripto varlıktır (1.34). Her NFT farklıdır ve başka bir NFT ile birebir değiştirilemez. Dijital sanat eserleri, koleksiyon ürünleri, oyun içi varlıklar ve müzik gibi alanlarda yaygın olarak kullanılır.

2.13. İŞLEM ÜCRETİ (GAS FEE)

Bir blokzincir ağı (2.1) üzerinde yapılan işlemlerin (transfer (1.30), akıllı sözleşme (1.4) çalıştırma vb.) gerçekleşmesi için ağ doğrulayıcılarına (madenciler (2.10) veya stake edenler (2.11)) ödenen ücrettir. Bu ücret, işlemin maliyetini ve önceliğini belirler. Özellikle Ethereum gibi akıllı sözleşme platformlarında, bu ücret “gas” terimiyle ifade edilir.

2.14. İŞ İSPATI (PROOF OF WORK - POW)

Blokzincir ağında (2.1) işlemlerin doğrulanması (1.18) ve yeni blokların eklenmesi için katılımcıların yüksek hesaplama gücü gerektiren matematiksel problemleri çözmesini esas alan bir konsensüs (uzlaşım) mekanizmasıdır. Bu mekanizmayla çalışan madenciler (2.10), doğru çözüme ulaşan ilk kişi olarak blok ödülü kazanır. Bitcoin (2.2) gibi ilk nesil kripto paralarda (2.40) yaygındır.

2.15. HİSSE İSPATI (PROOF OF STAKE - POS)

Blokzincir ağında (2.1) yeni blokların doğrulanması ve eklenmesi (1.18) sürecinde, katılımcıların (doğrulayıcıların) sahip oldukları kripto varlık (1.34) miktarına göre seçildiği bir konsensüs (uzlaşım) mekanizmasıdır. PoW (2.14) sisteminden farklı olarak enerji yoğun madencilik (2.10) yerine, kullanıcılar varlıklarını stake ederek (2.11) ağın güvenliğine katkı sağlar ve ödül kazanır.

2.16. KATMAN (LAYER)

Katman (Layer), blokzincir teknolojisinde (2.1) ağın mimari yapısını ifade eden kavramdır ve genellikle işlevsel farklılıkları ayırmak için kullanılır. Katmanlar, ölçeklenebilirlik, işlem hızı ve işlevsellik gibi amaçlarla tanımlanır. En yaygın ayrım Katman 1 ve Katman 2 şeklindedir:

- **Katman 1**: Ana blokzincir ağıdır (örneğin: Bitcoin (2.2), Ethereum).
- **Katman 2**: Ana zincirin üzerinde çalışan, işlem hızını artıran veya maliyeti düşüren protokollerdir (örneğin: Lightning Network, Arbitrum).

2.17. ANA AĞ (MAİNNET)

Blokzincir projesinin (2.1) tam olarak çalışır durumda olduğu, gerçek işlemlerin gerçekleştirildiği ve kripto varlıkların (1.34) gerçek değere sahip olduğu ana blokzincir ağıdır. Geliştirme ve test (2.18) sürecinden sonra projelerin resmen faaliyete geçtiği ortamdır.

2.18. DENEME AĞI (TESTNET)

Blokzincir sisteminin (2.1) geliştirme ve test amacıyla kullanılan, gerçek para değeri taşımayan alternatif versiyonudur. Geliştiriciler, akıllı sözleşmeleri (1.4) ve uygulamaları ana ağa (mainnet) (2.17) geçmeden önce testnet üzerinde güvenli şekilde deneyebilir.

2.19. MERKEZİYETSİZ OTONOM ORGANİZASYON (DAO)

Merkeziyetsiz Otonom Organizasyon (DAO), bir topluluk tarafından yönetilen ve karar alma süreçleri ile işleyişi, akıllı sözleşmelerle (1.4) otomatikleştirilmiş, merkeziyetsiz dijital yapılardır. DAO'lar, herhangi bir merkezi otoriteye bağlı olmadan, katılımcıların token'lar (2.4) aracılığıyla oy kullanmasıyla yönetilir.

