BLOCKCHAIN
TÜRKİYE

KRİPTO VARLIK SAKLAMA RAPORU

Kripto Hizmet Sağlayıcıları Çalışma Grubu

MART 2025

TBV
TÜRKİYE BİLİŞİM VAKFI

BLOCKCHAIN
TÜRKİYE

KRİPTO VARLIK SAKLAMA RAPORU

Kripto Hizmet Sağlayıcıları
Çalışma Grubu

TBV
TÜRKİYE BİLİŞİM VAKFI

KRİPTO VARLIK SAKLAMA
RAPORU

MART 2025

SORUMSUZLUK BEYANI

Türkiye Bilişim Vakfı altında çalışmakta olan Blockchain Türkiye Platformu'nun "Kripto Hizmet Sağlayıcıları Çalışma Grubu" tarafından hazırlanan işbu rapor blokzincir teknolojisinin mevcut kişisel verilerin korunması mevzuatı ve uygulamaları bakımından incelenmesinden ibaret olup; teknik kapsam ilgili teknolojinin hukuki açıdan özümsenebilmesi amacıyla yayımlanmıştır. Kişi ve kurumları bağlayıcı tavsiye veya görüş niteliği taşımaz. İşbu rapor kamuya açık kaynaklardan yararlanılmış bilgileri içermekte olup, söz konusu bilgilerin güncel ve eksiksiz olduğu taahhüt edilmemektedir. İşbu raporda verilen tüm bilgi ve görüşler zamanla değişkenlik gösterebilir. Bu bağlamda işbu raporun içeriğini okuyan kişilere veya herhangi bir üçüncü kişiye karşı sorumluluğu ve yükümlülüğü bulunmamaktadır.

Kripto Hizmet Sağlayıcıları
Çalışma Grubu

ÖNSÖZ

Dijital varlıklar ve bunların saklanması, bilhassa son yıllarda finansal dünyanın en dinamik ve kritik bileşenlerinden biri haline gelmiştir. Teknolojinin ilerlemesi, blokzincir tabanlı varlıkların yaygınlaşması ve geleneksel finans sistemleri ile dijital ekosistem arasındaki entegrasyon ihtiyacı, dijital varlıkların güvenli bir şekilde saklanmasını her zamankinden daha önemli hale getirmiştir. Bu bağlamda, Kripto Hizmet Sağlayıcıları Çalışma Grubu olarak hazırladığımız bu kapsamlı rapor, sektördeki en güncel gelişmeleri, regülasyonel dinamikleri ve geleceğe dair projeksiyonları ele almaktadır.

Küresel çapta, dijital varlık saklama hizmetleri finans sektörü için kritik bir rol oynamaya başlamış, büyük finansal kuruluşlar ve teknoloji şirketleri bu alana ciddi yatırımlar yapmıştır. Dünyanın çeşitli bölgelerinde regülasyonlar netleşmekte, dijital varlıkların yasal statüsü belirginleşmekte ve kurumsal yatırımcılar için daha güvenli bir ortam oluşturulmaktadır. Farklı ülkelerde, dijital varlık saklama çözümleri için çeşitli teknik ve hukuki yaklaşımlar benimsenmiştir. Bu çeşitlilik, küresel çapta dijital varlık ekosisteminin nasıl şekillendiğine dair önemli bir tablo sunmaktadır.

Ülkemizde de dijital varlıklara ve saklama hizmetlerine olan ilgi giderek artmaktadır. Son yıllarda kripto varlık hizmet sağlayıcılara yönelik önemli regülatif düzenlemeler hayata geçirilmiş ve bununla birlikte dijital varlık saklama hizmetlerine yönelik çerçeve daha da netleşmiştir. Yeni regülasyonlar; kripto varlıkların tanımını, dijital varlık saklama kurumlarının lisanslandırılmasını ve güvenli saklama standartlarını kapsamaktadır. Türkiye'de bu alanda çıkarılan regülasyonlar, dijital varlık saklama hizmetlerinin daha güvenilir hale gelmesini sağlarken, sektörün hukuki zeminde büyümesine de katkıda bulunmaktadır.

Bu rapor, dijital varlık saklama konusunda hazırlanmış ilk rapordur ve sektördeki teknik altyapıyı, hukuki düzenlemeleri ve dünyadan farklı örnekleri ele alması bakımından en kapsamlı çalışmadır. Çalışmamızda, saklama hizmetlerinde kullanılan farklı teknolojiler de kapsamlı bir şekilde incelenmiştir. Soğuk cüzdan (cold storage) ve sıcak cüzdan (hot storage) çözümlerinden, çoklu imza (multi-signature) ve MPC (multi-party computation) gibi ileri seviye güvenlik teknolojilerine kadar çeşitli yaklaşımlar değerlendirilmiştir. Dijital varlık saklamasında güvenliği sağlamak için benimsenen bu yenilikçi çözümler, yatırımcıların ve finansal kuruluşların varlıklarını koruma yöntemlerini dönüştürmektedir.

Tüm bu gelişmeler, dijital varlıkların yalnızca bir yatırım aracı olarak değil, finansal sistemlerin ayrılmaz bir parçası olarak değerlendirilmesini de beraberinde getirmektedir. Geleneksel finans kurumları ve merkeziyetsiz finans uygulamaları arasındaki geçiş süreci hızlanırken, düzenleyici kurumların ve piyasa aktörlerinin birlikte çalışması kaçınılmaz hale gelmiştir. Dijital varlık saklaması konusundaki teknik gelişmeler ve hukuki düzenlemeler, bu dönüşüm sürecinin en önemli yapı taşlarını oluşturmaktadır.

Bu rapor, dijital varlık saklama alanındaki yerel ve küresel mevcut durumu, riskleri ve hukuki çerçeveyi detaylı bir şekilde inceleyerek, sektöre yön veren katılımcılara, regülatörlere ve yatırımcılara değerli bir kılavuz sunmayı amaçlamaktadır. Teknolojinin ve regülasyonların gelişimiyle birlikte, dijital varlıkların güvenli saklanması finansal ekosistemin ayrılmaz bir parçası olacaktır.

Sizleri, bu alandaki en yeni bilgileri ve analizleri içeren raporumuzu keyifle okumaya davet ediyorum.

Yasin Oral

Paribu Kurucu ve CEO'su

KISALTMA LİSTESİ

- **MPC** - Çok Taraflı Hesaplama
- **Multi-sig** - Çoklu İmza
- **HSM** - Donanım Güvenlik Modülleri
- **SGX** - Yazılım Koruma Uzantısı
- **AML** - Kara Para Aklanmasının Önlenmesi
- **CFT** - Terörizmin Finansmanının Önlenmesi
- **KYC** - Müşterini Tanı
- **HTTPS** - Güvenli Hiper Metin Aktarım İletişim Protokolü
- **PGP** - Oldukça İyi Mahremiyet
- **ECDLP** - Eliptik Eğri Ayrık Logaritma Problemi
- **EdDSA** - Edwards-Curve Dijital İmza Algoritması
- **IoT** - Nesnelerin İnterneti
- **NIST** - Ulusal Standartlar ve Teknoloji Enstitüsü
- **FIPS** - Federal Bilgi İşleme Standardı
- **SHA** - Güvenli Özetleme Algoritmaları
- **SHAKE** - Genişletilebilir Çıktı Fonksiyonları
- **TSS** - Çok Taraflı İmzalama Algoritması
- **DSA** - Dijital İmza Algoritması
- **ZK** - Sıfır Kanıt
- **TRNG** - Rastgele Sayı Üreteçleri
- **RBAC** - Rol Tabanlı Erişim Kontrolü
- **DeFi** - Merkeziyetsiz Finans
- **RWA** - Gerçek Dünya Varlıklarının Tokenizasyonu
- **ETF** - Borsa Yatırım Fonu
- **CBDC** - Merkez Bankası Dijital Para Birimi
- **DLT** - Dağıtık Defter Teknolojisi
- **IMF** - Uluslararası Para Fonu
- **FATF** - Mali Eylem Görev Gücü
- **IOSCO** - Uluslararası Menkul Kıymet Komisyonları Örgütü
- **TradFi** - Geleneksel Finans
- **SPK** - Sermaye Piyasası Kurulu
- **MASAK** - Mali Suçları Araştırma Kurulu
- **BDDK** - Bankacılık Düzenleme ve Denetleme Kurumu
- **SerPK** - Sermaye Piyasası Kanunu
- **MiCA** - Avrupa Birliği Kripto Varlık Mevzuatı
- **KVHS** - Kripto Varlık Hizmet Sağlayıcı
- **FINMA** - İsviçre Finansal Piyasalar Denetleme Kurumu
- **FCA** - Finansal Yürütme Kurulu
- **BaFin** - Alman Bankacılık Düzenleme ve Denetleme Kurumu
- **KWG** - Alman Bankacılık Yasası
- **FIU** - Alman Mali İstihbarat Birimi
- **VARA** - Virtual Assets Regulation Authority, Dubai Sanal Varlık Düzenleme Kurumu
- **ICO** - İlk Token Arzı
- **SEC** - Securities and Exchange Commission, ABD Menkul Kıymetler ve Borsa Komisyonu
- **CFTC** - ABD Emtia Vadeli İşlemler Komisyonu
- **SSS** - Shamir'in Giz Paylaşımı
- **DDoS** - Hizmet Reddi
- **Pen-Test** - Sızma Testi
- **MFA** - Çok Faktörlü Doğrulama
- **SAR** - Şüpheli Aktivite Raporlama
- **STR** - Şüpheli İşlem Raporlama
- **TÜBİTAK** - Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
- **SOC** - Güvenlik Operasyon Merkezi
- **ISAE** - Uluslararası Güvence Taahhütleri Standartları
- **ISO** - Uuslararası Standardizasyon Kuruluşu
- **CCSS**- Ortak Çekirdek Devlet Standartları
- **PoR** - Rezerv Kanıtı
- **PoL** - Yükümlülük Kanıtı
- **AUC** - Saklama Altındaki Varlıklar
- **ML** - Makine Öğrenimi
- **AI** - Yapay Zeka
- **DAO** - Merkeziyetsiz Otonom Organizasyonlar
- **RegTech** - Düzenleyici Teknoloji

İÇİNDEKİLER

A. SAKLAMA KAVRAM VE TEKNOLOJİLERİ

Saklama Kavramı

Saklama hizmetleri, yatırımcıların varlıklarını güvenli bir şekilde koruyarak finansal sistemin güvenliğini ve bütünlüğünü sağlamaktadır. Yatırımcılara, varlıklarının profesyonelce yönetilmesi ile hem erişilebilirlik hem de likidite sunulmaktadır. Ayrıca, düzenleyici gerekliliklere uyum sağlanarak yatırımcıların yasal çerçevede korunması temin edilmekte ve süreçlerin şeffaf bir şekilde yürütülmesi garanti edilmektedir. Ülkemizde, kripto varlıklar için yasal düzenlemelerin hız kazandığı bir dönemde, Sermaye Piyasası Kanunu'nda Değişiklik Yapılmasına Dair 7518 sayılı Kanun'un Resmî Gazete'de yayımlanarak yürürlüğe girmesiyle birlikte, kripto varlıklara yönelik hukuki çerçeve de belirginleşmiştir. Bu düzenleme, yatırımcıların kripto varlıklarının korunmasına yönelik hukuki adımları güçlendirmekte, kripto varlıkların da artık geleneksel varlıklar gibi yasal güvenceye tabi olmasını sağlamaktadır. Günümüzde gerek kripto varlıklar gerekse geleneksel dijital varlıkların artan önemi ile birlikte saklama hizmetlerinin rolü de giderek daha kritik bir hale gelmiştir. Saklama hizmetleri, yalnızca varlık güvenliğini sağlamakla kalmayıp, aynı zamanda gelişmiş altyapılar ve teknolojilerle yatırımcıların risklerini minimize ederek, uzun vadeli sermaye büyüme potansiyellerini de desteklemektedir. Dijital varlıkların benimsenmesi ve kurumsal düzeydeki talebin artmasıyla birlikte, saklama hizmetlerinin profesyonellik, ölçeklenebilirlik ve güvenlik gereklilikleri de önemli ölçüde artmıştır.

Geleneksel Finansta Saklama

Geleneksel finansal sistemlerde saklama hizmetleri, yatırımcıların menkul kıymetler, nakit ve diğer finansal varlıklarını güvenli bir şekilde muhafaza etmelerini ve yönetmelerini sağlayan kritik bir hizmettir.

Bu hizmetler, banka, yatırım firmaları veya bağımsız saklama kuruluşları tarafından sunularak yatırımcıların varlıklarını kaydetme, takas ve mutabakat işlemlerini yönetme, temettü ve faiz ödemelerinin yapılmasını sağlama gibi önemli fonksiyonları içerir. Bu çerçevede Türkiye'de, Takasbank saklama ve takas hizmetlerinde merkezi bir rol oynamaktadır. Takasbank, Türkiye'deki menkul kıymetlerin ve vadeli işlem ve opsiyon sözleşmelerinin takasının gerçekleştirilmesi amacıyla kurulmuş önemli bir takas ve saklama kuruluşudur ve Türkiye'deki sermaye piyasalarının gelişimine katkıda bulunarak, finansal işlemlerin güvenli ve etkin bir şekilde yürütülmesine olanak tanır. Takasbank, hisse senetleri, tahviller, devlet tahvilleri, özel sektör tahvilleri, repo ve ters repo işlemleri, vadeli işlem ve opsiyon sözleşmeleri gibi birçok farklı finansal aracın takasını güvenle gerçekleştirir. Bu takas işlemleri, alıcı ve satıcı taraflar arasında güvenli bir köprü kurularak gerçekleşir ve finansal sistemin istikrarına katkı sağlar. Takasbank, aynı zamanda menkul kıymetlerin saklanması hizmetini de sunarak bu kıymetlerin fiziksel olarak korunmasını ve transfer edilmesini sağlar. Günümüzde bu işlemler, modern teknoloji sayesinde elektronik ortamda yapılmakta ve yatırımcıların menkul kıymetleri güvenle saklanmaktadır.

Saklama ve takas hizmetlerinin işleyişi, yatırımcıların sermaye piyasalarında güvenli ve verimli bir şekilde işlem yapmalarına olanak tanır. Bu hizmetler, yatırımcıların menkul kıymetlerini güvence altına almakla kalmaz, aynı zamanda işlem süreçlerini kolaylaştırarak piyasadaki likiditeyi artırır. Takasbank gibi kurumlar, menkul kıymetlerin saklanmasını ve transferini sağlarken, yatırımcılar için operasyonel yükü azaltır ve finansal sistemin güvenilirliğini artırır.

Saklama Hizmetlerinin Fonksiyonları

1. Varlıkların Kaydı ve Takibi:
Saklama kuruluşları, yatırımcıların portföylerindeki tüm varlıkları kaydeder ve bunların güncel değerlerini takip eder. Menkul kıymetlerin ve diğer finansal varlıkların kaydı, yatırımcıların mülkiyet haklarını güvence altına alır. Ayrıca, varlıkların sahipliği ile ilgili herhangi bir uyuşmazlık durumunda bu kayıtlar yasal dayanak olarak kullanılabilir. Yatırımcıların portföylerinde bulunan menkul kıymetler, nakit gibi varlıklar sürekli olarak güncellenir ve bu varlıkların değerlemesi yapılır.

2. Takas ve Mutabakat İşlemleri:
Saklama hizmetleri, varlıkların takas işlemlerinin sorunsuz bir şekilde gerçekleştirilmesini sağlar. Menkul kıymetler veya nakit transferleri, belirlenen kurallar çerçevesinde bir takas sistemi üzerinden yürütülür. Örneğin, hisse senedi alım satımında, takas süreci boyunca saklama hizmet sağlayıcıları alıcı ve satıcı arasında güvenli bir köprü görevi görerek, işlemin tamamlanmasını sağlarlar. Aynı şekilde, mutabakat işlemleri de saklama hizmet sağlayıcıları tarafından gerçekleştirilir; bu da tarafların anlaşmaya varması ve işlemlerin doğrulanması anlamına gelir. Bu süreçler, finansal sistemdeki likiditeyi artırır ve piyasa katılımcıları arasında güven sağlar.

3. Temettü ve Faiz Ödemeleri:
Saklama kuruluşları, yatırımcıların menkul kıymetlerinden elde ettikleri temettü ve faiz ödemelerini düzenli olarak takip eder ve yatırımcıların hesaplarına aktarır. Bu hizmet, yatırımcıların pasif gelirlerini sorunsuz bir şekilde almasını sağlar ve bu ödemelerin zamanında yapılmasını garanti eder. Özellikle hisse senedi sahipleri için temettü ödemeleri, tahvil sahipleri içinse faiz ödemeleri kritik bir öneme sahiptir. Saklama hizmet sağlayıcıları, bu gelirlerin hesaplara doğru bir şekilde ve zamanında geçmesini sağladıkları için yatırımcıların operasyonel yükünü hafifletir.

4. Hesap Yönetimi ve Raporlama:
Saklama hizmeti sağlayıcıları, yatırımcıların varlıklarını izleyerek detaylı hesap yönetimi ve raporlama hizmetleri sunar. Bu raporlar, yatırımcılara portföylerindeki değişiklikleri, kazançları, temettü ve faiz ödemelerini düzenli olarak gösterir. Raporlama hizmetleri, yatırımcıların portföy yönetim kararlarını daha sağlıklı bir şekilde almasına yardımcı olur. Yatırımcılar, bu raporlar sayesinde hangi varlıklardan ne kadar kazanç elde ettiklerini ve hangi varlıklarının değer kaybettiğini görebilirler.

Geleneksel Saklama Hizmetlerinin Sağlayıcıları

Geleneksel finansal sistemlerde saklama hizmetleri, genellikle üç ana kuruluş tarafından sağlanır:

1. Bankalar:
Bankalar, yatırımcıların nakit ve menkul kıymetlerini güvenli bir şekilde saklamak için kapsamlı altyapılar sunarlar. Büyük bankalar, ulusal ve uluslararası piyasalarda faaliyet gösteren yatırımcılar için geniş çapta saklama hizmetleri sağlarlar. Bankalar, müşterilerine sundukları saklama hizmetleri ile aynı zamanda güvenli bir finansal ortamın oluşmasına katkı sağlarlar.

2. Yatırım Firmaları:
Yatırım firmaları, özellikle büyük yatırım fonları ve varlık yönetim şirketleri için saklama hizmetleri sunar. Bu firmalar, yatırımcıların portföylerini yönetme sürecinde varlıkları güvenli bir şekilde saklar ve takas işlemlerini gerçekleştirirler. Yatırım firmaları, aynı zamanda yatırımcılara çeşitli finansal analizler sunarak portföy yönetimi konusunda destek olurlar.

3. Bağımsız Saklama Kuruluşları:
Bağımsız saklama kuruluşları, bankalardan veya yatırım firmalarından bağımsız olarak hizmet sunan ve sadece saklama hizmeti veren özel şirketlerdir.

Bu kuruluşlar, yatırımcılar için tarafsızlık ve bağımsızlık sağlar. Bağımsız saklama kuruluşları, genellikle büyük fon yöneticileri veya uluslararası yatırımcılar tarafından tercih edilir, çünkü bu kuruluşlar menkul kıymetlerin güvenli bir şekilde saklanmasını sağlar ve işlemleri şeffaf bir şekilde yönetir.

Kripto Varlık Sektöründe Saklama

Kripto varlık sektöründe saklama, kripto varlıkların güvenli bir şekilde muhafaza edilmesini ve yönetilmesini sağlayan hizmetlerdir. Bu hizmetler, gizli anahtarların güvenli saklanmasını, varlıkların kaydi olarak izlenmesini, transfer işlemlerinin güvenli bir şekilde gerçekleştirilmesini ve yatırımcıların varlıklarına hızlı ve kolay erişim sağlamasını içerir. Kripto saklama hizmetleri, siber güvenlik önlemleri ve çoklu imza teknolojileri gibi yöntemlerle dijital varlıkların kaybolma veya çalınma riskini minimize etmeyi amaçlar. Aynı geleneksel finansta olduğu gibi, düzenleyici gerekliliklere uyum sağlayarak yatırımcılara yasal güvence ve şeffaflık sunar. Kripto varlık sektörü hızla büyüme devam ederken, bu dijital varlıkların güvenli saklanması ve yönetimi kritik bir öneme sahiptir. Kripto varlık saklama hizmetleri, özellikle büyük ölçekli yatırımcılar ve kurumlar için, varlıklarının güvenliğini sağlamak ve siber tehditlere karşı korunmalarını temin etmek adına vazgeçilmezdir. Kripto varlıkların korunması, dijital çağın en büyük güvenlik zorluklarından biridir. Bu zorluk, özellikle kripto paraların geriye dönüşü olmayan işlemlere dayalı olmasıyla daha da önem kazanır. Örneğin, bir gizli anahtarın kaybolması veya çalınması durumunda, geri dönüşü olmayan şekilde varlıkların kaybına neden olabilir.

Saklama Hizmetinin Önemi ve Faydaları

Saklama hizmetleri hem geleneksel finansal varlıklar hem de kripto varlıklar için güvenlik, likidite ve profesyonel yönetim sağlayarak yatırımcılar için kritik bir rol oynamaktadır. Varlıkların çalınma, kaybolma veya zarar görme riskini minimize eden bu hizmetler, yatırımcıların varlıklarını güvenli bir ortamda muhafaza etmelerini temin etmektedir. Dijital varlıkların yaygınlaşmasıyla birlikte, saklama hizmetlerinin önemi ve kapsamı daha da artmakta, duyurulmaya başlanan düzenlemeler ile birlikte belirli güvenlik standartlarında geliştirilmekte ve yatırımcıların varlıklarını profesyonelce yönetmelerine olanak tanımaktadır. Kripto varlık saklama hizmetleri, dijital varlıkların güvenli bir ortamda saklanmasını sağlayarak, yatırımcıların varlıklarının kaybolma veya çalınma riskini azaltmayı amaçlar. Soğuk cüzdanlar (cold wallets) gibi internete bağlı olmayan cihazlarda saklama, varlıkların çevrimiçi saldırılara maruz kalmasını engellerken, sıcak cüzdanlar (hot wallets) hızlı işlem yapabilme avantajı sağlar. Bu iki saklama yöntemi, risk ve hız dengesine göre kurumlar ve bireysel kullanıcılar tarafından farklı senaryolarda kullanılmaktadır.

Kripto varlık saklama hizmetlerinin en temel bileşenlerinden biri, gizli anahtarların güvenli saklanmasıdır. Gizli anahtar, bir yatırımcının cüzdanına erişimini sağlayan ve varlıklar üzerinde tam kontrol sunan dijital anahtardır. Bu anahtarın ele geçirilmesi durumunda, kötü niyetli kişiler tarafından varlıkların transferi veya çalınması söz konusu olabilir. Saklama hizmetleri, gizli anahtarların güvenliğini sağlamak için ileri düzey şifreleme teknolojileri, çoklu imza (Multisig) ve çok partili hesaplama (MPC) gibi yöntemler kullanır. Multisig, bir işlemin onaylanması için birden fazla anahtarın gerektiği bir yapı sunarken, MPC, gizli anahtarın birden fazla kişi arasında dağıtılmasını ve böylece tek bir kişinin anahtarı ele geçirmesinin önlenmesini sağlar.

Kripto saklama hizmetlerinin düzenleyici çerçevelere uyum sağlaması, yatırımcıların güvenli bir ortamda varlıklarını korumalarına yardımcı olur. Bu uyum, yatırımcılar için sadece güvenlik sağlamaz, aynı zamanda şeffaflık ve sorumluluk yükümlülüklerini de beraberinde getirir. KYC (Know Your Customer) ve AML (Anti-Money Laundering) gibi standartlar, kripto varlık saklama hizmeti sağlayıcılarının müşteri bilgilerini doğrulamasını ve yasadışı faaliyetlere karşı önlem almasını zorunlu kılar.

Bununla birlikte, kripto varlık saklama hizmetlerinin siber güvenlik önlemleri de yasal gerekliliklerin bir parçası olarak büyük önem taşımaktadır. Yatırımcıların dijital varlıklarının çalınması veya kaybolması durumunda, saklama hizmeti sağlayıcılarının sunduğu sigorta poliçeleri ve geri alma mekanizmaları, yatırımcıların kayıplarını telafi etmeye yardımcı olabilir.

Saklama için Gerekli Kriptografik Mekanizmalar

Günümüzde dijital verilerin güvenliği, bilgi işlem dünyasında en kritik konulardan biridir. Bilginin güvenli iletimi, saklanması ve yetkisiz erişimlerden korunması için çeşitli kriptografik mekanizmalar kullanılmaktadır. Kripto varlıkların saklanmasında, dijital varlıkların güvenli bir şekilde muhafaza edilmesi, izlenmesi ve yönetilmesi için kriptografi olmazsa olmazdır. Bu bölümde, modern dijital dünyada en çok kullanılan ve kritik rol oynayan kriptografik mekanizmaları ele alınacaktır.

Açık Anahtarlı (Asimetrik) Şifreleme

Günümüzde, verilerin güvenli iletimi, saklanması ve gizliliğinin sağlanması amacıyla birçok farklı algoritmaya sahip şifreleme yöntemi kullanılmaktadır. Bu şifreleme yöntemlerini simetrik ve asimetrik (açık anahtarlı) olarak ikiye ayırabiliriz.

Simetrik şifrelemede, aynı anahtarın hem şifreleme hem de şifre çözme işlemleri için kullanıldığı bir yöntemdir ve bu yapısı bazı avantaj ve dezavantajlar barındırır. Hızlı ve verimli çalışması ile büyük veri setleri şifrelemeleri için avantajlı olabilecekken, şifreleme ve çözme için aynı anahtar kullanılması güvenlik zafiyeti oluşturabilir. Yetkisiz kişiler veya sistemler, alıcı ya da göndericinin anahtarını ele geçirirse güvenlik açığı oluşabilir. Bu durumda, şifrelenmiş veriler tehlikeye girebilir. Asimetrik şifreleme, simetrik şifrelemenin aksine iki farklı anahtar kullanır. Anahtarlardan biri veriyi şifrelemek için kullanılan açık anahtar, diğeri şifreyi çözmek için kullanılan gizli anahtardır. Bu şifreleme yöntemi daha fazla güvenlik sağlar ve açık anahtar dağıtılabilirken, gizli anahtar yalnızca sahibinde kalır. Asimetrik şifreleme, dijital imzalar sayesinde gönderenin kimliğini doğrulamaya da olanak tanır, böylece sadece yetkili kişilerin veriye erişimi sağlanır.

Asimetrik şifreleme, günümüzün dijital iletişiminde gizlilik ve güvenlik sağlamak için temel bir teknolojidir. Bu şifreleme yöntemi, kullanıcıların gizli bilgilerini güvenli bir şekilde paylaşmalarını sağlar ve bu süreci gerçekleştirmek için iki anahtar kullanır: bir açık anahtar ve bir gizli anahtar.

Açık ve Gizli Anahtarlar

Açık anahtarlı şifreleme sistemleri, iki farklı anahtarın birbirini tamamladığı bir yapıya dayanır. Bu anahtarlar matematiksel olarak birbirine bağlıdır, ancak bir anahtardan diğerini tahmin etmek pratikte imkânsızdır. Bu anahtarlardan biri (açık anahtar) herkesle paylaşılırken, diğeri (gizli anahtar) gizli tutulur.

• Açık Anahtar: Herhangi bir kişi tarafından kullanılabilir ve bu anahtar ile şifrelenen mesajlar sadece ilgili gizli anahtar tarafından çözülebilir.

Bu durum, bir kişinin güvenli bir şekilde mesaj almasına olanak tanır; zira gönderici, alıcının açık anahtarını kullanarak mesajı şifreler, ancak sadece alıcı bu mesajı çözebilir.

• Gizli anahtar: Bu anahtar ise sadece sahibine aittir ve başkalarıyla paylaşılmaz. Bu anahtar, açık anahtar ile şifrelenmiş mesajları çözmek için kullanılır. Eğer biri bu gizli anahtarı ele geçirirse, şifreli mesajlara erişim sağlayabilir, bu nedenle bu anahtarın güvenliği kritik öneme sahiptir.

Açık Şifrelemenin Çalışma Prensibi

Açık anahtarlı şifreleme, güvenliği sağlamak için karmaşık matematiksel algoritmalar kullanır. Bu sistemin temel çalışma prensibi şu şekildedir:

1. Anahtar Çifti Üretimi: Kullanıcı, bir açık anahtar ve bir gizli anahtar çifti oluşturur. Açık anahtar, herkesle paylaşılabilir; gizli anahtar ise güvenli bir şekilde saklanır.

2. Şifreleme: Gönderen, alıcının açık anahtarını kullanarak bir mesajı şifreler. Bu işlem, mesajı alıcı dışındaki herkes için anlaşılmaz hale getirir.

3. Çözme: Alıcı, gizli anahtarını kullanarak şifreli mesajı çözer ve orijinal içeriğe erişir.

Bu süreç, güvenli bir şekilde bilgi paylaşımı sağlar, çünkü sadece belirli bir gizli anahtara sahip kişi şifrelenmiş mesajları çözebilir.

Kullanım Alanları

Açık anahtarlı şifreleme, birçok farklı alanda kullanılmaktadır:

• E-posta Güvenliği: PGP (Pretty Good Privacy) gibi sistemler, e-posta içeriklerinin şifrelenmesini sağlar.

• SSL/TLS Protokolleri: İnternet üzerindeki güvenli iletişimi sağlar, web sitelerinin HTTPS kullanarak güvenli bağlantılar sunmasına olanak tanır.

• Dijital İmzalar: Verinin bütünlüğünü ve kaynağını doğrulamak için kullanılır.

Açık anahtarlı şifreleme, dijital dünyada güvenliği sağlamak için kritik bir araçtır. İki anahtar sistemi sayesinde, kullanıcılar güvenli bir şekilde bilgi paylaşabilir ve kimlik doğrulaması yapabilir. Bu şifreleme yöntemi, internetin güvenliğini sağlamada temel bir rol oynar ve günümüz dijital dünyasında vazgeçilmezdir.

Eliptik Eğriler

Eliptik Eğri Kriptografisi (ECC), günümüzün dijital güvenlik ihtiyaçlarına cevap veren ileri düzey bir kriptografi yöntemidir. ECC, açık anahtarlı kriptografi sistemlerinde kullanılan eliptik eğrilerin matematiksel yapısını temel alır. Geleneksel RSA gibi sistemlere kıyasla, daha küçük anahtar boyutlarıyla aynı güvenlik seviyesini sunar, bu da onu özellikle sınırlı işlem gücüne sahip cihazlar için cazip bir seçenek haline getirir.

ECC'nin Matematiksel Temelleri

Eliptik eğriler, $y^2=x^3+ax+b$ şeklinde tanımlanır. Bu denklemin çözümü, ?2=?3+??+? kriptografide güçlü bir zorluk oluşturan Eliptik Eğri Ayrık Logaritma Problemi'ne (ECDLP) dayanır. ECC, bu problemin çözülmesinin zorluğu üzerine kurulmuştur. Bu zorluk, ECC'nin sunduğu yüksek güvenliğin temelini oluşturur, çünkü büyük anahtar uzunluklarına gerek kalmadan güçlü güvenlik sağlar.

ECC'nin Avantajları

Eliptik Eğri Kriptografisi (ECC), kriptografide sunduğu birçok avantajla öne çıkmaktadır. En büyük avantajlarından biri, aynı güvenlik seviyesini sağlamak için daha küçük anahtar boyutlarına ihtiyaç duymasıdır. Örneğin, 256 bitlik bir ECC anahtarı, 3072 bitlik bir RSA anahtarına eşdeğer güvenlik sağlar. Bu özellik, ECC'yi özellikle mobil cihazlar ve sınırlı işlem gücü veya enerji kapasitesine sahip diğer sistemler için ideal bir kriptografik çözüm haline getirir.

Özetle, ECC aşağıdaki özelliklere sahiptir:

1. Daha Verimli Hesaplama: Daha küçük anahtar boyutları sayesinde ECC hem hesaplama süresi hem de bellek kullanımı açısından daha verimlidir. Bu, düşük enerji tüketimi ve daha hızlı işlem süreleri sağlar.

2. Bant Genişliği ve Depolama Tasarrufu: ECC, daha küçük anahtarlar ve dijital imzalar kullanarak veri iletiminde bant genişliği tasarrufu sağlar. Aynı zamanda depolama gereksinimlerini de minimize eder.

3. Yüksek Güvenlik: Daha kısa anahtar boyutlarıyla, RSA ve DSA gibi klasik algoritmalara kıyasla aynı veya daha yüksek seviyede güvenlik sunar. Eliptik Eğri Ayrık Logaritma Problemi (ECDLP), büyük anahtar uzunluklarına ihtiyaç duyulmadan çözülmesi çok zor bir problem olarak kabul edilir.

4. Düşük Güç Tüketimi: Küçük anahtarlar ve verimli hesaplama yapısı, ECC'yi düşük güç tüketimi gerektiren cihazlar için mükemmel bir tercih yapar. Özellikle IoT uygulamalarında ve mobil cihazlarda batarya ömrünü uzatmak için yaygın olarak kullanılır.

Uygulama Alanları ve Standartlar

ECC, çeşitli kriptografik işlemler ve protokoller için geniş bir uygulama yelpazesi sunar. Dijital imzalar (örneğin, ECDSA), anahtar değişimi (örneğin, ECDH) ve veri şifreleme gibi temel güvenlik işlemlerinde etkin bir şekilde kullanılır. Bu uygulama alanları, ECC'nin sağladığı yüksek güvenlik ve düşük kaynak kullanımı sayesinde birçok sektörde tercih edilmesini sağlamaktadır.

• Eliptik Eğri Temelli Dijital İmzalar (ECDSA/EdDSA):

Eliptik Eğri temelli dijital imzalar, dijital belgelerin kimliğini doğrulamak ve bütünlüğünü sağlamak için kullanılır. ECDSA, özellikle çevrimiçi işlemler, e-posta güvenliği ve blokzincir gibi alanlarda yaygın olarak kullanılır.

ECC'nin düşük hesaplama ve bellek maliyetleri, günümüzde başta Bitcoin olmak üzere kripto para cüzdanlarından güvenli iletişim protokollerine kadar pek çok alanda tercih edilmesine yol açmıştır.

• Eliptik Eğri Diffie-Hellman (ECDH) Anahtar Değişimi:

İki tarafın güvenli bir şekilde ortak bir anahtar oluşturmasını sağlar. ECDH, açık anahtarlı şifreleme ve SSL/TLS gibi güvenli iletişim protokollerinde tercih edilen bir anahtar değişim yöntemidir.

• Veri Şifreleme:

ECC, düşük işlem gücüne sahip cihazlarda bile verimli veri şifreleme işlemleri sunar. Özellikle mobil cihazlar ve IoT sistemleri gibi sınırlı kaynaklara sahip ortamlar için güçlü bir şifreleme çözümüdür.

ECC'nin yaygın kullanımıyla birlikte, güvenli ve uyumlu sistemler oluşturmak için çeşitli standartlar geliştirilmiştir. NIST, ECC tabanlı algoritmalar için birçok önemli standardı tanımlamıştır:

• FIPS 186-4:

Eliptik eğri tabanlı dijital imza algoritmaları (ECDSA) için bir standarttır. Bu standart, dijital imzaların güvenli bir şekilde oluşturulması ve doğrulanması için gereksinimleri belirler.

• SP 800-56A/B:

Bu standart, anahtar değişim protokollerine ilişkin kılavuzlar sunar. SP 800-56A, eliptik eğri tabanlı anahtar değişim protokollerini (ECDH) tanımlarken, SP 800-56B ise ECC'nin diğer açık anahtarlı şifreleme uygulamaları için kurallar koyar.

Güvenlik ve Kriptografik Dayanıklılık

ECC, yüksek güvenlik ve verimliliği bir araya getirerek modern dijital güvenlik dünyasında önemli bir yer edinmiştir. Ancak ECC'nin güvenliği, büyük ölçüde kullanılan eliptik eğrinin doğru seçilmesine ve bu eğrilerin doğru bir şekilde uygulanmasına bağlıdır. Eliptik eğrilerde yapılacak hatalar veya zayıf eğri seçimleri, ECC'nin güvenliğini tehlikeye atabilir. Özellikle eliptik eğrilerin güvenliğini sağlamak için seçilen eğrinin matematiksel özelliklerinin dikkatli bir şekilde incelenmesi ve uygulamanın doğru yapılması gerekir.

Özet (Hash) Fonksiyonları

Özet (hash) fonksiyonları, modern kriptografinin en temel yapı taşlarından biridir ve birçok kritik güvenlik uygulamasında kullanılır. Veri bütünlüğünün sağlanması, dijital imzaların oluşturulması ve parola saklama gibi alanlarda sıkça başvurulan özet fonksiyonları, aynı zamanda kripto varlıkların güvenliğini sağlayan cüzdan altyapılarında da önemli bir rol oynar. Bu fonksiyonlar, girdiyi sabit boyutlu bir özet değerine dönüştüren matematiksel fonksiyonlardır. Örneğin, bir özet fonksiyonuna ister birkaç harf isterse uzun bir metin girilsin, çıktı olarak sabit uzunlukta bir değer üretilir. Bu süreçte özet fonksiyonlarının belirli güvenlik özelliklerini taşıması beklenir. Kripto cüzdanları özet fonksiyonları gibi çeşitli kriptografik mekanizmalardan faydalanır.

Hash Fonksiyonlarının Temel Özellikleri

Bir özet fonksiyonu, belirli güvenlik özelliklerini karşılamalıdır. Bunlar, kriptografik dayanıklılık ve veri bütünlüğü için kritik öneme sahiptir:

1. Pre-image Direnci: Belirli bir özet değerine karşılık gelen girdiyi bulmak, yani tersine mühendislik yapmak zor olmalıdır. Bu özellik, verinin şifrelenmiş halinden orijinal veriye ulaşmayı zorlaştırır.

2. İkinci Pre-image Direnci: Verilen bir girdiye karşılık, aynı özet değerine sahip başka bir girdi bulmak çok zor olmalıdır. Bu, verinin değiştirilerek sahte bir özet değeri ile manipüle edilmesini engeller.

3. Çarpışma Direnci: Aynı özet değerine sahip iki farklı girdiyi bulmanın neredeyse imkânsız olması gerekmektedir. Hash fonksiyonunda çarpışma yaşanması, güvenlik açığı oluşturabileceğinden, bu özellik kritik öneme sahiptir.

Bu özellikler, özet fonksiyonlarını güvenilir kılarken, kripto cüzdanlarının da güvenli olmasını sağlar. Kripto cüzdanlarında kullanıcılar, işlemlerini doğrulamak için dijital imzalar oluşturur ve bu süreç özet fonksiyonlarına dayanır. Ayrıca, cüzdanların gizli anahtarları, güvenli bir şekilde saklanmak için özet fonksiyonları ile korunur.

Kripto Cüzdanlarda Hash Fonksiyonlarının Rolü

Kripto cüzdanları, özellikle Bitcoin, Ethereum ve diğer dijital varlıkların güvenli bir şekilde yönetilmesi için özet fonksiyonlarına dayalı olarak çalışır. Hash fonksiyonlarının kripto cüzdanlarındaki temel kullanım alanları şu şekilde sıralanabilir:

1. Anahtar Yönetimi: Kripto cüzdanları, kullanıcının varlıklarına erişimini sağlayan gizli anahtarları güvenli bir şekilde saklar. Bu anahtarlar, özet fonksiyonları ile işlenerek güvenli hale getirilir. Örneğin, cüzdan şifresi veya PIN kodu bir özet fonksiyonu aracılığıyla saklanır ve yalnızca doğru girdiler verildiğinde çözülür.

2. Adres Oluşturma: Kripto cüzdanlarında bir işlem yapmak veya bir varlık göndermek için oluşturulan adresler, genellikle özet fonksiyonlarına dayalı olarak üretilir.

Bitcoin ve Ethereum gibi kripto varlıklarda, bir açık anahtarı (public key) üzerinden bir özet fonksiyonu kullanılarak cüzdan adresi oluşturulur. Örneğin, Bitcoin adresleri genellikle SHA256 ve RIPEMD160 gibi özet algoritmalarıyla oluşturulur.

