



Kamu İç Denetçileri Derneği Meşrutiyet Caddesi Konur Sokak No: 36/6 Kızılay - ANKARA

www.kidder.org.tr/denetisim/ • denetisim@kidder.org.tr

ISSN 1308-8335

Yıl: 16, Sayı: 33, 178-196, 2025

Derleme Makale

MERKEZ BANKASI DİJİTAL PARALARINDA DENETİM VE RİSK YÖNETİMİ*

(AUDIT AND RISK MANAGEMENT IN CENTRAL BANK DIGITAL CURRENCIES)

Ayten ÇETİN¹, Serdar ALPAY²

ÖZ

Bu çalışma, merkez bankası dijital paralarının (CBDC) denetim ve risk yönetimi süreçleri üzerindeki etkilerini stratejik ve çok katmanlı bir bakış açısıyla incelemektedir. Dijital dönüşüm sürecinin merkezinde yer alan CBDC sistemleri; yalnızca ödeme altyapılarını değil, aynı zamanda kamu maliyesi denetimini, yönetim yapısını ve veri işleme sistemlerini dönüştürmektedir. Bu çerçevede Avrupa Birliği ile Çin Kanada, İngiltere ve ABD gibi öncü uygulamalar karşılaştırmalı olarak değerlendirilmiştir. Türkiye'nin Dijital Türk Lirası Projesi özelinde ise yasal düzenlemeler, kurumsal kapasite, veri koruma, siber güvenlik, çok paydaşlı denetim çerçevesi ve uluslararası uyum konularına yönelik stratejik çıkarımlar ve uygulama önerileri geliştirilmiştir. Sonuç olarak, CBDC'ler yalnızca dijital ödeme aracı değil; kamu denetimi, finansal şeffaflık ve risk yönetimi alanlarında yenilikçi kamu politikalarının uygulanmasına katkı sunabilecek çok işlevli bir araç olarak değerlendirilmektedir.

Anahtar Kelimeler: Merkez Bankası Dijital Parası, Finansal Denetim, Risk Yönetimi, Dijital Finansal Mimari, Kamu Maliyesi.

JEL Kodları: E42, E58, G21, G28, F65

ABSTRACT

This study examines the impact of central bank digital currencies (CBDCs) on financial audit and risk management processes from a strategic and multi-layered perspective. Positioned at the core of the digital transformation process, CBDC systems are reshaping not only payment infrastructures but also public financial oversight, governance structures, and data processing mechanisms. In this context, leading CBDC initiatives undertaken by the European Union, China, Canada, the United Kingdom, and the United States have been subject to comparative evaluation.. Focusing on Türkiye's Digital Turkish Lira Project, the study develops strategic insights and implementation recommendations regarding legal frameworks, institutional capacity, data protection, cybersecurity, multi-stakeholder audit models, and international compliance. In conclusion, CBDCs are considered not merely as digital payment tools but as multifunctional instruments capable of supporting the implementation of innovative public policies in areas such as financial transparency, public oversight, and risk governance.

Keywords: Central Bank Digital Currency, Financial Audit, Risk Management, Digital Financial Architecture, Public Finance

JEL Classification: E42, E58, G21, G28, F65

¹ Öğr. Üyesi, Prof. Dr., Marmara Üniversitesi, Muhasebe Finansman Anabilim Dalı, İstanbul, Orcid Id: 0000-0002-4212-5253, acetin@marmara.edu.tr

² Doktora Öğrencisi, Marmara Üniversitesi, Muhasebe Finansman Anabilim Dalı, İstanbul, Orcid Id: 0000-0003-2047-3799, alpay.serdar@gmail.com

* Bu makale yazarlar tarafından Marmara Üniversitesi, Sosyal Bilimler Enstitüsü, İşletme Anabilim Dalı için hazırlanan “Dijital Para Sistemlerinde Fırsatlar ve Riskler: Finans Sektörü Üzerine Bir Uygulama” adlı doktora tezinden üretilmiştir.

1. GİRİŞ

21. yüzyılda dijitalleşmenin etkisiyle finansal sistemler, yapısal bir dönüşüm sürecine girmiştir. Söz konusu dönüşüm; geleneksel bankacılık, ödeme altyapıları, sermaye piyasaları ve merkez bankası işleyişinde kapsamlı değişikliklere neden olmaktadır. Süreç, yalnızca teknolojik bir geçişin ötesinde; ekonomik ilişkilerin yeniden tanımlanmasını, para politikasının yeni dijital araçlarla şekillendirilmesini ve denetim sistemlerinin çağın ihtiyaçlarına göre yeniden tasarlanmasını içermektedir (Adrian & Mancini-Griffoli, 2021; BIS, 2020).

Dijital dönüşüm sürecinde merkezi bir konuma yerleşen Merkez Bankası Dijital Paraları (CBDC), merkez bankaları tarafından doğrudan ihraç edilen ve yasal ödeme aracı statüsüne sahip dijital para birimleridir. Bu özellikleriyle, özel sektörün geliştirdiği kripto varlık ve stabil kripto paralardan ayrılmakta olup, para politikası üzerindeki kamu gücünün dijital ortamda sürdürülebilirliğini sağlamaktadırlar. Bilhassa dijital cüzdanlar, mobil ödeme sistemleri ve fintech çözümlerinin yaygınlaştığı bir ortamda, merkez bankalarının dijital para alanında yeniden inisiyatif üstlenmesi gerekliliği, CBDC girişimlerini stratejik öncelikler arasına taşımıştır (BoE, 2023).

CBDC'ler yalnızca dijital ödeme sistemleri değil; aynı zamanda finansal kapsayıcılığın artırılması, kayıt dışı ekonomiyle mücadele, kamu ödemelerinin hedeflenmesi ve vergiye uyumun güçlendirilmesi gibi çeşitli kamu politikası hedeflerini destekleyebilecek çok işlevli araçlardır. Bu yapıların en çarpıcı yönlerinden biri ise, geleneksel finansal denetim ve risk yönetimi yaklaşımlarını dönüştürebilecek kapasiteye sahip olmalarıdır. Dijital ortamda kaydedilen işlemler sayesinde; anlık raporlama, blok zincir ile desteklenen izlenebilirlik, otomatik kontrol sistemleri ve yapay zekâ tabanlı anomali tespit mekanizmaları kamu maliyesi denetiminde önemli bir potansiyel sunmaktadır (FATF, 2021b).

Diğer taraftan bu fırsatlar yeni riskleri de beraberinde getirmektedir. Siber güvenlik tehditleri, veri mahremiyeti sorunları, teknik altyapı zayıflıkları ve yönetim karmaşası, CBDC uygulamalarının başarı şansını belirleyen temel faktörler arasındadır. Bu nedenle merkez bankaları sadece teknolojik bir çözüm üretmek ile kalmamalı; aynı zamanda kurumsal kapasiteyi artırmalı, düzenleyici çerçeveyi güncellemeli ve toplumsal kabulü sağlayacak bütüncül stratejiler geliştirmelidir (IMF, 2025; OECD, 2020).

Bu çerçevede makalenin temel amacı; CBDC sistemlerinin finansal denetim ve risk yönetimi üzerindeki etkilerini küresel ve yerel ölçeklerde kapsamlı şekilde analiz etmektir. Çalışmada Avrupa Birliği ile Çin, Kanada, İngiltere gibi ülkelerde CBDC deneyimleri ele alınmakta; bu örneklerden hareketle Türkiye için stratejik öneriler geliştirilmektedir. Özellikle Türkiye Cumhuriyet Merkez Bankası (TCMB) öncülüğünde yürütülen Dijital Türk Lirası Projesi, teknik boyutlarının ötesinde bir denetim reformu perspektifiyle incelenmektedir. Böylece, dijitalleşmenin merkez bankacılığına getirdiği yeni çerçevenin hem fırsatları hem de sınırları ortaya konulmaktadır.

2. DİJİTAL PARA KAVRAMI VE EKOSİSTEMİ

Dijital paralar, günümüz finans dünyasında dönüşüm süreçlerinin merkezinde yer almakta ve geleneksel yapıların yeniden şekillenmesinde etkili olmaktadır. Geleneksel anlamda fiziksel paraya dayalı para sistemlerinin dijital temsillere evrilmesi, sadece ödeme sistemlerinde değil, aynı zamanda denetim, finansal kapsayıcılık, veri politikaları ve kamu maliyesi gibi birçok boyutta etkili sonuçlar doğurmaktadır. Dijital para kavramı, teknoloji ile ekonomik yapılar arasındaki etkileşimin yoğunlaştığı yeni bir dönemin ifadesidir (Adrian & Mancini-Griffoli, 2021).

Dijital paralar, teknik ve hukuki niteliklerine göre dört ana gruba ayrılmaktadır: elektronik para, sanal para, kripto para ve merkez bankası dijital parası (CBDC). Bu sınıflandırma, yalnızca teknik farklara değil, aynı zamanda hukuki statü, regülasyon düzeyi ve sistem entegrasyonu gibi parametrelere de dayanmaktadır. Elektronik paralar genellikle ön ödemeli kartlar ve mobil cüzdanlarla ilişkilendirilir, düzenlenmiş ödeme kuruluşları tarafından çıkarılır. Sanal paralar, daha çok çevrimiçi platformlara özgü değer birimleri olup, yasal ödeme aracı değildir (OECD, 2020).

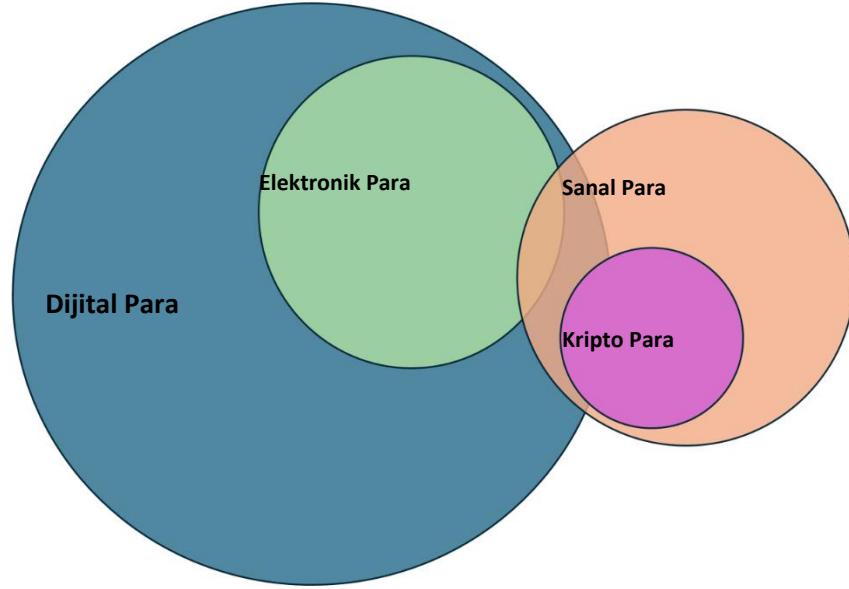
Kripto varlıklar, merkeziyetsiz yapıları ve şifreleme teknolojilerine dayalı sistemleriyle dijital finans dünyasında öne çıkan araçlardır. Bu sistem yapısı, özellikle denetim eksiklikleri nedeniyle kara para aklama, yasa dışı fon hareketleri ve spekülasyon işlemleri gibi ciddi riskleri beraberinde getirmektedir. Merkez bankası dijital paraları (CBDC), bu riskli alanlara karşı düzenlenmiş, denetlenebilir ve kamu yararını önceleyen bir alternatif sunma amacı taşımaktadır (FATF, 2021b).

CBDC'ler, diğer dijital para türlerinden farklı olarak doğrudan merkez bankaları tarafından ihraç edilmekte, yasal ödeme aracı niteliği taşımakta ve çoğunlukla geleneksel fiat para ile birebir değişim imkânı sunmaktadır. Bu özellikleri sayesinde CBDC'ler, ödeme sistemlerinde güvenlik, istikrar ve şeffaflık sağlamakta, devletlerin para politikası üzerindeki etkinliğini artırmaktadır. Ayrıca, finansal kapsayıcılık açısından da önemli olup, bu bağlamda bankacılık

hizmetlerine erişimi olmayan bireylerin, dijital cüzdanlar aracılığıyla ekonomik sisteme entegre edilmesini sağlamaktadır (Stanley, 2022).

