JOBIG Journal of Business, Innovation and Governance
ISSN 2717-9559 dergipark.org.tr/tr/pub/jobig
İZMİR KÂTİP ÇELEBİ ÜNİVERSİTESİ

DİJİTAL VARLIKLARIN BAĞIMSIZ DENETİMİ

INDEPENDENT AUDIT OF DIGITAL ASSETS

Hayrettin USUL
Prof. Dr., İzmir Kâtip Çelebi Üniversitesi, ORCID: 0000-0002-3930-0866, hayrettin.usul@ikc.edu.tr.

Kabul Tarihi / Accepted: 10 Haziran 2025

İletişim / Correspondence: Hatrettin USUL

Benzerlik Oranı/ Plagiriasim: %13

Makale Türü/Article Type: Araştırma Makalesi/ Research Article

ÖZET

Dijitalleşmenin yoğun olarak yaşandığı günümüzde, şüphesiz dijital varlıkları kayıt altına alınması kadar; bu varlıkların denetimi de ayrı bir öneme sahiptir. Bunun en büyük nedeni ise, dijital varlıkların denetiminin, geleneksel denetimden farklı süreci gerektirmesidir. Bu gerekliliğin sebebi ise, bu varlıkların kendine özgü yapısı ve karmaşıklığıdır. Bu karmaşık yapı, bu varlıkların muhasebe kayıtlarının yapılması kadar; denetimine de zorlu kılmaktadır. Çünkü; standartlar bu varlıklara ilişkin bir hüküm getirmemekte; uygulamacıların yorumunu dikkate almaktadır. Burada unutulmaması gereken husus uygulamacıların yorumlarının, yasal hükümlere ve standartları dikkate alarak yapılması gerekliliğidir. Ayraca; denetim kuruluşlarının dijital varlıkların denetimini yapmadan önce; kendi durum analizlerini yapmalarını standart istemektedir.

Anahtar Kelimeler: Dijital varlıklar, Denetim, Dijitalleşme

JEL Kodları: M 41, M42, M49

ABSTRACT

In today's world where digitalization is intensely experienced, undoubtedly, the auditing of digital assets is of particular importance as well as the recording of digital assets. The biggest reason for this is that the audit of digital assets requires a different process than the traditional audit. The reason for this necessity is the unique structure and complexity of these assets. This complexity makes the auditing of these assets as challenging as their accounting records. This is because the standards do not stipulate a provision regarding these assets; they take into account the interpretation of the practitioners. It should be noted that the interpretations of the practitioners should be based on legal provisions and standards. Furthermore, the standard requires audit firms to conduct their own due diligence before conducting an audit of digital assets.

Keywords: Digital assets, Audit, Digitalization

JEL Codes: M 41, M42, M49

1. GİRİŞ

Dijital varlıkların denetim süreci oldukça zor ve karmaşıktır. Bunun nedeni ise, finansal raporlama standartlarının dijital varlıkların muhasebeleştirilmesiyle ilgili standartlar tanımlamamaları ve muhasebeleştirme işini ise yorum bırakmasıdır.[1] Bu yorum, kayıt aşamasında mali müşavirin; denetim aşamasında da bağımsız denetçinin mesleki bilgisi ve yeteneği çerçevesinde olacaktır.

Bağımsız denetim; bir işletmenin finansal tablolarında yer alan varlıkların, yükümlülüklerin ve öz kaynakların; işletme gelir ve giderlerinin dönem içinde gerçekleşen faaliyetler sonucu oluştuğu (Var olma ve oluşum); işletmede gerçekleşen finansal faaliyetlerin bir bütün olarak finansal tablolarda yer aldığı (Bütünlük); bilanço tarihi itibariyle aktifinde bulunan varlıklar ile pasifinde bulunan yükümlülüklerin işletmeye ait olduğunu (Haklar ve yükümlülükler); işletme varlıklarının, borçlarının, öz kaynakların, gelir ve giderlerin doğru miktarlarla gösterildiği (Değerleme ve dağıtım) ve de işletmede gerçekleşen muhasebe hareketlerinin doğru hesaba kaydedildiğini, doğru şekilde sınıflandırıldığını, anlaşılabilir olduğunu ve bu işlemleri ilişkin açıklamaların doğru şekilde dipnotlarda yer aldığını (Sunuş ve açıklama) standartlar bazında incelemesini yapma ve sonucu raporlama işlevidir. Bu bağlamda, bağımsız denetçiler yukarıda verdiğimiz amaçlar doğrultusunda da dijital varlıkların incelemesini yaparlar. Ancak, dijital varlıkların incelemesi ciddi anlamda bilgi ve beceri istemektedir. Bu bilgi ve beceriler; finansal standartları veya denetim standartlarının bilmenin ötesinde, dijital varlıkları tanımaları ve yorum yapabilecek düzeyde vakıf olmalarını gerektirmektedir. Çünkü dijital varlık ekosistemi; uygulayıcılara benzersiz riskler ve yeterli uygun kanıt elde etmekten, bilgi teknolojileri (BT) ortamını anlamaya kadar; değişen daha karmaşık denetim zorlukları sunan ve devamlı gelişen bir süreç olarak karşımıza çıkmaktadır.

Dijital varlıklar genel olarak iki kategoriye. Bunlar; kripto dijital varlıklar ve kripto olmayan dijital varlıklardır. Kripto dijital varlıklar; coin, tokenler iken, kripto olmayan dijital varlıklar ise ses, video ve fotoğraflardır. Bu çalışmamızda sadece kripto dijital varlıkların denetimi incelenecektir.

2. DİJİTAL VARLIKLARIN DENETİM SÜRECİ

Genel olarak denetim süreci sözleşme öncesi ve sonrası olarak iki kategoride incelenir. Bu bağlamda bu incelemede, dijital varlıkların sözleşme öncesi ve sonrası süreç olarak iki kategoride ele alınacaktır.

2.1. Sözleşme Öncesi Denetim Süreci

Bağımsız denetim firmasının, bağımsız denetim sözleşmesi imzalanmadan önce kendi kapasitesinin değerlemesini yapması gerekmektedir. Denetim yetisinin, dijital varlıkların denetimi için yeterli görülmesi halinde, müşteri işletme ayrıntılı incelenmeye tabi tutulmalıdır. Bu incelemeler olumlu sonuç verirse, denetim sözleşmesi denetim firması tarafından imzalanır. Aksi durumda, denetim firmasının sözleşme imzalamamasında hem kendisi hem de müşteri işletme açısından faydalı olacaktır. Aşağıda bu hususlar ayrıntılı olarak incelenmeyi çalışılmıştır.

