

**Kripto Dolandırıcılık ve Hukuki Düzenlemeler: Japonya Örneği^(*)***Crypto Fraud and Legal Regulations: The Case of Japan***Fazilat MİRAKHMEDOVA**

Öğretim Üyesi

*Alfraganus Üniversitesi Sosyal Bilimler Fakültesi***Filiz TEPECİK^(**)**

Doktor Öğretim Üyesi

*Anadolu Üniversitesi Hukuk Fakültesi**Mali Hukuk Anabilim Dalı***Anahtar Kelimeler**

Japonya Kripto Varlık
Düzenlemeleri,
Mt.Gox Borsa
Saldırısı,
Coincheck Borsa
Saldırısı,
Ödeme Hizmetleri
Yasası (PSA),
Japonya Sanal Varlık
Borsaları Birliği
(JVCEA),
Hukuk ve Ekonomi.

Öz

Bu çalışma kripto varlık düzenlemelerinin gelişimini kripto borsa saldırı ile birlikte incelemeyi amaçlamaktadır. Bu amaca ulaşmada kripto para piyasalarının öncü ülkelerinden Japonya'da yaşanan 2014 Mt.Gox'un iflası ve 2018 Coincheck kripto borsası saldırılarından yararlanılmıştır. Her iki olayda kripto varlık piyasalarının kritik güvenlik açıklarını ortaya koymuş ve önemli kayıplara neden olmuştur. Kripto varlıkların henüz gelişimlerini tamamlamamış olması, hukuki düzenlemeler için küresel kararlar alınması ve ülkelerin ortak hareket etmesini gerektirmesi, ülke düzeyinde regülasyonu zorlaştırmaktadır. Bütün ülkelerin benzer sorunlarla yüzleştiği bu dönemde Japonya'nın deneyimi yol gösterici olabilir. Makalede tartışıldığı gibi Japonya saldırılar sonrası Ödeme Hizmetleri Yasası'nda (*Payment Services Act-PSA*) değişiklikler yapmış, tasarruf sahiplerini korumaya çalışmış, Sanal ve Kripto Varlık Borsaları Birliği (*The Virtual and Crypto Asset Exchange Association-JVCEA*) gibi sektörün içinden düzenleyici kurumlar oluşturmuş ve küresel çok taraflı etkileri dikkate almıştır. Sonuç olarak saldırılar sonrası Japonya sanal varlık piyasaları üzerindeki denetimini giderek daha kapsamlı ve detaylı bir şekilde artırmıştır.

Keywords

Japan Crypto Asset
Regulations,
Mt.Gox Attack,
Coincheck Attack,
Payment Services Act,
Japan Virtual Asset
Exchanges Association
(JVCEA),
Law and Economics.

Abstract

This study aims to examine the development of cryptoasset regulations in the context of crypto exchange hacking. In achieving this goal, the 2014 Mt.Gox bankruptcy and the 2018 Coincheck crypto exchange attacks in Japan, the home of cryptocurrency markets, were utilised. Both incidents exposed critical vulnerabilities in the crypto asset market and caused significant losses. Crypto-assets have not yet completed their development and legal regulations require global decisions and joint action by countries. These two challenges complicate regulation at the country level. Japan's experience may serve as a valuable reference during this period in which countries across the globe encounter similar challenges. As elaborated in this study, after the attacks Japan has undertaken amendments to the Payment Services Act (PSA), implemented measures aimed at safeguarding investors, engaged industry self-regulatory organizations such as the Japan Virtual and Crypto Assets Exchange Association (JVCEA) and incorporated considerations of multilateral international dynamics into its regulatory framework. Consequently, Japan has increased its supervision of virtual asset markets in an increasingly comprehensive and detailed manner in the aftermath of the attacks.

(*) Araştırma Makalesi.
Hakem denetiminden geçmiştir.

Gönderim Tarihi: 17.04.2025, Kabul Tarihi: 30.06.2025.

(**) Sorumlu Yazar.



GİRİŞ

Paranın evrimi ve gelişimi, kripto paraların kullanıma dek tarihsel süreçte çeşitli aşamalardan geçmiştir. Değişim aracı olarak kullanılan değerli madenlerin yerini kağıt paraya bıraktığı, kağıt paraların ise günümüzde yerini elektronik ödeme yöntemlerine bıraktığı bu süreç, özellikle bilgi işlem teknolojilerindeki ilerlemelerle ivme kazanmıştır. Bu teknolojik gelişmeler, sanal paralar gibi yeni ödeme araçlarının ortaya çıkmasına zemin hazırlamıştır. Söz konusu araçlar, gönderici ve alıcı kimliklerinin anonim kalmasını sağlarken, aynı zamanda geleneksel para arz mekanizmasında merkezi bir aktör olan devleti sürecin dışına itmektedir.

Son yıllarda kripto ödeme araçları küresel düzeyde kayda değer bir ilgi görmektedir. 2008’de piyasaya girmelerinden bu yana, hukuki düzenlemelerin eksikliği pek çok problemin yaşanmasına neden olmuştur. Borsa saldırıları ve bunun sonuçları bu problemler arasında yer almaktadır.

Kripto değerler bilgi işlem teknoloji açısından yüksek bir alt yapı gerektirmektedir. Japonya yetiştirmiş insan gücü ve fiziksel alt yapısı ile bu ihtiyaçlara cevap vermiştir. Bu durumda onu kripto varlıklar konusunda öncü ülkelerden biri haline getirmiştir. 2008’de ilk oluşturulan kripto ödeme araçları ile başlayan gelişmenin her basamağında yer almasına rağmen Japonya kripto borsa saldırılarından kendisini koruyamamıştır. Borsa saldırıları sonucunda Japonya’nın yatırımcıları koruma, sektörü şekillendirme amacıyla aldığı tedbirler, kripto varlıkların gelişiminin yönünü de göstermektedir. Bu makale, kripto varlıkların gelişimi, saldırılar ile hukuki düzenlemelerin doğası arasındaki ilişkiyi analiz etmektedir. Bağlantılı olarak Japonya’nın deneyiminin diğer ülkelere ve kripto varlıkların gelişimine etkisi değerlendirilmektedir.

Bu makalenin ilk bölümünde, sanal varlıklar için finansal sistemin genel özellikleri ve makalenin genelinde kullanılacak anahtar kavramlar anlatılmaktadır. İkinci kısımda sistemin güvenlik riskleri, üçüncü kısımda Japonya’nın kripto endüstrisinin nitelikleri incelenmektedir. Dördüncü ve beşinci kısımda Mt.Gox ve Coincheck borsalarının tarihi, uğradıkları saldırı ve saldırı sonrası Japonya’nın hukuki tepkisi tartışılmaktadır. Son olarak kripto ödeme araçlarının dönüşümü, hukuki düzenlemeler değerlendirilmektedir.

I. SANAL VARLIKLAR İÇİN FİNANSAL SİSTEM

2025 yılı için ortak kullanılan ismiyle kripto varlıklar, *“bir merkez bankası ya da kamu otoritesi tarafından çıkarılmayan ya da itibari bir para birimine bağlı olmayan, ancak gerçek ya da tüzel kişiler tarafından bir ödeme aracı olarak kabul edilen ve elektronik olarak transfer edilebilen, saklanabilen ya da ticareti yapılabilen dijital değerlerdir”*¹.

İnternetin yaygınlaşması ile dijital devrim ya da teknoloji devrimi yaşandığı kabul edilen 1990’larda dijital para oluşturmak için birçok girişim olmuştur. Örneğin Flooz, Been² ve DigiCash gibi internet üzerinden alışveriş imkânı sağlayan ödeme sistemleri denenmiş ancak başarısız olmuştur. Bu sistemlerin en önemli özellikleri güvenilir üçüncü taraf yaklaşımını kullanmış olmasıdır. Başka bir ifade ile bu sistemlerin arkasında bir kamu otoritesi veya şirketler grubu vardır ve işlemleri doğrulayıp kolaylaştırmaktadırlar.

Bu denemelerin başarısızlığı, Satoshi Nakamoto’nun³ 2008’deki makalesine kadar, kamu otoritesi onayının olmadığı dijital bir ödeme sistemi oluşturmanın imkânsız olduğunu düşündürmüştür. 2008’de

¹ CHUEN, David Lee Kuo: “Introduction to Bitcoin”, *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*, Elsevier Science Publishing Co Inc, 2024, s. 3-28.

² Ayrıntılı okuma için BIELSKI, Lauren: “A New Shot for Micropayments”, *American Bankers Association (ABA) Banking Journal*, 2005, Cilt 97, Sayı 4, s. 58.

³ Makalenin yazarı olarak bir Japon ismi tercih edilmiş olmasına rağmen, Satoshi Nakamoto’nun gerçek bir kişi olup olmadığı bilinmemektedir. Bir kişi mi bir grup mu olduğu konusunda bile tartışma olmasına rağmen, bu ismin Bitcoin protokolünün geliştiricisi ve yazılımın ilk versiyonunun yaratıcısı olduğu kabul edilmektedir. 1975 doğumlu olduğunu ve Japonya’da yaşadığını belirttiği iddialarına

Nakamoto, e-posta listesi'nde “*Bitcoin: Eşler Arası Elektronik Nakit Sistemi*” başlıklı makalesini yayınlamıştır⁴. Bu da yeni kripto varlık tarihinin başlangıç noktası kabul edilebilir. Nakamoto sistemi şu sözlerle açıklamaktadır:

“Eşler arası (peer to peer, P2P)⁵ bir elektronik nakit sistemi, çevrimiçi ödemeleri bir tarafın diğerine doğrudan göndermesine olanak tanır ve bir finansal kuruma ihtiyaç duymaz. Dijital imzalar çözümün bir kısmını sağlasa da, güvenilir bir üçüncü taraf gereksinimi temel faydaları ortadan kaldırır. (Olası bir) çift harcama sorununu⁶, işlemleri sürekli bir iş kanıtı (proof of work) zincirine dönüştürerek zaman damgası atan eşler arası ağ kullanarak çözme öneriyoruz”⁷.

Görülebileceği gibi Nakamoto'nun asıl amacı, bankalar ve diğer finansal kurumlar gibi aracıları ortadan kaldıran ve iki taraf arasında doğrudan işlem yapılmasını sağlayan, tümüyle merkezi sistem dışı (devlete ya da herhangi bir onay kurumuna ihtiyaç duymayan) bir ödeme sistemi oluşturmaktır. Dolayısıyla da tanımladığı yapı, devlet vb kurumsal denetleyici, gözetleyici, kural koyucu üçüncü taraf rolü oynayan merkezi bir otoriteyi içermeyen elektronik nakit sistemidir. Bu önerilen yapıda bir merkez bankası ya da kamu otoritesine bağlı bir kurum olmadığı için, ödeme aracının değerinin korunması, servet olarak saklanması veya ödemelerde kullanılması, bu işlemlerin kayıtların tutulması ile ilgili konularda bir devlet güvenliği (garantis) de yoktur. Bu güvencenin yerini şifre (kripto)⁸ programı ve onun üzerinde işlem yapan herkesin birbirini gördüğü ve işlemi onayladığı bir sistem almaktadır. “*Temelde yapılan işlem ... genel seçimlere benzetilebilir. Siz kabine girer ve oy verip pusulanızı zarfın içerisine koyarsınız. Sandıktaki görevli, sizin zarfı oy kutusuna attığınızı yani oy verdiğinizi onaylar fakat kime oy verdiğinizi bilmez*”⁹. Birbirini görmeyenler (tanımayanlar) arası bir onay mekanizması işlediği için kör imza (*blind signature*) olarak isimlendirilen bu teknoloji bir mesajın, içeriği ve göndericisinin kimliği gizli tutularak imzalanmasını sağlayan bir kriptografik tekniktir ve devletsiz bir ödeme sisteminde onun onaylayıcı rolünü üstlenmektedir.

İşlemin göndereni ve alıcısı için farklı tarafların tanıklığının kayda alınması da blokzincir olarak isimlendirilmektedir. Söz konusu kişilerin merkezi bir kamu otoritesi ile ilişkisi olmadığı gibi, göndericinin, alıcının ya da şahitlik eden tarafların kimliklerinin bilinmesine de ihtiyaç duyulmaz, bu anonimlik olarak adlandırılmaktadır. Sisteme dahil olan çok sayıda kişi işlemin kaydını tutarak blok zincirlerin güvenli olarak işlem gerçekleştirebilmesine olanak vermektedir. Kripto varlıkların bankalar ya da hükümetler gibi işlemleri onaylayan merkezi kuruluşları olmadığı için kayıt tutucular ya da doğrulayıcılar (kripto madenciler) önemlidir. Muhasebe kaydının herkese açık olması bir aleniyet kazandırmaktadır ve bu açık blok zincirlere “merkeziyetsiz finans (*decentralized finance*)” veya “DeFi” adı verilmektedir¹⁰.

rağmen, bu bilgilerin doğruluğu şüpheli kabul edilmektedir. Nakamoto'nun kimliğiyle ilgili yapılan çeşitli araştırmalar ve girişimler şimdiye kadar başarılı olamamıştır (GORCHAKOVA, Tatyana Evgenievna: “On the Development of Crypto Industry of Japan”, *Vostochnaya Aziya: Fakty i Analitika*, 2022, Cilt 3, s. 76; BIELSKI, s. 58).

⁴ NAKAMOTO, Satoshi: *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008 (<https://bitcoin.org/bitcoin.pdf>, ET: 01.09.2025).

⁵ *Peer-to-peer* ya da P2P, iki veya daha fazla istemci arasında veri paylaşmak için kullanılan bir ağ protokolüdür. Peer eş, denk olarak Türkçeye çevrilebilir. Bu nedenle *peer to peer*, Türkçeye sıkça eşler arasında olarak çevrilmektedir. Bilgi Teknolojileri ve İletişim Kurumu, Bilgi ve İletişim Teknolojileri Terimleri Kılavuzu'nda denkler arası, uçtan uca olarak karşılık önerilmektedir. Bkz. <https://www.btk.gov.tr/kilavuzlar> (ET: 13.11.2024).

⁶ Hesaptaki mevcut paranın tekrar harcanması.

⁷ NAKAMOTO; MILUTINOVIĆ, Monia: “Cryptocurrency”, *EKOONOMIKA*, 2018, Cilt 64, Sayı 1, s. 95-104.

