KRİPTO PARALARIN TERÖRİZMİN FİNANSMANI VE AKLAMA SUÇLARINDA KULLANILMASI

TERÖRİZMİN FİNANSMANINDA VE KARA PARA AKLAMADA NEDEN KRİPTO PARALAR TERCİH EDİLİYOR?

Merkeziyetsizdir. Kripto paralar merkezi otoriteye bağlı değildir.

Anonimdir. Kişi bilgileri ihtiva etmez.

Sınır ötesidir. İnternete ulaşılabilen her yerde işlem yapılabilir.

Regülasyonu zordur. Uluslararası işbirliği gerektirir.

TERÖRİZMİN FİNANSMANINDA KRİPTO PARALARIN PAYI NE KADARDIR?

Karapara aklama ya da terörizmin finansmanı gibi eylemler ilk kripto para olan Bitcoin ile ortaya çıkmamıştır.

Terörizmin finansmanında kripto paraların payı hala oldukça düşüktür.

Kripto para işlemlerinin yalnızca %1'inin yasadışı faaliyetler gerçekleştirmek amacıyla yapıldığı, bu yasadışı faaliyetlerin de yalnızca %0.05'inin terörizmin finansmanı amacıyla yapıldığı bilinmektedir .

HANGİ YÖNTEMLER KULLANILIR?

Bağış toplama: Terör örgütleri, kripto paralarla bağış toplamak için internet siteleri, sosyal medya hesapları veya karanlık ağ (dark web) üzerinden sanal cüzdan adresleri yayınlamaktadır.

2016 yılında gerçekleşen bir terörist organizasyonun ilk kitle fonlaması, Mücahitler Şura Konseyi'nin basın kolunun İbn Teymiyye Basın Merkezi tarafından düzenlenmiştir. Kampanya, "Bizi silahlandır." sloganıyla yürütülmüştür. Bu fon toplama faaliyeti, İzzeddin el-Kassam Tugayları adlı silahlı bir grup tarafından 2019 yılında kripto paraları kullanarak gerçekleştirilmiştir. Bu, o tarihte silahlı bir grubun gerçekleştirdiği en büyük kripto para fonlamasının bir parçası olarak kabul edilmiştir ve üç aşamada gerçekleşmiştir.

İlk Aşama: QR Kod Kullanımı Fonlama kampanyasının ilk aşamasında, bir QR kod kullanılmıştır. Kripto para göndermek isteyenler, bu QR kodu tarayarak belirli bir Bitcoin adresine gönderim yapmışlardır. QR kodu farklı yollarla yayılmış, ancak bu adresin Birleşik Devletler merkezli bir kripto para borsası tarafından kullanıcılarına sunulan bir adres olduğu tespit edilmiştir. Borsa bilgilendirilerek adres dondurulmuş ve fonlar ele geçirilmiştir.

İkinci Aşama: Özel Bitcoin Adresi İkinci aşamada, bir borsa hesabı kullanıldığında, adres üzerindeki tasarruf yetkisinin sınırlanabileceği ve adres ile ilişkili borsa hesabının takip edilebileceği anlaşıldığı için, özel bir Bitcoin adresi oluşturulmuş ve bu adrese kripto para gönderilmesi talep edilmiştir.

Üçüncü Aşama: Gelişmiş Yöntemler Üçüncü aşamada daha sofistike bir yöntem kullanılmıştır. Bağış için kullanılan web sitesine bir Bitcoin cüzdanı gömülmüş ve para aktarımı yapmak isteyenler, reCAPTCHA doğrulamasını geçerek her seferinde kendilerine özel üretilen bir adrese ulaşıp para aktarmışlardır.

Birleşik Krallık ve Fransa tarafından yürütülen soruşturmalar, DEAŞ terör örgütünün 2016-2020 yılları arasında kripto paralarla finanse edildiğini ortaya koymuştur.