3. Dijital İmzalar: Kripto cüzdanlarında, kullanıcıların işlem yapabilmesi için dijital imza gereklidir. Dijital imzalar, kullanıcının işlemlerini onaylamak ve doğrulamak için özet fonksiyonları kullanılarak oluşturulur. Bir işlem, kullanıcının gizli anahtarı ile özet fonksiyonu yardımıyla imzalanır ve bu sayede işlemin doğruluğu ve kaynağı güvence altına alınır.

4. Blokzincirleri ve Veri Bütünlüğü: Hash fonksiyonları, blokzincirlerinin temelini oluşturur. Her blok, bir önceki bloğun özet değerini içerir ve bu sayede blok zincirinin bütünlüğü korunur. Bir blokta yapılan en ufak bir değişiklik, o bloktan sonra gelen tüm blokların özet değerini etkiler, bu da zincirin bozulmasına yol açar. Bu durum, özet fonksiyonlarının kripto varlıkların güvenli saklanmasında ne kadar kritik bir rol oynadığını gösterir.

Güvenlik Tehditleri ve Güncel Algoritmalar

Eski özet algoritmaları, zamanla güvenlik açıkları nedeniyle çeşitli saldırılara karşı savunmasız hale gelmiştir. Örneğin, SHA1 gibi algoritmalar, çarpışma saldırılarına karşı zayıf kalmış ve artık modern kriptografide güvenilir bir seçenek olmaktan çıkmıştır. Bu güvenlik zafiyetleri nedeniyle, günümüzde SHA256 ve SHA3 gibi daha güvenli özet algoritmaları tercih edilmektedir. SHA256, özellikle Bitcoin gibi kripto varlık cüzdanlarında kullanılan temel özet fonksiyonlarından biridir. Bitcoin blokzincirinde her blok, SHA256 ile özeti alınır ve bir önceki bloğa bağlanarak zincirin bütünlüğü korunur. Bu yapı, blokzincirlerinin güvenliğini sağlar ve işlemler üzerinde oynama yapılmasını engeller.

Daha yeni bir algoritma olan SHA3, 2015 yılında NIST tarafından standardize edilmiştir. SHA3, kriptografideki gelişen ihtiyaçlara cevap vermek amacıyla tasarlanmış olup, Keccak algoritmasının hafifçe değiştirilmiş ve optimize edilmiş bir versiyonudur. SHA3'ün en önemli yeniliklerinden biri, sünger yapısı (sponge construction) adı verilen bir teknikle veri işlemesidir. Bu yapı, verinin sünger gibi "emilmesi" ve ardından özetin "sıkıştırılması" yoluyla çalışır, bu da SHA3'ü bazı saldırı türlerine karşı daha dirençli hale getirir. SHA3, SHA2 ile uyumlu bir güvenlik seviyesine sahiptir ancak yapısal olarak farklıdır, bu da belirli saldırılara karşı ek koruma sağlar.

SHA3, özellikle güvenli veri saklama, dijital imza ve kimlik doğrulama gibi çeşitli uygulamalarda kullanılır. Ayrıca, SHA3'ten türetilen SHAKE (Extendable-Output Functions) gibi fonksiyonlar, esnek çıktı uzunluklarıyla belirli uygulama ihtiyaçlarını karşılayabilir. SHAKE gibi genişletilebilir çıktı fonksiyonları, ihtiyaçlara göre özet değerlerinin uzunluğunu ayarlama imkânı sunar, bu da onu çok çeşitli kriptografik uygulamalarda daha esnek hale getirir.

Dijital İmzalama Algoritmaları

Dijital imzalama algoritmaları, bir mesajın bütünlüğünü ve kaynağını doğrulamak için kullanılan kriptografik protokollerdir. Bu algoritmalar, matematiksel temellere dayalı olup, bir verinin doğruluğunu kanıtlamada ve alıcıya güvenlik sağlamada kritik rol oynar. Bu bölümde, RSA, DSA, ECDSA, EdDSA, Schnorr ve Eşik İmzalama (Threshold Signature Scheme (TSS)) algoritmaları incelenecektir.

RSA İmza Algoritması

RSA dijital imza algoritması, büyük asal çarpanlara ayırma probleminin zorluğuna dayanır.

Anahtar Üretimi: RSA algoritmasında, iki büyük asal sayı p ve q seçilir ve bunların çarpımı $N = p.q$ hesaplanır. Ardından, Euler totient fonksiyonu $\phi(N)= (p-1)(q-1)$ hesaplanır. Şifreleme anahtarı e, $1 < e < \phi N$ olacak şekilde seçilir ve e ile $\phi(N)$ aralarında asaldır. Gizli anahtar d, $e \cdot d=1 \pmod{\phi(N)}$ eşitliğini sağlayacak şekilde hesaplanır.

İmzalama: Mesaj m, özet fonksiyonu ile özetlenir, $H(m)$, ve imza şu şekilde oluşturulur:

$$s = H(m)^d \mod N$$

Doğrulama: Alıcı, imzayı doğrulamak için şu denklemi kullanır:

$$H(m) \stackrel{?}{=} s^e \mod N$$

Eğer eşitlik sağlanırsa, imza geçerli kabul edilir.

DSA (Digital Signature Algorithm)

DSA, ElGamal imza şemasına dayanır ve ayrık logaritma probleminin zorluğuna bağlıdır.

Anahtar Üretimi: Bir asal p ve bir asal çarpan q ($bu, q|p-1$) seçilir. Bir g sayısı, $g^q= 1 \mod p$ olacak şekilde seçilir. Kullanıcının gizli anahtarı x, $1 \leq x \leq q-1$, ve açık anahtarı $y = g^x \mod p$ olarak belirlenir.

İmzalama: Mesaj m, özet fonksiyonu $H(m)$ ile özetlenir. Bir rastgele k, $1 \leq k \leq q-1$, seçilir ve imza şu şekilde oluşturulur:

$$r = (g^k \mod p) \mod q$$

$$s = k^{-1} (H(m)+ x \cdot r \mod q$$

İmza çifti (r, s)'dir.

Doğrulama: Alıcı, r ve s'yi doğrulamak için şu denklemleri kullanır:

$$w = s^{-1} \mod q$$
$$u_1 = H(m) \cdot w \mod q$$
$$u_2 = r \cdot w \mod q$$
$$v = (g^{u1} \cdot y^{u2} \mod p) \mod q$$

Eğer $v = r$, imza geçerli kabul edilir.

ECDSA

ECDSA, eliptik eğriler üzerinde ayrık logaritma probleminin zorluğuna dayanır.

Anahtar Üretimi: Eliptik eğri E üzerinde, bir G noktası seçilir ve kullanıcının gizli anahtarı d olur. Açık anahtar, $Q = dG$'dir.

İmzalama: Mesaj m, özet fonksiyonu $H(m)$ ile özetlenir. Rastgele bir k seçilir ve $kG = (r, \_)$ hesaplanır. İmza şu şekilde oluşturulur:

$$s = k^{-1}(H(m) + dr) \mod n$$

İmza çiftidir (r, s).

Doğrulama: Alıcı, r ve s'yi doğrulamak için şu adımları izler:

$$w = s^{-1} \mod n$$

$$u_1 = H(m) \cdot w \mod n$$

$$u_2 = r \cdot w \mod n$$

$$(x_1, y_1) = u_1 G + u_2 Q$$

Eğer $x_1 = r \mod n$, imza geçerlidir.

EdDSA (Edwards-Curve Dijital İmza Algoritması)

EdDSA, Edwards eğrileri üzerinde çalışır ve performans açısından optimize edilmiştir.

Anahtar Üretimi: Bir gizli anahtar a, ve buna karşılık gelen $A = aB$ hesaplanır.

İmzalama: Mesaj m, bir özet fonksiyonu $H(m)$ ile özetlenir. Rastgele bir r değeri, $r = H(a \| m)$ olarak belirlenir ve $R = rB$ hesaplanır. İmza şu şekilde oluşturulur:

$$s = r + H(R||A||m) \cdot a \bmod n$$

İmza çifti (R, s)'dir.

Doğrulama: Alıcı, şu denklemi kullanarak imzayı doğrular:

$$sB = R + H(R||A||m) \cdot A$$

Schnorr İmza Algoritması

Schnorr algoritması, ayrık logaritma probleminin zorluğuna dayanır ve imza boyutları daha küçüktür.

Anahtar Üretimi: Gizli anahtar x, ve açık anahtar $y = g^x \bmod p$ olur.

İmzalama: Rastgele bir k seçilir ve $r = g^k \bmod p$ hesaplanır. Özet fonksiyonu ile:

$$e = H(m \| r)$$

ve imza şu şekilde oluşturulur:

$$s = k - xe \bmod q$$

İmza çifti (e, s)'dir.

Doğrulama: Alıcı, $r' = g^s \cdot y^e$ mod hesaplar ve şu denklemi doğrular:

$$e \stackrel{?}{=} H(m \| r')$$

Çok Taraflı İmzalama Algoritması (Threshold Signature Scheme (TSS)

TSS, n sayıda imzalayıcının imza oluşturması için bir eşik değer t'ye dayanır. t sayıda imzalayıcı, imzanın geçerli olması için iş birliği yapmalıdır.

Anahtar Üretimi: TSS, gizli anahtarı n imzalayıcı arasında bölerek, her birine bir parça dağıtır.

İmzalama: t imzalayıcı, her biri kendi gizli anahtar payını kullanarak bir parça imza ?oluşturur. Parça imzalar, Lagrange interpolasyonu ile birleştirilir ve tam bir imza üretilir.

Doğrulama: Tam imza, sistemin açık anahtarı kullanılarak doğrulanır. İmzalama işlemi, imzalayanların güvenliği için gizlilik ve dağıtık güvenlik sağlar.

Çok Taraflı Hesaplamalar (Multi-Party Computation (MPC)

MPC, dağıtık sistemlerde güvenli hesaplama yapabilmeyi mümkün kılan kriptografik bir tekniktir. MPC, bir grup katılımcının, gizli verilerini açığa çıkarmadan ortak bir hesaplama yapmasını sağlar. MPC'nin amacı, katılımcılar arasında gizlilik ihlali olmadan verilerin işlenmesi ve hesaplama sonucunun elde edilmesidir. Bu teknik, özellikle güvenli veri paylaşımı, şifreleme anahtarlarının dağıtımı ve gizli verilerin işlenmesinde kritik bir rol oynar. Siber güvenlik ve kriptografide, gizli ve hassas verilerin güvenli bir şekilde işlenebilmesi için MPC giderek önem kazanmaktadır.

MPC'nin Matematiksel Temelleri

MPC, temelde güvenilir bir üçüncü taraf olmadan verilerin güvenli bir şekilde işlenmesini sağlayan kriptografik protokoller bütünüdür.

Hesaplama süreci boyunca her bir taraf, kendi gizli girdilerini korur. Sonuçlar hesaplanırken taraflar arasında bir bilgi sızıntısı meydana gelmez.

MPC'de, hesaplamalar şu prensiplerle gerçekleştirilir:

• Gizlilik: Her bir katılımcının girdisi gizli kalır ve diğer katılımcılarla paylaşılmaz.

• Doğruluk: Hesaplama doğru bir şekilde yapılır ve tüm katılımcılar doğru sonuca ulaşır.

• Güvenilirlik: Bir veya daha fazla katılımcının kötü niyetli olmasına rağmen sistemin güvenilir şekilde sonuç üretmeye devam edebilmesi gerekir.

Bu özellikler, Shamir'in Sır Paylaşımı (Shamir's Secret Sharing) gibi yöntemler kullanılarak sağlanır.

Shamir'in Sır Paylaşımı (Shamir's Secret Sharing)

Shamir'in Sır Paylaşımı, MPC'de kullanılan temel yöntemlerden biridir ve polinomlar yardımıyla verilerin paylaşılmasına dayanır. Bu teknik, bir sırrın SSS'nin ***n*** katılımcı arasında bölünmesi ve sırrın yalnızca belirli sayıda katılımcı tarafından bir araya getirilerek geri elde edilmesine olanak tanır.

• Sırrın Paylaştırılması: SSS, bir ***f(x)*** polinomu oluşturularak ***n*** parçaya bölünür. Bu polinomun sabiti ***f(0) = S*** sırrı temsil eder. Diğer katılımcılara ***f(1), f(2),.....*** şeklinde paylar dağıtılır.

• Sırrın Geri Elde Edilmesi: En az ***t*** katılımcı bir araya geldiğinde, Lagrange interpolasyonu kullanılarak orijinal sır (SSS) yeniden elde edilebilir.

Bu yöntem sayesinde, ***t***'den az sayıda katılımcının iş birliği yapması durumunda sırrın elde edilmesi imkansızdır. Bu da MPC için yüksek bir güvenlik sağlar.

MPC'nin Uygulama Alanları

MPC, birçok farklı alanda kullanılmaktadır. Aşağıdaki alanlar, MPC'nin kriptografi dünyasında en yaygın kullanım alanlarıdır:

• Gizli Veri Analizi: Şirketler ve kuruluşlar, MPC kullanarak birbirlerinin verilerini açığa çıkarmadan ortak analizler yapabilirler. Örneğin, bankalar arasındaki işlem verilerinin gizliliğini koruyarak dolandırıcılık tespit algoritmalarının çalıştırılması.

• Anahtar Yönetimi: Kriptografik anahtarların güvenli bir şekilde oluşturulması ve paylaşılması, MPC sayesinde çok taraflı iş birlikleri ile sağlanabilir. Örneğin, Threshold Signature Scheme (TSS) gibi algoritmalar MPC kullanarak güvenli imzalama sağlar.

• Kripto Cüzdanlar: MPC, özellikle çoklu imza gerektiren ve güvenliği artırmak amacıyla birden fazla tarafın imza atmasını sağlayan MPC cüzdanları için önemli bir teknolojidir. MPC cüzdanları, tek bir gizli anahtarın hiçbir tarafça tam olarak bilinmediği, anahtarın parçalar halinde paylaşıldığı cüzdanlardır. Bu cüzdanlar, kullanıcının anahtarlarını güvence altına alırken, birden fazla tarafın iş birliği ile işlemler yapmasına olanak tanır.

Zero-Knowledge Proofs (Sıfır Bilgi İspatları)

Sıfır Bilgi İspatları (ZKP), modern kriptografinin en yenilikçi ve etkili tekniklerinden biridir. Bu yöntem, ispatlayan tarafın (prover), doğrulayıcı tarafa (verifier), bir bilginin doğru olduğunu, doğrulayıcıya hiçbir ek bilgi sızdırmadan kanıtlamasını sağlar. Bu özelliği sayesinde ZKP'ler, özellikle veri gizliliğini ve güvenliğini en üst düzeyde korumak için kritik bir araç haline gelmiştir. ZKP'ler, kimlik doğrulama sistemlerinden kripto para işlemlerine kadar geniş bir yelpazede uygulama alanı bulmaktadır.

Sıfır Bilgi İspatlarının Temel Özellikleri

ZKP'lerin güvenli ve işlevsel olabilmesi için sahip olması gereken üç temel özellik bulunmaktadır:

1. Tamlık (Completeness): Eğer ispatlanan ifade doğruysa, dürüst bir ispatlayıcı, doğrulayıcıyı bu ifadenin doğruluğuna ikna edebilir. Yani, ispatlama süreci başarılı olur ve doğrulayıcıyı tatmin eder.

2. Sağlamlık (Soundness): Eğer ispatlanan ifade yanlışsa, hiçbir sahtekâr ispatlayıcı, dürüst bir doğrulayıcıyı yanlış bir ifadenin doğru olduğuna inandıramaz. Bu, yanlış bilginin doğrulanmasını imkânsız hale getirir.

3. Sıfır Bilgi (Zero-Knowledge): İspatlayan, doğrulayıcıya ifadenin doğruluğunu kanıtlarken, ifadenin kendisi hakkında ek hiçbir bilgi vermemelidir. Bu, doğrulayıcının ifadenin doğru olduğunu öğrenmesini sağlar, ancak doğrulayıcıya başka hiçbir bilgi sızdırmaz.

Sıfır Bilgi İspatlarının Türleri

1. Etkileşimli Sıfır Bilgi İspatları (Interactive ZKPs): İspatlayan ve doğrulayıcı arasında bir etkileşim süreci gerektirir. Bu süreçte doğrulayıcı, ispatlayan kişiye çeşitli sorular sorar ve doğru cevaplar alır. En klasik örneği "Mağara Metaforu"dur, burada ispatlayan taraf mağaranın gizli bir geçidini bildiğini doğrulayıcıya ispatlamaya çalışır, ancak geçidin nerede olduğunu açıklamaz. Etkileşimli ZKPs, bazı kullanım durumlarında yüksek güvenlik sağlar, ancak merkeziyetsiz sistemlerde kullanım zorlukları çıkarabilir.

2. Etkileşimsiz Sıfır Bilgi İspatları (Non-Interactive ZKPs): İspatlayan ve doğrulayıcı arasında herhangi bir etkileşim olmadan çalışan bir ispat türüdür. İspatlayan, tek bir kanıt sunar ve doğrulayıcı bu kanıtı kullanarak sonuca ulaşır. Blokzincir uygulamaları için oldukça uygundur, çünkü merkeziyetsiz sistemlerde etkileşim olmaksızın işlem yapılmasına olanak tanır. Etkileşimsiz ZKP'ler verimlilik ve ölçeklenebilirlik açısından avantaj sağlar.

3. zkSNARK (Succinct Non-Interactive Arguments of Knowledge): zkSNARK'lar, etkileşimsiz sıfır bilgi ispatlarının en popüler ve yaygın kullanılan versiyonlarından biridir. Özellikle blokzincir teknolojisinde işlem gizliliği ve ölçeklenebilirlik sorunlarını çözmek için kullanılır. zkSNARK'lar, kısa ispatlar üretir ve hızlı bir şekilde doğrulanabilir. Bu özellikleri, ZKP'leri büyük veri setlerinde ve işlem yoğun sistemlerde oldukça etkili kılar.

4. zkSTARK (Zero-Knowledge Scalable Transparent Arguments of Knowledge): zkSTARK'lar, zkSNARK'lara benzer şekilde çalışır ancak önemli bir farkı, güvenilir kurulum (trusted setup) gerektirmemesidir. zkSTARK'lar, daha yüksek ölçeklenebilirlik ve şeffaflık sunar. Özellikle büyük veri setleri üzerinde doğrulama yaparken daha hızlı ve güvenli sonuçlar üretir.

5. Kurşun Geçirmez İspatlar (Bulletproofs): ZKP'lerin boyutlarını küçültmek ve işlem maliyetlerini azaltmak amacıyla kullanılan bir tekniktir. Bulletproofs, zkSNARK'lara kıyasla daha küçük boyutlu ispatlar üretir ve doğrulama süreçlerini hızlandırır. Bu da blokzincir sistemlerinde işlem verimliliğini artırır ve işlem boyutlarını azaltarak ağ tıkanıklığını önler.

Sıfır Bilgi İspatları, günümüzün dijital güvenlik gereksinimlerine doğrudan hitap eden bir teknoloji olarak geniş bir uygulama yelpazesi sunar:

• Kripto Para İşlemleri: ZKP'ler, kripto para işlemlerinin gizliliğini ve güvenliğini sağlamak için yaygın olarak kullanılır. Özellikle Zcash gibi gizlilik odaklı kripto para birimlerinde, kullanıcıların kimlikleri veya işlem detayları ifşa edilmeden doğrulama yapılabilir.

• Kimlik Doğrulama: ZKP'ler, bir kullanıcının kimliğini ifşa etmeden bir sisteme giriş yapmasına olanak tanır. Örneğin, kullanıcı bir biyometrik veri tabanında kayıtlı olduğunu kanıtlayabilir ancak biyometrik verisini açığa çıkarmaz.

• Veri Gizliliği ve Paylaşımı: ZKP'ler, sağlık verileri veya finansal veriler gibi hassas verilerin doğruluğunun kanıtlanmasında kullanılır. Veriyi paylaşmadan doğrulama yapılabilir, bu da gizliliği korurken veri doğruluğunu sağlar.

• MPC ve ZKP Bileşimi: Multi-Party Computation (MPC) ve ZKP'ler bir arada kullanılarak dağıtık sistemlerde güvenli hesaplamalar yapılabilir. Bu, gizli verilerin paylaşılmadan işlenmesini sağlayarak gizlilik ve güvenlik dengesini güçlendirir.

Homomorfik Şifreleme

Homomorfik Şifreleme, modern kriptografinin en yenilikçi yaklaşımlarından biridir ve verilerin şifreli haliyle işlem görmesini sağlar. Bu sayede, veriler şifrelenmiş durumdayken bile üzerinde çeşitli işlemler yapılabilir ve sonuçlar çözüldüğünde (deşifre edildiğinde) anlamlı ve doğru sonuçlar elde edilir. Bu özellik, özellikle MPC ile entegre edilmiş kripto cüzdanları için kritik öneme sahiptir çünkü bu cüzdanlar, gizlilik ve güvenliği en üst düzeye çıkarmak için çok taraflı hesaplama tekniklerine dayanır.

Homomorfik Şifrelemenin Matematiksel Temelleri

Homomorfik şifreleme, bir şifreleme fonksiyonu ***Enc()*** ve bu fonksiyon üzerinde işlem yapabilme yeteneği sunar. Şifrelenmiş verilere, bu verilerin çözülmesine gerek kalmadan belirli matematiksel işlemler uygulanabilir. Homomorfik Şifrelemenin temel prensibi şu şekilde özetlenebilir:

Veriler m_1 ve m_2 olsun.

Bu veriler şifrelenmiş haliyle $Enc(m_1)$ ve $Enc(m_2)$ olarak verilsin.

Şifrelenmiş veriler üzerinde bir işlem uygulandığında, $Enc(m_1)$ ve $Enc(m_2)$, bu işlem sonucu elde edilen değerin şifrelenmiş halidir: $Enc(m_1 \circ m_2)$

Bu süreçte, işlem sonucu $m_1 \circ m_2$ şifresi çözülmeden doğrudan elde edilebilir.

Şifreleme fonksiyonu $Enc(x)$ ve şifre çözme fonksiyonu $Dec(x)$ şu özellikleri taşır:

$$Dec(Enc(m_1).\ Enc(m_2)) = m_1 \circ m_2$$

Bu özellik, belirli operasyonların şifrelenmiş veriler üzerinden yapılmasını sağlar ve sonuç, deşifre edildiğinde doğru sonucu verir.

Kripto Cüzdanlarında Homomorfik Şifrelemenin Kullanımı:

1. Anahtar Yönetimi: MPC tabanlı cüzdanlarda, gizli anahtarların birden fazla taraf arasında paylaşılması ve bu anahtarların güvenli bir şekilde işlenmesi gerekir. Homomorfik şifreleme, bu anahtarların şifrelenmiş şekilde hesaplanmasına olanak tanır. Anahtarlar şifreli kalırken, doğru hesaplamalar yapılır ve işlem sonucunda güvenli bir şekilde anahtarlar oluşturulabilir.

2. İşlem İmzalama: Bir işlem gerçekleştirileceğinde, MPC cüzdanındaki taraflar, şifreli bir biçimde işlemleri imzalayabilir. Homomorfik şifreleme sayesinde, imza işlemleri şifrelenmiş olarak yapılabilir ve imzanın doğruluğu, imzayı atan tarafların gizli anahtarlarını ifşa etmeden doğrulanabilir.

3. Gizlilik Koruması: Kripto cüzdan kullanıcıları, işlemlerini gizli tutmak isteyebilirler. Homomorfik şifreleme, işlem detaylarını şifreli tutarak bu gizliliği sağlar. Cüzdan kullanıcıları, işlem bilgilerini açığa çıkarmadan güvenli bir şekilde işlem yapabilirler. Özellikle çok taraflı imzalama gerektiren işlemlerde, şifreli verilerle işlem yapılması gizliliği artırır.

Homomorfik Şifrelemenin Avantajları

Homomorfik şifreleme, MPC tabanlı kripto cüzdanlarının güvenliğini ve gizliliğini artırır, ancak bunun yanı sıra bazı önemli avantajları da bulunmaktadır:

• Gizli Veriler Üzerinde İşlem Yapabilme: Veriler şifrelenmişken işlemler yapılabilir, bu da verilerin üçüncü taraflarla paylaşılmasını gerektirmez. Örneğin, bir kullanıcının cüzdan adresi veya işlem detayı, işlem süresince şifreli kalır ve kimse bu bilgilere erişemez.

• Çoklu Taraflı Hesaplamaların Güvenliği: MPC ile birleştirildiğinde, homomorfik şifreleme taraflar arasında yüksek güvenlikli hesaplamalar yapılmasını sağlar. Bu, cüzdanlardaki anahtar yönetimi ve işlem güvenliğinde kritik bir rol oynar.

• Veri Bütünlüğü ve Gizliliği: İşlemler sırasında verinin bütünlüğü korunur, şifreli veriler üzerinde yapılan işlemler sonucunda elde edilen veriler orijinal veriyle tutarlıdır. Bu, cüzdan işlemlerinin güvenliğini en üst düzeye çıkarır.

Homomorfik Şifrelemenin Zorlukları ve Sınırlamaları

Her ne kadar homomorfik şifreleme, MPC tabanlı cüzdanlarda önemli avantajlar sunsa da bazı zorluklar da mevcuttur:

• Hesaplama Maliyeti: Homomorfik şifreleme, diğer şifreleme yöntemlerine kıyasla daha fazla hesaplama gücü ve zaman gerektirir. Özellikle tam homomorfik şifreleme sistemlerinde, işlem süresi ve kaynak kullanımı oldukça yüksektir.

• Verimlilik: Kripto cüzdanları gibi gerçek zamanlı işlem gerektiren sistemlerde, homomorfik şifrelemenin yavaşlığı, sistemin performansını olumsuz etkileyebilir. Bu nedenle, performansı artırmak için hibrit sistemler kullanılabilir.

• Anahtar Yönetimi: Homomorfik şifreleme ile kullanılan anahtarların güvenliği ve yönetimi de ek bir zorluk oluşturur. Anahtarların doğru bir şekilde paylaştırılması ve korunması gerekir.

Cüzdan Kategorileri

Kripto para dünyasında kullanılan cüzdanlar, dijital varlıkların güvenli şekilde saklanmasını ve yönetilmesini sağlayan temel araçlardır. Güvenlik gereksinimlerine, işlem hızlarına ve kullanıcı ihtiyaçlarına göre farklı kategorilere ayrılırlar. Bu kategoriler genel olarak sıcak cüzdanlar, soğuk cüzdanlar ve ılık cüzdanlar olarak bilinir. Her kategori, kriptografik ve güvenlik açısından farklı yaklaşımlar sunar.

Tek İmzalı Cüzdanlar

Tek imzalı cüzdanlar, kripto para cüzdanlarının en basit formunu temsil eder. Geleneksel dijital cüzdanlar olarak bilinen bu cüzdanlar, varlıklara erişim sağlamak için genellikle tek bir gizli anahtara dayanır.

Temel olarak bu cüzdanlar basit bir prensip üzerine çalışır: Bir gizli anahtar, ilgili fonlar üzerinde tam kontrol sağlar. Bu anahtar, fonları hareket ettirmek için gereken tek imza olarak hareket eder, bu da bu cüzdanları kullanımı kolay hale getirir ancak belirli savunmasızlıklar da yaratır:

• Tek Hata Noktası: Bu cüzdanlar, tek bir gizli anahtara dayandığı için, bu anahtarın tehlikeye girmesi durumunda tüm cüzdan bakiyesi riske girer. Diğer bir deyişle, bu yaklaşım tek bir hata noktası oluşturarak, gizli anahtar kaybolur, çalınır veya tehlikeye girerse cüzdanı savunmasız hale getirir. Geleneksel finansal sistemlerde yedekleme seçenekleri ve dolandırıcılık koruması bulunurken, tek imzalı cüzdanlarda gizli anahtar kaybedilirse ve yedekleme yapılmamışsa fonları geri almak genellikle imkansızdır.

• Paylaşılan Erişim Eksikliği: Tek imzalı cüzdanlar, erişimi veya kontrolü paylaşma yeteneğine sahip değildir. Bu nedenle, ortak finansal yönetim gerektiren organizasyonlar veya gruplar için uygun değildir.

Küçük fonlara sahip bireysel kullanıcılar için kullanışlı olsalar da bu cüzdanların doğasında bulunan riskler ve esneklik eksikliği, kurumlar veya daha büyük güvenlik gereksinimi olan senaryolar için yetersiz kalmalarına neden olur.

Cüzdanlar, temel olarak gizli (özel) kripto anahtarının kullanılmasıyla gerçekleştirilen imzalama işlemiyle, dijital (kriptografik) imzaların (örneğin ECDSA, EdDSA, BLS) oluşturulmasını sağlar. Dijital imzalar, tüm merkeziyetsiz altyapıların temelini oluşturmaktadır. Bir işlem sahibince imzalandığında, bu işlem merkeziyetsiz ağa gönderilir. Ağın düğümleri, gönderenin açık anahtarını kullanarak imzayı doğrular ve bu, işlemin doğruluğunu sağlar. Merkeziyetsiz sistemlere duyulan güven, gizli anahtarların güvenliğini sağlamak kadar önemlidir.

Ancak, mevcut anahtar yönetimi çözümleri, istenen kullanılabilirlik, güvenlik ve gizlilik gereksinimlerini karşılamaktan uzaktır. Özel imzalama anahtarların korunması tamamen kullanıcıların kendi inisiyatifine bağlıdır. Mevcut geleneksel cüzdan teknolojileri aşağıdaki sorunlar ile karşı karşıyadır:

1. Kimliklerin Açığa Çıkması: İmzalayanlar, blokzincir üzerinde herkese açık olarak bilinir ve izlenebilir (takma adlar kimlikleri gizlemek için yeterli değildir). Bu nedenle, saldırganlar blokzincir ağındaki açık bilgilere dayanarak belirli bir imzalayanı hedef alabilir. Özellikle büyük miktarda fon sahibi olan bir kullanıcının kimliği elde edilirse, bu durum kullanıcının hayatını bile tehlikeye atabilir. Ayrıca, gizli anahtarlara sahip herhangi bir sistem, siber saldırılar için özel bir hedef olabilir.

2. Siber Tehditler: Her bireyin yalnızca bir adet gizli anahtarı bulunduğu için (bu anahtar mobil cihazlarda, masaüstü bilgisayarlarda, donanım belirteçleri veya USB'lerde fiziksel olarak saklanır), bu anahtarların karmaşık siber tehditlere karşı güvenli bir şekilde korunması zor olduğundan, tek hata noktası saldırılarına karşı savunmasızdır.

3. İç Tehditler: Bir işletmede iç tehditleri önlemek kolay değildir. Bu nedenle, eğer bir çalışan kötü niyetli hale gelirse, kurumsal fonlar tehlikeye girebilir. Bunu önlemenin yollarından biri, dağıtık bir yapı kurarak bir kişinin tek başına fonlara erişimini engellemektir.

Sıcak Cüzdan (Hot Wallets)

Sıcak cüzdanlar, sürekli internete bağlı olan ve anlık işlemler için kullanılan cüzdanlardır. Siber güvenlik açısından değerlendirildiğinde, sıcak cüzdanlar güvenlik ve hız arasında bir denge kurar. Anahtar çiftleri, genellikle ECDSA veya EdDSA gibi eliptik eğri tabanlı algoritmalarla üretilir. Kullanıcı, gizli anahtarını (private key) kullanarak dijital imzalar oluşturur ve bu imzalarla işlemler gerçekleştirilir.

Ancak, internete sürekli bağlı olma durumu, Man-in-the-Middle (MITM) ve key logging gibi saldırılara karşı savunmasız hale getirebilir.

Sıcak cüzdanların cebirsel modellemesini yaparken, p bir asal sayı olmak üzere, Z_p (mod p tam sayılar kümesi) üzerinde tanımlı bir eliptik eğrinin kullanıldığını varsayalım. Kullanıcının gizli anahtarı d ve açık anahtarı $P = dG$'dir, burada G eliptik eğri üzerinde bir üreteç noktadır. İşlem sırasında, kullanıcı gizli anahtar d ile dijital imza oluşturur. Ancak, saldırganların tekrarlama saldırısı (replay attack) ve yan kanal (side-channel) saldırılarına karşı sistemin koruması yetersiz kalabilir. Bu nedenle sıcak cüzdanlar, küçük miktarda kripto para birimini aktif olarak kullanmak için uygun olsa da, yüksek güvenlik gerektiren işlemler için tercih edilmemelidir.

Soğuk Cüzdan (Cold Wallets)

Soğuk cüzdanlar, kripto para birimlerinin güvenliğini sağlamak için gizli anahtarınızı tamamen çevrimdışı bir ortamda saklar. Bu, bilgisayar korsanlarının internet üzerinden gizli anahtarınıza erişmesini imkansız hale getirerek güvenlik risklerini önemli ölçüde azaltır. Donanım cüzdanları, en popüler soğuk cüzdan türüdür ve "air-gapped" sistemler olarak düşünülebilir. Yani, gizli anahtarınız ***(d)*** asla çevrimiçi ortama maruz kalmaz. İşlem yapmak istediğinizde, donanım cüzdanı, imzayı oluşturmak için gerekli hesaplamaları yapar, ancak gizli anahtarınızı asla cihazın dışına çıkarmaz.

Hash-based kriptografi ve çoklu faktör doğrulama, soğuk cüzdanların güvenliğini daha da artırır. Örneğin, SHA256 veya Blake2b gibi güçlü bir özet (hash) fonksiyonu, işlem verilerini güvenli bir şekilde özetlemek için kullanılır. Bu özet daha sonra donanım cüzdanına gönderilir ve imzalama işlemi burada, gizli anahtarın güvenli ortamından ayrılmadan gerçekleştirilir.

Ayrıca, Sıfır Bilgi İspatları (ZKP) gibi gelişmiş teknikler, işlemin doğruluğunu gizli anahtarı açığa çıkarmadan kanıtlama imkanı sunar. Soğuk cüzdanların en büyük dezavantajı, kullanım zorluğudur. Her işlem için cihazı çevrimiçi hale getirmek gerekir, bu da süreci yavaşlatabilir ve kullanıcı deneyimini olumsuz etkileyebilir. Ancak, özellikle büyük miktarda kripto para birimi saklanıyorsa, sağladığı üstün güvenlik, bu dezavantaja katlanmayı değerli kılar.

Ilık Cüzdan (Warm Wallets)

Ilık cüzdanlar, sıcak ve soğuk cüzdanlar arasında bir denge kurar. Genellikle cüzdan çevrimdışı olarak saklanır ancak gerektiğinde hızlıca çevrimiçi hale getirilebilir. Matematiksel olarak, ılık cüzdanlar çoğunlukla eşik imzalama (threshold signature) veya çoklu imzalama (Multisig) algoritmaları ile güvenliği artırır.

Bu tür protokoller, yalnızca belirli bir sayıda kullanıcı imza attığında işlemin geçerli olmasını sağlar.

Örneğin, Shamir Sır Paylaşımı protokolü bu tür cüzdanlar için ideal bir güvenlik mekanizmasıdır. Bu protokol, gizli anahtarın farklı parçalara bölünerek dağıtılmasını sağlar. Matematiksel olarak,

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}$$

şeklinde bir polinom oluşturulur ve bu polinomun ***t*** sayıda noktası bilindiğinde, a_0 yani gizli anahtar tekrar hesaplanabilir. Bu yöntem, güvenliğin artırılması amacıyla ılık cüzdanlar tarafından kullanılabilir.

Bu cüzdan türü, genellikle hem güvenlik hem de erişim kolaylığı sağlamak isteyen kurumsal kullanıcılar tarafından tercih edilir. Ancak, cüzdanın çevrimiçi hale getirilmesi bir miktar güvenlik riski oluşturabilir; bu nedenle çoklu imza ya da benzeri ek güvenlik önlemleri önerilir.

Çoklu İmza (Multisig) Cüzdanlar

Çoklu imza (Multisig) cüzdanlar, bir işlemin geçerli olabilmesi için birden fazla tarafın imzasını gerektiren bir yapıya sahiptir. Matematiksel olarak, bu cüzdanlar eşik kriptografisi (threshold cryptography) ile modellenir. Diyelim ki, bir işlemin onaylanabilmesi için n imza arasında en az imzanın gerekli olduğunu varsayalım. Bu durumda, her bir imza verisi, doğrulama için kullanılır ve işlem ancak belirlenen eşik sağlandığında başarılı olur.

Bir Multisig cüzdanın cebirsel modeli şu şekilde olabilir: Varsayalım ki, bir eliptik eğri ***E*** üzerinde ***n*** sayıda gizli anahtar ***d1, d2,.....dn*** var. Her bir kullanıcının açık anahtarı $P_i = d_i . G$ ile tanımlanır. Burada ***G***, eliptik eğri üzerinde jeneratör noktadır. İşlem doğrulaması için en az ***t*** kişinin d_i ile oluşturduğu dijital imzalar, bu eşik değerini karşılamalıdır. Bu mekanizma, güvenliği artırarak tek bir kişinin gizli anahtarına erişilse bile işlemi tamamlamayı zorlaştırır.

Bu yapılar özellikle kurumsal cüzdanlar, borsalar ve güvenli transferlerde tercih edilir. Siber güvenlik perspektifinden bakıldığında, bir kişinin saldırıya uğraması durumunda bile tek başına işlemi onaylayamaması nedeniyle Multisig, güvenliği ciddi şekilde artırır.

Çoklu İmza (Multisig) Cüzdanlar Nasıl Çalışır?

Multisig cüzdanların temelinde m-out-of-n prensibi yatar. Bu prensip, toplamda n adet anahtardan, bir işlemin geçerli sayılabilmesi için gereken minimum m adet imzayı tanımlar. Örneğin, 3-out-of-5 Multisig cüzdanı, belirlenen beş anahtardan herhangi üç tanesinin imzasını aldıktan sonra işlemin gerçekleşmesini sağlar. Bu mekanizma, güvenliği artırmanın yanı sıra, kaybolan gizli anahtarlardan kaynaklanabilecek riskleri de azaltmaya olanak tanır.

Gerekli eşik sayıda imza elde edildiği sürece işlemler gerçekleştirilebilir. Çoklu imza (Multisig) teknolojisi, dijital varlıkların güvenliğini artırmak amacıyla geliştirilmiş bir yöntemdir. Bu teknoloji, genellikle birden fazla tarafın onayını gerektiren ortak hesaplar veya organizasyonlar tarafından bir işlemi yetkilendirmek ve yürütmek için kullanılır. Ayrıca, ortak fonlar, iş ortaklıkları veya finansal operasyonlar gibi, toplu karar alınmasını gerektiren durumlar için özellikle uygundur. Geleneksel tek imzalı cüzdanlarda işlem, yalnızca bir gizli anahtarın imzasıyla doğrulanabilirken, çoklu imza cüzdanlarında birden fazla anahtarın imzası gerekmektedir. Bu yaklaşım, işlemler üzerinde daha fazla güvenlik ve kontrol sağlar.

Çoklu imza cüzdanları, blokzincir ağı üzerindeki akıllı sözleşmeler aracılığıyla yönetilir. Bu akıllı sözleşmeler, bir işlemi doğrulamak için gerekli koşulları ve katılımcıları belirleyerek, güvenliği artırır ve merkeziyetsizlik sağlar. Böylece, çoklu imza, tek bir hata noktasını ortadan kaldırır ve izinsiz işlemleri engelleyerek ek bir güvenlik katmanı oluşturur.

Çoklu İmza (Multisig) Arkasındaki Kriptografi

a) Eşik İmzalar

Eşik imzalar, çoklu imza cüzdanlarının güvenli bir şekilde çalışmasını sağlayan temel kavramdır. Eşik değeri m, bir işlemi yetkilendirmek için toplam imzalayan sayısından n kaç tanesinin imzasının gerektiğini belirler. Örneğin, 2-out-of-3 çoklu imza cüzdanında:

- Üç kişi veya kuruluşun her birinin kendi gizli anahtarı vardır.
- Bir işlemi başlatmak için, bu üç gizli anahtardan en az ikisinin imzalanması gerekmektedir.
- İşlem, gerekli imza sayısı (bu durumda iki) elde edildiğinde geçerli sayılır.

Bu mekanizma, gizli anahtarlardan biri ele geçirilse bile, saldırganın diğer imzalayanların iş birliği olmadan fonları taşıyamayacağı anlamına gelir.

b) Güvenlik Önlemleri

Çoklu imza cüzdanlarını uygularken maksimum güvenliği sağlamak için en iyi uygulamaları takip etmek önemlidir:

1. Coğrafi Dağılım: İmzalayanların coğrafi olarak dağıtılmış olmasını sağlamak, tek bir konumun tehlikeye girmesi riskini azaltır.

