

KRİPTO EKOSİSTEMİNDE İZ KAYBETTİRME: KRİPTO VARLIK MİKSERLERİ

Kripto varlık mikserleri, blokzincir üzerindeki işlem verilerini bölerek ve yeniden birleştirerek kullanıcıların gizliliğini artırmayı amaçlayan araçlar olarak geliştirilmiştir. Ancak bu sistemlerin sağladığı yüksek anonimlik, kripto varlıkların kaynağının gizlenmesini kolaylaştırmaktadır. Bu durum, suçtan elde edilen gelirlerin aklanması, dolandırıcılık yoluyla sağlanan fonların izinin kaybettirilmesi ve birden fazla düzenleyici yükümlülüğün ihlal edilmesinin örtülmesi gibi riskleri ciddi ölçüde artırmaktadır.

1. Kripto Varlık Mikseri Nedir?

Kripto varlık mikserleri birden fazla kullanıcının kripto varlıklarını tek bir havuzda toplayıp karıştırarak ve bu varlıkları farklı tutarlarda ve farklı zamanlarda yeni adreslere dağıtarak fonların kaynağını ve nihai sahibini gizlemeyi amaçlayan hizmetlerdir. Bu yapı, blokzincirde anonimlik esasına dayanmakta olup kullanıcıların kripto varlıklarını işlem geçmişiyle ilişkilendirilmeden takas etmelerine veya farklı adreslere yönlendirmelerine imkân tanımaktadır. Ayrıca bazı mikserler işlem ücretlerini değiştirerek veya farklı çekim adresleri kullanarak mikser kullanımının kendisini de gizlemeye çalışmaktadır.

Kripto varlık mikserleri temel olarak çalışma biçimlerine göre merkezi ve merkeziyetsiz olmak üzere iki kategoriye ayrılır:

- **Merkezi Mikserler:** Kullanıcıların kripto varlıklarını tek bir havuzda toplayarak belirli bir ücret karşılığında farklı kripto varlıklar iade eden ve bu işlem için kullanıcıdan tam yetki alan hizmet sağlayıcılarıdır; ancak işlemlere ilişkin kayıt tutulması ve üçüncü bir tarafa duyulan yüksek güven gerekliliği nedeniyle gizlilik ihlali ve veri sızıntısı riskleri barındırmaktadır.



- **Merkeziyetsiz Mikserler:** Merkeziyetsiz mikserler, *CoinJoin* ve benzeri protokoller ile “sıfır bilgi ispatı” tekniklerini kullanarak kullanıcı fonlarını tek bir havuzda birleştirip yeniden dağıtan ve saklama yetkisi bulunmayan karıştırma sistemleridir. Kayıt tutulmaması ve işlemlerin akıllı sözleşmeler üzerinden yürütülmesi nedeniyle fonların kaynağının tespiti güçleşmekte ve merkezi mikserlere kıyasla daha yüksek düzeyde gizlilik sağlanmaktadır.



2. Dolandırıcılık, Kara Para Aklama ve Siber Suçlarda Kripto Varlık Mikseri Kullanımı

Kripto varlık mikserleri, blokzincir işlemlerine ek bir gizlilik katmanı sağlamakla birlikte, işlem geçmişini parçalayarak fon akışlarının izlenebilirliğini azaltan yapıları nedeniyle dolandırıcılık, siber suçlar ve kara para aklama bakımından suç gelirlerinin gizlenmesine elverişli yüksek riskli araçlar olarak değerlendirilmektedir. Bu kapsamda kötü niyetli kullanıcılar, siber saldırı gelirleri, uyuşturucu ticaretinden elde edilen kazançlar, fidye yazılımı ödemeleri ve benzeri yasa dışı fonların kaynağını perdelemek için mikserlerden yararlanmaktadır. Nitekim siber suçlular da yasa dışı gelir elde ettikleri cüzdanlar ile bu fonları kripto borsalarına aktardıkları çıkış cüzdanları arasındaki bağlantıyı koparmak amacıyla mikserlerden yararlanmakta; böylece kara para aklama izleme mekanizmalarının tetiklenmesini ve fon hareketlerinin tespit edilmesini zorlaştırmaktadır. Europol’ün *ChipMixer* operasyonuna ilişkin bulguları da bu tespitleri doğrulamakta olup mikser üzerinden yönlendirilen işlemlerin önemli bir bölümünün darkweb pazarları, fidye yazılımı grupları, yasa dışı mal kaçakçılığı, çocuk istismarı materyallerinin dolaşımı ve çalınmış kripto varlıklarla bağlantılı olduğu ifade edilmiştir.