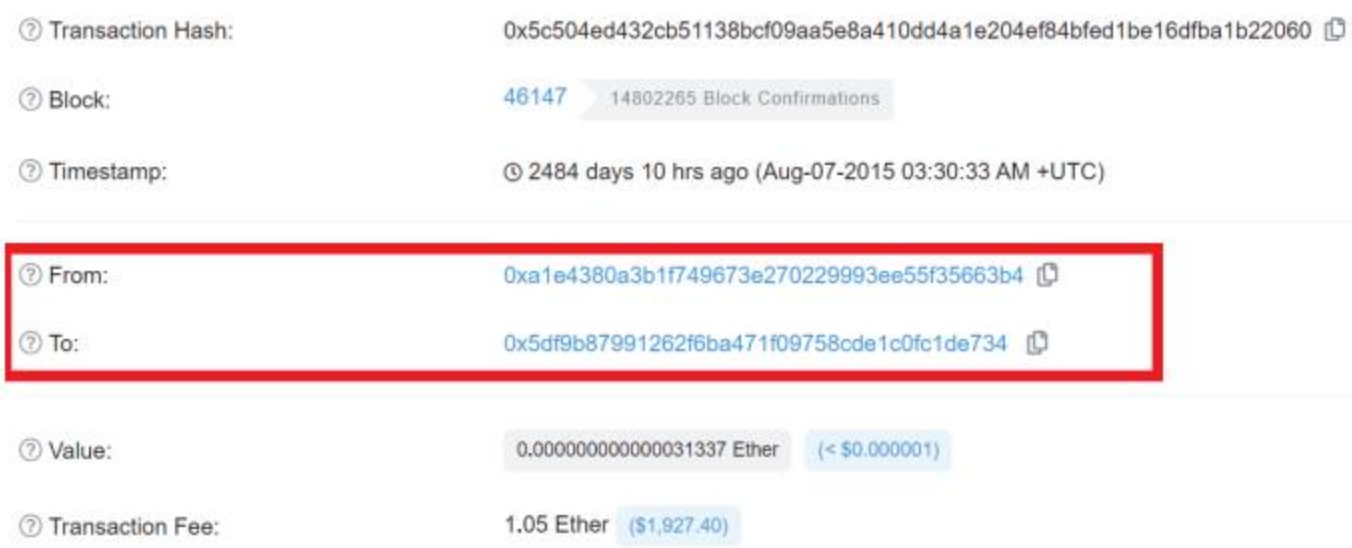
Ayrıca, Amerika Birleşik Devletleri'nde gerçekleşen ve terörist bir eylem olarak nitelendirilen "6 Ocak 2021 Kongre Baskını"ndan bir ay önce, olaya dahil olan aşırıcı grupların, tek bir bağışçıdan 500.000 Amerikan dolarının üzerinde Bitcoin bağışı aldıkları tespit edilmiştir.

ANONİMLİĞİN SINIRI

Bitcoin işlemleri KURAL OLARAK herkese açıktır, ağ üzerinde gerçekleşen işlemler herkes tarafından izlenebilir ve kontrol edilebilir. Bütün işlemler görülebilir olsa da işlemleri gerçekleştirenlerin kimliği, gerçekleştiren kimse bunu bir şekilde açıklamamış ya da yaptığı işlemler takip edilerek kim olduğu bilinemediği sürece anonim kalmaktadır.

Bu durum gizlilik odaklı kripto paralarda tersine dönmektedir.

Şekil 3. 4 Gerçekleştirilen ilk Ethereum transferi.



(Kaynak: Etherscan[515])

Burada gönderen ya da alıcı kimliğiyle alakalı hiçbir sonuç çıkarılamaz.

42 karakterli bu hesabın sahibi herhangi biri olabilir, bu da anonimlik anlamına gelir.

Fakat bu anonimliğin korunması, hesabı kontrol eden kişinin elindedir.

Nasıl?

İzzeddin el-Kassam Tugayları örneğinde, fon toplamanın ilk aşaması merkezi bir kripto para borsası üzerinde bulunan bir hesap aracılığıyla gerçekleşmiştir.

Merkezi borsalarda açılan hesapları kullanıcılar kontrol edebilir, ancak bu hesabın asıl sahibi borsadır, çünkü borsa hesabın özel anahtarına sahiptir.

Alıcı hesaplar, temelde anonim olabilir, ancak bir borsa ile ilişkilendirilebilir, bu nedenle kimlik tespiti yapılabilir.

Anonimlik, bir beyanla da bozulabilir. Örneğin, hesabın sahibi, bu hesabın kendisine ait olduğunu açıkça beyan ederse, bu beyanı duyanlar karşısında anonimlik ortadan kalkabilir.

Bir hesabın anonimliği, hesabın gerçekleştirmiş olduğu blok zincir işlemleri incelenerek de bozulabilir.

Blok zincirler üzerinde yapılan bütün işlemler izlenebilir ve şeffaftır. Bir hesabın gerek alıcısı gerek göndericisi olduğu bütün kripto para aktarımları, etkileşime girdiği akıllı sözleşmeler, kısaca blok zincir üzerinde yaptığı her faaliyet herkes tarafından (istisnaları olmak kaydıyla) izlenebilir, görülebilir ve kontrol edilebilir.

