KRİPTO MİKSERLERİNDE GÖRÜNMEZLİK: KRİPTO VARLIKLARIN TAKİBİ

1. Mikserlerden Çıkış: Blokzincir Üzerinde Fon Akışı

Kripto mikserler, farklı kullanıcılara ait kripto varlıkları tek bir havuzda bir araya getirerek ve sonrasında bu varlıkları farklı adreslere, farklı tutarlarda ve zaman aralıklarında yeniden dağıtarak işlem geçmişi ile varlığın nihai alıcısı arasındaki bağlantıyı zayıflatmayı amaçlayan çevrim içi hizmetlerdir. Bu yapı, uygulamada, özellikle suçtan kaynaklanan gelirlerin kaynağının tespit edilmesini zorlaştıran bir sonuç ortaya çıkarmaktadır. Bununla birlikte, blokzincirin temel niteliğinin geri alınamaz ve aleni olması sayesinde, söz konusu işlemler blokzincir üzerinde kayda geçmeye devam etmektedir.

Bu noktada temel soru, mikser kullanımının kripto varlıkların izlenmesini tamamen imkânsız hâle getirip getirmediğidir. Uygulamada, mikserler fon akışını karmaşıklaştırmakta ve izleme süreçlerini yavaşlatmaktadır; ancak bu durum, kripto varlık takibinin sona erdiği anlamına gelmemektedir. Blokzincirin herkese açık yapısı sayesinde, işlem kayıtları zincir üzerinde varlığını sürdürmekte ve uygun araçlar kullanıldığında analiz edilebilmektedir. Özellikle, mikserlerin sınırlı likiditeye sahip olması, yüksek tutarlı işlemlerin etkin şekilde seyreltilmesini zorlaştırmakta; kolluk kuvvetlerinin mikser altyapılarına yönelik müdahaleleri sonucunda elde edilen teknik veriler ise geçmiş işlemlerin geriye dönük olarak incelenebilmesine olanak sağlamaktadır.

Bu çerçevede, mikserler izlenebilirliği önemli ölçüde sınırlandırsa da kripto varlık hareketlerinin tamamen görünmez hâle geldiği söylenemeyecektir. Dolayısıyla mikserler, mutlak bir gizlilik sağlamaktan ziyade, fon akışının doğrudan ve hızlı biçimde izlenmesini zorlaştıran bir araç olarak değerlendirilmelidir.

2. Teknik İzleme Yöntemleri: Mikser Sonsuz Bir Kara Delik midir?

Kripto varlıkların mikser hizmetlerine girmesi ve bu hizmetlerden çıkmasının ardından, söz konusu kayıtların blokzincir üzerinde izlenebilmesi, blok zincirlerinin kamuya açık ve geri alınamaz yapısından kaynaklanmaktadır. Blokzincirler, bir varlığın gönderim ve alım geçmişini her işlem düzeyinde saklamakta; bu kayıtlar silinmemekte ve belirli yöntemlerle denetlenebilmektedir. Bu şeffaf yapı, mikserler gibi fon akışını karmaşıklaştıran araçlar kullanılsa bile, fon hareketlerinin izlenmesine yönelik kripto analizlerinin teknik temelini oluşturmaktadır. Bu bağlamda izleme yöntemleri, yalnızca işlem geçmişini değil, aynı zamanda işlem örüntülerini ve adresler arasındaki bağlantıları da değerlendiren sofistike algoritmalara dayanmaktadır.

Mikser sonrası takibin teknik araçları arasında **adres kümelendirme ve işlem grafiği analizi** yer almaktadır. Adres kümelendirme, birden fazla adresin muhtemelen aynı kişi ya da aktör tarafından kontrol edildiğini belirlemek için kullanıcı davranışları ve işlem örüntülerini istatistiksel olarak değerlendirmektedir; bu sayede mikser çıkışındaki adresler ve sonraki transferler arasındaki bağlantılar ortaya konabilmektedir. Zincir analizi ise adresler arasındaki para akışlarını grafiksel olarak haritalandırarak fonların izini sürmeyi kolaylaştıran yapısal modeller oluşturmaktadır. Bu yöntemler, blokzincir üzerindeki veriyi bir iz sürme patikasına dönüştürmede, analiz şirketlerinin ve kolluk birimlerinin başvurduğu standart tekniklerdir.