Dijital, elektronik, sanal ve kripto paralar, teknolojik altyapı ve kullanım amaçları açısından farklılıklar göstermesine rağmen, aralarında güçlü bağlantılar bulunmaktadır. Aşağıdaki şekil, bu para türlerinin özelliklerini ve birbirleriyle olan ilişkilerini en sade biçimde açıklamayı amaçlamaktadır:

Şekil 1Dijital, Elektronik, Sanal ve Kripto Paralar Arasındaki İlişkiler



Yazarlar tarafından (Adrian & Mancini-Griffoli, 2021) çalışmasına dayanarak oluşturulmuştur.

Dijital para ekosistemi yalnızca farklı para türlerini değil; aynı zamanda bu sistemler etrafında oluşan kurumsal yapıların ve paydaş ilişkilerinin tamamını kapsamaktadır. Merkez bankaları, ticari bankalar, ödeme aracı kuruluşları, düzenleyici otoriteler, denetim kurumları, siber güvenlik birimleri ve bireysel kullanıcılar bu yapının aktif ve etkileşimli unsurlarıdır. Bahis konusu paydaşların her biri, sistemin denetim kapasitesi ve risk yapısının şekillenmesinde doğrudan etki sahibidir.

Dijital merkez bankası para sistemleri, geleneksel finansal denetim anlayışını yeniden şekillendirmekte ve denetim uygulamalarında derin yapısal değişimlere neden olmaktadır. Blok zincir teknolojisinin sunduğu şeffaf işlem takibi, değiştirilemez veri yapıları ve zaman damgalı kayıtlar, iç denetim uygulamalarının doğruluğunu artırırken; dış denetim otoritelerine de gerçek zamanlı, izlenebilir veri akışı sunmaktadır. Ayrıca akıllı sözleşmeler (belirli koşullara bağlı olarak otomatik işlem gerçekleştiren dijital protokoller) sayesinde, belirli ödeme işlemlerinin yalnızca önceden tanımlanmış koşullar altında gerçekleşmesi sağlanabilir ki bu da kamu harcamalarında hata ve kötüye kullanım riskini azaltıcı bir etki yaratacaktır.

Öte yandan, dijital para sistemlerinin gelişimi, yeni türden tehditleri de beraberinde getirmektedir. Siber saldırı riski, dijital cüzdanlardaki güvenlik açıkları, kişisel veri mahremiyetine yönelik ihlaller, kimlik hırsızlığı ve teknik sistem arızaları gibi unsurlar; bu alanın risk yönetimi boyutunun dikkatle ele alınmasını zorunlu kılmaktadır. CBDC'lerin etkin bir şekilde yönetilebilmesi için, geleneksel risk yönetimi modelleri dijital çağa uygun şekilde yeniden yapılandırılmalı ve yeni nesil teknolojik çözümlerle desteklenmelidir (Consultative Group on Risk Management, 2023).

Ülkemiz özelinde dijital para ekosistemi, özellikle 2020 sonrası dönemde yoğun bir kurumsal ilgiyi beraberinde getirmiştir. TCMB, Dijital Türk Lirası Projesi ile CBDC alanında teknik pilot çalışmalar yürütmekte, eş zamanlı olarak veri güvenliği, işlem mahremiyeti ve sistem sürdürülebilirliği gibi alanlarda da stratejik analizler gerçekleştirmektedir. Yürütülen sürecin başarılı olabilmesi için, sadece teknik değil; hukuki, yönetim ve denetim boyutlarının da eşgüdüm içinde yapılandırılması önem arz etmektedir.

Ayten ÇETİN, Serdar ALPAY

Özetle, dijital para kavramı yalnızca teknolojik yenilikle sınırlı olmayan; aynı zamanda finansal sistemin denetim anlayışını yeniden tanımlayan çok katmanlı bir dönüşüm sürecini temsil etmektedir. Bu dönüşümün başarılı olabilmesi, düzenleyici çerçevenin güçlendirilmesi, teknolojik altyapının hazır olması ve toplum nezdinde kabul görmesiyle mümkündür. Takip eden bölümde, bu bağlamda en stratejik dijital para türü olarak öne çıkan Merkez Bankası Dijital Paraları (CBDC) ayrıntılı şekilde değerlendirilecektir.

3. MERKEZ BANKASI DİJİTAL PARALARI (CBDC)

CBDC, dijitalleşmenin kamu politikaları ile kesiştiği noktada geliştirilen en kritik stratejik araçlardan biri olarak öne çıkmaktadır. Bu yapı yalnızca teknolojik bir ödeme çözümü değil; aynı zamanda finansal denetim, yönetim ve risk yönetimi alanlarında sistemsel dönüşüm sağlayabilecek bir inovasyon platformu niteliğindedir (Adrian & Mancini-Griffoli, 2021).

CBDC’ler, doğrudan merkez bankaları tarafından ihraç edilen ve kamu güvencesi taşıyan dijital para biçimleridir. Bu özellikleri sayesinde, özel sektör tarafından geliştirilen kripto varlıklar ve stabil kripto paralardan belirgin şekilde ayrılırlar. Yasal ödeme aracı statüsü, merkez bankalarının dijital ortamda da para politikası üzerindeki etkisini sürdürmesine olanak tanımaktadır (BIS, 2020).

CBDC, genel işlevlerine ve hedeflenen kullanıcı kitlesine bağlı olarak iki ana kategoride sınıflandırılmaktadır:

- Perakende (Retail) CBDC, bireylerin günlük harcama ve ödeme işlemlerinde kullanılmak üzere geliştirilen ve genel halkın erişimine açık olarak tasarlanan dijital bir merkez bankası parası türüdür. Genellikle dijital cüzdanlar yoluyla kullanılmakta olup, fiziksel paranın dijital karşılığı olarak işlev görmektedir.
- Toptan (Wholesale) CBDC, finansal kurumlar arasında gerçekleştirilen yüksek hacimli işlemler ve mutabakat süreçleri için tasarlanmış bir merkez bankası dijital para türüdür. Özellikle bankalararası ödeme sistemleri ile sermaye piyasalarının altyapısında etkin bir rol üstlenmektedir.

Merkez bankası dijital para sistemlerinin altyapısı genel olarak üç ana mimari modele dayalı olarak tasarlanabilir:

- Merkezi sistemler, tüm işlem verilerinin tek bir yetkili otorite tarafından yönetildiği, yüksek işlem yoğunluğuna sahip ancak denetim süreçleri açısından erişimin hızlı ve doğrudan sağlandığı altyapılardır.
- Dağıtık Defter Teknolojisi (DLT), işlem verilerinin birçok bağımsız düğümde eş zamanlı ve değiştirilemez biçimde tutulmasını sağlayan şeffaf ve güvenli bir sistem altyapısıdır. Denetim süreçlerinde, özellikle zaman damgalı kayıtların sağladığı izlenebilirlik önemli avantajlar sunmaktadır.
- Hibrit altyapılar, merkezi sistemlerin denetim kolaylığı ile dağıtık yapıların güvenlik ve şeffaflık avantajlarını bir araya getiren entegre mimarilerdir.

Farklı CBDC altyapıları, kendilerine özgü risk profilleri barındırmaktadır. Örneğin, Dağıtık Defter Teknolojisi (DLT) denetimsel izlenebilirlik açısından güçlü avantajlar sunarken; ölçeklenebilirlik, işlem süresi ve enerji tüketimi gibi alanlarda bazı teknik kısıtlamalara sahiptir (BoE, 2023).

CBDC sistemleri, gerçek zamanlı veri analizi ve işlem izlenebilirliği sağlayarak denetim etkinliğini artırır. Örneğin, Çin’in dijital yuan (e-CNY) sisteminde düşük riskli işlemler için kullanıcı gizliliği korunmakta; yüksek tutarlı işlemlerde ise doğrudan merkezî gözetim devreye girmektedir (Jiang & Lucero, 2023).

Avrupa Merkez Bankası’nın 2023 yılında yayımladığı belgelerde, dijital euro sisteminin kamu denetimi ile bireysel veri gizliliğini dengeleyen “kontrollü anonimlik” ilkesiyle tasarlandığı ifade edilmektedir (ECB, 2023).

Merkez bankası dijital paralarının (CBDC) yaygın biçimde benimsenmesi, yalnızca teknik altyapının değil; aynı zamanda kurumsal yapıların ve yasal çerçevelerin uyum içinde geliştirilmesini gerektirmektedir. Türkiye Cumhuriyet Merkez Bankası’nın yürüttüğü Dijital Türk Lirası Projesi her ne kadar henüz teknik pilot aşamasında olsa da, bu süreçle eş zamanlı olarak denetim mimarisinin de oluşturulması kritik önem taşımaktadır. Vergi sistemleriyle entegrasyon, kamu harcamalarının izlenebilirliği ve sosyal yardımların daha hedefli şekilde aktarılması gibi bileşenler, kamu yararını artıracak stratejik işlevlerdir.

Ayrıca CBDC sistemlerinin sunduğu izlenebilirlik kapasitesi, kayıt dışı ekonomik faaliyetlerin azaltılması, kamu kaynaklarının daha etkin ve şeffaf yönetimi ile mali disiplinin güçlendirilmesi açısından ciddi potansiyel taşımaktadır. Bu yönüyle CBDC’ler yalnızca birer finansal yenilik değil; aynı zamanda kamu yönetimi alanında yapısal dönüşüm sağlayabilecek birer reform aracı olarak değerlendirilmektedir.

4. FİNANSAL DENETİM VE RİSK YÖNETİMİ PERSPEKTİFİNDEN CBDC'LER

CBDC sistemleri, denetim kurumlarına veri temelli altyapılar sağlamakta ve risk yöneticilerinin erken uyarı yeteneğini artırmaktadır (Consultative Group on Risk Management, 2023). CBDC sistemlerinin finansal denetim ve risk yönetimi perspektifinden değerlendirilmesi, bu dijital yapıların yalnızca bir ödeme aracı olmanın ötesinde kurumsal kontrol mekanizmalarına nasıl entegre edilebileceğini ortaya koymak açısından önemlidir. Bu bölümde, öncelikle CBDC'nin denetim süreçlerine nasıl katkı sunduğu analiz edilecek; ardından operasyonel, siber güvenlik ve yönetim gibi alanlarda karşılaşılan başlıca riskler değerlendirilecektir. Devamında, yönetim ve meşruiyet boyutları ile Türkiye özelinde kurumsal dönüşüm ve uygulama fırsatları ele alınarak, dijital denetim mimarisinin çok boyutlu yapısı bütüncül bir çerçevede sunulacaktır.

4.1. CBDC'nin Denetim Üzerindeki Potansiyel Katkıları

CBDC altyapıları, geleneksel finansal işlemlerde karşılaşılan denetim açıklarını dijital çözümlerle azaltma potansiyeline sahiptir. Blokzincir veya merkezi veri tabanı temelli sistemlerde zaman damgalı, değiştirilemeyen ve yapılandırılmış işlem kayıtlarının tutulması, örnekleme temelli klasik denetim yöntemlerinin yerine kapsamlı ve bütünsel veri analizine imkân tanımaktadır (BIS, 2020a).

Bu çerçevede, CBDC sistemlerinin denetim süreçlerine sağladığı katkılar aşağıdaki gibi özetlenebilir:

- Gerçek zamanlı işlem doğrulama sayesinde, kamu harcamalarının izlenebilirliğini ve denetlenebilirliğini artırır,
- Kamuya yönelik transferlerin gerçekten ihtiyaç sahibi hedef gruplara ulaşıp ulaşmadığını izlemeye ve doğrulamaya imkân tanır,
- Denetim API'leri aracılığıyla hem merkezi otoritelerin hem de bağımsız denetim organlarının sistem üzerinde eş zamanlı veri izlemesi ve analiz gerçekleştirmesi mümkün hale gelir,
- Yapay zekâ destekli anomali tespit sistemleri sayesinde, olağan dışı işlem örüntüleri erken aşamada tanımlanarak denetim birimlerine ön sinyal oluşturabilir.

