T.C. İSTANBUL TİCARET ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

METAVERSE'TE DOLANDIRICILIK TESPİTİ

Ali Halit DEMİRTAŞ

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
SİBER GÜVENLİK PROGRAMI
İSTANBUL - 2024

T.C. İSTANBUL TİCARET ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

METAVERSE'TE DOLANDIRICILIK TESPİTİ

Ali Halit DEMİRTAŞ

Danışman
Prof. Dr. Abdül Halim ZAİM

İkinci Tez Danışmanı
Prof. Dr. Muhammed Ali AYDIN

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
SİBER GÜVENLİK PROGRAMI
İSTANBUL – 2024

AKADEMİK VE ETİK KURALLARA UYGUNLUK BEYANI

İstanbul Ticaret Üniversitesi, Lisansüstü Eğitim Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında,

- tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- ve bu tezin herhangi bir bölümünü bu üniversitede veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

Ali Halit DEMİRTAŞ

İÇİNDEKİLER

	Sayfa
İÇİNDEKİLER	i
ÖZET	iii
ABSTRACT	iv
TEŞEKKÜR	v
ŞEKİLLER DİZİNİ	vi
SİMGELER VE KISALTMALAR DİZİNİ	vii
1. GİRİŞ	1
2. LİTERATÜR ÖZETİ	2
3. METAVERSE	7
3.1. Metaverse Tanımı ve Mimari Yapısı	7
3.2. Teknolojik Altyapı ve Güvenlik	9
4. DOLANDIRICILIK	12
4.1. Metaverse'de Dolandırıcılık Riskleri	13
4.1.1. Kimlik dolandırıcılığı	14
4.1.2. Sanal varlık hırsızlığı	14
4.1.3. Sosyal mühendislik	15
4.1.4. Akıllı kontrat saldırıları	15
4.1.5. Derin sahtecilik (Deepfake)	16
4.1.6. Kripto para dolandırıcılığı	16
4.1.7. Kara para aklama	17
4.1.8. Fiyat şişirme (Pump and Dump)	17
4.1.9. Yıkama ticareti (Wash Trading)	18
4.1.10. Halı çekme (Rug Pulls)	19
4.1.11. İçeriden bilgi alma (Inside Trading)	19
4.1.12. Ponzi ve piramit şemaları	20
4.2. Metaverse'de Yaşanmış Dolandırıcılık Vakaları	21
4.2.1. LooksRare yıkama ticareti dolandırıcılığı	21
4.2.2. Squid game token doldur boşalt dolandırıcılığı	22
4.2.3. Evolved Apes halı çekme dolandırıcılığı	23
4.2.4. OpenSea içeriden bilgi dolandırıcılığı	24
4.2.5. Forsage ponzi şeması dolandırıcılığı	25
4.3. Dolandırıcılıkları Önleme Stratejileri	25
4.3.1. Blokzincir tabanlı güvenlik ve kimlik doğrulama	26
4.3.2. Makine öğrenimi ve yapay zekâ tabanlı tespit sistemleri	27
4.3.3. Kullanıcı farkındalığı ve eğitim programları	28
4.3.4. Düzenleyici ve hukuki çerçevenin güçlendirilmesi	28
4.3.5. Teknolojik altyapının güçlendirilmesi	29
5. YÖNTEM	31
5.1. Araştırma Modeli	31
5.2. Çalışma Grubu	31
5.3. Veri Toplama Aracı	32
6. BULGULAR	33
6.1. Demografik Bulgular	33
6.2. Metaverse Güvenlik Risklerine İlişkin Algılar	38
6.3. Karşılaşılan Zorluklar	44
6.4. Kritik Teknolojiler ve Stratejiler	47

7. SONUÇ VE ÖNERİLER 50
KAYNAKLAR 52
EKLER 55
EK A. Anket Soruları 56
TEZ SÜRECİNDE ÜRETİLEN YAYINLAR 63

ÖZET

Yüksek Lisans Tezi

METAVERSE'TE DOLANDIRICILIK TESPİTİ

Ali Halit DEMİRTAŞ

İstanbul Ticaret Üniversitesi
Lisansüstü Eğitim Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı
Bilgisayar Mühendisliği Programı