Hesabın sahipleri anonim olsa da, anonim olmayan bazı hesaplar (özellikle borsa hesapları) ile yaptıkları işlemler hesabın sahibinin kimliğini ortaya çıkarabilir; ortaya çıkarmasa da en azından bazı kişi, kurum ve örgütler ile olan ilişiğini ortaya koyabilir.

Kripto paralar, terörizmin finansmanı için uygun bir araç olarak sıkça tartışılır. Ancak, izlenebilirlik ve şeffaflık özellikleri sayesinde terörizmin finansmanını önlemeye de yardımcı olabilirler.

Nakit para ile yapılan finansmanın izlenmesi zor olabilir. Paranın kimden kime, ne zaman ve ne kadar aktarıldığını belirlemek zorlayıcıdır.

Kripto paralarla yapılan işlemlerde ise herkes tarafından görülebilen bir blok zincirde kaydedilir. İşlem geçmişi, hangi adresten hangi adrese, ne zaman ve ne kadar aktarıldığını gösterir.

Bu şeffaflık, yetkililere terörizmin finansmanını izlemeleri ve tespit etmeleri için bir araç sağlar.

ANCAK GEREKLİ DENETİM, İSTİHBARAT VE SİBER GÜVENLİK MEKANİZMASININ VARLIĞININ TESİS EDİLMESİ KOŞULUYLA.

BU ÇIKARIMLARIN İSTİSNASI; GİZLİLİK ODAKLI KRİPTO PARALAR ve DİĞER GİZLİLİK YÖNTEMLERİ

Gizlilik odaklı kripto paralarda aksi seçilmemişse gönderenin ve alıcının adresleri ve gönderim miktarı gizlidir, diğer kişiler tarafından görülemez.

Yani izlenemez.

ÖRN: MONERO, DASH, Zcash (ZEC)

FATF de 2021 tarihli rehberinde gizlilik odaklı kripto paraları "anonimliği arttırıcı kripto para birimi [anonymityenhanced cryptocurrency (AEC)]" olarak adlandırmıştır. Bu doğrultuda FATF, AML/CFT'lerin (kara para aklamanın ve terörizmin finansmanının önlenmesi ile ilgili düzenlemeler) sanal varlık ve sanal varlık hizmeti sağlayıcıları hakkında "finansal eyleme konu olan sanal varlığın türüne bakılmaksızın" uygulanacağını belirtmekte, gizlilik odaklı kripto paraların da bu kapsama alınacağını ayrıca bildirmektedir.

MONERO

Monero gizlilik ve güvenlik odaklı bir kripto para birimidir.

Pek çok borsadan delist edilmiştir

Gönderici ve alıcı adresleri ile gönderilen miktarı kriptografi kullanara gizler. Bu nedenle takip edilemez, şeffaf değildir.

Kanunların yasakladığı eylemleri gerçekleştirmek isteyenlerin ilk tercihlerinden biridir.

AZTEC AĞI

Aztec ağı, terörizmin finansmanı amacıyla kullanıldığında oldukça elverişli bir araç olarak karşımıza çıkar.

Ağın özellikleri sayesinde, doğru bir şekilde kullanıldığında aktarılan fonların izlenmesi neredeyse imkânsız hale gelir.

Fon sağlamak isteyen bir kişi, zk.money adlı platform üzerinde bir hesap oluşturarak buraya kripto para transfer eder.

Terör örgütü veya finansman alıcısı da zk.money üzerinde kendi hesabını oluşturur.

Gönderen, bu hesap aracılığıyla fonu terör örgütünün zk.money hesabına aktarır.

Daha sonra terör örgütü bu fonu istediği bir Ethereum adresine çeker.

Bu işlem sonucunda, fonun kaynağı yani finansmanı sağlayan kişi bilinemez hale gelir.

Aynı şekilde, terör örgütünün hangi zk.money hesabını kontrol ettiği ve finansmanı sağlayan diğer kullanıcılar da tespit edilemez.

Bu nedenle, Aztec ağı bilinçli bir şekilde kullanıldığında terörizmin finansmanı için oldukça etkili bir araç haline gelebilir.

KÖPRÜLER

- Köprüler, farklı blok zincirlerini birbirine bağlayarak varlık aktarımını sağlayan araçlardır.
- Bu araçlar, kripto paraların farklı blok zincirlerine transfer edilmesine imkan tanır.