Örneğin, kamu ihalesi süreçlerinde ödeme tutarları ile alıcının vergi kaydı sistematik biçimde çapraz doğrulamaya tabi tutulabilir. Bu uygulama, yolsuzluk riskini azaltırken; kamu kaynaklarının etkin ve şeffaf kullanımını destekler. Avrupa Merkez Bankası tarafından geliştirilen modelde ise, işlem risk seviyelerine bağlı olarak kademeli denetim mekanizmalarının uygulanması öngörülmektedir (Panetta, 2023).

Bu doğrultuda, CBDC sistemleri yalnızca muhasebe süreçlerinin doğruluğunu artırmakla kalmaz; aynı zamanda iç kontrol yapılarının dijital ortama taşınmasını, kamu kaynaklarının şeffaf biçimde izlenmesini ve bütçe disiplini gibi makro düzeydeki kamu politikalarının uygulanmasını da destekler.

4.2. CBDC Uygulamalarında Karşılaşılan Risk Yönetimi Sorunları

CBDC'lerin yaygınlaşması, denetim avantajlarının yanı sıra operasyonel, siber güvenlik, hukuki ve yönetim kaynaklı yeni riskleri ortaya çıkarmaktadır.

Operasyonel risk kategorisine giren başlıca unsurlar şunlardır:

- Sistem erişim kesintileri veya altyapı hataları,
- Kritik donanım bileşenlerinde meydana gelen teknik arızalar,
- Yazılım güncellemeleri sırasında ortaya çıkabilecek sürüm uyumsuzlukları veya entegrasyon hataları,
- Ayrıca ağ bağlantısındaki kesintiler veya istikrarsızlıklar da operasyonel riskler arasında yer almaktadır.

Bu nedenle iş sürekliliği ("business continuity") protokollerinin oluşturulması ve felaket anı senaryolarına yönelik kurtarma sistemlerinin ("disaster recovery") tasarlanması kritik bir ihtiyaç halini almıştır (BoE, 2023).

Siber güvenlik alanında karşılaşılan temel tehdit başlıkları ise şunlardır:

- Dağıtık defter teknolojilerine (DLT) yönelik hedefli siber saldırılar,
- Dijital cüzdan sistemlerinin kötü niyetli üçüncü taraflarca ele geçirilmesi,
- Sistemlere yönelik yetkisiz erişim teşebbüsleri,

- Ayrıca hizmet engelleme (DDoS) saldırıları gibi erişilebilirlik tehditleri de siber riskler arasında yer almaktadır.

Bu tehditlere karşı, ISO/IEC 27001 ve NIST SP 800-53 gibi küresel güvenlik standartlarına uygun olarak sistem tasarımı yapılmalı; sızma testleri ve sürekli güvenlik izleme süreçleri etkin biçimde uygulanmalıdır (FATF, 2024).

Yönetişim kaynaklı riskler, özellikle denetim sorumluluğunun farklı kurumsal aktörler arasında nasıl dağıtılacağı ve kullanıcı mahremiyetinin hangi mekanizmalarla korunacağı sorularıyla öne çıkmaktadır. İşlemlerin merkezi denetime tabi olması veri güvenliğini artırsa da, bireysel gizlilik üzerinde çeşitli tehditleri de beraberinde getirebilir. Bu nedenle KVKK benzeri yasal düzenlemeler doğrultusunda “kademeli erişim,” “anonimleştirme mekanizmaları” ve “amaçla sınırlılık” ilkeleri sistem mimarisine entegre edilmelidir (KVKK, 2016).

4.3. Yönetişim ve Meşruiyet Boyutu

CBDC sistemlerinin sadece teknik güvenlik önlemleriyle değil, aynı zamanda kullanıcıların sistemle kurduğu ilişkiyi şekillendiren meşruiyet algısıyla birlikte değerlendirilmesi gereken çok boyutlu bir yönetim çerçevesine ihtiyacı vardır. Sistem mimarisi ne kadar sağlam, denetim araçları ne kadar gelişmiş olursa olsun; toplum nezdinde kabul görmeyen, kullanıcı güveni oluşturmeyen bir yapının uzun vadede sürdürülebilir başarı elde etmesi mümkün değildir.

Bu çerçevede, kullanıcıların doğal olarak yönelttiği bazı temel sorular şunlardır:

- “Veri setlerime kimler erişebilecek?”
- “Anonim şekilde işlem yapma hakkım korunacak mı?”
- “Devletin beni sürekli izlemesi mümkün mü?”
- “Bu dijital sistem bana mı hizmet ediyor, yoksa beni mi denetliyor?”

Bu sorular, yalnızca teknik açıklıkla yanıtlanabilecek kapsamda olmayıp; aynı zamanda etik ve politik denetim boyutlarını da doğrudan ilgilendirmektedir.

ECB tarafından önerilen “kontrollü anonimlik” ilkesi, kullanıcı mahremiyetini gözetirken şüpheli durumlarda düzenleyici otoritelere müdahale yetkisi tanıyan bir mimari vizyonun ürünüdür. Avrupa Merkez Bankası’nın 2023 tarihli açıklamalarında, düşük riskli işlemler için yüksek düzeyde gizlilik önerilmekte; ancak yüksek tutarlı ve riskli işlemlerde regülatif müdahale olanaklı kılınmaktadır (ECB, 2023).

Etik yönetim perspektifinden, aşağıdaki uygulamalar sistem tasarımına entegre edilmelidir:

- Erişim loglarının şeffaf şekilde tutulması ve kullanıcılar tarafından görüntülenebilir olması,
- Bireylerin kendi verileri üzerinde kontrol sahibi olması (veri portalları üzerinden silme, izleme ve onaylama hakları),
- Denetim raporlarının kamuya açık mecralarda düzenli olarak yayımlanması,
- Kamu güvenliğini tehdit etmediği sürece, üçüncü taraflarca yapılacak analiz çalışmalarının izinli biçimde desteklenmesi.

Bu bütüncül yaklaşım sayesinde CBDC sistemleri, yalnızca denetim araçlarıyla sınırlı kalmayan; aynı zamanda hesap verilebilirliği, şeffaflığı ve etik sorumluluğu merkezine alan hakkaniyetli dijital kamu platformları hâline gelebilecektir.

4.4. Türkiye Açısından Stratejik Uygulama Fırsatları ve Denetim Odaklı CBDC Yaklaşımları

TCMB’nin pilot düzeyde sürdürdüğü Dijital Türk Lirası (DTL) Projesi, yalnızca teknik test süreciyle sınırlı kalmamakta; aynı zamanda kamu kuruluşlarının dijital denetim yetkinliklerini yeniden şekillendirme potansiyeli taşımaktadır. Merkez bankası dijital paraları, ödeme sistemlerinin ötesinde, dijital kamusal denetim reformu için temel yapı taşları olarak değerlendirilmelidir.

Bu çerçevede, aşağıda sıralanan stratejik araçlar Türkiye açısından önemli yapısal fırsatlar barındırmaktadır (TCMB, 2023)

- Anlık kamu harcama denetimi: Sosyal destek ve teşvik ödemelerinin istenen demografik ve bölgesel gruplara ulaşip ulaşmadığı, dijital altyapılar sayesinde gerçek zamanlı biçimde izlenebilir.
- Kayıt dışı işlemlerle mücadelede, özellikle tüzel kişiler arası yüksek meblağlı transferlerin izlenebilirliği sayesinde vergi denetiminde şeffaflık sağlanabilir.
- Akıllı sözleşme tabanlı şartlı ödemeler sayesinde, eğitim desteği gibi kamu yardımları yalnızca ilgili

Ayten ÇETİN, Serdar ALPAY

harcama kategorilerinde kullanılmak üzere sınırlandırılabilir.

- Blokzincir destekli sistemler, işlem tarihleri ve içerik türlerine göre ayrı kategorilerde izlenebilir ve raporlanabilir denetim imkânı sağlar.
- Sayıştay, BDDK ve MASAK gibi otoriteler, dijital sistemler aracılığıyla eş zamanlı raporlamaya ve genişletilmiş veri erişimine kavuşabilir.

Bunun yanı sıra, milli cüzdan sistemleri üzerinden elde edilen kullanıcı davranış verileri, finansal okuryazarlığı artırıcı içeriklerin hazırlanmasında temel veri kaynağı olarak işlev görebilir..

Bu önerilerin uygulamaya konulması, Türkiye'nin sadece dijital altyapı değil, aynı zamanda yönetim kalitesi ve denetim esnekliği açısından da yapısal bir sıçrama gerçekleştirmesine olanak sağlayacaktır.

4.5. Sonuç Değerlendirmesi

CBDC sistemleri, klasik denetim modellerine alternatif olarak gerçek zamanlı, bütünsel ve veriye dayalı bir denetim mimarisi sunarak denetim paradigmasında radikal bir dönüşüm yaratmaktadır. Ancak bu dönüşümün başarıya ulaşabilmesi için üç temel alanın bir arada ve uyumlu şekilde geliştirilmesi kritik önemdedir::

- Kurumsal yetkinlik: Dijital çağın gerekliliklerine uygun şekilde, denetim otoritelerinin teknik kapasite, veri analizi becerisi ve insan kaynağı açısından güçlendirilmesi gerekmektedir.
- Hukuki ve yönetim altyapısı: Merkezi sistemlerin veri erişim kapasitesi ile bireysel haklar arasında denge kuracak biçimde, kişisel veri güvenliği ve yasal uyumun garanti altına alınması gereklidir.
- Toplum temelli güven: Dijital paraya geçiş sürecinin benimsenebilmesi, vatandaşların şeffaf, etik ve güvenilir bir sistem algısı geliştirmesiyle mümkündür.

Dijital Türk Lirası Projesi, yalnızca yeni bir para biçiminin hayata geçirilmesi değil; aynı zamanda mali şeffaflık, vergi sisteminde adalet ve finansal kapsayıcılığın yaygınlaştırılması adına stratejik bir araç olarak değerlendirilmelidir.

Bu çerçevede CBDC uygulamaları, teknik inovasyon olmanın ötesinde; dijital çağın kamu yönetimi anlayışını temsil eden, stratejik bir kamu politikası belgesi niteliği taşımaktadır (BIS, 2023b; Auer, Cornelli, & Frost, 2020; OECD, 2020).

5. ULUSLARARASI CBDC UYGULAMALARINDAN DENETİM VE RİSK PERSPEKTİFİNDE STRATEJİK ÇIKARIMLAR

CBDC uygulamaları, küresel ölçekte birçok ülke tarafından kendi ulusal hedeflerine uygun biçimde şekillendirilmektedir. Ülkeler, CBDC'yi farklı amaçlarla kurguladıkları için, bu sistemlerin denetim ve risk yapıları da farklılaşmakta ve özgün stratejik yaklaşımlar gerektirmektedir. Aşağıdaki alt başlıklarda Çin, AB, Kanada, İngiltere ve ABD gibi ülkelerin CBDC uygulamaları denetim ve risk yönetimi açısından değerlendirilerek, bu deneyimlerden elde edilebilecek stratejik kazanımlar özetlenmiştir.

5.1. Çin – e-CNY ve Kontrollü Anonimlik

Çin'in geliştirdiği dijital yuan (e-CNY), ödeme işlevinin ötesine geçerek çok katmanlı denetim yapısı ve merkezileşmiş veri kontrol kapasitesi ile dikkat çeken bir dijital finansal sistem modeli ortaya koymuştur. Bu sistemin ayırt edici yönü, işlemlerin merkezi bir altyapı aracılığıyla yürütülmesi ve her işlemin zaman damgalı, sınıflandırılmış ve değiştirilemez kayıtlarla belgelenmesidir. Bu yaklaşım, işlem takibinde maksimum düzeyde şeffaflık ve denetlenebilirlik sağlamaktadır.