2. Düzenli Anahtar Değişimi: Gizli anahtarları düzenli olarak değiştirmek, uzun vadeli anahtar ifşası risklerini azaltır.

3. Soğuk Depolama: Bazı gizli anahtarları çevrimdışı (soğuk depolama) olarak saklamak, onları çevrimiçi saldırılardan korur.

4. Denetim Günlükleri: Cüzdan aktivitelerinin ayrıntılı denetim günlüklerini tutmak, şüpheli eylemleri izlemek ve izini sürmek için önemlidir.

5. Farklı Platform Kullanımı: Farklı platformların (Windows, Linux, iOS gibi) bir arada kullanılması, olası bir zero-day saldırısının tüm sistem üzerinde etkili olma riskini azaltabilir. Bu çeşitlilik, platformlara özgü açıkların tek bir saldırıda tüm cüzdan yapısını tehlikeye atmasını engelleyerek ekstra güvenlik sağlar.

Çoklu İmza Kullanmanın Avantajları

1. Güvenlik Artışı: Çoklu imza cüzdanları, tek imzalı cüzdanlara kıyasla daha fazla güvenlik sunar. Bir işlemi yetkilendirmek için birden fazla gizli anahtar gerektiğinden, izinsiz erişim veya dolandırıcılık riski önemli ölçüde azalır. Bu yöntem, bir hata noktasının tek başına var olmasını önleyerek ek güvenlik sağlar.

2. Risk Azaltma: Bir işlemi onaylamak için birden fazla taraf gerektiğinden, tek bir kişinin hatası, yanılgısı veya kötü niyeti nedeniyle fonların kaybedilme riski önemli ölçüde azalır. Bu, özellikle organizasyonlar için büyük bir avantajdır.

3. Paylaşımlı Kontrol: Ortak hesaplar veya organizasyonlar için ideal olan çoklu imza cüzdanları, birden fazla kullanıcının fonları birlikte yönetmesine olanaktanır. Bu, işlemlerle ilgili kararların daha şeffaf ve demokratik bir şekilde alınmasını sağlar.

4. Dolandırıcılığı Önleme: Birden fazla imza gereksinimi, izinsiz işlemleri ve olası dolandırıcılık girişimlerini azaltır. Herhangi bir işlemin onaylanması için birden fazla tarafın onayı gerektiğinden, kötü niyetli işlemlerin yapılma olasılığı azalır.

5. Özelleştirilebilir Güvenlik Seviyeleri: Çoklu imza cüzdanları, bir işlemi gerçekleştirmek için gereken imzalayan sayısının özelleştirilmesine olanak tanır. Bu da güvenlik ve kullanılabilirlik arasında esneklik sağlar.

Çoklu İmza Kullanmanın Dezavantajları

1. Karmaşıklık: Çoklu imza cüzdan kurmak ve yönetmek, geleneksel tek imzalı cüzdanlara göre daha karmaşıktır. Birden fazla taraf arasında koordinasyon gerektirir ve çoklu imza sisteminin nasıl çalıştığını anlamayı gerektirir.

2. Erişim Kaybı Riski: Yetkili taraflardan birinin gizli anahtarını kaybetmesi veya kullanılamaz hale gelmesi durumunda, fonlara erişim engellenebilir. Bu durum, özellikle kritik işlemler söz konusu olduğunda büyük bir sorun olabilir.

3. Yüksek Kurulum Maliyetleri: Çoklu imza cüzdan oluşturmak ve sürdürmek, karmaşıklık ve ek güvenlik önlemleri nedeniyle bazen daha yüksek başlangıç maliyetleri gerektirebilir.

4. Yüksek İşlem Ücretleri: Çoklu imza işlemlerinin imza verisi daha büyük olduğundan, bu işlemler tek imzalı işlemlerden daha yüksek işlem ücreti gerektirir. Özellikle yoğun blokzincir ağlarında bu ekstra maliyet, kullanıcılar için önemli bir dezavantaj olabilir.

5. İşlem Gecikmeleri: İşlemler, birden fazla imza gerektiğinden, tek imzalı işlemlere göre gecikmelere yol açabilir. Özellikle bir imzalayan kullanılamaz durumda olduğunda gecikmeler yaşanabilir.

6. İmzalayanlara Bağımlılık: Çoklu imza cüzdanının işlevselliği, gerekli imzalayanlardan birinin yanıt vermemesi durumunda aksayabilir ve bu da işlem tıkanıklıklarına neden olabilir.

Bu avantajlar ve dezavantajları anlamak, bireylerin veya kuruluşların çoklu imza cüzdanının kripto para saklama ve işlem ihtiyaçları için doğru seçim olup olmadığını değerlendirmelerine yardımcı olabilir. Özetle, çoklu imza cüzdanı, içinde saklanan varlıklar üzerinde tek bir kişi veya kuruluşun tam kontrol sahibi olmasını engeller, böylece güvenliği artırır ve birden fazla yetkili kullanıcı arasında paylaşımlı kontrol sağlar.

MPC Cüzdanlar

Multi-Party Computation (MPC), dijital varlıkların güvenliğini artırmak için kullanılan ileri düzey bir tekniktir. MPC, birden fazla tarafın bireysel girdi verilerini ifşa etmeden ortak hesaplama yapmasını sağlayan devrim niteliğinde bir kriptografik tekniktir. MPC, güvenli, ortak hesaplama sağlarken özel verilerin korunmasını sağlar. Cüzdanlar bağlamında MPC, özel bir anahtarı parçalara ayırarak birden fazla tarafa dağıtır.

Bu, tek bir hata noktası riskini azaltarak güvenliği artırır. MPC cüzdanları, geleneksel Multisig cüzdanlara göre daha fazla esneklik sunar.

MPC, birden fazla tarafın özel verilerini ifşa etmeden ortak bir hesaplama yapmasını sağlar. Bu yöntemin temelinde Shamir Secret Sharing (SSS) protokolü yatmaktadır. Bu yöntemde, bir gizli anahtarı birden fazla parçaya bölerek her bir payın farklı taraflara dağıtması amaçlanır. Bu sayede, belirli bir eşik sayısı kadar pay bir araya gelmeden gizli anahtar ortaya çıkarılamaz.

MPC'nin güvenliği, iki temel özelliğe dayanır:

1. Gizlilik (Privacy): Tarafların sahip olduğu özel bilgiler, protokol yürütülürken diğer taraflar tarafından öğrenilemez.

2. Doğruluk (Correctness): Taraflardan bazıları protokolden sapmaya veya bilgiyi paylaşmaya çalışsa bile, MPC bu girişimlerin doğru sonucu etkilemesine veya dürüst tarafların bilgilerini sızdırmasına izin vermez.

3. Eşik İmzalama ve Dayanıklılık (Robustness): MPC'nin eşik özelliği, işlemin gerçekleştirilmesi için yalnızca belirli sayıda tarafın katılımının yeterli olmasını sağlar.

Bu özellik, sistemin dayanıklılığını artırarak bazı taraflar protokole katılamasa veya kötü niyetli hareket etse bile işlemin başarılı bir şekilde tamamlanmasını sağlar. Bu da MPC'yi güvenilir ve saldırılara karşı daha dirençli kılar.

MPC, tek bir gizli anahtarın oluşturulmasını gerektirmediği için "tek bir hata noktasını" (single-point-of-failure) ortadan kaldırır. MPC tabanlı çözümler, çoklu imza çözümlerine kıyasla operasyonel esneklik sağlar. Örneğin, bir MPC cüzdanında imza atanların sayısı artırılabilir veya azaltılabilir ve bu değişiklikler operasyonel süreçlerde herhangi bir kesintiye neden olmaz. Ayrıca MPC, farklı blokzincir protokolleriyle daha uyumlu olduğu için daha geniş bir kullanım alanına sahiptir.

MPC'nin dijital varlık güvenliği üzerindeki en önemli yeniliklerinden biri, gizli anahtarın sürekli olarak yenilenmesidir (key refresh). Bu özellik, bir saldırganın tüm anahtar paylarını ele geçirmesi için sadece birkaç dakikası olduğu anlamına gelir; bu süreden sonra paylar yenilenir ve saldırganın yeniden başlaması gerekir. Bu yöntem, güvenlik katmanını güçlendirerek siber saldırılara karşı ek bir koruma sağlar.

MultiSig ve MPC cüzdanlar, kontrolü dağıtarak ve izinsiz erişime karşı korumayı artırarak bu savunmasızlığı gideren güvenlik mekanizmaları sunar. Aşağıda, MultiSig ve MPC cüzdanlara odaklanarak bu teknolojilerin benzersiz özellikleri, benzerliklerini ve sınırlılıkları incelenmektedir.

MPC ve MultiSig Benzerlikleri

MPC ve MultiSig cüzdanların farklı mekanizmaları olsa da dijital varlıkların güvenliğini ve kontrolünü artırmak isteyen kurumlar için bazı ortak benzerlikleri vardır:

• Dağıtık Kontrol: Her iki teknoloji de cüzdan erişimi ve kontrolü birden fazla taraf veya kuruluşa dağıtma yeteneğine sahiptir.

Bu, kurumların işlemler üzerinde kolektif karar almasını sağlar ve izinsiz işlemler veya iç dolandırıcılık riskini en aza indirir.

• Güçlü Güvenlik ve Dayanıklılık (Strong Security and Robustness): MPC ve MultiSig cüzdanlar, bazı katılımcılar veya anahtarlar tehlikeye girse bile, yeterli sayıda katılımcı veya imza kaldığı sürece sistemin genel güvenliğini korur. Bu güvenlik katmanı, tek anahtarlı çözümlerden çok daha sağlam bir yapıya sahiptir.

• Minimum Güven: MPC ve MultiSig, kontrolü dağıtarak ve kriptografik algoritmalar kullanarak katılımcılar arasındaki güven ihtiyacını azaltır. Bu durum, özellikle karmaşık kurumsal yapılar veya dış ortaklarla çalışırken oldukça değerlidir.

• Esneklik: Hem MPC hem de MultiSig, belirli güvenlik ihtiyaçlarına ve operasyonel süreçlere uygun şekilde özelleştirilebilir. Kurumlar, işlem yetkilendirmesi için gerekli imzalayan sayısını ve tercih edilen kriptografik algoritmaları belirleyebilir.

MPC Cüzdanlarının Avantajları

MPC (Multi-Party Computation) cüzdanlar, MultiSig cüzdanlarda karşılaşılan birçok sınırlılığı ele alarak dijital varlıkların yönetiminde giderek daha popüler bir seçenek haline gelmektedir. İşte MPC cüzdanlarının bazı önemli avantajları:

• Esnek Çoklu Zincir Desteği: MPC cüzdanlar, blokzincir agnostik bir yapıya sahiptir ve ECDSA, EdDSA, BLS imzalama algoritmalarını kullanan birçok blokzinciri destekleyebilir. MultiSig cüzdanların aksine, tek bir MPC cüzdanı birden fazla blokzincir üzerindeki varlıkları yönetebilir.

• Gelişmiş Gizlilik: MPC cüzdanlar, işlem onayı için yalnızca tek bir gizli anahtar imzasının blokzincire yayınlanmasını sağlar. Diğer tüm hesaplamalar zincir dışında gerçekleşir ve hassas bilgiler kamuya açık görünmez. Bu da MPC cüzdanlarını gizliliği ön planda tutan kurumlar için ideal hale getirir.

• Anahtar Kurtarma Mekanizmaları: MPC cüzdanlar, anahtar kurtarma mekanizmaları sunarak, kayıp veya tehlikeye giren anahtarların geri kazanılmasına olanak tanır. Bu özellik, geleneksel MultiSig çözümlerinde genellikle bulunmayan bir güvenlik ağı sağlar.

• Düşük Gaz Ücretleri ve Artan İşlem Hızı: MPC cüzdanlar, blokzincir işlemleriyle ilgili gaz ücretlerini önemli ölçüde azaltabilir.

Karmaşık hesaplama zincir dışında gerçekleştiğinden, onay için blokzincire yayınlanan işlem daha küçük olur.

Bu durum, işlem boyutunu küçülterek madencilerin bu işlemleri önceliklendirmesine ve daha hızlı işlem onaylarına yol açar.

MultiSig Cüzdanlarının Sınırlılıkları

MultiSig cüzdanlar, tek anahtarlı cüzdanlara göre güvenlik artırırken, bazı sınırlılıklar da sunar:

• Protokol Agnostik Değil: MultiSig cüzdanlar her blokzincir protokolü ile uyumlu değildir ve her blokzincir için farklı uygulamalar gerektirebilir. Bu, farklı kripto varlıkları yönetmek için birden fazla cüzdan çözümü kullanma gerekliliği doğurur.

• Operasyonel Karmaşıklık: Organizasyonlar büyüdükçe, imzalayan sayısını değiştirme, anahtarları ekleme veya kaldırma gibi işlemler zor olabilir. MultiSig cüzdanlar genellikle önceden yapılandırılmış olduğundan, bu tür değişikliklerin yapılması esnek değildir.

• Şeffaflık Sorunları: Blokzincir üzerindeki işlemlerin kamusal doğası, MultiSig imzalarının ve onay eşiğinin izlenmesine olanak tanır. Bu durum, kötü niyetli aktörlerin dikkatini çekebilir ve potansiyel saldırı hedefleri oluşturabilir.

• Yüksek İşlem Maliyeti: MultiSig cüzdanlarda her işlem zincir üzerinde oluşturulduğu için, her cüzdan oluşturma, adres oluşturma ve imza gibi işlemler için bir işlem ücreti ödenmesi gereklidir. Bu durum, çoklu imza gerektiren işlemler için yüksek işlem maliyetlerine yol açar.

Kısaca özetlemek gerekirse, MPC çözümünün genel olarak faydaları şu şekilde sıralanabilir:

• Sistem Seviyesinde Eşik Güvenlik

• Threshold ECDSA, Threshold EdDSA ve Threshold BLS desteği

• Sorumluluğun Paylaşılması

• Kripto borsalarından kaynaklı finansal kayıpları önleme

• İmzalayanların gizliliğini sağlama

• İmzalama süreci ve imza taleplerinin ayrılması

• Kullanılabilirlik ve tek hata noktasının ortadan kaldırılması

• Daha düşük işlem ücreti

• Çok Taraflı Onaylama

• Çok faktörlü kimlik doğrulama

• Sıcak cüzdanlar için beyaz liste oluşturma (ek güvenlik katmanı olarak)

• iOS ve Android platformları için mobil uygulama desteği (kullanım kolaylığı ve artan kullanılabilirlik sağlamak amacıyla)

• Açık-gizli anahtar parametrelerini oluşturmak için merkezi bir güvenli tarafa ihtiyaç duyulmaması (trustless setup)

• Tek bir kullanıcı için imzalama sürecine katılan bulut hizmetleri

• Bağlı hizmetler arasında özgün iletişim
• Hizmetler arasında inkâr edilemezlik (non-repudiation)

• Son kullanıcılar için bulut hizmetleri ile eşik varlık anahtarı yönetimi

• Üçüncü Taraf Denetimleri

Blokzincir ve kripto para teknolojileri, dijital varlıkların saklanması ve güvenli bir şekilde yönetilmesi konusunda yenilikçi çözümler sunmaktadır. Çoklu imza kullanımı, soğuk depolama, HSM/TPM/SGX prosedürleri ve MPC gibi teknikler, dijital varlıkların güvenliğini artırmak amacıyla geliştirilmiştir ve özellikle siber güvenlik uzmanları için kritik öneme sahiptir. MPC'nin çoklu imza yöntemine kıyasla sağladığı operasyonel esneklik, protokol bağımsızlığı ve yüksek güvenlik, bu teknolojiyi dijital varlık güvenliği için daha ileri bir çözüm haline getirmektedir.

Gözetimli (Custodial) Cüzdanlar

Gözetimli (Custodial) cüzdanlar, kullanıcının gizli anahtarlarının üçüncü bir tarafça yönetildiği, daha merkezi bir yapıya sahip cüzdan türüdür. Bu cüzdanlarda kriptografik kontrol genellikle kullanıcıda değil, hizmet sağlayıcıda bulunur. Kullanıcılar, işlemlerini gerçekleştirmek için hizmet sağlayıcının API'lerini kullanırken, hizmet sağlayıcı anahtarları güvenli bir şekilde yönetir.

Matematiksel açıdan, gözetimli cüzdanlar daha çok hizmet sağlayıcının şifreleme altyapısı ve erişim denetim modelleriyle korunur. Şifreleme algoritmaları, hizmet sağlayıcının veri merkezlerinde saklanan anahtarlar için kullanılır. Özellikle Rol Tabanlı Erişim Kontrolü (RBAC) gibi erişim kontrol mekanizmaları, bu cüzdanların temel güvenlik bileşenlerini oluşturur. Bu cüzdan türü, merkezi borsalarda yaygın olarak kullanılır ve kullanıcılar adına işlemleri kolaylaştırır. Ancak, kullanıcılar anahtarların gerçek sahibi olmadığından, güvenlik açısından daha zayıf bir model olarak kabul edilir.

Gözetimsiz (Non-Custodial) Cüzdanlar

Gözetimsiz (Non-Custodial) cüzdanlar, kullanıcının kendi gizli anahtarları üzerinde tam kontrole sahip olduğu cüzdanlardır.

Bu cüzdanlarda, hiçbir üçüncü taraf kullanıcı varlıklarına veya gizli anahtarlarına erişemez. Kriptografik açıdan bakıldığında, her kullanıcı kendi cüzdanının anahtar çiftine sahiptir ve bu anahtarlar genellikle ECDSA gibi güvenli eliptik eğri algoritmalarıyla üretilir ve korunur.

Gözetimsiz cüzdanların temel kriptografik güvenliği, kullanıcıya ait gizli anahtarın (private key) güvenli bir şekilde saklanmasına dayanır. HD Cüzdanlar (Hierarchical Deterministic Wallets), tek bir tohum (seed) kullanarak birden fazla gizli anahtarın güvenli bir şekilde oluşturulmasını sağlayan bir teknolojidir. Matematiksel olarak, HD cüzdanlar, bir ana anahtardan (master key) türetilen alt anahtarlarla (child key) işlem yapar ve bu anahtarlar deterministik bir şekilde hesaplanır.

Tam Gözetimsiz Cüzdanlar

Tam gözetimsiz cüzdanlar, kullanıcının varlıkları üzerinde tam kontrol sahibi olmasını sağlar. Gizli anahtarlar tamamen kullanıcı tarafından saklanır ve hiçbir üçüncü taraf bu anahtarlara erişemez. Kriptografik olarak, her işlem için dijital imzalar kullanılarak cüzdan sahibinin yetkisi doğrulanır. Bu cüzdanlar yüksek güvenlik ve gizlilik sunar, ancak kullanıcı hataları (örneğin anahtar kaybı) ciddi sonuçlara yol açabilir.

Destekli Gözetimsiz Cüzdanlar

Destekli gözetimsiz cüzdanlar, kullanıcıya gizli anahtarları üzerinde tam kontrol sağlarken aynı zamanda belirli bir düzeyde üçüncü taraf desteği sunar. Örneğin, üçüncü taraflar sadece kurtarma mekanizmalarında devreye girebilir. Bu cüzdanlar genellikle sosyal kurtarma (social recovery) mekanizmalarıyla çalışır. Kriptografik açıdan, anahtarın tam kontrolü kullanıcıda olmakla birlikte, bazı ek güvenlik önlemleri (örneğin, çoklu imza veya kurtarma anahtarları) sunulur.

Bu cüzdan türü, gözetimsiz cüzdanların avantajlarını sunarken aynı zamanda kullanıcı hatalarına karşı koruma sağlayan güvenlik önlemleriyle öne çıkar.

Kâğıt Cüzdanlar

Kâğıt cüzdanlar, kullanıcıların dijital varlıklarını çevrimdışı olarak saklamak için kullanılan basit ve düşük maliyetli bir yöntemdir. Bir kâğıt cüzdan, genellikle QR kodu veya yazılı metin şeklinde, kullanıcının kripto varlıklarının özel ve açık anahtarlarını içerir. İnternete bağlı olmadıkları için siber saldırı riskini ortadan kaldırır. Kâğıt cüzdanların en büyük avantajı düşük maliyetli olmaları ve kullanıcılara tam kontrol sağlamalarıdır. Ancak, fiziksel hasar, kaybolma veya okunamaz hale gelme gibi riskler taşırlar(12). Bu nedenle, kağıt cüzdanları korumak için özel önlemler alınmalıdır. Kağıt cüzdanlarla işlem yapmak, dijital cüzdanlara göre daha karmaşık olabilir. Transfer veya harcama yapmak için anahtarları bir yazılım cüzdanına aktarmanız gerekir. Sonuç olarak, kağıt cüzdanlar düşük maliyetli ve güvenli bir çevrimdışı çözüm sunar, ancak fiziksel riskler ve kullanım zorlukları nedeniyle dikkatli kullanılmalıdır.

Ses Cüzdanları

Ses cüzdanları, dijital varlıkların gizli anahtarlarını şifrelenmiş ses dosyaları olarak saklayarak çevrimdışı koruma sağlar. Bu dosyalar, CD veya vinil plak gibi fiziksel ortamlarda saklanarak siber saldırılara karşı güçlü bir koruma sunar. Ses cüzdanları, yenilikçi bir güvenlik yöntemi olmasına rağmen, teknik bilgi gerektirmeleri ve fiziksel medyanın zarar görme riski nedeniyle kullanımı zor olabilir. Bu nedenle, daha çok teknik bilgiye sahip ve yenilikçi güvenlik arayışında olan kullanıcılar için uygundur.

Hafıza Cüzdanları

Hafıza Cüzdanı (Brain Wallet), kullanıcıların dijital varlıklarının gizli anahtarlarını hatırlayabilecekleri bir parola veya ifade (genellikle bir passphrase) ile oluşturdukları bir tür saklama tekniğidir. Hafıza cüzdanlarında, kullanıcıların cüzdanlarına erişim sağlamak için herhangi bir fiziksel veya dijital depolama cihazına ihtiyaçları bulunmamaktadır. Brainwallet.io gibi deterministik kripto adres üretici hizmetleri aracılığıyla oluşturulurlar (13).

Hafıza cüzdanlarının en büyük avantajlarından biri, herhangi bir fiziksel cüzdana gerek kalmadan varlıklarınızı koruma imkânı sunmasıdır. Ayrıca, varlıklarınıza yalnızca sizin bildiğiniz bir parola ile erişim sağlanması, gizliliği artırır. Ancak, hafıza cüzdanlarının bazı önemli dezavantajları da vardır. Parolanızı unutmanız durumunda dijital varlıklarınıza erişiminizi tamamen kaybedebilirsiniz. Ayrıca, basit veya tahmin edilebilir parolalar kullanmak, cüzdanınızın kırılma riskini artırır ve güvenliğinizi tehlikeye atabilir. Bu nedenle, hafıza cüzdanı kullanmayı düşünenlerin, unutulması zor ama güçlü parolalar seçmesi büyük önem taşır. Hafıza cüzdanları, dijital varlıklarını saklamak için yenilikçi ve minimal bir yaklaşım arayanlar için uygun bir seçenek olabilir, ancak kullanıcıların güçlü parola oluşturma konusunda dikkatli olması gerekmektedir.

Akıllı Kontrat Tabanlı Cüzdanlar

Dijital varlıkların, akıllı sözleşme olarak gerçeklenmiş cüzdan ya da bir başka deyişle, kontrat adresinde tutulmasına akıllı kontrat tabanlı cüzdanlar denilmektedir. Kullanıcıların transfer işlemleri akıllı sözleşme üzerinde yapılmaktadır. Tek bir gizli anahtar tarafından kontrol edilen geleneksel kripto para cüzdanlarıyla kıyaslandığında, akıllı sözleşme tabanlı cüzdanlar, güvenlik, otomasyon ve işlevselliğin artırılması açısından farklılık göstermektedir.

Akıllı kontrat tabanlı cüzdanlar, dijital varlıklarınızın bir dizi otomatik işlem ve kural çerçevesinde yönetilmesini sağlayan gelişmiş bir çözüm sunar. Bu cüzdanlar, geleneksel cüzdanlardan farklı olarak, tek bir gizli anahtar yerine, belirli şartlar yerine getirildiğinde devreye giren akıllı sözleşmeler tarafından yönetilir. Bu sayede, kripto varlıklarınızın yönetimi otomatikleşir ve güvenlik düzeyi artar. Örneğin, Gnosis Safe, çoklu imza gerektiren işlemler için kullanılan bir akıllı kontrat tabanlı cüzdandır. Argent ise arayüz sunarak Ethereum cüzdanı olarak hizmet verir. ERC4337, Ethereum ağı üzerinde akıllı sözleşme tabanlı hesap soyutlama standartları sağlayan bir çözüm olarak öne çıkar. Akıllı kontrat tabanlı cüzdanların en önemli avantajlarından biri, programlanabilir işlemler sunmasıdır. Otomatik ödemeler, zaman kilitli işlemler gibi karmaşık işlemler bu cüzdanlarla kolayca gerçekleştirilebilir. Ayrıca, akıllı sözleşmelerin sunduğu ek güvenlik katmanları, dijital varlıkların korunmasında önemli bir rol oynar. Ancak, bu cüzdanların kullanımı geleneksel cüzdanlara göre daha karmaşık olabilir ve teknik bilgi gerektirebilir (14).

Ayrıca, akıllı sözleşmelerin yanlış yapılandırılması durumunda geri dönüşümsüz işlemler söz konusu olabilir, bu da hatalı işlemleri geri almanın mümkün olmaması anlamına gelir. Bu nedenle, akıllı kontrat tabanlı cüzdanlar, teknik bilgiye sahip kullanıcılar için güvenli ve esnek bir çözüm sunarken, dikkatli yapılandırma ve kullanım gerektirir.

Yazılım Cüzdanları

Yazılım cüzdanları, kullanıcıların dijital varlıklarını güvenli bir şekilde saklamasını ve yönetmesini sağlayan uygulamalardır; bilgisayara indirilip kurulabilir, bulut üzerinden çevrimiçi olarak çalıştırılabilir veya bir mobil uygulama aracılığıyla akıllı bir cihazda çalıştırılabilmektedirler.

Kullanıcılar, yazılım cüzdanları aracılığıyla gizli anahtarlarını koruyabilir ve bu gizli anahtarları kullanarak diğer blokzincirlerle iletişim kurarak kripto para işlemleri yapabilmektedirler.

Yazılım cüzdanları genellikle kullanıcıların kripto para cüzdan adresleri oluşturmasına, kripto para gönderip alma işlemleri yapmasına, mevcut bakiyelerini görüntülemesine ve bazı durumlarda kripto para satın almasına veya takas etmesine imkân tanımaktadır. Ayrıca, DeFi (Decentralized Finance) hizmetlerini kullanarak çeşitli finansal işlemler gerçekleştirmelerine olanak sağlayabilmektedirler.

Paribu Self, Metamask, Phantom, Keplr, Temple, TrustWallet, myEtherWallet, Guarda gibi birçok yazılım cüzdan örneği bulunmaktadır.

Yazılım cüzdanları çevrimiçi olmaları nedeniyle siber saldırılara maruz kalabilirler. Kullanıcıların güçlü şifreler kullanarak bu riskleri minimize etmeye çalışmaları gerekmektedir. Ayrıca, yazılım cüzdanlarının güvenlik özelliklerinin güncellenmesi ve güvenilir kaynaklardan uygulamanın indirilmesi oldukça önemlidir (10). Güvenliği sağlamak için güçlü parolalar, iki faktörlü kimlik doğrulama ve düzenli yedekleme gibi ek önlemler alınması gerekmektedir. Yazılım cüzdanlarının güvenliği, kullanılan cihazın güvenliği ile doğrudan bağlantılı olduğundan, bu önlemler hayati öneme sahiptir.

Donanım Cüzdanları

Donanım cüzdanlar, kullanıcıların gizli anahtarlarını çevrimdışı olarak depolayarak dijital varlıklarının güvenliğini sağlamak için kullanılan fiziksel cihazlardır. Donanım cüzdanlar internete bağlı olmadıkları için siber saldırılara karşı ek bir koruma sağlamaktadır.

Bu nedenle, özellikle yüksek güvenlik gerektiren durumlarda ve uzun vadeli yatırımlar için donanımsal cüzdanlar önemli bir seçenek olarak öne çıkmaktadır.

Donanım cüzdanlarında yazılım cüzdanlarından farklı olarak, fiziksel erişim gereklidir ve ayrıca kurcalamaya karşı dayanıklı ek özelliklere sahip olabilirler. Örneğin, PIN kodu, parmak izi gibi fiziksel güvenlik önlemleri ve kurcalamaya karşı dayanıklı özellikleriyle dikkat çekerler. Ancak, bu cihazların kullanımı yazılım cüzdanlarına göre daha karmaşık olabilir ve kurulum süreçleri daha fazla zaman alabilir. Donanımsal cüzdanların kullanımı, yedekleme ve donanım arızası gibi bazı zorlukları içerebilmektedir. Ayrıca cihazın kaybolması gibi durumlar da söz konusudur. Ancak bu dezavantajlara rağmen, donanımsal cüzdanlar, dijital varlıkların güvenliği için yüksek düzeyde koruma sağlamak amacıyla tercih edilen çözümlerdir. Günümüzde Trezor, KeepKey, BitBox, CoolWallet S, ELLIPAL Titan ve Tengem gibi birçok donanım cüzdan sağlayıcısı bulunmaktadır (11).

Soğuk Depolama - HSM Prosedürleri

Soğuk depolama yöntemleri, kripto paraların çevrimdışı ortamda tutulmasına dayanır ve bu sayede çevrimiçi tehditlere karşı en üst düzeyde koruma sağlar. Donanım Güvenlik Modülleri (Hardware Security Modules (HSM)) kullanılarak kripto varlıkların soğuk depolama yöntemleri ile belirli güvenlik riskleri barındırmasına rağmen güvence altına alınabilir.

Soğuk Depolama ve HSM Kullanımı

Soğuk depolama yöntemi, özel imzalama anahtarların çevrimdışı ortamlarda saklanması anlamına gelir ve bu sayede internet üzerinden yapılacak siber saldırılara karşı etkili bir koruma sağlar. Ancak, soğuk depolama çözümlerinin kullanımı bazı operasyonel zorlukları da beraberinde getirir.

Kripto varlıkların saklanması, işlenmesi ve transferi sırasında çok adımlı, zaman alıcı işlemler gerekebilir. Bu noktada, HSM kullanımı, gizli anahtarların güvenli bir ortamda tutulması ve bu anahtarlarla yapılan işlemlerin güvenli bir şekilde gerçekleştirilmesi konusunda kritik bir rol oynar. HSM'ler, özel olarak tasarlanmış kriptografik işlemcilerdir ve gizli anahtarların güvenli bir ortamda saklanmasını ve bu anahtarlarla yapılan şifreleme, kimlik doğrulama ve imzalama işlemlerinin yüksek seviyede güvenlikle gerçekleştirilmesini sağlar. Bu özellikleriyle, soğuk depolama sistemlerinde HSM kullanımı hem çevrimdışı hem de fiziksel güvenlik katmanlarını birleştirerek gizli anahtarların çok yönlü korunmasını sağlar.

HSM Prosedürleri ve Teknik Detaylar

1. Anahtar Yönetimi ve Anahtar Oluşturma

• HSM'ler, kripto varlıkların gizli anahtarlarının oluşturulması ve saklanması için kullanılır. Anahtarların oluşturulması sırasında HSM'ler, rastgelelik seviyesini maksimuma çıkartan Donanımsal Rastgele Sayı Üretimi (Hardware Random Number Generation) kullanır. Bu sayede, anahtarların tahmin edilmesi veya yeniden oluşturulması son derece zor hale gelir.

2. Anahtar Saklama ve Fiziksel Koruma

• HSM'ler, gizli anahtarları fiziksel olarak koruyabilmek için tamper-resistant (müdahaleye dayanıklı) bir tasarıma sahiptir. Fiziksel bir müdahale girişimi algılandığında HSM, içerisindeki tüm gizli anahtarları ve hassas verileri otomatik olarak siler. Bu özellik, gizli anahtarların herhangi bir şekilde fiziksel olarak ele geçirilmesini engeller.

3. Kriptografik İşlemler ve Kimlik Doğrulama

• HSM'ler, kriptografik işlemleri doğrudan kendi içerisinde gerçekleştirir ve gizli anahtarların hiçbir zaman cihazın dışına çıkmamasını sağlar. Örneğin, bir transfer işlemi yapılacağı zaman, ilgili gizli anahtar HSM tarafından kullanılarak imzalanır ve bu işlem sadece HSM içerisinde gerçekleştirildiği için dış tehditlere karşı tam bir koruma sağlanır.

4. Politika Tabanlı Güvenlik ve Yetkilendirme

• HSM tabanlı soğuk depolama yöntemlerinde, işlemler üzerinde ek güvenlik politikaları uygulanabilir. Örneğin, belirli transfer limitleri, beyaz listeye alınmış cüzdan adresleri ve harcama sınırları gibi parametreler HSM kurulumu sırasında tanımlanabilir. Bu sayede, her bir işlem, bu politikalarla uyumlu olup olmadığı kontrol edilir ve uygun olmayan işlemler reddedilir.

Soğuk Depolama - HSM Entegrasyonu ve Kullanım Zorlukları

HSM entegrasyonu, mevcut altyapıya entegre edilmesi sırasında teknik bilgi birikimi gerektiren karmaşık bir süreç olabilir. HSM'lerin başarılı bir şekilde entegrasyonu için aşağıdaki adımlar izlenmelidir:

• Planlama ve Uyumluluk: HSM entegrasyonunda, şirketin mevcut altyapısı ve operasyonel gereksinimlerinin dikkate alınarak detaylı bir planlama yapılmalıdır.

• Test ve Doğrulama: HSM kurulumu yapıldıktan sonra, bütün işlemlerin uyumlu bir şekilde çalışıp çalışmadığı test edilmelidir. Bu aşama, HSM'lerin sıkı şekilde test edilmesini ve herhangi bir uyumsuzluk durumunun giderilmesini içerir.

• Güvenlik ve Bakım: HSM'lerin güvenlik açıklarına karşı korunması için periyodik bakım ve firmware güncellemeleri yapılmalıdır.

• Fiziksel Güvenlik Önlemleri: HSM'lerin güvenli bir ortamda saklanması, yalnızca yetkili kişiler tarafından erişim sağlanması gereklidir. Fiziksel güvenlik zafiyetleri, cihazların yetkisiz kişilerin eline geçmesini engellemek adına kritik öneme sahiptir.

• Erişim Kontrolleri ve Yetkilendirme: HSM'lere erişim kontrol altında tutulmalıdır. Yalnızca gerekli yetkilere sahip olan bireyler erişim sağlamalıdır. Aksi takdirde, kötü niyetli bir yönetici HSM'leri kötü amaçlı kullanarak, kritik fonlara veya hassas verilere erişim sağlayabilir. Bu yüzden, yetkilendirme seviyelerinin belirlenmesi ve yönetilmesi büyük önem taşır.

Saklama Sürecinde Karşılaşılan Tehditler ve Zorluklar

Dijital varlıkların hızla yaygınlaşması, finansal kurumlar için büyük fırsatlar sunmakla birlikte, yeni zorluklar ve tehditler de doğurmaktadır. Bu varlıkların güvenli bir şekilde saklanması, yalnızca teknik altyapı ve güvenlik önlemleriyle sınırlı olmayıp, aynı zamanda regülasyonlar, insan faktörü ve teknolojik riskler gibi geniş bir alanı kapsamaktadır. Kurumlar, dijital varlıkların korunmasıyla ilgili karşılaştıkları karmaşık zorlukları ve artan tehditleri anlamak ve yönetmek zorundadır. Bu süreçte tek bir çözüm yoktur; güvenilir yaklaşımlar, teknoloji ve prosedürlerin dengeli bir kombinasyonunu gerektirmektedir.

Dijital varlıkların saklanması süreçlerinde, varlıkların sahipliğini ve kontrolünü sağlamak için kriptografik tekniklerin kullanılması, akıllı sözleşmelerle güvenli etkileşim sağlanması ve tokenize menkul kıymetler için destek sunulması gibi her aşamada birden çok kontrol noktası yer almalıdır. Dış saldırganlar, içerideki tehditler veya kazara meydana gelen arızalara karşı, gizli anahtarların korunması; veri bütünlüğü, anahtarların geri yüklenebilirliği ve denetim izi gibi unsurların yanı sıra yazılım açıkları ve istismarlarına karşı teknik güvenlik önlemleri devreye sokulmalıdır. Ayrıca, güvenlik protokollerinin belirlenmesi (çok taraflı onay, tek oturum açma, felaket kurtarma gibi), güvenilir donanım kullanımı ve kriptografik protokollerin güvenlik seviyesi gibi güven varsayımları da prosedürel ve teknik güvenlik kontrollerinin bir parçası olarak değerlendirilmelidir.

Saklama mekanizması ne olursa olsun, (sıcak, ılık ya da soğuk) tohumların (seed) veya gizli anahtarların güvenli bir şekilde saklanması hayati önemdedir. En önemli hedeflerinden biri, bu tohumlara ya da anahtarlara yetkisiz erişimi engellemektir, aksi takdirde fonlar tehlikeye girebilir. Onay kurallarını manipüle etme girişimlerini önlemek için, genellikle belli bir oy çokluğuna dayanan bir onay mekanizması oluşturulması gerekmektedir. Bu mekanizma ile, belirli adreslerin beyaz listeye alınması, işlem tutarı sınırlarının belirlenmesi ve akıllı sözleşmelerde izin verilen eylemlerin belirlenmesi gibi eylemler tanımlanmalıdır. Platformun meşru kullanıcıları, gizli anahtarlara doğrudan erişmeden, onay mekanizmasından geçerek işlemleri imzalanmalıdır.

Yedekleme işlemleri, yetkisiz erişimi engellemek için çok katmanlı erişim kontrolü ile donatılmış güvenli ve kontrollü bir ortamda gerçekleşmelidir. Yedekleme süreci doğrulanabilir olmalı ve yedekleme bütünlüğü düzenli olarak kontrol edilmelidir. Anahtar üretimi ve yedekleme yönetiminde görev alan personelin, güvenlik protokollerine tam uyum sağlaması için kapsamlı geçmiş kontrollerinden ve eğitimden geçmesi gerekmektedir. Yedekleme sistemlerinin düzenli olarak test edilmesi, diğer kontrollerle entegrasyonunun sağlanması ve felaket kurtarma planları ile acil durum prosedürlerine entegre edilmesi zorunludur.

Bu zorlukların yanı sıra, dinamik bir sektör olan kripto para dünyasında kullanıcı arayüzü ve kullanıcı deneyimi büyük önem taşımaktadır. Bu iki faktör, müşterilerin tercihlerini doğrudan etkilemektedir. Bu nedenle, kullanıcı güvenliğini ön planda tutarken, deneyimi olumsuz etkilemeyecek tasarımlar yapılmalıdır. Güvenlik, şirketin itibar riskini etkilerken, kullanıcı deneyimi de uygulamanın benimsenmesini doğrudan etkileyecektir.

Siber Güvenlik Tehditleri ve Risk Yönetimi

Blokzincir tabanlı sistemlerdeki siber güvenlik tehditleri, yetkisiz erişim, kimlik avı (phishing) saldırıları, hizmet reddi (Distributed Denial of Service (DDoS) saldırıları) ve akıllı sözleşme zafiyetleri şeklinde çeşitlenmektedir. Dijital varlıkların saklanması söz konusu olduğunda, özellikle özel (gizli) anahtarların ele geçirilmesi ve güvenlik mimarilerinin açıklarının bulunması ciddi tehditler arasındadır.

• Yetkisiz Erişim: Saklama cüzdanlarına yönelik kaba kuvvet (brüte force) saldırıları ve güvenlik açıkları üzerinden gerçekleşen saldırılar, dijital varlıklara doğrudan erişim sağlar. Özellikle merkeziyetsiz cüzdanlarda, zayıf anahtar yönetimi sistemleri saldırganlar tarafından hedeflenmektedir.

• Kimlik Avı (Phishing) Saldırıları: Kullanıcıları yanıltarak gizli anahtarları veya cüzdan erişim bilgilerini ele geçirme amaçlı sosyal mühendislik saldırılarıdır. Gelişmiş URL sahteciliği (spoofing) ve Evil Twin (sahte kablosuz erişim noktası (Wi-Fi) saldırısı) teknikleri kullanılarak kurumsal erişimler hedef alınmaktadır.

