Bölüm 2

Kripto Muhasebe Hilelerine Zemin Hazırlayan Faktörler: Finansal Raporlama ve Adli Muhasebe Perspektifi

Elif Şarman Umut[1]

Özet

Kripto para birimleri ve dijital finans ekosistemleri, finansal piyasalarda önemli bir dönüşüm yaratmıştır. Ancak, merkeziyetsiz yapıları, düzenleyici boşluklar ve şeffaflık eksikliği nedeniyle muhasebe hileleri ve finansal manipülasyonlar açısından risk taşımaktadır. Bu çalışma, kripto muhasebe hilelerine zemin hazırlayan temel faktörleri, finansal raporlama ve adli muhasebe perspektifinden incelemektedir.

Kripto varlıklarla bağlantılı muhasebe hileleri genellikle manipüle edilmiş finansal tablolar, off-chain işlemler, yasa dışı fon transferleri ve sahte rezerv bildirimleri şeklinde ortaya çıkmaktadır. Özellikle merkeziyetsiz finans (DeFi) platformları ve kripto borsaları, geleneksel denetim mekanizmalarından kaçınarak finansal tablolarını yanıltıcı şekilde düzenleyebilmektedir.

Araştırmada, düzenleyici boşluklar, muhasebe standartlarındaki belirsizlikler ve blokzincir teknolojisinin sunduğu anonimlik gibi faktörlerin muhasebe sahtekarlıklarını kolaylaştırdığı ortaya konmuştur. Çalışma, ayrıca adli muhasebe tekniklerinin ve blokzincir analiz araçlarının bu tür hileleri tespit etmekte nasıl kullanılabileceğini tartışmaktadır.

Sonuç olarak, kripto muhasebe hilelerinin önlenmesi için daha kapsamlı düzenleyici çerçevelerin oluşturulması, finansal şeffaflığın artırılması ve adli muhasebe araçlarının daha etkin şekilde kullanılması gerekmektedir. Bu bağlamda, kripto varlıkların denetlenebilirliği konusunda uluslararası iş birliği oldukça önemli olmaktadır.

1 Dr., Başkent Üniversitesi, İktisadi İdari Bilimler Fakültesi, İşletme Bölümü, esarman@baskent.edu.tr, https://orcid.org/0000-0002-7755-6790

https://doi.org/10.58830/ozgur.pub689.c2909

GİRİŞ

Kripto para birimleri ve dijital finans ekosistemleri, son yıllarda finansal piyasaların önemli bir bileşeni haline gelmiştir. Geleneksel finansal sistemlere alternatif olarak ortaya çıkan bu varlıklar, merkeziyetsiz yapıları ve blokzincir teknolojisine dayalı işlem kayıt sistemleriyle dikkat çekmektedir (Schwarcz, 2024). Ancak, bu yenilikçi finansal yapıların getirdiği avantajların yanında, muhasebe ve finansal raporlama açısından ciddi riskler barındırdığı da bir gerçektir. Kripto varlıkların şeffaflık eksikliği, düzenleyici boşluklar ve yüksek volatiliteye sahip olmaları, muhasebe hilelerine zemin hazırlayan faktörler arasında yer almaktadır (Akanbi, 2024).

Muhasebe hileleri, genel bir bakış açısı ile, şirketlerin finansal tablolarında yanıltıcı bilgiler sunarak yatırımcıları ve düzenleyici kurumları yanlış yönlendirmesi anlamına gelmektedir (Cumming vd., 2025). Kripto muhasebesi özelinde bu hileler; manipüle edilen finansal raporlar, gizlenen dijital varlık işlemleri, off-chain kayıtlar ve yasadışı fon transferleri gibi unsurlar içerebilmektedir (Hossain, 2023; Akanbi, 2024). Adli muhasebe uzmanları, blokzincir analiz araçlarını kullanarak şüpheli işlemleri inceleyebilse de, kripto para birimlerinin anonimlik seviyesi, dolandırıcıların kimliklerini gizlemelerine yardımcı olmaktadır (Duan vd., 2024). Özellikle merkeziyetsiz finans (DeFi) platformlarında, sahte işlemler yoluyla piyasa manipülasyonu yapmak mümkün hale gelmiştir (Carletti vd., 2024).

Dijital finans dünyasında dolandırıcılık risklerini artıran unsurlar üç temel başlık altında incelenebilir:

1. Düzenleyici Boşluklar ve Hukuki Eksiklikler: Birçok ülkede kripto varlıklarla ilgili düzenlemeler hala gelişim aşamasındadır ve bu durum, şirketlerin muhasebe hilelerine açık kapı bırakmaktadır (Wats vd., 2023).
2. Muhasebe Standartlarının Belirsizliği: Kripto varlıkların nasıl muhasebeleştirileceği konusunda uluslararası standartların netleşmemesi, finansal raporlama süreçlerinde farklı yaklaşımlara neden olmaktadır (Akanbi, 2024).
3. Teknolojik Faktörler: Blokzincir teknolojisinin sunduğu şifreleme mekanizmaları ve akıllı kontratlar gibi unsurlar, dolandırıcılık vakalarının tespitini zorlaştırabilmektedir (Carey ve Webb, 2017).

Bu çalışma kapsamında öncelikle kripto varlıkların uluslararası düzenlemeler kapsamında nasıl raporlandığı ele alınacak, sonrasında ise kripto muhasebe hilelerine zemin hazırlayan faktörler, finansal raporlama perspektifinden incelenecek ve son olarak da adli muhasebenin bu bağlamda

nasıl bir çözüm sunabileceği değerlendirilecektir. Çalışmanın temel amacı, kripto para piyasalarındaki dolandırıcılık vakalarının nedenlerini anlamak, bu vakaların muhasebe uygulamaları üzerindeki etkilerini değerlendirmektir.

1. Kripto Varlıkların Uluslararası Düzenlemelerde Değerlendirilmesi

Kripto varlıklar, geleneksel finans sistemine alternatif bir yapı sunarak küresel ekonomide önemli bir yer edinmiştir. Ancak bu yeni finansal araçların getirdiği fırsatlar kadar, düzenleyici zorluklar da dikkat çekicidir. Kripto varlıkların merkeziyetsiz yapısı, ülkeler arasında farklı yasal çerçevelerin geliştirilmesine neden olmuştur. Avrupa Birliği, MiCA (Markets in Crypto-Assets) gibi düzenlemelerle sektöre kapsamlı bir yaklaşım getirirken, ABD ve Çin gibi büyük ekonomiler de farklı politikalar benimsemiştir. Kripto varlıkların yasa dışı faaliyetlerde kullanılma riski, finansal istikrar üzerindeki etkileri ve yatırımcı koruma gereklilikleri, uluslararası düzenleyicileri ortak çözümler üretmeye yönlendirmektedir. Bu bağlamda, uluslararası finans kuruluşları, G20 ve IMF gibi organlar, kripto varlıkların yasal çerçevesini şekillendirme sürecinde aktif rol oynamaktadır. Ancak, farklı ülkeler arasındaki düzenleyici farklılıklar, küresel uyumun sağlanmasını zorlaştırmaktadır.

1.1 IFRS Kapsamında Kripto Varlıkların Sınıflandırılması

Uluslararası Finansal Raporlama Standartları (IFRS) Yorumlama Komitesi tarafından yayınlanan düzenlemelere göre, kripto varlıkların "nakit" veya "nakit benzeri varlıklar" olarak sınıflandırılması mümkün değildir. Komite, IAS 32 Finansal Araçlar Standardı'nda "nakit" varlıkları, "tüm işlemlerin ölçüldüğü ve finansal tablolara yansıtıldığı değişim aracı" olarak tanımlamıştır (IAS 32.AG3). Ancak IAS 32 kapsamında, kripto varlıkların evrensel bir değişim aracı olarak kabul edilmediği ve çoğu ülke tarafından resmi para birimi olarak tanınmadığı belirtilmiştir (IFRS Foundation, 2023).

IFRS 9 Finansal Araçlar Standardı'na göre, finansal varlıklar bir sözleşmeye istinaden ortaya çıkan ve gelecekte ekonomik fayda sağlayan varlıklar olarak tanımlanmaktadır (IFRS 9.4.1.1). Kripto varlıklar, herhangi bir sözleşmeye dayalı bir hak doğurmadığı için IFRS 9 kapsamında "finansal varlık" olarak değerlendirilemez (EY, 2023). Kripto paralar, hisse senedi, borç senedi veya nakit benzeri varlık kategorilerine de girmemektedir ve bu nedenle finansal tablolarda "finansal varlıklar" başlığı altında raporlanamaz.

IAS 38 Maddi Olmayan Duran Varlıklar Standardı kapsamında, maddi olmayan varlıklar, fiziksel varlığı bulunmayan, belirlenebilir ve şirkete gelecekte

ekonomik fayda sağlaması beklenen varlıklar olarak tanımlanmaktadır (IAS 38.8). Kripto varlıklar fiziksel bir varlığa sahip olmadıkları ve belirlenebilir oldukları için genellikle IAS 38 kapsamında maddi olmayan duran varlık olarak muhasebeleştirilmektedir (IFRS Foundation, 2023).

Eğer bir şirket kripto varlıkları ticaret amacıyla alıp satıyorsa, IAS 2 Stoklar Standardı kapsamında stok olarak da sınıflandırılabilmektedir (IAS 2.6). Bu durumda, kripto varlıklarını stok olarak sınıflandıran şirketler, maliyet veya gerçeğe uygun değer yöntemlerinden birini kullanarak raporlama yapmak zorundadır. Özellikle kripto para borsaları ve aracılık hizmetleri sunan şirketler, kripto varlıklarını stok olarak raporlamaktadır (Deloitte, 2023).

Tablo 1. Uluslararası Finansal Raporlama Standartları Uyarınca Kripto Varlıkların Sınıflandırılması

Kategori	IFRS Standardı	Kripto Paralar İçin Uygulanabilirlik
Nakit / Nakit Benzeri	IAS 32	Uygulanamaz (Kripto paralar yasal nakit değildir)
Finansal Varlık	IFRS 9	Uygulanamaz (Kripto paralar finansal sözleşmeye dayalı değildir)
Maddi Olmayan Duran Varlık	IAS 38	Genellikle uygulanır (Fiziksel varlığı yok)
Stok	IAS 2	Ticaret amaçlı tutulan kripto paralar için uygulanabilir

(Kaynak: IFRS Foundation, 2023; EY, 2023; Deloitte, 2023)

1.2 FASB/US GAAP ASU 2023-08 Kapsamında Kripto Varlıkların Sınıflandırılması

Finansal Muhasebe Standartları Kurulu (FASB), Genel Kabul Görmüş Muhasebe İlkeleri (US GAAP) kapsamında kripto varlıkların muhasebeleştirilmesiyle ilgili ilk resmi düzenlemeyi içeren ASU 2023-08'i yayımlamıştır (FASB, 2023). Bu güncelleme, kripto varlıkların gerçeğe uygun değer ölçüm modeliyle muhasebeleştirilmesini zorunlu hale getirmiştir. IFRS ve US GAAP arasında değer düşüklüğü ve yeniden değerleme modelleri açısından bazı farklılıklar oluşmuştur (PwC, 2023).