Danışman: Prof. Dr. Abdül Halim ZAİM

İkinci Tez Danışmanı: Prof. Dr. Muhammed Ali AYDIN
2024, 63 sayfa

Metaverse, son yıllarda teknolojik gelişmelerin hızlanmasıyla birlikte sanal gerçeklik ve artırılmış gerçeklik deneyimlerini bir araya getiren yeni bir dijital evren olarak karşımıza çıkmaktadır. Büyük teknoloji şirketlerinin bu alana yaptığı yatırımlar, Metaverse'ün potansiyelini ve gelecekteki etkisini daha da artırmaktadır. Ancak, bu hızlı büyüme beraberinde yeni ve karmaşık güvenlik risklerini de getirmektedir. Özellikle dolandırıcılık, Metaverse ekosisteminin karşı karşıya olduğu en önemli tehditlerden biri olarak öne çıkmaktadır.

Bu tezin amacı, Metaverse'ün sunduğu fırsatlar ve riskler arasındaki dengeyi kurarak, bu yeni dijital dünyada dolandırıcılıkla mücadele için etkili stratejiler geliştirmeye katkıda bulunmaktır. Bu doğrultuda, çalışma kapsamında Metaverse ekosisteminin genel yapısı, dolandırıcılık türleri, risk faktörleri ve bu riskleri azaltmak için alınabilecek önlemler incelenmiştir.

Metaverse sanal dünyasının beraberinde getirdiği fırsatlar ve riskler nelerdir? Bu risklerin yol açabileceği dolandırıcılık faaliyetleri neler olabilir? Bu dolandırıcılık faaliyetleri nasıl tespit edilebilir, dolandırıcılıkla nasıl mücadele edilmesi gerekir, nasıl önlemler alınmalıdır? Sorularına cevap aramakta ve bir gelecek perspektifi ortaya koymaya çalışmaktadır. Metaverse ekosistemindeki riskler, dolandırıcılık yöntemleri, tespit ve önleme teknikleri gibi konularda detaylı bir bilgi birikimi elde edilerek konu hakkında stratejiler sunmaktadır.

Anahtar Kelimeler: *Dolandırıcılık, metaverse, sahtekarlık.*

ABSTRACT

M.Sc. Thesis

FRAUD DETECTION IN METAVERSE

Ali Halit DEMİRTAŞ

İstanbul Ticaret University
Institute of Graduate School
Department of Computer Engineering
Computer Engineering ProgramŞekil 1

Supervisor: Prof. Dr. Abdül Halim ZAİM

Co-Supervisor: Prof. Dr. Muhammed Ali AYDIN
2024, 63 pages

Metaverse is a new digital universe that combines virtual reality and augmented reality experiences with the acceleration of technological developments in recent years. The investments made by major technology companies in this field further increase the potential and future impact of the Metaverse. However, this rapid growth also brings new and complex security risks. In particular, fraud stands out as one of the most important threats facing the Metaverse ecosystem.

The aim of this thesis is to contribute to the development of effective strategies to combat fraud in this new digital world by balancing the opportunities and risks offered by the Metaverse. Accordingly, the general structure of the Metaverse ecosystem, types of fraud, risk factors and measures that can be taken to mitigate these risks are analysed within the scope of the study.

What are the opportunities and risks brought by the Metaverse virtual world? What are the fraudulent activities that may be caused by these risks? How can these fraudulent activities be detected, how should fraud be combated, what measures should be taken? It seeks answers to these questions and tries to put forward a future perspective. It provides a detailed knowledge of the risks in the Metaverse ecosystem, fraud methods, detection and prevention techniques and offers strategies on the subject.

Keywords: *Fraud, metaverse, scam.*

TEŞEKKÜR

Bu araştırma için beni yönlendiren, karşılaştığım zorlukları bilgi ve tecrübesi ile aşmamda yardımcı olan değerli Danışman Hocam Prof. Dr. Abdül Halim ZAİM'e teşekkürlerimi sunarım. Literatür araştırmalarımda yardımcı olan değerli hocam Prof. Dr. Muhammed Ali AYDIN'a teşekkür ederim. Fikirleri ile yol gösteren Doç. Dr. Mustafa Cem KASAPBAŞI hocama da teşekkürü bir borç bilirim.