Önde Gelen Blok Zincir Köprüleri:

- Blok zincirler arası köprülerin çeşitli türleri bulunur.
- En bilinen köprüler arasında Wormhole, Multichain, Connext, Hop Protocol ve Orbiter yer alır.

Köprülerin Kullanım Alanları:

- Köprüler, Ethereum ve Ethereum Virtual Machine (EVM) uyumlu diğer ağlar arasında varlık transferlerini kolaylaştırır.
- Diğer kullanım alanları arasında Fantom, Smart Chain, Gnosis gibi ağlar ile ikinci katman çözümleri yer alır.

Varlık Taşıma İşlemi:

- Köprüler, bir hesap üzerinde bulunan bir kripto parayı, başka bir ağa aktarma işlemini sağlar.
- Kripto paranın sahibi taşıyan kişi olarak kalır, yani sahiplik değişmez.

Gönderici ve Alıcı Adresi:

Köprü kullanıcıları, alıcı adresini kendi adresinden farklı bir adres olarak seçebilir.

Bu durumda alıcı adrese taşınan kripto para, işlem incelendiğinde göndericiden değil, köprüden gelmiş olarak görünür.

Üçüncü Kişilerin Takibini Engelleme:

- Köprüler, fon transferlerini yaparken üçüncü kişiler tarafından izlenmesini engellemek isteyen kullanıcılar için etkili bir seçenek sunar.

İlk Para Arzı (İCO)

ICO Nedir?

ICO'lar, projelerin finansmanını kripto para toplamak suretiyle yatırımcılardan sağlayan bir kitle fonlaması yöntemidir.

Bu yöntem, çeşitli alanlarda blok zincir teknolojisi kullanan projelerin finansmanını kolaylaştırır.

ICO'ların Terörizmin Finansmanı Riski:

ICO'lar ve benzeri fon toplama uygulamaları, blok zincir üzerinde gerçekleştiğinden, terörizmin finansmanı amaçlı kullanılma riski taşır.

Avrupa Parlamentosu, ICO'ların terörizmin finansmanı amacıyla kullanılma potansiyelini göz önünde bulundurulması gerektiğini vurgular.

Regülasyon ve Düzenleyici Kurumlar:

Hollanda Finansal Piyasa Otoritesi AFM, ICO'ların terörizmin finansmanı için cazip bir araç olduğunu belirtir ve düzenlemelerin ivedi bir şekilde yapılması gerektiğini ifade eder.

Türkiye'de Sermaye Piyasası Kurulu, ICO'ların birçoğunun düzenleyici kurumların gözetim alanı dışında olduğunu, herhangi bir düzenleme ve gözetime tabi olmadıklarını belirtir.

Ayrıca ICO'ların yüksek riskli ve spekülatif yatırımlar olduğu konusunda yatırımcıları uyarır.

BORSALAR

Kripto Para Borsaları Genel Bakış:

Kripto para borsaları, kripto paraların alım ve satımının gerçekleştirildiği platformlardır.

Merkezi olanlar "CEX," merkeziyetsiz olanlar "DEX" olarak sınıflandırılır.

Merkezi Kripto Para Borsaları (CEX):

CEX'ler, özel bir şirket tarafından yönetilen ve alım-satım ile varlık transferlerini düzenleyen kripto para borsalarıdır.

Kullanıcılar, e-posta adresleri ve web hesapları gibi bilgilerle kayıt yaparak CEX'leri kullanabilirler.

CEX'ler, genellikle belirli bir ülkeye kayıtlıdır ve ulusal ve uluslararası düzenlemelere uymak zorundadır.

Bu nedenle kullanıcılardan KYC (Know Your Customer) ve AML (Anti-Money Laundering) prosedürlerini tamamlamalarını isterler.

Kripto para adresleri, kullanıcılar tarafından kullanılsa da, gizli anahtarlarını elinde bulunduran borsalar tarafından sahiplenilir.

Bu nedenle CEX'lerin güvenlik sorunları yaşaması durumunda, kullanıcılar kripto paralarına erişemeyebilirler.

En yaygın kullanılan CEX'ler arasında Binance, Coinbase, KuCoin, Kraken gibi kripto para borsaları yer alır.

Türkiye merkezli CEX'ler arasında Paribu, BTCTurk ve Binance TR gibi platformlar bulunur.

DEX Nedir?

DEX'ler, merkeziyetsiz kripto para alım-satım platformlarıdır.

Kullanıcılar, kendi kripto para cüzdanlarını DEX'lere bağlayarak işlem yaparlar.

DEX'ler, kullanıcıların tam kontrole sahip olduğu cüzdanlarla çalışırlar.