Düşük miktartlı ve kişisel ödemelerde kullanıcı mahremiyeti korunurken, yüksek riskli veya olağan dışı işlemler otomatik şekilde merkezi izleme sistemine yönlendirilmektedir. Bu sistem tasarımı, risk düzeyine göre değişkenlik gösteren çok katmanlı kontrol mekanizmalarını içeren “kontrollü anonimlik” ilkesine dayanmaktadır. Söz konusu altyapı, kamu ödemelerinin izlenebilirliğini sağlamakta, vergi tahsilat süreçlerini dijitalleştirerek sistematik hâle getirmekte ve mali yönetimde şeffaflık düzeyini yükseltmektedir.

Bununla birlikte, sistemin yüksek düzeyde merkezileştirilmiş veri kontrolü ve izlenebilirlik yapısı, mahremiyet, şeffaflık ve etik denge açısından çeşitli eleştirileri de beraberinde getirmiştir. Özellikle veri tekelleşmesi ve kullanıcı gizliliğinin

Ayten ÇETİN, Serdar ALPAY

ihlali olasılığı, sistemin toplumsal kabul düzeyini olumsuz etkileyebilecek başlıca riskler arasında gösterilmektedir. Tüm işlemlerin merkezi kontrol altında yürütülmesi, kullanıcı davranışlarının ekonomik profillemeye algoritmalarıyla analiz edilmesine olanak tanımakta; tüketim alışkanlıkları, lokasyon bazlı işlem eğilimleri ve sosyal bağlantılara dayalı korelasyon analizleri gibi kişisel verilerin derinlemesine incelenmesi riskini doğurmaktadır. Bu gelişmiş analiz kapasitesi, denetim verimliliğini artırsa da, bireysel özgürlükler ve veri hakları bakımından önemli etik tartışmaları gündeme getirmektedir.

Çin Merkez Bankası, kamuoyunda oluşan gizlilik kaygılarına yanıt olarak, sisteme katmanlı erişim düzeyleri ve sınırlı veri işleme ilkeleri entegre edildiğini açıklamıştır. Ancak sistemin temel tasarım yaklaşımı, “mutlak anonimlik” sağlamak yerine, güvenlik ve izlenebilirlik arasında bir denge kurulmasına odaklanmaktadır. Bu nedenle Çin modeli, kamu güvenliğini sağlarken bireysel veri haklarını da belirli sınırlar içinde korumayı amaçlayan, teknik müdahale araçlarıyla desteklenen bir denge kurma girişimi olarak değerlendirilmektedir (Jiang & Lucero, 2023).

5.2. Avrupa – Dijital Euro ve Kontrollü Anonimlik İlkesi

Avrupa Merkez Bankası (ECB), dijital euro sistemini yalnızca teknik bir ödeme altyapısı olarak değil; aynı zamanda Avrupa Birliği’nin temel veri koruma ilkeleriyle bütünleşmiş bir yönetim yapısı olarak konumlandırmaktadır. Bu yaklaşım doğrultusunda, sistemin mimarisi hem bireysel gizliliği koruyacak hem de düzenleyici kurumların denetim yetkisini sürdürebilecek bir denge üzerine inşa edilmektedir. ECB, dijital euro kapsamında, kişisel verilerin işlenmesi ve erişilmesi süreçlerini yalnızca yasal zorunluluk hâlinde mümkün kılacak şekilde yapılandırmıştır. Sistem, Genel Veri Koruma Tüzüğü’ne (GDPR) tam uyum içinde tasarlanmış olup, hukuki çerçevenin sınırlarını aşmayacak şekilde çalışmaktadır.

Dijital euro sistemi, işlem risk seviyelerine göre farklılaştırılmış bir yapı sunmaktadır. Düşük tutarlı işlemlerde daha yüksek düzeyde gizlilik sağlanırken; yüksek risk taşıyan işlemlerde ise kontrollü ve denetlenebilir erişim mekanizmaları devreye girmektedir. ECB’nin bu yapısı, yalnızca teknik bir mimari değil; aynı zamanda kamu hukukunun temel ilkeleri olan amaçla sınırlılık, gereklilik ve şeffaflık ilkeleriyle uyumlu bir kamusal dijital sistem tasarımı olarak değerlendirilmektedir.

Kullanıcı verilerine erişim, yalnızca belirli koşullar altında ve meşru amaçlarla gerçekleştirilmekte; denetim mekanizmaları sadece risk durumlarında aktive edilmektedir. Bu tasarım, hem mali denetimi güçlendirme hem de dijital çağda birey haklarını koruma işlevini aynı anda yerine getirmeyi hedeflemektedir. ECB’nin stratejik yaklaşımı, sadece teknik uzmanları değil; sivil toplum kuruluşları, veri koruma ajansları ve kamu temsilcilerini de sistem tasarımı sürecine aktif biçimde entegre etmeye yöneliktir. Bu katılımcı süreç, sistemin toplumsal meşruiyetini artırmayı amaçlamaktadır.

Ayrıca ECB, dijital euroyu yalnızca bireyler arası ödemelerle sınırlı tutmamayı; kamu ödemeleri, vergi tahsilat süreçleri ve sosyal yardım transferleri gibi alanları da kapsayacak şekilde genişletmeyi planlamaktadır. Bu genişleme, kamu maliyesinde şeffaflık ve otomasyon düzeyini artırmayı hedefleyen AB düzeyinde entegre dijital denetim sistemlerinin devreye alınmasıyla desteklenmektedir. Örneğin, dijital harcamalar ile vergi bildirimleri arasında otomatik çapraz kontroller yapılabilecek; böylece vergi uyumu ve mali denetim süreçleri daha güçlü biçimde izlenebilir hâle gelecektir.

Avrupa modeli, hem dijital para mimarisi hem de veri hakları ile denetim dengesi açısından uluslararası düzeyde referans alınan örneklerden biridir. Dijital euro, Avrupa Birliği’nin dijital egemenlik vizyonunun temel bileşenlerinden biri olarak değerlendirilmektedir (Panetta, 2023).

5.3. Kanada – Senaryo Temelli Direnç Testleri ve Denetim Mimarisi

Kanada Merkez Bankası (Bank of Canada), henüz CBDC uygulamasına geçmiş olmasa da, dijital para sisteminin teknik ve denetimsel kapasitesine ilişkin oldukça kapsamlı hazırlık çalışmaları yürütmektedir. Bu çalışmalar arasında, potansiyel zayıf noktaları öngörmeye yönelik çok katmanlı senaryo temelli analizler önemli bir yer tutmaktadır. Bank of Canada’nın stratejisi, yalnızca normal işleyiş koşullarını değil; olağandışı durumlar ve sistem stresine karşı gösterilecek kurumsal refleksleri de test etmeyi amaçlamaktadır.

CBDC altyapısının ödeme sistemleri, teknolojik bütünlük ve veri koruma gibi alanlardaki kırılgan noktaları senaryolar aracılığıyla modellenmektedir. Özellikle işlem yoğunluğu artışı, altyapı kesintileri, dış kaynaklı siber saldırılar, kimlik doğrulama sorunları ve veri güvenliği açıkları gibi başlıklar, detaylı stres testlerine tabi tutulmaktadır. Bu süreçte hem teknik donanım hem de kurumlar arası eşgüdüm kapasitesi sınanmaktadır.

Bank of Canada, geliştirdiği "critical incident response" senaryoları ile yalnızca teknik müdahale yeterliliğini değil; aynı

Ayten ÇETİN, Serdar ALPAY

zamanda iletişim yönetimi, kamu bilgilendirme mekanizmaları ve dış paydaşlarla kriz koordinasyonu gibi alanları da analiz etmektedir. Bu yaklaşım, CBDC sisteminin yalnızca teknik olarak değil; aynı zamanda yönetsimsel açıdan da dirençli olmasını sağlamaya yöneliktir.

Kanada'nın bu hazırlık süreci, dijital para sisteminin uygulamaya alınmadan önce tüm yönleriyle test edilmesi gerektiği anlayışına dayanmaktadır. Bu çerçevede, CBDC sistemlerinin altyapı tasarımı ile denetim ve düzenleme mekanizmalarının eş zamanlı geliştirilmesi gerektiği yönündeki anlayış, Kanada'nın stratejik planlamasında belirgin biçimde vurgulanmaktadır (Arora, Du, Kazmi, & Le, 2025). Sistem devreye alındığında herhangi bir operasyonel kesinti ya da veri bütünlüğü zafiyeti yaşanmaması, bu ön hazırlık sürecinin başlıca hedefidir.

Bu yaklaşım yalnızca Kanada için değil; dijital para sistemine geçmeyi planlayan diğer ülkeler açısından da örnek teşkil etmektedir. Kanada modelinin önceliği, teknik uygulamadan önce kurumsal hazırlığı ve risk senaryosu yönetimini öne çıkarmasıdır. Bu model, CBDC'nin sadece teknolojik bir yenilik olarak değil; aynı zamanda kurumsal denetim kapasitesini artıran stratejik bir araç olarak ele alınmasını sağlamaktadır (Darbha & Arora, 2020).

5.4. Birleşik Krallık –Çok Paydaşlı Denetim ve Şeffaflık Modeli

İngiltere Birleşik Krallık Merkez Bankası (Bank of England), Dijital Pound projesini yalnızca bir ödeme aracı olarak değil, aynı zamanda kamu güveni ve yönetim açısından şeffaflığı önceleyen kurumsal bir dönüşüm fırsatı olarak değerlendirmektedir. İngiltere Merkez Bankası (BoE), dijital pound sisteminin yalnızca kamu otoriteleri değil; akademik çevreler, özel sektör ve sivil toplum kuruluşlarının da dâhil olduğu çok aktörlü bir denetim mekanizmasıyla yürütülmesini planlamaktadır. Bu model, geleneksel merkez bankası gözetiminin ötesine geçerek; akademi, teknoloji sağlayıcıları, özel sektör kuruluşları, düzenleyici kurumlar ve sivil toplum örgütlerinin sürece aktif katılımını teşvik etmektedir. Böylelikle, sistem üzerinde çok yönlü izleme ve hesap verebilirlik mekanizmaları kurulması hedeflenmektedir.

Dijital Pound sisteminde denetim yalnızca finansal işlemlerin izlenmesiyle sınırlı değildir. Aynı zamanda sistemin nasıl geliştirildiği, ne tür veri toplandığı, bu verilerin kimler tarafından ve ne amaçla kullanılabileceği gibi daha geniş kapsamlı sorular da denetim kapsamına dahil edilmektedir. BoE tarafından savunulan modelde, teknolojik sistemler “şeffaf kutu” prensibine göre tasarlanmalı, algoritmalar denetime açık tutulmalı ve yazılım kodları bağımsız otoritelerce doğrulanabilir olmalıdır. Böylelikle yalnızca kullanıcı güvenliği değil, aynı zamanda teknolojik tarafsızlık ve etik sorumluluk da gözetilmektedir.

BoE, açık kaynak yazılımlar, kamuya yönelik raporlamalar ve bağımsız uzman komiteleri içeren bir yönetim yapısını önererek kurumsal şeffaflığı güçlendirmeyi hedeflemektedir. Bu yönetim mekanizması, farklı uzmanlık alanlarından gelen aktörlerin sistemle ilgili karar alma süreçlerine katkı sunmasını mümkün kılmakta; böylece merkez bankasının toplumla kurduğu güven ilişkisini pekiştirmektedir.

BoE, kullanıcı gizliliğini gözetken ve yalnızca yasal gerekçelerle veri erişimine izin veren bir mimari anlayışı ön plana çıkarmaktadır. Bu ilkeye göre, kullanıcı verilerine erişim yalnızca düzenleyici veya yasal zorunluluk durumlarında ve belirli bir amaca hizmet edecek şekilde mümkün kılınmaktadır. Ayrıca bu tür veri erişimleri, bağımsız ve tarafsız denetim birimleri tarafından izlenmekte ve gerektiğinde kamuoyuna raporlanmaktadır. Bu yaklaşım, sistemin denetlenebilirliğini artırmakla birlikte, kullanıcıların dijital ortamda kişisel verileri üzerindeki kontrolünü de güçlendirmektedir.