Karşılaştığım prosedürel her türlü zorluklar da yardımlarını esirgemeyen kıymetli hocam Doç. Dr. Muhammet CEYLAN'a teşekkür ederim.

Tezimin her aşamasında beni yalnız bırakmayan başta annem, babam ve eşim olmak üzere tüm aileme sonsuz sevgi ve saygılarımı sunarım.

Ali Halit DEMİRTAŞ
İSTANBUL, 2024

ŞEKİLLER

Sayfa

Şekil 3.2. Metaverse mimarisi 8
Şekil 4.1. Doldur boşalt dolandırıcılığı 18
Şekil 4.2. Halı çekme dolandırıcılığı 19
Şekil 4.3. Ponzi şeması 21
Şekil 6.1. Katılımcı yaş aralığı 33
Şekil 6.2. Katılımcı eğitim durumu 34
Şekil 6.3. Katılımcı sektör grafiği 34
Şekil 6.4. Katılımcı çalışma pozisyonu 36
Şekil 6.5. Firma faaliyet süresi 37
Şekil 6.6. Katılımcı metaverse teknolojileri bilgi düzeyi 38
Şekil 6.7. Katılımcı güvenlik ve dolandırıcılık riski bilgi düzeyi 39
Şekil 6.8. Platformların dolandırıcılığa karşı savunmasızlığı 40
Şekil 6.9. Firmaların dolandırıcılık vakaları ile karşılaşma oranı 41
Şekil 6.10. En yaygın dolandırıcılık türleri 42
Şekil 6.11. Mevcut güvenlik sistemlerinin yeterlilik oranı 43
Şekil 6.12. Dolandırıcılık tespitindeki zorluklar 44
Şekil 6.13. Dolandırıcılık tespitindeki en büyük riskler 45
Şekil 6.14. Regülasyonların yeterliliği bilgisi 46
Şekil 6.15. Dolandırıcılığı önlemek için yatırım yapılması gereken alanlar . 47
Şekil 6.16. Dolandırıcılığı önlemek için ihtiyaç duyulan yeni teknolojiler 48
Şekil 6.17. Dolandırıcılıkla mücadelede sorumluluk 49

SİMGELER VE KISALTMALAR

AI	Artificial Intelligence
AR	Augmented Reality
ANN	Artificial Neural Network
DT	Dijital Twin
DL	Deep Learning
DNN	Deep Neural Networks
EC	Edge Computing
ETH	Ethereum
FL	Federated Learning
GPU	Graphics Processing Unit
GSYH	Gayri Safi Yurtiçi Hasıla
IOT	Internet of Things
KNN	K-Nearest Neighbors
ML	Machine Learning
MR	Mixed Reality
NFT	Non-Fungible Token
NLP	Naturel Language Processing
PPML	Privacy Preserving Machine Learning
SEC	Securities Exchange Commission
SVM	Support Vector Machine
TCK	Türk Ceza Kanunu
UI	User Interface
XR	Extended Reality
VR	Virtual Reality

1. GİRİŞ

Metaverse, artırılmış gerçeklik (AR) ve sanal gerçekliği (VR) internetle birleştiren sürükleyici dijital bir evreni temsil eder. Kullanıcılar sanal varlık ticareti, dijital ticaret ve sosyal etkileşimler dahil olmak üzere çeşitli faaliyetlerde bulunurken, Metaverse, hileli davranışlar ile güven, mahremiyet ve finansal güvenliği tehlikeye atmakla tehdit ediyor. Bu çalışma, araştırmacıların ve uygulayıcıların Metaverse ekosistemindeki dolandırıcılığı tespit etmek ve bunlarla mücadele etmek için bilimsel ilerlemelerden yararlandıkları yeni yolları keşfetmeyi amaçlamaktadır.