Kullanıcılar, istedikleri zaman DEX ile cüzdanlarını bağlayabilir veya bağlantıyı kesebilirler.

Terörizmin finansmanında, merkezi kripto para borsalarının kullanılabildiği bilinse de DEX'lerin kullanılması, kullanıcıların kripto paralarına daha fazla kontrol sağlar.

DEX'lerde kullanıcıların kendi cüzdanlarına sahip olmaları, finansman işlemlerinin daha gizli olmasını sağlar.

Terörizmin finansmanı amacıyla toplanan fonların nakit para olarak çekilmesi için kripto para borsaları da kullanılabilir.

Regülasyonlara uyumlu çalışan CEX'lerde gerçekleşen işlemlerin izlenmesi ve engellenmesi daha kolaydır.

CEX üzerinde gerçekleşen işlemler bazı yöntemlerle gizlenebilir.

Örneğin, emir defteri ince olan paritelerde fon transferi yapmak isteyen kullanıcılar, alış emirlerinin toplamından daha fazla miktarda satış yaparak işlemi gerçekleştirebilirler.

Emir defterinin ince olduğu paritelerde, kullanıcılar büyük miktarlarda işlem yapabilirler.

1 numaralı kullanıcı, terör örgütünü finanse etmek isteyen bir kişi olarak kabul edelim.

2 numaralı kullanıcı, bu fonu teslim almak isteyen bir başka kişidir.

2 numaralı kullanıcı, 0,1 USDT fiyatla 17.000 adet DEXE alım emri girer.

Bu işlem için elinde 1.700 USDT bulunması yeterlidir.

1 numaralı kullanıcı, 20.000 DEXE'yi market emri ile satar.

3.000 DEXE, diğer kullanıcıların emirlerini doldurur.

Geri kalan 17.000 DEXE, 2 numaralı kullanıcının alım emrini doldurur.

2 numaralı kullanıcı, 1.700 USDT harcayarak 49.300 USDT değerinde DEXE elde eder.

Bu işlem, bir dış gözlemci için sıradan bir borsa işlemi gibi görünür.

Merkezi bir kripto para borsasındaki işlemler, borsa platformu üzerinde gerçekleştiğinden, ağ üzerindeki inceleme bu tür işleme ulaşamaz.

Bu teknik, bir kripto para transferi gibi işlev görse de, ağdaki izlenemezlik nedeniyle kullanıcılar arasındaki işlemin detayları anlaşılamaz.

Karapara aklama: Terör örgütleri, kripto paralarla elde ettikleri gelirleri karapara aklamak için çeşitli yöntemler kullanmaktadır. Bunlardan bazıları şunlardır:

Tumbler (karıştırıcı) servisleri: Tumbler servisleri, kripto para transferlerinin izini kaybettirmek için birden çok sanal cüzdan arasında para akışı sağlayan servislerdir. Bu servisler, transfer edilen paraların kaynağını ve varış noktasını gizlemektedir.

Değişim (exchange) platformları: Değişim platformları, kripto paraları farklı para birimleri veya diğer kripto paralarla değiştirmeye yarayan platformlardır. Bu platformlar, terör örgütlerinin kripto paralarını farklı formlara dönüştürerek karapara aklamalarına imkân tanımaktadır.

Ön ödemeli kartlar: Ön ödemeli kartlar, kripto paraları fiziksel veya dijital kartlara yükleyerek harcanabilir hale getiren kartlardır. Bu kartlar, terör örgütlerinin kripto paralarını nakite çevirmelerine veya mal ve hizmet alımlarında kullanmalarına olanak sağlamaktadır.

Silah ve malzeme alımı: Terör örgütleri, kripto paralarla silah ve malzeme alımı yapmak için çeşitli kanallar kullanmaktadır. Bunlardan bazıları şunlardır:

Karanlık ağ (dark web): Karanlık ağ, internetin gizli ve erişimi zor olan bölümüdür. Karanlık ağ üzerinde, uyuşturucu, silah, sahte belge gibi yasadışı ürün ve hizmetler satılmaktadır. Terör örgütleri, karanlık ağ üzerinde kripto paralarla silah ve malzeme alımı yapabilmektedir.

Gizli anlaşmalar: Terör örgütleri, kripto paralarla silah ve malzeme alımı yapmak için gizli anlaşmalar yapabilmektedir. Bu anlaşmalar, terör örgütlerinin diğer suç örgütleri veya devlet destekli aktörlerle işbirliği yapmasını içerebilmektedir.