⁸ Kriptografi, bir bilginin istenmeyen kişilerce okunamayacak hâle dönüştürülmesinde yani şifrelenmesinde kullanılan matematiksel tekniklerdir. Bkz. KAYA, Elif Ebrin: *Kriptografi: Bilginin Anahtarı*, 2021 (<https://bilimgenc.tubitak.gov.tr/makale/kriptografi-bilginin-anahtari>, ET: 08.05.2025).

⁹ SOLAK, Ali Bertay: *Blind Signatures ve Gizlilik*, 2023 (<https://medium.com/@alibertay/b%C3%B6l%C3%BCm-14-blind-signatures-ve-gizlilik-e364ef070959>, ET: 20.04.2024).

¹⁰ NARAYANAN, Arvind / BONNEAU, Joseph / FELTEN, Edward / MILLER, Andrew / GOLDFEDER, Steven: “How Bitcoin Achieves Decentralization”, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, Princeton University Press, 2016, s. 27-51.

Kripto varlıkları almak, saklamak ve göndermek için kullanılan banka hesapları olan dijital cüzdanlara kullanıcının özel (*private*)¹¹ ve açık (*public*)¹² anahtarları aracılığı ile ulaşılmaktadır. Kripto varlıkları göndermek/almak için bir de adres oluşturulmaktadır. Adresler ile kişiler arasındaki bağlantı gizlenmekle birlikte işlemler izlenebilmekte ve kayıt altına alınabilmektedir¹³. Böylece kripto varlık sahipleri sadece istedikleri kişilerle adreslerini paylaşmakta, hesaplarındaki varlıkların giriş ve çıkışlarını kontrol edebilmektedir. Kişiler gizli olmakla birlikte el değiştiren finansal varlıklar takip edilebilmektedir. Cüzdanlar sadece kişisel belleklerde saklanabileceği gibi, saklama/koruma/dönüştürme hizmeti sunan bir aracı kurumda da çevrimiçi (*sıcak depolama*) veya çevrimdışı (*soğuk depolama*)¹⁴ olarak saklanabilmektedir.

II. SİSTEMİN GÜVENLİK RİSKLERİ

Kriptografik varlıklar, ödeme araçları olarak ortaya çıktıklarında güvenilir ve manipülasyona kapalı birer para birimi olmayı vadetmiş; savunucuları da fiat paranın (itibari veya ulusal kağıt para da denilebilir) yerine geçerek dünya çapında ilk özgür ve istikrarlı para birimi olacağını iddia etmişlerdir¹⁵. Bununla birlikte kripto varlıklar kullandıkları teknolojik altyapıya rağmen veya bu altyapı nedeniyle bazı sorunlarla karşılaşmaktadırlar.

Örneğin bu altyapının kişilerin isimlerini gizlemesi, diğer bir ifade ile anonimliği, finansal hareketlerin kişilerle ilişkilendirilmesini engellemektedir. Bu da fiat paralar için kullanılan normal bankacılık sistemlerinde kaynağı şaibeli olduğu için aktarılmasına izin verilmeyecek finansal hareketlere izin vermektedir. Ayrıca standart finansal sistemde sıkça görülen dolandırıcılıklar (ponzi planları¹⁶, menkul kıymet dolandırıcılıkları, kimlik hırsızları, içeriden bilgi ticareti¹⁷ vb) yanı sıra bilgi işlem teknolojilerinden kaynaklanan sorunların da (kötü amaçlı yazılımlar, kripto korsanlıkları, bilişim dolandırıcılıkları vb.) oluşmasına imkân vermektedir. Kimliklerin gizlenmesi nedeniyle örneğin kimlik hırsızları ile şifreler çalınmış ve takiben hesaplar boşatılmışsa, herhangi bir soruşturma ya da yargılama basamağında, hırsızlığın kanıtlanması, hırsızların kimliklerinin belirlenmesi zor bir süreç dönüşmektedir. Hırsızlar ya da dolandırıcılar için bir görünmezlik hırkası oluşmaktadır.

Bu sorunlar nedeniyle birçok ülke ve uluslararası kuruluş, kripto varlıklara dair riskleri yönetebilmek adına farklı hukuki düzenleme girişimlerinde bulunmaktadır¹⁸. Normal bankacılık sisteminde, kara para aklama, terörizmin finansmanı, siber saldırılar ya da başka finansal suçlara aracılık etme riski taşıyan finansal varlıklar, uluslararası anlaşmalarla oluşturulan küresel kamu düzeni tarafından kontrol edilmektedir. Fakat kripto varlıklar için oluşturulan küresel ortamda bu tür hukuki düzenlemeler henüz yoktur.

¹¹ Özel anahtarlar, genellikle rastgele sayısal verilerden oluşturulan ve genellikle 256 bit uzunluğunda olan karmaşık verilerdir. Bu anahtarlar genellikle güvenli bir rastgele sayı üretici kullanılarak oluşturulur. Oluşturulan bu anahtar, cüzdan sahibinin gizli anahtarı olarak saklanır ve güvenli bir şekilde korunması kişilerin sorumluluğundadır (DİRİ, Nurcan: *Blokzincir Uygulamasında Kişisel Verilerin Tutulması*, Yüksek Lisans Tezi, Marmara Üniversitesi Fen Bilimleri Enstitüsü, İstanbul, 2022, s. 12).

¹² Özel anahtarlarla ilişkili olan açık anahtarlar, genellikle özel anahtarın bir matematiksel türevidir ve kriptografik işlemlerle türetilir. Bu işlem, genellikle bir karma fonksiyonu kullanılarak gerçekleştirilir (DİRİ, s. 12-19).

¹³ DİRİ, s. 12-19.

¹⁴ Çevrimdışı (soğuk) saklama, bir kasada kilitli fiziksel bir cüzdan veya bir kişinin bilgisayarındaki bir dosyada yerel olarak saklanan bir anahtar içerebilir. Çevrim içi saklama internet aracılığı ile ulaşılabilen bir depolama olduğu anlamına gelir. Soğuk saklama genellikle daha güvenli kabul edilmektedir.

¹⁵ MILUTINOVIĆ, s. 99.

¹⁶ Ponzi şemaları ve yüksek getirili yatırım programları, yatırımlar karşılığında olağanüstü faiz oranlarının vaat edildiği Charles Ponzi'nin dolandırıcılık tekniğidir. Bu sistemde, yeni katılanların yatırdığı miktarlar, eskilerin getirilerini ödemek için kullanılır. Yeni kurban bulmak mümkün olmadığında sistem çöker. Diğer dolandırıcılıklarla ilgili ayrıntılı bilgi için TROZZE, Arianna / KAMPS, Josh / AKAR-TUNA, Eray Arda / HETZEL, Florian J. / KLEINBERG, Bennett / DAVIES, Toby / JOHNSON, Shane D: "Cryptocurrencies and Future Financial Crime", *Crime Science*, 2022, Cilt 11, Sayı 1, s.1-35.

¹⁷ Güvenlik görevini veya başka bir güven ve itimat ilişkisini ihlal ederek, menkul kıymetle ilgili maddi, kamuya açık olmayan bilgilere dayanarak bir menkul kıymetin satın alınması veya satılması olarak tanımlanabilir. Ayrıntılı bilgi için TROZZE vd, s. 29.

¹⁸ KREMINSKYI, Oleh / KUZMENKO, Olena / ANTONIUK, Anastasiia / SMAHLO, Olha: "International Cooperation in the Investigation of Economic Crimes Related to Cryptocurrency Circulation", *Studies of Applied Economics (Estudios de Economic Aplicada)*, 2021, Cilt 39, Sayı 6, s. 1-13.

Peters, Chappelle ve Panayi¹⁹ sistemin güvenlik açıkları ve oluşan riskler üzerine bir çalışma yapmışlardır. Peters vd. çalışmasında kripto varlıklara izin veren Nakamoto sisteminin özelliklerinden örneğin DeFi yönetiminin fiyat manipülasyonlarına ve oynaklığa²⁰; anonimliğin kara para aklama ve dolandırıcılığa; özel anahtarların dolandırıcılığa; işlemlerin geri alınamamasının kayıpların ağırlaşmasına neden olduğu belirtilmektedir.

Bhaskar ve Chuen²¹, dijital varlıkların değerlerinin artmasıyla birlikte cüzdanlardan hırsızlık amacıyla tasarlanmış virüslerin sayısının arttığını, 2024’de bu amaçla yaklaşık 150 kötü amaçlı yazılımın bulunduğunu ve bunların 100’den fazlasının son bir yıl içinde programlandığını iddia etmektedirler. Bhaskar ve Chuen’e göre “Başlangıçta, internet suçluları Bitcoin madenciliği yapmak için Botnet adı verilen kötü amaçlı yazılımlardan etkilenen büyük bilgisayar ağlarına yoğunlaştı. Madenciliğin zorluğu arttıkça, daha az kârlı olduğu ortaya çıktı ve cüzdanlardan ve borsalardan bitcoin çalmaya odaklandılar”²².

Benzer şekilde Charoenwong ve Bernardi, 2011-2021 arasında gerçekleşen büyük kripto suçları üzerine yaptıkları çalışmalarında, suçlara ilişkin üç ana nedeni aşağıdaki gibi tanımlamaktadırlar²³:

- İnsan Hatası Üzerine Kurulu Saldırıları (*Human Error Hack*): Bu tür bir ‘saldırı’ genellikle fidye e-postaları veya kötü amaçlı yazılımların, bilgisayarlar sistemlerine, e-postalara gönderilmesini ile başlamaktadır. Bu elektronik postalar, kişilere ait özel anahtarların elde edilmesine olanak tanıyan virüs programları içermektedir. Bu anahtarların elde edilmesi ile hesaplar ulaşılabilir hale gelmektedir.
- Güvenlik İhlali (*Security Breach*): Genellikle kripto alım satım ya da saklama hizmet sunucularının ya da benzeri kurumların bilgisayarlarında ya da programlarında güvenlik açığının bulunması nedeniyle bir suça imkân vermesi olarak tanımlanmaktadır. Örneğin borsaların sistemlerindeki bir boşluk, sistemin altyapısındaki bir kısmın pratikte korumasız hale gelmesine ve hesapların bir grubuna veya tamamına ulaşılarak hırsızlık yapılmasına neden olabilmektedir.
- Kurumsal Sorunlar veya Vekil Sorunu (*Agency Problem*): Son tür korsan saldırıları, ihmalkârlık veya yetersiz güvenlik önlemleri nedeniyle değil, daha çok içeriden bir bilgi kaynağı nedeniyle gerçekleşmektedir. Bu tür güvenlik sorununda, örneğin borsanın kurucuları müşterilerin fonlarını barındıran soğuk cüzdanları yanlarına alarak aniden kaybolmakta ya da korsanlarla birlikte çalışarak uzun bir süre boyunca cüzdanlardaki fonları yavaşça silerek hesapları boşaltmaktadırlar. Bu tür hırsızlık veya dolandırıcılık olayında, çalışanlar/yöneticiler sistemi iyi bildikleri için, hırsızlığın belirlenmesi zaman almakta, fonların kaybı belirlense bile yapanın kimliğinin tespiti zor olmaktadır.

Charoenwong ve Bernardi’nin çalışmasına göre 2011-2021 arasında yapılan büyük kripto para hırsızlıkları en çok insan hatasından kaynaklanmıştır (30 olaydan 20’si)²⁴. Büyük dolandırıcılıklar genellikle kimlik avlarıyla başlamaktadır.

¹⁹ PETERS, Gareth W. / CHAPPELLE, Ariane / PANAYI, Efsthathios: “Opening Discussion on Banking Sector Risk Exposures and Vulnerabilities from Virtual Currencies: An Operational Risk Perspective”, *Journal of Banking Regulation*, 2016, Cilt 17, Sayı 4, s. 239-272.

²⁰ Merkeziyetsiz yönetimde borsaların gerçekten ne kadar hesaba sahip olduğu, hesapların gerçek kaç kişiye dayandığı belli olmamaktadır. Borsalar az sayıda kişiye dayanan çok sayıda hesapla alım işlemleri yaparak, varlıkların değerlerini yükseltebilmekte ya da satarak fiyat düşüşlerine neden olabilmektedirler. Az sayıda hesapla fiyatın yönlendirilmesi manipülasyon, fiyatın hızlı düşüş ve yükselişleri volatilite olarak değerlendirilmektedir. PETERS / CHAPPELLE / PANAYI, s. 250-255.

²¹ BHASKAR, Nirupama Devi / CHUEN, David Lee Kuo: “Bitcoin Exchanges”, (Ed.) CHUEN David Lee Kuo: *Handbook of Digital Currency*, 2015, s. 559-573.

²² BHASKAR / CHUEN, 560-566.

²³ CHAROENWONG, Ben / BERNARDI, Mario: *A Decade of Cryptocurrency ‘Hacks’: 2011-2021*, 2021 (<https://ssrn.com/abstract=3944435> veya <http://dx.doi.org/10.2139/ssrn.3944435>, ET: 16.04.2024).

²⁴ Büyük hırsızlıklar için bu çalışmada IV. Mt.Gox Borsası ve Borsaya Saldırı başlığın altında kullanılan Tablo 1’e bakılabilir.

Görülebileceği gibi sistem pek çok noktada güvenlik riski taşımaktadır. Makalenin geri kalanında anlatılacak olan Japonya Mt.Gox ve Coincheck kripto varlık borsası saldırıları güvenlik risklerin büyük kayıplara neden olduğu örnekler arasında yer almaktadır. Makalede güvenlik sorunlarının nasıl oluştuğu, kayıplar ve Japonya'nın verdiği tepki incelenmektedir.

III. JAPONYA KRİPTO ENDÜSTRİSİNİN GELİŞİMİ

Japon kripto endüstrisi 2008'e Nakamoto'nun kripto para için ilk açıklamalarını yaptığı tarihe kadar geri götürülebilir. Daha önce bahsedildiği gibi, Nakamoto'nun gerçekten bir kişi mi, grup mu olduğu tartışmalı olmakla birlikte²⁵, vitrin ismi olarak bir Japon isminin tercih edilmesi de Japonya ve bilgisayar teknolojileri arasındaki paralellik algıyı artırmaktadır. Nakamoto 2008'de teorik altyapısını yayınladığı fikrini pratiğe geçirmek için 2009'da Bitcoin adını verdiği para için sanal bir cüzdanın ilk bilgisayar programı versiyonunu yayımlamış, başlangıç sermaye olan bir cüzdan oluşturmuş ve Bitcoin ağını başlatmıştır. Nisan 2011'e kadar da Martti Malmi ile dijital ödeme yöntemi için programı geliştirmeye devam etmiştir. 2011'den sonra Nakamoto Bitcoin üzerine yazmayı bırakmıştır ve bu tarihten sonra internet üzerinde herhangi bir gönderi paylaşmamıştır. Bununla birlikte Nakamoto, Japonya'nın adının kripto para gelişmeleri ile birlikte düşünülmesine neden olmaktadır. Malmi ve Nakamoto tarafından geliştirilen popüler internet hizmeti Bitcoin.org'un merkezi de Japonya'da bulunmaktadır²⁶.