Gartner Inc. (2022), yılında yayınlanan bir rapor, 2026 yılına kadar insanların %25'inin iş, alışveriş, eğitim, sosyal ve/veya eğlence amacıyla günde en az bir saatini Metaverse'te geçireceğini belirtiyor. Aynı rapor, 2026 yılına kadar dünyadaki kuruluşların %30'unun ürün ve hizmetlerini metaverse için hazır hale getireceğini gösteriyor. (Smaili ve de Rancourt-Raymond, 2022).

Metaverse, sanal gerçeklik ortamında var olma ve etkileşimde bulunma eylemini ifade eder. Bu dijital ekosistem, kullanıcıların kendi dijital varlıklarını oluşturup yönettikleri, gerçek dünyadan farklı ve kendine özgü bir alan olarak tanımlanır. Metaverse, sanal para birimleri, dijital varlıklar ve sanal mülkiyetler gibi çeşitli bileşenleri içerir. Bununla birlikte, Metaverse'ün sunduğu bu geniş imkânlar, dolandırıcılık faaliyetlerine de zemin hazırlamaktadır. Yetersiz güvenlik önlemleri, kimlik hırsızlığı, sahte ticaret işlemleri ve dijital varlıkların çalınması gibi çeşitli dolandırıcılık türleri Metaverse üzerinde ortaya çıkabilir. Bu bağlamda, Metaverse'ün güvenlik açıklarını analiz etmek ve dolandırıcılık eylemlerini tespit etmek için gerekli stratejilerin geliştirilmesi büyük önem arz etmektedir. Bu tez, metaverse'ün güvenlik problemleri ve özellikle dolandırıcılık üzerine yapılmış araştırmaların bir özetini sunmakta ve ortaya çıkan güvenlik zorluklarını tartışarak dolandırıcılığa karşı önleyici stratejiler önermektedir.

2. LİTERATÜR ÖZETİ

Bolton ve Hand (2002), istatistiksel yöntemlerin dolandırıcılık tespiti alanındaki kullanımını kapsamlı bir şekilde incelemektedir. Para aklama, e-ticaret kredi kartı dolandırıcılığı, telekomünikasyon dolandırıcılığı ve bilgisayar korsanlığı gibi çeşitli alanlarda istatistiksel ve makine öğrenmesi yöntemlerinin başarılı bir şekilde uygulandığını anlatmaktadır.

Kou vd. (2004), dolandırıcılık tespiti tekniklerine dair kapsamlı bir inceleme sunmaktadır. Özellikle telekomünikasyon, kredi kartı işlemleri ve bilgisayar ağlarına yönelik siber saldırılar gibi çeşitli alanlarda kullanılan dolandırıcılık tespiti yöntemlerini, bu yöntemlerin etkinliğini ve karşılaşılan zorlukları tartışır. İstatistiksel analiz, veri madenciliği, yapay zekâ gibi yöntemlerin dolandırıcılık tespitinde nasıl kullanıldığına dair geniş bir literatür incelemesi sunulmaktadır.

Hasham vd. (2019), siber güvenlik çağında finansal suçlar ve dolandırıcılık ile mücadeleye odaklanmaktadır. Finansal kurumların bu tehditlerle nasıl başa çıkması gerektiğini, siber güvenlik ve dolandırıcılık tespiti süreçlerinin entegrasyonunu, mevcut zorlukları ve gelecekteki stratejileri ele alır.

Nicholls vd. (2021), finansal siber suçlarla mücadele için derin öğrenme (DL) yaklaşımlarını kapsamlı bir şekilde incelemektedir. Çalışma finansal suçların evrimini ve bu suçların siber uzayda nasıl yayıldığını ele alır. Derin öğrenme ve makine öğrenimi yöntemlerinin, finansal dolandırıcılık, kara para aklama, vergi kaçakçılığı gibi suçların tespiti ve önlenmesinde oynadığı kritik rolü vurgular. Bu suçların siber uzayda gerçekleşme biçimlerini ve siber suçların artan karmaşıklığını ele alarak, mevcut ve gelecekteki zorlukları ve bu zorlukların üstesinden gelmek için geliştirilen yeni teknikleri tartışır.