Kara para aklamanın yanı sıra dolandırıcılık vakalarında da kullanılan mikserler, özellikle yatırım dolandırıcılıkları, sosyal mühendislik yöntemleriyle gerçekleştirilen yetkisiz transferler ve siber saldırılar sonucunda elde edilen fonların hızlı şekilde “ayrıştırılması” ve zincir üzerindeki izlerinin azaltılması amacıyla kullanılmaktadır. Kripto ödemelerinin izlenmesini güçleştirmek için mikser kullanımı yaygın bir ara aşama hâline gelmiş olup bu durum siber suç gelirlerinin takip ve tespit süreçlerini daha da karmaşıklştırmaktadır.



3. Mali Eylem Görev Gücü (“FATF”), Mali Suçları Araştırma Kurulu (“MASAK”) ve 5237 Sayılı Türk Ceza Kanunu (“TCK”) Kapsamında Değerlendirme

Kripto varlık mikserlerinin fon hareketlerini gizlemeye elverişli yapısı nedeniyle, uluslararası standart belirleyiciler ile ulusal düzenleyici ve ceza normları bu hizmetleri yüksek risk kategorisinde değerlendirmekte; bu çerçevede FATF rehberleri, MASAK düzenlemeleri ve TCK hükümleri mikser kullanımının doğurduğu kara para aklama ve suç gelirlerinin gizlenmesine ilişkin riskleri farklı düzenleyici perspektiflerden ele almaktadır.



3.1. FATF Rehberleri Uyarınca Değerlendirme

FATF rehberleri, kripto varlık mikserleri blokzincir üzerindeki işlem zincirini karmaşık, yarı rastlantısal sahte işlemlerle kırarak belirli sanal paraların belirli işlemlerle ilişkilendirilmesini son derece güçleştiren “anonimleştirici araçlar” olarak tanımlamakta ve bu nedenle yüksek düzeyde kara para aklama/terörizmin finansmanı riski taşıyan yapılar arasında saymaktadır. Yine 2019 tarihli Risk Temelli Yaklaşım (RBA) rehberinde ise, anonimlik artırıcı kripto paralarla birlikte gömülü mikser içeren kripto varlıkların ve bu tür ürün ve hizmetleri sunan iş modellerinin, işlemlerin şeffaflığını azaltmaları ve müşteri tanıma ile işlem izleme yükümlülüklerini fiilen işlevsiz hâle getirebilmeleri sebebiyle kripto varlık hizmet sağlayıcıları bakımından özel olarak dikkate alınması gereken, daha yüksek riskli faaliyetler olduğu; bu çerçevede ülkelerin ve kripto varlık hizmet sağlayıcıların ulusal risk değerlendirmelerinde mikser kullanımını açıkça tanımlayıp daha sıkı müşteri tanıma, kayıt tutma, şüpheli işlem bildirimi ve yaptırım taraması önlemleriyle bunları yönetmesi gerektiği vurgulanmaktadır.

