

Konu 07 – İnternet Bankacılığı, Elektronik Para, Dijital Para ve Kripto Para Hukuku



Konu 07 – İnternet Bankacılığı, E Para, Dijital Para ve Kripto Para Hukuku

I. İnternet Bankacılığı Dolandırıcılıkları ve Hukuki Sorumluluk

İnternet bankacılığı dolandırıcılıkları çoğunlukla iki adımda gerçekleştirilmektedir.

Birinci adımda, hacker diye tabir edilen kişiler müşterinin hesap bilgileri olan şifre ve parola gibi bilgilerini ele geçirmektedir.

Subject 07- Online Banking- Electronic Money- Crypto Currency- Central Bank Digital Currencies



Subject 07: Online Banking- Electronic Money, Crypto Currency, and Central Bank Digital Currencies

I. Online Banking Frauds and Legal Liability

Internet banking frauds are usually carried out in two steps.

In the first step, individuals known as hackers obtain the customer's account information, such as passwords and PINs.

İkinci adımda, hacker bu müşterinin bilgileri kullanarak mağdur kimsenin hesabındaki parayı çekmek için bir başka hesaba göndererek dolandırıcılık eyleminde bulunur.

İlk işlem için hacker müşterinin kişisel bilgilerini ele geçirmek için çoğunlukla aynı olmak üzere çok çeşitli yöntemler kullanır.

Casus programlar ile şifreleri ele geçiren korsanlar, bu şifreler ile rahatlıkla sanki hesap sahibiymiş gibi işlem yaparlar.

İkinci aşamada ise genellikle sahte kimliklerle açılan hesaplara aktarılan paralar ya banka şubeleri veya ATM'ler aracılığıyla nakit olarak çekilmekte, kredi kartlarına yüklemeler yapıp harcamalar yapılmakla veya son dönemlerde olduğu gibi cep telefonlarına kontör yüklenebilmektedir. Görüldüğü üzere bu tip dolandırıcılık olaylarında müşterinin şifresinin ele geçirilmiş olması eylemin tamamlanması ve zararın doğması için yeterli bir etken değildir. Nitekim son dönemlerde bu tip dolandırıcılık eylemleri neticesinde çalınan paralar harcanmadan bloke konulmak suretiyle müşteri hesabına geri döndürülebilmektedir. Bu durumu bir eve girip hırsızlık yapan ve ancak çaldığı malları ev dışarısına çıkaramayarak evin içerisinde bırakan kişinin durumuna benzetebiliriz.

- **T.C. Yargıtay Hukuk Genel Kurulu Esas: 2012/11-550 Karar: 2012/820 Karar Tarihi: 21.11.2012**

In the second step, the hacker uses this information to commit fraudulent activities by transferring the victim's money to another account.

For the initial step, hackers typically employ various methods to obtain the customer's personal information, which often involve using similar approaches.

Pirates who acquire passwords through spyware can easily conduct transactions as if they were the account owner using these obtained passwords.

In the second stage, stolen funds are typically withdrawn as cash through bank branches or ATMs, loaded onto credit cards for spending, or, as seen in recent times, used to top up mobile phone credits. It's evident that merely obtaining the customer's password is not sufficient to complete the action and cause harm in cases of this kind of fraud. In fact, stolen funds can be blocked and returned to the customer's account before they are spent. This situation can be likened to someone breaking into a house and leaving stolen items inside because they cannot take them outside.

- **Turkish Supreme Court General Assembly Main Case: 2012/11-550 Decision: 2012/820 Decision Date: 21.11.2012**

Hukuk Genel Kurulu önüne gelen uyuşmazlık; davalı banka nezdindeki hesapta bulunan paranın internet bankacılığı aracılığı ile davacının iradesi dışında üçüncü kişilerce çekilmesinde davacıya atfedilecek bir kusurun bulunup bulunmadığı noktasında toplanmaktadır.

Uyuşmazlığın çözümü için öncelikle, internet bankacılığı kavramı ile bankaların mudileriyle yaptığı sözleşmelerin hukuki niteliğinin açıklanmasında yarar bulunmaktadır.

İnternet, birden fazla haberleşme ağının (network) bilgisayarlar aracılığıyla meydana getirdikleri bir iletişim ortamıdır. (Sözer, B.; Elektronik Sözleşmeler, İst. 2002, S.7)

Günümüzde internet, tüm dünya üzerine yayılmış olan çok geniş bir bilgisayar ağı durumunu gelmiştir. **Bu iletişim ağından yararlanan internet bankacılığı; teknolojide meydana gelen gelişmeler sonucu ortaya çıkan ve hemen hemen bütün bankacılık işlemlerinin internet üzerinden yapılabilmesini sağlayan elektronik bir bankacılık türüdür. Es söyleyişle, interaktif bankacılık, bankacılık hizmetlerinin internet üzerinden sunulduğu bir bankacılık türü olarak da tanımlanabilir.**

Bankalar tarafından hazırlanan sözleşmelerde yer alan yaygın tarifile internet bankacılığı ise; şahsın kablolu, kablosuz iletişim sistemleri ile teknik şartlara haiz bilgisayar, GSM, telefon gibi araçlar üzerinden ve internet-wap aracılığı ile otomatik, sesli yanıt

The dispute brought before the General Assembly of the Court of Cassation revolves around whether there is any negligence on the part of the plaintiff in the case of money from the account at the defendant bank being withdrawn by third parties through internet banking without the plaintiff's consent.

In order to resolve the dispute, it is first beneficial to clarify the legal nature of the concept of internet banking and the contracts entered into between banks and their customers.

The internet is a communication environment created through computers by multiple communication networks. (Sözer, B.; Electronic Contracts, Istanbul 2002, p.7)

Today, the internet has become a vast global computer network. **Internet banking, which benefits from this communication network, is an electronic form of banking that allows almost all banking transactions to be conducted online due to technological advancements. In other words, interactive banking can also be defined as a form of banking where banking services are offered through the internet.**

As defined in common terms in contracts prepared by banks, internet banking is a method where individuals can carry out all kinds of transactions on their bank accounts, within the rules and limits set by the bank, using computers, GSM, phones, and other devices via cable, wireless communication systems, and technical

sistemi ile şifre ve parolayı kullanarak, bankanın belirleyeceği kurallar ve limitler dahilinde şahsın banka hesapları üzerinde her türlü işlem yapma yöntemidir.

İnternet bankacılığındaki en önemli sorun, hiç kuşkusuz güvenlik sorunudur. Güvenli bir internet bankacılık hizmetinin sunulmasında, böyle bir hizmetin alınmasında, hem bankanın hem de müşterinin üzerine düşen yükümlülükler ve sorumluluklar vardır. Bu bağlamda, internet bankacılığı hizmetini müşterilerine bankalar sunduğuna göre, bu sistemin güvenliğine yönelik tüm tedbirleri almaları ve sistemi bilinen en son teknolojik gelişmeye uygun hale getirmeleri büyük önem taşımaktadır. **Hiç kuşkusuz, müşterilerin de internet bankacılığında kullanılmak üzere kendilerine verilen kullanıcı adı, şifresi ve diğer bilgileri üçüncü kişilerin eline geçmesini önleyecek gerekli tedbirleri almaları ve bu konuda azami özeni göstermeleri gereklidir.**

İnternet ortamında ortaya çıkabilecek siber suç eylemleri, büyük ölçüde bu ortamı sağlayan bilgisayar sistemi veya verilerine çeşitli maksatlarda ve haksız olarak yapılan müdahaleleri ve bu sistemde zararlı içerikli bir takım yayınları bulundurmak şeklinde olmaktadır. Örneğin, bir bilgisayar sistemine zarar verme amacı taşıyan <hacking>, verilerin değiştirilmesi, bir bilgisayar sistemine zarar verici amaçlar için yetkisiz e-mailler (spam), virüsler, <truva atı> gibi zarar verici kodların ya da çocuk pornografisinin gönderilmesi gibi eylemler bu niteliktedir. ((Mahmut Koca, Ünal Tekinalp'e Armağan, C.3., İst. 2003, s.789-790)

conditions, as well as through the internet-wap, with an automatic, voice response system using a password and PIN.

The most significant issue in internet banking is undoubtedly security. In providing and receiving secure internet banking services, both the bank and the customer have obligations and responsibilities. In this context, since banks offer internet banking services to their customers, it is of utmost importance for them to take all necessary precautions to ensure the security of this system and make it compliant with the latest technological developments. **Without a doubt, customers should also take necessary measures to prevent their username, password, and other information provided for internet banking from falling into the hands of third parties and exercise the utmost care in this regard.**

Cybercrime actions that can occur in the online environment largely involve unauthorized interference with computer systems or data for various purposes, often causing harm to the system, and the presence of some harmful content in this system. For instance, actions with the intent of damaging a computer system, altering data, sending unauthorized emails for malicious purposes (spam), viruses, and harmful codes such as Trojan horses, or the distribution of child pornography fall into this category. (Mahmut Koca, Ünal Tekinalp Armağan, Vol. 3, Istanbul 2003, pp. 789-790)

Bankacılık işlemleri alanında sözleşme özgürlüğü ilkesinin etkili bir şekilde uygulanmaması nedeniyle bankaların sorumluluğu konusunda özel düzenlemelerin ve yorumların yapılması da bir gerekliliktir. (Ahmet Battal, Güven Kurumu Nitelendirmesi Işığında Bankaların Hukuki Sorumluluğu, Ankara, 2001, s.1)

İnternet bankacılığında asıl sorun, hiçbir kusuru olmayan hesap sahibinin internet bankacılığı sisteminden dolayı zarar görmesi halinde durumun ne olacağı noktasında toplanmaktadır.

Bankalar, yazılı veya sözlü duyurularla halktan faiz veya ivaz karşılığında topladıkları paraları Türk ekonomisinin güçlenmesi doğrultusunda değerlendiren ve aynı zamanda bu mevduatlardan para kazanan kuruluşlardır. Bankalar kendilerine yatırılan paraları istenildiğinde veya belli bir vadede aynı veya misli olarak iade etmekle yükümlüdürler. **Bu tanımlamaya göre mevduat ödünç (karz) ile usulsüz tevdi sözleşmelerinin niteliklerini taşıyan kendine özgü bir sözleşmedir. Bunun sonucu mevduatın niteliğine uygun düştüğü oranda karz (ödünç) veya usulsüz tevdi hükümlerinin kıyasen uygulanması gerekir (aynı ilkelere HGK'nun 15.06.1994, 1994/11-178-398 sayılı kararında da yer verilmiştir)**

Bilindiği üzere, ödünç sözleşmesi 818 sayılı Borçlar Kanunu'nun (BK) <Karz akdi> başlıklı 306. vd. maddesinde düzenlenmiş olup, anılan yasa hükmü; <Karz, bir akittir ki onunla ödünç veren, bir miktar paranın yahut diğer bir misli şeyin mülkiyetini ödünç alan kimseye nakil ve bu kimse dahi buna karşı miktar ve vasıfta müsavi aynı neviden şeyleri

Special regulations and interpretations regarding the liability of banks are necessary due to the ineffective application of the principle of freedom of contract in the field of banking transactions. (Ahmet Battal, Legal Liability of Banks in the Light of the Trust Agency Classification, Ankara, 2001, p.1)

The main issue in internet banking revolves around what will happen when an account holder with no fault suffers damage due to the internet banking system.

Banks are institutions that collect money from the public with interest or profit-sharing arrangements through written or verbal announcements and, at the same time, make profits from these deposits while contributing to the strengthening of the Turkish economy. Banks are obliged to return the deposited money, either upon request or at a specified maturity, in kind or in a similar manner. **In this respect, a deposit contract, which has characteristics of a loan (Karz) or an irregular deposit agreement, should be treated analogously as the qualities of the deposit allow (this principle is also mentioned in the decision of the General Assembly of the Court of Cassation dated 15.06.1994, numbered 1994/11-178-398).**

As is known, the loan agreement is regulated in Articles 306 and subsequent articles under the title "Contract of Loan" of the Turkish Civil Code No. 818. According to this provision, a loan is defined as follows: "A loan is an agreement by which the lender transfers to the borrower the ownership of a certain amount of money or other equivalent things, and

geri vermekle mükellef olur.> şeklindedir. Bu hükme göre; ödünç alan konumundaki banka, kendisine ödünç verilen parayı kararlaştırılmış faizi ile birlikte iadeye mecburdur.

Bu hükme paralel düzenleme 5411 sayılı Bankalar Kanunu'nun 61. maddesinde yer almaktadır. Anılan maddenin birinci fıkrasında; <4721 sayılı Türk Medenî Kanununun rehinlere ve hapis hakkına, BK'nun alacağın devir ve temlikine, takasa dair hükümleri ile diğer kanunların verdiği yetkiler ve koyduğu yükümlülükler saklı kalmak şartıyla mevduat ve katılım fonu sahiplerine ödenmesi gereken tutarları geri alma hakları hiçbir suretle sınırlandırılmaz.> şeklinde düzenleme yapılmıştır.

Vedia akitlerinde usulsüz tevdi durumunun hükme bağlandığı BK'nun 472/1. maddesi uyarınca da usulsüz tevdi durumunda paranın nef'i ve hasarı mutlak şekilde saklayana geçecektir.

TTK'nun 20. maddesi¹ hükmüne göre, banka basiretli tacirden beklenen özen derecesini de göstermek zorundadır, aksi halde hafif kusurundan dahi sorumludur. (Mustafa Çeker, Hukuki Yönüyle Banka Mevduatı, Adana 2004, S.281-233) Bu sorumluluğu kaldırmaya

the borrower is obliged to return to the lender an equal amount and equivalent things of the same kind, together with interest, if agreed." Consequently, the bank in the position of the borrower is obligated to return the borrowed money, along with interest if specified.

This provision is also regulated in Article 61 of Law No. 5411 on Banks. The first paragraph of that article states, "Without prejudice to the provisions of the Turkish Civil Code No. 4721 regarding pledges and the right of retention, the transfer of debt, and assignment under the Turkish Commercial Code, as well as the authority and obligations imposed by other laws, the right of deposit and Participation by fund holders to recover the amounts payable to them cannot be restricted in any way."

In the case of irregular deposits, as stipulated in Article 472/1 of the Turkish Civil Code, the absolute right to the money in case of an irregular deposit will pass to the person who holds it.

According to Article 20² of the Turkish Commercial Code, a bank is also required to demonstrate the degree of care expected from a prudent merchant; otherwise, it can be held liable even for a slight

¹ Bahsedilen hüküm 6762 Sayılı yürürlükten kalkmış olan Türk Ticaret Kanunu'dur. 6102 Sayılı Yeni Türk Ticaret Kanununda aynı düzenleme 18/2 maddede mevcuttur: "Her tacirin, ticaretine ait bütün faaliyetlerinde basiretli bir iş adamı gibi hareket etmesi gerekir"

² The aforementioned provision No. 6762 is the Turkish Trade Act, which has expired. The same provision is contained in article 18/2 of the New Turkish Trade Act No. 6102: "Every trader must act as a prudent businessman in all activities relating to his trade."

yönelik sözleşmeler de geçerli değildir. Zira BK'nun 99 ve 100/3 maddesine göre, hile ve ağır kusurun varlığı halinde borçluyu sorumluluktan kurtaran sözleşme şartları ahlak ve dürüstlük kuralına aykırı olduğundan geçersizdir.

Sorumsuzluk anlaşmalarına getirilen sınırlama daha güçlü durumdaki bankalara karşı daha zayıf durumdaki kişiyi koruma (sosyal adalet) nedenine dayanmaktadır.