Bununla birlikte, mikslenmiş fonların izini sürmek, yalnızca temel bir para akışı takibinden daha karmaşık olup gelişmiş yöntemler gerektirmektedir. Örneğin, En Düşük Ara Bakiye Kuralı *(LIBR)* gibi teknikler, bir mikser cüzdanına giren varlıkların farklı adreslere nasıl dağıldığını, hangi varlıkların izlenebilir kaldığını ve potansiyel "temiz" bakiyeleri analiz etmeye yardımcı olmaktadır. Bu tür yöntemlerde, mikser havuzuna giren ve çıkan işlemlerin bakiyeleri, zaman çizelgeleri ve transfer ağırlıkları gibi veriler kullanılarak fonların muhtemel iz sürme rotaları hesaplanmaktadır. Böylelikle, mikser haricinde yeni adreslere yapılan hareketlerin adım adım takip edilebilmesi mümkün olmaktadır. Tüm bu teknik araçlar ve analiz yöntemleri, fonların mikser sisteminden çıktıktan sonra tamamen görünmez hale gelmediğini göstermektedir.

Her ne kadar mikserler, işlem örüntülerini bulanıklaştırarak iz sürmeyi zorlaştırıyor olsa da mikser sonrası kripto varlıkların ilk giriş adresleriyle yeni adresler arasındaki bağlantılar büyük olasılıkla yeniden ortaya konabilmekte veya daraltılabilmektedir. Nitekim, mikser sonrası izleme faaliyetleri her zaman belirli bir girdinin belirli bir çıktıyla birebir eşleştirilmesini hedeflememekte; fonların hareket ettiği adres kümeleri ve ekosistemler üzerinde risk temelli bir değerlendirme yapılmasına odaklanmaktadır. Bu çerçevede, teknik izleme yöntemleri hem adli soruşturmalarda hem de suç gelirlerinin aklanmasının önlenmesi *(AML)* süreçlerinde mikser kullanımının etkinliğini değerlendirmek ve gerektiğinde delil elde etmek için kullanılmaktadır.

3. Şüpheli Adresleri Belirleme ve Risk Değerlendirme

Suç gelirlerinin aklanmasının önlenmesine *(AML)* yönelik uyum programları, kripto varlık platformlarında yüksek riskli fon hareketlerini tespit etmek ve bunlara karşı tedbir almak için sistematik risk değerlendirme süreçlerini zorunlu kılmaktadır. Bu bağlamda, kripto mikserlere giriş veya mikserlerden çıkış yapan kripto adresleri, uyum araçları tarafından yüksek risk kategorisine dahil edilebilmektedir. Zira mikserlerle bağlantılı fon geçmişi, fonun meşru kaynakla ilişkilendirilmesini güçleştirmektedir. Uyum yazılımları, mikro ve makro ölçekte adresler arası ilişkileri analiz ederek bir fonun mikser bağlantısı olup olmadığını belirlemekte ve mikser geçmişi olan adresleri düzenleyici risk tanımlamaları kapsamında yüksek riskli işlem göstergesi olarak işaretlemektedir. Bu tür risk etiketlemeleri, kripto varlık hizmet sağlayıcılarının *(CASP)* uyum yükümlülüklerini yerine getirmek ve suç gelirlerinin aklanmasının önlenmesine yönelik regülasyonlarının öngördüğü risk bazlı yaklaşıma uygun davranmak için kritik önemdedir.