ASU 2023-08'e göre, Bitcoin, Ether, Litecoin gibi merkeziyetsiz dijital para birimleri doğrudan kripto varlıklar olarak tanımlanmaktadır. Bunun yanında, blokzincir tabanlı ve kriptografi ile güvence altına alınan diğer

tüm varlıklar "dijital varlıklar" olarak sınıflandırılmıştır. Bu kapsama giren varlıklar şunlardır:

- Stablecoin
- Menkul kıymet tokenları
- NFT'ler (Non-Fungible Tokens)
- Merkez Bankası Dijital Para Birimleri (CBDC'ler)

ASU 2023-08'e göre kripto varlıklar finansal tablolarda gerçeğe uygun değeriyle muhasebeleştirilmelidir. Bu, diğer maddi olmayan varlıklardan ayrı olarak raporlanmalarını gerektirir. Ayrıca, varlıkların gerçeğe uygun değer değişimlerinden kaynaklanan kazanç ve kayıplar doğrudan net gelire yansıtılmalıdır, yani şirketin karını doğrudan etkileyecek şekilde muhasebeleştirilmelidir (FASB, 2023).

1.3 IFRS ve US GAAP Kripto Varlıklara İlişkin Uygulama Farkları

Kripto varlıkların IFRS kapsamında özel bir düzenlemeye tabi olmaması, muhasebeleştirilme sürecinde çeşitli zorluklar doğurmaktadır. IASB, kripto muhasebesi için özel bir standart oluşturmayı hedeflememekte, bunun yerine genel maddi olmayan duran varlıklar standardı (IAS 38) kapsamında kripto varlıkları ele almayı planlamaktadır (IFRS Foundation, 2023). Bu eksiklik, IFRS kullanan şirketler için belirsizlik yaratmakta ve her şirketin farklı muhasebe politikaları benimsemesine yol açmaktadır.

Öte yandan, US GAAP kapsamında, FASB (2023) tarafından yayınlanan Subtopic 350-60 dijital varlıkların muhasebeleştirilmesini düzenlemekte olup, kripto varlıkların gerçeğe uygun değer farkı kâr veya zarara yansıtılarak ölçülmesini zorunlu kılmaktadır (FASB, 2023). IFRS kapsamında ise, bu varlıklar genellikle maliyet bedeli ile ölçülür ve IAS 38 (Maddi Olmayan Duran Varlıklar) veya IAS 2 (Stoklar) standartları uygulanır. Ayrıca, ASU 2023-08 esasları kapsamında, şirketlerin değer düşüklüğünü tersine çevirmesi mümkün hale getirilmiştir Ancak, Regulation G, Rule 100 kapsamında finansal tabloların yanıltıcı olmaması için değer düşüklüğünü bilançoda geri almak yasaktır.

Tablo 2. IFRS ve US GAAP Kripto Varlık Muhasebesi Farkları

Muhasebe Konusu	IFRS Muhasebe Standartları	US GAAP (ASU 2023-08 Sonrası)
Kapsam	IAS 38 (Maddi Olmayan Duran Varlıklar), IAS 2 (Stoklar)	Subtopic 350-60 altında özel çerçeve
İlk Değerleme	Tarihi maliyet, ancak aktif piyasa varsa gerçeğe uygun değerle yeniden değerleme yapılabilir	Tarihi maliyetle kaydedilir, ardından gerçeğe uygun değerle ölçülür
Sonraki Ölçüm	Tarihi maliyet - değer düşüklüğü (IAS 38), Stoklar için maliyet veya net gerçekleşebilir değer (IAS 2)	Her dönem gerçeğe uygun değer üzerinden yeniden ölçüm, farklar kar/zarara yansıtılır
Değer Düşüklüğü	Değer düşüklüğü tersine çevrilebilir (IAS 36)	Değer düşüklüğü kalıcıdır ve geri çevrilemez
Kripto Varlıklarla Mal ve Hizmet Satışı	Alındıkları tarihteki gerçeğe uygun değer ile ölçülür	Sözleşmenin başlatıldığı tarihteki gerçeğe uygun değerle ölçülür

Kaynak: IFRS Foundation (2023), FASB (2023), Grant Thornton (2023)

Kripto varlıkların finansal raporlamada nasıl sınıflandırılacağı konusunda uluslararası muhasebe standartlarında hala net bir düzenleme bulunmamaktadır (Alamsyah vd., 2024). Uluslararası Finansal Raporlama Standartları (IFRS) doğrudan kripto paralar için özel bir muhasebe standardı oluşturmasa da, 2019 yılında IFRS Yorumlama Komitesi tarafından yapılan değerlendirmelerde, kripto varlıkların mevcut IFRS standartları kapsamında nasıl sınıflandırılması gerektiğine dair yönlendirmeler sunulmuştur (IFRS Interpretations Committee, 2019). Bu bağlamda, kripto varlıkların "nakit" olarak değerlendirilemeyeceği, finansal varlık statüsüne sahip olmadığı ve genellikle maddi olmayan duran varlıklar veya stoklar kategorisinde sınıflandırılabileceği belirtilmiştir (IAS 38, IAS 2) (IFRS Foundation, 2023).

2. Kripto Varlıklar Kullanılarak Gerçekleştirilen Hileli İşlemler

Kripto varlıkların finansal dünyadaki yükselişi, muhasebe ve denetim süreçlerinde yeni zorluklar ortaya çıkarmıştır. Geleneksel finansal sistemlerde belirgin denetleyici mekanizmalar bulunurken, kripto varlıkların merkeziyetsiz ve anonim yapısı, muhasebe sahtekarlıklarını daha karmaşık hale getirmektedir (Haddad et al., 2024).

Kripto varlıkların finansal tablolarda nasıl raporlanacağına dair net muhasebe standartlarının olmaması, düzenleyici boşlukların suistimal edilmesine yol açmaktadır. Kripto varlıkların farklı sınıflandırılması, şirketlerin finansal tablolarını manipüle etmesine olanak sağlamaktadır (Akanbi, 2024).

Bu bağlamda, bazı şirketler ve bireyler, finansal tablolarda varlıklarını yanlış beyan etmek, vergi kaçırmak, gelirleri olduğundan fazla göstermek veya finansal durumlarını manipüle etmek için kripto varlıkları kullanmaktadır (Hossain, 2023). Ponzi şemaları, off-balance işlemler ve stablecoin manipülasyonları gibi yöntemlerle dolandırıcılık yapan kişi ve kurumlar, denetim süreçlerinden kaçmayı başarabilmektedir.

Kripto varlıklarla gerçekleştirilen muhasebe hileleri, genellikle geleneksel finansal dolandırıcılık yöntemlerinin dijital varlıklar aracılığıyla daha sofistike hale getirilmesiyle ortaya çıkmaktadır. Kripto varlıkların şeffaf olmayan muhasebeleştirme süreçleri, düzenleyiciler için büyük bir sorun teşkil etmektedir (Alamsyah vd., 2024)

2.1 Merkeziyetsiz Finans (DeFi) Üzerinden Gerçekleşen İşlemler

Merkeziyetsiz finans (DeFi), blok zinciri teknolojisini kullanarak finansal hizmetleri merkezi otoritelere bağlı olmadan sunan bir sistemdir. Geleneksel finans sistemlerinden farklı olarak, aracılar olmadan kredi, borçlanma, sigorta ve ticaret gibi hizmetler sağlanabilmektedir (Casino & Zarpala, 2021). DeFi, bankalar veya finansal kurumlar yerine blok zinciri tabanlı akıllı sözleşmeler kullanan Ethereum gibi platformlar üzerinde inşa edilmiştir ve şeffaf, sansüre dayanıklı bir finansal sistem sunmayı amaçlamaktadır (Scharmann, 2023).

Blok zinciri teknolojisi, verilerin değiştirilemez olmasını sağladığı için dolandırıcılık ve veri manipülasyonu riskini azaltmaktadır. Ancak, DeFi'nin henüz tam olarak düzenlenmemiş olması bazı hukuki sorunlara yol açmaktadır (Chiu, Chiu & Wang, 2022). Akıllı sözleşmeler genellikle açık kaynaklıdır ve kötü niyetli kişiler tarafından istismar edilebilmektedir. DeFi işlemleri büyük ölçüde akıllı sözleşmeler üzerine kurulu olsa da, bu sözleşmelerin yasal bağlayıcılığı belirsizdir (Barnes, 2018).

Geleneksel banka hesaplarından farklı olarak, DeFi cüzdanlarının merkezi bir otorite tarafından denetlenmemesi, bireylerin ve şirketlerin gelirlerini eksik beyan etmesine veya gelirlerini manipüle etmesine olanak tanımaktadır (Casino & Zarpala, 2021). Bu sistemin sunduğu anonimlik, şeffaflık eksiklikleri ve mevcut muhasebe standartlarıyla uyumsuzluk, muhasebe uygulamalarında ciddi sorunlara yol açmaktadır. DeFi işlemlerinin muhasebe sistemlerinde kolayca izlenememesi, muhasebe denetiminde ciddi boşluklar

yaratmaktadır. Blok zinciri teknolojisinin sunduğu şeffaflık teoride işlemleri takip etmeyi mümkün kılsa da, anonimlik ve takma ad kullanımı nedeniyle işlem sahiplerinin belirlenmesi oldukça zor olmaktadır (Benedetti, Nikbakht & Sarkar, 2021).

DeFi işlemlerinin vergilendirilmesi de oldukça karmaşıktır. Mevcut finansal sistemlerde vergi mükellefiyetleri açıkça belirlenirken, DeFi'nin sınır tanımayan yapısı nedeniyle ülkeler arası düzenlemeler farklılık göstermektedir (Cong, Harvey & Rabetti, 2025). Merkeziyetsiz yapının getirdiği gözetim eksikliği nedeniyle, DeFi platformlarında Ponzi şemaları gibi dolandırıcılık faaliyetleri yaygınlaşmaktadır. Bu da şirketlerin varlıklarını olduğundan fazla göstermesine olanak tanımaktadır (Scharmann, 2023).