Bankalar, bir güven kurumları olup, özel yasa ile kurulan ve kendilerine alanlarında çeşitli imtiyazlar tanınan, topladıkları mevduatı sahteciliklere karşı özenle korumak zorunda olan kuruluşlardır. Objektif özen borcu altında bulunan bankalar, hafif kusurlarından dahi sorumludurlar.

Bankalar, diğer alanlarda olduğu gibi, internet ortamında yapılacak işlemlerde de sistem güvenliğini sağlama yükümlülüğü altındadırlar. Bu çerçevede, banka, mevduat sahiplerinin güvenli bir şekilde işlem yapabilmesini için gerekli güvenlik altyapısını hazırlamak zorundadır. Bu kapsamda, bankanın, interaktif bankacılık işlemleri sırasında şifre bilgilerinin üçüncü kişilerce ele geçirilmesini önleyecek bir güvenlik mekanizması oluşturması gereklidir. Sistem güvenliğinin sağlanamamasından kaynaklanan zararların sorumluluğu bankaya ait olacaktır. (Mustafa Çeker, İnternet Bankacılığı İşlemlerindeki Usulsüzlüklerden Bankaların Sorumluluğu, S.8)

defect. Contracts aimed at relieving this liability are not valid. This is because, as per Articles 99 and 100/3 of the Turkish Civil Code, contracts that exempt the debtor from liability in cases of fraud and gross negligence are considered unethical and against the principles of good faith, and therefore, invalid.(Mustafa Çeker, Hukuki Yönüyle Banka Mevduatı, Adana 2004, S.281-233)

Limitations placed on exemption agreements are based on the purpose of protecting weaker individuals against stronger entities (social justice).

Banks are considered institutions of trust, established by special laws, granted various privileges in their fields, and obliged to protect deposits against fraud carefully. Banks are under an objective diligence obligation, meaning they are responsible even for slight defects.

Banks, just like in other areas, have an obligation to ensure system security in transactions conducted in the online environment. Within this framework, the bank must establish a security mechanism that prevents third parties from obtaining password information during interactive banking transactions to enable depositors to transact securely. If system security cannot be maintained, the liability for damages arising from this failure will be attributed to the bank.(Mustafa Çeker, İnternet Bankacılığı İşlemlerindeki Usulsüzlüklerden Bankaların Sorumluluğu, S.8)

Bu açıklamalar ışığında, internet bankacılığı faaliyeti yürüten bankalar, bankadaki paranın internet ortamında üçüncü kişilerce usulsüz olarak havale edilmesi durumunda mudinin parasını yukarıda açıklanan mevzuat çerçevesinde iade etmekle yükümlüdürler. Usulsüz işlemlerle çekilen paralar aslında doğrudan doğruya bankanın zararı niteliğinde olup, mevduat sahibinin bankaya karşı alacağı aynen devam eder. Banka, usulsüz işlemin gerçekleşmesinde mevduat sahibinin müterafik kusurunun bulunduğunu ispat etmesi halinde tazminatta indirim isteyebilir.

Genel Kurulda bir kısım üyeler; internet bankacılığı sisteminden yararlanmak için gerekli şifre ve parola benzeri kişisel bilgilerin bankanın bilgisayar sistemine dışarıdan girilerek elde edilemediğini, müşteri bilgisayarlarına dışarıdan müdahale yöntemleriyle bu bilgilerin ele geçirildiğini, dolayısıyla kişisel bilgisini gerektiği gibi muhafaza etmeyen müşterilerin bilgisayar korsanlıklarıyla oluşan zararlardan sorumlu olmalarının gerektiğini belirtmişlerse de, bu görüş, kurul çoğunluğunca benimsenmemiş ve günümüzün teknolojik seviyesinde elektronik imza vb. gibi gelişmiş güvenlik önlemlerinin alınmasının mümkün bulunduğu ve bu tedbirleri almanın hizmet sunucusu olan bankaların yükümlülüğünde olduğu ifade edilmiştir.

Somut olayda davalı banka, davacının müterafik kusurunu ve suç teşkil edebilecek bir eyleminin varlığını da kanıtlayamadığından

In light of these explanations, banks engaged in internet banking activities are obligated to reimburse depositors' funds in the event that the funds are transferred irregularly by third parties in the online environment, in accordance with the legislation explained above. Funds withdrawn through irregular transactions are essentially considered a loss incurred by the bank, and the depositor's claim against the bank remains intact. The bank may request a reduction in compensation if it can prove that the depositor was partly at fault for the occurrence of the irregular transaction.

Some members in the General Assembly argued that certain personal information, such as passwords and similar data necessary for utilizing internet banking, cannot be obtained by external access to the bank's computer system. They argued that these details are typically acquired through external interventions on customers' computers, and as such, customers who fail to safeguard their personal information adequately should be held responsible for losses caused by computer hacking. However, this viewpoint was not adopted by the majority of the Assembly. It was stated that, given the current level of technology, it is possible to implement advanced security measures like electronic signatures, and it is the responsibility of service-providing banks to take such precautions.

In the specific case at hand, the defendant bank could not prove the plaintiff's contributory negligence or any actions that could constitute a crime. Consequently, the defendant bank is obliged to

davacı mudinin kendisine tevdi ettiği mevduatı aynen iade etmekle yükümlüdür.

Bu itibarla; Hukuk Genel Kurulu'nca da benimsenen Özel Daire bozma kararına uyulmak gerekirken, önceki kararda direnilmesi usul ve yasaya aykırıdır.

Bu nedenle direnme kararı bozulmalıdır.”

- **Yargıtay 11. Hukuk Dairesi Esas Numarası: 2017/4888 Karar Numarası: 2019/2015 Karar Tarihi: 11.03.2019**

“ Dava, davalı banka nezdinde açılmış olan hesapta bulunan paranın davacının bilgisi ve izni dışında internet yolu ile yapılan işlemler sonucu çekilmesi suretiyle uğranılan zararın tazmini istemine ilişkindir. Bankalar kendilerine yatırılan paraları mudilere istendiğinde veya belli bir vadede aynı veya misli olarak iade etmekle yükümlüdür. (4491 sayılı Yasa ile değişik 4389 sayılı Bankalar Kanunu'nun 10/4 ve 5411 sayılı Bankacılık Kanunu'nun 61. maddesi) Bu tanımlamaya göre, mevduat ödünç ile usulsüz tevdi sözleşmelerinin niteliklerini taşıyan kendine özgü bir sözleşmedir. BK'nın 306. ve 307. maddeleri uyarınca ödünç alan, akdın sonunda ödünç verilen parayı eğer kararlaştırılmışsa faizi ile iadeye mecburdur. Aynı Yasa'nın 472/1. maddesi uyarınca usulsüz tevdi paranın nef'i ve hasarı mutlak şekilde saklayana geçtiği için ayrıca açıklamaya gerek kalmadan saklayan bu parayı kendi yararına kullanabilir. **Bu açıdan değerlendirildiğinde, usulsüz işlemle çekilen paralar aslında doğrudan doğruya bankanın zararı niteliğinde olup, mevduat sahibinin bankaya karşı alacağı aynen devam etmektedir.**

reimburse the plaintiff for the deposit that the plaintiff entrusted to them.

In light of this, adherence to the Special Chamber's decision in line with the General Assembly's decision should have been followed. However, resisting the previous decision is procedurally and legally incorrect.

Therefore, the decision to resist should be overturned.”

- **Turkish Supreme Court 11th Civil Division E.2017/4888 K. 2019/2015 Date: 11.03.2019**

"The case pertains to the compensation of damages suffered due to the withdrawal of the funds in the account opened with the defendant bank, as a result of transactions made via the internet without the knowledge and consent of the plaintiff. Banks are obliged to return the funds deposited with them when requested by depositors or within a specified period, either in kind or with equivalent. (Law No. 4491 amended Banking Law No. 4389 and Article 61 of Banking Law No. 5411) According to this definition, it is a unique contract that possesses the characteristics of a deposit with a loan and unlawful deposit agreements. According to Articles 306 and 307 of the Turkish Civil Code, the borrower must return the borrowed money along with the agreed interest at the end of the agreement. Furthermore, Article 472/1 of the same Law stipulates that, in the case of an unlawful deposit, the ownership and damages of the money are transferred to the one who keeps it absolutely; hence, they can use this money in their favor without further explanation. **Therefore, from this perspective, the funds withdrawn through unauthorized transactions actually constitute a direct loss for the bank, and the**

Usulsüz işlemlerin gerçekleşmesinde ispatlandığı takdirde mevduat sahibinin kusurundan söz edilebilir ve banka bu kusur oranı üzerinden hesap sahibinin alacağından mahsup talebinde bulunabilir. Somut olayda davacıya ait para, davacı hesabından dava dışı kimliği belirli kişi adına hesaptan bir başka hesaba bankaya karşı gerçekleştirilen sahtecilik işlemi ile havale edilmiş olup, bu durum davalı bankayı aldığı mevduatı iade etme yükümlülüğünden kurtarmayacaktır. Dosya kapsamından, işlemlerde davacının üçüncü kişilerle el ve işbirliği ile veya başka şekilde kusurlu davrandığı kanıtlanmamıştır. Davalı banka tarafından, hesapta bulunan paranın güvenliğinin tam olarak sağlanmadığı, kötüniyetli kişilerin işlemlerine karşı korunamadığı, bu kişilerin eylem ve işlemlerine karşı koruyacak etkili mekanizmayı, güvenlik önlemlerini geliştirmediği, bu önlemleri kullanmayı, müşterileri için zorunlu hale getirmediği anlaşılmaktadır. O halde, davalı bankanın hesaptan çekilen tüm paradan sorumlu olduğunun, ilke olarak kabulü gerekir. Açıklanan nedenlerle mahkemece, davalı bankanın mevduatı iade yükümlülüğünün devam ettiği kabul edilerek sonucuna göre bir karar verilmek gerekirken, yazılı gerekçelerle hüküm tesisi doğru görülmemiş, kararın temyiz eden davacı yararına bozulmasına karar vermek gerekmiştir.”

depositor's claim against the bank remains unaffected. If it is proven that the unauthorized transactions occurred due to the plaintiff's collusion with third parties or in another way, the plaintiff may be found at fault, and the bank may request a setoff from the plaintiff's receivables based on the degree of this fault. In the specific case, the money belonging to the plaintiff was transferred from the plaintiff's account to another account under the name of an identified person, with a fraudulent transaction carried out against the bank. This situation will not exempt the defendant bank from its obligation to return the deposited funds. It is not proven from the case files that the plaintiff acted in collusion with third parties in the transactions or acted negligently in any other way. It is evident that the defendant bank did not ensure the complete security of the funds in the account, failed to protect it from malicious individuals' transactions, did not develop effective mechanisms and security measures against these individuals' actions and transactions, and did not make the use of these measures mandatory for its customers. Therefore, it should be accepted as a principle that the defendant bank is responsible for the entire amount withdrawn from the account. For the reasons explained, it should be ruled by the court that the defendant bank's obligation to return the deposit still continues, and a judgment should be issued accordingly. However, the decision, with its written justifications, was erroneously deemed correct, and the decision should be reversed in favor of the appellant for the reasons explained."

- **T.C Yargıtay 19. Hukuk Dairesi Esas: 2016 / 9607 Karar: 2017 / 5061 Karar Tarihi: 15.06.2017**

“Davacı vekili, müvekkilinin kartından bilgisi dışında 1.200-USD tutarlı harcama yapıldığını, müvekkilinin bu harcamayı bildiren mesajı alır almaz davalı bankayı arayarak işlemlerin bilgisi dışında olduğunu, onay vermediğini bildirmesine rağmen davalı tarafından herhangi işlem yapılmayıp borcun kartına yansıtıldığını, bu miktarın müvekkili tarafından ödendiğini, davalının yeterli önlemleri almayarak bu usulsüz harcamadan sorumlu olduğunu ileri sürerek, müvekkilinin ödemiş olduğu miktarın iadesine karar verilmesini talep ve dava etmiştir.

Davalı vekili, davaya konu işlemin "3D ..." sisteminden şifre girilerek yapıldığını, 3D güvenlik üyesi iş yerlerinden kart şifresi ve diğer bilgileri girilme suretiyle yapılan işlemlerden kart hamilinin sorumlu olduğunu ileri sürerek davanın reddini istemiştir.

Mahkemece, yapılan yargılama ve benimsenen bilirkişi raporuna göre, davaya konu işlemin 3D ... sistemi kullanılarak gerçekleştirildiği, bu sistemin internet üzerinden kredi kartı ile yapılan alışverişlerde güvenliği sağlamayı amaçladığı, internet üzerinden yapılacak dolandırıcılığın büyük bilgi birikimi

- **Turkish Supreme Court 19th Civil Chamber, Reference Number: 2016/9607, Decision Number: 2017/5061, Decision Date: June 15, 2017**

"The plaintiff's attorney has filed a lawsuit, stating that an expenditure of 1,200 USD was made from the client's card without their knowledge. The plaintiff claims that as soon as they received a message notifying them of this transaction, they immediately contacted the defendant bank to report that these transactions were unauthorized and that they did not give consent. However, despite the plaintiff's immediate action, the defendant did not take any measures, and the debt was charged to the plaintiff's card. The plaintiff alleges that the amount was paid by the client and that the defendant is responsible for this unauthorized expenditure due to their failure to take sufficient precautions. The plaintiff requests a decision for the refund of the amount paid by the client.

The defendant's attorney claims that the transaction in question was made by entering a password through the '3D Secure' system, and that the cardholder is responsible for transactions made by entering card passwords and other information from 3D security member merchants. As a result, the defendant requests the dismissal of the lawsuit.

According to the court's judgment based on the conducted trial and accepted expert report, it was determined that the transaction in question was carried out using the '3D Secure' system. This system aims to provide security for credit card transactions made over the internet. Committing fraud over the internet requires a substantial

gerektirdiği, bankaların müşterilerin internet işlemlerini sabit şifreler kullanarak yapmalarını engelleyerek her seferinde farklı şifre kullanmalarını sağlaması gerektiği, davalı bankanın farklı şifre kullandığına ilişkin bilgi ve belge olmadığı, işlemler sırasında yeterli güvenliği sağlayamayan davalı bankanın kusurlu olduğu gerekçesiyle davanın kabulüne karar verilmiş, hüküm davalı vekili tarafından temyiz edilmiştir.”

II. Ödeme ve Menkul Kıymet Mutabakat Sistemler, Ödeme Hizmetleri ve Elektronik Para Kuruluşları

1. Ödeme ve Menkul Kıymet Mutabakat Sistemleri ve Ödeme Hizmetleri

27/6/2013 Tarihli ve 28690 sayılı Resmi Gazetede yayımlanan 6493 Sayılı [Ödeme Ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri Ve Elektronik Para Kuruluşları Hakkında Kanun](#)da yer alan Tanımlara göre;

“Ödeme kuruluşu: Ödeme hizmeti sağlamak ve gerçekleştirmek için bu Kanun kapsamında yetkilendirilmiş tüzel kişi” şeklinde tanımlanmıştır.

Kanunun 12. maddesine göre ödeme hizmetleri aşağıdaki faaliyetleri içermektedir;

amount of knowledge. Banks should ensure that customers perform internet transactions using different passwords each time, rather than fixed passwords, to prevent this. There was no information or evidence indicating that the defendant bank used different passwords. Since the defendant bank did not provide sufficient security during the transactions, the court concluded that they were at fault, and the lawsuit was accepted. The judgment was subsequently appealed by the defendant's attorney."