• DDoS Saldırıları: Saklama kuruluşlarının API erişim noktaları veya ağ altyapısı, koordineli botnet saldırıları ile hedef alınarak sistem performansı düşürülür ve hizmet kesintileri yaşanır.

Risk yönetimi, siber tehditlerin önceden tespiti ve anında müdahale süreçlerini içeren çok katmanlı güvenlik stratejilerini gerektirir. Saklama kuruluşları, tehditleri minimize etmek için proaktif güvenlik protokolleriyle entegre çalışan aşağıdaki teknikleri kullanmalıdır:

Penetrasyon Testleri (Pen Testing) Saklama altyapısının güvenlik açıklarını tespit etmek amacıyla gerçekleştirilen simülasyon saldırılarıdır.	Beyaz Kutu Testi (White Box Testing): İç sistem mimarisi ve kod yapılarına yönelik analizlerdir. Siyah Kutu Testi (Black Box Testing): Saldırgan perspektifinden dış erişim noktalarının test edilmesidir. Gri Kutu Testi (Gray Box Testing): Kısmi bilgilere dayalı güvenlik testleridir.
Sıfır-Gün (Zero-Day) Saldırı Analizleri Bilinmeyen güvenlik açıklarından faydalanan saldırıları tespit etmek için davranış tabanlı anomali tespiti ve tehdit istihbaratı kullanılmalıdır. Yapay zekâ ve makine öğrenimi algoritmaları, sıfır-gün tehditlerini algılamakta önemli bir rol oynamaktadır.	Intrusion Detection Systems (IDS) ve Intrusion Prevention Systems (IPS) kullanarak anlık veri analizi sağlanmalıdır. Sandboxing: Güvenlik açığı içeren kodların yalıtılmış ortamlarda analiz edilmesi ile tehditlerin anında tespit edilmesi sağlanır.
Anlık Tehdit Tespiti (Real-Time Threat Detection) Sürekli izleme ve log analiz sistemleri kullanılarak, sistemdeki olağandışı aktiviteler belirlenir.	SIEM (Security Information and Event Management): Log verilerini gerçek zamanlı analiz ederek potansiyel tehditleri tespit eden entegre çözümlerdir. Anomali Tespiti: Ağ trafiği, işlem davranışları ve sistem erişimleri üzerinde anormallik analizleri gerçekleştirilir.

Gelişmiş risk analizi, siber güvenlik tehditlerini sürekli olarak değerlendiren ve sistemin dayanıklılığını artıran yöntemlerden oluşur. Saklama kuruluşlarının güvenlik seviyesini artırmak için kullanılan tekniklerden bazıları şunlardır:

• Tehdit Modelleme: Sistematik olarak potansiyel güvenlik risklerini analiz eden bir yaklaşımdır. Saklama altyapısının her katmanı detaylı olarak değerlendirilir:

  • Stride Modeli: Kimlik Sahtekarlığı (Spoofing), Yetkisiz Değiştirme (Tampering), İnkar Edilebilirlik (Repudiation), Bilgi Açığı (Information Disclosure), Hizmet Reddi (DDoS), Yetki Yükseltme (Elevation of Privilege) riskleri üzerinden tehditlerin sınıflandırılması.

• Kriptografik Güvenlik: Saklama çözümlerinde kriptografik algoritma ve protokollerinin güvenliği ve dayanıklılığı risk analizinde kritik rol oynar:

• Post-Quantum Kriptografi: Kuantum bilgisayarların, geleneksel kriptografi algoritmalarını kırma riskine karşı dayanıklı çözümler geliştirilmelidir.

• Gelişmiş Anahtar Yönetimi: Anahtar rotasyonu, çoklu imza (Multi-Sig) protokolleri ve dağıtık anahtar yönetimleri (örn. Shamir Secret Sharing) teknikleri uygulanmalıdır.

DREAD Analizi: DREAD Analizi, güvenlik risklerinin değerlendirilmesinde kullanılan bir çerçevedir. Microsoft tarafından geliştirilen bu yöntem, tehditleri sınıflandırarak etkilerini daha sistematik bir şekilde analiz etmeyi sağlar. DREAD, 5 temel kriter üzerinden risk değerlendirmesi yapar ve bu kriterlerin baş harflerinden oluşur:

DREAD ANALİZİ

Damage Potential (Zarar Potansiyeli	Bir saldırı gerçekleştiğinde hedef sisteme ne kadar zarar verebilir? Örneğin, veri tabanı ele geçirilirse hassas bilgiler sızdırılır mı? Veya sistem tamamen devre dışı mı kalır? Bunu engellemek için kritik sistemler üzerinde çok katmanlı güvenlik önlemleri uygulanmalıdır (örneğin, erişim kontrolleri, veri şifreleme).
Reproducibility (Yinelenebilirlik)	Saldırının ne kadar kolay tekrarlanabileceği analiz edilir. Örneğin, bir saldırı yöntemi, her denemede başarılı sonuç veriyor mu? Bu sorunu gidermek için sistemin güvenlik açıkları düzenli olarak tespit edilip yamalanmalıdır (örneğin, penetrasyon testleri ve güvenlik yamaları).
Exploitability (Sömürülebilirlik)	Saldırının ne kadar kolay gerçekleştirilebileceğini ifade eder. Örneğin, saldırı için karmaşık teknik bilgi veya özel donanım gerekiyor mu, yoksa düşük teknik seviyede saldırganlar bile bunu yapabilir mi? Bunun için çok faktörlü kimlik doğrulama sistemleri (MFA), erişim yetkilendirmesi ve yazılım güvenlik standartlarının uygulanması gerekir.
Affected Users (Etkilenen Kullanıcılar)	Saldırı sonucunda kaç kullanıcı veya sistemin etkilenebileceğini gösterir. Örneğin, küçük bir kullanıcı grubu mu yoksa geniş çapta bir etki alanı mı var? Bu nedenle, segmentasyon (bölümlendirme) ve yetki bazlı erişim kontrolleri ile potansiyel hasarın etkisi sınırlandırılmalıdır.
Discoverability (Keşfedilebilirlik)	Güvenlik açığının ne kadar kolay keşfedilebileceği değerlendirilir. Örneğin, açık herkes tarafından görülebilir mi, yoksa karmaşık analizler sonucu mu keşfedilebilir? Bunu engellemek için güvenlik zafiyet tarama araçları ve sürekli izleme sistemleri kullanılarak tehditler önceden tespit edilmelidir.

1. Varlıkların ve Müşteri Haklarının Korunması

• Saklama kuruluşları, emanet edilen varlıkları ve müşterilerin haklarını kayıptan ve kötüye kullanımdan, özellikle iflas durumunda korumalıdır.

• Operasyonel kontroller, siber dayanıklılık ve riskleri minimize eden saklama politikaları oluşturulmalıdır.

• Müşteri varlıklarına ilişkin doğru ve güncel kayıtlar tutulmalı, bu kayıtlar müşterilerin varlıklarını açıkça göstermelidir.

2. Varlıkların Ayrıştırılması ve Yeniden Kullanım

• Ayrıştırma: Emanet edilen kripto varlıklar, saklama kuruluşunun kendi varlıklarından tamamen ayrı tutulmalıdır.

• Yeniden Kullanım ve Mülkiyet Transferi: Müşteri varlıklarının mülkiyet transferi veya yeniden kullanımı yalnızca müşterinin önceden açık rızası ve kapsamlı ön bilgilendirme ile yapılabilir.

3. Dış Kaynak Kullanımı ve Ek Risk Yönetimi

• Eğer saklama hizmetleri dış kaynaklara devredilirse, benzer güvenlik önlemleri uygulanmalı ve müşteriler bu konuda bilgilendirilmelidir.

• Ek risk yönetimi mekanizmaları devreye alınmalıdır.

4. Şeffaflık Sağlama

Saklama kuruluşları, saklama sözleşmesinden doğan haklar ve yükümlülükler, güvenlik düzenlemeleri, dış kaynak kullanımı, omnibus hesapların (birden fazla müşterinin varlıklarının birleştirildiği hesaplar) kullanımı, müşteri varlıklarının yeniden kullanımına ilişkin düzenlemeler ve bu uygulamalardan doğabilecek risklere ilişkin konularda şeffaflık sağlamalıdır.

5. Çok İşlevli Hizmet Sağlayıcılar için Ek Önlemler

• Saklama hizmeti sunan ve diğer kripto varlık hizmetlerini de sağlayan kuruluşlar için çıkar çatışmalarını tanımlamalı, açıklamalı ve yönetmelidir.

• İşlevlerin zorunlu olarak ayrılması veya iş kollarının tamamen ayrıştırılması gerekmektedir.

6. Müşteri Koruması ve Finansal Güvence

• Müşteri fonlarının korunması ve ayrıştırılması regülatörler tarafından zorunlu tutulmaktadır.

• Saklama kuruluşları, müşteri varlıklarının kaybı veya çalınması durumunda tazmin sağlamak için ek özkaynaklara sahip olmalı ya da garanti mekanizmalarına katılmalıdır.

• Sigorta kapsamı sunarak varlıkların güvencesini sağlamalıdır.

7. Acil Durum ve Hesap Mutabakatı

• IMF Önerisi: Saklama kuruluşlarının etkin bir tasfiye planı oluşturması gereklidir.

• IOSCO Önerisi: Zincir içi (on-chain) ve zincir dışı (off-chain) mutabakatlar düzenli ve doğru bir şekilde gerçekleştirilmelidir.

8. Blokzincir Ağ Güvenliği

Saklama altyapısının çalıştığı blokzincir ağında, konsensüs algoritması ve akıllı sözleşme denetimleri, herhangi bir güncelleme olabileceği için düzenli olarak gözden geçirilmelidir.

9. Sıfır Güven (Zero Trust) Mimarisi

Her erişim noktasının sürekli olarak doğrulama mekanizmalarından geçirilmesi sağlanmalıdır. Kullanıcı, cihaz ve uygulama güvenliği ayrı ayrı kontrol edilmelidir.

10. Yapay Zekâ Destekli Öngörücü Analiz (Artificial Intelligence-Powered Predictive Analytics)

Siber güvenlik tehditlerini tahmin eden, veriye dayalı karar mekanizmaları kullanılarak riskler minimize edilmelidir.

Risk Yönetiminde Çok Katmanlı Yaklaşım

Dijital varlıkların güvenliğini sağlamak için çok katmanlı bir yaklaşım gereklidir. Bu yaklaşım hem teknik güvenlik önlemlerini hem de operasyonel süreçlerin sürekli değerlendirilmesini içerir.

1. Güvenlik Metrikleri ve Değerlendirme

• Risk yönetiminde ölçülebilir güvenlik metrikleri kullanılır. Örneğin:
• Sistemin çalışma süresi (uptime) oranı
• Sıfır-gün saldırılarına karşı güncelleme hızları
• Penetrasyon test sonuçları
• Anomali tespit sistemlerinin doğruluk oranı

2. Sürekli Güvenlik Değerlendirmesi

• Saklama platformlarının güvenlik zafiyetleri düzenli olarak değerlendirilmeli ve penetrasyon testleri gerçekleştirilmelidir.

• Kırmızı Takım (Red Team) ve Mavi Takım (Blue Team) çalışmaları veya Hata Ödül (Bug Bounty) Programı gibi yöntemler kullanılarak sistemin güvenlik açıkları sürekli olarak test edilmelidir. Bu programlar kapsamında, sistem sahipleri güvenlik açıklarını bulmak ve raporlamak için beyaz şapkalı hackerlara (Ethical Hackers) ödül sunar. Bu sayede hem açıklar kapatılır hem de güvenlik seviyesi artırılır.[1]

3. Zayıf Noktaların Raporlanması ve Giderilmesi

• Saldırı simülasyonları ve öngörücü analiz sistemleri kullanılarak zayıf noktalar proaktif olarak belirlenir.

• Bu açıkların giderilmesi, Sıfır Güven Mimarisi (Zero Trust Architecture) gibi güvenlik modelleriyle entegre edilir.

Saklama Kuruluşlarının Risk Yönetimi Politikaları

Saklama kuruluşlarının risk yönetimi politikaları, dijital varlıkların güvenliğini sağlamak, operasyonel aksaklıkları azaltmak ve çeşitli tehditlere karşı dayanıklılığı artırmak amacıyla geliştirilmiş kapsamlı stratejik çerçevelerden oluşur. Risk yönetimi politikalarının;
1. Yapı taşı,
2. Risk tanımlama,
3. Ölçüm,
4. Kontrol ve İzleme
aşamaları olmak üzere 4 temel adımdan oluşur. Bu süreçler, teknolojik, operasyonel, yasal ve piyasa risklerini ele alacak şekilde detaylandırılır.

Teknolojik Riskler

Teknolojik riskler, dijital varlıkların güvenliğiyle doğrudan ilgili olan risklerdir ve özellikle gizli anahtarların korunması, blokzincir ağlarının güvenliği ve çevresel altyapıların zafiyetleri üzerinden şekillenir. Dijital varlıkların kontrolü, gizli anahtarların bütünlüğüne bağlı olduğundan, bu alandaki güvenlik açıkları büyük finansal kayıplara yol açabilir. Bunu sağlamak için olası çözüm yöntemleri ve uygulamaları şu şekilde sıralanır.

1. Anahtar Yönetimi Protokolleri

• Donanım Güvenlik Modülleri (HSM): Gizli anahtarların fiziksel güvenliği için çevrimdışı HSM'ler kullanılır. Bu cihazlar, anahtarların yetkisiz erişime karşı korunmasını sağlar ve kurcalandığında otomatik olarak verileri imha eder.

• Çoklu İmza (Multi-Sig) ve MPC: Gizli anahtarların parçalar halinde tutulması ve işlemler için birden fazla yetkilinin onayının gerekmesi, tek bir hata noktasını ortadan kaldırır.

2. Çift-Yönlü İmzalama Sistemleri ve Zaman Damgalı işlemler

• Çift Taraflı Kimlik Doğrulama (Mutual Authentication): Çift yönlü kimlik doğrulama ile sistemler arasında güvenli iletişim sağlanır ve üçüncü taraf (orta adam) saldırıları engellenir.

• Çok faktörlü doğrulama (MFA): Anahtar yönetiminde ek bir güvenlik katmanı olarak kullanılarak yetkisiz erişim riski azaltılır.

• Zaman Damgalı İşlem Onayları: Kullanıcıların işlem detaylarını doğrulaması için belirli zaman aralıkları tanımlanır ve işlem izleme mekanizmaları entegre entegre edilerek güvenlik artırılır.

3. Blokzincir Güvenliği

• Akıllı Sözleşme Denetimleri: Akıllı sözleşmeler geliştirme aşamasında kapsamlı güvenlik denetimlerinden geçirilmelidir. Bu süreçte:

• Kod İnceleme: Manuel ve otomatik kod analiz araçları (örneğin, Slither, MythX, Manticore) kullanılarak hatalar ve zafiyetler tespit edilmelidir.

• Denetim (Audit): Bağımsız güvenlik firmaları tarafından detaylı akıllı sözleşme denetimleri gerçekleştirilmelidir.

• Testnet Üzerinde Testler: Ana ağa göndermeden önce testnet üzerinde sözleşme fonksiyonlarının güvenliği ve performansı test edilmelidir.

• Gas Optimizasyonu ve Denetimleri: Akıllı sözleşme saldırılarında yüksek gas ücretleri bazen istismar edilebilir; bu yüzden optimizasyon yapılmalıdır.

• Sıfır Gün Saldırılarına Karşı Analizler: Proaktif güvenlik önlemleriyle yeni bulunan zafiyetlere karşı hızlı aksiyon alınmalıdır.

• Akıllı sözleşme güncellemelerini mümkün kılmak için proxy sözleşmeler gibi yükseltilebilir (upgradeable) sözleşme yapıları tercih edilebilir.

• Güvenlik açıkları tespit edildiğinde, çoklu imza (multisig) yetkilendirme mekanizmaları kullanılarak acil durum aksiyonları uygulanabilir.

• Güvenli Dağıtım Süreçleri: Akıllı sözleşmelerin blokzincire dağıtımından önce sözleşme sahibi anahtarlarının güvenliği sağlanmalı ve yetkisiz erişim riskleri ortadan kaldırılmalıdır.

Operasyonel Riskler

Operasyonel riskler, insan hataları, süreçlerdeki eksiklikler ve sistem kesintileri gibi unsurlardan kaynaklanır. Bu riskler, genellikle kurumsal prosedürlerin zayıflığı ve yetersiz otomasyon nedeniyle ortaya çıkar. Çözüm yöntemleri ve uygulamalar şu şekilde listelenebilir.

1. Otomatik Doğrulama ve İzleme Sistemleri

• İşlemlerin manuel olarak onaylanmasını minimize eden otomatik doğrulama sistemleri, hata oranını önemli ölçüde azaltır.

• Şüpheli işlem aktivitelerini tespit eden makine öğrenimi tabanlı (Anomali Tespit) sistemler, gerçek zamanlı uyarılarla olası operasyonel hataların önüne geçer.

2. Yetki Bazlı Erişim Kontrolleri (Role Based Access Control (RBAC))

• Her çalışanın sistem üzerinde yalnızca yetkisi dahilindeki bilgilere erişebilmesi sağlanır. Yetki seviyeleri düzenli olarak gözden geçirilir ve güncellenir. Kullanıcılar, görevlerini yerine getirebilmek için sadece gerekli yetkilere sahip olmalıdır.

3. İş Sürekliliği ve Acil Durum Planları

• Sistem kesintileri veya siber saldırılar gibi durumlarda acil müdahale planları devreye alınır. Yedekleme mekanizmaları, varlıkların erişilebilirliğini garanti altına alır.

Yasal Riskler

Yasal riskler, düzenleyici kurumların belirlediği standartlara uyum sürecinde yaşanan belirsizlikler ve uyumsuzluklar nedeniyle oluşan risklerdir. Dijital varlık ekosistemi, dünya genelinde farklı regülasyonlara tabi olduğundan saklama kuruluşları için bu riskler kaçınılmazdır. Aşağıda bazı çözüm yöntemleri ve uygulamaları listeleyeceğiz.

1. Kara Parayı Aklamayı Önleme (AML) ve Terörizmin Finansmanının Önlenmesi (CFT) Politikalarına Uyum

AML, kara para aklamanın önlenmesi anlamına gelir. Finansal sistemlerin, suç gelirlerinin yasal yollardan dolaşıma sokulmasını engellemeye yönelik politikalar, prosedürler ve düzenlemeleri kapsar. CFT ise terörizmin finansmanının önlenmesi anlamına gelir. Terörist faaliyetleri finanse etmek amacıyla yapılan para akışlarının tespit edilmesi, engellenmesi ve cezalandırılmasını sağlayan tedbirlerdir. Bu iki kavram birlikte kullanıldığında, finansal kuruluşların ve dijital saklama hizmeti sağlayıcılarının kara para aklama faaliyetlerini ve terörizmin finansmanını önlemek için uyguladıkları yasal uyum çerçevelerini ifade eder. Özellikle kripto varlıklar ve dijital saklama hizmetleri alanında, AML/CFT politikaları büyük önem taşır. Bu çerçevede müşteri tanıma prosedürleri (KYC), şüpheli aktivite raporlama (SAR), şüpheli işlem raporlama (STR), ve finansal işlemlerin sürekli gözetimi gibi süreçler uygulanır.

• Müşteri Tanıma (KYC – Know Your Customer): Saklama platformları, müşterilerin kimliklerini doğrulamak ve AML/CFT politikalarına uyum sağlamak için güçlü KYC süreçlerini kullanır.

• Şüpheli Aktivite Raporlama (SAR- Suspicious Activity Reporting): Olası kara para aklama faaliyetlerini tespit eden sistemlerle anlık analiz yapılır ve raporlar düzenleyici kurumlara iletilir. Finansal kurumlar, belirli şüpheli faaliyetleri yetkili kurumlara raporlamakla yükümlüdür.

• Şüpheli İşlem Bildirimi (STR- Suspicious Transaction Reporting): Olası kara para aklama ve terörizmin finansmanı faaliyetlerini tespit eden sistemler aracılığıyla detaylı analizler yapılır ve şüpheli işlemler raporlanarak düzenleyici kurumlara iletilir. Finansal kurumlar, belirli şüpheli işlemleri zamanında yetkili kurumlara bildirmekle yükümlüdür.

2. Risk Transferi

• Yasal risklerin azaltılması için sigorta sağlayıcılarıyla yapılan risk transferi sözleşmeleri, siber güvenlik ihlalleri veya operasyonel kayıplarda tazminat sağlar.

3. Düzenleyici Çerçeveye Uyum Programları

• Bölgesel regülasyonlar (örneğin MiCA, SEC, FCA)[2] doğrultusunda iç denetim mekanizmaları oluşturulur ve bağımsız denetim firmaları tarafından düzenli kontrol sağlanır.

Piyasa Riskleri

Piyasa riskleri, dijital varlıkların yüksek değişkenli doğasından kaynaklanan fiyat dalgalanmalarını ve likidite risklerini kapsar. Kripto varlık piyasalarının hızlı fiyat değişimleri, saklama kuruluşlarını değer kaybı riskine maruz bırakabilir. Aşağıda bunun için bazı çözüm yöntemleri listelenmiştir.

1. Dinamik Varlık Değerleme Yöntemleri:

• Dijital varlıkların piyasa değerleri, gerçek zamanlı veri akışları ve yapay zekâ destekli analiz araçları kullanılarak sürekli olarak izlenebilir.

2. Portföy Çeşitlendirilmesi:
• Saklama kuruluşları, volatiliteyi dengelemek için müşterilerin varlık portföylerinde farklı dijital varlık türleri sunabilir.

3. Hedging Stratejileri:
• Türev ürünler ve opsiyon sözleşmeleri, piyasa dalgalanmalarına karşı riskten korunmak için kullanılabilir.

4. Stres Testleri ve Simülasyonlar:
• Olası piyasa şoklarının etkilerini ölçmek için düzenli olarak stres testleri gerçekleştirilir. Bu testler, kuruluşların kriz anındaki dayanıklılığını değerlendirebilir.

AML/CFT Kontrolleri

Kripto saklama kuruluşlarında Kara Para Aklama (AML) ve Terörizmin Finansmanıyla Mücadele (CFT) kontrolleri, yasa dışı faaliyetlerin önlenmesi ve uluslararası uyumluluğun sağlanması ve yerel düzenlemelere uyum açısından oldukça önemlidir. Bu kontroller, finansal ve teknolojik risklerin yönetilmesi amacıyla sıkı prosedürler ve politikalar gerektirir. Bu anlamda, kripto saklama kuruluşlarında uygulanabilecek başlıca AML ve CFT kontrolleri müşterini tanı (KYC) prosedürlerinin işletilmesiyle başlar. KYC kapsamında müşterilerin kimlik ve adres doğrulama işlemleri gerçekleştirilerek risk seviyeleri değerlendirilip risk profilleri oluşturulur. Müşteri segmentasyonunun belirlendiği, yüksek riskli ülkeler ya da bu bölgelerden işlemlerin yakından izlendiği, yüksek riskli işlemlere ilişkin ek inceleşerin gerçekleştirileceği risk odaklı bir yaklaşım benimsenir.

İşlemlerin takibi için otomatik işlem izleme sistemleri aracılığıyla şüpheli işlemleri tespit etmek için blok zinciri analiz araçları ve yazılımları kullanılarak ve bu şüpheli işlemlerin raporlamasının yasal otoritelere gerçekleştirilmesi sağlanır. Ek olarak, uluslararası yaptırım listelerine (OFAC, FATF vb.) uyumluluk ve kara liste kontrollerinin işletimi sağlanır. Yasadışı faaliyetleri tespit etmek için zincir üzerindeki işlemleri analiz eden uygulamalar tedarik edilebilir. Bu anlamda, kripto saklama kuruluşları destek hizmeti sağlayıcıları ve iş ortaklarının AML/CFT standartlarına uygunluğunu da sağlamalıdır.

Özetle, kripto saklama kuruluşlarında bu kontrollerin uygulanması hem yasal yükümlülüklere uyumu sağlamak hem de müşteri ve piyasa güvenini artırmak açısından kritiktir. Kripto saklama kuruluşları, AML ve CFT gereksinimlerini karşılamak için hem teknolojik hem de yetkin ve tecrübeli uyum çalışanlarına yatırım yapmalıdır.

1. Müşteri Kimlik Doğrulama (KYC) ve Sürekli İzleme

AML/CFT politikalarının temelinde KYC süreçleri yer alır. KYC, saklama hizmeti sağlayıcılarının müşteri kimliklerini doğrulamasını ve bu bilgileri düzenli olarak güncellemesini içerir:

• Kimlik ve Adres Doğrulama: Dijital saklama kuruluşları, kullanıcıların kimlik belgeleri (pasaport, ehliyet, ulusal kimlik kartı vb.) ve adres bilgilerini doğrulamak için biyometrik doğrulama ve optik karakter tanıma (OCR) gibi teknolojiler kullanır.

• Risk Tabanlı Değerlendirme: Müşteriler, faaliyetlerine ve işlem geçmişine göre düşük, orta veya yüksek riskli olarak sınıflandırılır. Bu sınıflandırma, müşteri davranışlarının anlık izlenmesi ve risk puanlama sistemleri ile desteklenir.

KYC süreçlerinin tek seferlik bir uygulama olmadığı unutulmamalıdır. Müşteri profilleri ve işlem aktiviteleri düzenli olarak analiz edilerek şüpheli işlem modelleri tespit edilir.

2. Blokzincir Analiz Araçları ile Şüpheli İşlem Tespiti

Blokzincir analiz araçları, AML/CFT kontrollerinin teknik boyutunu oluşturarak dijital varlık transferlerinde şeffaflığı artırır ve yasa dışı faaliyetleri tespit eder:

• İşlem İzleme ve Pattern Analizi: Blokzincir tabanlı analiz yazılımları (örneğin, Chainalysis, Elliptic, ve CipherTrace), dijital varlık transferlerini gerçek zamanlı olarak izleyerek anormal işlem kalıplarını tespit eder.

• Riskli Adres ve Kara Liste Kontrolü: Blokzincirde yer alan riskli veya kara listeye alınmış adreslerle ilişkili transferler otomatik olarak işaretlenir ve gerekli raporlama mekanizmaları devreye girer.

• Parçalanmış Transferlerin Tespiti: Kara para aklama amaçlı "smurfing" gibi tekniklerle yapılan mikro transferler analiz edilerek, bu işlemler zincir üzerinde birleşik bir model olarak incelenir.

Bu araçlar, özellikle "dark web" bağlantıları, riskli borsalar ve sahte kimlik kullanımı gibi tehditlere karşı etkin çözümler sağlar.

3. Otomatik Risk Puanlama ve Şüpheli İşlem Raporlama (SAR/STR)

Dijital varlık saklama kuruluşları, AML/CFT politikaları kapsamında otomatik risk puanlama sistemlerini kullanarak müşteri aktivitelerini sürekli değerlendirir:

• Risk Skorlama Algoritmaları: Yapay zekâ ve makine öğrenimi algoritmaları, müşterilerin işlem geçmişini analiz ederek dinamik risk skorları oluşturur.

• Şüpheli İşlem Raporlama (SAR/STR): Yüksek risk taşıyan veya şüpheli görülen işlemler, düzenleyici kurumlara raporlanır. SAR (Suspicious Activity Reporting) mekanizması, uluslararası AML standartlarına uygun olarak kullanılır.

4. Uluslararası Düzenleyici Uyum (FATF Standartları)

AML/CFT politikalarının etkinliği, uluslararası düzenleyici standartlara uyum ile ölçülür. Özellikle, FATF (Financial Action Task Force) tarafından belirlenen kurallar, global düzeyde bir çerçeve sunar:

• Seyahat Kuralı (Travel Rule): FATF'nin belirlediği Seyahat Kuralı, dijital varlık transferlerinde gönderen ve alıcı tarafların kimlik bilgilerinin toplanmasını ve paylaşılmasını zorunlu kılar. Bu, transferlerin anonim kalmasını engelleyerek yasa dışı faaliyetleri sınırlar.

• Düzenli Denetimler: Saklama hizmeti sağlayıcıları, düzenleyici kurumlar tarafından gerçekleştirilen periyodik denetimlere tabi tutulur. Bu denetimler, AML/CFT uyum politikalarının etkinliğini değerlendirir.

5. Veri Gizliliğinin Sağlanması

AML/CFT kontrolleri uygulanırken, veri gizliliği de göz önünde bulundurulmalıdır:

• KVKK (Kişisel Verilerin Korunması Kanunu), GDPR (General Data Protection Regulation) ve Diğer Veri Koruma Mevzuatlarına Uyum: Müşteri verileri, global veri koruma mevzuatlarına uygun olarak toplanmalı ve saklanmalıdır.

• Şeffaflık ve İzinli Erişim: Müşteri bilgilerine yalnızca yetkili personelin erişebilmesi sağlanarak veri sızıntıları ve yetkisiz erişim engellenir.

Denetim Süreçleri ve Uluslararası Standartlar

Bağımsız denetim firmalarının dijital varlık saklama hizmetleri için gerçekleştirdiği değerlendirmeler, uluslararası kabul görmüş standartlara dayanır. Bunlar arasında en yaygın kullanılanları şunlardır:

1. SOC 1/SOC 2 Raporlaması:
• SOC 1 (Service Organization Control 1): Finansal raporlama üzerinde kontrollerin etkinliğini test eder. Bu rapor, özellikle dijital varlık saklama hizmetlerinin finansal sistemlere entegrasyonunda güven sağlar.

• SOC 2 (Service Organization Control 2): Güvenlik, erişim kontrolü, sistem bütünlüğü, gizlilik ve veri koruma gibi teknik unsurların denetlenmesini kapsar. Bu rapor, dijital varlıkların saklanmasında kullanılan altyapıların güvenliğini değerlendirmede kritik rol oynar.

2. ISAE 3000 (International Standard on Assurance Engagements): Uluslararası Güvence Standartları'na dayanan ISAE 3000, veri güvenliği, süreç doğruluğu ve uyum açısından derinlemesine incelemeler sunar. Dijital varlık saklama hizmetlerinin siber güvenlik protokolleri ve operasyonel risk yönetimi bu standart çerçevesinde değerlendirilir.

3. ISO 27001 Sertifikasyonu: Bilgi güvenliği yönetim sistemlerinin standardizasyonunu sağlar. ISO 27001 kapsamında, dijital varlık saklama hizmeti sağlayıcılarının veri güvenliği politikaları, şifreleme teknikleri ve erişim kontrol mekanizmaları detaylı bir şekilde incelenir.

4. Akıllı Sözleşme Güvenliği ve Kod Denetimi: Bağımsız denetim firmaları, akıllı sözleşme güvenliğini sağlamak için kod incelemeleri ve formel doğrulama teknikleri kullanır. Özellikle blokzincir tabanlı platformlarda kullanılan akıllı sözleşmelerin hata toleransı, mantıksal tutarlılığı ve siber saldırılara karşı dayanıklılığı analiz edilir. Bu süreç, güvenlik açıklarının giderilmesine ve sistemlerin sürdürülebilirliğine katkı sağlar.

Denetim Sürecinde Odak Alanları

Bağımsız denetim firmaları, dijital varlık saklama hizmetlerini değerlendirirken şu alanlara odaklanır:

• Siber Güvenlik Protokolleri: Şifreleme yöntemlerinin doğruluğu, sızma testleri (penetration testing) ve ağ güvenliği değerlendirmeleri gerçekleştirilir.

• Operasyonel Kontroller: İş sürekliliği planları (Business Continuity Plans), sistem yedekleme ve kurtarma protokolleri analiz edilir.

• Uyum Yönetimi: AML/CFT politikalarının uygulanması, KYC süreçleri ve veri koruma standartlarının denetimi yapılır.

• Risk Yönetimi: Zayıf noktaların tespiti, risk azaltma stratejilerinin etkinliği ve olay müdahale planlarının uygunluğu değerlendirilir.

Güvenlik standartları açısından saklama kuruluşu soğuk (çevrimdışı) depolama, çoklu imzalı cüzdanlar, çok taraflı hesaplama (MPC), biyometri ve donanım güvenlik modülleri gibi en son siber güvenlik önlemlerini kullanılır. Rezerv kanıtı gibi protokoller düzenli olarak denetimlerden geçer. Sigorta kapsamı aracılığıyla ek koruma katmanları sağlanabilir. ISO, SOC ve CCSS gibi güvenlik sertifikaları da alınması gereken önemli belgeler arasında değerlendirilebilir. Gelişmiş siber güvenlik önlemleri arasında penetrasyon testi, veri şifreleme, dağıtılmış hizmet reddi (DDoS) saldırılarına karşı savunma ve ihlalleri ve veri kaybını önlemek için sürekli izleme faaliyetleri yer alır.

Saklama kuruluşlarında finansal tabloların doğruluğu, bütünlüğü ve güvenilirliğine ilişkin dayanak teşkil eden süreçlerin, kontrollerin ve bilgi sistemlerinin değerlendirilmesini adına bağımsız denetim faaliyeti gerçekleştirilir.

Bu denetim çalışmalarında, Rezerv Kanıtı (Proof of Reserves - PoR) tek başına bir kuruluşun ödeme gücünü (solvency) kanıtlamaya veya müşteri fonlarının kötüye kullanılmadığını göstermeye yeterli olmayıp PoR'nin, mevduat sahiplerine borçlu olunan miktarı gösteren Yükümlülük Kanıtı (Proof of Liabilities - PoL) ile desteklenmesi gerektiği de belirtilebilir. Rezerv Kanıtı (PoR): Yalnızca bir anlık görüntü olarak ele alındığında manipüle edilebilir. Örneğin, fonlar anlık görüntüden hemen önce ödünç alınabilir ve sonrasında asıl sahiplerine iade edilebilir. PoR, tamamen denetlenmeli ve blok zinciri adreslerinin sürekli izlenmesini içermelidir. Bu durum, sektör genelinde PoR için asgari standartlar (örneğin denetimler) getirilerek veya tüm platformlar için aynı anda (aynı zaman damgasıyla) anlık görüntüler alınarak ele alınabilir.

Yükümlülük Kanıtı (PoL):Toplam müşteri mevduatlarını ölçmek için önemlidir. Ancak, zincir dışı (off-chain) veya bilanço dışı (off-balance sheet) yükümlülükleri vurgulamaz ve bu yükümlülükler gizli kalabilir. Mali denetçiler tarafından yapılacak uygun denetimler bu sorunu çözmeye yardımcı olabilir, ancak bir denetimin başarabileceği şeylerin sınırları vardır. Bu nedenle, uygun düzenleme ve denetim, ek bir dayanak olarak gereklidir.

Varlık Yönetimi ve şeffaflık adına potansiyel düzenlemelerle aşağıdaki uygulamalar benimsenebilir:

• Varlıkların Saklama Altında Bulundurulması, AUC- Assets Under Custody): Kripto Platformları, saklama altındaki varlıklarını (AUC) yayımlayabilir. Düzenleyiciler, AUC'ye bireysel hesap seviyesine kadar erişim talep edebilir ve kripto platformlarının dahili kayıtlarına ulaşabilir.

• Zincir Üzerindeki Cüzdanların Açıklanması: CTP'ler, bugün birçok platformun yaptığı gibi zincir üzerindeki cüzdanlarını açıklayabilir. Bu bilgiler, zincir üzerindeki varlık sayısının dahili kayıtlarla eşleşip eşleşmediğini belirlemek için uzlaştırılabilir.

Gözetim Süreçlerinde Odak Alanları

1. Finansal Raporlama ve Şeffaflık: Düzenleyici kurumlar, saklama kuruluşlarının mali durumunu ve operasyonel süreçlerini belirli aralıklarla denetler. Periyodik finansal raporlar, şeffaflık, hesap verilebilirlik ve güven sağlar. Kuruluşların mali durumlarını detaylı şekilde analiz eden düzenleyiciler, iflas risklerini minimize etmek için gerekli aksiyonları belirler.

2. Müşteri Varlıklarının Ayrıştırılması (Asset Segregation): Saklama kuruluşlarının, müşteri varlıklarını kendi operasyonel varlıklarından ayrı tutması gerekmektedir. Bu uygulama, hizmet sağlayıcıların mali zorluklarla karşılaşması durumunda müşteri varlıklarının korunmasını sağlar ve güven kaybını önler.

3. AML/CFT Kontrolleri: AML (Kara Para Aklamayı Önleme) ve CFT (Terörizmin Finansmanını Önleme) kontrolleri, düzenleyici gözetim süreçlerinde kritik bir rol oynar. Saklama hizmeti sağlayıcıları, KYC, şüpheli işlem raporlaması (SAR/STR) ve blokzincir analiz araçları kullanarak risk bazlı kontroller gerçekleştirir.

4. Teknolojik Gözetim ve Risk Yönetimi: Düzenleyici kurumlar, otomatik izleme sistemleri, sızma testleri ve gerçek zamanlı işlem denetimlerini zorunlu kılar. Bu süreçte, anlık risk değerlendirme araçları kullanılarak olası tehditler tespit edilir ve önlenir.

5. Lisanslama ve Sürekli Denetim: Saklama hizmeti sağlayıcıları, faaliyet gösterebilmek için belirli yasal standartları karşılamak zorundadır. Düzenleyici kurumlar, lisanslama süreçlerinin yanı sıra sürekli gözetim ve denetim mekanizmaları uygulayarak hizmet kalitesinin sürdürülebilirliğini sağlar.

Düzenleyici Gözetimin Önemi ve Etkisi

Düzenleyici gözetim, dijital varlık saklama hizmetlerinin daha güvenilir, şeffaf ve sürdürülebilir hale gelmesini sağlamaktadır. Düzenleyici kurumların sıkı denetimi, sektördeki güven ortamını güçlendirir ve yatırımcıların varlıklarını daha güvenle saklamalarına olanak tanır. Özellikle lisanslama ve periyodik uyumluluk denetimleri, hizmet sağlayıcıların kalite standartlarını yükselterek sektörde sürdürülebilir büyümeyi destekler.

Düzenleyici gözetimin aynı zamanda teknolojik inovasyonu teşvik edici bir rolü de bulunmaktadır. Örneğin, regülatörlerin akıllı sözleşme denetimleri, blokzincir güvenliği ve veri gizliliği standartları gibi alanlarda katı gereklilikler belirlemesi, hizmet sağlayıcıların daha güvenli ve yenilikçi çözümler geliştirmelerini sağlar.

Ek Güvenlik Önlemleri

Dijital varlıkların güvenliğini sağlamak, yalnızca temel güvenlik önlemleriyle sınırlı kalamaz. Günümüzde artan siber tehditler ve gelişen saldırı teknikleri karşısında çok katmanlı güvenlik önlemleri hayati bir rol oynamaktadır. Ek güvenlik önlemleri; gelişmiş şifreleme teknikleri, fiziksel güvenliğin yanında anomali tespiti, öngörücü analiz ve doğrulanabilir şifreleme (verifiable encryption) gibi yenilikçi teknolojileri kapsar. Bu çözümler, dijital varlıkların gizliliğini, bütünlüğünü ve erişilebilirliğini korumak için bir arada çalışır.

Anomali Tespiti

Anomali tespiti, dijital varlık sistemlerinde anormal davranışları belirlemek için kullanılan güvenlik yöntemidir. Özellikle makine öğrenimi algoritmaları ve büyük veri analizi sayesinde yetkisiz erişim, dolandırıcılık ve güvenlik ihlalleri erken tespit edilir.

Teknik çözümler şu şekilde özetlenebilir:

1. Makine Öğrenimi (ML) Algoritmaları: Kullanıcı işlem kalıplarını analiz ederek anormallikleri tespit eder. Örneğin, büyük miktarda varlık hareketleri veya farklı IP adreslerinden yapılan işlemler işaretlenir.

2.Threshold-Based Detection: İşlem hacmi, coğrafi konum gibi eşik değerler tanımlanarak belirli kriterleri aşan işlemler otomatik olarak durdurulabilir veya manuel doğrulama istenir.

3. Gerçek Zamanlı İzleme: Sistem logları, gerçek zamanlı olarak analiz edilir ve anomali tespit edildiğinde hızlı müdahale sağlanır.

4. Blokzincir Analitiği: Blokzincir üzerinde adres hareketlerini izleyen sistemler kullanılarak dolandırıcılık veya kara para aklama (AML/CFT) faaliyetleri tespit edilir.