2.1.1. Bağımsız Denetim Firmasının Durum Analizini Yapması

Denetim firması, kendisine denetim talebiyle gelen müşteri firmayla anlaşma yapmadan önce bir durum analizi yapması gerekmektedir. Denetim firması, yeteneklerini değerlendirerek, yapılacak olan dijital varlıkların denetime yeterli olup, olmadığını belirlemesi gerekir. Kalite Kontrol Standardının (KKS) 1'in 26'ncı paragrafı uyarınca denetim şirketi durum analizi yaparken; denetimin yürütülmesi konusunda yetkin olmak, zaman ve kaynaklar dâhil olmak üzere, denetimi yürütmek için gerekli beceri ve kabiliyete sahip olmak ve etik

[1] Dijital varlıkların muhasebeleştirilmesi için bakınız; İzmir Dayanışma Dergisi, Cilt: 135, Sayı:7, 2024

hükümlere uygunluk sağlayabilme yeteneklerinin olması gerektiğini göz önünde bulundurmalıdır (KGK, 2022).

Yetkinlik, eğitim ve deneyimin bir sentezinden elde edilir, bağımsız denetçinin gerekli olan bilgi birikimine hakim olmasıyla başlar. Yetkinliğin sürdürülmesi, bağımsız denetçinin meslek hayatı boyunca devam etmesi gereken öğrenme ve mesleki gelişim taahhüdünü gerektirir. Bu durum, bağımsız denetçinin bireysel sorumluluğudur. Tüm görevlerde ve tüm sorumluluklarda, her bağımsız denetçi hizmetlerinin kalitesini, bu ilkelerin gerektirdiği yüksek profesyonellik seviyesini karşılamasını sağlayacak bir yetkinlik seviyesine ulaşmayı taahhüt etmelidir. Yetkinlik, bağımsız denetçinin kolaylıkla ve zekayla hizmet vermesini sağlayan bir anlayış ve bilgi seviyesine ulaşılmasını ve de sürdürülmesini temsil eder. Aynı zamanda, mesleki bir görevin veya denetim firmasının kişisel yeterliliğini aşması durumunda; danışma veya yönlendirme gerekebileceğini belirterek, bağımsız denetçinin yeteneklerinin sınırlarını da belirler. Her bağımsız denetçi; eğitim, deneyim ve muhakemesinin üstleneceği sorumluluk için yeterli olup olmadığını değerlendirerek kendi yetkinliğini değerlendirmekten sorumludur (AICPA, 2024).

Kısa adı AICPA olan Amerikan Sertifikalı Mali Müşavirler Enstitüsü tarafından tanımlanan yetkinlik kavramının incelenmesinde; her bir bağımsız denetçi kendi yeterliliğini belirlemesi gerekmektedir. Bu nedenle dijital varlıkların denetim işini üstlenmeyi düşünen bağımsız denetçi; kendi yeterliliğini sorgulaması gerekir. Denetçinin; dijital varlık işlemleriyle ilgili temel blok zinciri teknolojisini anlaması birinci öncelik olarak ele alınması gerekir. Çünkü dijital varlıkların denetimi oldukça karmaşık kriptografi ve bilgi teknolojisinin (BT) kullanımını içerir. Bazı durumlarda, ilgili kontrollerin etkin biçimde işlediğine güvenmeden kripto varlıkların denetimi mümkün olmayabilir. Bu nedenle, önemli kripto varlık işlemlerini içeren finansal tabloların denetimine ilişkin bir sözleşmeyi kabul etme veya devam ettirme konusunda karar verilirken, söz konusu denetimi yürüten kişilerin (Hem denetim ekibi üyeleri hem de denetçinin faydalandığı uzmanlar dâhil) uygun yetkinlik ve kabiliyetlere sahip olup olmadığına karar verilmelidir.

Durum analizi yapan denetim firması etik konusunu da dikkate almak zorundadır. Burada karşımıza etik ile beraber bağımsızlık kavramı bir bütün olarak karşımıza çıkar. Bağımsız denetçinin dijital varlıkların denetimi uygulamasında; mesleki standartlara uygun olarak davranması gerekmektedir. Ancak, bağımsız denetim ekibinin bir üyesi denetime tabi kuruluş tarafından ihraç edilen dijital varlıklara sahip olabilir. Bu durum etik bir durum yaratmakla beraber, denetim yapan firma açısından da bağımsızlığın ortadan kalkmasına yol açabilir.

Denetim firması durum analizi yaparken dikkate alması gereken değir bir hususta denetim firmasının kalite kontrol sisteminin yapısıdır. Dijital varlıkların çok yeni olması, denetim firmaları açısında mevcut kalite kontrol sistemini güncellemesini gerektirmektedir. Denetim firması; dijital ekosisteme katılan kuruluşlar için denetim işi yürütmeyi planlıyorsa ve işe alım ve eğitim programları şu anda bu ekosisteme özgü konuları dikkate almıyorsa; firmanın müşteri kabulü veya devamlılığı ve diğer kalite kontrol süreçlerinde gerekli yetkinlik ve yeteneklere sahip yeterli personele sahip olup olmadığının veya dışarıdan uzman istihdam etme ihtiyacının değerlendirilmesi üzerinde daha fazla düşünülmesi ve dikkat edilmesi gerekebilir (AICPA, 2024).

2.1.2. Müşteri İşletmenin İncelenmesi

Dijital varlık ekosistemindeki görevler teklifleri değerlendirmek için müşteri kabul ve devam sürecinde titiz sorgulamalar gerektirir. Bu durum büyük ölçüde temel teknolojinin karmaşıklığından, benzersiz risklerden ve yeterli ve uygun denetim kanıtı toplamadaki ilgili denetim zorluklarından kaynaklanmaktadır. Bu nedenle bağımsız denetçinin, işletmenin BT'ye nasıl bağımlı olduğunu veya BT tarafından nasıl etkinleştirildiğini ve bilgi sistemlerinin finansal bilgileri kaydetmek ve sürdürmek için nasıl kullanıldığını anlaması gerekmektedir.

Denetim firması müşteri işletmenin değerlemesini yaparken; denetim uygulamaları sırasında bir sürprizle karşılaşmamak için detaylı incelemesini yapması bir ihtiyaçtır. Örneğin, denetçi; denetim uygulamaları sırasında yönetimin finansal tabloların hazırlanması ve gerçeğe uygun sunumuna ilişkin sorumluluklarını yerine getirmediğini görebilir. Bu durum işletme yönetiminin kusurundan kaynaklandığı gibi, bilgisizliğinde de olabilir. Örneğin, müşteri işletme ilk kez önemli dijital varlık işlemleriyle karşılaşmış olabilir. Destekleyici defter ve kayıtlar veya dijital varlıkları veya ilgili işlemleri etkin bir şekilde muhasebeleştirmek ve finansal tablolarda adil bir şekilde sunmak için uygulanan iç kontrol sistemi yetersiz ve etkin değildir. Yine, müşteri işletme yönetimi dürüst olmayabilir. Dolayısıyla işletme yönetimi tarafından hazırlanan finansal tablolar önemli yanlışlık riski taşıyabilir. Bu durumda denetçi; denetim talep eden müşteri işletmeyle sözleşme imzalamaması gerekmektedir. Kamu Gözetim Kurumu (KGK), yayımlamış olduğu bültende denetçinin işi kabul etmeden önce, müşterinin dürüstlüğünü değerlendirmiş olmasını istemektedir (KGK, 2022).