Bahse konu uyum sistemlerinin etkinliği, yalnızca adres geçmişini tanımlamakla sınırlı olmamakta, aynı zamanda işlem risk puanlama modülleri ile Müşterini Tanıma ve İşlem Tanıma *(KYC/KYT)* süreçleri aracılığıyla şüpheli faaliyetlerin otomatik olarak tanımlanmasına ve gerekli uyum adımlarının tetiklenmesine de imkân tanımaktadır. İşlem Tanıma sistemleri, blokzincir üzerindeki işlemleri gerçek zamanlı izleyerek bir işlemde mikser geçmişi veya diğer yüksek riskli göstergeler bulunduğunda anında uyarı vermektedir; bu uyarılar, platformun otomatik olarak işlemi durdurmasına, ek bilgi talep etmesine veya ilgili fonları dondurmasına imkân sağlayacak şekilde düzenlenmektedir. Benzer şekilde, Müşteri Tanıma süreçleri kullanıcının kimliğini doğrularken, mikserle bağlantılı geçmiş yüksek riskli fonlara sahip kullanıcılar için artırılmış inceleme gibi ek uyum tedbirlerinin uygulanmasını gerektirmektedir. Bu risk odaklı yaklaşım, suç gelirlerinin aklanmasının önlenmesi standartlarının gerektirdiği proaktif izleme mekanizmasının bir parçası olup kripto platformlarının hem yerel düzenlemelere hem de uluslararası standartlara uyum sağlama yükümlülüğünü güçlendirmektedir.

4. Mikserlerle Mücadelede Adli ve Cezai Uygulamalar

Kripto varlıkların gizlenmesine hizmet eden mikserlerle mücadele kapsamında, özellikle son yıllarda adli ve cezai yaptırımların somut biçimde uygulandığı görülmektedir. Bu kapsamda, ABD Hazine Bakanlığı'na bağlı Yabancı Varlıklar Kontrol Ofisi *(OFAC)*, 6 Mayıs 2022 tarihinde bir Bitcoin mikserini, Kuzey Kore ile bağlantılı bir siber suç yapılanması tarafından gerçekleştirilen blokzincir ağına yönelik saldırı sonucunda ele geçirilen yaklaşık 620 milyon ABD doları tutarındaki kripto varlığın aklanmasında kullanıldığı gerekçesiyle yaptırım listesine almıştır.

Bunu takiben, OFAC, 8 Ağustos 2022 tarihinde ise Ethereum tabanlı bir miksere yaptırım uygulanmış; söz konusu hizmetin 2019'dan itibaren 7 milyar ABD dolarını aşan tutarda kripto varlığın izinin kaybettirilmesinde kullanıldığını ve bu fonların önemli bir kısmının siber suçlar ve uluslararası yaptırımlara tabi aktörlerle bağlantılı olduğunu açıklamıştır. Bu yaptırımlar, yalnızca mikser hizmetlerinin kendisini değil, bu hizmetlerle ilişkili akıllı sözleşme adreslerini de kapsayacak şekilde genişletilmiş; böylece ilgili adreslerle işlem yapılması ABD hukuku bakımından yasaklanmıştır.

Güncel ve çarpıcı örneklerden bir diğeri, *Bitcoin Fog* adlı miksere yöneliktir. Mart 2024'te Washington D.C. Federal Mahkemesi'nde görülen davada; suç gelirlerinin aklanmasına aracılık etme, para aklama komplosu ve lisanssız para iletimi suçlarından hüküm verilmiş, mikseri işleten şahıs, 12 yılı aşkın hapis cezasına çarptırılmış ve milyonlarca dolar değerindeki kripto varlığa ilişkin müsadere kararı verilmiştir. Benzer şekilde, uluslararası kolluk iş birliğinin mikserlere karşı yürütülen mücadelede kritik rol oynadığı görülmekte olup Aralık 2025'te İsviçre ve Almanya'daki federal makamların Avrupa Birliği Kolluk İş Birliği Ajansı (*Europol)* koordinasyonunda gerçekleştirdiği operasyonla *Cryptomixer.io* adlı büyük ölçekli Bitcoin mikseri kapatılmış; fidye yazılımı ve siber suç gelirleriyle bağlantılı işlemleri gizlemek amacıyla kullanıldığı tespit edilen altyapıya el konulmuş, 25 milyon EUR değerinde Bitcoin ile 12 terabaytın üzerinde veri ele geçirilmiştir.