Öngörücü (Predictive) Analiz

Öngörücü analiz, büyük veri analitiği ve AI tabanlı algoritmalar kullanarak potansiyel riskleri ve güvenlik tehditlerini önceden tahmin eder. Teknik olarak su teknolojiler kullanılarak olası tehditler bertaraf edilebilir.

1. Büyük Veri Analitiği: Geçmiş işlem verilerinin analizi ile gelecekteki tehditler tahmin edilir. Özellikle blokzincir üzerinde anomali hareketleri izlenerek riskli adresler belirlenir.

2. Davranışsal Analiz: Kullanıcıların normal işlem davranışları öğrenilerek anormallikler tespit edilir. Örneğin, sürekli aynı IP'den erişim sağlayan bir kullanıcının başka bir ülkeden erişmesi riskli davranış olarak işaretlenir.

3. Dinamik Risk Skorlama: Kullanıcı cüzdanları ve işlemleri için dinamik risk skoru oluşturulur ve yüksek riskli işlemler ek doğrulama gerektirir.

4. Proaktif Güvenlik Önlemleri: AI tabanlı tahmin sistemleri, riskli senaryoları önceden analiz ederek güvenlik önlemlerinin proaktif şekilde devreye alınmasını sağlar.

Saklama Çözümlerinin Geleceği ve Gelişim Alanları

Dijital varlıkların benimsenme hızı arttıkça, saklama hizmetlerinin de bu trende ayak uydurması kaçınılmazdır. Geleneksel finans sistemlerinde güvenilir olarak kabul edilen saklama çözümleri, blokzincir teknolojisinin getirdiği yeniliklerle yeniden tanımlanmaktadır. Güvenlik, erişim kolaylığı ve operasyonel maliyetler açısından kullanıcıların ihtiyaçları, gelecekteki saklama çözümlerinin tasarımında kritik bir rol oynayacaktır. Bu çerçevede hem bireysel hem de kurumsal kullanıcıların taleplerine yönelik olarak yeni teknolojiler ve çözümler geliştirilmesi beklenmektedir.

Gelişim Alanları

1. Kullanıcı Dostu Saklama Çözümleri

Dijital varlıkların yaygınlaşmasıyla birlikte, teknik bilgi gerektiren mevcut saklama yöntemleri, geniş kitleler tarafından erişilebilir olma noktasında sınırlı kalmaktadır. Bu nedenle, kullanıcı deneyimini iyileştiren ve teknik engelleri azaltan saklama çözümleri giderek daha fazla ön plana çıkacaktır.

• Otomatik Anahtar Yönetimi: Kullanıcıların gizli anahtarlarını güvenli bir şekilde saklayan ve otomatik yedekleme mekanizmalarıyla kaybolma riskini en aza indiren çözümler geliştirilecektir. Anahtarların parçalara bölünerek farklı güvenlik seviyelerine dağıtılması, kullanım kolaylığı ile güvenliği bir arada sunacaktır.

• osyal Kurtarma Mekanizmaları: Kullanıcıların anahtar kaybı durumunda arkadaşlar, aile üyeleri veya güvenilir üçüncü taraflar aracılığıyla erişimlerini kurtarmalarını sağlayan sosyal kurtarma (social recovery) çözümleri yaygınlaşacaktır.

• Biyometrik Kimlik Doğrulama: Geleneksel şifreler yerine parmak izi, retina tarama veya yüz tanıma gibi biyometrik kimlik doğrulama teknolojileri, kullanıcıların dijital varlıklarına kolay erişim sağlarken güvenliği de artıracaktır.

• Çapraz Zincir Uyum ve Entegrasyon: Farklı blokzincir ağları arasında uyumluluk ihtiyacı giderek daha önemli hale gelmektedir. Kullanıcılar, Bitcoin ve Ethereum'dan yeni altcoinlere kadar çeşitli dijital varlıkları tek bir arayüzde yönetebilecekleri cüzdanlara yönelmektedir.

• AI ve Makine Öğrenimi Entegrasyonu: Kripto cüzdanlarında yapay zekâ (AI) ve makine öğrenimi teknolojilerinin kullanımı artmaktadır. AI destekli analiz araçları, yatırım içgörüleri, risk analizi ve otomatik işlem önerileri sunarak kullanıcı deneyimini iyileştirmektedir.

2. Ölçeklenebilirlik

Blokzincir teknolojisinin en büyük zorluklarından biri olan ölçeklenebilirlik sorunu, saklama hizmetleri için de kritik bir gelişim alanı olarak öne çıkmaktadır. Mevcut saklama çözümlerinin artan kullanıcı sayısı ve işlem hacmi ile başa çıkabilmesi için yenilikçi teknolojiler geliştirilmektedir.

• MPC: Gizli anahtarların tek bir noktada saklanması yerine farklı parçalara bölünerek coğrafi olarak dağıtılması, ölçeklenebilir güvenlik sağlama potansiyeline sahiptir. MPC tabanlı çözümler, anahtar parçalarının farklı taraflarda işlenerek işlem onayının tamamlanmasına olanak tanır.

• Layer-2 Çözümleri: Blokzincir ağlarının ölçeklenebilirliğini artırmak için Layer-2 çözümleri (örneğin, rollup teknolojileri) kullanılacaktır. Bu çözümler, ana blokzincir üzerindeki işlem yükünü azaltarak hızlı ve düşük maliyetli işlemleri mümkün kılacaktır.

• Hibrit Saklama Yapıları: Hem on-chain (blokzincir üzerinde) hem de off-chain (blokzincir dışında) veri depolama yöntemlerini birleştiren hibrit çözümler, hızlı erişim ve ölçeklenebilirliği artırırken güvenlikten ödün vermeyecektir.

3. Kurumsal Saklama Çözümleri

Kurumsal yatırımcıların dijital varlık piyasasına olan ilgisi, güvenilir ve regülasyonlara uygun saklama hizmetlerine olan talebi artırmaktadır. Büyük ölçekli yatırımcılar için özel olarak tasarlanmış kurumsal saklama çözümleri, operasyonel verimlilik ve risk yönetimini ön planda tutmaktadır.

• Risk Yönetimi ve Uyum: Kurumsal saklama hizmetlerinde AML/CFT kontrolleri ve KYC süreçleri sıkı bir şekilde uygulanmaktadır. Saklama hizmet sağlayıcılarının, regülasyonlara uyum konusunda denetim mekanizmaları ve raporlama sistemleri geliştirmeleri gerekmektedir.

• Sigortalı Saklama Çözümleri: Dijital varlıkların sigortalanması, büyük ölçekli yatırımcılar için bir güven unsuru oluşturmaktadır. Kurumsal çözümler, üçüncü taraf sigorta sağlayıcıları ile entegre edilerek potansiyel kayıplara karşı risk transfer mekanizmaları sunacaktır.

• Programlanabilir Güvenlik ve Akıllı Sözleşmeler: Akıllı sözleşmelerle otomatik güvenlik politikalarının devreye alınması, kurumsal saklama hizmetlerinde hem operasyonel maliyetleri azaltacak hem de risk yönetimini daha etkin hale getirecektir. Örneğin, çoklu imza mekanizmaları ile işlemlerin farklı yetki seviyelerine göre onaylanması sağlanabilir.

4. Merkeziyetsiz Saklama (Decentralized Custody) Girişimleri

Geleneksel merkezi saklama çözümlerine alternatif olarak merkeziyetsiz saklama (Decentralized Custody) modelleri, blokzincir teknolojisinin temel prensiplerinden biri olan merkeziyetsizlik ilkesini benimsemektedir.

Geleneksel saklama hizmetleri merkezi bir yapıya dayanırken, merkeziyetsiz çözümler dağıtık ve güvene dayalı olmayan (trustless) sistemler ile çalışır. Böylece, kullanıcıların varlıkları üzerinde tam kontrol sağlarken, tekil başarısızlık noktalarını ortadan kaldırmaktadır.

Gelecek Beklentileri

Merkeziyetsiz finans (DeFi) ve Web3.0 ekosistemlerinin hızlı büyümesi, dijital varlıkların yönetimi için merkeziyetsiz saklama çözümlerine olan talebi artırmaktadır. Bu gelişim, bireysel ve kurumsal kullanıcıların daha güvenli, erişilebilir ve aracıya ihtiyaç duymayan çözümlere yönelmesini sağlayacaktır. Merkeziyetsiz teknolojiler, kullanıcılara varlıkları üzerinde tam kontrol sunarken güvenlik ve esneklik açısından önemli yenilikler getirecektir.

1. Self-Custody Platformları

Self-custody platformları, kullanıcıların kendi gizli anahtarlarını yönettiği saklama çözümleridir. Bu sistemlerde merkezi aracılar ortadan kaldırıldığı için güvenlik riskleri önemli ölçüde azalır.

• Kullanıcılar, kendi cüzdanları aracılığıyla gizli anahtarlarını saklar ve kontrol eder. Donanım cüzdanlar ve yazılım cüzdanlar self-custody çözümlerinin temelini oluşturur.

• Anahtarların çoklu faktör doğrulama (MFA) ve bölünmüş anahtar yönetimi ile daha güvenli hale getirilmesi, self-custody çözümlerini bir üst seviyeye taşımaktadır.

Bu sayede, kullanıcıların varlıkları üzerinde tam kontrol sahibi olması ve merkezi saldırı risklerinin ortadan kalkabilir.

2. DAO Tabanlı Saklama

Merkeziyetsiz otonom organizasyonlar (DAO), kullanıcıların topluluk tabanlı karar mekanizmaları aracılığıyla saklama hizmetlerini yönetmelerine olanak tanır. DAO tabanlı saklama çözümleri, kolektif güvenlik anlayışını ve demokratik yönetim modelini birleştirir.

• DAO yapısında, dijital varlıkların saklanması için karar alma süreçleri akıllı sözleşmeler üzerinden otomatikleştirilir. Çoklu imza mekanizmaları ve MPC teknolojileri kullanılarak güvenlik sağlanır.

Bu sayede, tekil hata noktalarının (single-point-of-failure) ortadan kalkması ve şeffaf topluluk kontrolü sağlanabilir.

3. Kriptografik Anahtar Parçalama

Kriptografik anahtar parçalama teknikleri, gizli anahtarların güvenliğini artırarak tek bir noktadan saldırı riskini ortadan kaldırır.

• Verifiable) Shamir Secret Sharing (SSS) gibi mekanizmalar kullanılarak, Anahtarlar, birden fazla parçaya bölünerek farklı lokasyonlarda saklanır. Anahtarın tamamına erişim için belirli sayıda parçanın birleştirilmesi gereklidir.

• Merkeziyetsizlik sağlanırken, tekil kayıpların önüne geçilir. Örneğin, 3ün 5lisi (beş parçadan üçünün bir araya gelmesi) gibi yapılandırmalar uygulanabilir.

Self-custody platformları ve kurumsal saklama çözümlerinde, anahtarların coğrafi olarak dağıtılmış güvenli sistemlerde saklanması bu yöntemi daha etkili hale getirmektedir.

Hukuki Düzenlemelerin Saklama Hizmetlerine Etkileri

Dijital varlık piyasasının hızlı büyümesi ve finansal ekosistemdeki dönüşüm, düzenleyici kurumların saklama hizmetlerini sıkı bir şekilde denetlemesini zorunlu hale getirmiştir. Uluslararası düzenlemeler, hizmet sağlayıcılar için yeni yükümlülükler ve operasyonel standartlar belirlemektedir. Regülasyonlar, dijital varlıkların güvenliğini artırmayı hedeflerken, hizmet sağlayıcıların şeffaflık, risk yönetimi ve tüketici koruma açısından yüksek standartlar benimsemesini zorunlu kılmaktadır.

1. Şeffaflık Gereksinimleri

Şeffaflık, regülatörler tarafından sıkı bir şekilde talep edilen bir unsurdur. Saklama kuruluşlarının, müşteri varlıklarının durumunu periyodik raporlarla beyan etmesi ve şeffaf finansal denetimlerden geçmesi gerekmektedir.

Teknik Gereksinimler:

• Raporlama Standartları: Uluslararası raporlama çerçeveleri (SOC 1/SOC 2, ISAE 3000) ve bağımsız denetimler, saklama hizmetlerinin finansal ve operasyonel durumlarını düzenleyicilere sunmayı zorunlu kılar.

• Blokzincir Tabanlı Doğrulama: Şeffaflık için blokzincir üzerinde gerçek zamanlı varlık kanıtı (Proof of Reserves) çözümleri kullanılabilir. Bu sayede müşteri varlıklarının doğruluğu sürekli olarak denetlenebilir.

• Etkisi: Şeffaflık gereksinimleri, saklama hizmeti sağlayıcılarının düzenli raporlama süreçlerini otomatikleştirmesini ve teknolojik altyapılarını geliştirmesini gerektirir. Bu durum, hizmet kalitesini artırarak müşteri güvenini güçlendirir.

2. Müşteri Varlıklarının Ayrıştırılması

Düzenlemeler, müşteri varlıklarının saklama hizmeti sağlayıcısının operasyonel hesaplarından tamamen ayrıştırılmasını zorunlu hale getirmiştir. Bu uygulama, hizmet sağlayıcının olası bir finansal sorun yaşaması durumunda müşteri varlıklarının korunmasını sağlar.

Teknik Uygulamalar:

• Segmentasyon ve İzleme: Müşteri varlıkları, blokzincir üzerinde farklı cüzdanlar veya alt-hesaplar aracılığıyla ayrı ayrı takip edilir. Bu yöntem, hem operasyonel riskleri azaltır hem de müşteri varlıklarının şeffaf yönetimini sağlar.

• Akıllı Sözleşmeler: Self-Custody veya DAO tabanlı çözümler kullanılarak, müşteri varlıklarının otomatik ve doğrulanabilir bir şekilde ayrıştırılması sağlanır.

• Dijital Kimlik ve İzlenebilirlik: Müşteri varlıklarının hareketleri, KYC/AML uyumluluğu sağlanarak detaylı olarak kaydedilir.

• Etkisi: Varlık ayrıştırma, müşteri güvenliğini artırırken hizmet sağlayıcıların operasyonel şeffaflık ve yasal uyum açısından daha sağlam bir altyapı oluşturmasını sağlar.

3. Sigorta ve Risk Yönetimi

Regülasyonlar, saklama hizmeti sağlayıcılarının finansal teminat sağlamasını ve müşterilere sigorta güvencesi sunmasını zorunlu kılmaktadır. Bu uygulamalar, özellikle kurumsal yatırımcıların risklerini minimize etmek için hayati önem taşır.

Teknik Çözümler:

• Siber Sigorta Poliçeleri: Saklama hizmetleri için siber saldırılar veya anahtar kaybı durumlarına karşı sigorta kapsamı oluşturulmaktadır.

• Risk Transferi Mekanizmaları: Hizmet sağlayıcılar, üçüncü taraf sigorta şirketleri ve risk yönetim platformları ile anlaşmalar yaparak finansal riskleri paylaşır.

• Dinamik Risk Puanlama: Makine öğrenimi ve büyük veri analitiği kullanarak, müşteri hesapları için dinamik risk skorlaması yapılır ve riskli işlemler otomatik olarak tespit edilir.

• Etkisi: Sigorta çözümleri, olası finansal kayıpların önlenmesini sağlarken kurumsal yatırımcılar için piyasaya güvenli bir giriş imkânı sunar.

4. Düzenleyici Uyumun Teknolojik Entegrasyonu

Regülasyonlara uyum süreci, saklama hizmeti sağlayıcılarının teknolojik altyapılarını uyumlu ve esnek hale getirmelerini zorunlu kılar.

• RegTech Çözümleri: Düzenleyici teknoloji (RegTech) uygulamaları, AML/CFT kontrollerini otomatikleştirir, şüpheli işlem raporlama (STR) ve uyumluluk raporlaması süreçlerini kolaylaştırır.

• Akıllı Denetim Sistemleri: Blokzincir tabanlı verifiable encryption ve izlenebilir doğrulama mekanizmaları, regülatörlerin işlemleri şeffaf ve anlık olarak incelemesini sağlar.

• AI ve Öngörücü Analiz: Regülasyonlara uyum sağlamak amacıyla AI destekli risk analizleri ve anomali tespiti sistemleri entegre edilir.

B. KRİPTO VARLIK SAKLAMA SÜREÇLERİNE İLİŞKİN HUKUKİ ÇERÇEVE

Kripto varlık piyasası, özellikle geçtiğimiz yıl içinde önemli bir kripto varlık hizmetine yoğunlaştı: kripto varlıkların saklanması (crypto-asset custody). Stablecoin'ler, CBDC (Central Bank Digital Currency)'ler, hisse senetleri, tahviller, emtialar ve gayrimenkul gibi gerçek dünya varlıklarının (RWA- real world asset) tokenizasyonu ve ETF(Exchange Traded Funds)'lar gibi yeni yenilikçi kullanım örnekleri, bankacılık ve finans kuruluşları genelinde dijital varlıklara yönelik kurumsal ilgiyi artırmış durumdadır. Özellikle Bitcoin ve Ether ETF'lerinin benimsenmesi, ana akım finans alanında da artan bir kabulü tetikledi. Mevcut kripto saklama piyasası hala nispeten küçük olsa da sektörün yıllık %30 büyüdüğü belirtilmektedir. Tüm bu gelişmeler regüle edilmiş, güvenli ve dayanıklı saklama hizmetlerine yönelik kurumsal talebi artırmıştır.[1]

1. Kripto Varlık Saklama Süreçlerinde Hukuki Çerçevenin Belirlenmesinin Önemi

Saklama (custody), genel olarak, varlıkların üçüncü kişiler adına muhafaza edilmesini ve genellikle yönetilmesini de içeren süreci ifade eden bir kavramdır. Saklayan kuruluş, kendisine saklaması için bırakılan varlıkları güvenle tutmak ve bunlar üzerinde hukuki kesinliği sağlamakla yükümlüdür.

Birçok durumda, saklayan kuruluş varlıkların korunmasından fazlasını yapar ve saklatan kişi veya kurumun hesabını ya da işlemlerini, temettü toplanması, regülasyonlara uyum sağlanması, ödünç verme gibi işlemlerin yapılması kapsamında yönetir.[2] Geleneksel finansta 1940'lardan beri saklama kuruluşları varlıkları, son kullanıcılar adına elektronik veya fiziksel olarak tutmaktadır. Ancak gelişmekte olan merkeziyetsiz finansın (Decentralised Finance-DeFi) dinamikleri geleneksel finanstan ve orada kullanılan mekanizmalardan oldukça farklıdır.

Kripto varlıkların saklanması konusu DLT (Distrubeted Ledger Technology) tabanlı işlemlerin regülasyonu süreçlerindeki güncel sorunlardan biridir. Saklama konusunda Türkiye'de ve dünyada hızla gelişen yeni düzenlemelerin gündemde olduğu görülmektedir. Kripto varlıklar için küresel olarak ve yeknesak bir şekilde ayrıntılı tanımlanmış bir düzenleyici hukuki çerçeve mevcut değildir. Bu nedenle kripto varlık saklama cüzdanı sağlayıcıları tarafından sunulan hizmetler ve hatta kripto varlık saklama kavramının kapsamının nasıl belirleneceği büyük ölçüde farklılık gösterebilmektedir. Düzenleme bulunan ülkelerde saklamaya ilişkin olarak yürürlükte olan kurallar da birbirinden farklıdır.[3] Özellikle kripto varlık faaliyetlerinin hareketlendiği ülkelerdeki son duruma ve bu ülkelerdeki saklama regülasyonlarına değinmeden önce, kripto varlık saklama konusunun hukuki düzlemde ele alınmasının neden önemli olduğunun açıklanması yerinde olacaktır:

Bitcoin hayatımıza girdiğinden beri, kripto varlık dünyası çeşit zamanlarda iniş ve çıkış dönemlerine tanıklık etmiştir.

1 *Carlo R. W. De Meijer, Traditional financial custodians enter the crypto market (21.10.2024) https://www.finextra.com/blogposting/27059/traditional-financial-custodians-enter-the-crypto-market#:~:text=The%20growing%20institutional%20interest%20across,institutional%20demand%20for%20regulated%2C%20se cure*

2 *World Federation of Exchanges, Crypto-Asset Custody: A Blueprint for Regulatory and Operational Excellence (28.08.2024), https://www.world-exchanges.org/storage/app/media/Cally%20Billimore/Custody%20of%20Crypto%20-%20Final.pdf, s. 3.*

3 *World Federation of Exchanges, s. 2.*

Özellikle 2021-2023 arasındaki dönemde yaşanan, "kripto kışına" yol açan ve milyonlarca dolara ulaşan bazı kayıplar, kripto varlıklara ve dağıtık defter teknolojisine duyulan güvenin sarsılmasına neden olmuştur. Kripto varlıklarla ilgili yaşanan hatalı işleyiş ve kayıplar, aslında kripto varlıkların saklanması ile yakından ilgilidir.

Kripto varlıkların saklanmasına ilişkin düzenlemelerin yapılmadığı bir yargı çevresinde, kripto varlık hizmet sağlayıcılar müşterilerinin varlıklarını saklama konusunda özgürce farklı yöntemlere başvurabilirler. Bazı sağlayıcılar kendi uhdelerinde bulunan sıcak ve soğuk cüzdanları tercih ederken, diğerleri operasyonel anlamda problem yaratmayacak saklama çözümleri üreten üçüncü taraf saklama şirketleriyle çalışarak güvenlik seviyesini artırabilir, hatta müşteri varlıklarına ilişkin sigorta çözümlerine başvurabilirler.

International Monetary Fund (Uluslararası Para Fonu- IMF) bir politika belgesinde, FTX skandalına da sebebiyet veren zafiyetlerin neler olduğuna değinirken, saklama hizmetlerine ilişkin hukuki düzenlemelerin yapılmamış olmasına veya bunların yeterli olmamasına da dikkat çekmektedir: "Kripto hizmet sağlayıcılarının çoklu işlevleri ve faaliyetleri (aracılık, ticaret ve saklama hizmetleri gibi) düzenlemeye ve denetime tabi değildir. FTX özelinde, bu entegre ihraçlar müşterilere kaldıraçlı kredi verilmesine, likidite uyumsuzluklarına ve sonrasında daha yüksek çekim taleplerinin karşılanamamasına yol açtı."[4]

2024 yılında yapılan güncel bir çalışmada, kripto varlık yatırımcılarının güveninin sarsılmasına neden olan ve saklama faaliyetleriyle bağlantılı bazı temel olgular belirlenmiştir.

Buna göre, kripto varlık saklama hizmeti sunan kuruluşlar, müşterilerinin varlıklarına ait gizli anahtarların kaybını önlemekte başarısız olmuştur. Ayrıca, siber riskler, yanlış beyanlar, iç ve dış hırsızlıklar gibi tehditlere karşı yeterince iyi saklama politikaları geliştirememişlerdir. Bunun yanı sıra, kripto varlık saklama hizmetleri, kripto para borsaları tarafından aracılık, yatırım ve lending faaliyetleri gibi riskli işlerle aynı bilançoda birleştirildikleri için menfaat çatışmaları yaygınlaşmış ve kripto varlık saklama hizmetlerinin istikrarını tehlikeye atmıştır. Dikkate alınması gereken diğer bir önemli nokta, saklama hizmeti sunan kuruluşların, birçok müşterinin varlıklarının kendi varlıklarıyla karışmasına engel olamaması ve bu varlıkların sahibinin kimliği belirlenemez hale gelmiş olmasıdır. Son olarak, saklama hizmeti sunan kuruluşlar, müşteri varlıklarını kendi hesapları veya ilişkili bir kuruluşun hesabı için ticarette kullanmıştır. Özellikle yüksek miktarda kayıpları, müşterilerin saklama konusu olan varlıkları ile telafi etmişlerdir. Bugün bile, birçok saklama hizmeti sunan platform, kendi yatırım veya iş amaçları için emanet edilen varlıkları yeniden kullanma hakkını saklı tutmaktadır.[5]

Kripto varlık ekosisteminde yaşanan ve bazıları global skandal boyutuna ulaşan olaylar sonucunda şu gerçekler gözler önüne serilmiştir: Saklama faaliyeti kapsamında müşteri varlıklarının yeterli ölçüde korunamadığı takdirde, büyük kayıplar ortaya çıkabilmektedir. Belirtmiş olduğumuz dönemde kripto varlıkların hukuki niteliği ve bunlara icra ve iflas hukuku kapsamında uygulanacak hukuk kurallarına ilişkin gelişmeler henüz yeni yeni şekillenmekteydi. Çoğu yargı alanında eksik olan, ancak gelişmekte olan kripto varlıklar üzerindeki hakların tespitine ilişkin ve iflas durumunda uygulanacak kurallar, token sahipleri için yeterli özel koruma sağlamada eksik kalmıştır.

4 *IMF, Elements of Effective Policies for Crypto Assets (13.02.2023), https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/02/23/Elements-of-Effective-Policies-for-Crypto-Assets-530092, s. 39.*

5 *Dirk Zetzsche, Julia Sinnig, Areti Nikolakopoulou, Crypto custody, Capital Markets Law Journal, Volume 19, Issue 3, July 2024, Pages 207–229, https://doi.org/10.1093/cmlj/kmae010, s. 209*

Bu nedenle, uluslararası politika yapıcılar ve kanun koyucular, dikkatlerini kripto varlık saklama platformlarına ilişkin regülasyonların oluşturulmasına çevirmiştir. Gerçekten de 2022 yılı itibariyle, IMF, IOSCO, FSB gibi kuruşlar kripto varlık saklama konusunu mercek altına almış ve daha hassasiyet gereken konuları tespit ederek bunlara öncelik verilmesi hususunda çağrıda bulunmuştur:

IMF, kripto varlık hizmet sağlayıcıların lisansa tabi bir şekilde kayıtlı veya yetkilendirilmiş olarak faaliyet göstermelerinin önemine dikkat çekmektedir. Rezervlerin ve varlıkların depolanması, aktarılması, değiş tokuş edilmesi ve saklanması gibi faaliyetler sunan kuruluşların, yeni iş modellerine (birleşik borsalar ve cüzdanlar gibi) uygun düşecek ek gerekliliklerle birlikte finansal hizmet sağlayıcılara uygulananlara benzer kurallara tabi olmasının gerektiği belirtilmektedir.[6]

IMF Fintech Notes 2022'de cüzdan sağlayıcılar tarafından verilen saklama hizmetleriyle ilgili önemli bazı noktalara dikkat çekilmiştir. Buna göre, cüzdanlar tarafından saklama hizmetleri sunulması özellikle unbacked kripto varlık[7] ekosistemi bakımından kritik bir unsurdur ve regülatif açıdan sağlam bir şekilde konumlandırılması önem teşkil etmektedir. Bu çerçevede, tek işlevli kripto borsalarından farklı olarak bazı ek önlemler almalarını gerekli kılacak ve böylece daha katı düzenlemelere ihtiyaç duyulabilecektir. Bu kapsamda IMF, fonların ve kripto varlıkların kuruluşun kendi fon ve varlıklarından ayrı tutulması gerekliliğine dikkat çekmektedir.

Müşterilerin açık rızası olmadıkça ve uygun bir tazmin usulü belirlenmedikçe müşteri varlık ve fonların yeniden kullanımı veya lending faaliyetine konu edilmesine izin verilmemelidir. Bu kapsamda, kullanıcıların cüzdan adresleri ile platformun kendi cüzdan adresleri birbirinden farklı olmalıdır. Bunlara ek olarak, platformların etkili bir acil durum yönetimi usulü belirlemiş olmaları gerekmektedir. Operasyonel veya siber olayların raporlanması, piyasa bütünlüğünün sağlanması için zamanında ve doğru bir şekilde olmalıdır. Siber veya operasyonel süreçler üçüncü taraflara devredildiğinde de cüzdan sağlayıcısı, meydana gelen olaylardan sorumlu olmalıdır. Cüzdan sağlayıcıları, talep üzerine veya düzenli aralıklarla, kullanıcılarıyla varlıklarındaki değişiklikleri paylaşmalıdır. Platformlar, FATF tarafından öngörülmüş olan AML/CFT standartlarına uygun davranmalıdır. Ayrıca düzenleyici çerçevelerde, cüzdan sağlayıcılarının, tüketiciler için riskleri azaltmak amacıyla, bir siber saldırı durumunda sigorta kapsamına ilişkin belirlemelere yer verilebilir. Bunlara ek olarak IMF, müşteri fonlarının uygun şekilde ayrılmasının bir firmanın iflası durumunda müşterilerin zararını azaltabileceğine ve üçüncü taraf sağlayıcılarla çalışmanın ve kritik bilgi teknolojisi altyapısını sürdürmenin de önemli olduğuna değinmektedir. Son olarak, özellikle platformun birbirinden farklı işlevleri yerine getirdiği durumlarda, kullanıcıların menfaatlerinin ön planda tutulmasının ve bir menfaat çatışması ortaya çıktığında şeffaflık ve bilgilendirme yükümlülükleri çerçevesinde bunu müşterilere açıklamanın önemini de vurgulamaktadır. [8]

6 *IMF, Policy Paper- Elements Of Effective Policies For Crypto Assets, February 2023, s. 22.*

7 *Unbacked crypto asset, desteklenmeyen kripto varlıklar, dağıtık defter teknolojisi üzerinde işlenen herhangi bir fiziksel varlık ya da teminatla desteklenmeyen kripto varlıklardır. Bu varlıklar, genellikle transfer edilebilme ve ödeme aracı olarak kullanılması için tasarlanmıştır. En bilinen örnekleri Bitcoin ve Ether'dir.*

8*IMF Fintech Notes: Regulating the Crypto Ecosystem The Case of Unbacked Crypto Assets Parma Bains, Arif Ismail, Fabiana Melo, and Nobuyasu Sugimoto, 2022*

IOSCO, 2023 yılının sonunda hazırladığı Tavsiyeler'in 7. bölümünde[9], müşteri fon ve varlıklarının saklanmasına ilişkin risklere yönelik önerilere ve destekleyici rehber ilkelere yer verilmiştir. Bu risklerin özellikle varlıkların ayrı tutulmasına, yeniden kullanılmasına, sorumluluk ve mülkiyete dair konulara ilişkin olduğu belirtilmektedir. IOSCO Tavsiyelerinde, kripto varlık hizmet sağlayıcılar tarafından gerçekleştirilmesi gereken kontrol mekanizmalarına ve bu kapsamda kripto varlıkların saklanmasına ilişkin esaslara da değinmektedir.

Öneri 12'de IOSCO geçmişte saldırıya uğrayan ve/veya korumakla yükümlü oldukları müşteri varlıklarına erişim araçlarını kaybeden saklama platformlarına dikkat çekerek, müşteri varlıklarının uygun şekilde saklanması için, erişim araçları (gizli anahtarlar ve cüzdanlar gibi) dahil olmak üzere bir platformun politikalarının, prosedürlerinin ve kontrollerinin gücüne bağlı olduğunu belirtmektedir. Saklama hizmeti sunan bir platform, müşteri varlıklarının kaybolması, çalınması veya erişilememesi riskini en aza indirmek için yeterli politikaları, prosedürleri ve düzenlemeleri farklı cüzdan türleriyle (örneğin, sıcak ve soğuk) ilişkili riskler etrafında düzenlemelidir. Bu nedenle düzenleyici otoriteler, bir platformun müşteri varlıklarının çalınması veya kaybolması durumunda yürürlükteki kanunlar uyarınca müşterilerinin zararlarını tazmin edip edemeyeceğini ve nasıl tazmin edebileceğini değerlendirmelidir. Düzenleyiciler, bir KVHS'nin müşteri varlıklarının her daim özellikle kayıp veya kötüye kullanım riskini en aza indirmeyi hedefleyerek, platform tarafından seçilen bir üçüncü tarafa yerleştirildiğinde de dahil olmak üzere, yeterli şekilde korunmasını sağlamasını zorunlu kılmalıdır.

Geleneksel finansal varlıklarda olduğu gibi düzenleyici otoriteler, müşteri varlıklarının miktarını, yerini ve üzerindeki hak durumunu belirleyen doğru ve güncel kayıtlar ve hesaplar tutmaya yönlendirmelidir. Sonuç olarak, yeterli, güvenilir ve açık bilgiler müşterilere ve üçüncü taraflara (örneğin iflas prosedürlerini yürüten otorite, düzenleyici otoriteler ve mahkemeler) sunulmalı ve böylece müşterilerin varlıklarına ilişkin haklarını, özellikle saklamak için bırakmış oldukları varlıklarını veya eşdeğer bir karşılığını geri alabilmeleri sağlanmalıdır.[10]

Tavsiye 13, saklama hizmeti sunan platformların, müşteri varlıklarını kendi özel varlıklarından ve kendileri tarafından kurguya dahil edilen herhangi bir iştirak veya hizmet sağlayıcının varlıklarından ayırmasına ilişkindir. IOSCO, bu tavsiyesi ile bir platformun müşteri varlıklarının kayba veya kötüye kullanıma karşı nasıl korunacağını ve bu tür varlıkların KVHS'nin alacaklılarının taleplerine tabi olmayan müşteri varlıkları olarak nasıl ayrıldığını belirtmesinin önemine işaret etmektedir. Platformun müşteri varlıklarını ödünç vermek gibi amaçlarla kullanabilmesi için müşterinin bu konuda anlayabileceği bir dilde bilgilendirilmesinin ve risklerin neler olduğunu anladığından emin olarak açık rızasının alınması gerektiği belirtilmektedir.[11]

Tavsiye 14, kripto varlık hizmet sağlayıcının üçüncü bir tarafla bir alt saklama ilişkisine girmesi durumunda, bu alt saklama ilişkisine yönelik sözleşmesel düzenlemelerin şartlarını ve bunların müşteri için oluşturabileceği ek risklerin de ayrıntılı olarak belirtilmesi gerekliliğine işaret etmektedir.[12]

9 *The Board of the International Organization of Securities Commissions (IOSCO), Policy Recommendations for Crypto and Digital Asset Markets Final Report (16 Kasım 2023), s. 33-39*

10 *The Board of the International Organization of Securities Commissions (IOSCO), Policy Recommendations for Crypto and Digital Asset Markets Final Report (16 Kasım 2023), s. 33.*

11 *IOSCO, s. 34.*

12 *IOSCO, s. 35.*

FSB ise şu noktaya dikkat çekmektedir: TerraUSD/LUNA, Celsius Network ve FTX gibi olaylarda da görüldüğü gibi, başarısız piyasa katılımcılarının çoğu, geleneksel finanstakine (Traditional Finance-TradFi) oldukça benzer işlevler üstlenmiştir. Uygun yönetim yapıları olmadan veya düzenleyici gerekliliklere uymadan yürüttükleri bu işlevler, FSB tarafından belirlenen güvenlik açıkları yaratmıştır. Çıkarılan bu dersler ışığında, FSB her iki üst düzey tavsiye setini de üç alanda güçlendirdiğini belirtmektedir. Bunlardan ilki, müşteri varlıklarının korunmasına ilişkindir. Müşterilerin varlıklarını elinde tutan veya kontrolüne sahip olan finansal hizmet sağlayıcıları, bu varlıkların kendi varlıklarından etkili bir şekilde ayrıldığından emin olmalıdır. İkincisi, FSB, yetkililerin menfaat çatışmalarıyla ilişkili riskleri ele almak için birtakım gerekliliklere sahip olması gerektiğini belirtmektedir. Bu çerçevede, birden fazla işlevi ve faaliyeti birleştiren bağlı kuruluşları da dahil olmak üzere kripto varlık hizmet sağlayıcılar, uygun düzenlemeye, gözetime ve denetime tabi olmalı veya bunlara uygun hale getirilmelidir. Buna uygun olarak belirli işlevlerin yasal olarak ayrılması da dahildir. Son olarak, FSB kripto varlık ihraççıları ve hizmet sağlayıcılarının, düzenlemenin daha yumuşak olduğu yerlere yönelerek regülasyonlardan ve denetimden kaçmaya çalışabileceğine dikkat çekmektedir. Bu nedenle FSB'nin üst düzey önerileri, özellikle uluslararası standartları uygulamayan yargı bölgelerindekiler olmak üzere, birden fazla yargı bölgesine yayılan faaliyetlerin uyumluluk düzeyi de dahil olmak üzere bilgi paylaşımı konusunda güçlendirilmiştir.[13]

World Federation of Exchanges, 2024 yılında yaptıkları çalışmada, kripto varlıkların saklanmasındaki temel sorunun, saklama platformunun çöktüğü durumlarda, bu platform tarafından saklanmakta olan kripto varlıkların platformunun kendisinin mi yoksa müşterinin (saklatan gerçek veya tüzel kişi) mi olduğunun tespiti ile ilgili olduğunu belirtmektedir. Bu kapsamda saklama kavramının geçmişten günümüze kadar nasıl geliştiğinin ve düzenleyici otoriteler tarafından nasıl bir hukuki çerçeve oluşturulması gerektiği ele alınarak bazı önerilerde bulunulmuştur. Kripto varlık saklama hizmeti sunan platformların iflası durumunda, müşteri varlıklarının ayrılmış olması önem teşkil etmektedir. Hatta müşteri varlıklarının iflastan hariç tutulmasının yani gerçek veya tüzel kişiliğin malvarlığından ayrı olması sağlanmalıdır. İyi düşünülmüş teknoloji mimarisinin oluşturulması ve olgunlaşmış siber güvenlik programlarının işletilmesiyle siber risklerin önüne geçilmesi gerekmektedir. Mevcut veya potansiyel çıkar çatışmalarının yeterli ve etkili bir şekilde yönetilmesi sağlanmalıdır. Müşteriler bakımından mevcut olan risklerin, açık ve anlaşılır bir şekilde onlara açıklanması gerekmektedir. Sigortaya ilişkin politikaların yeterli olması ve müşterilere açık ve anlaşılır olarak aktarılması önem taşımaktadır. Son olarak, finansal tabloların, süreçlerin ve kontrollerin değerlendirmesini sağlamak için itibarlı ve güvenilir denetçilerden bağımsız denetimler istenmesi ile birlikte ileride yaşanacak kayıpların büyük olmasının önüne geçebilecektir.[14]

13 *FSB Global Regulatory Framework for Crypto-Asset Activities Umbrella public note to accompany final framework (17.7.2023) https://www.fsb.org/uploads/P170723-1.pdf s. 5–6.*

14 *World Federation of Exchanges, s. 5-11.*

IMF, FSB, IOSCO gibi kuruluşların hazırlamış oldukları politika belgelerini ve MiCA'daki saklamaya ilişkin öngörülen düzenlemeleri esas alan bazı yazarlar, tüm bu çalışmalardan hareketle, saklama faaliyetine ilişkin olarak aşağıdaki hususlarda düzenleme yapılmasının olmazsa olmaz nitelik taşıdığı sonucuna varmıştır[15]:

• Saklama faaliyetinde bulunan kuruluşlar kendisine saklamaları için bırakılan varlıkları ve müşterilerinin haklarını özellikle iflas söz konusu olduğu durumlarda kayıp ve kötüye kullanma ihtimallerine karşı koruyacak önlemleri almalıdır.

• Saklama faaliyetinde bulunan kuruluşlar, operasyonel, siber dayanıklılık ve riskleri minimize etmek için gerekli kontrol mekanizmalarını devreye sokmalıdır.

• Müşteri varlıklarına ilişkin doğru ve güncel kayıtlar tutulmalıdır.

• Kripto varlıklar, saklayıcının kendi varlıklarından ayrı tutulmalıdır.

• Müşteri varlıklarının devrine ilişkin aranjmanlar ve müşteri varlıklarının yeniden kullanılması için müşterinin önceden açık rızasının alınmış olması ve bu konuda bilgilendirme yükümlülüğünün gerçekleştirilmiş olması gerekmektedir.

• Saklama faaliyeti, harici bir kaynak desteği ile sağlandığında (outsourcing), aynı güvenceler ve risk yönetimi için gerekli önlemler yine alınmalıdır.

• Saklama faaliyetinde bulunan kuruluş, saklama faaliyetine ilişkin anlaşmadan kaynaklanan hak ve yükümlülükler konusunda şeffaf olmalıdır.

• Saklamanın da dahil olduğu birden çok işlevi yerine getiren kripto varlık hizmet sağlayıcılar her türlü menfaat çatışmasını tespit etmeli, açıklamalı ve yönetmelidir.