Yukarıda da ifade ettiğimiz gibi, blok zinciri teknolojisi ve dijital varlıklarla ilişkili karmaşıklık göz önüne alındığında; yönetimin işletmenin defterlerini ve kayıtlarını tutmak ve varlıklarını güvence altına almak için gereken beceri setlerinden veya yetkinliklerden yoksun olabilmesi söz konusu olabilir. Bu nedenle, işletmenin personelinin gerekli yetkinlik ve yeteneklere sahip olup olmadığının değerlendirilmesi, denetçinin bir denetim işini kabul etmesinde önemli bir faktör olabilir. Yönetim dürüst ve sağlam bir iş stratejisine sahip olsa bile, uygun beceri setlerine veya yetkinliklere sahip değilse, yönetim eksiklikleri gidermeden bir denetim mümkün olmayabilir. Bunun nedeni, uygun defter ve kayıtların tutulmaması, süreç ve kontrollerin uygulanmaması veya yönetimin denetçiye aşırı güvenmesi ve dolayısıyla, denetçinin finansal tablolar hakkında bağımsız ve tarafsız bir görüş sunma sorumluluğunu yerine getirememesi riski olabilir. Yönetim, dijital varlık ekosisteminde, alandaki benzersiz riskleri belirleyebilecek ve bu risklere yanıt vermek için iç kontroller tasarlayıp uygulayabilecek deneyime sahip olup, olmadığı denetçi tarafından sorgularken, aşağıda örnek olarak verilen hususları göz önüne almalıdır. Bunlar (AICPA, 2024);

- ✓ Yönetim, geçerli düzenleyici ortamı ve gelişen yasa ve yönetmelik hükümlerini anlıyor mu?
- ✓ Yönetim, blok zincirinden veya üçüncü bir taraftan bağımsız defter ve kayıtlar tutuyor mu veya işletmenin bakiye ve işlem kayıtlarını yalnızca blok zincirinden veya üçüncü bir tarafça sağlanan beyanlardan mı elde etmektedir?
- ✓ Yönetim, yeterli bilgi veya uzmanlığa sahip olmadığı durumlarda (Örneğin, kurum içi veya kurum dışı hukuk müşavirleri veya kriptografi ve siber güvenlik uzmanları dahil olmak üzere BT uzmanları) uygun ve nitelikli uzmanları veya muhasebe danışmanlarını görevlendiriyor mu ve bu uzmanlar tarafından gerçekleştirilen işlerin etkin incelemelerini yapıyor mu?
- ✓ Yönetim, geçerli finansal raporlama çerçevesinin faaliyetlerine nasıl uygulandığını anlayabiliyor mu?

2.2. Sözleşme Sonrası Denetim Süreci

Sözleşme sonrası denetim süreci klasik olarak geçici denetim planın yapılmasıyla başlar. Denetçi denetim planının yapılması aşamasında, işletmenin iç kontrol sisteminin etkinliği test etmesinden sonra, iç kontrol sisteminin etkinliğine göre; denetim planına son şeklini verirken, denetim riskini ve uygulayacağı denetim tekniklerini belirlemesi gerekmektedir. Bu teknikleri belirlerken unutulmaması gereken husus, dijital ekosisteminin karmaşık olması kadar, dijital varlıkların birbirinden farklı olmasından dolayı yoruma dayalı olarak kayıt altına alınması ve denetiminin de, bu bağlamda yapılmasıdır. Yine unutulmaması gereken diğer bir hususta, denetim sürecinde, blok zinciri teknolojisinin doğası ve dijital varlık bakiyelerini ve işlemlerini izlemek, toplamak, mutabakat sağlamak ve raporlamak için kullanılan teknoloji hakkında bir anlayış edinmek, denetçinin gerekli olabilecek denetim prosedürlerinin kapsamını değerlendirmesine yardımcı olacağı gerçeğidir. Aşağıda dijital varlıkların denetimi bazında sözleşme sonrası süreç anlatılmaya çalışılmıştır.

2.2.1. Denetim Programının Yapılması

Denetim programları; bağımsız denetimin yürütülmesi sırasında her bir denetim alanı için uygulanması düşünülen denetim işlemlerinin çalışma kağıtlarıyla ilişkilendirilerek, kalemler itibariyle çeşit, tarih ve süre ile görevlendirilen elamanlar bakımından ayrıntılı olarak belirlendiği belgelerdir. Diğer bir ifadeyle denetim programları, denetim planının ayrıntılı ve taktiksel dökümüdür. Bağımsız denetim programı çerçevesinde yapılacak görevlendirmede; ekip elamanlarının sorumluluk, mesleki teknik ve bilgi, yetenek ve deneyimlerle ilgili hususlara dikkat edilir ve görevler açıklıkla belirlenir. Başarılı bir denetim, başarılı bir şekilde yapılan denetim programıyla yapılır. Başarılı denetim programı, denetçiyi önce bilgi ve sonra kanaat sahibi yapacak denetim delili elde etmesini sağlar. Unutulmaması gereken husus ise dijital kanıtların niteliği, geleneksel denetimlerden büyük ölçüde farklılık gösterdiği gerçeğidir (Boillet,J., 2024).

Bu nedenle, bağımsız denetici, denetim programının yapılması sırasında azami ihtimamı göstermek zorundadır. Aşağıda örnek olarak bir denetim programı verilmeye çalışılmıştır (AICPA, 2024);