Uluslararası düzenlemeler henüz DeFi işlemlerini doğrudan ele almamaktadır. Bu durum, şirketlerin kendi muhasebe politikalarını belirlemelerine ve potansiyel yanlış ve hileli raporlamalara yol açmaktadır (Rezaee & Wang, 2024). DeFi platformlarında likidite sağlayıcılar, bir nevi kredi veren gibi hareket etmektedir. Ancak bu tür işlemler, mevcut muhasebe sistemlerinde tam anlamıyla tanımlanmadığı için, varlık değerlemelerinde yanlışlıklar meydana gelmektedir (Casino & Zarpala, 2021).

2.2 Bilanço Dışı İşlemler ve Sahte Rezervler

Kripto varlıklar, geleneksel banka hesaplarından farklı olarak bilanço dışı tutulabilmekte ve düzenleyici kurumların gözetimi dışında saklanabilmektedir. Bu durum, şirketlerin sahip olmadıkları varlıkları finansal tablolarına ekleyerek bilançolarını manipüle etmelerine olanak tanımaktadır (Kanu, 2025). Bilanço dışı işlemler, denetim kurumlarının bu işlemleri tespit etmesini zorlaştırdığı için büyük bir finansal risk oluşturur.

Örneğin, 2022'de iflas eden FTX borsası, mali tablolarında sahip olmadığı rezervleri göstermek suretiyle bilanço dışı işlemler yaparak mali durumunu olduğundan güçlü göstermiştir Bu tür dolandırıcılıklar, işlemlerin blok zincir dışında (off-chain) yürütülmesi nedeniyle tespit edilmesini zorlaştırmaktadır (Haddad, Alharasis & Fraij, 2024).

2.2.1 Gerçekte Olmayan Kripto Varlıkların Finansal Tabloya Eklenmesi: Initial Coin Offering (ICO)

Kripto para piyasalarının hızla büyümesiyle birlikte, girişimciler için alternatif finansman modelleri ortaya çıkmıştır. Bu bağlamda, Initial Coin Offering (ICO), blok zinciri tabanlı projelerin fon toplamak için kullandığı yenilikçi bir finansman yöntemi olarak dikkat çekmektedir (Hornuf, Momtaz & Schwienbacher, 2022). ICO'lar, geleneksel halka arz (Initial

Public Offering - IPO) modeline benzer bir yapı sunsa da, merkeziyetsiz finans ekosisteminde yatırımcıları doğrudan projelere bağlayarak daha kolay ve hızlı bir finansman süreci sağlamaktadır (Deng vd., 2018). Bununla birlikte, ICO'ların düzenleyici eksiklikleri ve bilgi asimetrisi nedeniyle dolandırıcılıklar için uygun bir zemin hazırlaması da kaçınılmaz olmaktadır (Yousif vd., 2024).

ICO süreçleri, yeni geliştirilen bir kripto para birimi veya blok zinciri tabanlı bir projenin fonlanması amacıyla düzenlenmektedir. ICO'lar, geleneksel yatırım süreçlerine kıyasla daha az bürokratik engel barındıran, geniş bir yatırımcı kitlesine hitap eden ve merkeziyetsiz bir yapı sunan sistemlerdir. Blok zinciri teknolojisi, ICO'ların şeffaf ve güvenilir bir şekilde işlemesine olanak tanımakta, böylece yatırımcıların projeleri doğrudan desteklemelerini sağlamaktadır (Collomb vd., 2019).

Yatırımcılar, ICO aracılığıyla belirli bir fiyat karşılığında yeni oluşturulan tokenları satın almakta ve bu tokenlar da yatırımcılara projeye erken erişim sağlama avantajı sunmaktadır (Agarwal vd., 2024). Yatırımcılar açısından ICO'ların cazibesi, erken aşamada düşük maliyetle alınan tokenların ilerleyen süreçte değer kazanarak büyük kazanç fırsatları sunmasına dayanmaktadır. Ancak ICO'ların sunduğu avantajlar, bazı durumlarda kötüye kullanılmakta ve dolandırıcılık amaçlı ICO projeleri yatırımcıları mağdur etmektedir (Lecompte, 2024).

Son yıllarda, ICO projelerinin büyük bir kısmının vaat edilen projeleri gerçekleştirmede başarısız olduğu veya tamamen dolandırıcılık amaçlı oluşturulduğu tespit edilmiştir (Bai ve Zhang, 2025). ICO projelerinin çoğu ya var olmayan bir hizmet vaat etmekte ya da vaat edilen teknolojiyi geliştirmek için yeterli teknik kapasiteye sahip olmamaktadır (Bergesen & Palm, 2018). Bu projeler genellikle profesyonel görünümlü ancak sahte whitepaper'lar (beyaz kağıtlar), agresif pazarlama kampanyaları ve sahte sosyal medya hesapları aracılığıyla yatırımcıları çekmektedir (Hornuf et al., 2022).

Sahte ICO'ların en yaygın özelliklerinden biri, fon toplandıktan sonra ekip üyelerinin ortadan kaybolması ve projenin vaat edilen hizmetleri yerine getirmemesidir. Bunun yanı sıra, bazı şirketler ICO'lar aracılığıyla büyük miktarlarda fon toplarken, bu gelirleri finansal tablolarına gerçekte olmadığı halde dahil ederek bilançolarını güçlü göstermeye çalışmaktadır (Ho vd., 2022). Momtaz (2020) çalışmasında, ICO'lardan elde edildiği iddia edilen gelirlerin çoğu zaman şişirilmiş veya tamamen sahte olduğunu belirtmiştir. Hornuf ve diğerleri (2022) manipülasyonların, ICO gelirlerinin bilançolarda nakit varlık veya öz kaynak olarak gösterilerek şirketin piyasa değerinin

yapay olarak artırılması biçiminde gerçekleştiğini vurgulamaktadır. Şirketler, ICO fonlarını içsel işlemler yoluyla hareket ettirerek, nakit akışlarını sağlıklı gösterebilmektedirler (Agarwal vd., 2024). Ancak bu taktikler uzun vadede yatırımcı güveninin kaybolmasına ve piyasalarda ciddi çöküşlere yol açabilmektedir (Nghiem vd., 2021).

Sahte ICO'lar aynı zamanda düzenleyici kurumlar için büyük bir sorun teşkil etmektedir. Finansal tabloların doğruluğunu denetleyen kurumlar, ICO'lardan elde edilen fonların gerçek olup olmadığını belirlemekte zorlanmaktadır. Özellikle blok zinciri tabanlı varlıkların şeffaf olmaması ve birçok ICO'nun offshore merkezler üzerinden yürütülmesi, düzenleyici kontrolleri zorlaştırmaktadır (Robusti vd., 2025). SEC (ABD Menkul Kıymetler ve Borsa Komisyonu), sahte ICO'ları ifşa etmek amacıyla kendi sahte ICO'sunu oluşturarak yatırımcıları bilinçlendirme yoluna gitmiştir (Cong, Li & Tang, 2018).

Piyasalardaki bilgi asimetrisi nedeniyle yatırımcılar, ICO projelerinin finansal sağlamlığını değerlendirmekte zorlanmaktadır. Aynı zamanda, whitepaper'larda sunulan teknik detayların karmaşıklığı, yatırımcıların sahte projeleri fark etmelerini güçleştirmektedir (Bellavitis vd., 2021). Bai ve Zhang (2025) tarafından yapılan bir çalışma, sahte ICO projelerinin sosyal medya manipülasyonu yoluyla yatırımcıları yanılttığını ortaya koymuştur. Aquilina vd. (2024) ise düzenleyici kurumların manipülasyonların önüne geçebilmesi için daha sıkı kontrol mekanizmaları geliştirmesi gerektiğini savunmaktadır. Deng vd. (2018) çalışmaları, yatırımcıların korunması adına akıllı sözleşmeler kullanılarak fonların belirli aşamalarda serbest bırakılmasının sağlanabileceğini önermektedir.

2.2.2 Off-Chain İşlemler Kullanılarak Rezerv Şişirme

Kripto para piyasalarının büyümesiyle birlikte finansal işlemler yeni ve çeşitli biçimlerde gerçekleşmeye başlamıştır. Bu bağlamda, kripto varlık işlemleri On-Chain ve Off-Chain olmak üzere iki temel gruba ayrılmaktadır. On-Chain işlemler, blokzincir ağı üzerinde kayıt altına alınan, şeffaf, değiştirilemez ve merkeziyetsiz bir şekilde gerçekleşen işlemleri ifade ederken, Off-Chain işlemler, blokzincir dışında, merkezi borsalar, tezgah üstü (OTC) piyasalar veya özel anlaşmalar yoluyla yürütülen işlemleri kapsamaktadır (Zetzsche vd., 2020; Nghiem vd., 2021).

Off-Chain işlemler, blokzincir kayıt sisteminin dışında gerçekleştiği için belirli avantajlar sunmaktadır. Öncelikle, bu işlemler daha hızlı ve düşük işlem ücretleri ile gerçekleştirilebilen işlemler olarak karşımıza çıkmaktadır. Diğer taraftan, Off-Chain işlemler düzenleyici denetim mekanizmalarından

kaçmayı kolaylaştırmakta ve bu nedenle vergi kaçırma, kara para aklama ve finansal manipülasyon risklerini de artırmaktadır (Koc., 2024; Banaei, 2023).

Blokzincir teknolojisi, şeffaf ve değiştirilemez işlem kayıtları sunarak finansal işlemleri güvence altına alırken, Off-Chain işlemler bu sistemin dışında gerçekleşerek geleneksel finans piyasalarındaki merkezi yapılarla benzerlik göstermektedir (Zetzsche vd., 2020; Abdulhakeem ve Hu, 2021). Off-Chain işlemler, merkezi borsalar (CEX'ler), özel anlaşmalar (P2P işlemler) ve OTC piyasalar aracılığıyla yürütülebilir (Eberhardt ve Tai, 2017; Ferris et al., 2024).

Off-Chain İşlemlerin Temel Özellikleri

- Blokzincir Kaydı İçermemesi: İşlemler, blokzincir ağında yer almadığı için merkezi kurumlar tarafından düzenlenmeyebilir.
- Hız ve Düşük Maliyet: İşlemler madenci ücretleri gerektirmediğinden hızlı ve düşük maliyetlidir.
- Düzenleyici Denetimlerin Dışında Kalabilmesi: Vergi kaçırma ve muhasebe manipülasyonu için kullanılabilmektedir.
- Finansal Raporlamada Belirsizlik: Mevcut muhasebe standartları, Off-Chain işlemleri tam olarak kapsayamamaktadır (Akanbi, 2024; Dashkevich vd., 2024).

Bu özellikler nedeniyle Off-Chain işlemler, finansal tablolarda muhasebe hileleri ve varlık manipülasyonları yapmak isteyen şirketler için bir fırsat alanı yaratmaktadır (Azgad-Tromer, 2018; Ferreira, 2024).