Japonya'nın bilgisayar teknolojisi ve bilgisayar oyunlarındaki öncü rolünün de Japon kripto endüstrisinin gelişmesinde önemli bir rolü söz konusudur. Bir sonraki kısımda Mt.Gox borsasının geçmişinde de görülebileceği gibi, bilgisayar oyunları, oyunlarda kullanılan kartlar, bu kartların sanal değerleri ve seyrek olan kartların daha sık olanlarla değiştirilmesi (ticareti) gibi konular, kripto paralarının gelişiminde önemli basamaklardan biri olarak kabul edilmektedir. Bilgisayar oyunları konusunda da Japonya 1970'lerdeki Nintendo ve Sega firmalarına kadar götürülebilecek bir tarihe sahiptir²⁷. Bilgisayar oyunları konusundaki bilgi birikimi, yetişmiş insan gücü Japonya'nın kripto varlıkların oluşturulmasında maliyeti düşük bir altyapı sunmasını sağlamıştır. 2010 yılında, dünyanın ilk dijital varlık borsalarından biri olan Mt.Gox da bir oyun web sayfası başlangıçlı olarak Japonya'da kurulmuştur.



Resim 1. Nintendo firmasının oyunlarından²⁸

Ayrıca Japonya'da kripto endüstrisinin gelişimi Japonya'nın genel ekonomik durumuyla da yakından bağlantılıdır. Japon ekonomisi, 1997-2015 yılları arasında 18 yıl boyunca kronik deflasyon yaşamıştır. Bu süre zarfında ülke, Gayri Safi Yurtiçi Hasıla (GSYİH) ve uluslararası ticaret açısından ABD'den sonra ikinci en büyük güç olma konumunu kaybetmiştir²⁹. Bu nedenle Japonya, yeni bir sanayi politikası uygulamayı hedeflemiştir. Kripto ekonomi, bu yeni politikanın önemli ayaklarından

²⁵ GORCHAKOVA, s. 76; BIELSKI, s. 58.

²⁶ POPPER, Nathaniel: *Digital Gold: The Untold Story of Bitcoin*, Penguin, Londra, 2015, s. 69.

²⁷ SHOCKVOICE: *Bilgisayar Oyunlarının İnanılmaz Evrimi Amiga'dan VR'a*, 2022 (<https://www.youtube.com/watch?v=GQizi9szb44>, ET: 18.01.2025); ŞAAN, Tayfun / TİLTAY, Muhammet Ali / İŞLEK, Mahmut Sami: "1980-2000 Yılları Arasındaki Video Oyun Sektörünün İncelemesi: Nintendo ve Sega Örneği", *Anadolu Üniversitesi Sosyal Bilimler Dergisi*, 2022, Cilt 22, Sayı 3, s. 911-930.

²⁸ Resimler Super Mario Bros sayfasından alınmıştır: <https://supermarioplay.com/tr/fullscreen> (ET: 20.05.2025).

²⁹ ЛЕВАШЕНКО, Антонина / ЕРМОХИН, Иван / КОВАЛЬ, Александра: "Перспективы Правового Регулирования Криптоэкономики И ICO В России И Других Странах", *Экономическая Политика*, 2019, Cilt 14, Sayı 5, s. 86.

biri olarak görülmektedir ve bu durum Japonya'nın Bitcoin'e yönelik ilk hukuki düzenlemeleri yapan ülkeler arasında olmasının nedenlerinden biri olarak değerlendirilmektedir³⁰.

Ayrıca bölge ülkelerinden Çin, 2013 yılında kripto varlıklarının değişimini sınırlayan bir dizi yasa çıkarmıştır³¹. Japonya'daki uygun alt yapı ve henüz sınırlayıcı bir düzenlemenin olmayışı Çin borsalarından çekilen kripto varlıkların Japonya'ya kaymasına ve mevcut yapıyı hızlandırmasına neden olmuştur³².

IV. MT.GOX BORSASI VE BORSAYA SALDIRI

Shibuya (Tokyo) merkezli Mt.Gox kripto para borsası, 2010 yılında faaliyete geçmiştir. Mt.Gox.com alan adı, aslında "Magic: The Gathering Online Exchange" ifadesinin kısaltmasıdır. Kurucusu Jed McCaleb³³, popüler bir fantezi kart oyunu olan "Magic: The Gathering" hayranlarının, oyunun kartlarının hisse senetleri gibi değiş tokuşunun yapabileceği bir platform olarak oluşturmayı hedeflemiştir³⁴. Bu amaçla 2006 yılında web sitesinin ilk versiyonu kurulmuştur. Bununla birlikte Bitcoin'deki gelişmelerin ardından, McCaleb, Mt.Gox alan adını kripto varlık borsası olarak kullanmaya karar vermiştir. Borsa 2014 yılına kadar son derece hızlı bir gelişim göstermiştir. Ocak 2014'e gelindiğinde Mt.Gox, dünyanın en büyük Bitcoin borsasıdır ve işlemlerin yaklaşık %70'ini gerçekleştirmektedir.



Resim 2. mtgox.com: Magic: The Gathering Online eXchange³⁵

Burada değerlendirilecek borsanın iflasına neden olan 2014 saldırısı olmasına rağmen, ilk sorun 19 Haziran 2011'de gerçekleşmiştir. Bir bilgisayar korsanı (*hacker*), Mt.Gox denetçisinin bilgisayarına erişerek kimlik bilgilerini ele geçirmiş ve bu bilgileri kullanarak sonrakine kıyasla küçük bir miktar Bitcoin'i kendi hesabına aktarmıştır³⁶. Fakat asıl hırsızlık müşteri özel anahtarlarının elde edilmiş olmasıdır. 2014'de müşteri özel anahtarları kullanılarak hesaplara girilmiş, hesaplar boşatılırken ve hesap bilgileri değiştirilmiştir. Mt.Gox bu bilgiye erişildiği bilmediği ya da anlamadığı için, 2011-2014 arası yapılan işlemlerin değiştirildiğini de fark etmemiştir.

Tablo 1, Charoenwong ve Bernardi çalışmasından alınmıştır. Tabloda büyük dolandırıcılık olaylarından bazıları görülmektedir. Tabloya göre ilk saldırıda 2643 Bitcoin, ikincinde 850000 Bitcoin çalınmıştır ve o tarihteki değeri sırasıyla yaklaşık 30 bin ve 460 bin dolar civarındadır. Tablo da her iki saldırının da güvenlik açığı olarak sınıflandığı görülmektedir³⁷. 2011 yılındaki ilk olaydan sonra borsanın kurucusu McCaleb, Japonya'da yaşayan Fransız yazılımcı Mark Karpelès'e şirketini satarken

³⁰ GORCHAKOVA, s. 77.

³¹ CHEUNG, Adrian (Wai-Kong) / ROCA, Eduardo / SU, Jen-Je: "Crypto-currency Bubbles: An Application of the Phillips-Shi-Yu (2013) Methodology on Mt. Gox Bitcoin Prices", *Applied Economics*, 2015, Cilt 47, Sayı 23, s. 2348-2358.

³² CHEUNG / ROCA / SU, s. 2348-2358.

³³ McCaleb, büyük hacimli materyalleri uçan uça aktarmaya yarayan eşler arası (*peer-to-peer*, *P2P*) eDonkey network uygulamasını, (XRPL, XRP olarak bilinen yerel kripto para birimlerini, token'ları, sık uçuş milleri veya mobil dakikalar gibi diğer değer birimlerini birbirine dönüştürmekte kullanılmak üzere oluşturulmuş) Ripple platformunu da geliştirmişti.

³⁴ SEMENOVA, Ekaterina Vyacheslavovna / MAKAREVICH, Marina Leonidovna: "Analiz Pravovogo Regulirovaniya Kriptovalyuty v Otdel'nikh Stranakh (na primere Yaponii, SShA i Rossii)", *Innovatsionnaya Ekonomika: Perspektivy Razvitiya i Sovershenstvovaniya*, 2017, Cilt 8, Sayı 26, s. 144.

³⁵ Resim, WIKIPEDIA: *Mt. Gox* (https://en.wikipedia.org/wiki/Mt._Gox, ET: 12.09.2024) sayfasından alınmıştır.

³⁶ ISHIKAWA, Mai: "Designing Virtual Currency Regulation in Japan: Lessons from the MTGox Case", *Journal of Financial Regulation*, 2017, Cilt 3, Sayı 1, s. 126.

³⁷ Reuters kaybın 480 milyon dolar, Fox Busines 500 milyon dolar olduğunu iddia etmektedir (REUTERS: *Bitcoin Exchange Mt.Gox Files for Bankruptcy, Blames Hackers for Losses*, 2014 (<https://www.techcircle.in/2014/02/28/bitcoin-exchange-mt-gox-files-for-bankruptcy-blames-hackers-for-losses>, ET: 14.11.2014); EGAN, Matt: *Bitcoin Exchange Mt. Gox Files for Bankruptcy After Losing Nearly \$500M*, 2014 (https://people.duke.edu/~charvey/Media/2014/FBN_February_28_2014.pdf, ET: 14.11.2024).

“Mt.Gox’un potansiyelini gerçekten gerçekleştirebilmek için şu anda sahip olduğum zamandan daha fazlasına ihtiyaç var. Bu yüzden bu siteyi bir üst seviyeye taşıyabilecek birine devretmeye karar verdim”³⁸ demektedir. Ancak, mahkemede sonradan ortaya çıkan bir e-postaya göre, McCaleb Mt.Gox borsasının zaten saldırıya uğradığını ve 80 bin BTC’lik bir açığın söz konusu olduğunu bilmektedir. O dönemde yaklaşık 60 bin dolar değerinde olan bu kayıp, büyük bir felaket olarak da görülmemiştir. Fakat Bitcoin fiyatları arttıkça bu açığı kapatmak her geçen gün daha zor hale gelmiştir³⁹.

Tarih	Olay	Çalınan miktar	BTC olarak değeri	USD olarak değeri	Dolandırıcılığın Tipi
Haziran 2011	Mt.Gox özel anahtar hacklenmesi (Japonya merkezli)	2 643 BTC	2 643	30 bin	Güvenlik ihlali
Mart 2014	Mt.Gox işlemlerinin değiştirilmesi	850 000 BTC	850 000	460 milyon	Güvenlik ihlali
Ocak 2018	Coincheck virüs hack (Japonya merkezli)	523 000 000 NEM	47 711	533 milyon	İnsan hatası
Aralık 2018	QuadrigaCX hırsızlığı (Kanada merkezli)	26 350 BTC	26 350	130 milyon	Vekil problemi
Eylül 2020	KuCoin security ihlali (Seyşeller merkezli)	BTC ve ETH	26 137	281 milyon	Güvenlik ihlali
Haziran 2021	Africrypt hack (Güney Afrika merkezli)	69 000 BTC	69 000	3,6 milyar	Vekil problemi
Ağustos 2021	Poly Network Hack	USDC, BTC ve ETH	12 964	600 milyon	Güvenlik ihlali

Tablo 1. En Büyük Dolandırıcılıklardan⁴⁰

Dolayısıyla açığın büyümesinde hem müşteri sayındaki hem de BTC değerindeki artışın etkisi söz konusudur. Bitcoin fiyatı Nisan 2013’te 1 dolardan haziran ayında 30 dolara ulaşmış, Mt.Gox’taki hesap sayısı da 6 binden 60 bine yükselmiştir. 2013’ün Nisan’ından 2014’e kadar Mt.Gox, dünya çapında Bitcoin ticaretinin %70’ini yöneten en büyük Bitcoin aracı kurumuna dönüşmüş, Bitcoin fiyatı da hızla artarak 1.200 doları geçmiştir⁴¹.

Sorun 2014 yılı başlarında, müşteriler, para çekme taleplerinde bulunduklarını ama paralarını alamadıklarını bildirinceye kadar açığa çıkmamıştır. Bunun üzerine şirket, yıllarca fark edilmeden 750 bin BTC’lik müşteri Bitcoin’in çalındığını ve borsanın sermayesi olarak düşünülebilecek kendi BTC’lerinden de yaklaşık 100 bin BTC kaybettiğini açıklamıştır.

³⁸ Detaylı okuma için NEFTURE SECURITY: *Mt. Gox Unveiled: The Real Story a Decade After the Collapse*, 2024 (<https://medium.com/coinmonks/mt-gox-unveiled-the-real-story-a-decade-after-the-collapse-84323be2f930>, ET: 20.02.2025)

³⁹ GORCHAKOVA, s. 75.

⁴⁰ Tablo 1, CHAROENWONG / BERNARDI, s. 4-5 çalışmasında bulunan tablonun bir kısmı olarak alınmış ve yazarlar tarafından Türkçeye çevrilmiştir.

⁴¹ MCMILLAN, Robert: *The Inside Story of Mt.Gox, Bitcoin’s \$460 Million Disaster*, 2014 (<https://www.wired.com/2014/03/bitcoin-exchange/>, ET: 14.11.2024); RASTOGI, Neha / BUDHIRAJA, Ishan / AHMAD, Shahnawaz: *Cyber Attacks on Blockchain & its Prevention*, 2024 (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4936255#, ET: 13.06.2025).