- ✓ BT genel kontrollerinin, uygulama kontrollerinin ve dijital varlıkları izlemek, bir araya getirmek ve mutabakatını sağlamak için uygulanan süreçlerin niteliğini anlamak ve aynı zamanda temel blok zinciri teknolojisi ve bilinen eksikliklerle ilişkili BT risklerini azaltmak için yönetimle, özellikle de BT departmanından kişilerle istişarede bulunun,
- ✓ İşletmenin kontroller ve süreçlerle ilgili personelinin yeterliliğini değerlendirin ve dijital varlıklarla işlem yapmak için kullanılan teknolojiyi anlayın,
- ✓ Kurumun BT uzmanlarını (İçeriden veya dışarıdan) kullanıp kullanmadığını ve dijital varlık işlemlerinin işlenmesine izin verecek yeni teknolojiyi uygulama planlarının olup olmadığını sorgulayın,
- ✓ Kuruluşun hizmet kuruluşlarını kullanımını (Örneğin, özel anahtarları güvence altına almak) ve SOC[2] raporlarının mevcudiyetini anlayın. Mevcut olan tüm SOC raporlarını edinin,
- ✓ Yönetimin SOC raporlarını ve uygun tamamlayıcı kullanıcı kuruluş kontrollerini gözden geçirmek için kontrollere sahip olup olmadığını sorgulayın,
- ✓ SOC raporundaki kontrollerin finansal raporlama risklerine karşı duyarlılığına odaklanın,
- ✓ Müşteri kabulü ve durum tespitiyle ilgili olarak üçüncü taraflarca gerçekleştirilen süreç ve kontrollerin anlaşılması da dahil olmak üzere, hizmet kuruluşları (Örneğin, saklama kuruluşları) üzerinde gerçekleştirilen durum tespiti prosedürlerini anlamak için yönetimle görüşün,
- ✓ Kurumun yeni dijital varlıklarda işlem yapmaya yönelik durum tespiti sürecini, örneğin mutabakat mekanizmasını nasıl değerlendirdiğini ve işlem yapmak için gerekli olabilecek mevcut cüzdan yazılımını değerlendirmeye yönelik yönetişim modelini ve sürecini sorgulayın,
- ✓ Bireysel gizliliği daha da artırmak için özel olarak tasarlanmış belirli varlıkların denetçinin yeterli ve uygun denetim kanıtı elde etme kabiliyetini etkileyip etkilemeyeceğini göz önünde bulundurun,

[2] SOC (Security Operations Center) yani "Güvenlik Operasyonları Merkezi", İşletmelerin güvenlik açıklarını izleyen, sızma testi yapan ve düzeltmeler için çalışan siber güvenlik raporlarına verilen isimdir.

- ✓ Aşağıdakiler de dahil olmak üzere, kuruluşun özel anahtarları ve diğer müşteri bilgilerini korumasını sorgulayın;
  - ➢ Özel anahtarların nasıl saklandığı da dahil olmak üzere, özel anahtarları oluşturmak ve saklamak için kullanılan altyapının yapısı (Örneğin, sıcak cüzdanlar ve soğuk cüzdanlar gibi),
  - ➢ Dijital varlık işlemlerinin yetkilendirilmesinde görevler ayrılığı olup, olmadığı,
  - ➢ Anahtarların şifrelenmesi ve bölünmesi veya çoklu imza adres imzalama gereksinimleri yoluyla bir işlemi işlemek için gereken kullanıcı sayısı,
  - ➢ Herhangi bir yetkisiz faaliyet için adreslerin izlenmesi gibi.
- ✓ İşletmenin ilişkili tarafların ve ilişkilerin yanı sıra ilişkili taraf işlemlerini belirleme, muhasebeleştirme ve açıklama sürecini sorgulayın,
- ✓ Siber suç veya sadakat sigortasının varlığını tespit edin,
- ✓ Cüzdan yazılımını ve cüzdan yedeklemesini sorgulayın. (Örneğin, sistem arızası durumunda tüzel kişinin özel anahtara sürekli erişimini sağlamak için şifrelenmiş özel anahtar bilgilerinin yedeklenip yedeklenmediği tespit edin).

2.2.2. Risk Değerlemesinin Yapılması

Denetim riski; iç kontrol sisteminin etkin olmamasından kaynaklanan riskler, işletmenin yapısından kaynaklanan riskler ile denetçinin denetim çalışması sırasında hata ve hileleri ortaya çıkaramama riski olmak üzere üç kavramın bileşeninden oluşur. Denetim riski, denetim uygulamalarını etkiler. Bu nedenle denetim risklerinin denetçi tarafından değerlendirilmesi oldukça önemlidir. Unutulmaması gereken husus, yapısal ve kontrol risklerinin (Bu iki riskin bileşeni, önemli yanlışlık riski olarak tanımlanır) işletmenin finansal tablolarında yer almasıdır. Önemli yanlışlık riskleri, yeterli ve uygun denetim kanıtı elde etmek amacıyla uygulanacak ilave denetim prosedürlerinin niteliğini, zamanlamasını ve kapsamını belirlemek üzere denetçi tarafından belirlenir ve değerlendirilir. Bu kanıtlar, denetçinin kabul edilebilir ölçüde düşük bir denetim riski seviyesinde finansal tablolar hakkında görüş bildirmesini sağlar. Bağımsız Denetim Standardı (BDS) 315 "Önemli Yanlışlık" risklerinin belirlenmesi ve değerlendirilmesinin 25'inci paragrafı uyarınca, denetçinin risk değerlendirme prosedürleri uygulayarak finansal tabloların hazırlanmasıyla ilgili bilgi sistemi ve iletişim sürecini anlaması gerekir. Bu kapsamda; denetçi tarafından anlaşılması gereken hususlardan birisi de işletmenin bilgi sisteminde bilgi akışının nasıl olduğudur. Ayrıca, BDS 315'in aynı paragrafı uyarınca denetçinin, işletmenin bilgi teknolojisi (BT) çevresini de çözmesi bir zorunluluktur.

Temel olarak, denetçinin riskleri ele almak için yeterli ve uygun denetim kanıtı elde etmesi gerekir. Dijital varlık ekosistemindeki riskler, kontroller ve kanıt türleri farklıdır ve benzersiz zorluklar sunar ve dolayısıyla daha fazla kanıta ihtiyaç duyulur. İkinci olarak, denetçiler genellikle önemli yanlış beyan risklerine yanıt vermek için bir kontrol testi ve esas prosedürlerin bir kombinasyonunun gerekli olduğu durumlarla karşılaşabilirler. Bu karşılaşma büyük ölçüde temeldeki blok zinciri teknolojisinin karmaşıklığından, benzersiz risklerden ve yeterli ve uygun denetim kanıtı toplamadaki ilgili denetim zorluklarından kaynaklanmaktadır (EY, 2004).

Her bir kurumun gerçekleri ve koşulları, dijital varlık ekosistemindeki faaliyetlerinin niteliğine bağlı olarak farklılık gösterir. Denetçi, işletmeyi ve çevresini anlamaya çalışırken, diğer hususların yanı sıra işletmenin stratejisi, faaliyetleri, iç kontrolleri ve dijital varlık ekosistemindeki rolüyle ilgili bilgileri toplar. İşletme yönetimi ve çevresi hakkında yeterli bir anlayış elde etmek için gerekli çaba düzeyi ve denetçinin risk değerlendirme prosedürleri, diğer hususların yanı sıra; işletme yönetiminin iş amacına, dijital varlık ekosistemindeki rolüne, yönetimin yetkinliklerine ve beceri setine ve hizmet kuruluşlarının katılımına bağlı olarak muhtemelen değişiklik gösterecektir.