II. Payment And Securities Settlement Systems, Payment Services And Electronic Money Institutions

1. Payment And Securities Settlement Systems, Payment Services

In accordance with the definitions set forth in [Law No. 6493 on n Payment and Securities Settlement Systems, Payment Services, and Electronic Money Institutions](#) published in the Official Gazette dated June 27, 2013, and numbered 28690, the following terms are defined as follows:

“Payment institution: Legal person authorized pursuant to this Law to provide and execute payment services”

In accordance with Article 12 of the law, payment services encompass the following activities:

a) Ödeme hesabına para yatırılması ve ödeme hesabından para çekilmesine imkan veren hizmetler de dâhil olmak üzere ödeme hesabının işletilmesi için gerekli tüm işlemleri,

b)Ödeme hizmeti kullanıcısının ödeme hizmeti sağlayıcısı nezdinde bulunan ödeme hesabındaki fonun aktarımını içeren, bir defaya mahsus olanlar da dâhil doğrudan borçlandırma işlemi, ödeme kartı ya da benzer bir araçla yapılan ödeme işlemi ile düzenli ödeme emri dâhil para transferini,

c) Ödeme aracının ihraç veya kabulünü,

ç) Para havalesini,

d)Gönderen tarafından ödeme işleminin yapılmasına ilişkin onayın bir bilişim veya elektronik haberleşme cihazı aracılığıyla verildiği ve ödemenin ödeme hizmeti kullanıcısı ile mal veya hizmet sağlayan arasında sadece aracı olarak faaliyet gösteren bir bilişim veya elektronik haberleşme işletmecisine yapıldığı ödeme işlemini,

e) Fatura ödemelerine aracılık edilmesine yönelik hizmetleri,

f) (Ek:12/11/2019-7192/8 md.) Ödeme hizmeti kullanıcısının isteği üzerine başka bir ödeme hizmeti sağlayıcısında bulunan ödeme hesabıyla ilgili sunulan ödeme emri başlatma hizmetini,

a) All the transactions required for operating a payment account including the services enabling cash to be placed on and withdrawn from a payment account,

b) Execution of payment transactions, including transfer of funds on a payment account with the user's payment service provider, direct debits, including one-off direct debits, payment transactions through a payment card or a similar device, credit transfers including standing orders,

c) Issuing or acquiring payment instruments,

ç) Money remittance,

d) Execution of payment transaction, where the consent of the payer to execute a

payment transaction is given by means of any telecommunication, digital or IT device and the payment is made to the telecommunication, IT system or network operator, acting only as an intermediary between the payment service user and the supplier of the goods and services,

e) Corresponding services enable bill payments

f) (Amendment: 12/11/2019-7192/8 Article) The service of initiating a payment order related to a payment account held with another payment service provider upon the request of the payment service user.

g) (Ek:12/11/2019-7192/8 md.) Ödeme hizmeti kullanıcısının onayının alınması koşuluyla, ödeme hizmeti kullanıcısının ödeme hizmeti sağlayıcıları nezdinde bulunan bir veya daha fazla ödeme hesabına ilişkin konsolide edilmiş bilgilerin çevrim içi platformlarda sunulması hizmetini,

ğ) (Ek:12/11/2019-7192/8 md.) Ödemeler alanında toplam büyüklük veya etki alanı açısından Bankaca belirlenecek seviyeye ulaşan diğer işlem ve hizmetleri ifade eder.

13. Maddede yer alan hükme göre Ödeme hizmeti Sağlayıcıları sınırlı sayıdadır ve banka ve ödeme hizmeti sağlayıcısı dışındaki kişiler ödeme hizmeti sunamazlar;

a) 5411 sayılı Kanun kapsamındaki bankalar,

b) Elektronik para kuruluşları,

c) Ödeme kuruluşları,

ç) (Ek: 17/4/2017-KHK/690-68 md.; Aynen kabul: 1/2/2018-7077/58 md.) Posta ve Telgraf Teşkilatı Anonim Şirketi,

ödeme hizmeti sağlayıcısıdır.

g) (Amendment: 12/11/2019-7192/8 Article) The service of initiating a payment order related to a payment account held with another payment service provider upon the request of the payment service user,

ğ) (Amendment: 12/11/2019-7192/8 Article) The service of providing consolidated information regarding one or more payment accounts held with one or more payment service providers on online platforms, subject to obtaining the approval of the payment service user,

According to the provision in Article 13, Payment Service Providers are limited in number, and individuals or entities outside of banks and payment service providers cannot offer payment services:

a) Banks within the scope of Law No. 5411,

b) Electronic money institutions,

c) Payment service providers,

ç) (Amendment: 17/4/2017-Decree Law/690-68th Article; Accepted as is: 1/2/2018-Law No. 7077/58th Article.) Post and Telegraph Corporation Incorporated Company are considered payment service providers.

2. Elektronik Para Kuruluşları

27/6/2013 Tarihli ve 28690 sayılı Resmi Gazetede yayımlanan 6493 Sayılı [Ödeme Ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri Ve Elektronik Para Kuruluşları Hakkında Kanun](#)da yer alan Tanımlara göre;

“Elektronik para: Elektronik para ihraç eden kuruluş tarafından kabul edilen **fon karşılığı ihraç edilen,** elektronik olarak saklanan, bu Kanunda tanımlanan ödeme işlemlerini gerçekleştirmek için kullanılan ve elektronik para ihraç eden kuruluş dışındaki gerçek ve tüzel kişiler tarafından da ödeme aracı olarak kabul edilen parasal değer

Elektronik para kuruluşu: Bu Kanun kapsamında elektronik para ihraç etme yetkisi verilen tüzel kişi” şeklinde tanımlanmıştır.

Elektronik para şirketlerinin kurulabilmesi için bir takım şartlar öngörülmüştür.

1. [Ödeme Hizmetleri ve Elektronik Para İhracı İle Ödeme Kuruluşları ve Elektronik Para Kuruluşları Hakkında Yönetmelik](#) 11. maddesinde belirtilen şekilde **Merkez Bankasından faaliyet izni alınması** zorunludur.

2. Electronic Money Institutions

In accordance with the definitions provided in [Law No. 6493 on Payment and Securities Settlement Systems, Payment Services, and Electronic Money Institutions](#) published in the Official Gazette dated 27/6/2013 and numbered 28690;

Electronic money: Monetary value which is issued on the receipt of funds by an electronic money issuer, stored electronically, used to make payment transactions defined in this Law and accepted as a payment instrument also by natural and legal persons other than the electronic money issuer,

Electronic money institution: Legal person who has been granted authorization to issue electronic money under this Law

In order to establish electronic money companies, certain conditions have been specified.

1. Pursuant to Article 11 of the [Regulation on Payment Services and Electronic Money Issuance, Payment Institutions, and Electronic Money Institutions](#), it is mandatory to obtain an **operating license** from the **Central Bank** as specified.

2. Kanunun 5. maddesine göre Elektronik Para Şirketlerinin kurulabilmesi için aşağıda belirtilen özellikleri sağlaması gerekmektedir:

- a. Anonim şirket şeklinde kurulması,
- b. Nakden ve her türlü muvazaadan arı olarak ödenmiş sermayesinin en az beş milyon Türk Lirası olması,
- c. Sistemi işletebilmek için yeterli sayıda nitelikli personel çalıştırması ve gerekli teknik donanım ile yönetime sahip olması,
- d. Yeterli risk yönetimine sahip olması ve bilgilerin güvenliği ile güvenilirliğine ve iş sürekliliğine dair gerekli tedbirleri alması,
- e. Sistemin, katılımcıların ve işletim kurallarının bu Kanuna ve bu Kanun uyarınca çıkarılacak düzenlemelere uygunluğunu sağlaması,
- f. Pay senetlerinin nakit karşılığı çıkarılması ve tamamının nama yazılı olması,
- g. Bankanın etkin gözetimini engellemeyecek şeffaf ve açık bir ortaklık yapısı ve organizasyon şemasına sahip olması,
- h. Sermayesinde yüzde on ve üzerinde paya sahip olanların ve kontrolü elinde bulunduranların 19/10/2005 tarihli ve

2. According to Article 5 of the Law, electronic money companies must meet the following requirements in order to be established:

- a. To be established as a joint stock company.
- b. To have at least five million Turkish Liras of paid-in capital which is cash and free of all kinds of collusions.
- c. To employ a sufficient number of qualified staff and to have adequate technical equipment and management to operate the system.
- d. To have sufficient risk management and to take necessary measures regarding information security, information reliability and business continuity.
- e. To ensure the compliance of the system, participants and operating rules with this Law and with the regulations to be issued pursuant to this Law.
- f. To have its shares issued against cash and be fully registered in its name,
- g. To have a transparent and open partnership structure and organizational chart that will not constitute an obstacle to the efficient oversight of the Bank.
- h. To have its shareholders, who own ten percent or more shares in capital and who have the control, meet the bank founders'

5411 sayılı Bankacılık Kanununda banka kurucuları için aranan nitelikleri haiz olması, gerekir.

Kanunun 28. maddesinde izinsiz ödeme sağlayıcısı gibi hizmet vermek suç olarak düzenlenmiştir;

“(1)Bu Kanuna göre alınması gereken izinleri almaksızın sistem işleticisi, ödeme kuruluşu veya elektronik para kuruluşu gibi faaliyet gösteren gerçek kişiler ile tüzel kişilerin görevlileri **bir yıldan üç yıla kadar hapis ve beş bin güne kadar adli para cezası ile cezalandırılır.**

(2) Bu Kanuna göre alınması gereken izinleri almaksızın ticaret unvanlarında, her türlü belgelerde, ilan ve reklamlarda veya kamuoyuna yaptıkları açıklamalarda sistem işleticisi, ödeme kuruluşu veya elektronik para kuruluşu gibi faaliyet gösterdiği izlenimini yaratacak söz ve deyimleri kullanan gerçek kişiler ile tüzel kişilerin görevlileri bir yıldan üç yıla kadar hapis ve beş bin güne kadar adli para cezası ile cezalandırılır.

(3) Birinci ve ikinci fıkra kapsamında tanımlanan suçların bir iş yeri bünyesinde işlenmesi hâlinde bu işyerinin iki aydan altı aya kadar, tekerrür hâlinde sürekli olarak kapatılmasına karar verilebilir.

(4) Bu Kanun kapsamında verilmiş olan faaliyet izni iptal edilen sistem işleticisinin, ödeme kuruluşunun veya elektronik para kuruluşunun faaliyetine devam etmesi durumunda da bu madde hükümleri uygulanır.”

eligibility criteria laid down in the Banking Law No. 5411 dated October 19, 2005.

Providing services as an unauthorized payment service provider is regulated as a crime in Article 28 of the law.

“(1)Natural persons and officers of legal persons who act as system operators, payment institutions or electronic money institutions without having licenses that should be obtained pursuant to this Law, shall be sentenced to imprisonment for **one year to three years** and a judicial fine of up to five thousand days.

(2) Natural persons or officers of legal persons who use words and expressions that could create the impression that they are acting as system operators, payment institutions, or electronic money institutions in their business titles, all kinds of documents, notices, advertisements, or public statements without having the license that should be obtained pursuant to this law shall be sentenced to imprisonment for one to three years and a judicial fine of up to five thousand days.

(3) In cases where the offenses defined in the first and second paragraphs are committed within the body of a business place, such business places may be closed for two to six months and permanently if such acts are repeated.

(4) Provisions of this article shall be enforced in cases in which a system operator, payment institution, or electronic money institution whose

2023 itibariyle [TCMB İnternet sitesinde yer alan](#) Aktif Ödeme Kuruluşları aşağıdaki gibidir;

Aktif Ödeme Kuruluşları (Kodlar)

Aypara Ödeme Kuruluşu A.Ş. (880)

Ceo Ödeme Hizmetleri A.Ş. (878)

Efix Ödeme Hizmetleri A.Ş. (876)

Elekse Elektronik Para ve Ödeme Kuruluşu A.Ş. (855)

Faturakom Ödeme Hizmetleri A.Ş. (858)

Föy Fatura Ödeme Kuruluşu A.Ş. (859)

Global Ödeme Hizmetleri A.Ş. (884)

GönderAl Ödeme Hizmetleri A.Ş. (851)

İstanbul Ödeme ve Elektronik Para A.Ş. (883)

Klon Ödeme Kuruluşu A.Ş. (881)

MoneyGram Turkey Ödeme Hizmetleri A.Ş. (871)

N Kolay Ödeme ve Elektronik Para Kuruluşu A.Ş. (852)

Nestpay Ödeme Hizmetleri A.Ş. (865)

Octet Express Ödeme Kuruluşu A.Ş. (874)

operating license granted pursuant to this law has been withdrawn continues its activity.

As of 2023, the active Payment Institutions listed on the [Central Bank of Turkey \(TCMB\) website](#) are as follows:

Aktif Ödeme Kuruluşları (Kodlar)

Aypara Ödeme Kuruluşu A.Ş. (880)

Ceo Ödeme Hizmetleri A.Ş. (878)

Efix Ödeme Hizmetleri A.Ş. (876)

Elekse Elektronik Para ve Ödeme Kuruluşu A.Ş. (855)

Faturakom Ödeme Hizmetleri A.Ş. (858)

Föy Fatura Ödeme Kuruluşu A.Ş. (859)

Global Ödeme Hizmetleri A.Ş. (884)

GönderAl Ödeme Hizmetleri A.Ş. (851)

İstanbul Ödeme ve Elektronik Para A.Ş. (883)

Klon Ödeme Kuruluşu A.Ş. (881)

MoneyGram Turkey Ödeme Hizmetleri A.Ş. (871)

N Kolay Ödeme ve Elektronik Para Kuruluşu A.Ş. (852)

Ödeal Ödeme Kuruluşu A.Ş. (868)
Paragram Ödeme Hizmetleri A.Ş. (888)
Pay Fix Elektronik Para ve Ödeme Hizmetleri A.Ş. (882)
Paybull Ödeme Hizmetleri A.Ş. (892)
Paynet Ödeme Hizmetleri A.Ş. (866)
Paytrek Ödeme Kuruluşu Hizmetleri A.Ş. (856)
Pratik İşlem Ödeme Kuruluşu A.Ş. (860)
Ria Turkey Ödeme Kuruluşu A.Ş. (879)
Sender Ödeme Hizmetleri A.Ş. (875)
Trend Ödeme Kuruluşu A.Ş. (862)
Tronapay Ödeme Hizmetleri A.Ş. (887)
Vezne24 Tahsilat Sistemleri ve Ödeme Hizmetleri A.Ş. (885)
Western Union Turkey Ödeme Hizmetleri A.Ş. (886)

Faaliyet İzni İptal Edilen Ödeme Kuruluşları

Buradaöde Ödeme Kuruluşu A.Ş.

Nestpay Ödeme Hizmetleri A.Ş. (865)
Octet Express Ödeme Kuruluşu A.Ş. (874)
Ödeal Ödeme Kuruluşu A.Ş. (868)
Paragram Ödeme Hizmetleri A.Ş. (888)
Pay Fix Elektronik Para ve Ödeme Hizmetleri A.Ş. (882)
Paybull Ödeme Hizmetleri A.Ş. (892)
Paynet Ödeme Hizmetleri A.Ş. (866)
Paytrek Ödeme Kuruluşu Hizmetleri A.Ş. (856)
Pratik İşlem Ödeme Kuruluşu A.Ş. (860)
Ria Turkey Ödeme Kuruluşu A.Ş. (879)
Sender Ödeme Hizmetleri A.Ş. (875)
Trend Ödeme Kuruluşu A.Ş. (862)
Tronapay Ödeme Hizmetleri A.Ş. (887)
Vezne24 Tahsilat Sistemleri ve Ödeme Hizmetleri A.Ş. (885)
Western Union Turkey Ödeme Hizmetleri A.Ş. (886)

Payment Institutions Whose Operating Licenses Have Been Revoked

Misyon Ödeme Hizmetleri A.Ş.