Sonuç olarak, Birleşik Krallık'ın önerdiği bu çok aktörlü denetim yapısı, merkez bankası dijital paralarının yalnızca finansal değil; aynı zamanda toplumsal ve yönetsimsel boyutlarına da odaklanan bütüncül bir model sunmaktadır. BoE'nin Dijital Pound girişimi, güvenlikten etik sorumluluğa kadar çok boyutlu bir yapı önererek dijital merkez bankası parası tasarımlarında küresel ölçekte örnek teşkil etmektedir (BoE, 2023).

5.5. ABD – Aracılı CBDC Modeli ve Anayasal Denge Arayışı

Amerika Birleşik Devletleri Merkez Bankası (Federal Reserve), merkez bankası dijital para birimi (CBDC) konusunda henüz uygulamaya geçmemekle birlikte, stratejik ve çok yönlü analizlere dayanan bir yaklaşım benimsemektedir. Ocak 2022'de yayımlanan Money and Payments: The U.S. Dollar in the Age of Digital Transformation başlıklı rapor, Federal Reserve'in bu konudaki temel perspektifini ortaya koymakta ve CBDC'nin finansal, teknik ve hukuki yönlerine ilişkin bütüncül bir değerlendirme sunmaktadır. Bu raporda, kamu-özel sektör iş birliğini temel alan, gizliliğe öncelik veren ve ölçeklenebilir hibrit modellerin ön plana çıkması gerektiği ifade edilmektedir (Federal Reserve, 2022).

Ayten ÇETİN, Serdar ALPAY

Federal Reserve'in vizyonu, dijital doların doğrudan merkez bankası eliyle yönetilmesi yerine, özel sektör kuruluşlarının aktif rol aldığı bir aracılı dağıtım modeli etrafında şekillenmektedir. Bu senaryoda, kullanıcıya ulaşan dijital paranın dağıtımı ve arayüz hizmetleri; bankalar, ödeme hizmet sağlayıcıları ya da teknoloji şirketleri gibi lisanslı kurumlar tarafından yürütülmektedir. Merkez bankası ise yalnızca altyapıyı sağlamakta ve sistemin güvenliğini garanti altına almaktadır; kimlik doğrulama, dijital cüzdan yönetimi ve kullanıcı deneyimi gibi alanlar tamamen aracı kuruluşların sorumluluğuna bırakılmaktadır.

Bu yapı, operasyonel esnekliği artırmakla kalmayıp; kamu-özel iş birliğini kurumsallaştırarak daha dengeli ve çok aktörlü bir denetim mimarisi oluşmasına da katkı sunmaktadır. CBDC'nin kullanımı sırasında ortaya çıkabilecek veri akışı, yasal uygunluk kontrolleri, kara para aklama karşıtı tedbirler ve tüketici haklarının korunması gibi işlevler yalnızca merkez bankası değil, aynı zamanda yetkilendirilmiş platform operatörleri tarafından da izlenmekte ve raporlanmaktadır. Bu da sistemin ölçeklenebilirliğini artırmakta ve düzenleyici yükün paylaşılmasını mümkün kılmaktadır.

Federal Reserve, bu süreci yalnızca teknolojik bir mesele olarak değil, aynı zamanda anayasal bir sorumluluk alanı olarak ele almaktadır. Özellikle bireysel verilerin anayasal koruma altında olduğu ABD'de, CBDC tasarımı veri mahremiyeti, şeffaflık ve kamu yararı arasında hassas bir denge gözetilmesi gerektiği vurgulanmaktadır (Federal Reserve, 2022).

Sonuç olarak, Federal Reserve'in önerdiği modelde merkez bankası yalnızca çekirdek teknolojiyi geliştirirken, özel sektör aktörleri kullanıcılarla etkileşimde bulunur. Bu çok katmanlı yapı, finansal kapsayıcılık, dijital altyapı güvenliği ve bireysel hakların korunması gibi alanlarda CBDC'nin stratejik bir kamu politikası aracı olarak konumlandığını ortaya koymaktadır (Federal Reserve, 2022).

5.6. Uluslararası Çıkarımlar: Denetim-Risk Dengesi

Beş farklı ülkenin merkez bankası dijital para birimi (CBDC) konusundaki uygulamaları ve stratejik yaklaşımları, denetim altyapısı ile operasyonel risk yönetimi arasındaki dengeyi sağlama açısından Türkiye için önemli bir referans çerçevesi sunmaktadır. Her ülkenin kendi siyasi, teknolojik ve hukuki bağlamına göre geliştirdiği model, ülkemizin DTL projesi kapsamında dikkate alınması gereken çok boyutlu çıkarımlar üretmektedir: (TCMB, 2023)

Denetim ve Mahremiyet Dengesi

Avrupa Merkez Bankası'nın geliştirdiği Dijital Euro mimarisi, bireysel veri hakları, amaçla sınırlılık, ve veri minimizasyonu ilkelerine odaklanırken, kullanıcı gizliliğinin korunmasını sistemin temel prensiplerinden biri olarak ele almaktadır. Düşük tutarlı işlemlerde yüksek düzeyde anonimlik sağlanmakta, yüksek tutarlı işlemlerde ise denetimsel erişim sınırlı ve kademeli olarak uygulanmaktadır. Buna karşın Çin Halk Bankası'nın geliştirdiği e-CNY sistemi, veri izlenebilirliği ve merkezî denetimi ön planda tutmakta, kullanıcı hareketlerinin yüksek düzeyde merkezî bir sistemde izlenmesine olanak tanımaktadır. Bu iki uç model arasında Türkiye'nin, hem Kişisel Verilerin Korunması Kanunu (KVKK) hem de toplumsal beklentiler çerçevesinde hibrit ve dengeli bir veri erişim modeli benimsemesi önerilmektedir. Kontrollü anonimlik, sınırlı kimlik eşleştirme ve veri koruma ilkelerinin birlikte uygulanacağı bir mimari, hem denetimsel etkinliği hem de vatandaş güvenini artırabilir (Panetta, 2021).

Veri Bütünlüğü ve Şeffaflık

Kanada, Çin, İngiltere ve Avrupa modellerinin ortak özelliği, veri bütünlüğünü garanti altına alan sistem mimarileridir. Bu sistemlerde her işlem, zaman damgalı, değiştirilemez ve denetlenebilir şekilde kaydedilmektedir. Bu yapı, sadece işlem güvenliğini değil, aynı zamanda denetim süreçlerinin otomasyonunu ve geriye dönük analizlerin doğruluğunu da artırmaktadır. Türkiye'nin Dijital Türk Lirası projesinde de, işlem kayıtlarının dağıtık veya merkezî sistemler üzerinde siber güvenlik önlemleriyle birlikte değiştirilemez biçimde tutulması, hem vergi uyumu hem de kamu finansmanında şeffaflığı destekleyecektir (Arora, Du, Kazmi, & Le, 2025).

Birden Fazla Kurumun Katıldığı Denetim Süreçleri

İngiltere ve ABD'nin CBDC yaklaşımları, birçok kurumun birlikte çalışmasını sağlayan bir yönetim anlayışı benimseyerek kamu-özel sektör iş birliğini denetim süreçlerine dahil etmektedir. Bu modellerde yalnızca merkez bankası değil; özel sektör platformları, akademik çevreler, düzenleyici kurumlar ve sivil toplum örgütleri de süreçte

Ayten ÇETİN, Serdar ALPAY

dahil edilmektedir. Bu durum, denetim kapasitesinin sadece merkezî bir otoriteye yüklenmeden, dağıtılmış sorumluluk yapısı içinde daha esnek ve hesap verebilir hale gelmesini sağlamaktadır. Türkiye'nin de Dijital Türk Lirası sürecinde Merkez Bankası, TÜBİTAK, BDDK³, MASAK⁴ ve ilgili teknoloji firmaları arasında kurumsallaşmış iş birlikleri ile bu tür bir çoğulcu yapı kurması stratejik fayda sağlayacaktır (BoE, 2023; Board of Governors of the Federal Reserve System, 2022).

Operasyonel Risk Analizi ve Simülasyon Temelli Yaklaşım

Kanada Merkez Bankası'nın CBDC uygulamasına geçmeden önce yürüttüğü senaryo temelli stres testleri, proaktif denetim anlayışının güçlü bir örneğini sunmaktadır. Özellikle sistem çökmesi, siber saldırı, kimlik doğrulama aksaklıkları gibi potansiyel tehditlerin önceden modellenmesi; sadece teknik değil, yönetsimsel risklerin de görünür kılınmasını sağlamaktadır. Türkiye'nin pilot uygulama sürecinde, 'red team' testleri, operasyonel dayanıklılık simülasyonları ve kriz senaryoları gibi ileri analiz yöntemlerini kullanması, potansiyel sistem açıklarının erkenden tespit edilmesine olanak tanıyacaktır. Bu yaklaşım, denetimsel kapasitenin teknik güvenlik ile entegre biçimde gelişmesine katkı sunacaktır (Darbha & Arora, 2020; BIS Innovation Hub, 2023c).

CBDC sistemleri, sadece teknik altyapı projeleri değil; aynı zamanda kamu politikası tasarımı yön verici, ekonomik ve sosyal politikaların uygulanmasını destekleyici çok boyutlu araçlardır (BIS, 2023b; Auer, Cornelli, & Frost, 2020); OECD, 2020). Ülkemiz açısından ise denetim, mahremiyet, yönetim ve risk yönetimi gibi unsurlar arasında denge kuran bir mimarinin benimsenmesi, Dijital Türk Lirası'nın sürdürülebilir ve toplumsal meşruiyeti yüksek bir yapıda gelişmesini mümkün kılacaktır.

6.DTL BAĞLAMINDA TÜRKİYE İÇİN ÇOK KATMANLI DENETİM VE RİSK YÖNETİMİ STRATEJİLERİ

DTL, Türkiye açısından yalnızca bir dijital ödeme aracının hayata geçirilmesi değil; aynı zamanda kamu mali yönetimi, denetim yapısı ve finansal istikrar alanlarında köklü bir reformu tetikleyebilecek stratejik bir hamle olarak değerlendirilmelidir. Bu dönüşüm sürecinin başarıyla ilerleyebilmesi için, sadece teknik testler ve pilot uygulamalar değil; eşzamanlı olarak düzenleyici çerçevenin güçlendirilmesi, kurumsal işleyişin yeniden yapılandırılması ve toplumsal katılımın artırılması gerekmektedir.

Bu bağlamda geliştirilecek CBDC sisteminin Türkiye'deki finansal denetim mimarisi içinde yerini alabilmesi, çok katmanlı risk yönetimi araçlarının oluşturulmasına bağlıdır. Söz konusu dönüşüm süreci; hukuki temeller, teknolojik kapasite ve toplumsal katılım olmak üzere üç temel boyutta ele alınmalıdır:

- Mevzuat ve kurumsal yapı,
- Teknik altyapı ve denetim teknolojileri,
- Sosyal katılım ve uluslararası uyum.

Aşağıda, bu dönüşüm sürecini yönlendirmek amacıyla yedi temel stratejik başlıkta analiz ve öneriler sunulmaktadır:

6.1. Hukuki ve Düzenleyici Altyapının Güçlendirilmesi

DTL gibi CBDC'lerin etkili biçimde uygulamaya alınabilmesi için en öncelikli koşul, açık, tutarlı ve teknolojik gelişmelere uyumlu bir hukukî çerçevenin oluşturulmasıdır. ülkemizde mevcut finansal mevzuat CBDC'lerin tanımı, işlevi ve yasal kapsamı konusunda yeterli açıklığı henüz sunmamaktadır. Bu durum, hem uygulayıcı kurumlar hem özel sektör aktörleri hem de kullanıcılar açısından belirsizlik doğurmakta ve sistemin meşruiyetini zayıflatmaktadır. Bu çerçevede öncelikle atılması önerilen stratejik adımlar şunlardır: (TBMM, 2005; TBMM, 2013).