Aşağıda örnek olarak denetçinin, işletme ve çevresini anlamaya yönelik risk değerlendirme sürecinin bir parçası olarak; yönetime, yönetişimden sorumlu olanlara veya kurum içinde hile veya hatadan kaynaklanan önemli yanlışlık risklerinin belirlenmesine

yardımcı olabilecek sorular verilmeye çalışılmıştır. Ancak, listenin her şeyi kapsaması amaçlanmamıştır ve örnek sorular sadece bir başlangıç noktası olarak görülmelidir. İşletmenin gerçeklerine ve koşullarına bağlı olarak muhtemelen ilave takip sorularına ihtiyaç duyulacaktır (AICPA, 2024);

- ✓ İşletmenin mevcut ve gelecekte beklenen dijital varlık tutma veya işlem yapma ile ilgili iş amacı ve işletmenin dijital varlık ekosistemindeki rolü nedir?
- ✓ İşletme ne tür dijital varlıklara sahiptir? İşletme bu dijital varlıkları nasıl elde etmiştir? Özel anahtarların korunması da dahil olmak üzere, varlıkların korunmasına ilişkin kontrolleri nelerdir?
- ✓ İşletme ile saklama kuruluşu arasındaki anlaşmanın yasal yönlerini değerlendirmek için uygun yasal analizin yapılmasına yönelik bir süreç mevcut mudur?
- ✓ İşletme likit olmayan veya az işlem gören dijital varlıklar bulundurmakta mıdır? Eğer öyleyse, işletmenin bu varlıkların likit olmayan veya az işlem gören varlıklar olup olmadığını belirlemeye yönelik politikaları ve bu varlıkların muhasebeleştirilmesine ilişkin politikaları nelerdir? İşletme bu dijital varlıkları nasıl değerlemektedir ve değeri ölçmek ve belirlemek için kullandığı kaynaklar nelerdir? İşletmenin bu dijital varlıkları kaydetmeye yönelik muhasebe politikaları mevcut mudur?
- ✓ İşletme, olası dijital varlık kayıplarını karşılamak için uygun sigorta kapsamının mevcut olup olmadığını değerlendirmek üzere, gerek işletmede gerekse işletme adına varlıkları elinde tutan tüm kuruluşlarda kontrollere ve politikalara sahip midir? Eğer varsa, bu poliçeler elde tutulan dijital varlıkların tamamını mı yoksa sadece bir kısmını mı kapsamaktadır? Poliçeler ne tür kayıpları kapsamaktadır ve sahipliğin kanıtlanması kanıtlar var mıdır?
- ✓ İşletme, dijital varlıkları nakit, diğer dijital varlıklar veya diğer mal ve hizmetlerle (Örneğin satıcılara, çalışanlara, yüklenicilere ödeme yapmak için) takas ediyor mu?
- ✓ Dijital varlık işlemleri blok zincirine kaydediliyor mu? İşletmenin defterlerini ve kayıtlarını tutma ve defterlerini ve kayıtlarını desteklemek için harici blok zinciriyle mutabakat sağlama yöntemi nedir? Zincir dışı işlemler varsa bunlar nasıl yönetilmekte, kaydedilmekte ve mutabakatı sağlanmaktadır?
- ✓ İşletmenin dijital varlığın değerlemesini etkileyen potansiyel piyasa risklerine ilişkin görüşleri nelerdir (Örneğin, işletmenin dijital varlık piyasasının volatilitesi ve olgunluk seviyesi gibi hususlar)?

Ayrıca bunlara ek olarak denetçinin risk değerlendirme süreci, analitik prosedürlerin yanı sıra gözlem ve incelemeyi de içermelidir. Risk değerlendirme süreci olarak uygulanan analitik prosedürler; risk faktörlerinin tanımlanmasında ve değerlendirilmesine yardımcı olabilir. Örneğin denetçi, olağandışı işlemleri belirlemek amacıyla işlem hacimleriyle ilgili analitik incelemeyi gerçekleştirmek için bir blok zincirinden elde edilen bilgileri kullanmayı düşünebilir. Blockchain teknolojisi akıllı sözleşme kimliği üzerinde yapılan bir aramada eksiksiz bir denetim izi sağlar ve harici bir denetimde blok zinciri verilerinin veri odaklı kontrolü nispeten hızlı ve kısa sürede yapılmasına imkan vermektedir (Rewin ;Doekhi: 79).

Risk değerlemesinin yapılmasında dikkate alınması gereken diğer bir husus ise, önemli yanlışlık riski arttıkça, denetim kanıtının yeterli ve uygun olmasının yanı sıra; denetim sonuçlarının daha ikna edici olması gerekliliğidir. Yeterli ve uygun denetim kanıtının neyin oluşturduğu, belirlenen riskin özelliklerine bağlı olarak mesleki bir muhakeme konusudur. Bu nedenle ihtiyaç duyulan kanıtlara ilişkin denetçi yargıları; denetçilerin ilave denetim prosedürlerinin niteliğini, zamanlamasını ve kapsamını nasıl tasarlayacaklarını etkileyecektir. Denetçi, ilgili iddia düzeyinde tek başına yeterli ve uygun denetim kanıtı sağlayan etkili maddi doğrulama prosedürleri tasarlamayı imkânsız bulabilir. Bu gibi durumlarda, maddi doğrulama prosedürlerine ek olarak, denetçi dijital varlıklarla ilişkili kontrollerin işleyiş etkinliği hakkında yeterli ve uygun denetim kanıtı elde etmek için kontrol testleri tasarlamalı ve gerçekleştirmelidir (Örneğin, dijital varlıkların korunması ve özel anahtarlara erişim üzerindeki yönetimin kontrollerinin test edilmesi gibi).

2.2.3. Dış Kaynaktan Bilgi Alınması

Bağımsız denetçi; yeterli denetim kanıtı elde etmek amacıyla dış kaynaklardan hizmet alabilir. Bu hizmet alımları; dijital varlıkların performansın beklentilere ve sözleşme yükümlülüklerine uygun olduğunu doğrulamak, CSP'den[3] (Could service provioder) düzeltme talebinde bulunmak için yapılır. Denetçinin, dış kaynaklı hizmetler üzerindeki kontrol düzeyi hakkında genel bir sonuca varmak için bu süreçleri değerlendirmesi gerekmektedir. Denetçi ihtiyaç duyduğu güvenceyi elde etmek için CSP tarafından sunulan mevcut güvence raporlarını ve sertifikaları kullanır. Bağımsız denetçi, dışarıdan almış olduğu bilgileri kullanmadan önce aşağıda verilen hususları dikkate alma zorundadır. Bunlar (Putters, et al., 2021);

- ✓ Denetçinin mesleki kanaatine göre, bilginin rutin olarak güvenilir bilgi sağlama geçmişi olan bir dış bilgi kaynağı tarafından sağlanıp sağlanmadığı da dâhil olmak üzere; dış bilgi kaynağının bilgiye ilişkin yetkinliği ve itibarı,
- ✓ Denetçinin dış bilgi kaynağı tarafından sağlanan bilgilerin güvenilirliğine ilişkin geçmiş deneyimini sorgulaması,
- ✓ Bilginin yönetim veya denetçi tarafından kullanıldığı amaca benzer bir amaç için harici bir bilgi kaynağından alınan bilginin uygunluğunun veya güvenilirliğinin kullanıcılar tarafından genel piyasa kabulüne ilişkin kanıt,
- ✓ Raporlayan işletmenin, elde edilen ve kullanılan bilgilerin uygunluğunu ve güvenilirliğini ele alan kontrollere sahip olup olmadığı.