Tam Fatura Ödeme Hizmetleri A.Ş.

Paytrek Ödeme Kuruluşu Hizmetleri A.Ş.

Faaliyet İzni Sona Eren Ödeme Kuruluşları

PayU Ödeme Kuruluşu A.Ş.

2023 itibariyle [TCMB internet sitesinde yer alan](#) aktif Elektronik Para şirketleri aşağıdaki gibidir;

A Ödeme ve Elektronik Para Hizmetleri A.Ş. (913)

Ahlatıcı Ödeme ve Elektronik Para Hizmetleri A.Ş. (894)

As Ödeme Hizmetleri ve Elektronik Para A.Ş. (911)

Aköde Elektronik Para ve Ödeme Hizmetleri A.Ş. (836)

Belbim Elektronik Para ve Ödeme Hizmetleri A.Ş. (828)

Birleşik Ödeme Hizmetleri ve Elektronik Para A.Ş. (825)

BPN Ödeme ve Elektronik Para Hizmetleri A.Ş. (850)

Cemete Elektronik Para ve Ödeme Hizmetleri A.Ş. (826)

Ceo Ödeme ve Elektronik Para Kuruluşu A.Ş. (878)

Buradaöde Ödeme Kuruluşu A.Ş.

Misyon Ödeme Hizmetleri A.Ş.

Tam Fatura Ödeme Hizmetleri A.Ş.

Paytrek Ödeme Kuruluşu Hizmetleri A.Ş.

Payment Institutions Whose Operating Licenses Have Expired

PayU Ödeme Kuruluşu A.Ş.

As of 2023, the active Electronic Money Institutions listed on the [TCMB \(Central Bank of the Republic of Turkey\) website](#) are as follows

A Ödeme ve Elektronik Para Hizmetleri A.Ş. (913)

Ahlatıcı Ödeme ve Elektronik Para Hizmetleri A.Ş. (894)

As Ödeme Hizmetleri ve Elektronik Para A.Ş. (911)

Aköde Elektronik Para ve Ödeme Hizmetleri A.Ş. (836)

Belbim Elektronik Para ve Ödeme Hizmetleri A.Ş. (828)

Birleşik Ödeme Hizmetleri ve Elektronik Para A.Ş. (825)

BPN Ödeme ve Elektronik Para Hizmetleri A.Ş. (850)

Cemete Elektronik Para ve Ödeme Hizmetleri A.Ş. (826)

Ceo Ödeme ve Elektronik Para Kuruluşu A.Ş. (878)

D Ödeme Elektronik Para ve Ödeme Hizmetleri A.Ş. (830)
Dgpara Ödeme ve Elektronik Para Kuruluşu A.Ş. (893)
DSM Ödeme ve Elektronik Para Hizmetleri A.Ş. (848)
Erpa Ödeme Hizmetleri ve Elektronik Para A.Ş. (837)
Fastpay Elektronik Para ve Ödeme Hizmetleri A.Ş. (891)
Faturamatik Elektronik Para ve Ödeme Kuruluşu A.Ş. (861)
Fzypay Elektronik Para ve Ödeme Hizmetleri A.Ş. (896)
Hızlıpara Ödeme Hizmetleri ve Elektronik Para A.Ş. (833)
IQ Money Ödeme Hizmetleri ve Elektronik Para A.Ş. (889)
İninal Ödeme ve Elektronik Para Hizmetleri A.Ş. (832)
İstanbul Ödeme ve Elektronik Para A.Ş. (883)
İyzi Ödeme ve Elektronik Para Hizmetleri A.Ş. (864)
Lydians Elektronik Para ve Ödeme Hizmetleri A.Ş. (890)
Moka Ödeme ve Elektronik Para Kuruluşu A.Ş. (857)
Moneyout Elektronik Para ve Ödeme Hizmetleri A.Ş. (917)
Moneypay Ödeme ve Elektronik Para Hizmetleri A.Ş. (842)
N Kolay Ödeme ve Elektronik Para Kuruluşu A.Ş. (852)
Nomu Pay Ödeme ve Elektronik Para Hizmetleri A.Ş. (831)

D Ödeme Elektronik Para ve Ödeme Hizmetleri A.Ş. (830)
Dgpara Ödeme ve Elektronik Para Kuruluşu A.Ş. (893)
DSM Ödeme ve Elektronik Para Hizmetleri A.Ş. (848)
Erpa Ödeme Hizmetleri ve Elektronik Para A.Ş. (837)
Fastpay Elektronik Para ve Ödeme Hizmetleri A.Ş. (891)
Faturamatik Elektronik Para ve Ödeme Kuruluşu A.Ş. (861)
Fzypay Elektronik Para ve Ödeme Hizmetleri A.Ş. (896)
Hızlıpara Ödeme Hizmetleri ve Elektronik Para A.Ş. (833)
IQ Money Ödeme Hizmetleri ve Elektronik Para A.Ş. (889)
İninal Ödeme ve Elektronik Para Hizmetleri A.Ş. (832)
İstanbul Ödeme ve Elektronik Para A.Ş. (883)
İyzi Ödeme ve Elektronik Para Hizmetleri A.Ş. (864)
Lydians Elektronik Para ve Ödeme Hizmetleri A.Ş. (890)
Moka Ödeme ve Elektronik Para Kuruluşu A.Ş. (857)
Moneyout Elektronik Para ve Ödeme Hizmetleri A.Ş. (917)
Moneypay Ödeme ve Elektronik Para Hizmetleri A.Ş. (842)

Ozan Elektronik Para A.Ş. (839)
Paladyum Elektronik Para ve Ödeme Hizmetleri A.Ş. (834)
Papara Elektronik Para A.Ş. (829)
Papel Elektronik Para ve Ödeme Hizmetleri A.Ş. (914)
Parakolay Elektronik Para A.Ş. (847)
ParaQR Elektronik Para ve Ödeme Hizmetleri A.Ş. (897)
Parolapara Elektronik Para ve Ödeme Hizmetleri A.Ş. (846)
Payco Elektronik Para ve Ödeme Hizmetleri A.Ş. (849)
Paypole Ödeme Hizmetleri ve Elektronik Para A.Ş. (916)
Paytr Ödeme ve Elektronik Para Kuruluşu A.Ş. (863)
Pratik İşlem Ödeme ve Elektronik Para A.Ş. (860)
Rubik Elektronik Para ve Ödeme Hizmetleri A.Ş. (899)
Sipay Elektronik Para ve Ödeme Hizmetleri A.Ş. (838)
Token Ödeme Hizmetleri ve Elektronik Para A.Ş. (840)
Tom Pay Elektronik Para ve Ödeme Hizmetleri A.Ş. (912)
TT Ödeme ve Elektronik Para Hizmetleri A.Ş. (870)
TTM Elektronik Para ve Ödeme Hizmetleri A.Ş. (843)
Turk Elektronik Para A.Ş. (827)

N Kolay Ödeme ve Elektronik Para Kuruluşu A.Ş. (852)
Nomu Pay Ödeme ve Elektronik Para Hizmetleri A.Ş. (831)
Ozan Elektronik Para A.Ş. (839)
Paladyum Elektronik Para ve Ödeme Hizmetleri A.Ş. (834)
Papara Elektronik Para A.Ş. (829)
Papel Elektronik Para ve Ödeme Hizmetleri A.Ş. (914)
Parakolay Elektronik Para A.Ş. (847)
ParaQR Elektronik Para ve Ödeme Hizmetleri A.Ş. (897)
Parolapara Elektronik Para ve Ödeme Hizmetleri A.Ş. (846)
Payco Elektronik Para ve Ödeme Hizmetleri A.Ş. (849)
Paypole Ödeme Hizmetleri ve Elektronik Para A.Ş. (916)
Paytr Ödeme ve Elektronik Para Kuruluşu A.Ş. (863)
Pratik İşlem Ödeme ve Elektronik Para A.Ş. (860)
Rubik Elektronik Para ve Ödeme Hizmetleri A.Ş. (899)
Sipay Elektronik Para ve Ödeme Hizmetleri A.Ş. (838)
Token Ödeme Hizmetleri ve Elektronik Para A.Ş. (840)

Turkcell Ödeme ve Elektronik Para Hizmetleri A.Ş. (869)
Turkonay Elektronik Para ve Ödeme Hizmetleri A.Ş. (915)
UPT Ödeme Hizmetleri ve Elektronik Para A.Ş. (853)
Vepara Elektronik Para ve Ödeme Hizmetleri A.Ş. (845)
Vizyon Elektronik Para ve Ödeme Hizmetleri A.Ş. (854)
Vodafone Elektronik Para ve Ödeme Hizmetleri A.Ş. (835)

III. Kripto Para Hukuku

1. Genel Olarak

Teknoloji ile birlikte gelişen ve değişen her şey gibi para da çağın gereklerine ayak uydurarak değişmektedir. Son yıllarda Dijital Para, Sanal Para Kripto para kavramları artık hayatımızda yerini almıştır.

Dijital paralar, henüz yasal olarak yeknesak şekilde düzenlenip kabul edilebilmiş değildir. Türkiye'de de Elektronik Para ve Ödeme Kuruluşları ile ilgili düzenleme olsa da, dijital para, sanal para ya da

Tom Pay Elektronik Para ve Ödeme Hizmetleri A.Ş. (912)
TT Ödeme ve Elektronik Para Hizmetleri A.Ş. (870)
TTM Elektronik Para ve Ödeme Hizmetleri A.Ş. (843)
Turk Elektronik Para A.Ş. (827)
Turkcell Ödeme ve Elektronik Para Hizmetleri A.Ş. (869)
Turkonay Elektronik Para ve Ödeme Hizmetleri A.Ş. (915)
UPT Ödeme Hizmetleri ve Elektronik Para A.Ş. (853)
Vepara Elektronik Para ve Ödeme Hizmetleri A.Ş. (845)
Vizyon Elektronik Para ve Ödeme Hizmetleri A.Ş. (854)
Vodafone Elektronik Para ve Ödeme Hizmetleri A.Ş. (835)

III. Crypto Currencies Law

1. In General

Like everything that evolves and changes with technology, money is also adapting to the requirements of the age. In recent years, concepts such as Digital Money, Virtual Money, and Cryptocurrency have found their place in our lives.

Digital currencies have not yet been legally regulated and accepted in a consistent manner. Although there are regulations regarding Electronic Money and Payment Institutions in Turkey, concepts referred to as

kripto para olarak isimlendirilen kavramlar hukuken düzenlenmemiştir.

.Kripto paralar "Blok Zincir Teknolojisi" (Blockchain) adı verilen şekilde bir çok sunucunun bir araya gelmesiyle oluşan ağ üzerinde işlem görürler.

2. Kripto Paranın Özellikleri

Kripto paralar, çok yüksek işlemcisi olan bilgisayarlarla, kompleks algoritmaları çözerek üretilebilmektedir. Kripto üretimine "kripto madenciliği" ismi de verilir.

[Kripto paranın güvenliği ile ilgili BDDK tarafından yayınlanan rapora göre](#): "Kripto paralar içerdikleri karmaşık matematiksel fonksiyonlar nedeniyle taklit edilemedikleri, özel kurallara bağlı kalmadan hızla el değiştirebildikleri ve aynı kripto para aynı anda birden çok yerde kullanılmadığı için kullanıcı güvenini kazanmakta ve gerçek paralara alternatif olabilmektedirler. Ancak bu durum kripto paraların çalınmadıkları anlamına da gelmemektedir. Aynen gerçek paralar da olduğu gibi kripto paralarda çalınabilmekte ve dolandırıcılık gibi bir çok suç içeren faaliyete konu olabilmektedir. Kripto paralar basılı paradan farklı olarak dijital ortamda üretildiği için bunların korunması fiziki paraya göre daha fazla teknik bilgi içermekte ve her ne kadar kripto paranın kendisi güvenli olsa da üzerinden kullanıldığı cihazlar ve ağın güvenlik açıkları nedeniyle çalınabilir hale gelmektedir.

digital money, virtual money, or cryptocurrency have not been legally defined.

Cryptocurrencies operate on a network formed by the convergence of many servers, known as "Blockchain Technology."

2. Key Features of Cryptocurrency:

Cryptocurrencies can be produced by solving complex algorithms using high-performance computers, a process often referred to as "crypto mining."

Regarding the security of cryptocurrency, [according to a report published by the Banking Regulation and Supervision Agency \(BDDK\)](#):

"Cryptocurrencies are not easily counterfeited due to the complex mathematical functions they contain, they can change hands rapidly without adhering to specific rules, and they can gain user trust since the same cryptocurrency can be used in multiple places simultaneously as an alternative to real currencies. However, this does not mean that cryptocurrencies cannot be stolen. Just like real money, cryptocurrencies can be stolen, and they can be subject to various criminal activities. Cryptocurrencies, unlike printed money, are produced in a digital environment, which requires more technical knowledge for their protection. While the cryptocurrency itself may be secure, the devices and network vulnerabilities used with it can make it susceptible to theft.

Bütün bunlara ek olarak kripto paranın ödeme aracılığıyla kullanılması durumunda karşı tarafın talep 24 edilen ürün ya da hizmeti gerçekten sunan kişi ya da işletme olduğundan emin olabilmek için başka ek güvenlik önlemleri de gerekmektedir çünkü kripto paraların sunduğu en önemli olanaklardan biri de izlerinin takip edilmesinin neredeyse imkansız olmasıdır.

Konu bu bağlamda değerlendirildiğinde sahip olunan kripto paraları korumak için herhangi bir dijital varlığı korumak için alınan önlemlerden bir seviye daha yüksek önlemler almak ve bu paraları kullanarak yapılan alışverişlerde e-ticaretteki güvenlik prosedürlerinin en katılarını uygulayarak kripto paranın gönderileceği kişinin gerçekten gönderilmesi gereken kişi olduğuna kanaat getirmeyi temin eden mekanizmalar kurmak yerinde olacaktır. “

3. Dünya Üzerinde Kripto Para Uygulamaları

Türkiye’de elektronik paraların hukuki statüsü ve yasal düzenlemesi bulunurken, kripto paraların bir yasal düzenlemeye tabi olmadığı görülmektedir.

Amerika Birleşik Devletleri sanal ve kripto paralar konusunda yasası olan ülkelerden birisi. **Token Taxonomy Act of 2019**, sanal para birimleri gibi dijital paraların düzenlenmesi amacıyla yapılmıştır. Bu kanuna göre sanal para birimleri menkul kıymetlerden değildir, ancak sanal mülkler değerler olarak vergilendirilebilir hale gelmiştir. ([Kaynak](#))

Furthermore, when considering this context, taking precautions one level higher than those taken to protect any digital asset is advisable to safeguard the acquired cryptocurrencies. Establishing mechanisms that ensure the recipient of the cryptocurrency in e-commerce transactions is indeed the intended party by implementing the strictest security procedures in e-commerce can be vital because one of the most significant advantages of cryptocurrencies is their almost impossible traceability."

In this context, it would be appropriate to take a level higher measures than those taken to protect any digital asset to protect the cryptocurrencies in possession, and to establish mechanisms to ensure that the person to whom the cryptocurrency is sent is really the person who should be sent, by applying the strictest security procedures in e-commerce for the transactions that are made using that currency. “

3. Cryptocurrency Applications Worldwide

While there is a legal status and regulatory framework for electronic money in Turkey, it is observed that cryptocurrencies are not subject to legal regulation.