Ali vd. (2022), makine öğrenmesi (ML) tabanlı finansal dolandırıcılık tespiti üzerine yapılmış sistematik bir literatür taramasını sunmaktadır. Ayrıca finansal dolandırıcılık tespiti alanındaki ana sorunları, boşlukları ve sınırlamaları tartışmakta ve gelecekteki araştırmalar için önerilerde bulunmaktadır.

Katterbauer vd. (2022), metaverse ortamında İslami finansla ilgili finansal siber suçların doğasını ve bu suçlarla başa çıkmak için gereken düzenleyici ve siber güvenlik önlemlerini ele almaktadır. Kripto para birimleri, sahte NFT'ler ve dijital varlıklar üzerinden gerçekleştirilen dolandırıcılık faaliyetlerini incelemektedir. İslami finansın Metaverse'de nasıl uygulanabileceği ve bu süreçte karşılaşılabilecek zorluklar tartışılmaktadır.

Kshetri (2022), NFT (Non-Fungible Token) pazarında meydana gelen dolandırıcılık, sahtekarlık ve diğer suçları detaylı bir şekilde ele almaktadır. Bu tür dolandırıcılıkların nasıl gerçekleştiğini, kullanılan yöntemleri ve bunların hedeflerini ayrıntılı olarak incelemekle birlikte bu tür suçlarla mücadele etmek için gerekli olan farkındalık ve önlemler üzerinde durulmaktadır.

Mackenzie (2022), metaverse'deki kripto para dolandırıcılıkları, gri ekonomi ve teknolojik-sosyal yapıların kesişim noktasını inceleyen bir kriminolojik çalışmadır. Araştırmacı, kripto para piyasalarını, büyük ölçüde düzenlenmemiş ve yüksek riskli bir finansal sistem olarak tanımlar. Bu sistem, suç kontrol mekanizmalarının büyük ölçüde eksik olduğu ve dolandırıcılıkların yaygın olduğu bir ortam sunmaktadır. Kripto ticaretinin sosyal ve kültürel yönlerini araştırmak için etnografik bir çalışma yürütür ve bu bağlamda dolandırıcılıkların nasıl geliştiğini ve gri ekonominin bu yeni teknolojik-sosyal dünyadaki rolünü tartışır.

Smaili ve de Rancourt-Raymond (2022), metaverse ekosisteminin risklerini incelemeyi amaçlamaktadır. Metaverse'ün gelişimi, bu ekosistemin sunduğu fırsatlar ve içerdiği riskler hakkında kapsamlı bir inceleme sunar. Özellikle, metaverse'ün dolandırıcılık risklerine odaklanır ve bu risklerin nasıl azaltılabileceği konusunda stratejiler önerir.

Trozze vd. (2022), kripto para birimlerinin gelecekteki mali suçlar üzerindeki etkilerini incelemekte ve bu tür suçların nasıl gelişebileceğini araştırmaktadır. Kripto para birimlerinin sunduğu anonimlik, merkeziyetsizlik ve şeffaflık gibi özelliklerin, dolandırıcılık ve diğer mali suçların işlenmesine nasıl olanak tanıdığı

üzerinde durur. Aynı zamanda, kripto para birimleri ile ilgili mevcut dolandırıcılık türlerini ve bu suçların nasıl evrilebileceğini tartışmaktadır.

Al-Tkhayneh vd. (2023), metaverse'deki suçların gelecekteki senaryolarını ve bu suçlarla başa çıkmak için gerekli yasal zorlukları ele alır. Metaverse'ün suç faaliyetleri için nasıl bir zemin hazırlayabileceğini, bu suçların hangi biçimlerde ortaya çıkabileceğini ve bu suçlarla mücadele için hangi yasal düzenlemelerin gerekli olduğunu tartışır.

Başbüyük (2023), blokzincir, kripto varlıklar ve akıllı sözleşmeler gibi teknolojik gelişmelerin, malvarlığına yönelik yeni sahtekarlık türlerine nasıl zemin hazırladığını incelemektedir. Özellikle kripto para borsaları, sahte kripto varlıklar, likidite boşaltma, fiyat manipülasyonu, sahte yatırım ve madencilik uygulamaları gibi sahtekarlıklar ele alınmıştır. Makale, Türk Ceza Kanunu'nun (TCK) mevcut dolandırıcılık suçunun bu yeni haksızlıklarla mücadelede ne kadar yeterli olduğunu tartışır ve yeni düzenleme ihtiyaçlarını vurgular.