Dijital Paranın Hukuki Statüsünün Netleştirilmesi hedefi doğrultusunda;

- 1211 sayılı TCMB Kanunu, 5411 sayılı Bankacılık Kanunu ve 6493 sayılı Ödeme Hizmetleri Kanunu CBDC'ye özgü düzenlemelerle güncellenmelidir.
- Türk Borçlar Kanunu, Türk Ticaret Kanunu ve Vergi Usul Kanunu kapsamında, dijital parayla yapılan sözleşmelerin, ödemelerin ve mülkiyet devirlerinin hukuki güvenliği sağlanmalıdır.

³ Bankacılık Düzenleme ve Denetleme Kurumu

⁴ Mali Suçları Araştırma Kurulu

- Miras, haciz, sigorta gibi özel hukuk alanlarında dijital paranın niteliği açık şekilde düzenlenmelidir.

KVKK Uyumu ve Veri Hakları Rejiminin CBDC'ye Uygunlaştırılması hedefi doğrultusunda; (KVKK, 2016; European Parliament and Council, 2016).

- 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında CBDC'ye özel veri işleme protokolleri oluşturulmalıdır.
- Kullanıcı rızası, şeffaflık ve erişim hakkı ilkeleri sistem mimarisine entegre edilmelidir.
- Avrupa Birliği'nin GDPR normlarına benzer şekilde, "kontrollü anonimlik" ilkesine dayanan veri koruma yapıları oluşturulmalı ve Türkiye'ye uyarlanmalıdır.

MASAK Uyum Süreçlerinin Dijital Paraya Entegre Edilmesi bağlamında;

- MASAK, CBDC işlemleri için şüpheli işlemler için otomatik uyarı sistemleri barındıran bir AML/CFT5 modülü geliştirmelidir.
- TCMB ve MASAK arasında anlık ve çift yönlü veri paylaşımı sağlayacak teknik protokoller hayata geçirilmelidir.

Akıllı Sözleşmelerin Hukuki Statüsünün netleştirilmesi bağlamında;

- CBDC sistemlerinin programlanabilir para altyapısına uygun şekilde, akıllı sözleşmelerin hukuki geçerliliği tanımlanmalıdır.
- Söz konusu sözleşmelerle ilgili mahkeme, tahkim gibi uyuşmazlık çözüm yöntemleri netleştirilmelidir.

Pilot Regülasyon Alanlarının Geliştirilmesi hedefi doğrultusunda;

- Fintek firmalarının dijital ödeme çözümlerini kontrollü biçimde test edebileceği "düzenleyici deneme ortamları" (sandbox) oluşturulmalıdır.
- Bu alanlarda yapılacak testlerin gerçek kullanıcı verisi içermemesi ve kamu denetimi altında gerçekleştirilmesi önem arz etmektedir.

6.2. Denetim Kurumlarının Dijital Kapasitesinin Artırılması

CBDC'lerin sunduğu izlenebilirlik ve anlık veri üretimi potansiyeli, klasik kamu denetimi yaklaşımlarında köklü bir dönüşümü beraberinde getirebilir. CBDC ile birlikte, kamu harcamalarının etkinliği, sosyal transferlerin doğruluğu ve kamu alımlarındaki şeffaflık çok daha derinlemesine izlenebilir hâle gelecektir. Ancak bu potansiyelin gerçeğe dönüşebilmesi için denetim kurumlarının teknolojik yetkinliklerinin eşgüdümlü biçimde artırılması gerekmektedir. Bu çerçevede önerilen yapısal dönüşüm başlıkları şunlardır (BCBS, 2018):

- Kamu Denetim Panelleri: Kamu denetim otoritelerinin gerçek zamanlı veri takibi gerçekleştirebileceği merkezi ve bütünsel bir "dijital denetim paneli" altyapısı inşa edilmelidir. Bu sistem sayesinde kamu harcamaları, sosyal yardımlar ve doğrudan transferler kapsamlı bir şekilde izlenebilir hale gelecektir.
- Yapay Zekâ Tabanlı Denetim Algoritmaları: Özellikle sosyal yardımlar, doğrudan destek ödemeleri ve kamu ihaleleri gibi alanlarda kullanılmak üzere, anomali tespiti yapabilen yapay zekâ destekli denetim mekanizmaları geliştirilmelidir. Bu tür algoritmalar; işlem örüntülerini analiz ederek vergi kaçağı, usulsüzlük ve yolsuzluk gibi riskleri önceden saptama yeteneğine sahip olmalıdır (Arner, Barberis, & Buckley, 2017).
- Ortak Dijital Altyapı: Sayıştay, SPK, KGK gibi üst denetim kurumlarının ortak kullanımına açık, güvenli ve entegre bir dijital denetim altyapısı oluşturulmalıdır.
- Yetkinlik Geliştirme: SPK ve TCMB iş birliğiyle "Dijital Denetim Uzmanlığı" sertifika programları düzenlenmeli; bu alana özel lisansüstü programlar üniversitelerde yaygınlaştırılmalıdır.

6.3. Kurumlararası Koordinasyon ve Yetki Paylaşımı

CBDC sistemleri, çok paydaşlı bir yapıya sahip dijital kamu altyapısının (Digital Public Infrastructure – DPI) tipik bir örneği olarak değerlendirilebilir. Bu tür sistemlerin başarılı biçimde işleyebilmesi için, yalnızca teknik yeterlilik değil,

⁵ Karaparanın Aklanması ve Terörizmin Finansmanının Önlenmesi

Ayten ÇETİN, Serdar ALPAY

aynı zamanda kurumlar arası yönetim çerçevesinin de güçlü olması gereklidir. OECD (2024) tarafından yayımlanan çalışmada, dijital kamu altyapısının etkin kullanımı için “stratejik yönetim çerçevesi”, “çok paydaşlı iş birlikleri” ve “uzun vadeli fonlama mekanizmaları” gibi temel yapıtaşlarına vurgu yapılmaktadır. Bu bağlamda, Türkiye’de TCMB, BDDK, MASAK, Sayıştay ve TÜBİTAK⁶ gibi kurumlar arasında rollerin netleştirileceği bir “Dijital Türk Lirası Üst Kurulu” oluşturulması, yönetsimsel karmaşayı önlemek açısından kritik olacaktır.

Ayrıca, TCMB tarafından oluşturulan “Dijital Türk Lirası İşbirliği Platformu”, bu tür bir üst kurulun öncülü niteliğinde olup, kurumlar arası eşgüdüm ve teknik iş birliğini geliştirme amacı taşımaktadır (TCMB, 2023). OECD’nin önerdiği gibi, böyle bir üst kurul yalnızca teknik işleyişe değil, aynı zamanda kriz durumlarına müdahale, kamu-özel sektör koordinasyonu ve uluslararası etkileşim konularında da stratejik sorumluluk üstlenmelidir (OECD, 2024).

6.4. Siber Güvenlik ve Operasyonel Direnç Yapılarının Güçlendirilmesi

DTL sisteminin başarısı yalnızca ekonomik ve denetimsel etkinlikle değil, aynı zamanda siber dayanıklılık kapasitesiyle de doğrudan ilişkilidir. CBDC altyapıları, karakteristik olarak yoğun veri üretimi, kesintisiz çevrimiçi erişim ve çok paydaşlı bir yapı ile çalışmaktadır. Bu da onları hem dış tehditlere hem de iç zaafılara açık hale getirir. Ülkemizde DTL altyapısının sürdürülebilirliği için proaktif, modüler ve senaryo tabanlı bir siber güvenlik ve operasyonel direnç politikası gereklidir.

CBDC’ye yönelik ulusal bir siber güvenlik stratejisinin net biçimde tanımlanması, sistem bütünlüğü açısından kritik öneme sahiptir. Bu çerçevede, TCMB koordinasyonunda, TÜBİTAK-BİLGEM⁷ liderliğinde “CBDC Siber Güvenlik Strateji Belgesi” hazırlanmalıdır. Bu kapsamda belgenin aşağıdaki başlıkları içermesi önemlidir:

- Tehdit modellemesi,
- Güvenlik mimarisi tasarımı,
- Kritik bileşen listesi (veri merkezleri, mobil cüzdanlar vb.),
- İyileşme ve olay müdahale senaryoları,
- Kamu-özel iş birliği modeli.

Farklı alanlar bazında değerlendirilen öneriler aşağıda sıralanmıştır:

Kritik altyapıların belirlenmesi ve yedeklenmesi açısından:

- Veri merkezleri, ödeme köprü sunucuları, kimlik doğrulama altyapıları, “kritik dijital varlık” statüsüne alınmalıdır.
- Bu altyapılar, farklı coğrafi bölgelerde yedekli çalışacak şekilde yapılandırılmalı ve DDoS, ortadaki adam (MITM) saldırıları ile node manipülasyon girişimlerine karşı sürekli gözetim altında tutulmalıdır.
- Cold backup mimarisi uygulanmalı; yedek veriler belirli aralıklarla offline ortamlara alınmalıdır.

Bağımsız güvenlik testleri ve sürekli denetim açısından:

- ISO/IEC 27001, ISO 22301, NIST SP 800-53 gibi çerçeveler ile tam uyum sağlanmalıdır.
- TÜBİTAK destekli bağımsız test laboratuvarlarında, sistemler yılda en az iki defa sızma testi (penetrasyon testi) süreçlerinden geçirilmelidir.
- Dijital cüzdan sağlayıcıları ve ödeme arayüzleri için “güvenlik sertifikasyonu” şartı getirilmelidir.

Kullanıcı tarafı güvenlik katmanları açısından:

- DTL kullanıcılarının mobil uygulamalara erişiminde çok aşamalı kimlik doğrulama, biyometrik tanıma, cihaz eşleştirme ve konum tabanlı güvenlik önlemleri (geofencing) gibi çeşitli katmanlı önlemler uygulanmalıdır.
- İşlemlerde “harcama üst limiti alarmı”, “riskli işlem için ek doğrulama” gibi önlemler uygulanmalıdır.

Olay müdahale ve kurtarma senaryoları açısından:

- TCMB bünyesinde “CBDC Olay Müdahale Ekibi (CIRT)” kurulmalı; bu ekip içinden 7/24 görevli “acil müdahale hattı” tanımlanmalıdır.
- Siber saldırı anında sistemin otomatik olarak güvenli moda geçişi (safe mode fallback) mümkün olmalıdır.

⁶ Türkiye Bilimsel ve Teknolojik Araştırma Kurumu

⁷ TÜBİTAK Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi

- Her paydaş kurum (örneğin Ziraat Bankası, PTT, Vakıf Katılım) kendi içinde olay yönetim planı oluşturmali ve yılda bir kez tatbikat yapmalıdır.

Bu bölümde çizilen yapı, yalnızca teknik bir savunma kurgusu değil; aynı zamanda kurumsal koordinasyonu, kamu güvenini ve operasyonel sürekliliği bütüncül biçimde ele alan stratejik bir altyapı vizyonudur (CPMI & IOSCO, 2016; ENISA, 2022).

6.5. Veri Mahremiyeti ve Kullanıcı Haklarının Korunması

Veri mahremiyeti, CBDC sistemleri açısından yalnızca teknik bir tasarım unsuru değil; aynı zamanda toplumsal güveni şekillendiren ve anayasal düzeyde değerlendirilmesi gereken çok katmanlı bir konudur. DTL sistemi üzerinden yapılan her işlem, kullanıcıya dair zaman, yer, harcama kalemi ve tutar gibi pek çok bilgiyi içerdiğinden; bu verilerin nasıl toplandığı, işlendiği, paylaşıldığı ve korunduğu açık bir şekilde düzenlenmelidir. Özellikle 6698 sayılı KVKK ve Avrupa Birliği Genel Veri Koruma Tüzüğü, bu başlığın yasal temelini oluşturmaktadır: (KVKK, 2016; European Parliament and Council, 2016).

Kontrollü Anonimlik Modelinin Uyarlanması: Kullanıcı güveni, CBDC'nin toplumsal kabulünde kilit önemdedir. Avrupa Merkez Bankası'nın Dijital Euro tasarımı kapsamında geliştirdiği "Kontrollü Anonimlik" (tiered privacy) modeli, mahremiyet ile finansal gözetim arasında denge kuran bir çerçeve sunmaktadır. Bu çerçevede; (Panetta, 2023);

- Düşük tutarlı işlemler tamamen anonim tutulabilir,
- Yüksek tutarlı işlemler için denetim eşikleri belirlenebilir (örneğin 100.000 TL üzeri işlem),
- Şüpheli işlemler yalnızca mahkeme kararıyla ve bağımsız kurul onayıyla incelenmelidir.