The United States is one of the countries with a law related to virtual and cryptocurrencies. The Token Taxonomy Act of 2019 was introduced with the aim of regulating digital currencies. According to this law, virtual currencies are not considered securities, but virtual assets can be taxed as values. ([Source](#))

Kanada, Bitcoin gibi kripto paralar ve dijital dövizler açısından uygulamada ılımlı yaklaşım sunan dünya ülkelerinden birisidir. Karapara aklama haricinde kullanımı desteklemektedir. Sanal para kabul eden yerlerde hizmet ve ürünleri satın almak için serbestçe kullanabilmekte ve diğer dövizlere dönüştürülebilmektedir. Kanada'da kripto paralar emtia kabul edilmekte ve geçerli olan vergi hukuku aynen kripto paralara da uygulanmaktadır. ([Kaynak](#))

Avustralya, Bitcoin'i ne para ne de bir yabancı para birimi olarak kabul etmektedir ve Avustralya Vergi Dairesi (ATO) onu sermaye kazancı vergisi amaçları için bir varlık olarak kabul etmektedir. ([Kaynak](#))

Avrupa Birliği, Haziran 2023'te [MICA \(Markets in Crypto-Assets Regulation\)](#) Kripto Varlık Regülasyonunu yayınlamıştır. Bu düzenlemeye göre "kripto varlık", "bir değer veya bir hakkın, dağıtılmış defter teknolojisi veya benzer teknoloji kullanılarak elektronik olarak transfer edilebilir ve saklanabilir dijital temsili" şeklinde tanımlanmıştır.

4. Türk Hukukunda Kripto Varlıkların Yeri

4.1. 2013 BDDK Açıklaması

[BDDK 2013 yılında](#) kripto para ile ilgili aşağıdaki basın açıklamasını yapmıştır:

"Herhangi bir resmi ya da özel kuruluş tarafından ihraç edilmeyen ve karşılığı için güvence verilmeyen bir sanal para birimi olarak bilinen

Canada is known for its moderate approach to cryptocurrencies and digital currencies like Bitcoin. It supports their use, except for money laundering. Cryptocurrencies can be freely used to purchase goods and services in places that accept digital money and can be converted into other currencies. In Canada, cryptocurrencies are considered commodities, and the existing tax law is applied to cryptocurrencies as well. ([Source](#))

Australia does not classify Bitcoin as a currency or a foreign currency. The Australian Taxation Office (ATO) considers it an asset for capital gains tax purposes. ([Source](#))

The European Union has published the [MICA \(Markets in Crypto-Assets Regulation\)](#) in June 2023. According to this regulation, a "crypto-asset" is defined as a "digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology."

4. Place of Crypto Assets in Turkish Law

4.1. 2013 BDDK Statement

In 2013, the [Banking Regulation and Supervision Agency \(BDDK\)](#) issued the following press release regarding cryptocurrencies:

"Bitcoin, known as a virtual currency that is not issued by any official or private institution and is not guaranteed for its counterpart, is not considered electronic money within the scope of the law due to its

Bitcoin, mevcut yapısı ve işleyişi itibarıyla Kanun kapsamında elektronik para olarak değerlendirilmemekte, bu nedenle de söz konusu Kanun çerçevesinde gözetim ve denetimi mümkün görülmemektedir.

Diğer taraftan, Bitcoin ve benzeri sanal paralar ile gerçekleştirilen işlemlerde tarafların kimliklerinin bilinmemesi, söz konusu sanal paraların yasadışı faaliyetlerde kullanılması için uygun bir ortam yaratmaktadır. Ayrıca Bitcoin, piyasa değerinin aşırı oynak olabilmesi, dijital cüzdanların çalınabilmesi, kaybolabilmesi veya sahiplerinin bilgileri dışında usulsüz olarak kullanılabilmesi gibi risklerin yanı sıra yapılan işlemlerin geri döndürülemez olmasından dolayı operasyonel hatalardan ya da kötü niyetli satıcıların suistimalinden kaynaklı risklere de açıktır. “

4.2. 2021 Kripto Para Yönetmeliği

16 Nisan 2021 tarihli Resmi Gazete’de yayınlanarak yürürlüğe giren “[Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik](#)” (Yönetmelik) ile Türk hukukunda kripto varlıklara ilişkin düzenlemeler yapılmıştır.

Yönetmelik 3’üncü maddesi uyarınca kripto varlık; dağıtık defter teknolojisi veya benzer bir teknoloji kullanılarak sanal olarak oluşturulup dijital ağlar üzerinden dağıtımını yapılan, ancak itibari para, kaydi para, elektronik para, ödeme aracı, menkul kıymet veya diğer sermaye piyasası aracı olarak nitelendirilmeyen gayri maddi varlıkları ifade eder.

existing structure and operation. Therefore, its supervision and regulation are not deemed possible within the framework of the law.

On the other hand, transactions involving Bitcoin and similar virtual currencies where the identities of the parties are not known create a suitable environment for the illegal use of these virtual currencies. In addition, Bitcoin is susceptible to risks such as extreme market volatility, theft or loss of digital wallets, and unauthorized use without the knowledge of the owners, as well as irreversible transactions, leading to risks stemming from operational errors or the misuse by malicious sellers.”

4.2. 2021 Cryptocurrency Regulation

Regulations regarding crypto assets have been introduced into Turkish law with the "[Regulation on the Non-Use of Crypto Assets in Payments.](#)" which was published in the Official Gazette on April 16, 2021.

According to Article 3 of the Regulation, a crypto asset is defined as an intangible asset that is created virtually using distributed ledger technology or a similar technology and distributed through digital networks. These assets are not classified as fiat money, book money, electronic money, payment instruments, securities, or other capital market instruments.

Yönetmelik uyarınca kripto varlıklara ilişkin olarak;

- ödemelerde doğrudan veya dolaylı kullanılmaması,
- ödemelerde doğrudan veya dolaylı şekilde kullanılmasına yönelik hizmet verilmemesi,
- ödeme hizmeti sağlayıcılarının, ödeme hizmetlerinin sunulmasında ve elektronik para ihracında kripto varlıkların doğrudan veya dolaylı olarak kullanılacağı bir şekilde iş modelleri geliştirmemesi,
- ödeme ve elektronik para kuruluşları, kripto varlıklara ilişkin alım satım, saklama, transfer veya ihraç hizmeti sunan platformlara veya bu platformlardan yapılacak fon aktarımlarına aracılık etmemesi gerektiği düzenlenmiştir.

4.3. 2021 Yılı Kripto Varlıklar, Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesi Yönetmelik Değişikliği

01.05.2021 tarihinde [Suç Gelirlerinin Aklanmasının Ve Terörün Finansmanının Önlenmesine Dair Tedbirler Hakkında Yönetmelik](#)'te yapılan değişiklik ile Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanunun uygulanmasına yönelik olarak "yükümlülüler" arasına **kripto para hizmet sağlayıcılar** da dahil edilmiştir.

In accordance with the Regulation, the following rules apply to crypto assets:

- Crypto assets should not be used directly or indirectly for payments.
- Services should not be provided to enable the direct or indirect use of crypto assets in payments.
- Payment service providers should not develop business models that involve the direct or indirect use of crypto assets in providing payment services and issuing electronic money.
- Payment and electronic money institutions are regulated not to act as intermediaries for buying, selling, holding, transferring, or exporting services related to crypto assets or fund transfers made through these platforms.

4.3. Regulation Amendment on Crypto Assets in the Context of Preventing Money Laundering and Financing of Terrorism for the Year 2021

With an amendment to the [Regulation on Measures Regarding the Prevention of Money Laundering and the Financing of Terrorism](#), published on May 1, 2021, **crypto asset service providers** have been included among the "obligated parties" in the context of enforcing the Law on Preventing Money Laundering.

“Yükümlü” olarak tanımlanan finansal ve finansal olmayan kuruluşlar ile bazı iş ve meslek gruplarının, faaliyet alanları ve verdikleri hizmetlerden dolayı suçlular tarafından aracı olarak kullanılabilme ihtimali bulunmaktadır. Diğer bir deyişle, yükümlüler tarafından yapılan işlemler ve verilen hizmetler suçlular tarafından suç işlemek amacıyla kullanılabilir. Bu durumun önlenmesi, yükümlülerin aklama ve terörizmin finansmanı suçu ve bu suçlarla mücadele konusunda bilinçlendirilmeleri ve farkındalıklarının artırılması amacıyla “önleyici” bir fonksiyon üstlenmeleri sağlanmaya çalışılmıştır.

Dolayısıyla, yükümlüler suçla mücadelede Mali Suçları Araştırma Kurulunun en önemli paydaşı konumundadır. Yükümlüler, 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanunun 2/1-d maddesi ile Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesine Dair Tedbirler Hakkında Yönetmeliğin (Tedbirler Yönetmeliği) 4/1 inci maddesinde belirlenmiştir. Tedbirler Yönetmeliğinin 4 üncü maddesinin birinci fıkrasına 01 Mayıs 2021 tarihli ve 31471 sayılı Resmi Gazete’de yayımlanan Yönetmelik değişikliği ile eklenen (ü) bendine göre, “kripto varlık hizmet sağlayıcılar” anılan tarih itibarıyla yükümlüler arasına alınmıştır. (<https://ms.hmb.gov.tr/uploads/sites/12/2021/05/Kripto-Varlik-Hizmet-Saglayicilar-Rehberi.pdf>)

Financial and non-financial institutions, as well as certain professions and occupations, are defined as "obligated parties" due to the possibility of being used as intermediaries by criminals in their areas of activity and the services they provide. In other words, the transactions and services provided by these obligated parties can be potentially used by criminals for the purpose of committing crimes. To prevent this, the obligated parties are expected to take on a "preventive" function by being educated and increasing their awareness about money laundering and combating terrorism financing.

Therefore, obligated parties are considered vital stakeholders in the fight against financial crimes, playing a significant role alongside the Financial Crimes Investigation Board. The status of obligated parties is defined in Article 2/1-d of Law No. 5549 on the Prevention of Money Laundering and in Article 4/1 of the Regulation on Measures Regarding the Prevention of Money Laundering and the Financing of Terrorism. According to an amendment to the Regulation published in the Official Gazette with issue number 31471 on May 1, 2021, a new subparagraph (u) has been added to Article 4 of the Regulation. This amendment includes "crypto asset service providers" among the obligated parties as of the date mentioned.

(Source: <https://ms.hmb.gov.tr/uploads/sites/12/2021/05/Kripto-Varlik-Hizmet-Saglayicilar-Rehberi.pdf>)

Yönetmelik Uyarınca Kripto Para Hizmet Sağlayıcıların Yükümlülükleri

- **Kimlik Tespit Yükümlülüğü:**

Yükümlüler, kendileri nezdinde yapılan veya aracılık ettikleri işlemlerde işlem yapılmadan önce, işlem yapanlar ile nam veya hesaplarına işlem yapılanların kimliklerini tespit etmelidir. Kimlik tespiti, iş ilişkisi tesisinden veya işlem yapılmadan önce tamamlanır. Sürekli iş ilişkisi tesisinde, iş ilişkisinin amacı ve mahiyeti hakkında bilgi alınır.

- **Şüpheli İşlem Bildirim Yükümlülüğü:**

5549 sayılı Kanunun "Şüpheli işlem bildirim" başlıklı 4 üncü maddesi gereğince, yükümlüler nezdinde veya bunlar aracılığıyla yapılan veya yapılmaya teşebbüs edilen işlemlere konu malvarlığının yasa dışı yollardan elde edildiğine veya yasa dışı amaçlarla kullanıldığına dair herhangi bir bilgi, şüphe veya şüpheyi gerektirecek bir hususun bulunması halinde bu işlemlerin, yükümlüler tarafından Mali Suçları Araştırma Kurulu Başkanlığına (MASAK) bildirilmesi zorunludur.

- **Bilgi ve Belge Verme Yükümlülüğü:**

Kamu kurum ve kuruluşları, gerçek ve tüzel kişiler ile tüzel kişiliği olmayan kuruluşlar, Başkanlık ve denetim elemanları tarafından istenilecek her türlü bilgi, belge ve bunlara ilişkin her türlü ortamdaki kayıtları, bu kayıtlara erişimi sağlamak veya okunabilir

Obligations of Crypto Asset Service Providers According to the Regulation

- **Obligation for Identity Verification:**

Obligated parties must identify the identities of those conducting transactions with them or on behalf of whom they mediate before any transaction is made. Identity verification is completed before establishing a business relationship or conducting a transaction. In the case of an ongoing business relationship, information is obtained about the purpose and nature of the business relationship.

- **Obligation to Report Suspicious Transactions:**

According to Article 4 of Law No. 5549 titled "Suspicious Transaction Reporting," obligated parties are required to report transactions that are conducted within their scope or through their intermediation if there is any information, suspicion, or circumstance that indicates that the assets involved in these transactions have been obtained through illegal means or are being used for illegal purposes. These transactions must be reported to the Financial Crimes Investigation Board (MASAK) by the obligated parties.

- **Obligation to Provide Information and Documents:**

Public institutions and organizations, natural and legal persons, as well as entities without legal personality, are required to provide all kinds of information, documents, and records in any medium requested by the Presidency and inspection staff. They must provide all necessary

hale getirmek için gerekli tüm bilgi ve şifreleri tam ve doğru olarak vermek ve gerekli kolaylığı sağlamakla yükümlüdür.

- **Muhafaza ve İbraz Yükümlülüğü:**

Yükümlüler, bu Kanunlarla getirilen yükümlülüklerle ve işlemlerine ilişkin her türlü ortamdaki; belgeleri düzenleme tarihinden, defter ve kayıtları son kayıt tarihinden, kimlik tespitine ilişkin belgeleri ise son işlem tarihinden itibaren sekiz yıl süreyle muhafaza ve istenmesi halinde yetkililere ibraz etmekle yükümlüdür.

4.4. Kripto Para ile İlgili Mahkeme Kararları

- **Antalya Bölge Adliye Mahkemesi 6. Hukuk Dairesi Dosya No: 2020/1149, Karar No: 2020/905**

“...Alıntılanan Yargıtay ilamı çerçevesinde eldeki dosyada hiç bir araştırma yapılmaksızın talebin reddine karar verilmesinin hatalı olduğu anlaşılmaktadır. Bununla birlikte eldeki dosyada özel bir durumun söz konusu olduğu da açıktır. Zira talep eden müteveffanın **“Apple iCloud”** kimliğinin terekenin aktifinde olduğunun da tespitini talep etmiştir.

Gelişen teknolojilerin insan hayatını kolaylaştırması yanında bir kısım yeni kavramlar ve hukuki sorunlar yarattığı bilinen bir gerçektir. Bunların en başında da mülkiyet kavramının başkalaşımının geldiği söylenebilir.

Düne kadar mülkiyet kavramı menkul ve gayrimenkul mülkiyeti ile bir kısım sınırlı aynı haklar etrafında şekillenirken, son dönemde fikri

information and passwords to access these records or make them readable accurately and completely.

- **Obligation to Preserve and Produce:**

Obligated parties must preserve and produce all documents related to the obligations and transactions imposed by these laws for eight years starting from the date of document issuance, the last entry date for books and records, or the last transaction date for identity verification documents when requested by the authorities.