2.3 Ponzi ve Piramit Şemaları

Ponzi ve piramit şemaları, finansal dolandırıcılığın en yaygın ve en yıkıcı türleri arasında yer almaktadır. Ponzi şeması, yeni yatırımcılardan gelen paranın eski yatırımcılara ödeme yapmak için kullanıldığı bir finansal dolandırıcılık modelidir (Carey ve Webb, 2017). Piramit şemaları ise yatırımcıların sisteme yeni yatırımcıları dahil etmelerini gerektiren ve gelir akışının sürekli olarak yeni katılımcılar tarafından sağlandığı sistemlerdir (Bosley ve Knorr, 2018).

Ponzi şemaları, adını 1920'lerde sahte bir yatırım planı işleten Charles Ponzi'den almıştır. Yatırımcılara yüksek ve garantili getiri vaat edilmekte, ancak yatırımlar genellikle var olmamaktadır. Yeni yatırımcılardan elde edilen fonlar, eski yatırımcılara ödeme yapmak için kullanılmakta ve sistem, yeni yatırımcı girişleri durduğunda çökmektedir (Hock ve Button, 2023).

Piramit şemaları ise Ponzi sistemlerine benzer bir yapıdadır, ancak temel fark, her yatırımcının daha fazla yatırımcı getirmesi gerektiği bir modele dayanmasıdır. Burada kazanç, yatırılan paradan ziyade sisteme yeni katılanların sağladığı girişlerden elde edilmektedir. Ponzi şemalarına kıyasla, piramit şemaları daha geniş katılımcı ağlarına ve doğrudan satış mekanizmalarına sahiptir (Maurushat ve Halpin, 2020).

Her iki model de yatırımcıları büyük kayıplara uğratırken, finansal piyasaların güvenilirliğini de ciddi şekilde zedelemektedir. Özellikle muhasebe hileleriyle birleştiğinde, bu dolandırıcılık sistemleri mali tabloların manipüle edilmesi, gelirlerin yanlış raporlanması ve yatırımcıların yanıltılması gibi büyük riskler yaratmaktadır (Carey ve Webb, 2017).

Ponzi ve piramit şemaları, yatırımcıların sisteme para yatırmaları karşılığında yüksek getiri vaat edilen dolandırıcılık türleridir (Henriques, 2018). İki sistem arasındaki temel farklar şu şekildedir:

i. Ponzi şemasında, katılımcılar sisteme yatırım yapar, ancak yeni yatırımcıları dahil etme zorunluluğu yoktur. Eski yatırımcılar, yeni gelenlerin yatırımlarıyla finanse edilir.

ii. Piramit şemasında, yeni üyeler, sisteme dahil olmak için bir ücret öder ve kazanç sağlamak için yeni katılımcılar getirmek zorundadır.

Ponzi ve piramit şemalarının temel özelliklerinden aşağıdaki biçimde söz edebilmek mümkündür:

i. İlk yatırımcılar genellikle kâr elde ederken, sistemin sonunda yer alanlar zarar etmektedir.

ii. Sürdürülebilir değildir, çünkü sistemin genişlemesi sonsuza kadar devam edemez.

iii. Yatırımcılar, yasal olarak korunmadıkları için dolandırıcılığa maruz kalabilmektedir.

Ponzi şemalarında dolandırıcılar, yatırımcılara güven vermek için mali tabloları manipüle ederek sistemin sağlıklı işlediği izlenimini vermeye çalışırlar (Carey ve Webb, 2017; Giroux, 2017). Ponzi sistemleri, yatırımcıları çekebilmek için finansal raporlarda sürekli büyüme gösterir. Şirketler, kâr marjlarını yüksek göstererek yatırımcı ilgisini artırır, ancak bu kazançlar genellikle gerçekçi değildir. Bernie Madoff'un Ponzi şeması, yatırımcılara sürekli kâr raporlayan ancak gerçekte hiçbir işlem yapmayan bir yatırım fonu olarak faaliyet göstermiştir (Modesta Amaka ve Chindengwike, 2024). Yapay kazanç raporları, yatırımcıları cezbetmek için kullanılır (Maurushat ve Halpin, 2020).

Ponzi şemaları, şirketlerin finansal sağlamlığını göstermek için sahte rezervler oluşturmasına neden olabilir. Yatırımcılara yüksek rezerv gösteren düzmece mali tablolar hazırlanırken, gerçekte rezervlerin büyük ölçüde eksik olduğu gözlemlenmektedir (Hossain, 2023). Ponzi sistemleri, borçlarını yatırımcılarından gizleyerek bilanço hileleri yapabilir. Uzun vadeli yükümlülükler, mali tablolarda gösterilmeyerek şirketin olduğundan daha sağlıklı görünmesi sağlanır (Bosley ve Knorr, 2018). Yeni yatırımcı fonları bilanço dışı hesaplara aktarılabilir ve yükümlülükler bu şekilde gizlenebilir (Hock ve Button, 2023).

Ponzi ve piramit sistemleri, yalnızca bireysel yatırımcıları değil, tüm finansal piyasaları da olumsuz etkileyebilmektedir (Giroux, 2017; Moskovicz, 2020; Carey ve Webb, 2017).

2.4 Gidiş-Dönüş Ticareti (Wash Trading)

Finansal piyasalarda manipülasyon yöntemlerinden biri olan gidiş-dönüş ticareti (wash trading), yatırımcıları ve düzenleyicileri yanıltmak amacıyla gerçekleştirilen sahte ticaret işlemlerini ifade etmektedir (Bellavitis vd., 2021). Gidiş-dönüş ticareti, finansal varlıkların alım ve satım işlemlerinin yapay olarak artırılması sürecidir ve hisse senetleri, NFT'ler, emtia piyasaları ve kripto para piyasalarında yaygın olarak uygulanmaktadır (Ho vd., 2022; Alexander ve Cumming, 2020). Bu yöntemde, alıcı ve satıcının aynı kişi veya iş birliği içinde olduğu hesaplar olması nedeniyle gerçek bir mülkiyet transferi gerçekleşmemektedir.

Gidiş-dönüş ticareti genellikle iki ana yöntemle gerçekleştirilmektedir (Gan vd., 2024; Bellavitis vd., 2021):

i. Kendi Kendine İşlem Yapma (Self-Trading): Aynı kişi veya kuruluş, aynı varlığı defalarca kendi hesapları arasında alıp satarak işlem hacmini yapay olarak şişirmektedir (von Wachter vd., 2022).

ii. Koordineli İşlemler (Collusive Trading): Birden fazla yatırımcı veya kuruluş, işlem hacmini artırmak ve piyasayı manipüle etmek için organize bir şekilde alım satım yapmaktadır (Bellavitis vd., 2021).

Geleneksel finans piyasalarında gidiş-dönüş ticareti yasadışı olarak kabul edilse de, kripto para piyasaları gibi yetersiz denetlenen alanlarda oldukça yaygın olarak uygulandığı bilinmektedir (Ho vd., 202; Alexander ve Cumming, 2020).

Şirketler, yatırımcı ilgisini çekmek ve piyasa değerlerini artırmak amacıyla sahte işlem hacimleri yaratarak gelirlerini yapay olarak artırabilmektedirler (Aloosh ve Li, 2024; Gan vd., 2024). Özellikle kripto para piyasalarında,

bazı şirketler ve projeler, piyasada yüksek talep varmış gibi bir algı yaratmak için kendi hesapları arasında aynı varlığı defalarca alıp satmaktadırlar (Gan vd., 2024). Yatırımcılar, bu hareketi piyasada yüksek talep olarak algılamakta ve sonuç olarak varlık fiyatları yükselmektedir (Oh, 2024). Bu durum, finansal raporlarda gidiş-dönüş ticaretinden gelen yapay kazançların gerçek gelir olarak gösterilmesine neden olabilir (Bellavitis vd., 2021).

Şirketler, gidiş-dönüş ticareti uygulamalarıyla hisse senedi fiyatlarını ve kripto varlıklarının değerlerini yapay olarak artırabilir (Seifert & Van Linden, 2024). Bu sayede, şirket yöneticileri insider trading yaparak, hisse fiyatları en yüksek seviyeye ulaştığında satış yapabilirler (Agrawal & Cooper, 2015). Yeni halka arz edilen şirketler ve kripto projeleri, ilk aşamalarda fiyatları yapay olarak artırmak için gidiş-dönüş ticareti işlemlerinden faydalanabilmektedir (Alexander ve Cumming, 2020). Bu tür manipülasyonlar fark edildiğinde, yatırımcılar büyük kayıplar yaşayabilmektedir (Eigelshoven vd., 2021).

Gidiş-dönüş ticareti vergi kaçırma amacıyla da kullanılabilmektedir. Şirketler, aynı varlığı farklı hesaplar arasında zarar edecek şekilde alıp satarak yapay zararlar yaratabilmekte ve vergi yükümlülüklerini düşürebilmektedir (von Wachter vd., 2022).

Offshore hesaplar ve vergi cennetleri aracılığıyla yürütülen işlemler, şirketlerin vergi yükümlülüğünü azaltmasına olanak tanımaktadır (Marian, 2013).

İşlemler merkezi olmayan finans (DeFi) platformlarında yapıldığında izlenmesi daha da zor hale gelmektedir (Uzougbo vd., 2024).

Bir varlık değer kazandığında, şirket o varlığı değer kaybetmiş gibi göstererek sermaye kazancı vergisini minimize edebilir (Agrawal & Cooper, 2015).

Kripto para piyasalarında, yatırımcılar yıl sonuna doğru zarar göstererek vergi yükümlülüklerini azaltmak için gidiş-dönüş ticareti uygulamalarına başvurabilmektedirler (Alexander ve Cumming, 2020).

2.5 Stablecoin Manipülasyonu ve Sahte Likidite

Stablecoin'ler, itibari para birimleri, emtialar veya algoritmik mekanizmalara sabitlenen ve kripto piyasalarında fiyat istikrarı sağlamak amacıyla kullanılan bir kripto varlık türüdür. Bitcoin ve Ethereum gibi volatil kripto paralardan farklı olarak, stablecoin'ler istikrarlı fiyat yapıları sayesinde ödeme sistemleri, ticaret ve merkeziyetsiz finans (DeFi) uygulamalarında yaygın olarak kullanılmaktadır (Lipton et al., 2020). Stablecoin, geleneksel finans ile blokzincir tabanlı ekonomiler arasındaki boşluğu kapatarak

likiditeyi artırmakta, volatiliteyi azaltmakta ve dünya çapında kesintisiz işlemler sağlamaktadır (Kirkpatrick et al., 2021).