Kripto varlıkların saklanması konusundaki bu genel bilgilerden sonra, çalışmamızın bu kısmında Türkiye'de ve Dünya'da özellikle kripto varlık ekosisteminde önde gelen ülkelerde ne gibi adımlar atıldığına ilişkin güncel duruma ilişkin bilgi verilecektir.

2. Türkiye'deki Durum

Kripto varlık saklamanın temelleri birçok ülkede olduğu gibi Türkiye'de de geleneksel finansa ve özellikle banka hukukunda uygulama bulan saklama sözleşmesine dayanmaktadır. Türk Borçlar Kanunu md. 561'e göre, saklama sözleşmesi, saklayanın, saklatanın kendisine bıraktığı bir taşınırı güvenli bir yerde koruma altına almayı üstlendiği sözleşmedir. Açıkça öngörüldüğü veya durum ve koşullar gerektirdiği takdirde, saklayan ücret isteyebilir. Aynı Kanun'un 568. maddesine göre, bir üçüncü kişi, saklanan üzerinde ayni hak iddiasında bulunsa bile, saklanan haczedilmedikçe veya saklayana karşı istihkak davası açılmadıkça saklayan, onu saklatana geri vermekle yükümlüdür. Para ve kıymetli evrakların saklanması ise, Kanun'un "mislî şeylerin saklanması" başlıklı 570. maddesinde ayrıca düzenlenmektedir. Buna göre, saklayanın kendisine bırakılan parayı aynen geri vermek zorunda olmaksızın mislen geri vermesi açıkça veya örtülü olarak kararlaştırılmışsa, o paranın yararı ve hasarı kendisine ait olur. Paranın mühürsüz ve açık olarak bırakılmış olması, örtülü anlaşma sayılır. Saklayan, saklatan tarafından kendisine açıkça yetki verilmedikçe, saklanan diğer mislî eşya veya kıymetli evrak üzerinde tasarrufta bulunamaz.

15 *Dirk Zetzsche, Julia Sinnig, Areti Nikolakopoulou, Crypto custody, Capital Markets Law Journal, Volume 19, Issue 3, July 2024, Pages 207–229, https://doi.org/10.1093/cmlj/kmae010, s. 211 vd.*

Borçlar Kanunu saklama sözleşmesinin temel esaslarını belirlemekle birlikte, özellikle bankacılık işlemleri kapsamında saklama sözleşmesine ilişkin daha ayrıntılı ve zaman zaman farklılaşan uygulamalar söz konusu olmaktadır.

Dünya'da pek çok ülkede olduğu gibi, Türkiye'de geleneksel finans merkeziyetsiz finansa doğru evrilmektedir. Türkiye'de faaliyet gösteren kripto varlık borsaları, kullanıcıların kripto varlık alım satımı yapmasına olanak tanımanın yanı sıra, aynı zamanda saklama hizmetleri de sunmaktadır. Yerel borsalar, kullanıcıların kripto varlıklarını güvenli bir şekilde saklamalarını sağlamak için çeşitli güvenlik protokolleri ve teknolojik çözümler kullanmaktadır. Bunun dışında, bağımsız saklama hizmet sağlayıcıları da, kripto varlıkların güvenli bir şekilde saklanması konusunda uzmanlaşmış firmalardır. Bu firmalar, kullanıcıların varlıklarını güvenli bir şekilde saklamak için soğuk cüzdanlar, çoklu imza protokolleri ve diğer güvenlik önlemleri kullanmaktadır. Türkiye'de bu alanda faaliyet gösteren ve uluslararası standartlara uygun hizmetler sunan firmalar bulunmaktadır.

Temmuz 2024'e kadar kripto varlık saklama faaliyetlerinin düzenlenmesini konu edinen bir hukuki çerçeve mevcut değildi ya da buna daha önceden herhangi bir mevzuatta değinilmemişti. Kripto varlıkların saklanması, 2021 yılında yürürlüğe giren Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik m.4/2'de ödeme ve elektronik para kuruluşlarının aracılık edemeyeceği faaliyetler kapsamında geçmekteydi: Ödeme ve elektronik para kuruluşları, kripto varlıklara ilişkin alım satım, saklama, transfer veya ihraç hizmeti sunan platformlara veya bu platformlardan yapılacak fon aktarımlarına aracılık edemez. Burada belirtilen "saklama" faaliyetinden kasıtın ne olduğu belirtilmemişti.

Bununla birlikte, saklama faaliyetine ilişkin bazı çalışmalar sektörün ihtiyaçları doğrultusunda öneriler sunmaktaydı. Örneğin Türkiye Bankalar Birliği tarafından 2022 yılında yayınlanan raporda şu ifadelere yer verilmişti: "Dijital varlıkların lisanslı saklama kuruluşları tarafından saklanması ve kurumsal muhatapların piyasadaki yerini alması, karmaşık süreçlerin ve riskin azaltılması, güvenilirliğin artması açısından yatırımcılar üzerinde olumlu etki yaratacaktır. Diğer taraftan bankaların, dijital varlık piyasasında etkin bir aktöre dönüşmesini sağlayacak saklama hizmetini vermeye başlamaları, her geçen gün sayıları artan biçimde yeni müşteri kazanımı, (genç müşteri kitlelerine ulaşabilme), yeni ya da geleneksel bankacılık ürünleri ile hibrit ürünler tasarlama fırsatı ve rekabette teknoloji avantajı ile öne çıkmalarına katkıda bulunacaktır. Bunun yanında saklama hizmetleri ve kripto ekosistemine entegrasyonun bankalara yeni müşteri kazanımı, büyüme, bilinirlik, yenilikçi marka imajı ve adını sayamayacağımız onlarca alanda değer katması mümkün gözüküyor. "[16] Diğer taraftan, aynı raporda bu hizmetin bankalar tarafından verilmesi halinde ortaya çıkabilecek risk ve zorlukların da altı çizilmiştir: "Bunların başlıcaları; süreçlerin karmaşık ve çok aşamalı yapısı, KYC/AML süreçleri, izlenebilirlik ve mutabakat problemleri, işlem hacimlerindeki volatilite, saklama altında tutulacak varlık değerinin büyüklüğü nedeniyle saldırıların hedefi olma riski, siber güvenliğin sağlanması, risk kontrolü ve sigorta vb. kalemlerin yaratacağı maliyet artışı, regülasyon yokluğu/ belirsizlikleri (varlığın güven altında olmasının nasıl sağlanacağı ve varlıkların sınıflandırılması vb.) olarak sayılabilir."

Türkiye'de kripto varlık saklama hizmetlerine yönelik yasal çerçeve, Sermaye Piyasası Kurulu (SPK), Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) ve Mali Suçları Araştırma Kurulu (MASAK) tarafından belirlenen düzenlemelerle şekillendirilmektedir.

16 *Türkiye Bankalar Birliği, Dijital Varlıklara Yönelik Bankacılık Açısından Genel Bakış, Potansiyel İş Modelleri ve Dijital Varlıkların Hukuki Açıdan Değerlendirmesi (07.02.2022), s. 23*

Sermaye Piyasası Kurulu, 2 Temmuz 2024'te yürürlüğe giren 7518 sayılı Sermaye Piyasası Kanununda Değişiklik Yapılmasına Dair Kanun ile 6362 sayılı Sermaye Piyasası Kanunu çerçevesinde, kripto varlık saklama hizmet sağlayıcılarının faaliyetlerini denetleme ve düzenleme yetkisine sahip olduğu belirlenmiş oldu. SPK, kripto varlıkların saklanması ve yönetilmesi ile ilgili olarak gerekli standartları ve yükümlülükleri belirler, ayrıca bu hizmetlerin yasalara uygunluğunu ve piyasa şeffaflığını sağlamayı hedefler.

Sermaye Piyasası Kanunu (SerPK) md. 3'te, kripto varlık hizmet sağlayıcı, kripto varlık saklama hizmeti ve platform kavramlarının tanımlarına yer verilmiştir. Buna göre, kripto varlık hizmet sağlayıcıların kapsamına; platformlar, kripto varlık saklama hizmeti sağlayan kuruluşlar ve bu Kanuna dayanılarak yapılacak düzenlemelerde kripto varlıkların ilk satış ya da dağıtımı dâhil olmak üzere kripto varlıklarla ilgili olarak hizmet sağlamak üzere belirlenmiş diğer kuruluşlar girmektedir. Aynı maddede kripto varlık saklama hizmetinden ne anlaşılması gerektiğine ilişkin bir tanıma da yer verilmiştir. Bu çerçevede, kripto varlık saklama hizmeti, platform müşterilerinin kripto varlıklarının veya bu varlıklara ilişkin cüzdandan transfer hakkı sağlayan gizli anahtarların saklanmasını, yönetimini veya Sermaye Piyasası Kurulunca belirlenecek diğer saklama hizmetlerini ifade etmektedir.

SerPK 35B/4 maddesine göre, platformlar üzerinden kripto varlıkların alınıp satılmasına ve ilk satış ya da dağıtımının yapılmasına, kripto varlıkların takasına, transferine ve saklanmasına ilişkin usul ve esaslar Kurul tarafından düzenlenir.

SerPK 35C/6 maddesine göre, platformların müşterilerine ait kripto varlıkların müşterilerin kendi cüzdanlarında bulundurulması esastır. Müşterilerin kendi cüzdanlarında bulundurmayı tercih etmedikleri kripto varlıklara ilişkin saklama hizmetinin, Kurul tarafından yapılacak düzenleme uyarınca yetkilendirilmiş ve Bankacılık Düzenleme ve Denetleme Kurulu tarafından uygun görülen bankalarca veya Kurulca kripto varlık saklama hizmeti sunma konusunda yetkilendirilmiş diğer kuruluşlarca sunulması ve müşterilere ait nakitlerin bankalarda tutulması zorunludur. Bankalar nezdinde saklanan kripto varlıklar ile müşterilere ait bu kapsamdaki nakitler 5411 sayılı Kanunun 63.maddesinde düzenlenen mevduat ve katılım fonunun sigortalanması hükümlerine tabi değildir. Kurul, her bir kripto varlık için veya bunların dayandığı teknolojik özellikler ya da kripto varlıkların nitelik ve nicelikleri kapsamında saklama konusunda ayrı esaslar belirlemeye yetkilidir.

SerPK madde 35/C/7 uyarınca,müşterilere ait nakit ve kripto varlıklar, kripto varlık hizmet sağlayıcıların mal varlığından ayrı olup, kayıtlar da bu hükme uygun olarak tutulur. Müşterilerin her ne suretle olursa olsun kripto varlık hizmet sağlayıcıların nezdinde bulunan nakit ve kripto varlıkları, kripto varlık hizmet sağlayıcılarının borçları nedeniyle, kripto varlık hizmet sağlayıcılarının mal varlığı ise müşterilerin borçları nedeniyle kamu alacakları için olsa dahi haczedilemez, rehnedilemez, iflas masasına dâhil edilemez ve üzerlerine ihtiyati tedbir konulamaz. Kripto varlık hizmet sağlayıcıları tarafından müşteri nakitlerinin bankalarda tutulmasına ilişkin olarak bu Kanunun 46. maddesinin 7. ve 8. fıkraları kripto varlık hizmet sağlayıcıları bakımından da uygulanır.

SPK'da değişiklik yapılmasına ilişkin kanunun yürürlüğe girmesiyle birlikte, SPK bir dizi rehber, bildiri ve ilke kararı yayınlamış ve kripto varlık ekosisteminde halihazırda faaliyet gösteren ve faaliyet göstermek isteği bulunan firmalardan başvuruları toplamıştır.

SPK'nın web sitesinde SerPK Geçici 11.maddesi uyarınca faaliyette bulunacaklarını beyan eden kuruluşlara dair kamunun bilgilendirilmesi amacıyla oluşturulan bir liste yayınlamıştır. Bu çerçevede, Mart 2025 itibariyle belirtilen listede yer alan kuruluşların ilgili mevzuat uyarınca yetkilendirildiği anlamına gelmemekle birlikte, başvurusunun yanında "saklama başvurusu" yazan on bir adet kuruluş bulunmaktadır.

SPK, Kanun'da meydana gelen değişikliklerden sonra, kripto varlık ekosistemine ilişkin düzenlemeleri ilke kararı ve duyurularla devam ettirmiştir. Bu kapsamda, Sermaye Piyasası Kurulu Karar Organı'nın i-SPK.35.B.1 (19/09/2024 tarih ve 1484 s.k.) sayılı İlke Kararı'nda saklama konusunu da ilgilendiren noktalar bulunmaktadır:

• Sermaye Piyasası Kanunu'nun 35/C maddesinin 6. fıkrasında müşterilere ait nakitlerin bankalarda tutulmasının zorunlu olduğu; aynı maddenin 7. fıkrasında ise müşterilere ait nakit ve kripto varlıkların, kripto varlık hizmet sağlayıcıların mal varlığından ayrı olduğu ve kayıtların da bu hükme uygun olarak tutulması gerektiği düzenlenmiştir. Kanun'un 46.maddesinin 7. fıkrasında ise, bankalar nezdinde tutulmakta olan müşteri nakitlerinin platform müşterileri için açılacak olan münferit bir hesapta, platformun kendi nakit varlığından ayrı olarak izlenmesinin esas olduğu düzenlenmiştir. Bu kapsamda platform müşterilerinin nakit transferlerinin bankalar veya ilgili mevzuat uyarınca bu konuda yetkilendirilmiş kuruluşlar aracılığıyla gerçekleştirilmesi zorunludur. Platformlarca müşteri nakitleri elden alınamaz, müşteriye elden teslim edilemez ve platformlar nezdinde herhangi bir şekilde saklanamaz.

• 2. maddede uygun görülen ortam veya yöntemler dışında, döviz bürosu benzeri yapıda çalışmak suretiyle kripto varlıkların alım satım, ilk satış ya da dağıtım, takas, transfer, bunların gerektirdiği saklama işlemlerini gerçekleştirilmesi veya müşterilerin kripto varlıklarının nakde veya nakdinin kripto varlıklara çevrilmesi vb. işlemlerin düzenli uğraşı, ticari veya mesleki faaliyet olarak icra edilmesi, Kanun'un 99/A ve 109/A maddeleri kapsamında değerlendirilir.

• 7/b (a) bendinde açıklanan hususlar sermaye piyasası mevzuatı bakımından da geçerli olup, kripto varlıkların saklama altyapısının ve rezerv kanıt mekanizmalarının henüz işler hale gelmediği dikkate alınarak; Kanun'un 13. maddesi uyarınca sermaye piyasası araçlarının kripto varlık olarak ihracına yönelik Kurulca düzenleme yapılmadan önce, Kanun'un 3. maddesinde tanımlanan sermaye piyasası araçları ve sermaye piyasası araçları ile ilişkili olarak değeri belirlenen endeksler, çeşitli varlık gruplarının (kripto varlıklar dahil) bir araya getirildikleri sepetler, kıymetli madenler ile VII-128.3 sayılı Varantlar ve Yatırım Kuruluşları Sertifikaları Tebliği'nde düzenlenen dayanak varlıklara dayalı olarak kripto varlık ihraç edilemez ve platformlarda listelenemez.

• Kripto varlıkların müşterilerin kendi cüzdanlarında saklanmaması halinde, platformlar nezdindeki kayıtlarda müşteri hesaplarında yer alan kripto varlıkların saklandığı cüzdanların anahtarlarına ilişkin kontrolün, en geç 08.11.2024 tarihine kadar platformlarda olması gerekir. Bu hükme aykırı uygulamalar Kanunun 110/A maddesi kapsamında değerlendirilir.

Mevcutta, kripto varlık saklama hizmeti vermeyi taahhüt eden firmaların SPK'na başvuru yaparak belli başlı belgeleri iletmeleri gerekmektedir. Buradaki başvuru, kripto varlık saklamasına yönelik lisans başvurusu değil, bir nevi faaliyette bulunacağına yönelik bir taahhüt niteliğindedir.

Bu başvuru kapsamında, ortaklar, yönetim kurulu üyeleri, genel müdür ve genel müdür yardımcılarına yönelik birtakım belgelerin, başvuru yapan Şirket'in kullandığı bilgi sistemleri altyapısına, müşteri varlıklarının korunmasına ilişkin süreç ve araçlarına, yapılan işlemlerin blokzinciri sistemine işlenmesine ilişkin süreçlere, AML/CFT sistemleri ya da kamu otoritelerine raporlama vb. iç ve dış sistemlerle yapılmış olan entegrasyonlara, operasyon ve raporlama süreçlerine, risk yönetim süreçlerinin işleyişine ilişkin belgelere, kripto varlıkların ve müşterilerin nakit varlıklarına ilişkin saklama sisteminin işleyişine, kripto varlıkların saklanmasına yönelik alınan hizmetlere, saklama süreçlerinin hangi cüzdan teknolojileri kullanılarak yapıldığına yönelik belgelerin iletilmesi gerekmektedir.[17] Bundan sonra SPK tarafından yapılacak değerlendirmeye istinaden, ilgili Şirket'in saklama hizmeti vermesine yönelik faaliyette bulunanlar listesine[18] girmesine izin verebilir.

13.03.2025 tarihinde Resmi Gazete'de yayımlanan Kripto Varlık Hizmet Sağlayıcıların Kuruluş ve Faaliyet Esasları Hakkında Tebliğ (III-35/B.1), Kripto Varlık Hizmet Sağlayıcıların Çalışma Usul ve Esasları Hakkında Tebliğ (III-35/B.2), Bilgi Sistemleri Bağımsız Denetim Tebliği (III-62.2.b) ve Bilgi Sistemleri Yönetimine İlişkin Usul ve Esaslar Tebliği (VII-128.10) adlı Sermaye Piyasası Kurulu tebliğleri, saklama konusunda Türkiye'de bugüne kadar yapılmış olan en geniş ve detaylı düzenlemeleri içermektedir. Saklama hizmeti veren banka, kripto varlık hizmet sağlayıcılar gibi farklı kuruluşlara yönelik kural, ilke ve esasların yer aldığı bu düzenlemeler saklama faaliyetlerinin kapsamının anlaşılması hususunda oldukça açıklayıcı olmuştur. Kripto Varlık Hizmet Sağlayıcıların Kuruluş ve Faaliyet Esasları Hakkında Tebliğ (III-35/B.1)'in amacı kripto varlık hizmet sağlayıcıların kuruluşuna, faaliyete geçmesine, faaliyetine ve faaliyetlerinin durdurulmasına ilişkin usul ve esasları düzenlemektir.

Tebliğ'in 4. Maddesinde, kripto varlık saklama faaliyetini, "Müşterilerin kripto varlıklarının veya bu varlıklara ilişkin cüzdandan transfer hakkı sağlayan özel anahtarların saklanmasını, yönetimini veya Kurulca belirlenecek diğer saklama hizmetleri" olarak tanımlanmaktadır. Tebliğ'in 5. 6. 7. Maddelerinde kripto varlık saklama hizmeti verecek olan şirketin kuruluşa dair şartları; 9 ile 19. Madde arasında ise kripto varlık saklama faaliyetine geçmek için aranan şartların neler olduğu belirtilmektedir.

Kripto varlık saklama kuruluşlarının internet sitelerinde, anlaşmalı oldukları platformların ünvanlarına, saklama hizmeti sundukları kripto varlıkların listesinde yer vermeleri ve bunları güncel tutmaları zorunludur. Bu sayede, kripto varlık saklama kuruluşlarının şeffaf bir şekilde hangi firmalar tarafından kullanıldığı kontrol edilebilmektedir.

Tebliğ'in 1. Geçici Maddesi'ne göre, 13 Mart 2025, yani Tebliğ'in yayımlandığı tarih itibariyla SPK'nın internet sitesinde "Faaliyette Bulunanlar Listesi"nde yer alan saklama kuruluşları ile bu Tebliğ'in yayımı tarihinde önde başvuru yapmış saklama kuruluşlarının 30 Haziran 2025 tarihine kadar faaliyet izninine başvurmaları gerekir.

Kripto Varlık Hizmet Sağlayıcıların Çalışma Usul ve Esasları ile Sermaye Yeterliliği Hakkında Tebliğ (III-35/B.2)'in 2. maddesinde açıkça kripto varlık hizmet sağlayıcıların sunabilecekleri hizmet ve faaliyetler, bunlara ilişkin esaslar, kripto varlıkların listeleme esasları, mutabakat sistemi ile sermayelerine ve sermaye yeterliliklerine ilişkin ilke ve esasların düzenlendiği görülmektedir. Aynı tebliğin "Kripto Varlık Hizmet Sağlayıcıların Hizmet ve Faaliyetleri" başlıklı 5. maddedesinde saklama kapsamına giren faaliyetler belirtilmektedir:

17 *https://spk.gov.tr/data/668412388f95db0c2c4e36d5/Ek-1%20Duyuru-Talep%20Edilen%20Belgeler.pdf*

18 *https://spk.gov.tr/kurumlar/kripto-varlik-hizmet-saglayicilar/faaliyette-bulunanlar-listesi*

a) Kripto varlıklarla ilgili emirlerin alınması ve gerçekleştirilmesi, takası, kripto varlıkların transferi ile bunların gerektirdiği saklama hizmetleri ve c) Kripto varlıkların veya bu varlıklara ilişkin özel anahtarların saklanması, yönetimi veya Kurulca belirlenecek diğer saklama hizmetleri. Bu faaliyetler ile uğraşan her bir saklama kuruluşunun mutlaka Sermaye Piyasası Kurulu'ndan izin alması gerekir.

Tebliğ (III-35/B.2)'in "Platform Faaliyetlerine İlişkin Esaslar" başlıklı 3. bölümünde ilk olarak platformların faaliyetleri ve genel esasları hakkında düzenleme yapılmakta ve ardından platformların işlem ortamı oluşturabilmesi, müşteri emirlerini karşı taraf olarak gerçekleştirebilmesi, fiyat gözetim sistemi kurabilmesi için tabi olduğu yükümlülükler sıralanmaktadır. Tebliğ (III-35/B.2)'in "Müşterilere Ait Kripto Varlıkların Platformlar Nezdinde Saklanması" başlıklı 17. maddesinde, platformların müşterilerine ait kripto varlıkları, sermaye yeterliliği yükümlülüklerinde belirlenen sınırlamalara uygun olmak kaydıyla, toplu bir şekilde bir veya birden fazla cüzdanda saklanabileceği husus ile açıkça platformlara saklama hizmeti verme yetkisi tanındığı görülmektedir.

Tebliğ (III-35/B.2)'in "Saklama Hizmeti ve Transfer Esasları" başlıklı 5. bölümünde yer alan 24. maddede kripto varlık saklama hizmeti, "platform müşterilerinin kendi cüzdanlarında bulundurmayı tercih etmedikleri kripto varlıkların veya bu varlıklara ilişkin özel anahtarların saklanmasını, yönetimini veya Kurulca belirlenecek diğer saklama hizmetleri" şeklinde belirtilmektedir. Bununla birlikte, saklama kuruluşlarının platform müşterileri haricinde, müşterilere doğrudan saklama hizmeti vermesi mümkün kılınmaktadır. Ancak özel anahtarın bütün kontrolünün yatırımcıya bırakıldığı yöntemle cüzdan hizmetlerinin sunulması saklama hizmeti olarak değerlendirilmez. Tebliğ (III-35/B.2)'in 25. maddesinde, saklama hizmetinde bulunabilecek kuruluşların bu Tebliğ uyarınca kripto varlık saklama hizmeti vermeye yetkili kılınmış ve BDDK tarafından uygun görülen bankalar veya Sermaye Piyasası Kurulunca kripto varlık saklama hizmeti sunma konusunda yetkilendirilmiş diğer kuruluşlar olduğu belirtilmektedir.

Saklama kuruluşları, müşterilere ait kripto varlıkları, kendi hesaplarından ayrı olarak platform adına toplu olarak saklamakla yükümlüdür. 5549 sayılı Kanun ve ilgili mevzuat hükümleri saklı kalmak üzere, platformların müşterilerinin saklama kuruluşu ile harici bir sözleşme imzalamalarına gerek bulunmamaktadır. Saklama kuruluşlarının Tebliğ (III-35/B.2)'in 24. maddesinin 2. fıkrası kapsamında müşterilere doğrudan saklama hizmeti vermesi durumunda, söz konusu hizmete ilişkin olarak saklama kuruluşunun bu müşterilerle ayrıca bir sözleşme yapması ve bu hizmetten doğabilecek riskleri müşterilere açık ve detaylı bir şekilde aktarılmasını sağlaması zorunludur. Saklama kuruluşunun müşteri varlıklarının kontrolü için kullandığı tüm anahtar ve parçalarının güvenli donanım modüllerinde TÜBİTAK Altyapı Kriterlerinde belirlenen esaslar kapsamında tutulması gerekir.

Saklama hizmetinin bu Tebliğ (III-35/B.2)'de belirlenen esaslar kapsamında sunulmasına ilişkin hususların yer aldığı ve saklama kuruluşunun yönetim kurulu kararıyla yürürlüğe girecek yazılı bir prosedür oluşturulması ve bu prosedürün yılda en az bir kez gözden geçirilerek güncelliğinin sağlanması gerekmektedir. Saklama kuruluşlarının, kripto varlıkları sakladıkları sıcak cüzdan büyüklüğünün toplam müşteri varlığının %5'ine kadar olması gerektiği öngörülmektedir.

Kripto varlık hizmet sağlayıcılar tarafından özel anahtarlar ve özel anahtarların üretiminde kullanılan mekanizmalar ile yedeklenmeleri sürecinde kullanılan anahtarlar gibi varlık ve mekanizmaların yönetilmesine ve erişilmesine ilişkin olarak TÜBİTAK Altyapı Kriterlerinde belirlenen esaslara uyulmalıdır. Özel anahtarların, çok taraflı eşik kriptografisi gibi mekanizmalarla parçalara ayrılması durumunda her bir parçanın ve anahtar parçalarının kullanıldığı mekanizmaların, yedekleri dahil olmak üzere Türkiye'de tutulması ve bunlara ilişkin kontrolün kripto varlık hizmet sağlayıcılarda olması gerekir.

Tebliğ (III-35/B.2)'in 31. maddesi uyarınca, platformlar ile saklama kuruluşları arasında bir hizmet sözleşmesi imzalanması zorunludur. Bu sözleşmede, saklama kuruluşları tarafından işlemlerin dağıtık defter ağı sistemine işlenmesi, dağıtık defter ağı sisteminin yürütülmesinden kaynaklı olarak katlanacağı maliyetin nasıl yansıtılacağı ve sözleşmenin feshi durumunda tarafların hak ve yükümlülükleri hususlarına yer verilir. Saklama kuruluşunun bu Tebliğ (III-35/B.2)'de aranan şartları kaybetmesi halinde platformların başka bir saklama kuruluşu ile sözleşme imzalaması şarttır. Yeni sözleşme yürürlüğe girene kadar eski sözleşmeye taraf olan saklama kuruluşunun sorumluluğu devam eder. Saklama kuruluşlarının kuruluş sermayeleri, Tebliğ (III-35/B.2)'in 34. maddesi gereğince asgari 500.000.000 Türk Lirası olması zorunludur.

Tebliğ (III-35/B.2)'in "Saklama Limitleri ve Likit Rezerv Yükümlülüğü" başlıklı 41. maddesi uyarınca, müşterilerin kendi cüzdanlarında bulundurmayı tercih etmedikleri kripto varlıkların asgari %95'inin bu Tebliğ (III-35/B.2)'de belirtilen hükümler dahilinde saklama kuruluşunda saklanması esastır. Saklama kuruluşunda saklanmayan azami %5'lik kısım platform nezdindeki cüzdanlarda ilgili Tebliğ'in 26. maddesinde belirlenen esaslar çerçevesinde saklanır.

3. Kripto Varlık Ekosisteminde Ön Plana Çıkan Diğer Bazı Ülkelerdeki Mevcut Hukuki Çerçeve

3.1 Avrupa Birliği'nde Kripto Varlıkların Saklanması Süreci ve MiCA Tüzüğü (Markets in Crypto Assets Regulation- MiCAR) Düzenlemeleri

MiCA'nın Avrupa Birliği'nde yürürlüğe girmesi, AB dışındaki ülkeler açısından da önemli bir dönüm noktası olarak kabul edilmektedir. MiCA, kripto varlık hizmet sağlayıcıları (KVHS) ve saklama hizmetleri gibi alanlarda detaylı düzenlemeler getirmek suretiyle, yalnızca Avrupa Birliği sınırları içinde değil, aynı zamanda küresel kripto varlık piyasalarında da bir standart oluşturmaktadır. MiCA'nın kapsamlı düzenleyici yapısı, kripto varlık piyasasında faaliyet gösteren firmalar için bir referans niteliği taşırken, diğer ülkelerin de kendi dijital finans stratejilerini gözden geçirmesine ve MiCA ile uyumlu bir çerçeve geliştirmesine yol açabileceği düşünülmektedir.

MiCA kapsamında kripto varlık hizmet sağlayıcıların hangi hizmetleri verebilecekleri tek tek sayılmıştır. MiCA, m. 3/1/16 kapsamında sayılmış olan kripto varlık hizmetlerini sunan kripto varlık hizmet sağlayıcılarını lisanslama ve diğer bazı finansal yükümlülüklerine tabi tutmaktadır. Sayılmış olan bu kripto varlık hizmetleri içinde kripto varlıkların müşteriler adına saklanması ve idare edilmesi de yer almaktadır (crypto assets custody services).[19]

19 *MiCA'nın "Tanımlar" (Definitions) başlıklı 3. maddesinin 16. fıkrasında "kripto varlık hizmeti" (crypto assets service) veya kripto varlıklarla ilişkilendirilebilecek faaliyetler arasında spesifik olarak "müşteriler adına kripto varlıkların saklama ve yönetimini sağlamak" şeklinde bir hizmet türü belirtilmiştir. Yine aynı düzenlemenin 17. fıkrası gereğince ise, müşteriler adına "kripto varlıkların saklama ve yönetimini sağlama"nın ise "müşteriler adına kripto varlıkların veya bu kripto varlıklara erişim araçlarının, uygulanabildiği durumlarda özel kriptografik anahtarlar şeklinde, saklanması veya kontrol edilmesi anlamına geleceği" belirtilmiştir.*

Sundukları hizmetlere bağlı olarak ve her bir hizmet türünün ortaya çıkardığı spesifik riskler nedeniyle, kripto varlık saklama hizmeti sunanlar, bu hizmetlere özgü gerekliliklere tabi olmalıdır.

MiCA'nın sunduğu saklama hizmetleri ile ilgili yükümlülükler ve güvenlik önlemleri, bu hizmetleri sunan şirketlerin operasyonel süreçlerini ve uyum politikalarını yeniden şekillendirebilecektir. Bundan dolayı da AB dışında kalan ülkelerdeki kripto varlık hizmet sağlayıcılarının MiCA'nın temel prensiplerini içeren benzer düzenlemeler geliştirmesi veya kendi iç hukuklarında MiCA'ya uyumlu eklemeler yapması da beklenebilecektir.

MiCA, saklama hizmetleri de dahil olmak üzere KVHS'lere yukarıda sunacakları hizmetlerle ilgili belirli bir lisans gerekliliği de öngörmektedir.[20] Bu bağlamda MiCA m. 59 gereğince kripto varlık hizmet sağlayıcı, mesleği veya uğraşı sebebiyle üçüncü kişilere yönelik profesyonel şekilde bir veya birden çok kripto varlık hizmeti sunan ve bu faaliyetleri sunmasına izin verilen tüzel kişi veya kuruluşlar şekilde belirtilmiştir.[21] Dolayısıyla, KVHS olarak faaliyet göstermek isteyen kuruluşların Avrupa Birliği'ne üye bir devlette kayıtlı bir ofisinin bulunması zorunludur.[22] Bu amaçla, AB üyesi devletteki yetkili makamlar nezdinde resmi bir başvuru yapılması gerekmektedir.[23]

Genel itibariyle, KVHS'ler açısından lisans koşulları incelendiğinde, KVHS'lerin verecekleri hizmetlere bağlı olarak lisans koşulları değişkenlik göstermekle beraber (i) belirli bir asgari sermaye bulundurma gereksinimi, (ii) organizasyonel gereksinimler (ortaklık yapısı, çalıştırılan personel vb.) ile (iii) iş davranışı gereksinimi (dürüst, adil, profesyonel şekilde ve müşteri menfaatini ön planda tutma vb.) gibi farklı kriterler belirlenmiştir.[24]

MiCA m.83'e göre, müşteriler adına kripto varlıkların saklama ve idaresini sağlayan KVHS'ler, müşterileriyle belirli zorunlu hükümler içeren bir sözleşme imzalamalı ve müşterilerin talebi üzerine elektronik formatta sunulması gereken bir saklama politikası oluşturmalı ve uygulamalıdır. Buna göre, KVHS'ler müşterileri ile elektronik ortamda akdedecekleri sözleşmede müşterilere ait kripto varlıkların tutulmasını veya bu tür kripto varlıklara erişim araçlarını içerebilecek şekilde hizmetin niteliğini belirtmelidir. Bu durumda müşteri, kripto varlıkların kontrolünü kendi gözetimi altında tutma imkanını haiz olmalıdır. Alternatif olarak, kripto varlıklar veya bunlara erişim araçları kripto varlık hizmet sağlayıcısının tam kontrolüne devredilebilir. Müşterilere ait kripto varlıkları veya bu kripto varlıklara erişim araçlarını elinde bulunduran kripto varlık hizmet sağlayıcıları, bu kripto varlıkların kendi hesapları için kullanılmadığından emin olmalıdır. Kripto varlık hizmet sağlayıcıları, tuttukları tüm kripto varlıkların herhangi bir yükümlülük veya sınırlamaya tabi olmamasını devamlı olarak sağlamalıdır.

20 *MiCA m. 63. "Lisans Verilmesi veya Reddedilmesinin Değerlendirilmesi" (Assessment of the Application for Authorisation and Grant or Refusal of Authorisation) başlıklı ilgili düzenlemede, KVHS'lerin lisans süreçleri ile ilgili başvuruları açısından sürecin hangi kriterler bağlamında nasıl değerlendirileceğine dair detaylı hükümler söz konusudur.*

21 *MiCA m. 3/f. 1 (15)*

22 *ÇETİN, Müge: "Sermaye Piyasası Hukuku Bakımından Kripto Varlıklar", On İki Levha Yayıncılık, 1. Baskı, İstanbul, 2023, s. 103; ilgili esere elektronik ortamda ulaşmak için: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4346795 (S.E.T.: 09.10.2024)*

23 *ANNUNZİATA, Filippo: "The Licensing Rules in MiCA", Fintech Regulation and the Licensing Principle", (Ed: Moura Vincente, Diogo Pereira Duarte ve Catarina Granadeiro, European Banking Institute, 2023.*

24 *ÇETİN, s. 103*

Bu kripto varlık hizmet sağlayıcıları, siber saldırı, hırsızlık veya herhangi bir arızadan kaynaklanan bir olay da dahil olmak üzere, bilgi ve iletişim teknolojisiyle ("ICT") ilgili bir olaydan kaynaklanan herhangi bir kayıptan da sorumlu tutulmalıdır. Ancak hükmün içeriğinden anlaşıldığı üzere, burada KVHS'lerin bu tarz olası zararlar sebebiyle sorumluluğu kusur sorumluluğu şeklinde düzenlenmiştir.

Özellikle belirtilmesinde fayda bulunmaktadır ki kripto varlık saklama hizmeti ile ilgili KVHS'lere detaylı yükümlülükler öngören en önemli hükümlerinden birisi, MiCA'nın 75. maddesidir. İlgili hükmün içeriği incelendiğinde, maddenin ilk fıkrasında müşteriler adına kripto varlıkların saklanmasını ve idaresini sağlayan kripto varlık hizmet sağlayıcılarının, görevlerini ve sorumluluklarının çerçevesini belirlemek amacıyla müşterileriyle bir sözleşme[25] yapması gerektiği hüküm altına alınmıştır. Söz konusu sözleşmenin: (a) taraflarının kimliği; (b) sağlanan kripto varlık hizmetinin niteliği ve bu hizmetin bir tanımı; (c) saklama politikası; (d) müşterinin kimlik doğrulama sistemi de dahil olmak üzere kripto varlık hizmet sağlayıcısı ile müşteri arasındaki iletişim araçları; (e) kripto varlık hizmet sağlayıcısı tarafından kullanılan güvenlik sistemlerinin bir tanımı; (f) kripto varlık hizmet sağlayıcısı tarafından uygulanan ücretler, maliyetler ve masraflar; (g) uygulanacak hukuk gibi zorunlu unsurları içermesi öngörülmüştür.

Saklama noktasında, MiCA'da dikkat çeken bir diğer husus ise, kripto varlıkların saklama ve idaresini sağlayan KVHS'lerin müşterileri adına ve her bir müşterinin kripto varlıklar üzerindeki hak ve varlıklarına karşılık gelecek şekilde ayrı bir kayıt tutmalarının zorunlu kılınmasıdır.[26] Böylelikle kripto varlık hizmet sağlayıcıları, müşterilerinin talimatlarını takip eden her türlü hareketi mümkün olan en kısa sürede kaydetmekle yükümlüdür. MiCA, bu tür kayıtların iç prosedürlerle desteklenmesini ve kripto varlıkların kaydını etkileyen herhangi bir hareketin, müşterinin pozisyon kaydına düzenli olarak işlenen bir işlemle izlenip kanıtlanmasını sağlamaktadır. Buna ilaveten, ilgili KVHS bu tür kripto varlıkların saklanmasını veya kontrolünü ya da kripto varlıklara erişim araçlarını sağlamak için dahili kurallar ve prosedürler içeren bir saklama politikası [27] oluşturmalıdır. Saklama politikasının bir özeti, talep etmeleri halinde müşterilere elektronik bir formatta sunulacaktır.

Bunun dışında, MiCA yine önemli bir düzenleme olarak kripto varlıkların saklama ve idaresini sağlayan KVHS'ler açısından, müşterilerine en az üç ayda bir ve ilgili müşterinin talebi üzerine, bu müşteriler adına kaydedilen kripto varlıkların bir pozisyon kaydını sunma yükümlülüğü getirmektedir. [28]

25 *Türk Hukuku'nda olduğu gibi Avrupa Birliği Hukuku'nda da sözleşme denildiğinde mutlaka yazılı olması gibi bir hukuki zorunluluk bulunmamaktadır; KVHS gibi dijital ortamda faaliyet gösteren platformların müşterileri ile yaptıkları sözleşmeler çoğu kez dijital ortamda elektronik sözleşme olarak akdedilmektedir. Bu konuda ayrıntılı bilgi için bkz. MARYKE, Silalahi Nuth: "Electronic Contracting in Europe Benchmarking of National Contract Rules of United Kingdom, Germany, Italy and Norway in Light of the EU E-Commerce Directive", Universitet i Oslo, Complex nr. 2/2008, s. 33 vd.; ilgili esere elektronik ortamda erişim için bkz. https://www.jus.uio.no/ifp/forskning/om/publikasjoner/complex/2006-2011/complex-2008-02.pdf (S.E.T.: 09.10.2024)*

26 *MiCA m. 75/f. 2'de söz konusu kayıt, pozisyon kaydı (a register of positions) olarak nitelendirilmektedir.*

27 *Bahsi geçen KVHS'ler tarafından hazırlanacak saklama politikası ile dolandırıcılık, siber tehditler veya ihmal nedeniyle müşterilerin kripto varlıklarının veya bu kripto varlıklarla ilgili hakların veya kripto varlıklara erişim araçlarının kaybedilmesi riskinin en aza indirgenmesi öngörülmektedir. Bkz. MiCA, m. 75/f. 2/c. 3*

28 *KVHS'lerin pozisyon kaydına dair beyanları MiCA m. 75/f. 5'de "statement of position of the crypto-assets" şeklinde ifade edilmektedir.*

Bahsi geçen pozisyon kaydının, elektronik olarak düzenleneceği ve içeriğinde ilgili kripto varlıkları, bunların bakiyesini, değerini ve ilgili dönemde yapılan kripto varlık transferini tanımlayacağı belirtilmiştir.[29] Saklama hizmeti veren KVHS'ler açısından bir başka ön plana çıkan husus ise, KVHS'lerin özellikle müşterileri adına tuttukları kripto varlıkları kendi varlıklarından ayırması ve müşterilerinin kripto varlıklarına erişim araçlarının bu şekilde açıkça tanımlanmasının sağlanmasının öngörülmüş olmasıdır.[30] Saklanan kripto varlıklar, KVHS'nin alacaklılarının, özellikle iflas durumunda, KVHS tarafından saklanan kripto varlıklara başvurmamaları için yürürlükteki düzenlemelere uygun olarak KVHS'nin müşterilerinin çıkarına olacak şekilde KVHS'nin mal varlığından yasal olarak ayrılır. KVHS, saklanan kripto varlıkların operasyonel olarak kripto varlık hizmet sağlayıcısının mal varlığından ayrı tutulmasını sağlayacaktır.