4.4. Court Decisions Related to Cryptocurrency

- **Antalya Regional Court of Justice, 6th Civil Division, Case No: 2020/1149, Decision No: 2020/905**

“...Within the framework of the quoted Court of Cassation decision, it is evident that the decision to dismiss the request was made without conducting any investigation in the current case. However, it is clear that there is a specific situation in this case. The claimant has also requested the determination that the **'Apple iCloud'** identity is included in the estate's assets.

It is a well-known fact that while evolving technologies make human life more convenient, they also give rise to new concepts and legal issues. The transformation of the concept of property can be cited as the primary example of this. Until recently, the concept of property was centered around movable and immovable property, as well as certain limited real rights. However, in recent times, with the development of

mülkiyet kavramının gelişimi üzerine ilgili otoritelerce “Fikir ve Sanat Eserleri” mülkiyet hukuku çerçevesinde koruma altına alınmış, bu yönde bir kısım yasal düzenlemelere gidilmiştir.

Ancak çağımızın kaçınılmaz şekilde dijitalleşen hayat tarzı karşısında dijital mal varlığına dair dijital mülkiyet ile ilgili henüz yasal bir düzenleme yapılmadığı görülmektedir.

Yakın zamana kadar elektronik posta hesapları, sosyal medya hesapları ve benzeri dijital uygulamalar yalnızca kişisel kullanıma yönelik olup maddi bir değer taşımazken günümüzde bu hesapların reklam gelirleri elde edilen maddi bir karşılığı olan hesaplar halini alabildiği gibi, yine **sosyal medya hesaplarının** ve **dijital para cüzdanlarının bağlı olduğu e posta hesaplarının** da artık kişisel kullanımı aşırp ticari değeri olan **dijital mal varlığı** kapsamına girmeye başladığı anlaşılmaktadır.

Bu konuda Tokat Gaziosmanpaşa Üniversitesi Hukuk Fakültesi Medeni Hukuk Anabilim Dalı Araştırma Görevlisi Yasemin Maraşlı DİNÇ’in <http://tbbdergisi.barobirlik.org.tr/m2019-142-1849> adresinde yayınlanan makalesinden yararlanılarak katıldığımız bir kısım tespitlerinin altına çizilmesi anlamında alıntılama yapılmıştır.

“Teknolojinin, dolayısıyla da internetin bu denli gelişmesi sonucunda sosyal medya kullanımı hayatımızın ayrılmaz bir parçası haline almıştır. Artık bir kısım insan, sosyal medya platformları aracılığıyla maddi kazanç elde etmeye dahi başlamıştır. Özellikle son zamanlarda “YouTuber” olarak nitelenmeye başlanan insan sayısı gün geçtikçe artmaktadır. Öte yandan “Facebook” veya “Instagram”

the concept of intellectual property, "Intellectual and Artistic Works" have been protected within the framework of property law, and various legal regulations have been made in this regard.

Yet, it can be observed that there is no legal regulation regarding digital property in the face of the inevitable digitization of our contemporary lifestyle. Until recently, email accounts, social media accounts, and similar digital applications were only for personal use and did not carry any financial value. However, in today's world, these accounts have evolved into assets with monetary value generated through advertising revenue. Additionally, it is now evident that **social media accounts** and **digital wallets, as well as the email accounts they are linked to**, have gone beyond personal use and have become part of **digital property** with commercial value.

In this regard, citations have been made for the purpose of emphasizing some of the observations made during our participation, based on the article published by Yasemin Maraşlı DİNÇ, a Research Assistant in the Department of Civil Law at Tokat Gaziosmanpaşa University Faculty of Law, at the address <http://tbbdergisi.barobirlik.org.tr/m2019-142-1849>.

The use of social media has become an integral part of our lives as a result of the significant advancements in technology and the internet. Some individuals have even started to earn a living through social media platforms. In recent times, the number of people referred to as "YouTubers" has been increasing day by day. Moreover, selling products through "Facebook" or "Instagram" accounts or generating income by

hesapları üzerinden, bir meslek icra edercesine satış yaparak yahut genellikle takipçi sayısı fazla olanların kişisel sayfalarında reklamlar yaparak maddi kazanç elde etmeleri sıradan hale gelmiştir.

Tüm bu gelişmelerin sonucu olarak ortaya çıkan dijital mal varlığı veya dijital miras kavramları ise ülkemiz hukuk sistemi içerisinde çok yaygın bir kullanıma sahip değildir. Türk kanunlarında bu konuda yasal düzenlemeler de henüz mevcut değildir. Bunun yanında konu Türk hukuk öğretisinde de, uygulamada bir sorun olarak ortaya çıkmamasından olsa gerek, yeterli derecede incelenmemiştir.”

“Dijital malvarlığı kavramı, videolar, fotoğraflar, e-postalar, kişisel sosyal medya hesapları gibi elektronik olarak depolanan ve yalnızca dijital formda bulunan diğer varlıklar anlamına gelmektedir. Ancak dijital dünyanın sürekli değişmesine bağlı olarak dijital malvarlığının nelerden oluştuğu net olarak belirlenememektedir.”

“Dijital miras ise bu tür soyut malvarlığı değerlerinin mirasçılara intikal etmesi, mirasa konusu olmasıdır”

Aynı makalede değinildiği üzere mirasta intikal prensiplerinin kanunda şekil bulmuş hali olan TMK m. 599/2 hükmünde; “Kanunda öngörülen ayırık durumlar saklı kalmak üzere mirasçılar, mirasbırakanın aynî haklarını, alacaklarını, diğer malvarlığı haklarını, taşınır ve taşınmazlar üzerindeki zilyetliklerini doğrudan doğruya kazanırlar ve mirasbırakanın borçlarından kişisel olarak sorumlu olurlar” denilmektedir.

advertising on personal pages, especially those with a high number of followers, has become commonplace.

As a result of all these developments, the concepts of digital property or digital inheritance are not widely used within our legal system in Turkey. There are no legal regulations on this matter in Turkish law yet. In addition, this issue has not been adequately examined in Turkish legal doctrine and practice, possibly because it has not posed a problem in practice.

The concept of digital property refers to electronically stored assets such as videos, photos, emails, personal social media accounts, and other assets that exist solely in digital form. However, due to the constant evolution of the digital world, it is not possible to clearly define what constitutes digital property.

"Digital inheritance, on the other hand, is the transfer of such abstract assets to the heirs, making them part of the inheritance."

As mentioned in the same article, the principles of inheritance, as embodied in Article 599/2 of the Turkish Civil Code (TCC), state: “Assigned heirs win with the legacy of the inheritance. The legal heirs are obliged to hand over the inherited legacy to the assigned heirs in accordance with the provisions of their possession.”

Günümüzde dijital mal varlığının yadsınamaz ve göz ardı edilemez bir gerçeklik olduğu, kripto para adı verilen ve uluslararası ödemelerde dahi kullanılmaya başlanmış dijital sistemlerin var olduğu, yine astronomik reklam gelirleri sağlayan sosyal medya hesaplarının gün geçtikçe arttığı, aynı şekilde youtube ve benzeri dijital platformlarda salt reklam geliri ve hatta ücretli üyelik sistemi ile hizmet veren kanallar oluşturulduğu bir ortamda dijital mal varlığı ve dijital miras ile ilgili olarak yasal bir düzenleme bulunmadığı, bu konuda yasal bir boşluk bulunduğu değerlendirilmiştir.

4721 sayılı Türk Medeni Kanununun 1.maddesi; “Kanun, sözüyle ve özüyle deđindiđi bütün konularda uygulanır.

Kanunda uygulanabilir bir hüküm yoksa, hakim, örf ve adet hukukuna göre, bu da yoksa kendisi kanun koyucu olsaydı nasıl bir kural koyacak idiyse ona göre karar verir.” düzenlemesini içermektedir.

Murisin e posta hesabı ve buna bađlı olarak kullanılan sosyal medya hesapları, dijital cüzdan hesapları vb maddi deđer ifade eden ve TMK'nun 599.maddesi kapsamında terekesine dahil olup mirasçılara intikali gereken dijital mal varlığının da tespiti gerekeceđi kanaatine varılmıştır.

Dosya özelinde bakıldığında, talep eden özellikle “*****@gmail.com” hesabının murise ait olduğunun, yani müteveffanın apple kimliđi ile iliřkili hesapların sahibi olduğunun ve müvekkilinin müteveffanın temsilcisi olduğunun ve mahkemece

In today's world, it is an undeniable and unignorable reality that digital assets exist. There are digital systems, known as cryptocurrencies, that are used even in international payments. Additionally, social media accounts that generate astronomical advertising revenues are increasing day by day. Similarly, channels are being established on digital platforms like YouTube and others, offering services based on advertising revenue and even subscription systems. In such an environment, it has been assessed that there is no legal regulation regarding digital property and digital inheritance and that there is a legal void in this regard.

According to Article 1 of Law No. 4721 of the Turkish Civil Code, “The law shall apply to all matters referred to by the word and its essence.

If there is no applicable provision in the law, the judge decides according to the customary law, otherwise whatever rule he would have made if he were a legislator.”.

It has been concluded that the determination of digital assets with financial value, including the deceased's email account, associated social media accounts, digital wallet accounts, and other assets falling within the scope of Article 599 of the Turkish Civil Code, which should be included in the inheritance and transferred to the heirs, will be necessary.

When examined in the context of the file, the claimant specifically requests the determination that the ‘*****@gmail.com’ account belongs to the deceased, in other words, the owner of the accounts associated with the deceased's Apple ID, and that the client is the

verilecek yetkilerinin, Elektronik Haberleşmenin Gizliliği Kanunu'nda kullanıldığı şekliyle "yasal rıza" teşkil ettiğinin tespitini istemektedir.

Sonuç olarak, mahkemece tespit talebi gereğince murisin ölüm tarihi itibarıyla tüm aktif ve pasif mal varlığının tespiti ve bu minvalde dijital mal varlığının terekesine dahil olması gerektiği nazara alınarak dijital terekesinin de tespiti yapılarak araştırma ve inceleme sonucunda bir karar verilmesi gerekirken, ölü kişinin e posta hesabının özel hayatın gizliliği kapsamında değerlendirilerek talebin reddine karar verilmiş olması hatalı olmuştur.

İzah olunan gerekçeler karşısında talep eden vekilinin istinaf talebinin kabulü ile ilk derece mahkemesinin kararının HMK' nun 353/1-a.6 maddesi gereğince kaldırılması gerektiği değerlendirilmiş ve aşağıdaki şekilde hüküm kurulması gerekmektedir."

III. Merkez Bankası Dijital Parası

1. Genel olarak Dijital Para

Dijital para, kripto para, elektronik para gibi isimsel benzerlik taşıdığı kavramlarla çok karışsa da, karakteristik olarak önemli farklılıklar içermektedir.

Dijital para, "Merkez Bankası Dijital Parası" (Central Bank Digital Currency) olarak da adlandırılmakta ve CBDC şeklinde veya ilgili

representative of the deceased. The claimant also seeks the establishment of the powers to be granted by the court as 'legal consent' in the manner used in the Electronic Communications Privacy Act.

As a result, considering that all of the deceased's active and passive assets as of the date of the deceased's death need to be determined as part of the request for determination by the court and that the digital assets should be included in the estate, a decision should have been made after the determination of the digital estate following the research and examination. However, by considering the deceased person's email account within the scope of the privacy of private life, the decision to reject the request was erroneous.

In light of the reasons provided, it is considered that the appellant's request for appeal should be accepted, the decision of the first-instance court should be annulled in accordance with Article 353/1-a.6 of the HMK, and the following judgment should be made."

III. Central Bank Digital Currency (CBDC)

1. In General, Digital Currency

Although the terms digital currency, cryptocurrency, electronic money, and similar-sounding concepts are often confused, they contain important characteristic differences.

Digital currency is also referred to as "Central Bank Digital Currency" (CBDC) and can be used in the form of CBDC or by adding the word "digital" to the country's currency (e.g., digital euro, digital Turkish lira).

ülkenin para birimine “dijital” sözcüğü eklenerek kullanılabilir. (örneğin dijital euro, dijital türk lirası)

AB Birliği Merkez Bankası'nın [tanımına](#) göre,

“Dijital euro, euro banknotları gibi ama dijital olacaktır. Dijital euro, nakit paranın yerini almaz, aksine onu tamamlar. Dijital bir euro, insanlara nasıl ödeme yapacakları konusunda ek bir seçenek sunacak ve bunu yapmayı kolaylaştıracak, erişilebilirlik ve kapsayıcılığa katkıda bulunacaktır.”

AB Merkez Bankası'nın konu ile ilgili yayınladığı [sıkça sorulan sorular](#) dökümanında konu ile ilgili temellerin çerçevesi çizilmiştir:

Avrupa neden bir dijital euro'ya ihtiyaç duyar?

Dijitalleşme, ödeme şeklimizi değiştiriyor. Nakit kullanımı azalıyor ve COVID-19 pandemisi online alışveriş ve dijital ödemelere yönelimin hızlanmasına neden oldu. Dijital euro, dijital dünyada nakdin elektronik bir formu olacaktır. Bu, tüketicilere dijital bir formatında merkez bankası parasını kullanma seçeneği sunarak, banknot ve madeni paraları tamamlayacaktır.

Dijital euro, kişilerin yaşamlarını kolaylaştıracak ve şu anda mevcut olmayan bir şey sunacaktır: euro bölgesi genelinde, mağazalarda, çevrimiçi veya kişiden kişiye ödemeler için evrensel olarak kabul edilen dijital bir ödeme aracı. Dijital euro, nakit gibi risksiz, geniş erişilebilir, kullanıcı dostu ve temel kullanım için ücretsiz olacaktır.

According to the European Central Bank's [definition](#),

"The digital euro will be digital, but, like euro banknotes, it will not replace cash; it will complement it. A digital euro will offer people an additional choice on how to pay and make it easier, contributing to accessibility and inclusivity."

[The frequently asked questions document](#) released by the European Central Bank outlines the framework for this topic:

Why does Europe need a digital euro?

Digitalization is changing the way we pay. The use of cash is decreasing, and the COVID-19 pandemic has accelerated the trend towards online shopping and digital payments. A digital euro will be an electronic form of cash in the digital world. It will offer consumers the option to use central bank money in a digital format, complementing banknotes and coins.

A digital euro will make people's lives easier and provide something that is not currently available: a universally accepted digital payment instrument for payments in stores, online, or peer-to-peer throughout the euro area. Like cash, the digital euro will be risk-free, widely accessible, user-friendly, and free for basic use.

Ayrıca, bir dijital euro, Avrupa'nın stratejik bağımsızlığını ve para egemenliğini güçlendirecek ve Avrupa ödeme ekosisteminin verimliliğini artırarak, yeniliği teşvik ederek ve enerji kesintileri gibi potansiyel siber saldırılara veya teknik kesintilere karşı dayanıklılığını artırarak katkı sağlayacaktır.

Dijital euro, nakit para yerine mi geçer?

Hayır, dijital euro, nakit parayı tamamlar, onun yerini almaz. Dijital euro, insanların hızlı ve güvenli bir şekilde dijital olarak ödeme yapma eğilimini karşılamak için nakit paranın yanında var olacaktır. Nakit para, euro bölgesinde mevcut olmaya devam edecektir, aynı şekilde şu anda kullanılan özel elektronik ödeme araçları da mevcut olmaya devam edecektir.

Bir dijital euro, Eurosystem içinde alternatif bir para birimi mi olacak?

Hayır, bir dijital euro, Avrupa'da euro kullanarak ödeme yapmanın başka bir yoludur, yani Avrupa'nın tek para birimi olan euronun bir türüdür. Bir dijital euro, banknotlarla 1'e 1 değiştirilebilir olacaktır. Bir dijital euro, insanların ve şirketlerin dijital ödeme yapma eğilimlerine yanıt olarak ortaya çıkacaktır.