Ağustos 2015'te Japon polisi, Karpelès'i dolandırıcılık, zimmetine para geçirme ve Mt.Gox bilgisayar sistemini manipüle ederek bir hesapta bakiye artırma suçlarından tutuklamıştır. Gerçekten ne olduğunun anlaşılması ve tutuklama sonrası yargılama süreci uzun sürmüştür. Yargılama sırasında, Mt.Gox, eski formatta dijital cüzdanlarda 200 bin BTC bulduklarını açıklamış, şirket iflas koruması altındayken yapılan farklı açıklamalar, finansal zorlukların yanı sıra alacaklıların paralarını geri alma sürecini de etkilemiştir⁴². 2018 Haziran'ında Tokyo Bölge Mahkemesi, borsayı iflastan tasfiye sürecine taşımıştır. Bu gelişme, eski Mt.Gox kullanıcılarına en az 1 milyar dolar değerinde kripto varlık geri ödemesinin yapılmasının önünü açmıştır⁴³. Karpelès'de zimmete para geçirme de dahil olmak üzere diğer suçlamalardan aklanırken sadece şirket kayıtlarını tahrif etmekten suçlu bulunmuş ve 2,5 yıl ertelenmiş hapis cezası almıştır⁴⁴.

Mt.Gox iflasına neden olan bu saldırılarının, bütün kayıtlar sadece blokzincir üzerinde yani bilgisayar programları üzerinde olduğu için hem anlaşılması hem de bir mahkemede mağdur, fail sürecinin gerektirdiği kanıtları üretmesi çeşitli zorluklar içermektedir. Örneğin mağduriyet durumunda bir cüzdan sahibinin blokzincirde kaydı bulunan bir işlemi kendisinin yapmadığının ya da onay vermediğinin, kendi özel anahtarı kullanılmışsa, anahtarın elde edilmesinde kendi kusurunun olmadığı belgelenmesi gerekmektedir. Failler açısından da benzer sorunlar söz konusudur: Cüzdan değerlerinin aktarıldığı hesapların kimlere ait olduğu belirlenebilir mi? Bir sonraki adım işlemlerin dünyanın herhangi bir yerinden yapılması mümkün olduğu için faillerin kimlikleri belirlenebilirse, hırsızlık konusu varlıkların geri alınıp alınamayacağı sorunu içermektedir. Anonimlik hem fail hem de mağdurlar için bir görünmezlik kalkını yaratmaktadır. Dolayısıyla Mt.Gox Borsasının iflası ile sonuçlanan mahkemenin, bilgisayar ve sanal dünyaya ilişkin uzmanlık bilgisine sahip kişilerle birlikte yürütülmesi gerekmiştir ve mağduriyetlerin belirlenmesi sonrasında ise, faillerin tespiti mümkün olmamış, borsanın sorumluluğu konusunda ise aracı kurumun sermayesi mağdurların kayıplarının tamamının karşılanmasını sağlamamıştır⁴⁵.

Fakat olayın asıl etkisi, Japon kripto varlık sektörü üzerinde olmuştur. Kripto piyasaların kayıplarının telafisi oldukça tartışmalı görünmektedir. Bu durum Japonya para otoritesini kripto ekosistemindeki zayıf noktaların giderilmesi için önlemler almaya yönlendirmiştir.

V. MT.GOX SONRASI JAPONYA'NIN DÜZENLEYİCİ TEPKİSİ

Mt.Gox saldırısı sonrası, Mart 2014'te Senatör Tsutomu Okubo hükümete Bitcoin hakkında 2 soru önergesi vermiştir. Hükümet bu sorulara cevap verirken, kripto varlıklar hakkındaki hukuki mevcut durumu ortaya koymuştur. e sunulan yazılı cevapta, Bitcoin'i yasal ödeme aracı olarak tanıyan yabancı bir ülke olmadığı sürece, Bitcoin'i yabancı ulusal bir para birimi olarak tanımlanamayacağı; (1981 tarihli ve 59 sayılı) Bankacılık Kanunu'nda hırsızlığa konu olan kripto varlık Bitcoin'i yasaklayan bir madde bulunmadığı ve Bitcoin borsaları için izin belgesini gerektiren bir hukuku düzenlemenin olmadığı belirtilmiştir⁴⁶.

Saldırı sonrası boşaltılan hesapların takip edilememesi konusunda verilen diğer soru önergesine cevapta ise, (2007 tarihli ve 22 sayılı) Suç Gelirlerinin Aktarılmasının Önlenmesi Hakkında Kanun (The Act on Prevention of Transfer of Criminal Proceeds, Act No.22 of 2007) gereğince, Bitcoin kul-

⁴² FURUKAWA, Yuki: *Former Mt. Gox CEO Mark Karpeles Gets Suspended Jail Term*, 2019 (<https://www.bloomberg.com/news/articles/2019-03-15/former-bitcoin-baron-mark-karpeles-gets-suspended-jail-term>, E.T: 14.11.2024); BEATTIE, Elizabeth: *The Unsinkable Mark Karpeles is Willing to Give Tokyo Another Shot*, 2024 (<https://www.japantimes.co.jp/business/2024/10/21/markets/karpeles-japan-return/>, E.T: 20.02.2024).

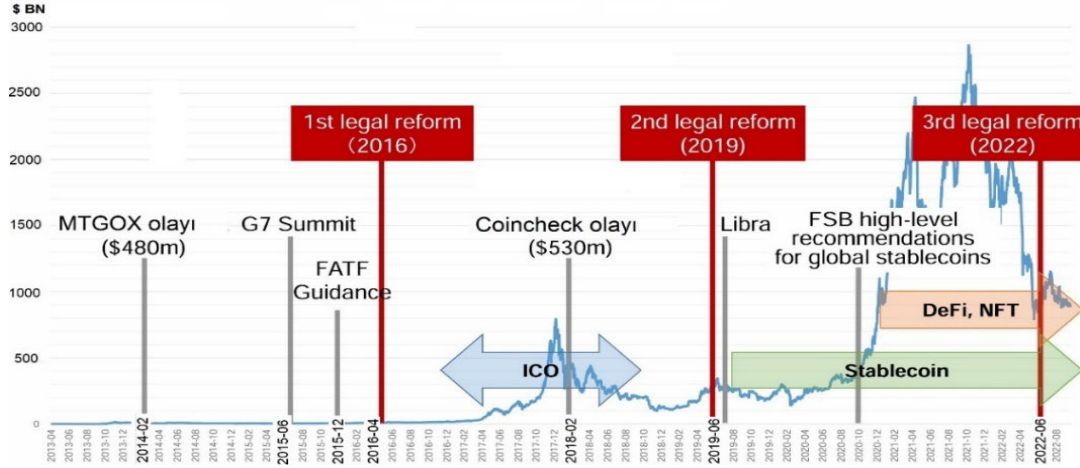
⁴³ FURUKAWA.

⁴⁴ BEATTIE.

⁴⁵ NORRY, Andrew: *The History of the Mt Gox Hack: Bitcoin's Biggest Heist*, 2023 (<https://blockonomi.com/mt-gox-hack/>, ET: 13.06.2025).

⁴⁶ 18.03.2014 tarihli Yazılı Yanıt No. 39 (Danışmanlar Meclisi Üyesi T. Okubo'nun Yazılı Sorusu Üzerine) için bkz. <http://www.sangiin.go.jp/japanese/johol/kousei/syuisyo/186/touh/t186039.htm> (ET: 14.11.2024); ISHIKAWA, s. 127.

lananlarda dahil olmak üzere ticari işletmelere, müşteri kimlik bilgilerini doğrulama yükümlülüğü getirilebileceği⁴⁷ ve ek olarak suç olduğu ya da suç geliri olduğu belirlenebilirse ya da şüphe edilirse, Suç Gelirleri Yasası'nın 21. maddesinde belirtilen denetleyici idari kurum Finansal İstihbarat Birimi'ne (*Financial Intelligence Unit-FIU*)⁴⁸ bildirimde bulunulabileceği ifade edilmiştir. Bu bakış açısına bir destek de Mali Eylem Görev Gücü'nün (*Financial Action Task Force-FATF*) yeni tavsiyelerini içeren kılavuzlardan gelmiştir (Grafik 1'de sürecin gelişimi tarihsel olarak görülebilir).



Grafik 1. Japonya'da Kripto Varlık Düzenleyici Çerçevesinin Geliştirilmesi⁴⁹

Sonuç olarak, düzenleme eksikliği olduğu ve bunun FIU ile ilişkilendirilerek çözümlenebileceği düşünülmüştür. Mt.Gox saldırısı ve hırsızlığı sonrasında, Japonya Finansal Hizmetler Ajansı (*Financial Services Agency, J-FSA, 2000 öncesi Finansal Denetim Ajansı- Financial Supervisory Agency*), 2014 yılının sonlarına doğru sanal varlık düzenlemelerini incelemek amacıyla bir çalışma grubu kurmuştur⁵⁰. 2015 yılında çalışma grubu raporunda, *sanal varlıkların tanımlanması*; müşteri fonlarının ayrı tutulması ve sermaye yeterliliği şartları getirilmesi aracılığı ile *sanal varlık borsa hizmeti sağlayıcılarının düzenlenmesi* olarak genellenebilecek iki temel öneride bulunulmuştur⁵¹.

A. Sanal Varlıkların Tanımlanması

Kripto varlıklar geleneksel yasalar tarafından sınıflandırılmadıkları için bu onların belgelenmesi, kaydedilmesi, varlıkların sahiplerinin gelirlerinin vergilendirilmesi gibi konularda boşluklar yaratmakta veya hizmet sunucularının sermaye, kayıt vb yükümlülüklerini de zorlaştırmaktadır. Hatta uygun bir hukuki düzenleme olmadığı için, fiilen hukuki bir muafiyet de oluşmaktadır⁵².

Japon hükümetine yöneltilen soru yönergelerine verilen cevaplarda görüldüğü gibi, Mt.Gox saldırısı sırasında sanal varlıkların yasal statüsü ve tanımlanması konusunda önemli belirsizlikler söz konusudur. Mevcut düzenlemeler, özellikle Para Birimi Kanunu ve Bankacılık Kanunu, Bitcoin gibi sanal var-

⁴⁷ 07.03.2014 tarihli Yazılı Yanıt No. 28 (*Danışmanlar Meclisi Üyesi T. Okubo'nun Yazılı Sorusu Üzerine*) için bkz. <http://www.sangiin.go.jp/japanese/joho1/kousei/syuisyo/186/touh/t186028.htm> (ET: 14.11.2024); ISHIKAWA, s. 127.

⁴⁸ Japonya Mali İstihbarat Merkezi (*The Japan Financial Intelligence Center-JAFIC*), Japonya'nın Finansal İstihbarat Birimi (*Financial Intelligence Unit-FIU*) olarak hizmet vermektedir. <https://www.npa.go.jp/sosikihanzai/jafic/jafic/about.htm> (ET: 13.12.2024).

⁴⁹ Grafik için bkz. AMAYA, Tomoko: *Regulating the Crypto Assets Landscape in Japan, 2022* (<https://www.fsa.go.jp/en/news/2022/20221207/01.pdf>, ET: 20.02.2024).

⁵⁰ Çalışma grupları ile politika oluşturmak Japon politik geleneğinde oldukça yaygın bir uygulamadır. Çalışma grubu, sektörün hem teorisyenleri olan akademisyenlerden hem de pratik tarafı kabul edilebilecek sivil toplum kuruluşları, bankalar ve menkul kıymet kurumları gibi taraflardan oluşmaktadır (DOEGE, Felix: "Who is Driving Financial Market Governance of Cryptocurrencies in Japan? Actors and Institutions behind Japan's FinTech Revolution", *ASIEN: The German Journal on Contemporary Asia*, 2021, Sayı 160/161, s. 118-135).

⁵¹ ENDŌ, Genichi: "Legal Restrictions Surrounding Bitcoin: To What Extent Does Japan's Legal System Apply?", *ITU (International Telecommunication Union) Journal*, 2014, Cilt 44, Sayı 12; ISHIKAWA, s. 128-129.

⁵² AYDINER, Tuncay: *Howey Testi Nedir? İşte Bilmeniz Gereken Her Şey*, 2023 (<https://cryptopotato.com/language/tr/howey-testi-nedir/>, ET: 20.02.2025).

lıkları (hükümetler ya da merkez bankaları tarafından çıkarılmadıkları için) para kapsamı dışında bırakmaktadır. Ayrıca teorik olarak itibari paraların sahip olduğu bazı fonksiyonlarda eksiklikler söz konusudur. Benzer şekilde, menkul kıymetleri düzenleyen diğer yasalar da Bitcoin gibi dijital varlıkları menkul kıymet saymadığı için, bu hukuki düzenlemelere de uygun olmadığı kabul edilmektedir⁵³.

Sanal varlıklar geliştikçe bu konuda düzenlemeler de değişmiştir. Örneğin ABD, Bitcoin hariç diğer kripto paraları özellikle ICO⁵⁴ları, “kâr beklentisi ile yapılan parasal ortak girişim olduğu ve bu kâr üçüncü bir tarafın çabasıyla elde edileceği” için menkul kıymet kabul etmektedir⁵⁵. Bu nedenle de ABD’de sanal varlıkların büyük çoğunluğu Menkul Kıymetler ve Borsa Komisyonu (*Securities and Exchange Commission-SEC*) tarafından yapılan düzenlemelere tabidir. Bitcoin ise başlangıç sermayesi için halka açık bir borç talep edilerek oluşturulmadığı için ABD bakış açısından menkul kıymet sayılmamakta, emtia kabul edilmektedir.

Japonya, çalışma grubunun önerileri doğrultusunda Ödeme Hizmetleri Yasası’nda (*The Payment Services Act-PSA*) 2016 yılında yapılan ve Nisan 2017’de yürürlüğe giren değişiklikle, kripto varlıkları da içeren sanal para birimlerini (*kasō tsūka*), yasal para olarak değil, “ödemelerde kullanılabilen ya da diğer varlıklarla değiştirilebilen tescilli bir değer” olarak tanımlamıştır⁵⁶. Bu ifade ile kripto varlıkların ödeme aracı olarak (Bitcoin’in de satın alma işlemleri için) kullanılabileceği, bununla birlikte (karşı tarafın hukuken kabul etmesi zorunlu olan) yasal bir ödeme aracı olmadığı vurgulanmaktadır⁵⁷. Dolayısıyla mevcut olan durum hukuki bir çerçeveye bağlanmış, kripto para (*crypto currency*) olarak kullanılagelen ifade kripto varlığa (*cryptoasset*) dönüştürülmüştür.