Dış kaynaklardan bilgi edinme ne kadar önemliyse, aynı oranda teyitte o kadar önemlidir. Dış kaynaklardan elde edilen bilgiler denetçi tarafından nasıl sorgulanması gerekiyorsa, aynı şekilde teyitlerinde uygunluğu ve güvenilirliği ile ilgili hususlar ve verilen cevapların doğruluğu sorgulanmalıdır. Denetçi bu sorgulamaları yaparken (Putters, et al., 2021);

- ✓ Üçüncü tarafın SOC raporuna sahip olup olmadığı,
- ✓ SOC raporunun içeriğinin denetçinin yanıtın güvenilirliğine ilişkin değerlendirmesini nasıl etkilediği,
- ✓ İşletmenin bağımsız dijital varlık işlem kayıtları ile üçüncü taraf bilgilerinin mutabakatı da dahil olmak üzere, üçüncü taraftan elde edilen bilgilerin güvenilirliğini değerlendirmek için işletme tarafından uygulanan kontrollerin tasarımı ve işleyiş etkinliği,
- ✓ Üçüncü tarafın harici gözetim veya düzenlemeye tabi olup olmadığı ve nasıl tabi olduğu (Örneğin, ilgili yargı düzenlemeleri kapsamında nitelikli bir saklama kuruluşu olarak) veya belirli güvene dayalı sorumluluklara sahip olup olmadığı,
- ✓ Üçüncü tarafın mali tablolarının mesleki yeterlilik ve bağımsızlığını kanıtlamış bir denetim firması tarafından denetlenip denetlenmediği,
- ✓ Üçüncü tarafın itibarı ve geçmişi (Örneğin, kurumun siber saldırı geçmişi).

2.2.4. Gerçeğe Uygun Değerin Bulanması

Dijital varlıklar, piyasa fiyatlarının günlük olarak dalgalanmasıyla son derece değişkendir (Yatsyk; Shvets 2020). Bu varlıklar ister kısa vadeli, ister uzun vadeli amaçlarla elde tutulsun; tarihi maliyeti cari değerlerinden farklı olacaktır. Dijital varlıkların gerçeğe uygun değerle finansal tablolarda gösterilmesi gerekir. Bağımsız denetçi, işletmenin finansal tablolarda yer alan dijital varlıkların gerçeğe uygun değerle yer alıp, almadığını incelemesi gerekir. Gerçeğe uygun değer, piyasa katılımcılarının bakış açısını yansıtır ve bu nedenle işletme için bir çıkış fiyatını temsil eder. Gerçeğe uygun değer, finansal tablo kullanıcılarına, gelecekteki nakit akışlarının tutarı, zamanlaması ve belirsizliği hakkında fikir verir (Klopper,et al, August 2023). Bu nedenle denetçi, dijital varlıkların miktar olarak incelenmesi kadar, tutarlarının da incelenmesi gerekir. Denetçi, finansal tabloların tutarlarını belirlerken, dijital varlıkların gerçeğe uygun değerini dikkate almak zorundadır. Ancak, burada sorun gerçeğe

[3] Bulut bilişim hizmetleri sağlayan firmalar ve kuruluşlar CSP olarak adlandırılır.

uygun değerinin tespiti aşamasında "Aktif piyasa"nın tespitidir. Aşağıda bu konu ayrıntılı olarak incelenmeye çalışılmıştır.

Genel olarak; dijital varlık için normalde işlem yaptığı pazarın, aksine bir kanıt olmadığı sürece, ana pazar olduğu varsayılır. Bir dijital varlığın gerçeğe uygun değerini belirlemek için, bir kripto varlığın işlem gördüğü ana (Veya en avantajlı) piyasayı belirlemesi; bu piyasanın aktif mi yoksa pasif mi olduğunu değerlendirilmesi gerekir. İlaveten; raporlanan piyasa işlemlerinin düzenli olup olmadığını incelenmesi ve piyasa tarafından üretilen bilgilerin güvenilir olup olmadığını belirlenmesi söz konusudur. Aktif piyasa TFRS (Türkiye Finansal Raporlama Standartları)13' de "Varlık veya borca ilişkin işlemlerin, fiyatlandırma bilgisi sağlamaya yönelik yeterli sıklıkta ve hacimde sürekli bir şekilde gerçekleştiği piyasadır" şeklinde tanımlanmıştır (KGK 2024).

Genellikle Dijital varlıkların piyasa işlemleri dışında gerçeğe uygun değerin bağımsız olarak ölçmek zor olabilir. Özellikle, az işlem gören dijital varlıkların gerçeğe uygun değerini tahmini sıkıntı yaratabilir. Dolayısıyla, bu tür varlıkların uygun şekilde değerlenmediği için yanlış beyan edilmesi riskinin daha yüksek olma ihtimal dâhilindedir. Bu durum, yönetimin kazançları yönetmek için önyargılı varsayımlar kullandığı bir dolandırıcılık riski faktörünün göstergesi olabilir. Bu nedenle, problemli bir piyasanın olduğu durumlarda, denetçinin, piyasayı sorgulaması gerekir. Bu durumda, denetçi gereceğe uygun değeri tespit etmek amacıyla aşağıda verilen yöntemlere başvurmalıdır.

Denetçi, ana piyasanın bulunmaması durumunda, varlığın satılabileceği en avantajlı piyasayı belirlemelidir. Bu piyasa, işlem maliyetleri ve taşıma maliyetleri dikkate alındıktan sonra, varlığın satılması için elde edilecek tutarı maksimize eden veya yükümlülüğün devredilmesi için ödenecek tutarı minimize eden piyasa olarak tanımlanır (FASB ASC 820-10-35-5A). Ayrıca, belirlenen dijital varlıkların gerçeğe uygun değeri, ana piyasadaki (Ana piyasa yoksa en avantajlı piyasa) katılımcıları arasında bir işlemin gerçekleşeceği fiyatı yansıtmalıdır. Ana piyasa, varlık veya yükümlülük için en büyük hacme ve faaliyet düzeyine sahip piyasa olarak tanımlanır. En avantajlı piyasa ise, işlem maliyetleri (Örneğin, borsa veya komisyoncu ücretleri) dikkate alındıktan sonra kripto varlığın satılması için elde edilecek tutarı maksimize eden piyasadır. (FASB ASC 820). Denetçi en avantajlı piyasa kavramını, değerlemesi yapılan kripto varlık için bir ana piyasa olmadığı durumlarda uygular.