Son olarak saklama hizmeti de dahil olmak üzere kripto varlıkların transfer hizmetini vermek isteyen KVHS'ler açısından MiCA'da 125.000 Euro gibi bir asgari sermaye zorunluluğu öngörülmektedir.[31]

MiCA'nın saklama rejimi, Avrupa Birliği'nde kripto varlık hizmet sağlayıcıları için kapsamlı bir çerçeve sunmakta olup sektörde güvenliği ve müşteri haklarını korumayı amaçlamaktadır. AB'de dijital finans alanında bir dönüm noktası olarak değerlendirilen bu düzenleme, hizmet sağlayıcıların lisans şartlarından iç prosedürlerin şeffaflığına kadar geniş bir yelpazede önemli gereklilikler getirmektedir. Ayrıca, hizmet sağlayıcıların müşterilere ait kripto varlıkları ve bu varlıklara erişim araçlarını kendi varlıklarından ayrı tutma zorunluluğu, müşteri güvenliğini artırarak kripto varlıkların korunmasını sağlamaktadır. MiCA'nın 2024 yılı sonunda tam anlamıyla yürürlüğe girmesiyle birlikte, AB içindeki kripto varlık piyasalarının daha güvenli, şeffaf ve düzenlenmiş bir yapıya kavuşması beklenmektedir.

MiCA'nın özellikle kripto varlık saklama kapsamında belirlemiş olduğu esasların sektördeki dengelere ve MiCA'nın amaçlarına uygun olup olmadığı, Avrupa ülkelerinde de tartışma konusudur. MiCA'nın odak noktasının "kurumsal dayanıklılık" (institutional resilience) olduğu belirtilmektedir. Kurumsal dayanıklılık, saklama servis sağlayıcısının sağlam bir şekilde organize olduğundan, yönetildiğinden ve müşterilerin varlıklarını kendi hesabına yeniden kullanmadığından emin olunması anlamına gelmektedir.

29 *MiCA m. 75/f. 5/c. 2*

30 *MiCA m. 75/f. 7 temelde MiCA'da öngörülen Türkiye'de 6362 Sayılı Sermaye Piyasası Kanunu'na da yansıyan ayırma kuralı (segregation rule) gereğince, KVHS'lerin müşterilerine ait malvarlıkları (fiyat para ve kripto varlık) kendi malvarlıklarından ayrılır. Böylece yine MiCA'nın ilgili düzenlemesine bakıldığında bu sayede örneğin iflas gibi bir durumda KVHS'lerin alacakları doğrudan alacakları için KVHS'lere başvuracak olup alacaklıların müşterilere karşı herhangi bir rücu hakkı olmayacağı hüküm altına alınmıştır.*

31 *MiCA'da EK 4 (Annex IV) başlığının altında Sınıf 2 (Class 2) olarak tanımlanan hizmetler,*

- *müşteriler adına kripto varlıkların saklama ve idaresinin sağlanması;*
- *fonlar için kripto varlıkların takası;*
- *ve/veya diğer kripto varlıklar için kripto varlıkların takası olarak nitelendirilmiş olup bu hizmetler açısından KVHS'lerin sağlaması gereken asgari sermaye miktarının 125.000 Euro olduğu belirtilmiştir. Türkiye'de ise kripto varlıklar ve KVHS'ler açısından önemli düzenlemeler öngören 7518 Sayılı Kanun ve akabinde SPK tarafından yayınlanan ilke kararları neticesinde (bkz. SPK'nını-SerPK.35.B (08/08/2024 tarih ve 42/1259 s.k.) sayılı İlke Kararı), Türkiye'de faaliyet iznine başvurmak isteyen KVHS'ler açısından asgari sermaye ve öz sermaye miktarının asgari 50 milyon TL olarak düzenlenmiştir.*

MiCA'ya göre saklama hizmeti sunan tüm KVHS'ler, yönetişim, çıkar çatışmaları, varlıkların ayrılması ve operasyonel risk yükümlülükleri gibi tüm kurallara tabidir. Bununla birlikte, MiCA'nın "varlıkların dayanıklılığı" (asset resilience) konusunda eksik noktaları olduğu belirtilmektedir. Varlıkların dayanıklılığı, saklama kuruluşunun, üçüncü tarafların, token ihraççısının veya DeFi uygulamasının, durum ne olursa olsun, zorluklarla karşılaştığı durumlarda güvenceler sağlama gücünü ifade etmektedir. Bu görüşte olan yazarlara göre, bu eksiklik kısmen DLT'nin doğasından ve kısmen de MiCA'nın özel hukuka ve özellikle kripto varlıklarla ilgili iflas işlemlerine dair düzenlemeler içermemesinden kaynaklanmaktadır. Her ne kadar ART'ler ve EMT'ler için ürün düzenlemeleri bu boşluğu bir nebze telafi etse de diğer kripto varlık sahiplerinin korumasız bırakıldığı belirtilmektedir. Bu bağlamda, MiCA'nın, koruma açısından emanetçilerin, diğer hizmet sağlayıcıların denetlenmesine ve üçüncü taraflara karşı yürütülen yasal süreçlerde müşterilerin çıkarlarının temsil edilmesine izin veren açık yetkiler aracılığıyla varlık dayanıklılığını sağlamada çok daha güçlü bir rol oynadığı TradFi düzenlemesinin gerisinde kaldığı belirtilmektedir.[32]

3.2. İsviçre

İsviçre, blokzinciri teknolojisini benimseyen ve "kripto vadisine" ev sahipliği yapan ülkelerden biri olarak, blokzinciri ve kripto varlık girişimlerinde aktif bir ekosisteme sahiptir. İsviçre, Finansal Piyasalar Denetleme Kurumu'nun (FINMA) pragmatik ve kapsayıcı yaklaşımı ve doğru zamanda yapılan hukuki düzenlemeler sayesinde, kripto varlık ekosistemindeki teknolojik gelişmelere hızla ayak uydurabilmektedir.

2018'den beri FINMA, hazırlamış olduğu ICO Guidelines isimli Rehber ile ödeme, hizmet ve varlık tokenleri arasında ayrım yapmaktadır[33]. Özellikle "varlık tokenleri"nin ihracı süreçlerini kolaylaştırmak ve cüzdan sağlayıcıları ile dijital varlık hizmet sağlayıcıları kullanan müşterilere daha yüksek koruma sağlamak amacıyla İsviçre'de dijital varlıkları düzenleyen bir hukuki çerçeve oluşturulmuştur. 2021 yılında yürürlüğe giren ve kısaca "DLT Act" olarak bilinen "Dağıtık Defter Teknolojisindeki Gelişmeleri Dikkate Almak İçin Federal Yasaların Değiştirilmesine İlişkin Federal Kanun" mevcut birçok farklı kanunda değişiklik yapılmasını öngörerek dijital varlıkların ihraç edilmesini daha kolay uygulanabilir bir süreç haline getirmiştir.

DLT Act'in yürürlüğe girmesiyle birlikte, Bankacılık Kanunu'nda m.16/1'e göre, müşteriler için saklama hizmeti kapsamında tutulan ödeme tokenlerinin iflas durumunda ayrı tutulmasına yönelik özel bir hukuki dayanak oluşturulmuştur. Saklama hesaplarının bu şekilde ayrılması ve sermaye gereksinimlerinden kaçınmak için bankalar, ödeme tokenlerini saklama hesabını müşterileri için her zaman hazırda tutmakla yükümlü kılınmıştır. Eğer bankalar kripto varlıkları kendileri saklamazlarsa, alt saklayıcının iflası durumunda da, İsviçre yasalarına göre veya yurtdışında benzer şekilde güvenli bir yasal dayanakla, müşterilerine iflas hukuku kapsamında koruma sağlandığından emin olmalıdırlar.

İsviçre, dijital varlık saklama alanında da öncü ülkelerden biri haline gelmiştir. Bu başarının, yeniliği ve çeşitliliği teşvik eden bir düzenleyici çerçevenin oluşturulması sayesinde elde edildiği düşünülmektedir.

32 *Dirk Zetzsche, Julia Sinnig, Areti Nikolakopoulou, Crypto custody, Capital Markets Law Journal, Volume 19, Issue 3, July 2024, Pages 207–229, https://doi.org/10.1093/cmlj/kmae010, s. 221 vd.*

33 *FINMA, Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs) Published 16 February 2018, https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf*

Şubat 2023'te FINMA tarafından hazırlanan raporda, yaklaşık 6 milyar CHF değerinde kripto varlığın saklama hizmeti kapsamında yer aldığı belirtilmektedir. Ayrıca, kripto varlık alanında faaliyet gösteren kurumların çoğunun saklama hizmeti sunduğu ancak bu hizmet için diğer bankalar ve menkul kıymet şirketlerinden üçüncü taraf saklama hizmeti sağlayıcıları olarak yararlandığı ortaya koyulmuştur.[34]

Haziran 2023'te İsviçre Dijital Varlık Saklama Raporu ülkedeki dijital varlık saklama ortamını, hizmet sağlayıcılarının sunduğu hizmetler, lisans durumları ve kullandıkları saklama türleri açısından incelemiş ve İsviçre'de saklama hizmeti sunan 57 şirket bulunduğunu tespit etmiştir. Bu şirketlerin %44,1'i banka veya eşdeğer bir lisansa sahip kurumlardır. Bu kurumlar arasında Swissquote gibi perakende ve çevrimiçi bankalar, Maerki Baumann gibi özel bankalar, Credit Suisse gibi evrensel bankalar, Sygnum gibi kripto bankalar ve Hypothekarbank Lenzburg gibi bölgesel bankaların yer aldığı belirtilmektedir.[35]

2024 yılında yayınlanan aynı isimli raporda[36], kripto varlık saklama hizmeti sunan kuruluşlar için üç temel risk bulunduğunun altı çizilmektedir: (i) Kullanıcı hataları gibi operasyonel riskler; (ii) hackleme veya sosyal mühendislik gibi siber güvenlik riskleri ve (iii) lisanslama ve iflas süreçlerine ilişkin hukuki belirsizlikler. Ayrıca, bir taraftan işlemlerin kullanıcı dostu bir şekilde gerçekleştirilmesini sağlarken, aynı anda gizli anahtarların güvenli bir şekilde saklanmasının, kripto varlık saklama hizmeti sunan kuruluşların en büyük zorluğu olduğu da belirtilmektedir.

İsviçre'de dijital varlık saklama hizmeti sunan tüm bankalar, müşteri varlıklarını bilançolarının dışında tutmakta ve böylelikle iflas durumunda koruma altına almaktadır. Bu korumanın sağlanıp sağlanmadığı, FINMA tarafından yakından takip edilmektedir. Bu uygulama, hem kurumsal müşteriler hem de varlıklı özel müşteriler için giderek daha önemli hale gelen bir güvenlik özelliği olarak değerlendirilmektedir.

İsviçre'de saklama hizmeti sunan sağlayıcılardan %30.6'lık bir kesim, NFT'leri de desteklemektedir. Bunlar genellikle kripto varlık hizmet sağlayıcı veya bu konuda özelleşmiş bankalardır.

İsviçre'de finansal kuruluşlar kayıp veya çalınma durumlarına karşı sigortayla güvence altına alınmıştır. Saklama hizmeti sunan bankaların sayısındaki artışla birlikte, sigortalanmış kripto varlık hizmet sağlayıcıların sayısı da bir önceki yıldaki %41.2'den %50'ye çıkmıştır.

İsviçre bankaları tarafından sunulan dijital varlık saklama hizmetinin bir diğer özelliği, İsviçre Banka Gizliliği Kanunu (Bank Secrecy Act) kapsamında sağlanan veri gizliliği korumasıdır. Saklama hizmeti sağlayıcılarının 16 tanesi, yani tüm sağlayıcıların %44,4'ü, yasal bir zorunluluk olarak İsviçre bankacılık gizliliği standartlarına uymaktadır.

2024 yılının sonunda bütünüyle yürürlüğe girecek olan MiCA'nın İsviçre'de saklama hizmeti sunan kripto varlık hizmet sağlayıcıları nasıl etkileyeceği de yukarıda bahsi geçen raporda değerlendirilmiştir. MiCA, saklama hizmeti sunan hizmet sağlayıcılar için lisanslama ihtiyacı, müşteri varlıklarının ayrıştırılması, sağlam yönetim yapısı, doğru kayıt tutma ve yeterli finansal kaynakların bulundurulması gibi katı yükümlülükler öngörmektedir.

34 *FINMA, Resolution Report 2020, https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/finma-publikationen/resolution-bericht/20200225-resolution-bericht-2020.pdf?sc_lang=en&hash=CCE986A47FCDE3D13A8DD4A748BC12DF'*

35 *Swiss Digital Custody Report 2023, https://static1.squarespace.com/static/6641b46de2c26a6478ff8f6e/t/666b18cdfb4ce0015152d037/1718294737562/Swiss+Digital+Asset+Custody+Report+2023.pdf*

36 *Swiss Digital Asset Custody Report 2024, https://static1.squarespace.com/static/6641b46de2c26a6478ff8f6e/t/668323ba60d1d203f76fff68/1719870411796/Swiss_+Digital_Asset_Custody_Report_2024.pdf, s. 36.*

İsviçre'deki mevcut saklama düzenlemeleriyle karşılaştırıldığında MiCA'nın çok daha katı olduğu belirtilmektedir. Bu nedenle AB içinde hizmet sunmayı hedefleyen İsviçre merkezli dijital varlık saklama kuruluşlarının – lisanslı veya AML düzenlemelerine tabi olup olmadıklarına bakılmaksızın – önünde iki seçenek bulunmaktadır: AB merkezli bir yan iştirak kurarak MiCA ile tam uyum sağlamak veya "reverse solicitation"[37] muafiyetini kullanarak, müşterinin talebi üzerine aktif pazarlama yapmadan hizmet sunmaktır. İlk seçeneğin tercih edilmesi halinde, Lihtenştayn'ın bir iştirak kurmak için iyi bir tercih olacağı düşünülmektedir. [38]

3.3 Birleşik Krallık

Birleşik Krallık'ta kripto varlıklarla ilgili hizmetler sunulabilmesi için kara para aklama düzenlemeleri (Money-Laundering Regulations-MLRs) kapsamında yer alan bu tür hizmetlerle ilgili olarak FCA'e başvurarak kayıt yapılması gerekmektedir. Kayıt gerekliliği, MLR'ın 8. ve 9. maddelerinde belirlenmiştir. İlgili Kanun'un 14/A maddesinde ise; kara para aklamanın önlenmesine ilişkin düzenlemelere tabi olan kripto varlık hizmetlerinin hangileri olduğu tanımlanmaktadır.

Hâlihazırda diğer hizmetler için FCA ile kayıtlı veya yetkilendirilmiş olan işletmeler (örneğin, elektronik para kurumları, ödeme kurumları ve Financial Services and Markets Authority kapsamında yetkilendirilmiş firmalar) dahil olmak üzere, kripto varlık saklama hizmeti sunmak isteyen işletmelerin de FCA'e kaydolması gerekmektedir.

Birleşik Krallık' ta saklama hizmeti sunmak isteyen şirketlerin FCA' ya kaydolmaları gerektiği gibi bazı kriterlere de sahip olması beklenmektedir. Bu kriterlerden aşağıda detayları ile bahsedilecektir.

Öncelikli olarak faaliyetin Birleşik Krallık'ta aktif bir iş olarak yürütülüp yürütülmediğine dair değerlendirme, FCA tarafından somut duruma göre yapılacaktır. Bu değerlendirmede dikkate alınacak hususlar şunlardır:

• Ticari Unsur: Kişi veya kuruluşun, kripto varlık hizmetleriyle ilgili olarak bir iş yaptığını öne süren şekilde reklam yapıp yapmadığı, faaliyet gösterip göstermediği veya kendisini böyle tanıtıp tanıtmadığı değerlendirilecektir.

• Ticari Fayda: Kişi veya kuruluşun bu hizmetten doğrudan veya dolaylı olarak fayda elde edip etmediği değerlendirilecektir.

37 *Reverse solicitation; MiCA'nın 61. Maddesi'nde bahsedilen bir uygulamadır. Genellikle "tersine talep istisnası" olarak anılsa da aslında bir yasaklamadır: Üçüncü ülke firmalarının, yalnızca müşterinin kendi isteği ve inisiyatifiyle, Avrupa Birliği içinde yerleşik veya bulunan müşterilere kripto varlık hizmeti sunmalarını yasaklayan bir düzenlemedir.*

38 *38 Swiss Digital Asset Custody Report https://static1.squarespace.com/static/6641b46de2c26a6478ff8f6e/t/668323ba60d1d203f76fff68/1719870411796/Swiss_+Digital_Asset_Custody_Report_2024.pdf, s. 35. Bu kapsamda, Lihtenştayn'da bir iştirak kurulması, ülkenin MiCA'yı uygulamada kaydettiği ilerleme ve mevcut lisansları MiCA lisanslarına dönüştürme konusundaki verimli süreçleri göz önüne alındığında avantajlı olabilecektir. Böylece, gerekli lisansın alınması muhtemelen daha hızlı olacaktır. Ayrıca, Lihtenştayn'ın İsviçre'ye yakınlığı sayesinde saklama hizmeti sunan şirketler, Zürih veya Zug'daki ofisler aracılığıyla Lihtenştayn otoritelerinin öngörmüş olduğu içerik gereksinimlerini yerine getirmesini sağlayabilir. Bu şekilde bir hamle, hem İsviçreli ana şirket hem de Lihtenştayn'daki iştirak için aynı içeriklerin kullanılmasına izin verebilir, operasyonları düzene sokabilir ve verimliliği en üst düzeye çıkarabilir.*

• Diğer İşlerle İlgisi: Kripto varlık hizmetlerinin, genel iş faaliyetlerinin yalnızca bir bölümünü oluşturması mümkündür. Bu hizmetlerin diğer hizmetlerle ilişkisi değerlendirilerek önemi tespit edilecektir.

• Düzenlilik/Sıklık: Kripto varlık hizmetinin yürütülme sıklığının bir iş olarak yürütüldüğünü gösterip göstermediği değerlendirilecektir.

Her bir başvuru, yürütülen işin niteliği ve iş modeli dikkate alınarak kendi şartlarına göre değerlendirilmelidir. İşin Birleşik Krallık'ta yürütülüp yürütülmediğine karar verilirken ise aşağıdaki çeşitli faktörler dikkate alınacaktır:

• Birleşik Krallık'ta Ofisin Bulunması: İşletmenin Birleşik Krallık'ta bir ofisi veya merkezi varsa, bu durum hizmetin Birleşik Krallık'ta yürütüldüğüne işaret edebilir (9. madde). Ofis, kayıtlı bir ofis veya merkez değilse, bu ofisin yürüttüğü hizmet türü ve bu ofisin varlığının Birleşik Krallık'ta iş yapıldığı anlamına gelip gelmediği değerlendirilecektir.

• Birleşik Krallık'ta Ofis Bulunmaması veya Faaliyet Gösterilmemesi: İşletmenin Birleşik Krallık'ta ofisi veya başka bir faaliyeti olmaksızın yalnızca Birleşik Krallık'ta bir müşterisi olması durumunda, bu işin Birleşik Krallık'ta yürütülmediği sonucuna varılabilir. Örneğin, bir KVHS, Birleşik Krallık dışında bir yargı yerinde kayıtlıysa ve Birleşik Krallık'ta ofisi veya temsilcisi yoksa, ancak yine de Birleşik Krallık müşterilerinin işlem hesapları açmasına, kripto varlık alıp satmasına veya saklamasına izin veriyorsa, bu otomatik olarak Birleşik Krallık'ta iş yapıldığı anlamına gelmez.

Kripto varlık saklama hizmeti sunmak isteyen şirketler, FCA'e kayıt başvurusu yaparken bazı bilgi ve belgeleri sunmakla yükümlüdür:

• İşletmenin sunacağı belirli kripto varlık hizmetlerinin neler olduğunun faaliyet programı çerçevesinde açıklanması gerekmektedir.

• İşletmenin hedefleri, müşterileri, çalışanları, yönetim yapısı, planları ve projeksiyonlarına düzenleyici iş planında yer verilmelidir. Finansal ve finansal olmayan kaynakların yeterliliği dikkate alınarak, teklifin düşünülmüş olduğuna dair yeterli detay sunulmalıdır. İşlem hacmi ve değeri, müşteri sayısı ve türleri, fiyatlandırma, ana gelir ve gider kalemleri ve gelecekte sunulması planlanan ek ürün veya hizmetler hakkında bilgi içermelidir.

• İşletmenin nasıl organize edildiğinin tanımlanması (şirket yapısı şeması, yakın bağlantılar ve grup varlıkları dahil) organizasyon yapısı şemasında ortaya koyulması beklenmektedir. Herhangi bir dış kaynak kullanım düzenlemesi varsa bunun tanımını içermelidir.

• İşletmenin operasyonlarının yürütülmesi için kullanılacak olan sistemlerin detayları, güvenlik politikaları ve prosedürlerinin detaylarının sunulması gerekmektedir.

• İşletmenin ve işletmenin organizasyonunda yer alan bireylerin güncel bilgileri sunulmalıdır.

• İşletmenin yönetiminden sorumlu olacak olan müdür ve diğer kişilerin, iyi bir itibara sahip olduklarını ve uygun bilgi ve deneyime sahip olduklarını ortaya koyma yükümlülükleri bulunmaktadır. Organizasyon şemasının bir parçası olarak, bu bölümde kilit kişilerin rollerinin ve sorumluluklarının detaylarının yer alması gerekmektedir.

• Kara para aklama prosedürlerine uyumdan sorumlu bir kişinin belirlenmiş olması gerekmektedir. AML/CTF çerçevesinin, yürürlükte olan kara para aklamanın önlenmesi mevzuatına uyumu sağlamak için tasarlanmış politikalar, prosedürler ve eğitim materyalleri dahil olmak üzere bir tanımı yapılmak zorundadır.

• Üst yönetimin sorumluluğu, denetimi, organizasyon yapısı, bütçe tahminleri ve ilk 3 mali yıl için finansal tablo ve iş sürekliliği düzenlemelerinin detaylarına yer verilmelidir.

• İşletmenin doğası gereği karşı karşıya olduğu risklerin değerlendirilmesi ve bu risklerin etkisi ve ortaya çıkma olasılığı hakkında bilgi ve belgeler sunulmalıdır. Risk değerlendirmesinin nasıl oluşturulduğuna dair metodoloji ortaya koyulmalıdır.

• Mali tanıtım politikasının detayları, tanıtımların Birleşik Krallık'taki ilgili mevzuata uygun olduğundan ve adil, açık ve yanıltıcı olmadığından emin olmak için kullanılan sistemler, kontroller ve süreçler dahil açıklanmalıdır.

• Kripto varlık transferleri yaparken alıcı ve gönderici bilgilerini almak ve iletmek için kara para aklamaya ilişkin düzenlemelerde yer alan şartların nasıl sağlanacağını tanımlayan politika ve prosedürlere ve desteklemek için kullanılacak teknoloji çözümleri hakkında detaylar içermelidir.

• İşletmenin üzerinde kontrol yetkisine sahip olduğu ve iş faaliyetinde kullandığı tüm kripto varlık adreslerinin bildirilmesi gerekmektedir.

Birleşik Krallık yakın gelecekte daha ayrıntılı düzenlemeler yapma planları açıklamış olmakla birlikte, hükümet değişikliği sonrasında durumun nasıl ilerleyeceği henüz netlik kazanmamıştır.

3. 4 Almanya

Alman Bankacılık Yasası (KWG-Kreditwesengesetz) Bölüm 1/11 cümle 4'te kripto varlıkların tanımına yer verilmiştir. Buna göre, kripto varlıklar, merkezi bir banka veya kamu kurumu tarafından çıkarılmamış veya garanti edilmemiş, yasal para birimi statüsüne sahip olmayan, ancak gerçek veya tüzel kişiler tarafından bir değişim aracı veya yatırım amacıyla kabul edilen dijital değer temsilleridir.

Kripto varlıklar, elektronik olarak transfer edilebilir, saklanabilir ve bunların ticareti yapılabilir. Kripto varlıklar KWG Bölüm 1(11) cümle 1 no. 10'a göre finansal araç niteliği taşımaktadır.

Almanya'da, Dördüncü AB Kara Para Aklama Direktifi'ni (AMLD4) değiştiren düzenlemeyi uygulayan kanun[39] kripto varlık saklama işini KWG'ye göre yeni bir finansal hizmet olarak eklemiştir. Bu yasa, 1 Ocak 2020'den itibaren yürürlüktedir ve bu tür hizmetleri sunmak isteyen şirketlerin BaFin'den ("Bundesanstalt für Finanzdienstleistung")[40] izin alarak faaliyete geçmeleri gerektirmektedir. Ancak, bu iş faaliyetlerini kanun çıktığı tarih itibariyle halihazırda zaten gerçekleştirmekte olan şirketler için geçici hükümler mevcuttur.

BaFin, kripto varlıkların hukuki çerçevesine ilişkin yasal durum hakkında web sitesinde düzenli olarak bilgi yayınlamaktadır ve bu site sürekli olarak güncellenmektedir. Ayrıca, BaFin özel olarak kripto saklama işiyle ilgili çeşitli rehber ve kılavuzlar da yayınlamıştır. Bu rehberler arasında kripto saklama işinin tanımına ilişkin kılavuz, KWG'nin 64/y maddesinin yorumlanmasına ilişkin rehber[41], yetkilendirme başvuruları için kılavuzlar ve kara para aklama gereksinimlerine ilişkin kılavuzlar bulunmaktadır.

39 *19 Aralık 2019 tarihli Federal Kanun Gazetesi I, s.2602, Gesetz zur Umsetzung der Änderungsrichtlinie zurVierten EU-Geldwäscherichtlinie – GwRLÄndG*

40 *BaFin, Almanya'nın finansal düzenleyici otoritesi olan Federal Finansal Denetleme Kurumu'nun (Bundesanstalt für Finanzdienstleistungsaufsicht) kısaltmasıdır. 1 Mayıs 2002'de kurulmuş olan BaFin, Alman finansal sektörünün güvenli ve düzgün çalışmasını sağlamakla görevlidir. BaFin, bankalar, sigorta şirketleri ve menkul kıymet piyasalarını denetler ve bu kurumların sağlamlık, bütünlük ve istikrarını garanti altına alır.*

41 *https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Auslegungsentscheidung/BA/ae_Hinweise_zur_Auslegung_64y_KWG_en.html;jsessionid=46D99BD1E20DC2DEC63AAA39C118ED20.internet001?nn=19578884*

i. Alman Hukuku'nda Kripto Saklama Hizmetlerinin Tanımlanması

Alman Bankacılık Yasası (KWG) 1 (1a) cümle 2 no.6'ya göre , kripto varlık saklama işi, kripto varlıkların veya kripto varlıkları saklamak, depolamak veya transfer etmek için kullanılan özel kriptografik anahtarların başkaları için saklanması, yönetimi ve korunması olarak tanımlanmaktadır.

Bu hüküm anlamında saklama, kripto varlıkların üçüncü taraflara sunulan bir hizmet olarak muhafaza edilmesi anlamına gelir. Dolayısıyla bu, özellikle müşterilerinin kullanılan kriptografik anahtarlara dair bilgisi olmadan, müşterilerinin kripto varlıklarını toplu olarak tutan hizmet sağlayıcıları kapsamaktadır.

Yönetim, kripto varlıklardan kaynaklanan hakların yerine getirilmesini ifade etmektedir.

Koruma, hem üçüncü kişilerin hizmet olarak sunulan özel kriptografik anahtarlarının dijital olarak saklanması hem de bu anahtarların saklandığı fiziksel veri ortamının (örneğin bir USB bellek veya bir kağıt parçası) saklanması anlamına gelir. Yalnızca depolama alanının sağlanması, örneğin web barındırma veya bulut depolama sağlayıcıları tarafından sağlanan hizmetler, bu sağlayıcılar özel kriptografik anahtarların depolanmasına yönelik hizmetlerini açıkça sunmadıkça tanımı karşılamayacaktır.[42]

ii. BaFin'e Başvuru

BaFin, Alman finans sistemine yönelik hem ulusal hem de uluslararası düzeydeki riskleri minimuma indirmeyi, Almanya'daki finansal süreçlerin düzgün bir şekilde işlemeye devam etmesini ve bütünlüğünün korunmasını sağlamayı amaçlamaktadır. Almanya'da ticari olarak organize edilmiş iş operasyonları gerektiren bir ölçekte kripto varlık saklama işi yapmak isteyen herkes, KWG 32/1 cümle 1'deki düzenlemeye uygun olarak BaFin'den önceden yazılı izin almalıdır. KWG'nin 1/1a maddesi kapsamındaki finansal hizmetlerin çoğunluğu bakımından, belirli bir finansal hizmeti sağlama yetkisine sahip olan şirketler, kripto varlıklarla ilgili olarak da bu hizmeti sağlayabilir. Ancak bu, kripto varlık saklama işi için geçerli değildir. Zira finansal hizmetleri sağlama yetkisine zaten sahip olanların da kripto varlık saklama işi yapmak için ek bir yetkiye ihtiyacı vardır.[43]

Kripto varlık saklama yetkisi için yapılacak başvuru için en az 150.000 Euro başlangıç sermayesi, güvenilir kurucular ve nitelikli yöneticiler gibi çeşitli gereksinimlerin belgelendirilmesi gerekmektedir. Başvuruya bir iş planı da eklenmelidir. Bu plan, ilk üç mali yılın bilanço ve kar-zarar hesaplarını, şirketin organizasyon yapısını ve iç kontrol mekanizmalarını içermelidir. Ayrıca plan, ilgili muhasebe ve finans standartlarına uygun olmalıdır. İşletmeler, uygun bir iş organizasyonuna sahip olmalıdır ve IT stratejileri ve güvenliği hakkında bilgi vermelidir.

42 *https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Merkblatt/mb_200302_kryptoverwahrgeschaeft_en.html;jsessionid=46D99BD1E20DC2DEC63AAA39C118ED20.internet001?nn=19578884*

43 *https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Merkblatt/mb_200302_kryptoverwahrgeschaeft_en.html?nn=19578884*

Yeterli IT güvenliği, KWG'nin 25a maddesi anlamında düzgün bir iş organizasyonunun ayrılmaz bir parçasıdır. MaRisk [44] ve BAIT [45] gereksinimleri, risk yönetim sistemi kapsamında uygulanmalıdır. BaFin, IT sistemlerinin ve süreçlerinin detaylı bilgilerini beklemektedir. Kripto varlık saklama yetkisi başvuruları için, kriptografik anahtarların güvenliği ön planda tutulmalıdır.

Başvuru kapsamında sunulması gereken belgeler arasında güvenlik stratejisi, güvenlik olaylarının yönetimi ve risk değerlendirmesi bulunmaktadır. Şirketin iş modeline göre, kripto varlıkların teknik olarak nasıl saklandığı (örneğin "hot wallet", "cold wallet") ve varlıkların ayrı veya toplu cüzdanlarda tutulup tutulmadığı açıklanmalıdır.
Başvuru ile sunulması gereken bilgilerin ana noktaları şu şekilde sıralanabilir:
Planlanan faaliyetle ilgili iş stratejisi; uzun vadeli IT stratejisi; IT sistem mimarisinin kapsamlı tanımı; güvenlik stratejisi ve şifreleme yöntemleri; nemli dış kaynak kullanımı ve bulut çözümleri hakkında bilgiler; risk değerlendirmesi ve alınan önlemler; kripto konseptinin detaylı tanımı; hassas verilere ve kriptografik anahtarlara erişim rolleri ve güvenlik konsepti; izleme prosedürlerinin tanımı şeklindedir. Bu bilgiler, orantılılık ilkesi ve şirketin özel durumu göz önünde bulundurularak sunulmalıdır.
Kurucular, KWG'nin 25c (1) maddesi uyarınca nitelikli ve güvenilir olmalı ayrıca görevlerini yerine getirmek için yeterli zamana sahip olmalıdır. Bu, kripto varlık saklama işini yürütenler için de geçerlidir. Yeterli niteliklere sahip olmayan kurucular, yetkilendirme başvurusunun reddedilmesine neden olabilir.

Bir kurucu, ilgili iş alanlarında yeterli teorik ve pratik bilgiye ve yönetim deneyimine sahip olmalıdır.

Kripto varlık saklama işinde BaFin, işletmenin büyüklüğü ve yapısını, ayrıca kripto saklama işinin yeni bir finansal hizmet olduğunu dikkate alacaktır. Bu nedenle, kurucunun teknik uzmanlığına özel önem verilecektir. Özellikle IT güvenliği konularında eğitim almış ve pratik deneyime sahip olması aranacaktır.

Başvurularda, kurucuların niteliklerini ve güvenilirliğini kanıtlamak için el yazısı ile imzalanmış özgeçmiş, yetkili makama sunulacak iyi hal belgesi ve Ticaret ve Sanayi Sicilinden alınacak belge gereklidir. BaFin, başvuru için gerekli belgeleri belirten bir kontrol listesi yayınlamıştır.

BaFin, kripto saklama işindeki faaliyetleri, ilgili hiyerarşik seviyede pratik deneyim olarak kabul edecektir. Ayrıca, kurucuların geçiş süresi boyunca eksik uzmanlık alanlarını geliştirmeleri beklenmektedir. Özel durumlarda BaFin, bir kurucunun eksik uzmanlığını geçici olarak telafi edebilecek insan kaynakları ve organizasyon yapısını da değerlendirecektir. Bu değerlendirmeler, her işletmenin büyüklüğü ve yapısına göre bireysel olarak yapılacaktır.

Bir kurum yalnızca KWG'nin 1/11 no'lu maddesi[46] anlamında kripto varlıkları saklıyorsa, genellikle yalnızca bir kurucu atanması yeterlidir. Ancak, ilgili kripto varlıklar başka bir finansal enstrüman kategorisine de giriyorsa veya şirket başka türde işler yapıyorsa, durum farklı olabilir.

44 *MaRisk; Almanya' da geçerli olan risk yönetimi için asgari gerekliliklere atıfta bulunan bir kısaltmadır; Alman Federal Mali Denetleme Kurumu tarafından, Almanya'da finansal olarak ticaret yapan bankaların, sigortaların ve diğer şirketlerin risk yönetimine ilişkin kavramlar sağlayan bir genelgedir.*
45 *MaRisk'teki Asgari Risk Yönetimi Gereksinimlerine benzer şekilde, BAIT de Alman Bankacılık Kanunu'nun 25a. Maddesi'nin yasal gerekliliklerini belirler. BAIT; denetim otoritesinin gereklilikler kataloğu, finansal kurumların BT sistemleri için uygun teknik ve organizasyonel kaynakları nasıl oluşturması gerektiğini açıklar.*
46 *KWG 1(11) "Ödemeler için ön ödemeli kartların düzenlenmesi, kartın düzenleyicisinin aynı zamanda hizmet sağlayıcı ve dolayısıyla kartla yapılan ödemenin alıcısı olmadığı sürece (ön ödemeli kart işlemleri)."*

BaFin, belirli durumlarda birden fazla kurucu atanmasının gerekli olabileceğini belirtebilir. Kurumun büyüklüğü ve iş faaliyetlerinin kapsamı nedeniyle, düzgün bir iş organizasyonu tek bir kurucuyla sağlanamıyorsa, ikili kontrol ilkesinin uygulanması gerekir. Bu, başvuru sürecinde sunulan belgelere dayanarak BaFin tarafından her durumda ayrı ayrı incelenecektir. Bu nedenle, yetki sürecinde yönetim kurulunun sorumluluklarını gösteren bir organizasyon şeması da eklenmelidir. Ayrıca, kurumun yeterli insan kaynakları ve teknik ve organizasyonel yapıya sahip olduğunu gösteren belgeler sunulmalıdır. Kurucular; görevlerine yeterli zaman ayırmak zorundadır.

iii. Kara Para Aklamanın Önlenmesi

GwG (Geldwäschegesetz), Almanya'da faaliyet gösteren ekonomik aktörlerin kara para aklama ve terörizmin finansmanını önleme çabalarına katılmasını zorunlu kılar. Kripto varlık saklama işi yürüten kurumlar, GwG'nin 2. maddesi kapsamında yükümlü kurumlar arasında yer almaktadır.

Kara para aklama önlemenin üç temel direği, Almanya'daki Kara Para Aklama Yasası (GwG) çerçevesinde belirlenmiştir. İlk olarak, GwG'nin 4. maddesi, yükümlü kurumların etkin bir risk yönetim sistemine sahip olmalarını zorunlu kılar; bu sistem, kara para aklama ve terörizmin finansmanı risklerini analiz etmeli ve uygun iç kontrolleri oluşturmalıdır. İkinci olarak, GwG'nin 10. maddesi, müşteri tanıma yükümlülüklerini belirler; buna göre kurumlar, müşterilerin kimliğini doğrulamak, yararlanıcı sahiplerini tespit etmek ve iş ilişkisinin amacını değerlendirmek zorundadır. Son olarak, GwG'nin 43. maddesi, şüpheli işlemlerin bildirilmesini zorunlu kılar ve bu bildirimlerin Mali İstihbarat Birimi'ne (FIU) yapılması gerektiğini belirtir; aynı zamanda yükümlü kurumlar FIU'ya kayıt yaptırmalıdır. Bu üç temel direk, saklama faaliyetleri kapsamında kara para aklama ve terörizmin finansmanına karşı etkili bir mücadele sağlamak için kritik öneme sahiptir.

3. 5 Birleşik Arap Emirlikleri (BAE)

BAE, kripto varlık saklama hizmetleri sektörünü büyütmeyi hedeflemekle birlikte, bu alandaki riskleri de en aza indirgemeyi amaçlayan kapsamlı bir lisanslama süreciyle sektöre denetim getirmektedir. Bu sayede, uluslararası yatırımcılar ve işletmeler için güvenli bir faaliyet ortamı sunulmak istenmektedir. Kripto varlık saklama hizmetleri, kullanıcıların dijital varlıklarını güvenli bir şekilde muhafaza eden ve bunları yöneten hizmet sağlayıcılarını kapsamaktadır. Bu hizmetlerin sunulabilmesi için işletmelerin belirli finansal ve güvenlik standartlarını yerine getirmesi gerekmektedir. Aynı zamanda kara para aklama ve terör finansmanıyla mücadele regülasyonlarına uyması zorunludur.

Birleşik Arap Emirlikleri Anayasası'nın 121. maddesi serbest bölgelerin kurulmasına izin vermektedir. 2004 tarihli 8 numaralı Federal Kanun, özellikle finansal serbest bölge olarak adlandırılan ve serbest bölgelerin bir alt kümesi olan bölgelerin kurulmasına imkan tanımaktadır. İlgili düzenlemeye göre, finansal serbest bölgenin temel unsurları şu şekildedir: Federal düzeydeki medeni kanun ve ticaret kanunlarından muaf olmakla birlikte, AML de dahil olmak üzere ceza kanunlarıyla bağlıdırlar. Birleşik Arap Emirlikleri'nde iki serbest ekonomik bölge bulunmaktadır: Abu Dhabi Global Market (ADGM) ve Dubai Internal Financial Centre (DIFC). Raporumuzun bu bölümünde, BAE kapsamında kripto varlık saklama hizmetlerine ilişkin olarak ADGM, DIFC ve diğer düzenlemelere ana hatlarıyla yer verilecektir.

3. 5.1. VARA (Virtual Asset Regulatory Authority-Sanal Varlıkları Düzenleme Otoritesi) Kapsamında

9 Mart 2022'de Dubai'de 4 2022/4 numaralı kanun ile Dubai Virtual Asset Regulatory Authority (VARA) kurulmuştur. 7 Şubat 2023 tarihinde VARA Düzenlemesi'ni yayınlanmıştır.