Ancak, stablecoin piyasası, finansal manipülasyonlar ve muhasebe hileleri açısından ciddi riskler barındırmaktadır. Desteksiz stablecoin ihraç eden bazı kuruluşlar, finansal tablolarında olmayan varlıkları göstermekte ve kullanıcı güvenini suistimal etmektedir (Cumming et al., 2019). Örneğin, Tether (USDT) rezervlerinin tam olarak desteklenmediği iddiaları, stablecoin manipülasyonlarının büyük finansal çöküşlere yol açabileceğini ortaya koymaktadır (Eigelshoven et al., 2021).

Stablecoin'ler, destek mekanizmalarına bağlı olarak üç ana kategoride değerlendirilmektedir:

i. İtibari Para Destekli Stablecoin'ler

Bu tür stablecoin'ler, ABD Doları (USD), Euro (EUR) veya diğer itibari para birimlerine birebir oranında sabitlenmektedir. Genellikle bir emanetçi tarafından banka hesaplarında tutulan nakit veya eşdeğer rezervlerle desteklenmektedir (Resende Franco, 2022). Önde gelen itibari para destekli stablecoinler arasında Tether (USDT), USD Coin (USDC) ve Binance USD (BUSD) bulunmaktadır. Ancak, bu stablecoin'lerin merkezi bir yapıya sahip olması, kullanıcıların üçüncü taraf emanetçilere güvenmesini gerektirmektedir. Düzenleyiciler, stablecoin ihraççılarının finansal mevzuatlara uygun hareket ettiğinden emin olmak için denetimleri artırmaktadır (Kochergin, 2020).

ii. Kripto Destekli Stablecoin'ler

Bu stablecoin'ler, itibari para yerine diğer kripto varlıklar tarafından teminatlandırılmaktadır. Teminatlar akıllı sözleşmelerde saklanır ve piyasa koşullarına bağlı olarak otomatik olarak ayarlanır (Lyons & Viswanath-Natraj, 2023). DAI (MakerDAO) ve Synthetix USD, en yaygın kullanılan kripto destekli stablecoin'ler arasındadır. Bu sistemin avantajı, merkeziyetsiz yapısı nedeniyle geleneksel finansal kurumlara bağımlı olmamasıdır. Ancak, stablecoin değerinin korunabilmesi için varlıkların %150 veya daha fazlası teminat olarak yatırılması gerekmektedir. Teminat varlıklarının değer kaybetmesi durumunda stablecoin dengesiz hale gelebilir (Soba-ski et al., 2022).

iii. Algoritmik Stablecoin'ler

Bu stablecoin'ler, itibari para veya kripto varlık rezervlerine dayanmak yerine, arz ve talebi otomatik olarak ayarlayan akıllı sözleşmelere güvenir (Echelpoel et al., 2020). TerraUSD (UST) ve Ampleforth

(AMPL) en bilinen algoritmik stablecoin'ler arasındadır. Algoritmik stablecoin'ler geleneksel rezervlere ihtiyaç duymaz; ancak, sistemin sürdürülebilirliği doğrudan algoritmanın başarısına bağlıdır. Algoritma başarısız olursa, stablecoin değeri çökebilir. Örneğin, TerraUSD'nin çöküşü, algoritmik stablecoin'lerin finansal sistem için büyük riskler oluşturduğunu göstermiştir (MacDonald & Zhao, 2022).

Stablecoin'ler, finansal raporlamada yapılan muhasebe hileleriyle doğrudan bağlantılıdır. Şirketler, stablecoin rezervlerini finansal tablolarında olduğundan farklı gösterebilmekte, gerçekte sahip olmadıkları varlıkları kaydedebilmekte veya stablecoin ihraç ederek yapay piyasa değerleri oluşturabilmektedirler.

Stablecoin ihraç eden bazı kuruluşlar, rezervlerini tam olarak desteklemeden büyük miktarda stablecoin çıkararak yatırımcıları yanıltmaktadır. Örneğin, Tether'in rezervleriyle ilgili şeffaflık sorunları yıllardır tartışılmaktadır (Geva ve Muraj, 2021). Rezervlerin gerçekte var olup olmadığının belirsizliği, stablecoin piyasasında büyük bir güven eksikliği yaratmaktadır.

Stablecoin ihraç eden şirketler, rezervlerini olduğundan fazla göstererek bilançolarını güçlendirebilir. Özellikle merkeziyetsiz finans (DeFi) platformları, stablecoin'leri teminat göstererek kredi alabilir ve finansal tablolarda aldıkları bu borçları gizleyebilmektedirler (Alamsyah vd., 2024).

Şirketler, stablecoin'leri kullanarak piyasa manipülasyonu yapabilirler. Özellikle USDT gibi stablecoin'lerin borsa manipülasyonlarında kullanıldığı iddia edilmektedir (Trozze et al., 2023). Gidiş-dönüş ticareti (wash trading) gibi yöntemler ile stablecoin hacimleri şişirilerek piyasalarda yapay bir likidite yaratılmaktadır.

Stablecoin'ler, şirketlerin muhasebe kayıtlarını manipüle ederek vergi kaçırmalarına olanak tanımaktadır. Şirketler, stablecoin işlemlerini bilanço dışı tutarak vergi yükümlülüklerinden kaçınabilir . Örneğin, stablecoin'lerin offshore hesaplara taşınması ve kayıt dışı işlemler için kullanılması, denetim süreçlerini zorlaştırmaktadır.

2.6 Kara Para Aklama

Kripto varlıklar, finansal sistemde devrim yaratırken, aynı zamanda yasa dışı faaliyetler için bir araç olarak da kullanılmaktadır. Kara para aklama faaliyetleri, dijital varlıkların merkeziyetsiz ve izlenmesi zor yapısından faydalanarak yasa dışı fonların sisteme kolayca entegre edilmesini sağlamaktadır (Longa, 2025). Kripto varlıkların sağladığı anonimlik,

suç gelirlerinin finansal sistemde iz bırakmadan dolaşmasına da olanak tanımaktadır (Carletti vd., 2024).

Finansal tablolar üzerindeki etkileri bağlamında, kripto varlıklar aracılığıyla yapılan kara para aklama işlemleri muhasebe kayıtlarının manipülasyonuna, finansal raporların yanıltıcı hale gelmesine ve düzenleyici kurumların denetim süreçlerini zorlaştırmasına neden olmaktadır (Yousif et al., 2024).

Kara para aklama, yasa dışı yollarla elde edilen fonların yasal finansal sisteme entegre edilerek kaynağının gizlenmesini amaçlayan bir süreçtir. Kripto varlıklar, bu sürecin her aşamasında kullanılabilmektedir:

i. Yerleştirme (Placement): Yasa dışı elde edilen fonlar, kripto varlıklara dönüştürülerek finansal sisteme sokulur (Longa, 2025).

ii. Katmanlaştırma (Layering): Kripto cüzdanlar arasında yapılan birden fazla transfer ile izlerin kaybolması sağlanır (Calafos ve Dimitoglou, 2022).

iii. Entegrasyon (Integration): Kara para, yasal finansal varlıklar gibi gösterilerek finansal sisteme entegre edilir (Yousif et al., 2024).

Blokzincir teknolojisinin sağladığı izlenebilirlik, geleneksel bankacılığa kıyasla daha fazla şeffaflık sunsa da, kripto varlıkların doğasında bulunan merkeziyetsizlik, denetleyici kurumlar için büyük bir zorluk oluşturmaktadır (Verma, 2024).

Kripto varlıklar aracılığıyla gerçekleştirilen kara para aklama, şirketlerin ve finansal kuruluşların finansal tablolarında çeşitli manipülasyonlara yol açabilmektedir. Bu etkiler şu şekilde sıralanabilir:

Kripto varlıklar kullanılarak yapılan sahte işlemler, şirketlerin gelirlerini yapay olarak artırmalarına ve finansal tablolarında gerçek dışı kâr göstermelerine neden olmaktadır (Leuprecht vd., 2023). Özellikle merkeziyetsiz borsalar (DEX), sahte işlemlerle hacim şişirme (gidiş-dönüş ticareti) yoluyla finansal raporları manipüle etmektedir (Hou, 2024).

Şirketler, sahip olmadıkları kripto varlıkları bilançolarına dahil ederek finansal sağlamlıklarını olduğundan daha iyi gösterebilirler (Sheikh, 2024). Örneğin, bazı şirketler, likidite krizlerine rağmen sahip olduklarını iddia ettikleri stablecoin rezervlerini olduğundan fazla göstererek piyasaya yanlış sinyaller vermektedirler (MacDonald ve Zhao, 2022).

Kripto varlıklar, bilanço dışı işlemler için kullanılabilmekte ve yükümlülüklerin gizlenmesini sağlayabilmektedir (Verma, 2024). Örneğin,

bir şirket, gerçekte borçlu olduğu miktarı kripto varlıklarla yapılan içsel işlemlerle dış finansal kayıtlardan gizleyebilir (Sheikh, 2024).

Kripto varlıklarla yapılan işlemler, düzenleyici denetimlerden kaçınmayı kolaylaştırdığı için vergi kaçırma amaçlı kullanılabilmektedir (Azgad-Tromer, 2018). Özellikle offshore borsalarda yapılan işlemler, vergi otoritelerinin takibinden kaçırılarak şirketlerin daha düşük vergi ödemesine neden olmaktadır.

Düzenleyici otoriteler, kripto varlıklarla gerçekleştirilen kara para aklama faaliyetlerini engellemekte zorlanmaktadır. Bunun başlıca sebepleri şu şekilde sıralanabilir:

i. Merkeziyetsizlik: Geleneksel finans sisteminde banka denetimleri aracılığıyla takip edilen işlemler, merkeziyetsiz finans sistemlerinde doğrudan kontrol edilememektedir (Salami, 2021).

ii. Anonim İşlemler: Bazı kripto cüzdanları, kimlik doğrulaması gerektirmediği için suç gelirlerinin anonim bir şekilde taşınmasına olanak sağlamaktadır (Yousif et al., 2024).

iii. Zincir Üzerinde (On-Chain) ve Zincir Dışı (Off-Chain) İşlemler: Kripto varlıklar, zincir dışı işlemlerle manipüle edilerek finansal tabloları yanıltıcı hale getirebilmektedir.

Bu zorluklar nedeniyle, finansal denetim kurumları, blockchain tabanlı denetim araçlarını daha etkin hale getirmeye çalışmaktadır (Bakhshi ve Ghita, 2021).

3. Adli Muhasebe ve Blokzincir Analitiği

Blokzincir tabanlı finansal işlemler, muhasebe denetimi ve dolandırıcılıkla mücadelede devrim yaratmıştır. Kripto varlıkların merkeziyetsiz yapısı ve işlemlerin değiştirilemez niteliği, adli muhasebe süreçlerinde hem fırsatlar hem de zorluklar yaratmaktadır (Morshed Khrais, 2025,; Vijayalakshmi ve Jeevan, 2024). Blokzincir analitiği, suç gelirlerinin izlenmesi ve yasa dışı fon akışlarının tespiti açısından önemli bir araç olarak değerlendirilmektedir (Djeffal ve Khaldi, 2024).