Birçok piyasanın hala düzenlenmediği düşünülürse, kripto bir varlık için gözlemlenebilir girdiler aktif piyasa dışındaki iki yönlü işlemleri, brokerlerden alınan bazı fiyatları ve diğer bilgileri içerebilmektedir. Broker fiyatlarının kullanıldığı durumlarda bunlar dikkatle değerlendirilmelidir. Broker fiyatları gözlemlenebilir piyasa işlemlerine dayalı olmak yerine modellerden elde edilmiş olabilir. Genel olarak, bir değerleme modeli dönemden döneme tutarlı olarak uygulanmalıdır. Kripto varlıklara yönelik piyasa hızla gelişmektedir ve bu nedenle piyasa katılımcılarınca kullanılan değerleme teknikleri de yüksek ihtimalle gelişecektir. Değişimin şartlar altında eşit derecede veya gerçeğe uygun değeri daha iyi temsil edecek şekilde sonuç verdiği durumlarda TFRS 13 işletmenin değerleme tekniklerinde (Veya çoklu değerleme teknikleri arasında uygulanan ağırlıklarda) değişiklik yapmasına izin vermektedir. Sonuç olarak; denetçi aktif piyasası olmayan ya da az işlem gören dijital varlıkların değerlemesini yaparken aşağıda verilen hususları dikkate alması gerekir. Bunlar (FASB ASC 820);

- ✓ Denetçi, işletme tarafından yapılan analizin tutarlılığını test etmeli,
- ✓ İşletmenin uygulamış olduğu değerleme modeli, önemli varsayımlar ve yönetim tarafından kullanılan temel veriler de dahil olmak üzere, işletmenin değerleme metodolojisinin anlaşılması, değerlendirilmesi ve test edilmesi,
- ✓ Piyasa derinliği ve likidite de dahil olmak üzere, işletmenin aynı veya karşılaştırılabilir kripto varlıkları için piyasanın aktif olup olmadığına ilişkin değerlendirmesinin elde edilmesi ve değerlendirilmesi gerekmektedir.

2.2.5. Dijital Varlıkların Sunumunun İncelenmesi

Daha önceden de ifade ettiğimiz gibi, genelde muhasebe bilgi sistemleri dijital varlık işlemlerini karşılayacak şekilde tasarlanmamıştır. Bu nedenle dijital varlıkların sunumu oldukça önemlidir. Her şeyden önce muhasebe sistemlerindeki işlemlerin uygun sınıflandırmasını belirlemekten yönetim sorumludur. Bu nedenle, bu işlemlerin işletmenin muhasebe sistemine doğru şekilde kaydedilmesi için, (Örneğin işletmeye ait varlıkların müşteriler adına tutulan varlıklardan ayırt edilmesi gibi) ilave süreçler gerekebilir. Bu ek süreçler ilave riskler doğurabilir. İşlemin özünün anlaşılması, işletmenin muhasebe kayıtlarını belirleyebilmesi için gereklidir. İşletme, dijital varlıkların işletmenin mali kayıtlarına nasıl kaydedileceğini veya kaydedilip kaydedilmeyeceğini ele alan politika ve prosedürler tasarlamalı ve uygulamalıdır.

Dijital varlıklar, doğrulama ve güvenlik amacıyla kriptografi kullanılarak dağıtılmış bir defter (Blockchain) üzerinde yapılan dijital kayıtlar olarak tanımlanmaktadır. Dağıtılmış defter blockchain ağındaki tüm işlemlerin kaydını tutar. Dijital varlıklar, bir değişim aracı, mal veya hizmet sağlamak veya bunlara erişmek için bir finansman aracı olarak gibi çeşitli amaçlar için kullanılma kabiliyetleri söz konusudur. Bu nedenle, bir dijital varlığın muhasebe uygulamasının nihai olarak belirli şartlarına, biçimine, temel hak ve yükümlülüklerine dayanmaktır (Afterman, May, 2023).

Dijital varlıkların doğru şekilde finansal tablolarda gösterilmesi, daha önceden de ifade ettiğimiz gibi, işletme yönetiminin sorumluğundadır. Denetçi ise, işletme yönetiminin dijital varlıkların işletmenin yayımlamış olduğu finansal tablolarda doğru şekilde sunumu mevzuata uygun olarak gösterildiğini tespitini yapmak zorunluluktur. Burada unutulmaması gereken husus ise; dijital varlıklar birbirinden farklı olduğundan, kayıt altına alınması büyük ölçüde mesleki muhakeme ve yoruma dayalıdır. Örneğin, dijital varlık tanımı içinde yer alan coinler ile tokenlerin muhasebeleştirilmesi farklılıklar gösterecektir. Bu nedenle denetçi işletme yönetiminin yapmış olduğu yorumları, tekrar gözden geçirmesi gerekmektedir. Örneğin; bitcoin gibi varlıklar genel olarak maddi olmayan duran varlıklar olarak tanımlanırken, stablecoinler, sahibine ihraç eden işletmede bir mülkiyet payı sağlıyorsa, (FASB ASC 321) finansal yatırım olarak değerlendirilecektir. Yine, stablecoin bir finansal varlık veya gömülü bir türev içeren bir finansal araç ise, (FASB ASC 815) türevler ve riskten korunma kapsamında değerlendirilmelidir.

5. SONUÇ

Dijital varlıkların denetimi ciddi olarak bilgi ve beceri istemektedir. Bu nedenle denetim firması kendisine gelen denetim teklifini kabul etmeden önce; teklif edilen denetim sürecini başarılı bir şekilde götürebilecek yeterli ekip ve teknolojiye sahip olup, olmadığını irdelemedir. Bu irdeleme olumlu sonuçlanırsa; daha sonra müşteri işletmenin dijital varlıklara karşı gösterdiği tavrı test etmelidir. Bu amaçla sorumlu denetçi, bazı denetim tekniklerini kullanarak sorgulama yapması gerekir.

Denetim sözleşmesinin imzalanmasından sonra denetçi; denetlenecek işletmenin iç kontrol sisteminin dijital varlıkların korunması ve kaydedilmesi gibi aktiviteleri yerine getirip, getiremediğini sorgulayıp, denetim planına son şeklini verirken; denetim riskini belirlemelidir. Denetçi bu riskleri tahmin ederken mutlaka, işletmenin dijital eko sistemi içindeki yerini sorgulamalıdır.