Takiben 27 Ekim 2017’de bankacılık ve sigorta denetiminden sorumlu otorite olan J-FSA, yatırımcıları ICO’ların riskleri konusunda uyarın bir basın bülteni yayınlamıştır. Bülten, sorumluluklarını hatırlatarak, “aşırı fiyat oynaklığı ve potansiyel dolandırıcılık” konusunda yatırımcıları uarmıştır⁵⁸. Ayrıca kripto varlık arz edicileri, “ICO’ların nasıl oluşturulduğuna bağlı olarak Japonya Ödemeler Hizmet Yasası ve Finansal Araçlar ve Borsa Yasası’nda mevcut düzenlemelerin gereklerini yerine getirmeleri gerekebileceği, aksi takdirde hukuku sorunlarla karşılaşabilecekleri” konusunda bilgilendirmiştir⁵⁹. Böylece, hem tasarruflarını yatıracak olanlara hem de arz ve borsa hizmeti sunmakta olan kişilere sorumlulukları hatırlatılmaktadır.

Japonya kripto varlıkların tanımlanmasını sonrasında bu tür tescilli değerler için değişim ve saklama hizmeti sunan borsaları da yeniden düzenlemiştir.

B. Sanal Varlık Borsa Hizmeti Sağlayıcıları (*Virtual Asset Service Providers - VASPs*)

Japonya’nın Ödeme Hizmetleri Yasası ve Suç Gelirlerinin Aktarılmasının Önlenmesi Yasası’nda Değişiklik (*Amendment of the Payment Services Act and the Act for Prevention of Transfer of Criminal Proceeds*) ile “sanal varlık borsa hizmet sağlayıcıları” (*Kasō-Tsūka-Kōkan-Gyōsha*) için yeni bir kategori oluşturulmuştur. Bu düzenlemeyle sanal varlık borsa hizmet sağlayıcıları daha önce var olan “ön ödemeli araç ihracatçıları” ve “para transferi hizmet sağlayıcıları” gibi başlıklara ek olarak düzenlenmiştir⁶⁰. Yeni düzenlemeyle sanal varlık alım satımı yapan, takas eden ya da aracılık hizmeti sunan işletmeler J-FSA’ya kayıt

⁵³ DOEGE, s. 121.

⁵⁴ ICO (*Initial Coin Offering*), geleneksel finansal piyasalardaki İlk Halka Arz’ın kripto para dünyasındaki karşılığıdır. Bir yatırım için başlangıç sermaye oluşturulması olarak da düşünülebilir.

⁵⁵ Bu tanımlama Howey testi aracılığı ile oluşturulmaktadır. Howey Testi için AYDINER.

⁵⁶ DOEGE, s. 123.

⁵⁷ DOEGE, s. 124.

⁵⁸ DASKALAKIS, Nikos / GEORGITSEAS, Panagiotis: *An Introduction to Cryptocurrencies: The Crypto Market Ecosystem*, Taylor & Francis, 2020.

⁵⁹ DASKALAKIS / GEORGITSEAS, s. 75.

⁶⁰ ISHIKAWA, s. 128.

yaptırma yükümlülüğü altına girmiştir. Mevcut borsaların yeni düzenlemelere uyum sağlaması için altı aylık bir geçiş süresi tanınarak operasyonlarını yasal çerçevede sürdürebilmeleri sağlanmıştır.

Kayıt, lisans gibi olmasa da sanal varlık hizmet sunucularının bazı bilgileri yetkilendirilmiş kurumlarla paylaşması anlamına gelmektedir. Ek olarak, Mt.Gox vakasından kaynaklanan tecrübe ile, VASPs'nin kullanıcı varlıklarını kendi varlıklarından ayrı tutmaları, hizmetler ve ücretler hakkında şeffaf bilgi sunmaları ve uyuşmazlıkları alternatif uyuşmazlık çözümü (*Alternative Dispute Resolution-ADR*) yöntemleriyle çözmeleri düzenlenmektedir⁶¹. Bu şekliyle düzenleme borsa hizmeti sunacak kurum ya da bireylere bir miktar sermaye zorunluluğu getirmektedir. Ek olarak müşterilerine daha üye kabul ederken, sorun çıktığında nasıl çözümleneceğini ve borsanın ne kadar sorumluluk kabul ettiğini açıkça söylemiş olması beklenmektedir.

Bu düzenlemeler, Japonya'nın kripto varlık piyasasında daha yüksek hesap verebilirlik ve şeffaflık sağlamayı amaçlarken tüketici koruması açısından da önemli bir adım olarak değerlendirilmiştir⁶². Bununla birlikte lisanslama yerine kayıt tercihi⁶³, pek çok ülke henüz bir düzenleme yapmadığı için (küresel bir düzenlemenin olmadığı bir ortamda), kripto sermayenin ülkeyi terk etmesinden kaçınan esnek bir düzenleyici yaklaşıma da işaret etmektedir.

C. Suç Gelirlerinin Aktarılmasının Önlenmesi

İnternet üzerindeki suçların sadece bir ülke aracılığı ile düzenlenmesi mümkün değildir. Sosyal medya üzerindeki yanlış bilgilendirmeler, hırsızlıklar vb. suçlar bir ülkenin yargı sınırları ile sınırlandırılmamaktadır. Bu nedenle bir ülkenin sınırlarını aşan suçlar küresel düzenlemeler gerektirmektedir. Kripto varlıklarla bağlantılı suçlar öncesinde de benzer suçlar bulunmaktadır. Bu nedenle daha önce de BM çatısı altında, çok taraflı sözleşmeler aracılığı ile uyuşturucu maddeler, silah ticareti, insan ticareti, göçmen kaçakçılığı vb konular ile bağlantılı küresel düzenleyici kurumlar oluşturulmuştur⁶⁴. Benzer örgütlerden olan Mali Eylem Görev Gücü (*The Financial Action Task Force-FATF*), web sayfalarında da belirtildiği gibi, “ulusal makamların uyuşturucu kaçakçılığı, yasadışı silah ticareti, siber dolandırıcılık ve diğer ciddi suçlarla bağlantılı yasadışı fonların peşine etkili bir şekilde düşebilmesini sağlamak için uluslararası standartları” belirlemek üzere oluşturulmuştur⁶⁵.

Görev Gücü yaptırım gücüne sahip tavsiye kararları almaktadır. FATF'nin Kara Para Aklama ve Terörizmin Finansmanı ile Mücadelede Risk Tabanlı Yaklaşım Kılavuzu (*The Guidance on the Risk-Based Approach to combating Money Laundering and Terrorist Financing*), ilk kez 2007'de hazırlanmıştır. Ülkelerin bankacılık ve finans kurumları, kılavuzdaki tavsiye kararlarına yüksek oranda uymaktadırlar. Kripto varlıklar için ilk tavsiyeler, Mt.Gox saldırısından sonra, kılavuzda yer almaya başlamıştır.

Mt.Gox sonrası Japonya G7 zirvesinde “sanal para birimlerinin ve diğer yeni ödeme yöntemlerinin uygun bir şekilde düzenlenmesi de dâhil olmak üzere, tüm finansal akışların şeffaflığını sağlamak için daha fazla adım atacağını” vaat etmiştir⁶⁶ (Grafik 1’den tarihsel seyrin görülmesi mümkündür). FATF kılavuzunda da “Her ülke, sanal para birimleri ile yasal para birimlerini takas eden borsalarda, müşteri kimliğini doğrulama zorunluluğu, kayıt / lisans gereklilikleri ve AML / CFT⁶⁷ düzenlemeleri getirmelidir” denmektedir.

⁶¹ KARAIKOS, Antonios: “Financial instruments: Transactions and consumer protection in Japan”, *Data Governance in AI, FinTech and LegalTech*, Edward Elgar Publishing, Londra, 2022, s. 133.

⁶² DOEGE, s. 129.

⁶³ CHENG, Evelyn: *The SEC Just Made It Clearer that Securities Laws Apply to Most Cryptocurrencies and Exchanges Trading Them*, 2018 (<https://www.cnbc.com/2018/03/07/the-sec-made-it-clearer-that-securities-laws-apply-to-cryptocurrencies.html>, ET: 21.02.2025).

⁶⁴ Ayrıntılı okuma için bkz. <https://www.unodc.org/unodc/en/about-unodc/index.html> (ET: 20.05.2025).

⁶⁵ Bkz. <https://www.fatf-gafi.org/en/the-fatf/who-we-are.html> (ET: 01.02.2025).

⁶⁶ AMAYA.

⁶⁷ AML/CFT (*anti-money laundering/combating the financing of terrorism*), “kara para aklama/terörizmin finansmanı ile mücadele” olarak çevirmektedir.

Japonya'nın Ödeme Hizmetleri Yasası ve Suç Gelirlerinin Aktarılmasının Önlenmesi Yasası'nda yaptığı değişiklikler (*Amendment of the PSA and...*) Coincheck saldırısından önce Nisan 2017'de yürürlüğe girmiştir. Temelde FATF ile uyumlu olarak "hesapların açılmasında kimlik doğrulamasını önermektedir. Ek olarak kullanıcı koruması perspektifinden bir düzenleyici çerçeve de geliştirilmiştir (asgari sermaye gereklilikleri, müşterilere bilgi sağlanması, müşterilerin varlıklarının ayrıştırılması ve sistemlerin güvenli yönetimi önerilmektedir).

Yukarıdakilerden anlaşılağı üzere, Mt.Gox borsasına yönelik iflas işlemlerinin başlamasından neredeyse iki yıl, saldırıdan üç yıl sonra, Japonya PSA'da yapılan değişikliklerle sanal varlıkları düzenleyen ilk yasal uygulamalarını yürürlüğe koymuştur.

Yapılan değişiklikler, bir tepki olduğundan, bir yandan tüketicinin korunmasını sağlarken bir yandan da FATF tavsiyeleri ile hukuki düzenlemeleri birleştirmeye çalışmak olarak anlaşılabılır⁶⁸. Sanal varlıklar değişim hizmet sağlayıcılarına ve sanal varlıkların tanımına ilişkin yeni kurallar, daha iyi hukuki düzenlemeler yolunda önemli bir adım olarak görülebilir ve Mt.Gox gibi krizlerin tekrar yaşanmaması için yenilik (*innovation*) ve denetim dengesini sağlamak amacı taşımaktadır⁶⁹.

Bununla birlikte, Mt.Gox tecrübesine rağmen, Japon yetkililerin bu tarihlerde piyasayı aşırı düzenlemekten kaçınmaya çalıştıkları da söylenebilir. Küresel bir düzenleme olmadığı için, herhangi bir ülkenin diğerlerinden önce sıkı düzenlemeler getirmesi, hızlı sermaye çıkışlarına neden olacağından, bütün ülkeler son derece dikkatli ve küçük adımlar atmaktadırlar. Dolayısıyla alınan önlemler yeterli olmamış ve yeni bir borsa saldırısı gerçekleşmiştir.

VI. COINCHECK SOYGUNU

Coincheck Borsası 2014 yılında Japonya'da kurulmuştur ve Mt.Gox gibi ülkedeki popüler kripto para borsalarından biridir. Bu borsada Bitcoin, Ether, LISK ve NEM dahil olmak üzere çok çeşitli dijital varlıkların ticareti, itibari paralarla değişimi ve saklama (muhafaza) işlemleri yapılabilmektedir.

Coincheck soygunu NEM kripto varlıkları üzerinden yapılmıştır. NEM (veya XEM olarak kısaltılmaktadır, *New Economy Movement*-Yeni Ekonomi Hareketi) açık kaynaklı bir kripto varlık birimidir ve Bitcoin gibi aynı zamanda bir blokzinciri platformudur. Farklı borsalarda bu dijital varlığa ilişkin alım satım işlemleri yapılabilmektedir.



Resim 3. NEM Simgeleri

26 Ocak 2018 tarihinde bilgisayar korsanları Coincheck kripto varlık borsasının güvenlik sistemini ihlal etmiş ve 500 milyon NEM tokeni çalıp ve daha sonra ağdaki 19 farklı adrese dağıtmışlardır⁷⁰. (Mt.Gox saldırısı sırasında bahsedilen Tablo 1'den hırsızlığın büyüklüğüne ilişkin tahmini rakamlar görülebilir).

⁶⁸ ISHIKAWA, 127-128.

⁶⁹ SYGNA: *Japan's History of Crypto Asset Regulation: 2014-2020* (<https://www.sygna.io/blog/japan-crypto-regulation-history-2014-2020>, ET: 15.11. 2024).

⁷⁰ TSUCHIYA, Yoichi / HIRAMOTO, Naoki: "How Cryptocurrency is Laundered: Case Study of Coincheck Hacking Incident", *Forensic Science International: Reports*, 2021, 4 (100241), s. 3; RASTOGI / BUDHIRAJA / AHMAD, s.4-5

İlk adımda hırsızlığına neden olan güvenlik sorununun iki noktadan kaynaklanabileceği düşünülmüştür:

- NEM'i geliştiren yani kripto varlığı üreten taraftan,
- İşlemleri yapan/cüzdanları saklayan borsa tarafından.

Olayı takiben NEM geliştiricileri, sorunun kendilerinden kaynaklanmadığını iddia etmişler, Coincheck Borsası yöneticileri de kendi sorumlulukları olduğunu kabul etmişlerdir⁷¹. Borsa yöneticilerinin açıklamalarına göre, Bitcoin dışındaki kripto varlıkların yüksek bir korumaya ihtiyacı olduğunu düşünmedikleri için NEM dahil diğer kripto varlıkları sıcak cüzdanlarda saklamışlar ve bu varlıkların transfer ve değişimlerinde çok taraflı akıllı imza teknolojisini (*Multisig Contract Smart Signing Uygulamasını*) gerekli görmemişlerdir⁷². Bilgisayar korsanları NEM cinsi kripto varlıkların depolandığı bir sıcak cüzdanın özel anahtarını elde etmiş ve ağ bağlantılı sıcak cüzdanlardan kripto varlıklar çok kısa süre içinde boşatılmıştır⁷³. Büyük hesap aktarımları için akıllı imza teknolojisinin kullanılmıyor olması, çok sayıda hesaba ulaşılmasını ve ulaşıncı da alanın ve gönderenin anonim olduğu bir dünyada herhangi bir yere aktarılabilmesini sağlamış; zararın çok büyümesine neden olmuştur⁷⁴.