VARA Düzenlemeleri kapsamında, bir KVHS için lisanslama rejimi, KVHS'nin sunduğu hizmet türüne bağlıdır. VARA, bir KVHS'nin sunabileceği hizmet yelpazesinin kapsamını belirlemek için birbirine geçen yedi ayrı sanal varlık faaliyeti kategorisini tanımlamaktadır. Bir KVHS, birden fazla faaliyet için başvuruda bulunabilmekte ve bunları tek bir genel lisans altında toplayabilmektedir. Genel olarak, yedi faaliyet kategorisi içinde şunlar yer almaktadır: danışmanlık hizmetleri; aracı kurum hizmetleri; saklama hizmetleri; değişim hizmetleri; sanal varlıkların ödünç verilmesi ve alınması hizmetleri; sanal varlıkların ödenmesi ve gönderilmesi hizmetleri; ve sanal varlık yönetimi ve yatırım hizmetleri.

Kripto varlık saklama hizmetine ilişkin olarak ana düzenlemenin yanında, kuruluşlar tarafından uyulması gereken bir Kural Kitabı (Custody Services Rulebook) da bulunmaktadır.[47] Burada yer alan kurallar, Sanal Varlıklar ve İlgili Faaliyetler Yönetmeliği 2023, uyarınca yayınlanmış olup bu yönetmeliğin bir parçasını oluşturmaktadır. Ayrıca Emirlik'te Saklama Hizmetleri yürütmek üzere VARA tarafından lisans verilmiş tüm hizmet sağlayıcılar için geçerlidir.

Bu faaliyetlerden bir veya birkaçını gerçekleştirmek olan bir KVHS'nin VARA'ya başvurarak lisans alması gerekmektedir. Başvuru ücretleri, uzatma ücretleri ve yıllık denetim ücretleri çeşitli oranlarda uygulanır.

Bir danışmanlık hizmetleri lisansı 40.000 AED bir başvuru ücreti ve 80.000 AED yıllık bir denetim ücreti ile birlikte gelirken, eşdeğer borsa hizmetleri lisans ücretleri sırasıyla 100.000 AED ve 200.000 AED'dir.

Ağustos 2023'te VARA, Staking faaliyetleri ile ilgili olarak revize Saklama Hizmetleri Kural Kitabını yayınlamıştır. Buna göre, saklama hizmetleri sağlama lisansı olan KVHS'lerin VARA'dan ek onay alarak, Sanal Varlık Yönetimi ve Yatırım Hizmetleri faaliyet kategorisi için ayrı bir lisans almadan müşterilerine aynı tüzel kişilikten staking hizmetleri sağlamaları mümkün hale gelmiştir.

3. 5.2. Dubai Finansal Hizmetler Otoritesi (Dubai Financial Services Authority)

Dubai, kripto varlık saklama hizmetleri için hızla gelişen bir merkez haline gelmiştir ve bu alanda faaliyet gösteren önemli oyuncuların dikkatini çekmektedir. DIFC'de bulunan Dubai Finansal Hizmetler Otoritesi (Dubai Financial Services Authority-DFSA), kripto varlıkların düzenlenmesi için "Kripto Token Rejimi"ni oluşturmuştur. Bu rejim, kripto tokenlerle ilgili ürün ve hizmetlerin sunulmasına yönelik mevcut birçok finansal hizmet faaliyetinin kapsamını genişletmektedir.

8 Mart 2024'te DIFC, Dijital Varlıklar Kanunu'nu yürürlüğe girmiştir. Hemen ardından, DIFC Değişiklikleri Kanunu'nu yayınlamış ve bu yeni kanunla Borçlar Hukuku, Trust Hukuku ve Şirketler Hukuku'nda dijital varlıkların niteliğine uyum sağlayacak şekilde değişiklikler yapılmıştır.

Dijital Varlıklar Kanunu, aşağıdaki durumlarda, dijital varlık olarak tanır ve tanımlar:

(a) bir katılımcı ağı tarafından yazılımın aktif işletimi ve ağ tarafından örneklenen verilerin birleşimiyle

47 *https://rulebooks.vara.ae/rulebook/custody-services-rulebook*

ortaya çıkan kavramsal bir nicelik birimi olarak var olan; (b) herhangi bir belirli kişiden ve yasal sistemden bağımsız olarak var olan; ve (c) çoğaltılamayan ve bir kişi veya belirli bir kişi grubu tarafından kullanılması veya tüketilmesi, bir veya daha fazla başka kişi tarafından o şeyin kullanılmasını veya tüketilmesini zorunlu olarak engelleyen şeyler.[48]

Dijital Varlıklar Kanunu, bir dijital varlığın kontrolü, üzerinde mülkiyet hakkının kurulması, mülkiyetin devri ve zilyetliği geri alınması için bir çerçeve belirlemektedir.

3. 5.3. Abu Dhabi Kanunları

Abu Dhabi, 2018 yılında uygulanmaya başlayan Kripto Varlık Çerçevesi'ni güncelleyerek yeniden adlandırmış ve Sanal Varlıklar (VA) Çerçevesi haline getirmiştir. Abu Dhabi Global Market (ADGM) içindeki ayrı bir finansal düzenleyici olan Finansal Hizmetler Düzenleme Otoritesi (FSRA), Kripto Varlık Faaliyetlerinin Düzenlenmesine İlişkin Rehberi yayınlamıştır[49]. Bu Rehberin, FSRA tarafından daha önce hazırlanmış olan ICO/ITO'lara ve Sanal Para Birimlerine ilişkin düzenlemelerle ilgili olarak hazırladığı Rehberle birlikte dikkate alınması gerekmektedir[50]. ADGM Düzenlemeleri, sanal varlıkların kullanımını düzenleyen FSRA kuralları ve Rehber birlikte, "Sanal Varlık Çerçevesi" olarak anılmaktadır.

FSRA sanal varlıkları, dijital olarak alınıp satılabilen ve bir değişim aracı ve/veya bir hesap birimi ve/veya bir değer deposu işlevi gören, ancak hiçbir yargı bölgesinde yasal ödeme statüsüne sahip olmayan bir değerin dijital temsili olarak tanımlamıştır.
Sanal varlıklar, hiçbir yargı bölgesi tarafından ihraç edilmez veya garanti edilmez ve yukarıdaki işlevleri yalnızca sanal varlık kullanıcıları topluluğu içinde anlaşmayla yerine getirir ve Fiat Para Birimi ve E-paradan farklıdır."

Kripto saklama hizmeti lisansı almak için başvuru süreci, FSRA ile görüşmeleri, titiz bir başvuru sunumunu, prensipte onayı, nihai onayı ve operasyonel lansman testini içerir. Başvuru sahipleri, sanal varlıkların ve müşteri fonlarının saklanması için sağlam bir yönetim, sistem ve kontrol mekanizması göstermelidir. Geleneksel düzlemde aracı, satıcı veya saklayıcı olarak faaliyet göstermek isteyen bir kişinin, sanal varlıklarla ilgili düzenlenmiş faaliyet yürütmek için onay almanın yanı sıra, söz konusu geleneksel belirtilen yatırımlar veya finansal araçlar için geçerli FSRA onaylarına başvurması ve bunları elde etmesi gerekecektir.[51]

FSRA, sanal varlıklar üzerinde genel olarak hosted, unhosted ve outsourced olmak üzere üç tür saklama yöntemi olduğundan hareket etmektedir. FSRA, mevcut veya gelecekte ortaya çıkabilecek başka alternatif sanal varlık saklama modelleri olabileceğini dikkate almaktadır. Bu tür alternatif modeller sunmayı amaçlayan ve bunların çekebileceği düzenleyici yükümlülüklerden emin olmayan kuruluşların mümkün olan en kısa sürede FSRA ile iletişime geçmeleri önerilmektedir.

48 *Digital Asset as a thing that:*
"(a) exists as a notional quantity unit manifested by the combination of the active operation of software by a network of participants and network-instantiated data; (b) exists independently of any particular person and legal system; and (c)is not capable of duplication and use or consumption of the thing by one person or specific group of persons necessarily prejudices the use or consumption of that thing by one or more other persons."
49 *https://www.adgm.com/documents/legal-framework/guidance-and-policy/fsra/guidance-virtual-asset-activities-in-adgm-20231218.pdf*
50 *https://www.adgm.com/documents/legal-framework/guidance-and-policy/fsra/guidance-icos-and-crypto-assets_20180625_v11.pdf*
51 *https://en.adgm.thomsonreuters.com/sites/default/files/net_file_store/Guidance-Regulation_ofVirtual_Asset_Activities_in_ADGM_(VER05.181223).pdf*

3. 6 ABD'de Kripto Varlıkların Saklanması Süreci ve SEC Düzenlemeleri

Amerika Birleşik Devletleri'nde bir kripto varlık saklama hizmeti sunan kuruluş ile müşteri arasındaki hukuki ilişki, federal düzeyde farklı düzenlemeler ve lisans gereklilikleri de mevcut olmakla beraber, öncelikle eyalet yasalarına tabidir. Bu ilişki, somut olaya göre bankalar, yatırım danışmanları, trust şirketleri ve broker-dealer'lar gibi devlet tarafından düzenlenen ve denetlenen kripto varlık saklama hizmeti sunanlar için geçerli olan yasal ve düzenleyici gerekliliklerinden de etkilenebilmektedir. Federal hukuk, yüksek miktarda nakit veya menkul kıymet işlemi gerçekleştiren yatırım danışmanları ve aracı kurumların, işlem konusu varlıkların belirli nitelikleri sağlayan kuruluşlarda tutulmalarını şart koşmaktadır.[52]

Yatırım Danışmanları Yasası kural 206(4)-2 [17 CFR 275.206(4)-2]'de düzenlenen Saklama Kuralı, müşteri fonları veya menkul kıymetleri üzerinde saklama yetkisine sahip olan ve Menkul Kıymetler ve Borsa Komisyonu (SEC)'e kayıtlı ya da kayıt yaptırmakla yükümlü yatırım danışmanlarının bu varlıkların; kaybı, hırsızlığı, kötüye kullanımı, zimmete geçirilme risklerinden ve yatırım danışmanının mali sıkıntıları, iflas dahil olmak üzere, olumsuz etkilerinden korunmasını temin etmek amacıyla belirli yükümlülüklere uymasını zorunlu kılmaktadır. Bu yükümlülükler arasında, ilgili varlıkların "nitelikli saklama kuruluşu" tarafından saklanması yer almaktadır.

Bu kural, müşterilerinin fonlarını veya menkul kıymetlerini doğrudan ya da dolaylı olarak saklayan tüm yatırım danışmanlarını kapsamaktadır. Saklama Kuralı, nitelikli saklama kuruluşunu, belirli bankalar, aracı kurumlar, vadeli işlem komisyoncuları ve yabancı finansal kuruluşlar olarak tanımlamaktadır.[53] Trust şirketleri ve kayıtlı broker-dealer'lar bu tanıma girebilmekle birlikte her birinin müşterilerinin kripto varlıklarını güvenli ve ayrı şekilde saklayabilme yetkinliğine sahip olması gerekmektedir. Bu bağlamda, söz konusu kurumların belirli güvenilirlik ve güvenlik standartlarını karşılaması zorunludur. Ancak belirtilmelidir ki, son dönemde saklamaya ilişkin kuralların, kripto varlık sektörünün esneklik ve yenilikçilik gereksinimlerine uyum sağlayıp sağlamadığı girişimciler arasında tartışılmaktadır.[54]

Kurumsal piyasalarda, saklama ilişkisi genellikle hak sahibi ile ilgili eyalette yürürlüğe girdiği şekliyle Uniform Commercial Code (UCC) madde 8 tarafından düzenlenen ilgili menkul kıymet aracısı arasında kurulmaktadır.[55] Saklanan varlığın bir "finansal varlık" niteliği taşıması durumunda, bu saklama ilişkisi UCC madde 8 çerçevesinde değerlendirilebilmektedir. Uluslararası Finansal Raporlama Standartları Yorum Komitesi'nin Haziran 2019 tarihli Gündem Kararı uyarınca kripto varlıkların nakit veya bir kuruluşun sermaye aracı olmaması sebebiyle bu varlıklar "finansal varlık" olarak sınıflandırılmamalıdır.[56] Bazı durumlarda, kripto varlıklar, sahibine temsil ettiği varlıkla ilgili belirli haklar tanıyabilmektedir.

52 *Clifford Chance, "Custody of Cryptoassets: Moving Towards Industry Best Practice" Haziran 2023, 34: https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2023/06/custody-of-cryptoassets.pdf*

53 *https://www.ecfr.gov/current/title-17/chapter-II/part-275*

54 *Sidley Austin LLP, "Crypto-Focused Private Fund Adviser Settles with U.S. SEC for Custody Rule and Other Violations," Eylül 2024, https://www.sidley.com/en/insights/newsupdates/2024/09/crypto-focused-private-fund-adviser-settles-with-us-sec-for-custody-rule-and-other-violations..*

55 *Uniform Commercial Code, Article 8, "Investment Securities," American Law Institute and Uniform Law Commission.*

56 *International Monetary Fund, "Recording Crypto Assets in Macroeconomic Statistics," Haziran 2022, : https://www.imf.org/external/pubs/ft/gfs/gfsac/pdf/Recording_Crypto_Assets_MacroStats_July_22.pdf.*

Bu tür varlıklara örnek olarak altın veya petrol gibi emtialar, fikri mülkiyet hakları veya gayrimenkuller verilebilir.[57] Bazı varlık teminatlı tokenlar, doğrudan varlığa yönelik bir hak sağlarken diğerleri temsil ettiği varlığı geri alma imkanı sunmamaktadır. Kripto varlık, temsil ettiği varlığın değerine eşdeğer nakit alma hakkı sağladığı takdirde bir finansal varlık olarak nitelendirilebilecektir. Mevcut durumda IRS'ye (Internal Revenue Service/İç Gelir Servisi) göre ise kripto varlıklar "dijital varlık" olarak nitelendirilmekte ve dolayısıyla eşya olarak vergilendirilmektedir. Ancak belirtilmelidir ki, UCC madde 8'in kapsamına menkul kıymetler ve ayrıca menkul kıymet aracısı ile müşterinin, eşyaya bir finansal varlık olarak muamele edileceği konusunda anlaşmasıyla, menkul kıymet aracısının müşteri için bir "menkul kıymet hesabında" tuttuğu herhangi bir eşya da girmektedir. Bu nedenle kripto varlıkların UCC madde 8 kapsamında finansal varlıklara benzer şekilde işlem görmesi için düzenlenecek saklama sözleşmesinde mutlaka ilgili maddeye açıkça atıfta bulunulmalıdır.[58] Eğer saklama ilişkisi UCC Madde 8'e tabi olursa, menkul kıymet aracısı olarak kripto varlık saklama hizmeti sunan kuruluş, müşterinin menkul kıymetlerini karşılamak için yeterli miktarda varlık bulundurma ve müşterinin talimatlarına uyma yükümlülüklerine sahiptir. Ayrıca, müşterinin rızası olmaksızın varlıklarda teminat faizi vermemesi gibi birtakım yasaklara tabidir. Genel olarak, taraflar aksini kararlaştırmadıkça, kripto varlık saklama hizmeti sağlayıcısı gerekli özeni göstermekle yükümlüdür.

Belirtilmelidir ki, UCC madde 8, bir menkul kıymet aracısının sakladığı varlıklar üzerinde mülkiyet hakkına sahip olmadığını düzenlerken her hak sahibinin mülkiyet hakkının, menkul kıymet aracısının hak sahibi adına tuttuğu belirli türdeki finansal varlıklardaki tüm menfaatlerle orantılı bir mülkiyet hakkı olduğunu vurgulamaktadır.

Saklama ilişkisi, eyalet hukukuna göre kefalet veya trust ilişkisi olarak da kurulabilmektedir. Eyalet hukukuna göre bir kefalet veya güven ilişkisi kurulması için yazılı bir sözleşme şartı bulunmamakla birlikte; mahkeme, somut olayın koşullarına göre böyle bir ilişkinin kurulduğuna karar verebilir. Uygulamada, özellikle kurumsal bağlamda, kripto varlıkların saklanmasına yönelik tipik saklama sözleşmeleri yaygın olarak kullanılmaktadır. Sözleşme içerisinde kripto varlık saklama hizmeti sunan kuruluş ile müşteri arasında böyle bir ilişkinin var olduğuna dair hükümlerin bulunmaması halinde kefalet veya trust ilişkisi kurulamaz. Eğer saklama hizmeti sağlayıcısı müşterinin kefili veya yediemini olarak kabul edilirse, eşyanın saklanmasında dikkat, özen ve sadakat yükümlülüğü bulunmaktadır. kripto varlık saklama hizmet sağlayıcısı ile müşteri arasındaki hukuki ilişki başka biçimlerde de kurulabilir.[59] Örneğin, kripto varlık saklama hizmeti sunan kuruluşa herhangi bir özel yükümlülüğün getirilmediği bir borç ilişkisi, borçlu ve alacaklı arasında kurulan tipik bir borç ilişkisi veya müşterinin gerçek saklanan varlıklara yönelik olmaksızın yalnızca kripto varlık saklama hizmeti sunan kuruluşun iflasına ilişkin teminatsız bir parasal talebi olduğu bir sözleşme ilişkisi mevcut olabilir.

57 *PwC, "About the Crypto Assets Guide," https://viewpoint.pwc.com/dt/us/en/pwc/accounting_guides/crypto-assets-guide/crypto_assets_guide/aboutthecryptoassets.html.*

58 *Clifford Chance, "Custody of Cryptoassets: Moving Towards Industry Best Practice", 35.*

59 *Clifford Chance, "Custody of Cryptoassets: Moving Towards Industry Best Practice", 35.*

SEC, 15 Şubat 2023'te, Saklama Kuralı'nda değişiklik yapmayı ve müşterileri adına varlık saklayan kayıtlı yatırım danışmanlarına yeni ve kapsamlı yükümlülükler getirmeyi teklif etmiştir.[60] Teklif, saklama tedbirlerine tabi olan varlık türlerini fon ve menkul kıymetlerin ötesine genişleterek müşteri varlıklarının kaybolma riskini azaltmayı ve varlıkların uygun şekilde ayrı tutulmayı hedeflemektedir. Dolayısıyla dijital varlıklar da kapsam altına alınmıştır. Teklif, müşteri varlıklarını saklayan yatırım danışmanlarının bu varlıkları kendi mülkiyetlerinden ayrı tutmasını gerektirmektedir. Yatırım danışmanlarına, müşteri varlıklarının saklama konusundaki uygulamaları hakkında bilgilendirme yükümlülüğünün de arasında yer aldığı belirli raporlama ve uyum gereklilikleri getirilmiştir. Teklif uyarınca, yatırım danışmanlarının nitelikli bir saklama kuruluşu ile yazılı bir sözleşme yapmaları gerekmektedir. Bu sözleşmeler, müşterilerin korunması amacıyla nitelikli saklama kuruluşlarının kamu denetçileri tarafından yürütülen yıllık denetimlere tabi olması ve talep üzerine ilgili kayıtların kamuya sunulması gibi makul güvenceler içermelidir. Bu durum, yatırım danışmanlarının mevcut piyasa uygulamasında değişiklik meydana getirmektedir. Nitekim, danışmanlar her zaman saklama kuruluşu ile müşteri arasındaki saklama sözleşmelerine taraf olmamaktadır. Böylelikle, SEC'in uygulaması SEC'in doğrudan düzenleme yetkisinin bulunmadığı banka ve diğer saklama kurumlarının faaliyetlerine de sirayet edecektir.

Saklama hizmeti sunan nitelikli bir banka veya yabancı finans kuruluşunun ise müşteri varlıklarını iflas durumunda bankanın alacaklılarından koruyacak bir hesapta tutması gerektiği düzenlenmiştir.

Ayrıca yetkili kripto varlık saklama hizmeti sunan kuruluşlar, müşteri varlıklarının nerede ve nasıl saklandığı konusunda şeffaf olmalı ve müşterilere bu konuda yeterli bilgi vermelidir. Teklif uyarınca müşteri varlıklarının müşterinin adına kaydedilmesi veya başka bir şekilde müşterinin yararına tutulması, danışmanın varlıkları ya da danışmanla ilişkili kişilerin varlıkları ile karıştırılmaması gerekmektedir. Ayrıca müşteri tarafından yazılı olarak kabul edilmediği ya da yetki verilmediği durumlar haricinde, danışman, ilgili kişilerin ya da alacaklıların lehine herhangi bir hak, ücret, teminat faizi, haciz veya talepte bulunamayacaktır. Teklif ek olarak, kripto varlık saklama hizmeti sunanın ihmalen veya kasıtlı olarak sebep olduğu müşteri varlıklarının kaybıyla ilgili tazminat yükümlülüklerine ilişkin düzenleme de getirmektedir. Böylelikle müşteri varlıklarının kötüye kullanımını veya kötü yönetimini önlemek hedeflenmektedir. Ancak bu teklif henüz kabul edilmemiş olup, önümüzdeki dönemde kabul edilmesi beklenmektedir.

Ek olarak, SEC tarafından 2022'de yayınlanan Staff Accounting Bulletin No. 121 (SAB 121)[61], kripto varlıklarla ilgili saklama hizmeti sunan kuruluşların bu varlıkları bilanço tablolarında tutmalarını zorunlu kılmaktadır. Bu düzenleme, bankalar için önemli maliyetler ve riskler getirirken aynı zamanda yatırımcılara daha fazla şeffaflık sağlamak ve kripto şirketlerinin iflası durumunda müşteri varlıklarının korunmasını garanti altına alma amacı taşımaktadır. Öte yandan ilgili düzenleme, bankaların kripto varlık saklama hizmetleri sunma kabiliyetini sınırlamakta ve bu hizmetlerin bankacılık dışı kuruluşlara kaymasına neden olmaktadır. ABD Temsilciler Meclisi, bu sınırlamaları kaldırmak amacıyla 8 Mayıs 2024'te H.J. Res. 109'u kabul etmiş[62], ancak Başkan Biden bu tasarıyı veto etmiştir ve bu veto kararı aşılamamıştır.

60 *Proskauer Rose LLP, "Regulation in the Post-FTX Environment: SEC's Proposed Enhanced Custody Rule and Its Effects on Crypto", Şubat 2023: https://www.proskauer.com/blog/regulation-in-the-post-ftx-environment-secs-proposed-enhanced-custody-rule-and-its-effects-on-crypto.*

61 *SEC. Staff Accounting Bulletin No. 121, 31 Mart 2022. https://www.sec.gov/regulation/staff-interpretations/accounting-bulletins/old/staff-accounting-bulletin-121*

62 *https://blockchain.bakermckenzie.com/2024/05/13/u-s-house-passes-bill-to-undo-sec-guidance-that-limited-banks-ability-to-custodian-crypto-assets/*

SAB 121 bu nedenle yürürlükte kalmaya devam etmektedir[63] . Bununla birlikte, SEC, bazı büyük bankalara, müşteri varlıklarının korunmasını sağlayarak bu düzenlemeye uymaları konusunda istisnalar sağlamıştır. ABD'de kripto varlık saklama hizmeti sunanlar, SEC'in yanı sıra Commodity Features Trading Commission ve Financial Crimes Enforcement Network gibi diğer federal düzenleyici kurumların belirlediği kurallara da uymak zorundadır. Bu kurumlar, kripto varlık saklama hizmeti sunanların dijital varlıkları korumak için sağlam güvenlik protokollerine sahip olmasını öngörmektedir. Bununla birlikte kripto varlık saklama hizmeti sunanların Müşterini Tanı (KYC) ve Kara Para Aklanmasının Önlenmesi (AML) kuralları dahil olmak üzere ilgili yasalar ve düzenlemelere de uyması gerekmektedir. ABD'de özellikle dijital varlıkları korumak için bazı yerel saklama girişimleri kurulmuştur. Bu girişimler, henüz SEC tarafından onaylanmamış olmakla birlikte teknik anlamda nitelikli saklama statüsünde bulunmaktadır. Girişimler, 1940 tarihli Yatırım Danışmanları Yasası ve Yatırım Şirketi Yasası uyarınca düzenlenen "banka" tanımından yararlanarak eyalet bazlı sınırlı amaçlı trust şirketleri olarak tescil edilmiş ve her iki yasa kapsamındaki saklama kuruluşu tanımını karşılamışlardır.

SEC, 3 Eylül 2024 tarihinde, dijital varlıklara yönelik Saklama Kuralı ihlallerine ilişkin ilk yaptırımı uygulamıştır. Kurum, bünyesinde kayıtlı bir yatırım danışmanının, Yatırım Danışmanları Yasası'nın 206(4)-2 numaralı kuralı uyarınca, özel fon müşterisi tarafından tutulan ve "menkul kıymet olarak sunulan ve satılan kripto varlıkların" nitelikli bir saklama kuruluşunda tutmadığını saptamıştır.

SEC'in tespit ettiği üzere, danışman fona ait belirli kripto varlıkları nitelikli saklayıcı olmayan, FTX Trading Ltd. gibi dijital varlık ticaret platformlarındaki hesaplarda tutmuştur. Fon ise ilgili platformun çöküşünün ardından varlıklarının yaklaşık yarısını kaybetmiştir. Bununla birlikte, SEC, danışmanın, yatırımcıları geri çekilme dönemleri ve uyum eksiklikleri konusunda yeterli düzeyde bilgilendirmediğini tespit etmiştir. Netice olarak danışman, saklama kuralının ihlalinden etkilenen fon yatırımcılarına dağıtılmak üzere 225.000 ABD doları tutarında ceza ödemeyi kabul etmiştir[64].
Sonuç olarak ABD'deki mevcut finansal piyasa altyapısı, kriptografik olarak kodlanmış varlıklara uygun şekilde tasarlanmamıştır. Kripto varlıklarının mevcut sistemlere entegrasyonu, önemli ölçüde finansal kaynaklar ve insan sermayesi gerektirmektedir. Özellikle, saklama hizmeti sunanların siber güvenlik alanında etkili ve önemli tedbirler alması ve müşteri varlıklarını siber saldırılardan korumak amacıyla teknolojik altyapılarını güçlendirmesi gerekmektedir.

ABD'deki yatırım danışmanları, müşteri portföyünde yer alan dijital varlıkları yönetirken çeşitli uyum zorlukları ile karşılaşabilecektir. Bunlardan ilki, dijital varlıkların 1933 tarihli Menkul Kıymetler Yasası'nda[65] yer alan "menkul kıymet" tanımının kapsamına girip girmediğine ilişkin süregelen belirsizliktir. SEC, daha önceki açıklamalarında bir blockchain tokeninin tek başına menkul kıymet olmadığını kabul etmiştir. Bununla birlikte, tokenlar ve diğer dijital varlıkların, ABD Yüksek Mahkemesi'nin SEC v. W.J. Howey, Co. davasında belirlediği yatırım sözleşmesi testi uyarınca menkul kıymet olarak sunulup satıldığını öne süren SEC, aktif olarak çeşitli dava süreçleri içinde yer almaktadır[66].

63 *https://blockchain.bakermckenzie.com/2024/07/16/house-fails-to-override-veto-of-bill-to-undo-sec-guidance-that-limits-banks-ability-to-custodian-crypto-assets/*

64 *Sidley Austin LLP, "Private Fund Adviser Settles with. SEC for Custody Rule".*

65 *https://www.sec.gov/files/rules/final/2009/ia-2968.pdf*

66 *Sidley Austin LLP, "Private Fund Adviser Settles with. SEC for Custody Rule"*

Bir diğer zorluk, dijital varlıkların sayısının ve çeşitliliğinin fazla olması sebebiyle tüm dijital varlıklar için nitelikli saklama kuruluşlarının mevcut olmamasıdır. Bu durum, söz konusu varlıkların "menkul kıymet olarak sunulup satıldığı" varsayıldığında dahi, danışmanların bu varlıklar için saklama kuralına tam olarak uyum sağlamasını engellemektedir. Bu belirsizlikler ve zorluklar dikkate alınmakla birlikte, dijital varlıklar üzerine yoğunlaşan yatırım danışmanları da dahil olmak üzere tüm danışmanların, SEC'in saklama kuralına uyumuna yönelik sürdürdüğü denetim ve yaptırım odaklı yaklaşımı ışığında, varlık koruma politikalarını ve prosedürlerini gözden geçirmeleri önerilmektedir.

Belirtilmelidir ki SEC'in önerdiği değişiklikler, kripto varlıkları saklayan nitelikli saklama kuruluşlarının sayısını azaltabilecek ve yatırımcıları, halihazırda güçlü koruma prosedürleri uygulayan platformlardan fonlarını çekmeye zorlayabilecektir. Önerilen değişiklikler ayrıca hedge fonları, özel sermaye fonları ve emeklilik fonları için kripto varlıklara yatırım yapmayı ve bu varlıkların saklamasını daha maliyetli hale getirdiği ve böylelikle ek uyum yükümlülüklerini üstlenmek istemeyen danışmanlar için kriptoyu bir varlık sınıfı olarak erişilemez kıldığı için eleştirilmektedir. Eleştirenler, bu durumun yatırımcılar ve firmaları da daha az düzenlenmiş offshore hizmetlere yönlendireceğinden ve FTX'in çöküşüne yol açan benzer koşullara sebep olacağından endişe duymaktadırlar.[67] Öte yandan SEC, kuralın kapsamının genişlemesiyle müşteri varlıklarının kaybı riski, nitelikli saklama kuruluşu tarafından tutulması gereken varlıkların durumu ve saklama düzenlemelerine ilişkin hukuki belirsizliklerin azalacağını ileri sürmektedir. Bu gerekçeyle, SEC, bu tür adımların kripto varlıklarına yönelik yatırım fırsatlarını ve danışmanlık hizmetlerinin erişilebilirliğini artırabileceğini savunmaktadır.

67 *Proskauer Rose LLP, "Regulation in the Post-FTX Environment".*

KAYNAKÇA

ANNUNZİATA, Filippo: "The Licensing Rules in MiCA", Fintech Regulation and the Licensing Principle", (Ed: Moura Vincente, Diogo Pereira Duarte ve Catarina Granadeiro, European Banking Institute, 2023.

Atlantic Council CBDC Report, https://www.atlanticcouncil.org/blogs/econographics/a-report-card-on-chinas-central-bank-digital-currency-the-e-cny/

Bank of England CBDC Design Proposal 2024, https://www.bankofengland.co.uk/research/digital-currencies

Ben-Sasson, E., et al. (2014). "Zerocash: Decentralized Anonymous Payments from Bitcoin."

BIS Annual Economic Report 2024, https://www.bis.org/about/bisih/topics/cbdc/mcbdc_bridge.htm

BIS Environmental Impact Study, https://www.bis.org/publ/othp82.pdf

BIS mBridge Project Documentation, https://www.bis.org/publ/othp59.htm

Blum, M., Feldman, P., & Micali, S. (1988). "Non-interactive zero-knowledge and its applications."

Boneh, D., & Shoup, V. (2020). A Graduate Course in Applied Cryptography.

Bünz, B., et al. (2018). "Bulletproofs: Short Proofs for Confidential Transactions."

Carlo R. W. De Meijer, Traditional financial custodians enter the crypto market (21.10.2024)- https://www.finextra.com/blogposting/27059/traditional-financial-custodians-enter-the-crypto-market#:~:text=The%20growing%20institutional%20interest%20across,institutional%20demand%20for%20regulated%2C%20secure

China's Progress Towards CBDC, https://www.csis.org/blogs/new-perspectives-asia/chinas-progress-towards-central-bank-digital-currency

Clifford Chance, "Custody of Cryptoassets: Moving Towards Industry Best Practice" Haziran 2023, 34: https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2023/06/custody-of-cryptoassets.pdf.

ÇETİN, Müge: "Sermaye Piyasası Hukuku Bakımından Kripto Varlıklar", On İki Levha Yayıncılık, 1. Baskı, İstanbul, 2023, s. 103; ilgili esere elektronik ortamda ulaşmak için: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4346795

Digital Yuan Technical Overview, http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf

Dirk Zetzsche, Julia Sinnig, Areti Nikolakopoulou, Crypto custody, Capital Markets Law Journal, Volume 19, Issue 3, July 2024, https://doi.org/10.1093/cmlj/kmae010

Eli Ben-Sasson, et al. (2018). "Scalable, transparent, and post-quantum secure computational integrity."

KAYNAKÇA

FINMA, Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs) Published 16 February 2018, https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf

FINMA, Resolution Report 2020, https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/finma-publikationen/resolution-bericht/20200225-resolution-bericht-2020.pdf?sc_lang=en&hash=CCE986A47FCDE3D13A8DD4A748BC12DF

FSB Global Regulatory Framework for Crypto-Asset Activities Umbrella public note to accompany final framework (17.7.2023) https://www.fsb.org/uploads/P170723-1.pdf s. 5–6.

F. Yan, Y. Gu, Y. Wang, C. M. Wang, X. Y. Hu, H. X. Peng, et al., "Study on the interaction mechanism between laser and rock during perforation," Optics and Laser Technology, vol. 54, pp. 303-308, Dec 2013.

Goldreich, O. (2001). Foundations of Cryptography: Volume 1, Basic Tools.

Goldwasser, S., Micali, S., & Rackoff, C. (1985). "The Knowledge Complexity of Interactive Proof Systems."

IMF Central Bank Survey 2024, https://www.imf.org/en/Publications/digital-money-research

IMF, Elements of Effective Policies for Crypto Assets (13.02.2023), https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/02/23/Elements-of-Effective-Policies-for-Crypto-Assets-530092.

IMF Fintech Notes: Regulating the Crypto Ecosystem The Case of Unbacked Crypto Assets Parma Bains, Arif Ismail, Fabiana Melo, and Nobuyasu Sugimoto, 2022.

International Monetary Fund, "Recording Crypto Assets in Macroeconomic Statistics," Haziran 2022, https://www.imf.org/external/pubs/ft/gfs/gfsac/pdf/Recording_Crypto_Assets_MacroStats_July_22.pdf .

Lindell, Y., & Katz, J. (2014). Introduction to Modern Cryptography.

PWC CBDC Implementation Guide, https://www.pwc.com/it/it/publications/assets/docs/central-bank-digital-currency.pdf

Project Dunbar Technical Framework, https://www.bis.org/about/bisih/projects/dunbar.htm

Proskauer Rose LLP, "Regulation in the Post-FTX Environment: SEC's Proposed Enhanced Custody Rule and Its Effects on Crypto", Şubat 2023: https://www.proskauer.com/blog/regulation-in-the-post-ftx-environment-secs-proposed-enhanced-custody-rule-and-its-effects-on-crypto.

PwC, "About the Crypto Assets Guide," https://viewpoint.pwc.com/dt/us/en/pwc/accounting_guides/crypto-assets-guide/crypto_assets_guide/aboutthecryptoassets.html.

KAYNAKÇA

SEC. Staff Accounting Bulletin No. 121, 31 Mart 2022. https://www.sec.gov/regulation/staff-interpretations/accounting-bulletins/old/staff-accounting-bulletin-121

Sidley Austin LLP, "Crypto-Focused Private Fund Adviser Settles with U.S. SEC for Custody Rule and Other Violations," Eylül 2024, https://www.sidley.com/en/insights/newsupdates/2024/09/crypto-focused-private-fund-adviser-settles-with-us-sec-for-custody-rule-and-other-violations.

Swiss Digital Custody Report 2023, https://static1.squarespace.com/static/6641b46de2c26a6478ff8f6e/t/666b18cdfb4ce0015152d037/1718294737562/Swiss+Digital+Asset+Custody+Report+2023.pdf

Swiss Digital Asset Custody Report 2024, https://static1.squarespace.com/static/6641b46de2c26a6478ff8f6e/t/668323ba60d1d203f76fff68/1719870411796/Swiss_+Digital_Asset_Custody_Report_2024.pdf

The Board of the International Organization of Securities Commissions (IOSCO), Policy Recommendations for Crypto and Digital Asset Markets Final Report (16 Kasım 2023)

Türkiye Bankalar Birliği, Dijital Varlıklara Yönelik Bankacılık Açısından Genel Bakış, Potansiyel İş Modelleri ve Dijital Varlıkların Hukuki Açıdan Değerlendirmesi (07.02.2022)

Uniform Commercial Code, Article 8, "Investment Securities," American Law Institute and Uniform Law Commission

World Federation of Exchanges, Crypto-Asset Custody: A Blueprint for Regulatory and Operational Excellence (28.08.2024), https://www.worldexchanges.org/storage/app/media/Cally%20Billimore/Custody%20of%20Crypto%20-%20Final.pdf

https://blockchain.bakermckenzie.com/2024/05/13/u-s-house-passes-bill-to-undo-sec-guidance-that-limited-banks-ability-to-custodian-crypto-assets/
https://blockchain.bakermckenzie.com/2024/07/16/house-fails-to-override-veto-of-bill-to-undo-sec-guidance-that-limits-banks-ability-to-custodian-crypto-assets/

Sidley Austin LLP, "Private Fund Adviser Settles with. SEC for Custody Rule".

https://www.sec.gov/files/rules/final/2009/ia-2968.pdf

https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Auslegungsentscheidung/BA/ae_Hinweise_zur_Auslegung_64y_KWG_en.html;jsessionid=46D99BD1E20DC2DEC63AAA39C118ED20.internet001?nn=19578884
https://blog.arksigner.com/blokzinciri-teknolojisi/web-3-0-doneminde-regulasyon-avrupa-birliginin-mica-tuzugu

https://blockworks.co/news/what-are-smart-contract-wallets

https://brainwallet.io/

https://en.adgm.thomsonreuters.com/sites/default/files/net_file_store/Guidance-Regulation_ofVirtual_Asset_Activities_in_ADGM_(VER05.181223).pdf

KAYNAKÇA

https://www.adgm.com/documents/legal-framework/guidance-and-policy/fsra/guidance-icos-and-crypto-assets_20180625_v11.pdf
https://www.adgm.com/documents/legal-framework/guidance-and-policy/fsra/guidance-virtual-asset-activities-in-adgm-20231218.pdf

https://www.ecfr.gov/current/title-17/chapter-II/part-275

https://www.investopedia.com/terms/p/paper-wallet.asp

https://www.kaspersky.com.tr/resource-center/definitions/what-is-a-hardware-wallet

https://www.liminalcustody.com/knowledge-center/understanding-digital-asset-custodians/

https://rulebooks.vara.ae/rulebook/custody-services-rulebook

https://spk.gov.tr/data/668412388f95db0c2c4e36d5/Ek-1%20Duyuru Talep%20Edilen%20Belgeler.pdf

https://spk.gov.tr/kurumlar/kripto-varlik-hizmet-saglayicilar/faaliyette-bulunanlar-listesi

https://www.world-exchanges.org/our-work/articles/crypto-asset-custody-blueprint-regulatory-and-operational-excellence

KATKI SAĞLAYANLAR

- **Dr. Mustafa Takaoğlu**
Tübitak

- **Dr. Taner Dursun**
Tübitak

- **Doç Dr. Mehmet Sabir Kiraz**
De Montfort University

- **Dr. Süleyman Kardaş**
Batman Üniversitesi

- **Dr. Pınar Çağlayan Aksoy**

- **Ahmet Mesut Şahinoğlu**
Paribu Custody

- **Aysu Düz**
Paribu

- **Cem Sağlam**
Paribu Custody

- **Nergis Nurcan Karababa**
Paribu Custody

- **Meva Öztürk**
Paribu

- **Deniz Parlaöz**
BCTR

- **Merve Öztürk Günaltay**
BCTR

- **Ozan Eğe**
Web3 Meta Hub

- **İlayda Aydın**
Web3 Meta Hub

- **Bekir Yenidoğan**
KPMG Türkiye

- **Bartu Kaan Ertuğrul**
KPMG Türkiye

- **Gizem Koçak**
PwC

- **Reşat Uğur Ulu**
Togg

- **Hasan H. Yaşar**
Kolcuoğlu Demirkan Koçaklı Hukuk Bürosu

- **Sinem Nilsu Bayazıt**
Kolcuoğlu Demirkan Koçaklı Hukuk Bürosu

- **İrem Cansu Demircioğlu Mercan**
Kolcuoğlu Demirkan Koçaklı Hukuk Bürosu

- **Yağmur Gündoğdu**
Akıncı Hukuk Bürosu

- **Murat Yılmaz**
Akbank

- **Onur Çakır**
Halkbank

- **Cemal Araalan**
CBC Hukuk Bürosu

- **İzel Beliz Taylan**
Defy

- **Suat Özkan**
Defy

BLOCKCHAIN
TÜRKİYE

KRİPTO VARLIK SAKLAMA
RAPORU

Kripto Hizmet Sağlayıcıları
Çalışma Grubu

TBV
TÜRKİYE BİLİŞİM VAKFI