2.20. LİKİDİTE

Likidite, bir varlığın değer kaybına uğramadan hızlı ve kolayca nakde (veya başka bir varlığa) çevrilebilme kabiliyetini ifade eder. Kripto varlık (1.34) piyasalarında likidite, bir kripto paranın (2.40) alım-satım işlemlerinin hızlı ve düşük fiyat farkıyla (spread) yapılabilmesini sağlar. Yüksek likidite, daha sağlıklı ve istikrarlı bir piyasa anlamına gelir.

2.21. MÜŞTERİ TANIMA (KNOW YOUR CUSTOMER - KYC)

Finansal kuruluşlar ve kripto varlık hizmet sağlayıcılarının (1.35), müşterilerinin kimlik bilgilerini doğrulamak ve tanımak amacıyla uyguladığı düzenleyici süreçtir. KYC, kara para aklamayı önleme (AML) (2.38) ve terörizmin finansmanını engelleme politikalarının bir parçasıdır.

2.22. BEYAZ KİTAP (WHİTEPAPPER)

Beyaz Kitap (Whitepaper), bir kripto varlık (1.34) projesinin teknik altyapısını, amacını, kullanım alanlarını, token (2.4) ekonomisini ve yol haritasını detaylı şekilde açıklayan resmî belgedir. Yatırımcılara ve topluluğa projenin nasıl çalıştığını ve hangi sorunu çözmeyi hedeflediğini anlatır.

2.23. KURTARMA KELİMELERİ

Kurtarma Kelimeleri, bir kripto cüzdanın (1.8) özel anahtarını (1.40) temsil eden ve genellikle 12 ila 24 kelimeden oluşan, cüzdanın yedeklenmesini ve yeniden erişimini sağlayan kelime dizisidir. Bu kelimeler, cüzdan kaybı, cihaz bozulması gibi durumlarda kripto varlıklara (1.34) tekrar erişilebilmesini mümkün kılar.

2.24. YARILANMA (HALVİNG)

Bazı kripto para birimlerinde (2.40) (özellikle Bitcoin'de (2.2)) madencilere (2.10) verilen blok ödülünün, belirli aralıklarla yarıya düşürülmesi sürecidir. Bu mekanizma, yeni coin (2.5) arzını zamanla azaltarak enflasyonu kontrol altına almayı ve dijital varlığın kıtlığını korumayı amaçlar.

2.25. %51 SALDIRISI

%51 Saldırısı (51% Attack), bir blokzincir ağında (2.1) toplam işlem doğrulama gücünün (1.18) (hashrate veya stake'in (2.11)) %51'inden fazlasının tek bir kişi veya grup tarafından ele geçirilmesiyle yapılan saldırıdır. Bu durumda saldırgan, işlemleri durdurabilir, çifte harcama yapabilir ve geçmiş blokları geri alabilir. En çok İş İspatı (Proof of Work – PoW) (2.14) sistemlerinde gündeme gelir.

2.26. SERT ÇATALLANMA

Sert Çatallanma (Hard Fork), bir blokzincir protokolünde (2.1) yapılan ve geriye dönük uyumluluğu olmayan radikal bir güncellemedir. Bu tür bir güncelleme sonrası zincir ikiye ayrılabilir: biri eski kurallarla devam ederken, diğeri yeni kurallarla çalışan ayrı bir blokzincir oluşturur. En bilinen örneklerden biri Bitcoin (2.2) → Bitcoin Cash çatallanmasıdır.

2.27. YUMUŞAK ÇATALLANMA

Yumuşak Çatallanma (Soft Fork), bir blokzincir protokolünde (2.1) yapılan ve geriye dönük uyumlu olan güncellemedir. Eski yazılımı kullanan düğümler (node'lar) (1.18), yeni kurallarla oluşturulan blokları tanımaya devam edebilir. Bu sayede ağ bölünmeden güncelleme yapılabilir. Örnek olarak SegWit (Bitcoin Segregated Witness) güncellemesi verilebilir.