Tablo 2, kripto varlık piyasasında Coincheck ile ilgili olaylara odaklanarak davanın zaman çizelgesini özetlemektedir. Tablodan görülebileceği gibi, soygun sonrası, NEM ekibi, soygunda çalınan tüm NEM'leri, diğer borsaların kabul etmemesi için fonları çalıntı olarak tanımlayan bir mesajla etiketlenmiştir. Bu hırsızlık işaretine rağmen, çalınan kripto varlıkların küçük, hukuki kayıt ya da lisans düzenlemesi olmayan borsalarda veya Monero ve ZCash gibi daha çok gizlilik amacı ile kurulmuş borsalarda, indirimli fiyatlarla Bitcoin'e ya da yerel paralara dönüştürülerek aklandığı ve farklı hesaplara aktarıldığı düşünülmektedir. Çalıntı olarak işaretlenmiş (etiketlenmiş) olmasına rağmen hesapların dönüştürülmesi engellenememiştir. Saldırıda bir süre sonra sorumluluğu üstlenen Coincheck borsası, saldırıdan etkilenen 260 bin kullanıcının tamamına Japn yeni cinsinden geri ödeme yapacaklarını duyurmuştur⁷⁵. Etkilenenlerin tüm zararlarını karşılamayı seçtikleri için Coincheck yetkileri, kripto varlık dünyasında açık bir destek de almışlardır⁷⁶.

Tarih	Olay
26 Ocak	Saldırı gerçekleşiyor ve korsanlar NEM'i birçok adrese transfer etmeye ve dağıtmaya başlıyorlar.
27 Ocak	Coincheck tarafından açıklama yapılıyor.
1 Şubat	Kripto piyasasında takas işlemleri için muhtemelen test operasyonu ile korsanlar Bitcoin adresleri ilk Bitcoin ödemesini alıyor.
7 Şubat	Kripto piyasasında takas başlıyor.
12 Mart	Korsanlar, satışlardan elde ettikleri kazancı Bitcoin adreslerinden transfer ediyorlar.
20 Mart	NEM, izlemeyi devre dışı bırakıyor.
22 Mart	Çalınan NEM varlıklar satılıyor.
23 Nisan	Korsanlar satışlardan elde ettikleri toplam kazancı Bitcoin adreslerinden transfer ediyorlar.

Tablo 2. Coincheck Saldırısından Sonra Olayların Gelişimi⁷⁷

⁷¹ BUCK, Jon: *Coincheck: Stolen \$534 M in NEM were Stored on Low Security Hot Wallet*, 2018 (<https://cointelegraph.com/news/coincheck-stolen-534-mln-nem-were-stored-on-low-security-hot-wallet>, ET: 10.05.2025);

⁷² BUCK, s. 1; TSUCHIYA / HIRAMOTO, s. 3.

⁷³ BUCK, s. 1; TSUCHIYA / HIRAMOTO, s. 3.

⁷⁴ CURRAN, Brian: *The History of the Coincheck Hack: One of the Largest Heists Ever*, 2018 (<https://blockonomi.com/coincheck-hack/>, ET: 15.10.2024).

⁷⁵ BUCK, s. 1; TSUCHIYA / HIRAMOTO, s. 3; CURRAN.

⁷⁶ CURRAN; TSUCHIYA / HIRAMOTO, s. 4.

⁷⁷ Tablo TSUCHIYA / HIRAMOTO, s. 2'den alınmıştır.

Sorumluların araştırılmasında kolluk kuvvetleri, Ocak 2021’de 31 kişiyi, çalıntı olduğunu bilmelerine rağmen (etiketler nedeniyle) NEM kripto para birimini diğer dijital para birimleriyle takas etmekle suçlamıştır. Bununla birlikte, Coincheck saldırısını gerçekleştiren bilgisayar korsanlarının kimlikleri belirlenememiştir. 31 şüpheli, çalınan değer yaklaşık %30’una tekabül eden toplam 20 milyar yen değerinde NEM’in ticareti ile suçlanmışlardır⁷⁸.

VII. COINCHECK SONRASI DÜZENLEYİCİ REFORMLAR

Mt.Gox ve Coincheck’in yaşadığı başarısızlıklar, Japon hükümetinin kripto varlık yönetimine yönelik farkındalığını erken bir aşamada artırmış ve bir strateji geliştirmesini zorunlu hale getirmiştir. Bankacılık, menkul kıymetler ve borsa ile sigortacılık sektörlerini denetleyen, Japon hükümetine bağlı entegre finansal düzenleyici bir kurum olarak J-FSA, 15 kayıtsız kripto varlık borsasında yerinde denetimler gerçekleştirmiş ve nihayetinde 7 borsaya iş geliştirme uyarıları gönderilmiştir⁷⁹. Ayrıca 2 borsanın operasyonları geçici olarak durdurulmuştur.

Yeniden bir çalışma grubu (*The Study Group on Virtual Currency Exchange Services*) oluşturulmuş, önerileri sorulmuştur. Çalışma grubu Aralık 2018’de raporunu sunmuş ve kripto para birimi değişim sağlayıcılarının daha fazla ve daha sıkı düzenlenmesini önermiştir⁸⁰.

Japonya bu önerileri dikkate alarak 2019 ve 2022’de iki defa, birbirini takip eden hukuki düzenlemelerle daha sıkı bir çerçeve oluşturmuştur. İlk düzenleme Ödeme Hizmetleri Yasası ile Finansal Araçlar ve Borsa Yasası’nda yapılan değişiklik ile kripto varlık türev işlemleri için, ikincisi stablecoin⁸¹ ihraççıları ve aracıları için, normal finans sisteminde zaten var olan müşteri bilgisi (*Müşterini Tanı, Know Your Customer-KYC*) ve kayıt sistemi zorunluluğunu getirerek düzenlemiştir⁸².

Ayrıca bu süreçte, Japonya Merkez Bankası (*Bank of Japan-BOJ*), Maliye Bakanlığı’ndan kurumsal bağımsızlığını kazanmıştır. Sektör içi bir denetim ve düzenleme kuruluşu (Japonya Sanal ve Kripto Varlıklar Borsası Birliği (*Japan Virtual and Crypto Assets Exchange Association-JVCEA*)) oluşturulmuştur. Ödeme Hizmetleri Yasası, Finansal Araçlar ve Borsa Yasası (*Financial Instruments and Exchange Act*), Bankacılık Yasası gibi ilgili yasalarda yeni değişikliklere gidilmiştir. Değişikliklerle oluşturulan hukuki yapı halihazırda mevcut olan tüm kripto varlık ve token çeşitlerini düzenlemektedir. Sıkı düzenlemeleri takip etmek, denetlemek vb gereklilikler için yeni kurumlar da oluşturulmuştur.

A. Sektör İçi Düzenleyici Bir Kuruluşun Oluşturulması

Japonya Sanal ve Kripto Varlıklar Borsası Birliği (JVCEA) sistemi sektör içinden denetlemek ve düzenlemek için 2018 yılında oluşturulmuştur⁸³. Bir kamu kurumu olmamakla birlikte J-FSA tarafından resmi olarak tanınmaktadır.

JVCEA’nın sektör içi özerk bir düzenleyici (*self-regulation*) olarak oluşturulmasının nedeni, kripto varlık birimi gibi hızla gelişen endüstrilerde bürokratlardan ziyade uzmanların hızla kararlar almasının daha iyi olacağı düşüncesidir. Çünkü kripto varlıklar piyasasının uzmanlık gerektiren bazı bilgiler olmadan takip edilmesi,

⁷⁸ TSUCHIYA / HIRAMOTO, s. 2

⁷⁹ SEPTIANSYAH, Veris / FITRI, Ich Cahyaning / SETYAWAN, Fendi / PRAKOSO, Bhim: “Accountability of the Financial Services Authority in Indonesia, Australia, Germany, France and Japan”, *International Journal of Social Science and Education Research Studies*, 2024, Cilt 4, Sayı 6, s. 531-544.

⁸⁰ AMAYA.

⁸¹ Stablecoinler (Sabit kripto paralar), dijital varlığın değerinin ulusal bir paraya (Dolar, Euro vb), borsada işlem gören bir emtiaya (kıymetli metaller veya endüstriyel metaller gibi) veya başka bir kripto paraya birebir (1:1) sabitlendiği varsayılan bir kripto para türüdür. Bu çeşit kripto varlıklarla, diğer kripto varlıklarda görülen yüksek fiyat oynaklığının azaltılması hedeflenmiştir. Fakat pek çok Stablecoin örneğinde varsayımın çalışmadığı, yüksek kayıpların olduğu gözlenmektedir.

⁸² AMAYA.

⁸³ Bkz. <https://jvcea.or.jp/about/> (ET: 01.01.2025); AOKI, Shunsuke / KAWAI, Ken / MIYAKE, Akihito: *Japan: Getting a Grip*, 2020 (<https://www.iflr.com/article/2a63733ixysbvclr183e0/japan-getting-a-grip>, ET: 20.01.2025).

düzenlenmesi ya da kontrol edilebilmesi mümkün görünmemektedir. Ayrıca uzman bilgisi ile JVCEA'nın teknolojik yeniliklerle eskimeyen yasaların çıkarılmasına yardımcı olabileceği de düşünülmektedir.

JVCEA, kripto piyasalar için pek çok alanda karar yetkisine sahiptir. Birlik, kripto varlıklar için borsa yeterliliklerinin belirlenmesi ve denetlenmesi, kayıtların takibi, borsalara ve işlem gören varlıklara ilişkin istatistiki bilginin üretilmesi konusunda yetkilendirilmiştir⁸⁴. Tüm kripto varlık borsalarının ve kripto varlık saklama hizmeti sunucularının JVCEA'ye kayıt olması ve yönergelerini izlemesi de beklenmektedir⁸⁵. Bu tarihten itibaren Japonya'da işlem yapan kripto varlık borsalarının JVCEA'nın belirlediği sermaye yeterliliklerine sahip olması ve kuruma kayıt olarak lisans yeterliliklerini sağlama-sı gerekmektedir. Ayrıca JVCEA borsada işlem görebilecek kripto varlıklara ilişkin bir liste belirle-mektedir. JVCEA'nın ve J-FSA'nın listelemediği kripto varlıklar Japonya'da işlem görememektedir.

B. Kişileri Koruma ve Şeffaflık

JVCEA ve J-FSA düzenlemeleri sonrasında, Japonya'da faaliyet gösteren tüm borsaların müşteri-lerin varlıklarını güvenilir bir şekilde yönetmek için, müşterilerinin kripto varlıklarıyla “*aynı türde ve aynı miktarda kripto varlık*” elde tutmaları, yani işlem yapılan kadar sermayeye sahip olmaları bek-lenmektedir⁸⁶. Mt.Gox saldırısı sonrası, ilk çalışma grubunun önerdiği sermaye yeterlilikleri başlığı altında düşünülebilecek bu şart, Coincheck saldırısı sonrası netlik kazanmıştır. Borsaların BTC, Eter-nium, NEM vb. kripto varlıklar üzerinden kabul ettikleri tasarruflar karşılığında, aynı varlık cinsinden sermayeye sahip olmaları gerekmektedir.

Diğer şartlar arasında borsaların “kullanıcıların kripto varlıklarının en az %95’ini çevrimdışı bir ortamda (soğuk cüzdana) yönetmek, saklamak zorunda olmaları”, “sistem güvenliği için bilgisayar program güvenliğini daima güncel tutmaları”, “eğer hırsızlık, saldırı vb ile kayıplar olursa, bu kayıpla-rı hangi oranda, hangi cins varlık ile karşılaştacaklarını, kuruluşta açıklamış olmaları”, “bilanço ve gelir tablolarını yayınlamaları, denetleyici kurumlar ve kullanıcılar için yeterli bilgi temin etmeleri”, “piyasa manipülasyonu vb haksız rekabet uygulamalarından sakınmaları” sayılabilir⁸⁷.

Bu düzenlemelerden umulan fayda, saldırılara hedef olan kripto borsaların, sermaye ve sistem ye-terliliklerine zorlanarak, kendilerini ve müşterilerini koruyabilir hale gelmeleridir. Bu nedenle ilk madde borsaların sermaye gerekliliklerini yükseltmektedir. Diğer şartlardan soğuk depolama ve sistem zorunlulukları ile hizmet sunucu birimlere güvenlik önlemleri konusunda sorumluluk yüklenmektedir. Diğer talepler ise, olası bir kayıp durumunda tarafların sorumluluklarının belirlenmesinde önceden ilan edilen sözleşme hükümleri aracılığı ile yargılama sürecini kısaltmayı, yargının üzerindeki yükü azalt-mayı ve borsaların kendi değerleri ve işlem hacimleri konusunda yanıltıcı bilgi üretmelerinin engel-lenmesini hedeflemektedir. Son olarak borsaların mali durumları hakkında şeffaf olmalarının ve müş-terine doğru bilgi aktarmalarının sağlanabilmesi için denetleyici kurumlara görevler yüklenmektedir.

C. Kaldıraç Oranın Düzenlenmesi

J-FSA ayrıca, operasyonel kararlarda almıştır. Kripto varlık marjın ticaretinde⁸⁸ kaldıraç oranını⁸⁹ ilk adımda yatırılan teminatın dört katı ile sınırlandırmıştır⁹⁰. Tedbirler, kamu güvenliğini yeniden tesis

⁸⁴ JVCEA.

⁸⁵ AOKI / KAWAI / MIYAKE.

⁸⁶ AMAYA; MORITA, Hatsuru: “Regulatory and Policy Reforms in Japan”, *Law and Practice of Crowdfunding and Peer-to-Peer Lending in Australia, China and Japan*, Springer Nature, Singapore, 2010, s. 217-235.

⁸⁷ AMAYA; MORITA, s. 220.

⁸⁸ Kripto varlık marj ticareti, yatırımcıların kendi sahip oldukları sermayeden daha fazla para ile işlem yapmalarına imkân tanır.

⁸⁹ Kaldıraç oranının başlangıç mevduatının 2 katı ile sınırlanması, örneğin, eğer bir yatırımcı 2.000 dolar yatırıyorsa, en fazla 4.000 dolar değerinde bir işlem açabileceğini gösterir. Kaldıraçlı işlemler, yatırımcıların kazançlarını artırabilse de aynı zamanda kayıplarını da bü-yütebilir.