KVKK ve GDPR Uyumlu Veri İlkeleri: Dijital Türk Lirası sisteminde, açık rıza, unutulma hakkı, şeffaflık ve gereklilik odaklı veri işleme gibi ilkeler doğrudan sistem tasarımına entegre edilmelidir. Bu kapsamda, kullanıcıların kendi verilerinin işlenme miktarı, paylaşım kapsamı ve saklama süresi gibi bilgilere erişim sağlayabileceği bir 'Veri Şeffaflık Paneli' oluşturulmalıdır. Kullanıcıların, kendi verilerini tek adımda anonimleştirme veya sistemden tamamen kaldırma yetkisine sahip olması güven tesisinde kritik bir unsur olacaktır.

CBDC'ye Özgü Veri Koruma Rehberi ve Kurumsal Yükümlülükler: KVKK ile uyumlu hazırlanacak "CBDC Veri Koruma Rehberi" şu unsurları içermelidir:

- TCMB'nin veri sorumluluğu sınırları,
- Alt yapı sağlayıcılarının (örneğin cüzdan operatörleri) yasal yükümlülükleri,
- Kullanıcı rızasının alınma yöntemi ve saklanma süreci,
- Her bir işlem için 'Veri İşleme Etki Analizi' yapılması yasal bir gereklilik haline getirilmelidir.

Şeffaflık Araçları ve Toplumsal Denetim: Toplum nezdinde hesap verebilirliği artırmak amacıyla:

- TCMB, her 6 ayda bir "CBDC Veri Kullanım Raporu" yayımlamalı,
- Bu raporda işlenen veri kategorileri, denetim talepleri, kullanıcı şikâyetleri gibi metrikler yer almalıdır,
- STK'lara ve üniversitelere bağımsız gözlemci erişimi verilerek dış denetim güçlendirilmelidir.
- Üniversitelerle iş birliği içinde kullanıcı deneyimi ve veri mahremiyeti konusunda etki analizleri yapılmalıdır.

Teknik Olarak Mahremiyetin Korunması: Kriptografik çözümler, özellikle zero-knowledge proof (ZKP) gibi teknikler aracılığıyla, işlemlerin doğruluğu sağlanabilirken; kimlik bilgileri gizli tutulmaya devam edebilir. Zero-knowledge proof (ZKP), bir tarafın belirli bir bilgiye sahip olduğunu karşı tarafa bu bilgiyi ifşa etmeden matematiksel olarak kanıtlamasını sağlayan bir kriptografik yöntemdir. Bu sayede kullanıcı işlem geçmişi cüzdan içinde yerel olarak şifreli tutulabilir, merkez bankasına ise yalnızca özet değer olarak iletilmesi sağlanabilir. Ayrıca, her bir kullanıcı için veri koruma profil seviyesi tanımlanarak tercihe göre değişen mahremiyet seviyeleri sunulmalıdır. Bu bölümde geliştirilmesi önerilen veri koruma mekanizmaları, yalnızca yasal bir gereklilik değil; aynı zamanda sisteme olan toplumsal güvenin inşası açısından da vazgeçilmez önemdedir (NIST, 2020; TCMB, 2023).

6.6. Uluslararası Uyumluluk ve Teknik Entegrasyon Stratejileri

CBDC'lerin yalnızca ulusal sınırlar içerisinde çalışan para birimleri değil, aynı zamanda sınır ötesi finansal entegrasyonun temel yapı taşları olacağı artık yaygın bir şekilde kabul görmektedir. Bu nedenle ülkemizin DTL Projesi,

Ayten ÇETİN, Serdar ALPAY

iç piyasaya odaklanmakla sınırlı kalmamalı; aynı zamanda bölgesel ve uluslararası düzeydeki CBDC girişimlerine entegre olabilecek biçimde yapılandırılmalıdır. Bu başlık altında hem kurumsal uyum, hem teknik standartlar hem de dijital finans diplomasisi açısından çok katmanlı öneriler sunulmaktadır: (BIS, 2021a; FATF, 2021b; BIS Innovation Hub, 2023e).

Küresel Kurumlarla Teknik ve Politik Uyum açısından:

- Türkiye, IMF'nin 2024 yılında yayımladığı CBDC Virtual Handbook⁸ dahil olmak üzere, BIS, ECB ve FATF gibi kurumların geliştirdiği rehber belgelerle teknik ve yönetsimsel uyum içinde olmalıdır (IMF, 2025).
- BIS'in Atlas Projesi kapsamında ortaya koyduğu denetim altyapısı, kullanıcı gizliliği ve şeffaf veri yönetimi ilkeleri Türkiye'nin dijital para sisteminde öncelikli olarak dikkate alınmalıdır (BIS Innovation Hub, 2023n).
- FATF tarafından sanal varlık hizmet sağlayıcılarına (VASP) yönelik yayınlanan AML/CFT çerçevesi, Türkiye'de dijital Türk Lirası ekosisteminde faaliyet gösteren cüzdan sağlayıcıları için bağlayıcı standartlar haline getirilmelidir.

Sınır Ötesi CBDC Pilotlarına Katılım açısından, Türkiye, Project mBridge, Project Dunbar, Icebreaker, Jura gibi sınır ötesi ödeme sistemlerini test eden CBDC projelerine aktif teknik ve diplomatik katılım sağlamalıdır. DTL'nin diğer dijital para sistemleriyle birlikte çalışabilirliğini test etmek amacıyla gerçek zamanlı döviz dönüşüm senaryoları denenmeli; PvP (payment versus payment) ve HTLC (hashed time-locked contracts) gibi güvenli ve otomatik yürütülen sınır ötesi ödeme mekanizmaları hayata geçirilmelidir.

Teknik Standardizasyon ve API Uyum Rehberleri açısından:

- DTL sistemi, ISO 20022 mesajlaşma standardı ile tamamen uyumlu hâle getirilmeli ve sınır ötesi işlemler bu protokol üzerinden yapılandırılmalıdır.
- Uluslararası geçerliliği olan API rehberleri, Türkiye'nin hem kamu hem özel sektöre sunacağı teknik entegrasyon dokümanları içinde yer almalıdır.
- Türkiye, uluslararası CBDC API standartlarının oluşturulduğu platformlara aktif katılım göstermeli ya da bölgesel düzeyde teknik iş birlikleri kurarak stratejik uyum sağlamalıdır.

Bölgesel İttifaklar ve Dijital Finans Diplomasisi açısından:

- Türkiye, İslam Kalkınma Bankası, Türk Devletleri Teşkilatı, Ekonomik İş Birliği Teşkilatı (ECO) gibi organizasyonlarla bölgesel CBDC entegrasyon ağı kurma girişiminde bulunmalıdır.
- Bu sayede hem siyasi hem ekonomik yakınlaşma, dijital altyapı iş birlikleri ile desteklenebilir.
- "Dijital Lira Diploması Platformu" oluşturularak, Ankara merkezli dijital ekonomi vizyonu bölgesel olarak yaygınlaştırılabilir.

Uluslararası Hukuki Uyum ve Veri Transferi Rejimi açısından:

- KVKK ve GDPR uyumu yanında, sınır ötesi veri paylaşımı rejimi oluşturulmalıdır.
- Özellikle işlem verilerinin hangi ülkelerle, ne tür koşullarda paylaşılacağı önceden belirlenmelidir.
- Veri emanet sistemleri (data escrow) yoluyla hem düzenleyici denetime uygunluk hem de bireysel gizlilik ilkesi dengeli biçimde sağlanabilir.
- Avrupa Veri Koruma Kurulu (European Data Protection Board-EDPB) ile iş birliğine dayalı eşgüdüm mekanizmalarının kurulması, uluslararası uyum sürecine katkı sağlayacaktır.

Bahis konusu başlıklar altında inşa edilecek küresel entegrasyon kapasitesi, yalnızca teknik değil, aynı zamanda Türkiye'nin bölgesel dijital güç olma potansiyelini doğrudan etkileyecek stratejik bir araç olarak değerlendirilmektedir.

6.7. Dijital Okuryazarlık ve Toplumsal Katılımın Artırılması

CBDC'ler artık yalnızca ulusal para birimleri değil; aynı zamanda küresel finansal entegrasyonun dijital altyapısı olarak görülmektedir (BIS, 2021a) Bu nedenle, Türkiye'nin DTL Projesi yalnızca iç piyasaya yönelik değil; aynı zamanda sınır ötesi ödeme sistemlerine entegre edilebilir, teknik olarak uyumlu ve politik olarak iş birlikçi bir yapıda kurgulanmalıdır. Aşağıda, bu sürecin başlıca stratejik boyutları sunulmaktadır: (Koonprasert, Kanada, Tsuda, &

⁸ CBDC Dijital Kılavuzu

Reshidi, 2024; OECD, 2022).

Ülkemizdeki farklı kullanıcı grupları (gençler, emekliler, KOBİ⁹'ler, çiftçiler, sosyal yardım alıcıları) için özgün bilgilendirme stratejileri geliştirilmeli ve söz konusu bilgilendirme içerikleri görsel, işitsel ve interaktif dijital medya unsurlarıyla desteklenmelidir.

İlköğretim düzeyinden başlayarak, ortaokul ve lise müfredatlarına "Dijital Para Okuryazarlığı" modülleri entegre edilmelidir. e-Devlet platformu üzerinden "Dijital Cüzdan Kullanımı", "Siber Güvenlikte Bireysel Korunma" gibi interaktif modüller halinde sunulması sağlanmalıdır". Bu eğitim modülleri, TÜBİTAK BİLGEM gibi yerel kurumların dijital okuryazarlık platformlarıyla entegre edilebilir (TÜBİTAK BİLGEM, 2025). Üniversitelerde, özellikle ekonomi, işletme ve hukuk bölümlerinde "CBDC ve Dijital Finans Uygulamaları" dersleri zorunlu/seçmeli hâle getirilebilir.

Esnaflık, çiftçi, bakkal gibi küçük ölçekli işletmelere yönelik; uygulamalı eğitim kitapçıkları, video rehberler, dijital platform eğitimleri hazırlanmalıdır. Dijital ödeme altyapısına sahip olmayan küçük işletmelere ücretsiz QR kodlu DTL ödeme kabul cihazları tahsis edilmelidir. Vergi kolaylıkları, dijitalleşme teşvikleri ve ödeme platformlarına katılım ödülleriyle KOBİ'lerin sisteme entegrasyonu hızlandırılmalıdır.

DTL kullanıcılarına açık olacak şekilde bir "Kullanıcı Geri Bildirim Platformu" kurulmalı; bu platform üzerinden; öneriler, şikâyetler, teknik hata bildirimleri toplanmalıdır. Toplanan geri bildirim verileri hem denetim raporlarına hem de sistem güncellemelerine doğrudan entegre edilmelidir. Kullanıcı temsiliyeti için yılda en az bir defa "DTL Forum Türkiye" düzenlenmeli, farklı bölgelerden seçilecek kullanıcı temsilcileri karar vericilerle doğrudan iletişim kurmalıdır. Benzer şekilde, BIS Innovation Hub tarafından geliştirilen Rosalind Projesi'nde de kullanıcı geri bildirimlerine dayalı katılımcı test süreçleri uygulanmıştır (BIS Innovation Hub;BoE, 2023)

Şeffaflık ve düzenli bilgilendirme, kamu güveninin inşasında belirleyici olacaktır. Bu hedef doğrultusunda, TCMB, her altı ayda bir "DTL Şeffaflık Raporu" yayımlamalı ve raporda (harcama verisi işleme hacmi, şüpheli işlem bildirim oranları, olası veri ihlali veya siber güvenlik olaylarının sayısı, kamu kurumlarıyla yapılan veri paylaşımının istatistikleri) gibi veriler kamuoyuyla paylaşılmalıdır. Bu raporlar sadeleştirilmiş infografikler ve kısa video sunumlarıyla halka açık platformlarda yayımlanmalıdır.