Proje şu anda nerede duruyor ve Avrupa yasama organları nasıl dahil oluyor?

Haziran 2023'te Avrupa Komisyonu, muhtemel bir dijital euro için [bir yasa tasarısı önerisi](#) sundu. Bu yasal düzenleme, gelecekteki bir

Furthermore, a digital euro will strengthen Europe's strategic independence and monetary sovereignty and contribute to the efficiency of the European payment ecosystem by promoting innovation and enhancing resilience against potential cyberattacks or technical interruptions, such as energy outages.

Does the digital euro replace cash?

No, the digital euro complements cash; it does not replace it. The digital euro will coexist with cash to meet the growing trend of people making digital payments quickly and securely. Cash will continue to be available in the Euro area, just as the currently used private electronic payment instruments will persist.

Will the digital euro be an alternative currency within the Eurosystem?

No, a digital euro is not an alternative currency within the Eurosystem. It is a form of the euro, which is the single currency of Europe. A digital euro will be exchangeable one-to-one with banknotes. It will emerge in response to the growing trend of people and businesses making digital payments quickly and securely.

Where does the project stand now, and how are European legislative bodies getting involved?

In June 2023, the European Commission proposed a bill for a potential digital euro. This legal regulation aims to provide a widely accepted,

dijital euro ile euro bölgesi genelinde yaygın olarak kabul edilen, ucuz, güvenli ve dayanıklı bir kamu parasının kullanımını sağlamak amacını taşır.

Dijital euro'yu kimler kullanabilecek?

Avrupa Komisyonu tarafından sunulan yasa önerisi ve Avrupa Ekonomik Alanı Anlaşması'na uygun olarak, dijital euro, euro bölgesinde ikamet eden veya kurulu olan kişilere sunulacaktır. Bir euro bölgesi ülkesinde ikamet eden veya kurulu olan kişiler, ilkesel olarak bir dijital euro hesabına erişim sağlayabilirler.

Euro bölgesi dışındaki tüccarlar da, bir euro bölgesi ödeme hizmeti sağlayıcısına sahip oldukları sürece dijital euro ödemelerini kabul edebilirler.

Daha ileride, yasal gelişmelere bağlı olarak, Avrupa Ekonomik Alanı ve/veya seçilmiş üçüncü ülkelerdeki tüketiciler ve tüccarlar da dijital euro'ya erişebilirler.

İnsanlar neden bir dijital euro kullanmak isteyebilir?

Bir dijital euro, euro bölgesinin her yerinde ve her zaman kullanılabilen bir ödeme çözümü olacaktır. Tüketiciler, mağazalarda, çevrimiçi veya kişiden kişiye ücretsiz olarak kullanabilecekleri evrensel bir dijital ödeme aracına sahip olacaklardır. İnsanlar, kamusal bir ödeme aracını kullanırken dijital ödeme seçeneğini tercih etme seçeneğine sahip olacaklardır.

affordable, secure, and resilient public currency for use throughout the euro area in the future.

Who will be able to use the digital euro?

As per the bill proposed by the European Commission and in compliance with the European Economic Area Agreement, the digital euro will be made available to individuals residing in or established in the euro area. Individuals residing in or established in a euro area country can, in principle, access a digital euro account.

Merchants outside the euro area can also accept digital euro payments if they have a euro area payment service provider.

Further down the line, depending on legal developments, consumers and merchants in the European Economic Area and/or selected third countries may also have access to the digital euro.

Why might people want to use a digital euro?

A digital euro will be a payment solution that can be used universally and at all times throughout the euro area. Consumers will have access to a universally accepted digital payment instrument that they can use for free in stores, online, or for peer-to-peer transactions. People will have the option to use digital payments when using a public payment instrument.

Bir dijital euro, dijital çağda nakit benzeri özellikleri koruyacak ve yüksek gizlilik seviyesi ve kullanım kolaylığı gibi özellikler sunacaktır. Ayrıca, dijital ödemelerde en yüksek gizlilik düzeyini sağlayacaktır: Eurosystem, kullanıcıların kişisel verilerine erişmeyecek veya saklamayacaktır. Dahası, çevrimdışı dijital euro ödemeleri için daha yüksek gizlilik seçenekleri, ödemenin yalnızca ödeyici ve alıcı tarafından bilineceği anlamına gelecektir.

Bir dijital euro, güvenli ve kullanımı kolay olacaktır ve dijital veya finansal becerilere sahip olmayan veya banka hesabına veya dijital cihazlara erişimi olmayan kişilerin geride kalmamasını sağlamak için dijital finansal dahililiği teşvik etmeyi amaçlamaktadır. Dijital euro, temel dijital euro hizmetlerini kullanarak kimseyi geride bırakmamayı hedeflemektedir.

Dijital euro'nun euro bölgesinin her yerinde kullanılabilir ve erişilebilir olması için Avrupa Komisyonu tarafından sunulan yasa önerisi, tüccarlar tarafından zorunlu kabul ve denetlenen araçlar tarafından zorunlu dağıtım öngörmektedir.

Bir dijital euro nasıl çalışır?

Bir dijital euro, kişilerin, hangi euro bölgesi ülkesinde bulduklarına veya hangi ödeme hizmeti sağlayıcısına sahip olduklarına bakılmaksızın, fiziksel ve çevrimiçi mağazalarda ve bireyler arasında güvenli anlık ödemeler yapmalarına olanak tanır. ECB, bunun pratikte nasıl çalışabileceğini araştırmaktadır.

A digital euro will preserve cash-like features in the digital age and offer characteristics such as a high level of privacy and ease of use. Additionally, it will provide the highest level of privacy for digital payments: the Eurosystem will not have access to or store users' personal data. Moreover, higher privacy options for offline digital euro payments will mean that only the payer and the payee are aware of the payment.

A digital euro aims to be secure and easy to use and is designed to promote digital financial inclusion for those who do not have digital or financial skills or access to bank accounts or digital devices.

To make the digital euro available and accessible throughout the euro area, the bill proposed by the European Commission foresees mandatory acceptance by merchants and mandatory distribution by regulated intermediaries.

How does a digital euro work?

A digital euro allows individuals to make secure instant payments in both physical and online stores and between individuals, regardless of their location within the euro area or their payment service provider. The ECB is exploring how this could work in practice.

Örneğin, Eurosystem, herkesin eşit erişime sahip olabileceği özel bir dijital euro uygulaması geliştirebilir. Alternatif olarak, bankalar da dahil olmak üzere araçlar, müşterilerinin zaten aşına oldukları mevcut uygulamalarının içine dijital euro hizmetlerini entegre edebilirler. Her durumda, banka hesabına veya dijital cihazlara erişimi olmayan kişiler, postaneler gibi kamusal araçları kullanarak fiziksel bir kartla dijital euro ile ödeme yapabilirler.

Her durumda, bir dijital euro hem çevrimiçi hem de çevrimdışı işlevsellik sunar ve sınırlı bağlantı durumlarını öngörür. Dijital euro ödemeleri çevrimdışı yapıldığında, ödeme bilgileri sadece ödeyici ve alıcı tarafından bilineceği için en yüksek gizlilik seviyesini sağlar.

Dijital Euroda gizlilik nasıl olur?

Gizlilik, bir dijital euro'nun en önemli tasarım özelliklerinden biridir. Eurosystem, kişilerin kişisel ödeme verilerine ticari bir ilgi duymaz ve böyle verileri üçüncü taraflarla paylaşmak istemez. Bu nedenle, Eurosystem, kullanıcıların kişisel bilgilerini görmek veya saklamak istemez.

Bir dijital euro, kişilerin ödeme verilerini Avrupa düzenlemelerine uygun olarak yasadışı faaliyetleri önlemek için gerekenler dışında üçüncü taraflarla paylaşmadan ödemeler yapmalarına olanak tanır

Bir dijital euro, kişilerin ödeme verilerini Avrupa düzenlemelerine uygun olarak yasadışı faaliyetleri önlemek için gerekenler dışında üçüncü taraflarla paylaşmadan ödemeler yapmalarına olanak tanır.

For example, the Eurosystem could develop a dedicated digital euro app that everyone can access. Alternatively, intermediaries, including banks, can integrate digital euro services into their existing apps that their customers are already familiar with. In any case, individuals who do not have access to bank accounts or digital devices can make payments with a physical card through public intermediaries like post offices.

In any case, a digital euro provides functionality for both online and offline scenarios, anticipating limited connectivity situations. When digital euro payments are made offline, they provide the highest level of privacy because payment information is only known to the payer and the payee.

How will privacy work in a digital euro?

Privacy is one of the key design features of a digital euro. The Eurosystem has no commercial interest in individuals' personal payment data and does not wish to see or store such data. As a result, the Eurosystem does not want to share user's personal information with third parties, except for what is required to prevent illegal activities in compliance with European regulations.

A digital euro allows individuals to make payments without sharing their payment data with third parties beyond what is necessary to prevent illegal activities in compliance with European regulations.

Dahası, bir dijital euro'nun çevrimdışı işlevselliği, ödeme bilgilerinin yalnızca ödeyici ve alıcı tarafından bilineceği için daha yüksek bir gizlilik düzeyi sunar.

Bir dijital euro, blockchain gibi dağıtık defter teknolojilerine dayalı mı olacaktır?

Eurosystem, bir dijital euro'nun geliştirilmesinde, merkezi ve dağıtık olmak üzere farklı yaklaşımlar ve teknolojileri denemektedir, bu dağıtık defter teknolojilerini içerir. Ancak henüz bir karar alınmamıştır.

Bir dijital euro'nun tanıtılması, Avrupa'da ödemeleri siber saldırılara daha savunmasız hale getirir mi?

Diğer dijital altyapılar gibi bir dijital euro da siber saldırıların hedefi olabilir. Bu riski azaltmak için bir dijital euro tasarımı, siber saldırılara karşı dayanıklı ve geleceğe uygun bir ortam oluşturacak en son teknolojilere dayanacaktır.

Bir dijital euro, stablecoinler ve kripto varlıklardan nasıl farklı olacaktır?

Bir dijital euro, merkez bankası para birimidir. Bu, bir merkez bankası tarafından desteklenir ve bunu kullanan kişilerin ihtiyaçlarına uygun olarak tasarlanır. Risk içermez ve gizliliği ve veri korumasını sağlar. Merkez bankalarının, fiziksel veya dijital biçimde olsun, paranın değerini koruma görevleri vardır.

Furthermore, the offline functionality of a digital euro offers a higher level of privacy since payment information is known only to the payer and payee.

Will a digital euro be based on distributed ledger technologies like blockchain?

The Eurosystem is exploring various approaches and technologies, including both centralized and distributed ledger approaches, in the development of a digital euro. However, no final decision has been made yet.

Does the introduction of a digital euro make payments in Europe more vulnerable to cyberattacks?

Like other digital infrastructures, the digital euro could become a target for cyberattacks. To mitigate this risk, the design of a digital euro will be based on the latest technologies to provide a resilient and future-proof environment against cyberattacks.

How will a digital euro be different from stablecoins and cryptocurrencies?

A digital euro is a digital currency backed by a central bank and designed to meet the needs of its users. It carries no risk and respects privacy and data protection. Central banks have a mandate to maintain the value of money, whether in physical or digital form.

Stabilcoinlerin istikrarı ve güvenilirliği, nihayetinde onları ihraç eden varlığa ve zaman içinde paranın değerini koruma taahhütlerinin inanılabilirliğine bağlıdır. Özel ihraççılar, ticari amaçlar için kişisel verileri kullanabilirler.

2. Dijital Paranın Kullanım Alanları

([kaynak](#))

İnsandan insana (Person-to-person) - İki kişi arasında yapılan ödemeler.

Tüketiciden işletmeye (Consumer-to-business)- Fiziksel bir mağazadan (satış noktasında ödeme) veya e-ticaret yoluyla çevrimiçi olarak satın alınan mal veya hizmetler için yapılan ödemeler.

İşletmeler tarafından başlatılan ödemeler - Bir firmadan başka bir firmaya yapılan (B2B) ödemeler.

X2G-G2X ödemeleri - Devlete yapılan ödemeler (örneğin vergiler) ve devlet tarafından yapılan ödemeler (ödenekler ve sübvansiyonlar)

Makine tarafından başlatılan ödemeler - Önceden belirlenmiş koşullara dayalı olarak bir cihaz ve/veya yazılım tarafından başlatılan tam otomatik ödemeler.

The stability and reliability of stablecoins ultimately depend on the credibility of the issuer and their commitment to preserving the value of the currency over time. Private issuers may use personal data for commercial purposes

2. Use Cases of Digital Currency

([source](#))

Person-to-person (P2P) - Payments made between two individuals.

Consumer-to-business (C2B) - Payments for goods or services purchased in physical stores (point-of-sale payments) or online through e-commerce.

Business-initiated payments - Payments made from one business to another (B2B payments).

X2G-G2X payments - Payments to the government (e.g., taxes) and payments from the government (grants and subsidies).

Machine-initiated payments - Fully automated payments initiated by a device and/or software based on predefined conditions.

3. Dijital Para Sisteminin İşleyişi

3.1. Dijital Paranın Deftere Göre Yapılandırılması

Hesap Bazlı: Merkez bankasının defterlerindeki nakit mevduat hesaplarını dijitalleştirmek amacıyla kullanılır. Hesap tabanlı bir sistem, kaydın durumunu, her biri karşılık gelen bir bakiyeye sahip olan hesapların bir listesi olarak kaydeder. Bir işlem gerçekleştiğinde, sistem genellikle ödeme yapan hesap ve alıcı hesabının bakiyelerini artırarak ve azaltarak kayıtları günceller. Bu türün bir örneği Ethereum DLT'dir, burada kayıt durumu "hesaplar" adlı nesnelere oluşur ve bunlarla ilişkilendirilen bir bakiye vardır. ([kaynak](#))

Token Bazlı: Merkez bankası ve sahibi arasında bir hesap ilişkisi olmayan bir dijital jeton şeklinde tasarımı kullanılır. bir token tabanlı sistem, kaydın durumunu, her birinin karşılık gelen bir değere sahip olan bireysel nesnelere, yani tokenların bir listesi olarak kaydeder (örneğin 10€). Farklı tokenlar aynı kayıta kaydedilebilse de, her birinin belirli bir değeri olur, bu değer aynı zamanda ondalık bir sayı olabilir (örneğin 10.55€), ancak tokenın ömrü boyunca değişmez. Bu türün bir örneği Bitcoin DLT'dir. Her ödeme için, ödeme yapanın sahip olduğu harcanmamış token seti yok edilir ve (genellikle) toplam değeri aynı olan iki token eşzamanlı olarak oluşturulur: biri ödeme olarak alıcıya gider ve diğeri değişim olarak ödeme yapan kişiye geri döner. ([kaynak](#))

3. Functioning of the Digital Currency System

3.1. Structuring Digital Currency Ledger

Account-Based: Used to digitize the cash deposit accounts in the central bank's ledgers. An account-based system records the state of the ledger as a list of accounts, each having a corresponding balance. When a transaction occurs, the system typically updates the records by increasing and decreasing the balances of the paying and receiving accounts. An example of this type is Ethereum DLT, where the state of the ledger consists of objects called "accounts" with associated balances. ([source](#))

Token-Based: Designed as a digital token without an account relationship between the central bank and the owner. In a token-based system, the ledger's state is recorded as a list of individual objects, namely tokens, each with a corresponding value (e.g., 10€). While different tokens can be recorded in the same ledger, each has a specific value, which can also be a decimal number (e.g., 10.55€), but it remains unchanged throughout the token's lifetime. An example of this type is Bitcoin DLT. For each payment, the unspent token set owned by the payer is destroyed, and (usually) two tokens of equal total value are simultaneously created: one goes to the payee as payment, and the other returns to the payer as change. ([source](#))

3.2. Kullanım Modeli

WholeSale/Toptan Satış: Rezervin banka ve finans kuruluşları aracılığı ile kullanılmasıdır. Merkez Bankası tarafından çıkarılan (Merkez Bankası hesaplarındaki mevduatlara ek olarak) para biçimi, Merkez Bankası'nın mevcut iş ortaklarına (ticari bankalar gibi) yeni işlevsellikler sunar (örneğin finansal piyasa işlemleri için) ([kaynak](#)).