⁹⁰ PALOVAARA, Anton: *What is Crypto Margin Trading and How Does It Work?* (<https://leverage.trading/what-is-crypto-margin-trading/>, ET: 24.11.2024).

etmek, güvenliği artırmak ve Japonya'nın kripto varlık sektörüne daha sağlam bir düzenleyici çerçeve kazandırmak amacıyla bir bütün olarak uygulanmıştır. Kaldıraç oranları 2019 yılında kullanıcıların başlangıç mevduatlarının 2-4 katı ile ve 2020 yılında 2 katı ile sınırlandırılarak azaltılmaya devam etmiştir. Bu sınırlandırma aşırı riskli işlemlerden kaynaklanabilecek, yüksek hareketliliği ve büyük kayıpları önlemeyi hedeflemektedir. Ayrıca yatırımcıların daha temkinli işlem yapmalarını teşvik ederek, piyasanın istikrarını sağlamayı amaçlamaktadır⁹¹. Borsaların, riskli kripto varlık işlemlerinde yatırımcıların kaybedebilecekleri maksimum miktarı sınırlamasını sağlayarak, JVCEA'nın kılavuzuna da uyulmaya çalışılmaktadır.

D. AML/CFT Düzenlemeleri

FATF'ın Japonya'ya ilişkin Dördüncü Tur Karşılıklı Değerlendirme Raporu Ağustos 2021'de yayınlanmıştır⁹². Raporda Japon hükümetinin AML/CFT politikası için Bakanlıklararası Konsey oluşturduğu, Konseyin AML/CFT için eylem planı hazırladığından bahsedilmektedir. Plan finansal kuruluşlar ve sanal para birimi değişim sağlayıcıları ile denetleyicileri tarafından alınması gereken önleyici tedbirleri de içermektedir. Nihayet, Ekim 2022'de Japonya Ulusal Meclisine kripto varlıklar için Seyahat Kuralı ile ilgili revize edilmiş bir yasa tasarısı sunulmuştur.

Dolayısıyla AML/CFT düzenlemelerinin Müşterini Tanı ve Seyahat Kuralı kripto varlık hizmet sunucuları içinde geçerli hale gelmektedir. FATF'nın tavsiyelerinin kripto varlıkları içerecek şekilde güncellenmesi, kripto varlıklar için takas, saklama hizmeti ve diğer hizmetleri veren kuruluşların, artık kara para aklama ve terörizmin finansmanına karşı diğer finansal varlıkların uyduğu önlemlere tabi olacakları anlamına gelmektedir.

Japonya'da, "Kripto Varlık Borsası Hizmet Sağlayıcıları", "Finansal Araç İşletmecileri" ve "Elektronik Ödeme Aracı Borsası Hizmet Sağlayıcıları" dahil olmak üzere kripto ile ilgili tüm hizmet sağlayıcıların geçerli tüm AML/CFT önlemlerini alması gerekmektedir⁹³.

"Müşterini Tanı" (KYC) ya da "Nihai Faydalanıcıyı Tanı" (*The Ultimate Beneficial Owner-UBO*) olarak adlandırılan süreç, herhangi bir ülkede bankacılık hizmetlerinden yararlanmak için uyulması gereken bir kuraldır ve tüm kara para aklama karşıtı mevzuat ve düzenlemelerin temel ilkesini oluşturmaktadır. KYC kuralı herhangi bir banka hesabı açıldığında, bu hesapla işlem yapıldığında, işlemi yapanın geçerli kimlik ve ikametgâh belgelerinin olmasını ve bu bilgilerinin hizmet sunucu tarafından saklanması gerektirmektedir. Dolayısıyla bu kural kripto varlık borsa hizmet sağlayıcılarına, herhangi bir hesabın açılışında, kişilerin kimlik bilgilerini almak ve hatta teyit etmek sorumluluğu yüklemektedir.

"Seyahat Kuralı" (*Travel Rule*)⁹⁴ ise belli bir miktarın üstündeki para hareketlerinde, parayı alanın ve gönderenin isimlerinin, hesap numaralarının ve adres bilgilerinin hizmet sunucular tarafından kayıt altına alınması⁹⁵ ve mali istihbarat kurumlarıyla bu bilgilerin paylaşılması anlamına gelmektedir. Ayrıca aktarılan söz konusu finansal varlığın kaynağı yani nereden elde edildiği de sorgulanabilir. KYC gibi Seyahat Kuralı da bankacılık sisteminde ulusal paralar için zaten uygulanmaktadır.

⁹¹ SYGNA: Guide: *Japan Crypto Asset Regulation* (<https://www.sygnia.io/blog/japan-crypto-asset-regulation-guide/>, ET: 26.11.2024); MAEDA, Rick: *State of the Japanese Crypto Market*, 2024 (<https://www.prestolabs.io/research/state-of-the-japanese-crypto-market>, ET: 24.11.2024).

⁹² MINISTRY OF FINANCE JAPAN: *AML/CFT/CPF in Japan*, (https://www.mof.go.jp/english/policy/international_policy/amlcftcpf/3_efforts.html, ET: 29.11.2024).

⁹³ AMAYA; SUZUKI, Yuri / OCHIAI, Takafumi / OUE, Ryosuke / KANEHISA, Naoki / TANIZAKI, Kenicki: *Japan: A New Dose of Regulation and Promotion*, 2019 (www.aplawjapan.com/archives/pdf/A-fresh-dose-of-regulation-and-promotion.pdf, ET: 25.10.2024).

⁹⁴ İşlem yapan kişilere ait kişisel veriler aktarımlarıyla birlikte seyahat ettiği için düzenlemeye "Seyahat Kuralı" denilmektedir.

⁹⁵ KAUR, Guneet: *The Crypto Travel Rule: An Overview*, 2023 (<https://cointelegraph.com/learn/articles/crypto-travel-rule>, ET: 26.11.2024).

Kripto varlıkların anonim yapısı, yasa dışı faaliyetlerden elde edilen gelirin kullanılabilmesini ya da örneğin bir borsa saldırı sonrası, kripto varlıkların herhangi bir cüzdana girmesini kolaylaştırmaktadır. Siber suçlar üzerine yapılan araştırmalar, kripto varlıklardan sadece Bitcoin üzerinden bile bilgisayar korsanlıklarının ciddi boyutlarda olduğunu iddia etmektedir. CipherTrace Raporu göre, suç teşkil eden Bitcoin'in yüzde 97'si AML yasalarının zayıf olduğu, regüle edilmemiş ülkelerdeki borsalara aktararak dönüştürülmekte ve Bitcoin ya da itibari (Euro veya dolar gibi ulusal) para cüzdanlarına girmektedir⁹⁶. Diğer bir ifade ile bilgisayar korsanları çalınan fonları, hukuki düzenlenmesi olmayan ülkelerdeki kripto para borsaları aracılığıyla kolayca servete ya da harcanabilir bir hale dönüştürebilmektedirler. Seyahat Kuralı ile büyük miktarlardaki varlıklar el değiştirdiğinde kayıt altına alınması, KYC ile de hesabın sahibinin doğru kimlik bilgilerine ulaşılabilmesi hedeflenmektedir.

Bununla birlikte gerek KYC gerek Seyahat Kuralı, kripto varlıkların felsefi temelleri ile ve anonimlik özellikleri ile çelişmektedir. Japonya, AML/CFT rejimini güçlendirmek için Ekim 2022'de Ulusal Meclis'e kripto varlıklar için Seyahat Kuralı ile ilgili uygulamalar için revize edilmiş bir yasa tasarısı sunmuş olmasına rağmen, hali hazırda uygulanabilir bir çerçeve oluşturulamamıştır. Japonya VASP'lerde uygulama yöntemleri üzerinde 2023'ten beri çalışılmaktadır⁹⁷.

SONUÇ

Kripto piyasalarda bulunan finansal fonların büyüklüğü hem ülkelerin hem de kötü niyetli kişilerin ilgisini çekmektedir. Ülkeler bu fonları kendi sınırları içinde tutabilmek için kripto varlık piyasasındaki hızlı gelişmeyi teşvik etmek ile daha sıkı hukuki düzenlemeler yapmak arasında bir denge yakalamaya çalışmaktadırlar. Kripto varlıklar alanında öncü ülkelerden Japonya'nın borsa saldırıları konusundaki deneyimi, bu piyasalardaki gelişimin yönünün daha sıkı düzenlemelere doğru olduğunu göstermektedir.

Japonya'nın kripto varlık piyasalarının geçmişi, bilgisayar programları ve oyun teknolojisi alanındaki öncülüğüne kadar dayanmaktadır. Bu çalışmada vurgulandığı üzere, bu teknolojiye yakınlık, 2000'li yılların başında Bitcoin'in doğuşunda Japonya'ya öncü bir rol sunmuştur. Bu statü beraberinde ilk adımları atan ülke olmanın zorluklarını da getirmiştir. Bu makalede değerlendirilen Mt.Gox borsası saldırısı, hukuki olarak neredeyse hiç düzenlenmemiş bir ortamda yaşanmış ve borsanın iflası ile sonuçlanan yüksek finansal kayıplara neden olmuştur. Saldırı sonrası, Japonya hukuki düzenleme yapabilmek için kripto varlıkları tanımlamaya çalışmış, kripto varlık borsalarını düzenleyerek kayıt zorunlulukları getirmiştir. Ayrıca kripto varlık sektöründeki tüm büyük oyuncular, güvenlik sistemlerini yeniden tasarlamak ya da gözden geçirmek için ve sermayelerini artırmak için daha fazla kaynak ayırmak zorunda kalmışlardır.

Bu düzenlemeler henüz hayata geçirilmişken Coincheck kripto varlık borsası bilgisayar korsanlarının saldırısına uğramıştır. Mt.Gox borsa saldırısı sonrası getirilen sermaye zorunlulukları Coincheck borsasının yeterli sermayesi bulunmasını sağladığı için kayıplar karşılanmış, bununla birlikte bilgisayar korsanlarının kimlikleri belirlenememiştir. Japonya saldırı sonrası önceki düzenlemenin sorunu çözmediği görerek, borsaların sermaye yeterliliklerini yükseltmiş, sektörü içerden düzenleyen bir öz denetim kurumu Sanal ve Kripto Varlık Borsaları Birliği'ni (JVCEA) oluşturmuş, kayıpların büyümesine neden olan kaldıraç oranlarını birkaç yıl içerisinde düşürmüş, borsalarda işlem görecektir kripto varlıklar için J-FSA'da listelenmesi şartı getirmiş, dolayısıyla düzenlemenin dozunu yükseltmiştir.

Bu çalışmanın kapsamına girmemekle birlikte başka ülkelerde de benzer borsa saldırıları ve soygunları devam etmektedir. Her olayda bir öncekine göre daha yüksek kayıplardan söz edilmektedir. Saldırıların ve kayıpların devamlılığı, borsaların siber suçlular için bir hedef olduğunu ve kripto koruma tekniklerinin açıklar içerdiğini göstermektedir. Korsanların kimlikleri genellikle belirlenemediği, boşalttıkları hesaplar için bir ceza görmedikleri için, kripto piyasalarda hırsızlığı ve dolandırıcılığı teşvik edici bir ortam oluşmaktadır.

⁹⁶ CIPHERTRACE: *CipherTrace Cryptocurrency Intelligence 2018 Q3*, 2018 (<https://www.ciphertrace.com/crypto-aml-report-2018q3.pdf>, ET: 18.10.2024).

⁹⁷ Bkz. <https://www.fsa.go.jp/> (ET: 29.12.2024).

Diğer sorun, saldırılar ceza adalet sisteminin önüne geldiğinde, çözüm uzmanlık gerektirmekte, uzun zaman almakta ve bu makale kapsamında aktarılan Japonya'daki örneklerde ya da Türkiye'de çeşitli ponzi dolandırıcılıklarında görülebileceği gibi tüm kayıplar tazmin edilememektedir. Bu makalede belirtildiği gibi Japonya kripto varlık borsalarının ve borsalarda işlem görmesine izin verilen kripto varlıkların müşterilerine şeffaflık kurallarını belirlemektedir. Bu kurallar kuruluş sözleşmelerinde sorun çözümlerinin ve olası kayıpların tazmin miktarlarının belirtilmesini de içermektedir. Bu mahkeme sürecinin kısılmasını sağlayabilecek bir örnek gibi görülmektedir.

Bu saldırılar sonrası Japonya gibi pek çok ülke, öncelikle kripto varlıkları tanımlayarak, kayıt ya da lisans veren ve borsa olabilmenin şartlarını düzenleyen kurumlar oluşturmuşlardır. Kripto varlık dünyasında her gün bir yenisi eklenen varlıklar için ülkelerinden tasarruf yönlendirilebilmesi için asgari standartlarını belirlemişlerdir. Türkiye'de Temmuz 2024'de Sermaye Piyasası Kanunu'nda değişiklikle kripto varlık hizmet sağlayıcıları SPK'nın düzenleme ve denetim yetkisi altına alınmıştır. Mart 2025'de kuruluş ve sermaye yeterlilikleri düzenlenmiştir. Kripto varlıklara özel olmamakla birlikte, lisans ve işlem görecekt varlıkların listelenmesi gibi bir prosedür içermemesine rağmen, kripto varlık borsaları için SPK'nın faaliyet onayı vermesi bile mevcut duruma bir hukuki çerçeve getirmiştir. Sadece faaliyet onayı başlığını içermesi nedeniyle Türkiye minimum düzenleme yapan ülkeler arasındadır. Hukuki düzenleme yapmakta bekle gör politikası pek çok ülke tarafından izlenmektedir. Bununla birlikte Türkiye'de de alanında teknik bilgisi yüksek bir kurumun ya da bir koordinasyon biriminin oluşturulması olası kayıpların azaltılmasını sağlayabilir ve gelecekte yapılacak düzenlemelere hızlı karar verebilmesinde etkili olabilir.

Japonya'nın borsa saldırıları deneyimi, kripto paraların anonimlik özelliklerinin azaltılarak daha önce itibari paralar için oluşturulan küresel düzenlemelerin kripto varlıklar için de denendiğini göstermektedir. Ulusal paralar için, servetlerin kaynakları ile ilgili sorgulamalar ve para transferleri için hukuki düzenlemeler küresel bir çerçevede FATF çatısı altında yürütülmektedir. Borsa saldırıları sonrası benzer bir gelişme kripto varlıklar için de söz konusudur. Hesaplarının kime ait olduğuna dair belgelerin alınması, saklanması (müşterini tanı, KYC), hesap hareketleri belli bir miktarı aştığında ulusal mali istihbarat kurumlarına bilgi verilmesi (*travel rule*) taleplerine ilişkin FATF tavsiyeleri 2018'den beri kripto paralar için de geçerlidir. Tavsiye kararı, FATH üye ülkelerinin çoğunda zaman içinde uygulanmaya başlanmıştır. Türkiye'de de Aralık 2024'da Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesine Dair Tedbirler Hakkında Yönetmelik'te değişiklik ile kripto varlık hizmet sağlayıcılarından kimlik tespiti ve belli bir bedelin üzerindeki işlemlerin mali istihbarat kurumu olan MASAK'a bildirilmesi düzenlenmiştir.