Geleneksel muhasebe denetim süreçlerinden farklı olarak blokzincir üzerindeki işlemler şeffaf ve denetlenebilir olmasına rağmen, anonimlik, off-chain işlemler, kimlik gizleme teknikleri ve merkeziyetsiz finans (DeFi) protokolleri suçluların izlerini gizlemelerine olanak tanımaktadır (Eghe-Ikhurhe, Roni ve Bonsu, 2024; El-Kady vd., 2025). Bu nedenle, veri analitiği, yapay zeka destekli izleme sistemleri ve blokzincir analiz araçları,

adli muhasebecilerin ve düzenleyicilerin dolandırıcılık faaliyetlerini tespit etmesi açısından kritik bir rol oynamaktadır (Ferris vd., 2024).

Blokzincir, dağıtık defter teknolojisi (DLT) sayesinde işlemlerin değiştirilemez ve şeffaf bir şekilde kaydedilmesini sağlayarak muhasebe denetimini daha güvenilir hale getirmektedir (Bello vd., 2024; El-Kady vd., 2025). Ancak, gizlilik odaklı kripto varlıklar (örneğin Monero ve Zcash), karışık cüzdan (mixing/tumbling) sistemleri ve akıllı kontratlar, dolandırıcılık tespitini zorlaştırmaktadır (Eghe-Ikhurhe vd., 2024).

Özellikle merkezi borsalar dışında gerçekleşen peer-to-peer (P2P) işlemler ve off-chain kayıtlar, düzenleyicilerin ve adli muhasebecilerin kripto varlık hareketlerini izlemesini kısıtlamaktadır (Makarenkov ve Kosa, 2024). Bu sebeple, blokzincir teknolojisi kullanılarak anomali tespiti, sahte işlemlerin belirlenmesi ve dolandırıcılık şemalarının deşifre edilmesi kritik hale gelmiştir (Hassan vd., 2022).

Adli muhasebeciler, blokzincir üzerindeki işlem hareketlerini inceleyerek finansal suçları ortaya çıkarmak için gelişmiş analiz araçlarından faydalanmaktadır. Bu araçlar, zincir içi (on-chain) ve zincir dışı (off-chain) verileri birleştirerek dolandırıcılık faaliyetlerinin tespit edilmesine yardımcı olmaktadır (Oladejo ve Jack, 2020; Djeffal ve Khaldi, 2024). En yaygın kullanılan blokzincir analiz araçları şunlardır:

i. Chainalysis – Kripto para işlemlerini izleme, cüzdan analizi yapma ve yasa dışı fon akışlarını belirleme.

ii. Elliptic – Kara para aklama ve dolandırıcılık faaliyetlerini tespit etmek için yapay zeka destekli analiz sistemleri.

iii. CipherTrace – Bankalar ve düzenleyiciler için risk yönetimi ve finansal suç analizleri.

iv. TRM Labs – Blokzincir analizleri ve risk değerlendirme süreçlerinde kullanılan bir denetim aracı.

v. GraphSense – Blokzincir üzerindeki işlem ilişkilerini ve cüzdan hareketlerini analiz eden bir platform.

Bu analiz araçları, şüpheli cüzdanları ve işlemleri izlemek, yasa dışı faaliyetleri tespit etmek ve dolandırıcılık ağlarını haritalandırmak için kullanılmaktadır (Bello vd., 2024; Oladejo ve Jack, 2020) Kripto tabanlı finansal suçların tespiti için adli muhasebeciler tarafından kullanılan yöntemler aşağıda sıralanmıştır:

i. Anomali Tespiti ve Veri Analitiği: Büyük veri analitiği ile normal işlem kalıplarından sapmaların belirlenmesi, şüpheli işlemlerin ortaya çıkarılmasını sağlar (Eghe-Ikhurhe vd., 2024).

ii. Makine Öğrenmesi Destekli Dolandırıcılık Tespiti: Yapay zeka algoritmaları, şüpheli işlem hareketlerini belirleyerek dolandırıcılığı önceden tespit etmeye yardımcı olur (Alexander ve Cumming, 2020).

iii. Cüzdan Takip ve Kimliklendirme: Şüpheli cüzdan adreslerinin izlenmesi ve yasa dışı işlemlerle bağlantılarının belirlenmesi, dolandırıcılık ağlarının haritalandırılmasını kolaylaştırır (Makarenkov ve Kosa, 2024).

iv. Zincir Dışı (Off-Chain) Verilerin Analizi: Kripto para işlemleri sadece blokzincir üzerinde gerçekleşmediği için, merkezi borsa kayıtları, banka hesapları ve sosyal medya verileri gibi ek kaynaklar incelenmelidir (Djeffal ve Khaldi, 2024).

Blokzincir teknolojisi, finansal işlemlerin güvenli, şeffaf ve değiştirilemez bir yapıda kaydedilmesini sağlayarak muhasebe sistemlerinde önemli bir dönüşüm yaratmıştır. Özellikle finansal denetim ve adli muhasebe alanlarında, blokzincir tabanlı sistemler, dolandırıcılığın tespiti ve önlenmesi açısından büyük bir potansiyele sahiptir (Haddad vd., 2024). Ancak, kripto varlıklarla ilgili işlemlerin doğası gereği anonim olması, sahte işlemler ve yasadışı faaliyetlerin izlenmesini zorlaştırmaktadır (Djeffal ve Khaldi, 2024).

Blokzincir tabanlı muhasebe sistemleri, dağıtık defter teknolojisi (DLT) sayesinde işlemleri değiştirilemez ve izlenebilir hale getirerek, muhasebe denetimlerinde önemli bir yenilik sunmaktadır. Ancak, bu sistemlerin sunduğu şeffaflığa rağmen, suçluların kimliklerini gizlemek için çeşitli tekniklerden faydalandıkları görülmektedir (Makarenkov ve Kosa, 2024). Bu bağlamda, blokzincir tabanlı muhasebe sistemlerinin dolandırıcılıkla mücadelede karşılaştığı başlıca sınırlamalar aşağıda ele alınmaktadır.

i. **Anonimlik ve Gizlilik Odaklı Coin'ler**

Kripto varlıkların anonimlik sağlaması, finansal işlemlerin şeffaflığını ve izlenebilirliğini ciddi şekilde sınırlamaktadır. Özellikle gizlilik odaklı coin'ler (örneğin Monero ve Dash), işlem detaylarını şifreleyerek, kullanıcıların izlenmesini zorlaştırmaktadır (Bello vd., 2024). Bu durum, yasa dışı faaliyetlerin tespitini güçleştirirken, geleneksel finansal izleme mekanizmalarının etkinliğini azaltmaktadır (Wronka, 2023).

Blokzincir analiz araçları (örneğin Chainalysis, Elliptic ve CipherTrace) kullanılarak bazı anonimlik sağlayan işlemler tespit edilebilse de, bu araçlar tüm gizlilik odaklı kripto varlıkları izleyememektedir (Oladejo ve Jack, 2020).

ii. **2. Off Chain İşlemler**

Blokzincir üzerindeki işlemler değiştirilemez ve izlenebilir olsa da, off-chain olarak gerçekleşen işlemler blokzincirin sunduğu şeffaflık avantajını ortadan kaldırmaktadır. Merkezi borsalar, özel anlaşmalar ve fiziksel varlık alımları gibi off-chain işlemler, suçluların kara para aklama süreçlerini blokzincir dışına taşımasına olanak sağlamaktadır (Eghe-Ikhurhe vd., 2024).

Örneğin, bir kişi kripto varlıklarını merkezi bir borsaya aktardıktan sonra itibari paraya çevirerek işlemi blokzincir dışına çıkarabilir. Bu durum, blokzincir tabanlı denetim mekanizmalarının yetersiz kalmasına ve denetim süreçlerinde eksikliklere yol açmaktadır (Makarenkov ve Kosa, 2024).

iii. **Uluslararası Düzenlemelerdeki Farklılıklar**

Kripto varlıklarla ilgili düzenleyici çerçeveler ülkeden ülkeye büyük farklılıklar göstermektedir. Bazı ülkeler kripto varlık işlemlerini sıkı bir şekilde düzenlerken, diğerleri daha gevşek bir yaklaşım benimsemektedir (Djeffal ve Khaldi, 2024). Bu durum, sınır ötesi dolandırıcılık faaliyetlerinin artmasına ve suçluların düzenleyici boşluklardan faydalanmasına yol açmaktadır.

Özellikle merkeziyetsiz finans (DeFi) protokolleri, uluslararası denetim mekanizmalarından kaçınmak isteyen suçlular için bir çıkış noktası olarak değerlendirilmektedir (Vijayalakshmi ve Jeevan, 2024). Uluslararası iş birliklerinin ve veri paylaşımının artırılması, sınır ötesi dolandırıcılık faaliyetleriyle mücadelede önemli bir adım olabilir (Haddad vd. 2024).

4. Değerlendirme ve Öneriler

Kripto varlıklar, finansal sistemlerde önemli yenilikler sunarken, aynı zamanda muhasebe hileleri ve finansal manipülasyonlar için yeni fırsatlar yaratmaktadır. Blokzincir teknolojisinin sunduğu merkeziyetsizlik, anonimlik ve sınır ötesi işlem yapabilme olanakları, kripto varlıkları dolandırıcılık, kara para aklama ve finansal tablo manipülasyonları açısından cazip hale getirmiştir (Trozze vd., 2022). Son yıllarda yaşanan FTX, TerraUSD ve diğer kripto skandalları, piyasadaki istikrarsızlıkların büyük ölçüde finansal raporlama eksikliklerinden ve şeffaflık sorunlarından kaynaklandığını göstermektedir (Cumming, Johan & Pant, 2019).

Kripto varlıklar, muhasebe sahtekarlıkları ve finansal manipülasyonlar açısından yeni riskler barındırmaktadır. Özellikle merkeziyetsiz finans (DeFi) platformları, kripto borsaları ve stablecoin ihraç eden kuruluşlar, muhasebe standartlarının yetersizliği nedeniyle finansal tablolarını manipüle edebilmektedir (Uzougbo vd., 2024).

Kripto borsaları ve merkeziyetsiz platformlar, bilanço dışı işlemler yaparak yükümlülüklerini gizleyebilirler. Örneğin, bazı borsalar müşterilere ait varlıkları kendi operasyonel harcamalarında kullanırken, finansal raporlarında bu varlıkları hâlâ rezervde tutuyormuş gibi gösterebilirler (Carè & Cumming, 2024). Bu durum, yatırımcıları ve düzenleyici kurumları yanıltarak piyasalarda sahte bir güven ortamı oluşturabilir.