RetailSale/Perakende Satış: Rezervin doğrudan kişiler tarafından kullanılmasıdır. Merkez Bankası tarafından (nakdin yanı sıra) çıkarılan ve banka olmayan kişilere (bireysel kişiler ve varsa şirketler) mal veya hizmetlerin dijital ödemesi için kullanılabilen bir para biçimi. ([kaynak](#))

3.3. Piyasaya Sürülme şekli

Doğrudan: Merkez bankası kendisi piyasaya sunar ve dolaşımı idare eder. Bu senaryoda, bireyler ve işletmeler, CBDC'leri bir Merkez Bankasındaki özel hesapları aracılığıyla tutar ve böylece aracıları ortadan kaldırır. Bu durum mevcut finansal sistemin yapısını etkileyerek Merkez Bankası'nın rol ve sorumluluklarını artırabilir. ([Kaynak](#))

Dolaylı: İşlemler bankalar ve finans kuruluşları aracılığı ile yürütülür. Dolaylı perakende CBDC senaryosunda, dijital para biriminin ihracı, doğrudan bireylere ve işletmelere verilen parayı desteklemekten sorumlu finansal kuruluşlar tarafından gerçekleştirilir. Ayrıca diğer finansal kuruluşlara ödeme mesajlarının

3.2. Usage Model

Wholesale: The use of the reserve through banks and financial institutions. The form of money issued by the central bank (in addition to deposits in central bank accounts) offers new functionalities to existing business partners of the central bank (such as commercial banks) for financial market transactions, for example. ([source](#))

Retail: The direct use of the reserve by individuals. A form of money issued by the central bank (in addition to cash) that can be used for digital payment of goods or services to non-bank individuals (individuals and, if applicable, companies). ([source](#))

3.3. Launch Method

Direct: The central bank introduces and manages circulation itself. In this scenario, individuals and businesses hold CBDCs through special accounts with a central bank, thus eliminating intermediaries. This situation may impact the structure of the current financial system, enhancing the role and responsibilities of the central bank. ([source](#))

Indirect: Transactions are carried out through banks and financial institutions. In the indirect retail CBDC scenario, financial institutions responsible for supporting the issuance of the digital currency are responsible for providing money directly to individuals and businesses. They are also responsible for sending payment messages to other financial institutions and transmitting payment instructions to the central bank for payment settlement. ([source](#))

gönderilmesinden ve ödeme tasfiyesi için ödeme talimatlarının Merkez Bankası'na iletilmesinden de sorumludurlar.([Kaynak](#))

3.4. Dijital Para Kullanan Ülkeler

3.4.1. Bahamalar Sand Dolar

Sand Dollar, Ekim 2020'de Bahamalar Merkez Bankası tarafından çıkarıldı. Sand Dollar, dünyada ülke çapında çıkarılan ilk CBDC olma özelliğini taşımaktadır.

Bahamalar'da, birçok farklı adaya bölünmüş olan ülkenin coğrafyası nedeniyle ticari aktörlerin her alanda faaliyet göstermesi mümkün olmadığından nüfusun bir kısmı finansal hizmetlere erişemiyor. Nüfusun yüzde 20'sinin bir banka hesabı olmadığı tahmin edilen Bahamalar'da Sand Dollar'ın finansal katılımın iyileştirilmesine ve kara para aklama ve yasa dışı ekonomik faaliyetlere karşı güvenliğin güçlendirilmesine yardımcı olabileceği öngörülmektedir.

Sand Dollar, hem toptan hem de perakende uygulamalar için mevcuttur. Toptan satış uygulaması, takas odası işlemlerine benzer şekilde, bankalararası düzeydeki ödeme mutabakatları için kullanımı kısıtlamaktadır.

3.4. Countries Using Digital Currency

3.4.1. Bahamas Sand Dollar

The Sand Dollar was issued by the Central Bank of the Bahamas in October 2020. The Sand Dollar holds the distinction of being the first CBDC (Central Bank Digital Currency) issued nationwide in the world.

In the Bahamas, due to the country's geography, which is divided into many different islands, it is not possible for commercial actors to operate in every area, and a portion of the population lacks access to financial services. The Sand Dollar is expected to improve financial inclusion and enhance security against money laundering and illegal economic activities in The Bahamas, where it is estimated that 20% of the population does not have a bank account.

The Sand Dollar is available for both wholesale and retail applications. The wholesale application is used for interbank payment settlements, similar to clearinghouse transactions.

The retail application enables the general public to make and receive digital payments. Each holder can legally possess equivalent accounts

Perakende uygulaması, genel halkın dijital ödemeler yapmasına ve almasına imkan vermektedir. Her hamil, Merkez Bankası üzerinde doğrudan hak iddia etmek suretiyle yasal olarak Merkez Bankası nezdinde eşdeğer hesaplara sahip olabilmektedir. ([Kaynak](#))

3.4.2. Karayipler D-Cash

Doğu Karayip Birliği'ndeki ülkeler, işlemleri hızlandırmak ve banka hesabı olmayan insanlara hizmet vermek amacıyla kendi dijital para birimi biçimlerini oluşturdu. Katılan yedi ülke, Antigua ve Barbuda, Dominika, Grenada, Montserrat, St. Kitts ve Nevis, Saint Lucia ve St. Vincent ve Grenadinler'dir.

Doğu Karayip Merkez Bankası, bazı bireysel ulusların benzer mevcut sistemlere sahip olmasına rağmen, "DCash"ın dünyanın herhangi bir para birliği tarafından piyasaya sürülen ilk blok zinciri tabanlı para birimi olduğunu öne sürüyor.

Sistem, kullanıcıların banka hesabı olmasa bile - ancak bir akıllı telefonla - indirilmiş bir uygulamayı kullanmalarına ve bir QR kodu aracılığıyla ödeme yapmalarına olanak tanıyor.

Nüfusun finansal olarak dışlanmış kesimlerine ulaşmak minimum bir CBDC bakiyesi veya minimum harcama tutarı gerekmemektedir. ([Kaynak](#))

with the Central Bank by directly asserting claims against the Central Bank. ([Source](#))

3.4.2. Caribbean D-Cash

Countries in the Eastern Caribbean Union have created their own digital currency formats to expedite transactions and serve individuals without bank accounts. The seven participating countries are Antigua and Barbuda, Dominica, Grenada, Montserrat, St. Kitts and Nevis, Saint Lucia, and St. Vincent and the Grenadines.

The Eastern Caribbean Central Bank claims that "DCash" is the world's first blockchain-based currency issued by any currency union, even though individual nations have similar existing systems.

The system allows users to download an app on a smartphone and make payments using a QR code, even if they do not have a bank account. There is no minimum CBDC balance or minimum spending requirement to reach financially underserved segments of the population. ([Source](#))

3.5. Dijital Para ve Gizlilik

Avrupa Birliđi merkez bankası, gizlilik konusunda farklı modeller üzerinde çalışmaktadır. Yayınladıkları [rapora göre](#), Dijital para, kullanım amacı ve tasarım geređi gizliliđi sađlamakta ve bireylere kişisel verileri ve paraları üzerinde kontrol yetkisi vermektedir. Merkez bankasının kişisel verilere erişimi olmayacak (insanların varlıklarını, işlem geçmişlerini veya ödeme modellerini göremeyecek), ancak yasal gerekliliklere uyulduđunun takibini sađlayabilmek için aracı kurumlar kişisel ve işlem verilerine erişim sađlayabilecektir.

Çevrimdışı dijital euro kullanımı, nakit kullanımına yakın bir derecede gizlilik sađlayabilecek olup potansiyel olarak en yüksek düzeyde gizlilik gereksinimini karşılaması (siyasi karara bađlı olarak deđişiklik göstermek suretiyle) öngörülmektedir.

Riske dayalı bir yaklaşımla sınıflandırma yapılması, daha az riskli/düşük deđerli işlemler söz konusu olduđunda daha fazla mahremiyet sađlanması önünü açabilecektir.

Dijital para tasarımı, nihai olarak yasa koyucular tarafından mahremiyet için belirlenen koşullara uymakla yükümlü olacaktır. ([kaynak](#))

3.6. Dijital Paranın Hukuki Altyapısı

IMF Çalışma grubunun 2020 yılında yayınladıđı [raporda](#) dijital para için yapılacak mevzuat çalışmaları dikkate alınması gereken hususlar tavsiye edilmiştir:

3.5. Digital Currency and Privacy

The European Union central bank is working on different models regarding privacy. According to their [report](#), digital currency inherently provides privacy by design and purpose of use, giving individuals control over their personal data and money. The central bank will not have access to personal data (it won't be able to see people's assets, transaction histories, or payment patterns), but intermediary institutions will be able to access personal and transaction data to ensure compliance with legal requirements.

Offline use of digital euros is expected to provide a degree of privacy close to cash usage, potentially meeting the highest privacy requirements, subject to political decisions.

A risk-based classification approach could open the way for greater privacy when less risky or low-value transactions are involved.

The design of digital currency will ultimately have to comply with conditions set by legislators. ([Source](#))

3.6. The Legal Framework for Digital Currency

In a [report](#) published by the IMF Working Group in 2020, several considerations for legislative efforts regarding digital currency were recommended:

- There should be strong legal foundations.

- Güçlü Yasal temeller olmalıdır
- Dijital para, mevzuatta “para” olarak düzenlenmelidir
- Banka Mevzuatı, Para Mevzuatı dijital para içerecek şekilde regüle edilmelidir.
- Vergi Hukuku, Özel Hukuk (mülkiyet hukuku dahil), sözleşme hukuku, ödeme sistemleri, kişisel verilerin korunması hukuku, milletlerarası özel hukuk alanında mevzuat çalışmaları gerekir
- Merkez Bankasına mevzuatta, “hesap bazlı” veya dijital token bazlı” dijital para ihraç etme yetkisi verilmelidir.
- Güvenlik siber suçlar düşünülerek sağlanmalıdır.

3.7. Dijital Türk Lirası Çalışmaları

25 Ekim 2022 Tarihli Resmi Gazete’de yayımlanan [2023 Yılı Cumhurbaşkanlığı Yıllık Programı](#)’nda blokzincir tabanlı dijital Türk Lirası için test aşamasına gelindiği açıklandı.

Merkez Bankası Dijital Türk Lirası Araştırma Geliştirme Projesi ikinci faz pilot bulguları doğrultusunda, Dijital Türk lirasının ödemeler için gelecek seneden itibaren kullanılabilmesi bilgisi paylaşıldı.

Bankaların da bu süreçte aktif yer alacağı; birlikte araştırma, geliştirme ve test çalışmaları yapılacağı belirtildi. Programa göre, Dijital Türk Lirası sistemlerinin dijital kimlik ve FAST sistemleri ile araştırmageliştirme kapsamında entegrasyon çalışmaları tamamlanacaktır.

29 Aralık 2022 tarihinde yayınlanan [duyuru](#) ile Türkiye Cumhuriyet Merkez Bankası (TCMB) öncülüğünde yürütülmekte olan Dijital

- Digital currency should be regulated in legislation as "money."
- Banking regulations and monetary laws should be amended to encompass digital currency.
- Legislation work is required in areas such as tax law, private law (including property law), contract law, payment systems, personal data protection law, and international private law.
- The legal framework should grant the central bank the authority to issue digital currency, either "account-based" or "digital token-based," with provisions ensuring cybersecurity.

3.7. Digital Turkish Lira Initiatives

The 2023 [Presidential Annual Program](#), published in the Official Gazette on October 25, 2022, announced that the testing phase for a blockchain-based digital Turkish Lira had been reached. Following the second-phase pilot findings of the Central Bank's Digital Turkish Lira Research and Development Project, it was shared that the digital Turkish Lira could be used for payments starting in the following year.

Banks will actively participate in this process and collaborate on research, development, and testing. According to the program, integration work for the Digital Turkish Lira systems with digital identity and FAST systems will be completed as part of research and development.

In an [announcement](#) released on December 29, 2022, it was stated that, within the scope of the first-phase work of the Digital Turkish Lira Project, the first payment transactions on the Digital Turkish Lira Network had been successfully completed under the leadership of the

Türk Lirası Projesi'nin birinci faz çalışmaları kapsamında, **Dijital Türk Lirası Ağı üzerindeki ilk ödeme işlemleri başarılı bir şekilde gerçekleştirildiği açıklanmıştır. Duyuruya göre,** TCMB, teknoloji paydaşları ile birlikte yürüttüğü dar kapsamlı ve kapalı devre pilot uygulama testlerine 2023 yılının ilk çeyreğinde de devam edecektir. Yapılan testler sonucu elde edilen bulgular geniş kapsamlı bir değerlendirme raporu ile kamuoyu ile paylaşılacaktır.

4. Sanal Para Terminolojisi Arasındaki Farklar

Konu	Elektronik Para	Kripto Para	Dijital Para (CBDC)
Yetki ve Denetim	Merkez Bankası-Lisanslı Kuruluşlar	Merkeziyetsiz	Merkez Bankası
Yasalık/Tedavül	Yasalarla Düzenlenmiş	Yasalarla (kısmi) Düzenlenmiş	Yasalarla Düzenlenmiş
Karşılık	Fiziki karşılığı var	Fiziki karşılığı yok	Fiziki karşılığı yok
Gizlilik/Anonimlik	Kimlik Doğrulama (Anonim ön ödemeli araçlar hariç)	Anonim	Yarı Anonim

Central Bank of the Republic of Turkey (TCMB). According to the announcement, **the TCMB, along with technology stakeholders, will continue limited-scale and closed-circuit pilot application tests in the first quarter of 2023.** The findings from these tests will be shared with the public in a comprehensive evaluation report.

4. Differences in Virtual Currency Terminology

Subject	Electronic Money	Cryptocurrency	Digital Currency (CBDC)
Authority and Control	Central Bank-Licensed Institutions	Decentralized	Central Bank
Legality/Circulation	Regulated by Laws	is partially regulated by Laws	Regulated by Laws
Receipt of funds	Has receipt of funds	No Physical fund	No Physical fund
Privacy/Anonymity	Identity Verification (Excluding Anonymous Prepaid Instruments)	Anonymous	Semi-Anonymous

Güvenlik	Fiziki, idari ve teknik güvenlik	Blokzincir	DLT
Ödeme Aracı mı?	Ödeme Aracı	Ödemelerde Kullanılması Yasak	Ödeme Aracı
İhraç	Eşit değerinde itibari paranın koruma hesabına aktarılması gerekir.	Madencilik	Doğrudan Merkez Bankası ihraç eder. İtibari para yoktur.

Security	Physical, Administrative, and Technical Security	Blockchain	DLT
Payment Instrument?	Payment Instrument	Forbidden for Payments	Payment Instrument
Issuance	Transfer of Equivalent Value to the Protection Account	Mining	Direct Issuance by Central Bank