2.28. HALI ÇEKME (RUG PULL)

Rug Pull olarak bilinen Halı Çekme işlemi merkeziyetsiz finans (DeFi) (2.9) projelerinde görülen bir dolandırıcılık yöntemidir. Geliştiriciler, yatırımcılardan fon topladıktan sonra projeyi ani bir şekilde terk eder ve likiditeyi (2.20) çekerek yatırımcıların varlıklarını (1.34) değersiz bırakır. Genellikle denetlenmemiş akıllı sözleşmelerde (1.4) ve sahte token (2.4) projelerinde rastlanır.

2.29. KULLANIM AMAÇLI TOKEN (UTİLİTY TOKEN)

Kullanım Amaçlı Token (Utility Token), bir kripto varlık (1.34) projesi veya platformu içinde belirli hizmetlere erişim, işlem yapma ya da fayda sağlama amacıyla kullanılan token (2.4) türüdür. Bu token'lar, genellikle yatırım aracı değil, bir platformun işlevlerini kullanmak için tasarlanmıştır.

2.30. İLK KRİPTO PARA ARZI (ICO)

Bir kripto varlık (1.34) projesinin geliştirme sürecinde, yatırımcılardan fon toplamak amacıyla token (2.4) satışı gerçekleştirdiği bir halka arz yöntemidir. ICO süreci genellikle bir beyaz kitap (whitepaper) (2.22) yayınlanması ile başlar ve yatırımcılar proje başladığında dağıtılacak token'ları önceden satın alarak katkı sağlar. ICO'lar, erken aşama finansman aracı olarak kullanılır ve genellikle merkeziyetsiz borsa (2.7) ya da doğrudan cüzdanlar arasında yapılan işlemlerle gerçekleştirilir.

2.31. İLK MERKEZİYETSİZ BORSA ARZI (IDO)

İlk Merkeziyetsiz Borsa Arzı (IDO), bir kripto varlık (1.34) projesinin token'larını (2.4) ilk kez bir merkeziyetsiz borsa (DEX) (2.7) üzerinden halka arz etmesidir. IDO'lar, yatırımcılara doğrudan akıllı sözleşmeler (1.4) aracılığıyla token satın alma imkânı sunar.

Genellikle hızlı, sansürsüz ve merkezi borsalardan (2.6) bağımsız bir fon toplama yöntemidir.

2.32. İLK BORSA ARZI (IEO)

İlk Borsa Arzı (IEO), bir kripto varlık (1.34) projesinin token'larının (2.4) ilk kez bir merkezi borsa (CEX) (2.6) aracılığıyla halka arz edilmesidir. IEO sürecinde, token satışı doğrudan borsa platformu üzerinden yapılır ve borsa, proje denetimi, listeleme, güvenlik gibi konularda aracı rolü üstlenir.

Yatırımcılar, borsada hesapları aracılığıyla token satın alabilir ve işlemler genellikle borsa tarafından önceden doğrulanmış projeler üzerinden gerçekleştirilir.

2.33. KİLİT TOPLAM DEĞER (TVL)

DeFi (Merkeziyetsiz Finans) (2.9) protokolünde, akıllı sözleşmeler (1.4) aracılığıyla kilitlenmiş toplam kripto varlık (1.34) değerini ifade eder. TVL, bir DeFi platformunun likidite (2.20) düzeyini, güvenilirliğini ve kullanıcı ilgisini ölçmek için yaygın olarak kullanılan bir metriktir.

2.34. GETİRİ ÇİFTÇİLİĞİ (YİELD FARMİNG)

Getiri Çiftçiliği, kullanıcıların kripto varlıklarını (1.34) DeFi protokollerine (2.9) likidite (2.20) sağlamak amacıyla kilitleyerek (1.36) karşılığında faiz, ödül ya da yeni token'lar (2.4) kazandıkları bir gelir elde etme yöntemidir. Genellikle likidite havuzlarına katkı sağlamak ve bu katkıya karşılık pasif gelir elde etmek için kullanılır.