Bağımsız denetçi; yeterli denetim kanıtı elde etmek amacıyla dış kaynaklardan hizmet alabilir. Bu hizmet alımları; dijital varlıkların performansın beklentilere ve sözleşme yükümlülüklerine uygun olduğunu doğrulamak, CSP'den düzeltme talebinde bulunmak için yapılır. Denetçinin, dış kaynaklı hizmetler üzerindeki kontrol düzeyi hakkında genel bir sonuca varmak için bu süreçleri değerlendirmesi gerekmektedir. İkinci yaklaşımda, elde tutulan kuruluş ihtiyaç duyduğu güvenceyi elde etmek için CSP tarafından sunulan mevcut güvence raporlarını ve sertifikaları kullanır. Güvence raporlarının kapsamı ve uygulanabilirliğinin yanı sıra dış denetçinin yeterliliği, raporun kalitesi vb. hususların da değerlendirilmesi gerekecektir. Üçüncü yaklaşım, muhtemelen diğer müşterilerle işbirliği içinde CSP'de denetimler gerçekleştirmeyi amaçlamaktadır.

Dijital varlıkların denetimde bir başka zorluk ise; bu varlıkların gerçeğe uygun değerinin bulunmasıdır. Özellikle, az işlem gören dijital varlıklara ait gerçeğe uygun değerinin bulunması daha riskli olabilir. Bu nedenle denetçi; dijital varlıkların işlem gördüğü piyasayı sorgulaması gerekmektedir. Son olarak denetçi; bu varlıkların sunumunun doğru şekilde yapılıp, yapılmadığını irdelemesi gerekmektedir.

KAYNAKÇA

AICPA; (American Institute of Certified Public Accountants), Accounting for and Auditing of Dijital Assets, June 30, 2024, https://www.aicpa-cima.com

Afterman, A. B„"Special Report A Closer Look at The AICPA Practıce Aid On Accounting and Financial Reporting For Digital Assets", Thomson Reuters, May, 2023

Boillet, J., "When auditors encounter digital assets such as cryptocurrencies in financial statements, do they audit them as cash, financial instruments or something else?",

EY,"how-to-audit-the-next-generation-of-digital-assets"https://www.ey.com

Financial Stability Board (FSB) High-level Recommendations for the Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets, Final report, 17 July 2023

Kamu Gözetim Kurumu (kgk), "Kripto Varlıkların Bağımsız Denetime Etkisi", 2022, kgk.gov.tr

Kamu Gözetim Kurumu (kgk), Türkiye Finansal Raporlama Standartları, kgk.gov.tr

Klopper, N.,Brink, B.S. Magaretha, S., "Determining the Appropriate Accounting Treatment of Cryptocurrencies Based on Accounting Theory", Journal of Risk and Financial Management, 23 August 2023

Putters, J., Hashemi, J., B., and Yavuz, A., "Demystifying Public Cloud Auditing for IT Auditors", Advanced Digital Auditing, Theory and Practice of Auditing Complex Information Systems and Technologies ,(Ed. Berghout, E, et al), Springer

Rewin J. M. Doekhi "The Intercompany Settlement Blockchain: Benefits, Risks, and Internal IT-Controls", Advanced Digital Auditing, Theory and Practice of Auditing Complex Information Systems and Technologies ,(Ed. Berghout, E, et al), Springer

Yatsyk, T., Shvets, V., "Cryptoassets as an Emerging Class of Digital Assets in Financial Accounting" Economic Analys-XXI, 2020

Extended abstract

In the contemporary era marked by rapid digital transformation, auditing digital assets has emerged as a complex and essential function within financial oversight. This paper, delves into the intricacies of auditing digital assets, especially in the absence of direct and comprehensive regulatory standards. Unlike traditional financial assets, digital assets present unique structural characteristics and technological challenges, requiring auditors to adopt innovative approaches and develop new competencies.The auditing of digital assets, particularly cryptocurrencies such as coins and tokens, demands more than just familiarity with financial reporting standards. It necessitates proficiency in blockchain technology, understanding of IT ecosystems, and the ability to assess risk within an environment that is both decentralized and dynamic. The paper underscores that the ambiguity surrounding the classification and treatment of digital assets in accounting standards leaves room for

professional judgment—both at the recording stage by accountants and at the auditing stage by independent auditors.The study outlines a two-phase audit approach: pre-engagement and post-engagement. In the pre-engagement phase, the auditing firm must conduct a comprehensive self-assessment to determine its capacity and technical capability to audit digital assets. This includes evaluating personnel expertise, technological infrastructure, ethical independence, and the adequacy of quality control systems. Ethical considerations are critical, as ownership of digital assets by audit team members can compromise independence.Equally vital is the due diligence on the client company. Auditors must assess the management's awareness of digital asset risks, the adequacy of internal controls (especially IT-based ones), and the company's readiness in terms of qualified personnel and compliant record-keeping systems. If the management lacks competence in handling digital asset processes or shows signs of dishonesty, the auditor may rightfully decline the engagement. In the post-engagement phase, the auditor designs and implements a risk-based audit plan, taking into account the nature of digital assets and their associated risks. Since blockchain-based assets can vary significantly in how they are recorded and presented, auditors must tailor their audit programs accordingly. These plans should incorporate detailed assessments of general IT controls, blockchain transaction verifiability, wallet security, custody arrangements, and third-party service providers. The paper also elaborates on the necessity of evaluating audit risks, particularly those stemming from the complexity of blockchain systems, potential management bias in valuation, and the reliability of external information sources. To address these risks, auditors are encouraged to apply analytical procedures using blockchain data, verify the operation of control systems, and seek corroborative evidence from external service organizations (e.g., cloud providers or custodians), including SOC (System and Organization Controls) reports. A critical part of auditing digital assets is determining their fair value. Given the volatility of cryptocurrency markets and the absence of active, regulated markets for many tokens, auditors face challenges in identifying "principal" or "most advantageous" markets. Valuation requires scrutiny of market depth, price consistency, and broker reliability. Where market data is insufficient, valuation models may be employed, and auditors must assess their inputs and assumptions rigorously. Furthermore, the presentation and disclosure of digital assets in financial statements must be accurate and comply with applicable financial reporting frameworks. This includes appropriate classification (e.g., intangible assets, financial investments, or derivatives), and clear distinction between company-owned assets and those held on behalf of clients. For example, Bitcoin might be classified under intangible assets, while stablecoins could be considered financial instruments, depending on the rights they confer. The paper concludes by emphasizing that digital asset auditing demands a combination of financial acumen, technological literacy, and robust judgment. Audit firms must ensure readiness before accepting such engagements and remain vigilant throughout the audit process. Continuous updates to audit methodologies and integration of IT and cryptographic insights are essential for ensuring audit quality in this emerging and high-risk domain.