3.2. MASAK Mevzuatı Uyarınca Değerlendirme

MASAK mevzuatı ve Kripto Varlık Hizmet Sağlayıcılarına Yönelik Uyum Rehberi çerçevesinde, kripto varlık mikserleri, kripto varlık transferlerinde işlemin taraflarını ve fonların kaynağını gizlemeye yönelik anonimlik artırıcı yapılar olarak, özellikle kayıtlı olmayan cüzdan adresleriyle veya gönderen/alıcı bilgilerini paylaşma yükümlülüğü bulunmayan yurtdışı platformlar üzerinden gerçekleştirilen transferlerle benzer mahiyette yüksek riskli işlemler kapsamında değerlendirilmelidir. Bu tür yapılara aracılık edilmesi, 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun ve ikincil düzenlemeler uyarınca kripto varlık hizmet sağlayıcılar bakımından sıkılaştırılmış müşteri tanıma tedbirleri, şüpheli işlem bildirimi yükümlülüğü, gerekli hâllerde 19/A maddesi kapsamında işlemlerin ertelenmesi veya malvarlığının dondurulması süreçlerinin tetiklenmesi, ayrıca uyum yükümlülüklerinin ihlali hâlinde idari yaptırımlar ve denetim riskinin artması gibi sonuçlar doğurabilecek niteliktedir; bu nedenle platformların mikser kaynaklı veya mikserlere yönelen transferler açısından risk temelli bir yaklaşımla işlem kabulü, geciktirme, limit uygulama veya işlemi reddetme kararlarını dikkatle tesis etmeleri gerekmektedir.



3.3. TCK Kapsamında Değerlendirme

TCK'nın 244. maddesinde düzenlenen bilişim sistemlerine yönelik fiiller ile 283. maddesinde düzenlenen suçtan kaynaklanan malvarlığı değerlerini aklama suçu birlikte değerlendirildiğinde, mikserler suçtan elde edilen kripto varlıkların çok sayıda işlemle rastlantısal şekilde dağıtılması ve yeni cüzdanlara aktarılması suretiyle fonların kaynağı ile fail arasındaki bağın koparılmasını amaçlayan bir anonimleştirme mekanizması yaratmasıyla suçtan elde edilen malvarlığı değerlerini gizleme, kaynağını belirsizleştirme veya bunların meşru bir kaynaktan geldiği izlenimini oluşturma şeklindeki aklama fiillerine teknik kolaylık sağladığı anlaşılmaktadır. Bu nedenle kripto varlık mikserlerinin, suç gelirlerinin izlenebilirliğini ortadan kaldırmaya elverişli yapıları itibarıyla hem TCK m.283 kapsamındaki aklama suçunun icrasına aracılık eden bir yöntem olarak hem de suçun ortaya çıkarılmasını ve delillendirilmesini güçleştiren bir "gizleme aracı" olarak değerlendirilmesi mümkündür.



4. Uluslararası Yaptırımlar: ABD ve OFAC Uygulamaları

ABD'de faaliyet göstermeyi planlayan kripto varlık hizmet sağlayıcıları açısından, ABD Adalet Bakanlığı'nın kripto varlık işlemlerini gizlemeye yönelik faaliyetlerin suç teşkil edebileceğine ilişkin açık tutumu belirleyici niteliktedir. Nitekim 6 Ekim 2021 tarihinde Bakanlık, mikser ve karıştırıcıların suç amaçlı kullanımını soruşturmak ve kovuşturmak üzere Ulusal Kripto Para Yaptırım Ekibi'ni (National Cryptocurrency Enforcement Team - NCET) kurduğunu duyurmuştur. Mali Suçları Araştırma Ağı (FinCEN), saklamalı mikser hizmeti sunan kişi ve kuruluşları Banka Gizliliği Yasası (Bank Secrecy Act - BSA) kapsamında para transferi hizmet sağlayıcısı olarak tanımlamakta ve bu kapsamda FinCEN'e kayıt, etkin bir AML/KYC programı oluşturma ve ilgili raporlama ile kayıt tutma yükümlülüklerinin yerine getirilmesini zorunlu kılmaktadır. Bunun yanı sıra, ABD Hazine Bakanlığı'na bağlı OFAC'ın uyguladığı yaptırımlar da dikkate çekmektedir.