ABD SEC, İngiltere FCA ve Avrupa Birliği MiCA gibi kurumlar, kripto işlemlerini düzenlemeye yönelik yeni politikalar geliştirmektedir (Cumming vd., 2025). Önemli düzenlemeler şu şekilde olmalıdır:

- Stablecoin ihraççılarının düzenli olarak bağımsız denetimlerden geçmesi gerekmektedir.
- Kripto borsalarının KYC (Müşterini Tanı) ve AML (Kara Para Aklamayı Önleme) kurallarına tam uyum sağlamaları zorunlu hale getirilmelidir.
- Muhasebe standartlarında kripto varlıkların nasıl raporlanacağı açıkça belirtilmelidir (Hossain, 2023).

Blokzincir teknolojisi, muhasebe sahtekarlıklarını tespit etmek için etkin bir şekilde kullanılabilir. Geliştirilecek bazı çözümler şunlardır:

- Yapay zeka destekli adli muhasebe araçları, şüpheli işlem kalıplarını tespit edebilir (Bello vd., 2024).
- Gerçek zamanlı denetim mekanizmaları, dolandırıcılıkları erken aşamada ortaya çıkarabilir (Hossain, 2023).

3. Proof-of-Reserves (Rezerv Kanıtı) Uygulamalarının Zorunlu Hale Getirilmesi

- Merkezi borsalar ve stablecoin ihraççılarının rezervlerini şeffaf bir şekilde paylaşması gerekmektedir.
- Kripto şirketleri, rezervlerini blokzincir üzerinde denetlenebilir hale getirmelidir (Bello vd., 2024).

Kripto para piyasalarının büyümesi, finansal dolandırıcılıkla mücadelede yeni yöntemlerin geliştirilmesini zorunlu hale getirmiştir. Geleneksel muhasebe denetim teknikleri, merkeziyetsiz finans (DeFi) ve blokzincir

tabanlı işlemler nedeniyle yetersiz kalmaktadır. Bu bağlamda, adli muhasebe, finansal suistimallerin tespiti ve önlenmesinde önemli bir disiplin olarak öne çıkmaktadır (Bello vd., 2024). Blokzincir analitiği, şeffaf ve değiştirilemez işlem kayıtları sayesinde adli muhasebecilere önemli avantajlar sağlarken, dolandırıcılık faaliyetlerini izlemek ve finansal suçlarla mücadele etmek için yenilikçi tekniklerin benimsenmesini gerektirir (Hossain, 2023).

Kaynakça

Abdulhakeem, S. A., & Hu, Q. (2021). Powered by Blockchain technology, DeFi (Decentralized Finance) strives to increase financial inclusion of the unbanked by reshaping the world financial system. *Modern Economy*, *12*(01), 1.

Agarwal, U., Rishiwal, V., Tanwar, S., & Yadav, M. (2024). Blockchain and crypto forensics: Investigating crypto frauds. *International Journal of Network Management*, *34*(2), e2255.

Agrawal, A., & Cooper, T. (2015). *Insider trading and market manipulation through wash trading*. Journal of Financial Economics, 22(4), 102-126.

Akanbi, A. (2024). Financial Reporting and Accounting Treatment of Crypto Assets: Professional Accountants Perspectives. *International Journal of Accounting, Finance and Risk Management*, *12*(2), 1-11.

Alamsyah, A., Kusuma, G. N. W., & Ramadhani, D. P. (2024). A review on decentralized finance ecosystems. *Future Internet*, *16*(3), 76.

Alexander, C., & Cumming, D. (Eds.). (2020). *Corruption and Fraud in financial markets: Malpractice, Misconduct and Manipulation*. John Wiley & Sons.

Almeida, H., Pinto, P., & Vilas, A. F. (2023). A review on cryptocurrency transaction methods for money laundering. *arXiv preprint arXiv:2311.17203*.

Aloosh, A., & Li, J. (2024). Direct evidence of bitcoin wash trading. *Management Science*, *70*(12), 8875-8921

Aquilina, M., Frost, J., & Schrimpf, A. (2024). Decentralized finance (DeFi): a functional approach. *Journal of Financial Regulation*, *10*(1), 1-27.

Ayoob, F. M., Jose, M., & Kumar, S. U. (2024). *Forensic analysis and detection of illicit transactions in Bitcoin network*. IEEE Xplore.

Azgad-Tromer, S. (2018). Crypto securities: on the risks of investments in blockchain-based assets and the dilemmas of securities regulation. *Am. UL Rev.*, *68*, 69.

Bai, Y., & Zhang, B. (2025). Fundamental analysis of initial coin offerings. *International Journal of Finance & Economics*, *30*(1), 879-892.

Bakhshi, T., & Ghita, B. (2021). Perspectives on Auditing and Regulatory Compliance in Blockchain Transactions. In *Trust Models for Next-Generation Blockchain Ecosystems* (pp. 37-65). Cham: Springer International Publishing.

Banaei, B. S. (2023). Response to Blockchain Transaction Ordering as Market Manipulation. *Ohio St. Tech. LJ*, *20*, 89.

Barnes, P. (2018). Crypto currency and its susceptibility to speculative bubbles, manipulation, scams and fraud. *Journal of Advanced Studies in Finance (JASF)*, *9*(2 (18)), 60-77.

Bellavitis, C., Fisch, C., & Wiklund, J. (2021). A comprehensive review of the global development of initial coin offerings (ICOs) and their regulation. *Journal of Business Venturing Insights*, *15*, e00213.

Bello, H. O., Idemudia, C., & Iyelolu, T. V. (2024). Integrating machine learning and blockchain: Conceptual frameworks for real-time fraud detection and prevention. *World Journal of Advanced Research and Reviews*, *23*(1), 056-068.

Benedetti, H., Nikbakht, E., & Sarkar, S. (2021). Blockchain and corporate fraud. *Journal of Financial Crime*.

Benedetti, H., Nikbakht, E., & Sarkar, S. (2021). *Blockchain and corporate fraud*. Journal of Financial Crime, Emerald Publishing.

Bergesen, Ø., & Palm, L. M. (2018). *An exploratory study of initial coin offerings: A better understanding of the ICO market and its fraudulent and unregulated nature*. University of Agder.

Boreiko, D. (2024). *Understanding Initial Coin Offerings: A New Era of Decentralized Finance*. Google Books.

Bosley, S., & Knorr, M. (2018). Pyramids, Ponzis and fraud prevention: Lessons from a case study. *Journal of Financial Crime*, *25*(1), 81-94.

Calafos, M. W., & Dimitoglou, G. (2022). Cyber laundering: Money laundering from fiat money to cryptocurrency. In *Principles and Practice of Blockchains* (pp. 271-300). Cham: Springer International Publishing.

Camelo, F. D., & Duarte, F. D. (2024). *Venture capital affiliation in decentralized finance: Evidence from ICOs in the blockchain ecosystem*. Financial Markets and Portfolio Management.

Carè, R., & Cumming, D. (2024). *Technology and automation in financial trading: A bibliometric review*. *Research in International Business and Finance*.

Carey, C., & Webb, J. K. (2017). Ponzi schemes and the roles of trust creation and maintenance. *Journal of Financial Crime*, *24*(4), 589-600.

Carletti, R., Luo, X., & Adelopo, I. (2024). Understanding criminogenic features: case studies of cryptocurrencies-based financial crimes. *Journal of Financial Crime*.

Casino, F., Zarpala, L. (2021). A blockchain-based forensic model for financial crime investigation: The embezzlement scenario. *Digital Finance*.

Chiu, T., Chiu, V., & Wang, T. (2022). Using textual analysis to detect initial coin offering frauds. *Journal of Forensic Accounting Research*.

Collomb, A., De Filippi, P., & Klara, S. O. K. (2019). Blockchain technology and financial regulation: a risk-based approach to the regulation of ICOs. *European Journal of Risk Regulation*, *10*(2), 263-314.

Cong, L. W., Li, X., & Wang, N. (2018). *Tokenomics: Dynamic adoption and valuation*. The Review of Financial Studies, 34(5), 1043-1084.

Cong, W., Harvey, C., & Rabetti, D. (2025). An anatomy of crypto-enabled cybercrimes. *Management Science*

Cumming, D. J., Johan, S., & Pant, A. (2019). *Regulation of the crypto-economy: Managing risks, challenges, and regulatory uncertainty. Journal of Risk and Financial Management, 12(3), 126.*

Cumming, D., Drobetz, W., Momtaz, P. P., & Schermann, N. (2025). Financing decentralized digital platform growth: The role of crypto funds in blockchain-based startups. *Journal of Business Venturing*, *40*(1), 106450.

Daraojimba, R. E., Farayola, O. A., & Olatoye, F. O. (2023). Forensic accounting in the digital age: A US perspective: scrutinizing methods and challenges in digital financial fraud prevention. *Finance & Accounting Review*.

Dashkevich, N., Counsell, S., & Destefanis, G. (2024). Blockchain financial statements: Innovating financial reporting, accounting, and liquidity management. *Future Internet*, *16*(7), 244.

Deloitte. (2023). FASB Issues Final Standard on Crypto Assets. *Heads Up, 30 (24)*.

Deng, H., Huang, R. H., & Wu, Q. (2018). The regulation of initial coin offerings in China: problems, prognoses and prospects. *European Business Organization Law Review*, *19*(3), 465-502.

Djeffal, K., & Khaldi, A. (2024). *Forensic accounting research trends: A comprehensive review of key themes and future directions.* Economics and Finance.

Duan, Y., Ge, F., & Wen, Z. (2023, August). Exploring the Risks of Blockchain to the Financial Market and Its Countermeasures. In *International Conference on Economic Management and Green Development* (pp. 633-641). Singapore: Springer Nature Singapore.

Dupuis, D., Smith, D., & Gleason, K. (2023). Bitcoin and Beyond: Crypto Asset Considerations for Auditors/Forensic Accountants. *Journal of Forensic & Investigative Accounting*.

Eberhardt, J., & Tai, S. (2017, September). On or off the blockchain? Insights on off-chaining computation and data. In *European Conference on Service-Oriented and Cloud Computing* (pp. 3-15). Cham: Springer International Publishing.

Eghe-Ikhurhe, G. O., Roni, N. N., & Bonsu, M. O. A. (2024). *Forensic accounting in fraud detection and prevention: A qualitative investigation of microfinance institutions.* International Journal of Economics.

Eghe-Ikhurhe, G. O., Roni, N. N., & Bonsu, M. O. A. (2024). *Forensic accounting in fraud detection and prevention: A qualitative investigation of microfinance institutions.* International Journal of Economics.

Eigelshoven, F., Ullrich, A., & Parry, D. (2021, December). Cryptocurrency Market Manipulation-A Systematic Literature Review. In *ICIS*.