Bu faaliyetler, geçici çözümler yerine toplum genelinde dijital farkındalık ve güven kültürünü kalıcı hale getirecek yapısal bir yaklaşımla sürdürülmelidir.

7. SONUÇ

CBDC, yalnızca dijital ödeme sistemlerinin bir uzantısı değildir; aynı zamanda kamu maliyesi denetimi, finansal istikrar ve yönetim süreçlerinde köklü bir dönüşümün anahtarı olarak değerlendirilmektedir. Dijital Türk Lirası (DTL), teknolojik bir yenilik olmanın ötesinde, kamu kaynaklarının şeffaf biçimde izlenmesini ve risk izleme kapasitesinin artırılmasını mümkün kılan stratejik bir kamu aracı olarak öne çıkmaktadır.

Dijital denetim sistemleri, geleneksel yöntemlerin sınırlarını aşarak kamu harcamalarının izlenebilirliğini artırmakta ve hesap verebilirlik düzeyini güçlendirmektedir. Finansal denetim kurumlarının, anlık veri izleme yeteneklerine sahip API¹⁰'ler, otomatik raporlama araçları ve risk sınıflandırma algoritmalarıyla donatılmış dijital mimarilere geçiş yapması gerekmektedir. Blok zincir altyapısının sunduğu şeffaflık ve izlenebilirlik, anomali tespiti gibi ileri denetim modüllerini mümkün kılmakta; bu da kamu maliyesi yönetiminde yeni bir standart oluşturmaktadır.

Öte yandan bu dönüşüm yalnızca fırsatlarla sınırlı değildir. CBDC sistemleri; sistem çökmesi, siber saldırılar, veri ihlalleri ve uluslararası yasal uyumsuzluk gibi çok katmanlı riskler barındırmaktadır. Bu nedenle Türkiye'nin, yalnızca kriz sonrası müdahalelere değil; aynı zamanda dijital erken uyarı mekanizmaları, senaryoya dayalı stres testleri ve operasyonel sürdürülebilirlik planları gibi önleyici risk yönetimi araçlarına öncelik vermesi gereklidir.

DTL ekosistemi içinde MASAK, BDDK, TCMB, Sayıştay ve KVKK gibi kurumlar arasında açık şekilde tanımlanmış görev paylaşımı, veri erişim protokolleri ve denetim sorumlulukları tesis edilmelidir. Kurumsal rollerin belirsiz kaldığı bir ortamda hem veri güvenliği hem de kamu kaynaklarının etkin kullanımı riske girebilir. Etkili bir yönetim yapısı, bu risklerin en aza indirilmesini sağlayacaktır.

Bununla birlikte, CBDC sistemlerinin sunduğu tam şeffaflık ilkesi, bireysel mahremiyet hakları açısından çeşitli

⁹ Küçük ve Orta Büyüklükteki İşletme

¹⁰ Uygulama Programlama Arayüzü

Ayten ÇETİN, Serdar ALPAY

endişeleri de beraberinde getirmektedir. Bu çelişkiyi yönetebilmek adına; veri sınırlama, anonimleştirme ve kontrollü anonimlik gibi teknik çözümler sistem mimarisine entegre edilmeli, aynı zamanda yasal düzenlemelerle desteklenmelidir. Mahremiyet ile denetim arasında kurulacak hassas denge, sistemin meşruiyeti ve toplumsal kabulü açısından kritik öneme sahiptir.

Ulusal ölçekte geliştirilen CBDC sistemlerinin yanında, Türkiye'nin sınır ötesi dijital para platformlarında da aktif rol alması stratejik açıdan önemlidir. Ortak denetim algoritmaları, çapraz ülke uyum protokolleri ve veri paylaşım rejimleri gibi alanlarda sorumluluk üstlenilmesi, ülkemizin dijital finans alanında küresel ölçekte görünürlüğünü ve etki gücünü artıracaktır.

Sonuç olarak, Dijital Türk Lirası'nın başarısı sadece teknik yeterliliğe değil; güçlü bir denetim altyapısı, etkili risk yönetimi politikaları ve kurumlar arası koordinasyona dayalı yönetim kapasitesine bağlıdır. Bu sistem, kamu maliyesinin şeffaflığını ve güvenliğini artırırken; dijital kamu yönetiminin yeni nesil bir aracı olma potansiyeline de sahiptir. Bu nedenle, DTL'nin yalnızca TCMB'nin değil, tüm kamu yönetim kurumlarının dijital dönüşüm stratejilerinin merkezine alınması önerilmektedir.

KAYNAKÇA

- Adrian, T., & Mancini-Griffoli, T. (2021). The rise of digital money. *Annual Review of Financial Economics*, 13(1), s. 57-77.
- Arner, D. W., Barberis, J., & Buckley, R. P. (2017). FinTech, RegTech and the reconceptualization of financial regulation. *Northwestern Journal of International Law & Business*, 37(3), s. 371-413. <https://scholarlycommons.law.northwestern.edu/njilb/vol37/iss3/2/> adresinden alındı
- Arora, R., Du, H., Kazmi, R. A., & Le, D.-P. (2025). Privacy-enhancing technologies for CBDC solutions. *Bank of Canada*. doi:<https://doi.org/10.34989/sdp-2025-1>
- Auer, R., Cornelli, G., & Frost, J. (2020). Rise of the central bank digital currencies: drivers, approaches and technologies. *BIS*. <https://www.bis.org/publ/work880.pdf> adresinden alındı
- Darba, S., & Arora, R. (2020, 6). Privacy in CBDC technology. (B. o. Canada, Prodüktör) Staff Analytical Note 2020-9: <https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-9/> adresinden alındı
- European Parliament and Council. (2016, 4 27). Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679> adresinden alındı
- FATF. (2021b). Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. Paris. <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf> adresinden alındı
- FATF. (2024). Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers. FATF. <https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2024-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf> adresinden alındı
- Jiang, J., & Lucero, K. (2023). Background and Implications of China's Central Bank Digital Currency: E-CNY. *Journal of Law and Public Policy*, 33, s. 237-271. <https://ssrn.com/abstract=3774479> adresinden alındı
- Koonprasert, T. T., Kanada, S., Tsuda, N., & Reshidi, E. (2024). Central Bank Digital Currency Adoption: Inclusive Strategies for Intermediaries and Users. IMF. <https://www.imf.org/en/Publications/fintech-notes/Issues/2024/09/21/Central-Bank-Digital-Currency-Adoption-Inclusive-Strategies-for-Intermediaries-and-Users-555118> adresinden alındı
- KVKK. (2016). 6698 Sayılı Kişisel Verilerin Korunması Kanununun Amacı ve Kapsamı. <https://www.kvkk.gov.tr/Icerik/4185/6698-Sayili-Kisisel-Verilerin-Korunmasi-Kanununun-Amaci-ve-Kapsami> adresinden alındı
- Panetta, F. (2021, 11 5). Central bank digital currencies: a monetary anchor for digital innovation. Speech by Fabio Panetta, Member of the Executive Board of the ECB, at the Elcano Royal Institute. Madrid. <https://www.ecb.europa.eu/press/key/date/2021/html/ecb.sp211105~08781cb638.en.html> adresinden alındı
- Panetta, F. (2023, 9 4). Shaping Europe's digital future: the path towards a digital euro. Brussels.

<https://www.ecb.europa.eu/press/key/date/2023/html/ecb.sp230904~8f5dff1e57.en.html> adresinden alındı

Stanley, A. (2022). The ascent of central bank digital currencies: A new payment frontier. Finance & Development, 59(3), s. 44–49. <https://www.elibrary.imf.org/downloadpdf/view/journals/022/0059/003/article-A016-en.pdf> adresinden alındı

TBMM. (2005). 5411 sayılı Bankacılık Kanunu. TBMM.

TBMM. (2013). 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun. TBMM.

TCMB. (2023). Dijital Türk Lirası Araştırma Geliştirme Projesi Birinci Faz Değerlendirme Raporu. TCMB.

İnternet Kaynakları

BCBS. (2018). Sound practices: Implications of fintech developments for banks and bank supervisors. Basel Committee on Banking Supervision. BIS. <https://www.bis.org/bcbs/publ/d431.htm> adresinden alındı

BIS. (2020). Central bank digital currencies: foundational principles and core features. BIS. <https://www.bis.org/publ/othp33.htm> adresinden alındı

BIS. (2020). Enhancing cross-border payments: Building blocks of a global roadmap. Committee on Payments and Market Infrastructures. BIS. <https://www.bis.org/cpmi/publ/d193.pdf> adresinden alındı

BIS. (2021a). Central bank digital currencies: Financial stability implications. Basel: BIS. https://www.bis.org/publ/othp42_fin_stab.pdf adresinden alındı

BIS. (2023b). BIS Innovation Hub Annual Report 2023. BIS. 1 21, 2025 tarihinde <https://www.bis.org/about/areport/areport2023.pdf> adresinden alındı

BIS Innovation Hub. (2023e). Project Atlas: mapping the world of decentralised finance. BIS. 3 1, 2025 tarihinde <https://www.bis.org/publ/othp76.pdf> adresinden alındı

BIS Innovation Hub; BoE. (2023). Project Rosalind: Building API prototypes for retail CBDC ecosystem innovation. BIS. <https://www.bis.org/publ/othp69.pdf> adresinden alındı

Board Of Governors Of The Federal Reserve System. (2022). Money and Payments: The U.S. Dollar in the Age of Digital Transformation. <https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf> adresinden alındı

BoE. (2023). The digital pound: Technology Working Paper. The Bank of England. <https://www.bankofengland.co.uk/-/media/boe/files/paper/2023/the-digital-pound-technology-working-paper.pdf> adresinden alındı

Consultative Group On Risk Management. (2023). Central bank digital currency (CBDC) information security and operational risks to central banks. BIS. <https://www.bis.org/publ/othp81.pdf> adresinden alındı

CPMI & IOSCO. (2016). Guidance on cyber resilience for financial market infrastructures. BIS. <https://www.bis.org/cpmi/publ/d146.pdf> adresinden alındı

ECB. (2023). Shaping Europe's digital future: the path towards a digital euro. European Central Bank. <https://www.ecb.europa.eu/press/key/date/2023/html/ecb.sp230904~8f5dff1e57.en.html> adresinden alındı

ENISA. (2022). Cybersecurity for Digital Finance: Threat Landscape. European Union Agency for Cybersecurity (ENISA). <https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202022.pdf> adresinden alındı

Federal Reserve. (2022, 6 10). Money and payments: The U.S. dollar in the age of digital transformation. 3 15, 2025 tarihinde Board of Governors of the Federal Reserve System: <https://www.federalreserve.gov/publications/money-and-payments-discussion-paper.htm> adresinden alındı

IMF. (2025). Virtual Handbook on Central Bank Digital Currency. Washington, D.C. International Monetary Fund (IMF). (2024). Virtual Handbook on Central Bank Digital Currency. Washington, D.C.: IMF. Link: <https://www.imf.org/en/Topics/digital-payments-and-finance/central-bank-digital-currency/virtual-handbook> adresinden alındı

NIST. (2020). Security and Privacy Controls for Information Systems and Organizations. National Institute of Standards and Technology (NIST).

OECD. (2020). The OECD Digital Government Policy Framework: Six Dimensions of a Digital Government. OECD Publishing. . <https://doi.org/10.1787/f64fed2a-en> adresinden alındı

OECD. (2022). OECD/INFE Guidance on Digital Delivery of Financial Education. OECD. https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/04/oecd-infe-guidance-on-digital-delivery-of-financial-education_367fa011/c980ce2b-en.pdf adresinden alındı

OECD. (2024). Digital Public Infrastructure for Digital Governments. OECD. https://www.oecd.org/en/publications/digital-public-infrastructure-for-digital-governments_ff525dc8-en.html adresinden alındı

TÜBİTAK BİLGEM. (2025, 2 23). Eğitimler. TÜBİTAK BİLGEM: <https://bilgem.tubitak.gov.tr/> adresinden alındı