Ayrıca kripto varlıkların ülkelerin sınırları ile bağlı olmayan yapısı herhangi bir hukuki düzenlemenin etkin olabilmesi için küresel düzeyde uygulanmasını da gerektirmektedir. Kripto varlıkların hem arzının (oluşturulmasının) hem de varlıkların hesap hareketlerinin üzerinde devletlerin tam bir kontrolü bulunmamaktadır. Hali hazırda pek çok ülke mevcut yapıyı düzenlemek ve düzenlememek arasında çeşitli basamaklarda yer almaktadırlar. Çin hükümetinin sert düzenlemeleri sonrası Japonya'nın kripto endüstrisinin gelişiminden de görülebileceği gibi yatırımcıların (ve bilgisayar korsanlarının) düzenlemelerin az olduğu ülkeleri tercih etmektedirler. Hızlı sermaye hareketlerinden kaçınmak için ülkeler küçük adımları tercih etmektedirler.

Kripto varlıklar gelişimlerini henüz tamamlamamışlardır. Mevcut durumları, ülkelerin ulusal paraları ile yapılan her türlü sermaye ve yatırım hareketi alanında gelişme gösterebileceklerini düşündürmektedir. Bu gelişmenin yönünün ülkelerin refah artışlarını destekleyici, yüksek kayıpları engelleyici olacak şekilde hukuki düzenlemelerle çerçevelenmesi gerekmektedir.

Katkı Oranı Beyanı:

Çalışmaya Fazilat MİRAKHMEDOVA ve Dr. Öğr. Üyesi Filiz TEPECİK eşit oranda katkı sağlamıştır.

KAYNAKÇA

- AMAYA, Tomoko: *Regulating the Crypto Assets Landscape in Japan*, 2022 (<https://www.fsa.go.jp/en/news/2022/20221207/01.pdf>, ET: 20.012.2024).
- AOKI, Shunsuke / KAWAI, Ken / MIYAKE, Akihito: *Japan: Getting a Grip*, 2020 (<https://www.iflr.com/article/2a63733ixysbvclr183e0/japan-getting-a-grip>, ET: 20.01.2025).
- AYDINER, Tuncay: *Howey Testi Nedir? İşte Bilmeniz Gereken Her Şey*, 2023 (<https://cryptopotato.com/language/tr/howey-testi-nedir/>, ET: 20.02.2025).
- BEATTIE, Elizabeth: *The Unsinkable Mark Karpeles is Willing to Give Tokyo Another Shot*, 2024 (<https://www.japantimes.co.jp/business/2024/10/21/markets/karpeles-japan-return/>, E.T: 20.02.2024).
- BHASKAR, Nirupama Devi / CHUEN, David Lee Kuo: "Bitcoin Exchanges", (Ed.) CHUEN David Lee Kuo: *Handbook of Digital Currency*, 2015, s. 559-573.
- BIELSKI, Lauren: "A New Shot for Micropayments", *American Bankers Association (ABA) Banking Journal*, 2005, Cilt 97, Sayı 4, s. 58.
- BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU: *Bilgi ve İletişim Teknolojileri Terimleri Kılavuzu* (<https://www.btk.gov.tr/kilavuzlar>, ET: 13.11.2024).
- BUCK, Jon: *Coincheck: Stolen \$534 M in NEM were Stored on Low Security Hot Wallet*, 2018 (<https://cointelegraph.com/news/coincheck-stolen-534-mln-nem-were-stored-on-low-security-hot-wallet>, ET: 10.05.2025).
- CHAROENWONG, Ben / BERNARDI, Mario: *A Decade of Cryptocurrency 'Hacks': 2011-2021*, 2021 (<https://ssrn.com/abstract=3944435> veya <http://dx.doi.org/10.2139/ssrn.3944435>, ET: 16.04.2024).
- CHENG, Evelyn: *The SEC Just Made It Clearer that Securities Laws Apply to Most Cryptocurrencies and Exchanges Trading Them*, 2018 (<https://www.cnbc.com/2018/03/07/the-sec-made-it-clearer-that-securities-laws-apply-to-cryptocurrencies.html>, ET: 21.02.2025).
- CHEUNG, Adrian (Wai-Kong) / ROCA, Eduardo / SU, Jen-Je: "Crypto-currency Bubbles: An Application of the Phillips-Shi-Yu (2013) Methodology on Mt. Gox Bitcoin Prices", *Applied Economics*, 2015, Cilt 47, Sayı 23, s. 2348-2358.
- CHUEN, David Lee Kuo: "Introduction to Bitcoin", *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*, Elsevier Science Publishing Co Inc, 2024, s. 3-28.
- CIPHERTRACE: *CipherTrace Cryptocurrency Intelligence 2018 Q3*, 2018 (<https://www.ciphertrace.com/crypt-to-aml-report-2018q3.pdf>, ET: 18.10.2024).
- CURRAN, Brian: *The History of the Coincheck Hack: One of the Largest Heists Ever*, 2018 (<https://blockonomi.com/coincheck-hack/>, ET: 15.10.2024).
- DASKALAKIS, Nikos / GEORGITSEAS, Panagiotis: *An Introduction to Cryptocurrencies: The Crypto Market Ecosystem*, Taylor & Francis, 2020.
- DİRİ, Nurcan: *Blokzincir Uygulamasında Kişisel Verilerin Tutulması*, Yüksek Lisans Tezi, Marmara Üniversitesi Fen Bilimleri Enstitüsü, İstanbul 2022.
- DOEGE, Felix: "Who is Driving Financial Market Governance of Cryptocurrencies in Japan? Actors and Institutions behind Japan's FinTech Revolution", *ASIEN: The German Journal on Contemporary Asia*, 2021, Sayı 160/161, s. 118-135.
- EGAN, Matt: *Bitcoin Exchange Mt. Gox Files for Bankruptcy After Losing Nearly \$500M*, 2014 (https://people.duke.edu/~charvey/Media/2014/FBN_February_28_2014.pdf, ET: 14.11.2024).
- ENDŌ, Genichi: "Legal Restrictions Surrounding Bitcoin: To What Extent Does Japan's Legal System Apply?", *ITU (International Telecommunication Union) Journal*, 2014, Cilt 44, Sayı 12.
- EUTERS: *Bitcoin Exchange Mt.Gox Files for Bankruptcy, Blames Hackers for Losses*, 2014 (<https://www.techcircle.in/2014/02/28/bitcoin-exchange-mt-gox-files-for-bankruptcy-blames-hackers-for-losses>, ET: 14.11.2014).

- FURUKAWA, Yuki: *Former Mt. Gox CEO Mark Karpeles Gets Suspended Jail Term*, 2019 (<https://www.bloomberg.com/news/articles/2019-03-15/former-bitcoin-baron-mark-karpeles-gets-suspended-jail-term>, E.T: 14.11.2024).
- GORCHAKOVA, Tatyana Evgenievna: “On the Development of Crypto Industry of Japan”, *Vostochnaya Aziya: Fakty i Analitika*, 2022, Cilt 3, s. 73-83.
- ISHIKAWA, Mai: “Designing Virtual Currency Regulation in Japan: Lessons from the MT Gox Case”, *Journal of Financial Regulation*, 2017, Cilt 3, Sayı 1, s. 125-131.
- KARAIKOS, Antonios: “Financial instruments: Transactions and consumer protection in Japan”, *Data Governance in AI, FinTech and LegalTech*, Edward Elgar Publishing, Londra, 2022.
- KAUR, Guneet: *The Crypto Travel Rule: An Overview*, 2023 (<https://cointelegraph.com/learn/articles/crypto-travel-rule>, ET: 26.11.2024).
- KAYA, Elif Ebrin: *Kriptografi: Bilginin Anahtarı*, 2021 (<https://bilimgenc.tubitak.gov.tr/makale/kriptografi-bilginin-anahtari>, ET: 08.05.2025).
- KREMSKYI, Oleh / KUZMENKO, Olena / ANTONIUK, Anastasiia / SMAHLO, Olha: “International Cooperation in the Investigation of Economic Crimes Related to Cryptocurrency Circulation”, *Studies of Applied Economics (Estudios de Economic Aplicada)*, 2021, Cilt 39, Sayı 6, s. 1-13.
- ЛЕВАШЕНКО, Антонина / ЕРМОХИН, Иван / КОВАЛЬ, Александра: “Перспективы Правового Регулирования Криптоэкономики И ICO В России И Других Странах”, *Экономическая Политика*, 2019, Cilt 14, Sayı 5, s. 80-99.
- MAEDA, Rick: *State of the Japanese Crypto Market*, 2024 (<https://www.prestolabs.io/research/state-of-the-japanese-crypto-market>, ET: 24.11.2024).
- MCMILLAN, Robert: *The Inside Story of Mt.Gox, Bitcoin's \$460 Million Disaster*, 2014 (<https://www.wired.com/2014/03/bitcoin-exchange/>, ET: 14.11.2024).
- MILUTINOVIĆ, Monia: “Cryptocurrency”, *EKOONOMIKA*, 2018, Cilt 64, Sayı 1, s. 95-104.
- MINISTRY OF FINANCE JAPAN: *AML/CFT/CPF in Japan*, (https://www.mof.go.jp/english/policy/international_policy/amlcftcpf/3.efforts.html, ET: 29.11.2024).
- MORITA, Hatsuru: “Regulatory and Policy Reforms in Japan”, *Law and Practice of Crowdfunding and Peer-to-Peer Lending in Australia, China and Japan*, Springer Nature, Singapore, 2010, s. 217-235.
- NAKAMOTO, Satoshi: *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008 (<https://bitcoin.org/bitcoin.pdf>, ET: 20.01.2025).
- NARAYANAN, Arvind / BONNEAU, Joseph / FELTEN, Edward / MILLER, Andrew / GOLDFEDER, Steven: “How Bitcoin Achieves Decentralization”, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, Princeton University Press, 2016, s. 27-51.
- NEFTURE SECURITY: *Mt. Gox Unveiled: The Real Story a Decade After the Collapse*, 2024 (<https://medium.com/coinmonks/mt-gox-unveiled-the-real-story-a-decade-after-the-collapse-84323be2f930>, ET: 20.02.2025).
- NORRY, Andrew: *The History of the Mt Gox Hack: Bitcoin's Biggest Heist*, 2023 (<https://blockonomi.com/mt-gox-hack/>, ET: 13.06.2025).
- PALOVAARA, Anton: *What is Crypto Margin Trading and How Does It Work?*, (<https://leverage.trading/what-is-crypto-margin-trading/>, ET: 24.11.2024).
- PETERS, Gareth W. / CHAPPELLE, Ariane / PANAYI, Efstathios: “Opening Discussion on Banking Sector Risk Exposures and Vulnerabilities from Virtual Currencies: An Operational Risk Perspective”, *Journal of Banking Regulation*, 2016, Cilt 17, Sayı 4, s. 239-272.
- POPPER, Nathaniel: *Digital Gold: The Untold Story of Bitcoin*, Penguin, Londra, 2015.
- RASTOGI, Neha / BUDHIRAJA, Ishan / AHMAD, Shahnawaz: *Cyber Attacks on Blockchain & its Prevention*, 2024 (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4936255#, ET: 13.06.2025).

- SEMENOVA, Ekaterina Vyacheslavovna / MAKAREVICH, Marina Leonidovna: “Analiz Pravovogo Regulirovaniya Kriptoalyuty v Otdel’nikh Stranakh (na primere Yaponii, SShA i Rossii)” *Innovatsionnaya Ekonomika: Perspektivy Razvitiya i Sovershenstvovaniya*, 2017, Cilt 8, Sayı 26, s. 143-146.
- SEPTIANSYAH, Veris / FITRI, Icha Cahyaning / SETYAWAN, Fendi / PRAKOSO, Bhim: “Accountability of the Financial Services Authority in Indonesia, Australia, Germany, France and Japan”, *International Journal of Social Science and Education Research Studies*, 2024, Cilt 4, Sayı 6, s. 531-544.
- SHOCKVOICE: *Bilgisayar Oyunlarının İnanılmaz Evrimi Amiga’dan VR’a*, 2022 (<https://www.youtube.com/watch?v=GQizi9szb44>, ET: 18.01.2025).
- SOLAK, Ali Bertay: *Blind Signatures ve Gizlilik*, 2023 (<https://medium.com/@alibertay/b%C3%B6l%C3%BCm-14-blind-signatures-ve-gizlilik-e364ef070959>, ET: 20.04.2024).
- SUZUKI, Yuri / OCHIAI, Takafumi / OUE, Ryosuke / KANEHISA, Naoki / TANIZAKI, Kenicki: *Japan: A New Dose of Regulation and Promotion*, 2019 (www.aplawjapan.com/archives/pdf/A-fresh-dose-of-regulation-and-promotion.pdf, ET: 25.10.2024).
- SYGNA: *Guide: Japan Crypto Asset Regulation* (<https://www.sygna.io/blog/japan-crypto-asset-regulation-guide/>, ET: 26.11.2024).
- SYGNA: *Japan’s History of Crypto Asset Regulation: 2014-2020* (<https://www.sygna.io/blog/japan-crypto-regulation-history-2014-2020>, ET: 15.11. 2024).
- ŞAAN, Tayfun / TİLTAY, Muhammet Ali / İŞLEK, Mahmut Sami: “1980-2000 Yılları Arasındaki Video Oyun Sektörünün İncelemesi: Nintendo ve Sega Örneği”, *Anadolu Üniversitesi Sosyal Bilimler Dergisi*, 2022, Cilt 22, Sayı3, s. 911-930.
- TROZZE, Arianna / KAMPS, Josh / AKARTUNA, Eray Arda / HETZEL, Florian J./ KLEINBERG, Bennett / DAVIES, Toby / JOHNSON, Shane D: “Cryptocurrencies and Future Financial Crime”, *Crime Science*, 2022, Cilt 11, Sayı 1, s. 1-35.
- TSUCHIYA, Yoichi / HIRAMOTO, Naoki: “How Cryptocurrency is Laundered: Case Study of Coincheck Hacking Incident”, *Forensic Science International: Reports*, 2021, 4(100241).