EY. (2023). Technical Line - Accounting for digital assets, including crypto assets. *Ernst & Young IFRS Insights.*

FASB. (2023). Accounting for and disclosure of crypto assets (ASU 2023-08). *Financial Accounting Standards Board (FASB) Official Document.*

Ferreira, A. (2024). Decentralized finance (DeFi): the ultimate regulatory frontier?. *Capital Markets Law Journal*, *19*(3), 242-259.

Ferris, S., McGown, J., & Ravenscraft, J. (2024). Fraud and Unethical Behavior in Cryptoassets: Strategies and Recommendations for Improved Forensic Accounting. *Journal of Forensic & Investigative Accounting.*

Gan, R., Wang, L., Xue, L., & Lin, X. (2024). Exposing Stealthy Wash Trading on Automated Market Maker Exchanges. *ACM Transactions on Internet Technology*, *24*(4), 1-30.

Ganesh, N. S., Balasubramanian, V., Prasad, D., & Velan, S. S. (2022). *Deep learning-based user authentication with hybrid encryption for secured blockchain-aided data storage and optimal task offloading in mobile edge computing.* Wireless Networks, Springer.

Geva, B., & Muraj, M. (2024). The Digitization of Money: Stablecoins and CBDC. *Banking & Finance Law Review*, *40*(1), 115-141.

Haddad, H., Alharasis, E. E., & Fraij, J. (2024). *How do innovative improvements in forensic accounting and its related technologies sweeten fraud investigation and prevention?* WSEAS Transactions on Business and Economics.

Haddad, H., Alharasis, E. E., & Fraij, J. (2024). *How do innovative improvements in forensic accounting and its related technologies sweeten fraud investigation and prevention?* WSEAS Transactions on Business and Economics.

Haddad, H., Alharasis, E. E., & Fraij, J. (2024). How do innovative improvements in forensic accounting and its related technologies sweeten fraud investigation and prevention? *WSEAS Transactions on Business and Economics.*

Henriques, D. B. (2018). A case study of a con man: Bernie Madoff and the timeless lessons of history's biggest Ponzi scheme. *Social Research: An International Quarterly*, *85*(4), 745-766.

Ho, A., Darbha, S., Gorelkina, Y., & García, A. (2022). *The relative benefits and risks of stablecoins as a means of payment: A case study perspective* (No. 2022-21). Bank of Canada Staff Discussion Paper.

Hock, B., & Button, M. (2023). Why do people join pyramid schemes?. *Journal of Financial Crime*, *30*(5), 1130-1139.

Hornuf, L., Kück, T., & Schwienbacher, A. (2022). *Initial coin offerings, information disclosure, and fraud prevention.* Journal of Financial Stability, 58, 100993.

Hornuf, L., Momtaz, P. P., Nam, R. J., & Yuan, Y. (2025). *Cybercrime on the Ethereum blockchain.* Econsto

Hossain, M. Z. (2023). Emerging Trends in Forensic Accounting: Data Analytics, Cyber Forensic Accounting, Cryptocurrencies, and Blockchain Technology for Fraud Investigation and Prevention. *ResearchGate*

Hou, X. (2024). Decentralized exchanges and market manipulation: An empirical study. *Universidade Federal de Santa Catarina Research Papers*.

IFRS Foundation. (2023). Classification and measurement of crypto-assets under IFRS. *International Financial Reporting Standards Foundation*.

Jin, C., Zhou, J., Xie, C., Yu, S., & Xuan, Q. (2024). *Enhancing Ethereum fraud detection via generative and contrastive self-supervision*. IEEE Transactions on Information Forensics.

Joshipura, M., El Khoury, R., & Alshater, M. M. (2025). ICOs conceptual unveiled: scholarly review of an entrepreneurial finance innovation. *Financial Innovation*, *11*(1), 26.

Kabiru, H. S., Jika, A. J., & Mishra, R. (2024). *Company crime tracking system with blockchain technology to enhance security and accountability*. IEEE Xplore.

Kanu, C. (2025). *Digital currencies, financial reporting, and auditing: A new concern for accounting professionals in the accounting industry*. SSRN.

Kaur, H., & Van Belle, J. P. (2024). *Intelligent IT solutions for sustainability in Industry 5.0 paradigm*. Springer.

Kellaf, T. (2024). Blockchain in trade finance: The Good, the Bad and the Verdict. *Modern Finance*, *2*(2), 136-160.

Kirkpatrick, K., Stephens, A., & Gerber, J. (2021). *Understanding regulatory trends: Digital assets & anti-money laundering*. Journal of Investment Compliance.

Koc, S. (2024). Legal Compliance protocols for Blockchain smart contracts: A new era of regulatory compliance. *Authorea Preprints*.

Kutera, M. (2022). Cryptocurrencies as a subject of financial fraud. *Journal of Entrepreneurship, Management and Innovation*.

Lecompte, A. (2024). *The devil is in the details: a taxonomy of red flags of fraudulent initial coin offering projects*. SN Business & Economics.

Leuprecht, C., Jenkins, C., & Hamilton, R. (2023). Virtual money laundering: policy implications of the proliferation in the illicit use of cryptocurrency. *Journal of Financial Crime*, *30*(4), 1036-1054.

Longa, F. E. A. (2025). Cryptocurrency and Money Laundering. *American Journal of Industrial and Business Management*, *15*(2), 362-371.

MacDonald, C., & Zhao, L. (2022). Stablecoins and their risks to financial stability. *Bank of Canada Staff Discussion Paper/Document d'analyse du personnel—2022-20*.

Makarenkov, O., & Kosa, V. (2024). *Forensic technique for identifying corruption challenges to national security through digital technologies.* Baltic Journal of Economic Studies.

Marian, O. (2013). Are cryptocurrencies super tax havens?. *Mich. L. Rev. First Impressions*, *112*, 38.

Maurushat, A., & Halpin, D. (2022). Investigation of cryptocurrency enabled and dependent crimes. In *Financial technology and the law: combating financial crime* (pp. 235-267). Cham: Springer International Publishing.

Mishra, R., Kabiru, H. S., & Jika, A. J. (2024). *Company crime tracking system using blockchain*. IEEE Xplore.

Modesta Amaka, E., & Chindengwike, J. (2024). The Psychology Behind Financial Fraud: Unmasking Motives and Warning Signs. *James, The Psychology Behind Financial Fraud: Unmasking Motives and Warning Signs (October 08, 2024)*.

Momtaz, P. P. (2020). Initial coin offerings. *Plos one*, *15*(5), e0233018.

Morshed, A., & Khrais, L. T. (2025). *Cybersecurity in digital accounting systems: Challenges and solutions in the Arab Gulf region*. Journal of Risk and Financial Management, 18(1), 41.

Moskovicz, A. A. (2020). *Share price manipulation at the stock exchange market: Is a pyramidal scheme currently running?* ResearchGate.

Muslim, M. (2025). *The failure of governance and internal controls in preventing fraud in the company*. Advances in Managerial Auditing Research.

Netshifhefhe, K., Netshifhefhe, M. V., & Naphtali, M. (2024). *The role of forensic audits in strengthening corporate governance and mitigating compliance risks.* ResearchGate.

Nghiem, H., Muric, G., Morstatter, F., & Ferrara, E. (2021). Detecting cryptocurrency pump-and-dump frauds using market and social signals. *Expert Systems with Applications*, *182*, 115284.

Oladejo, M. T., & Jack, L. (2020). *Fraud prevention and detection in a blockchain technology environment: Challenges posed to forensic accountants.* International Journal of Economics and Accounting.

Rezaee, Z., & Wang, J. (2024). Toward Integration of Blockchain, Cryptocurrencies into Forensic Accounting Education. *Journal of Forensic Accounting Research*.

Robusti, C. D. S., Avelar, A. B. A., Farina, M. C., & Gananca, C. A. (2025). Blockchain and smart contracts: transforming digital entrepreneurial finance and venture funding. *Journal of Small Business and Enterprise Development*.

Salami, I. (2021). Challenges and approaches to regulating decentralized finance.

Scharmann, J. A. (2023). The cryptocurrency and digital asset fraud casebook. *Springer*.

Schwarcz, S. L. (2024). De-Mystifying Digital Currencies. *Law and Contemporary Problems, Forthcoming, Duke Law School Public Law & Legal Theory Series*, (2024-14).

Sheikh, F. (2024). *Challenging Accounting Fraud and the Corporate Psychopath Accountant Through Blockchain Technology* (Doctoral dissertation, University of Salford (United Kingdom)).

Sobański, K., Świder, W., Włosik, K., & Łęt, B. (2022). *Is the market success of dominant stablecoins justified by their collateral and concentration risks?* Eurasia Business and Economics Studies. Springer.

Tharani, J. S., Hóu, Z., & Charles, E. Y. A. (2024). *Unified feature engineering for detection of malicious entities in blockchain networks.* IEEE Transactions on Digital Forensics.

Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., & Johnson, S. D. (2022). Cryptocurrencies and future financial crime. *Crime science*, *11*, 1-35.

Uzougbo, N. S., Ikegwu, C. G., & Adewusi, A. O. (2024). Regulatory frameworks for decentralized finance (DEFI): challenges and opportunities. *GSC Advanced Research and Reviews*, *19*(02), 116-129.

Verma, H. (2024). The Impact of Cryptocurrency on Money Laundering Practices. *African Journal of Commercial Studies*, *5*(2), 51-60.)

Vijayalakshmi, D., & Jeevan, J. (2024). Forensic Accounting: Uncovering Fraud with Advanced Analytics. *Library of Progress-Library Science, Information Technology & Computer*, *44*(3).Library of Progress.

von Wachter, V., Jensen, J. R., Regner, F., & Ross, O. (2022, May). NFT wash trading: Quantifying suspicious behaviour in NFT markets. In *International Conference on Financial Cryptography and Data Security* (pp. 299-311). Cham: Springer International Publishing.

Wats, S., Singh, S., & Gupta, S. (2023). The quest for ICO: Identifying and prioritising the factors influencing initial coin offering selection. *International Social Science Journal*, *73*(250), 1035-1055.

Wronka, C. (2023). *Fighting financial crime in the digital age: With special regard to cyber-enabled money laundering.* ProQuest Dissertations Publishing.

Yousif, O., Dawood, M., Jassem, F. T., & Qasim, N. H. (2024). Curbing crypto deception: evaluating risks, mitigating practices and regulatory measures for preventing fraudulent transactions in the middle east. *Encuentros: Revista de Ciencias Humanas, Teoría Social y Pensamiento Crítico*, (22), 311-334.

Zetzsche, D. A., Arner, D. W., & Buckley, R. P. (2020). Decentralized finance. *Journal of Financial Regulation*, *6*(2), 172-203.