2.35. LİKİDİTE MADENCİLİĞİ

Likidite Madenciliği (Liquidity Mining), kullanıcıların DeFi protokollerine (2.9) likidite (2.20) sağlayarak, bunun karşılığında platformun yerel token'ları (2.4) ile ödüllendirildiği bir teşvik mekanizmasıdır. Yield farming (2.34) ile benzerlik gösterir; ancak odak noktası genellikle yeni token dağıtımı ve protokol benimsenmesini artırmaktır.

2.36. ZİNCİR ÜSTÜ (ON-CHAİN)

Zincir Üstü (On-Chain), bir blokzincir ağı (2.1) üzerinde gerçekleşen ve bloklara kalıcı olarak kaydedilen işlemleri ifade eder. Bu işlemler ağın tüm düğümleri (1.18) tarafından doğrulanır ve şeffaf bir şekilde izlenebilir.

Örnekler arasında token transferleri (2.4), akıllı sözleşme (1.4) etkileşimleri ve staking işlemleri (2.11) yer alır.

2.37. ZİNCİR DIŞI (OFF-CHAİN)

Zincir Dışı (Off-Chain), blokzincir ağı (2.1) dışında gerçekleşen ve blokzincire kaydedilmeyen işlemleri ifade eder. Bu tür işlemler genellikle daha hızlı ve düşük maliyetli olup, taraflar arasında mutabakatla yürütülür.

Örnek olarak borsa içi transferler, veya Lightning Network gibi 2. katman çözümleri (2.16) verilebilir.

2.38. KARA PARA AKLAMAYI ÖNLEME (AML)

Suç gelirlerinin yasal finansal sistemlere sokulmasını engellemek amacıyla uygulanan hukuki, idari ve teknik önlemler bütünüdür. Kripto varlık hizmet sağlayıcıları (1.35) da AML yükümlülükleri kapsamında, şüpheli işlemleri izlemek ve raporlamakla sorumludur.

2.39. KRİPTOGRAFİK ÖZET (HASH)

Kriptografik Özet (Hash), bir veri kümesini temsil eden, sabit uzunlukta ve benzersiz bir karakter dizisidir. Bu özet, bir kriptografik hash fonksiyonu (örneğin SHA-256) kullanılarak oluşturulur.

Hash'ler, blokzincirde (2.1) veri bütünlüğünü sağlamak, blokları zincirlemek ve işlemleri güvence altına almak için kullanılır.

2.40. KRİPTO PARA (CRYPTOCURRENCY)

Kripto para, blokzincir (2.1) teknolojisine dayanan, dijital olarak oluşturulan ve işlem gören, ödeme aracı veya değer transferi işlevi görebilen bir kripto varlık (1.34) türüdür. Coin (2.5) ve Token (2.4) olmak üzere iki ana türe ayrılır.

2.41. REZERV KANITI (PROOF OF RESERVES – POR)

Kripto varlık hizmet sağlayıcının (1.35) elinde tuttuğu müşteri varlıklarının, gerçekten ve eksiksiz şekilde mevcut olduğunu şeffaf ve doğrulanabilir biçimde kanıtlamak için kullanılan bir denetim mekanizmasıdır.

3. KAYNAKLAR

TÜBİTAK BİLGEM. (2025). Kripto Varlık Hizmet Sağlayıcıların Bilgi Sistemleri ve Teknolojik Altyapılarına İlişkin Kriterler (Sürüm 1.1). Türkiye Bilimsel ve Teknolojik Araştırma Kurumu.

https://bilgem.tubitak.gov.tr/wp-content/uploads/sites/8/TUBITAK-KVHS-Bilgi-Sistemleri-ve-Teknolojik-Altyapilarina-Iliskin-Kriterler_r1-1.pdf

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

https://bitcoin.org/bitcoin.pdf

III-35B.1 sayılı Kripto Varlık Hizmet Sağlayıcıların Kuruluş ve Faaliyet Esasları Hakkında Tebliğ

https://www.resmigazete.gov.tr/eskiler/2025/03/20250313-5.htm

III-35B.2 sayılı Kripto Varlık Hizmet Sağlayıcıların Çalışma Usul ve Esasları ile Sermaye Yeterliliği Hakkında Tebliğ

https://www.resmigazete.gov.tr/eskiler/2025/03/20250313-6.htm