Kshetri (2023). Web3 ve metaverse'ün gizlilik ihlalleri, güvenlik açıkları ve diğer tehditlerini ele almaktadır. Teknolojik yeniliklerin neden olduğu güvenlik zafiyetlerini ve bu zafiyetlerin kullanıcılar üzerindeki etkilerini inceler.

Lin vd. (2023). metaverse'ün hızlı gelişimi ile ortaya çıkan uygulamalar, suçlar ve yönetim konularını ele alır. Metaverse ekosisteminde mevcut olan suçları sınıflandırmakta ve bu suçlarla mücadeleye yönelik mevcut yönetim yaklaşımlarını özetlemektedir.

Wu vd. (2023), Web3 destekli metaverse ekosisteminde ortaya çıkan finansal suçların sınıflandırılmasını, bu suçlarla mücadele yöntemlerini ve olası fırsatları incelemektedir. Finansal suçların önlenmesi ve metaverse ekosisteminin uzun vadeli sağlıklı gelişiminin sağlanması için gerekli adımları ele almaktadır.

Xu vd. (2023). metaverse teknolojisinin finansal dolandırıcılık tespiti üzerindeki potansiyelini araştırmaktadır. Çalışma, finansal analistlerin Metaverse ortamını

kullanarak dolandırıcılık tespitindeki yeteneklerini nasıl geliştirebileceklerini incelemek için önceden kayıtlı, rastgele kontrollü bir deney yürütmüştür. Deneyde, finansal tablo incelemeleri gerçekleştiren üç farklı grup karşılaştırılmıştır: fiziksel ortamda çalışan bir kontrol grubu, video konferans yoluyla çalışan bir diğer kontrol grubu ve metaverse ortamında çalışan deneysel grup. Sonuçlar, metaverse ortamını kullanan deneysel grubun dolandırıcılık tespitindeki doğruluk oranının diğer iki gruba göre daha yüksek olduğunu göstermiştir. Bu başarının, veri görselleştirme tekniklerinin artan kullanımı ve kadın katılımcıların daha aktif katılımı ile ilişkilendirilebileceği belirtilmiştir.

Airlangga (2024), açık metaverse ortamında gerçekleşen blokzincir işlemlerinde anomali tespiti ve dolandırıcılık analizine yönelik derin öğrenme modellerinin uygulanmasını inceler. Çalışmanın bulguları, metaverse ortamındaki blokzincir işlemlerinin güvenliğini artırma ve dijital ekonomiyi daha güvenilir hale getirme konusunda önemli katkılar sunmaktadır.

Hudnurkar vd. (2024), metaverse'de gerçekleşen Ethereum işlemleri üzerinde dolandırıcılık tespitine odaklanmaktadır. Ethereum platformundaki dolandırıcılık faaliyetlerini tespit etmek için kullanılan çeşitli makine öğrenimi algoritmaları incelenmiştir. Ethereum tabanlı Metaverse işlemlerinde dolandırıcılık faaliyetlerini belirlemek için K-Nearest Neighbors (KNN), Decision Tree, Support Vector Machine (SVM), Random Forest, XGBoost, Artificial Neural Network (ANN) gibi algoritmaların kullanımını ve bu algoritmaların performansını karşılaştırmaktadır.

McAmis vd. (2024), metaverse'deki kimlik doğrulama ve dolandırıcılık önleme yöntemlerini inceliyor. Metaverse'de kimlik doğrulama ve dolandırıcılıkla mücadele için tasarım alanını ve teknik yönleri keşfederek, kullanıcı gizliliğini de göz önünde bulundurarak bir dizi çözüm sunmayı amaçlamaktadır.

Mooij (2024), metaverse üzerinden gerçekleşebilecek kara para aklama ve terörizmin finansmanı faaliyetlerini ve bu tür suçların önlenmesi için gerekli

düzenleyici çerçeveyi ele alır. Mevcut yasal ve düzenleyici çerçevelerin bu tür faaliyetlerle başa çıkmakta yetersiz kalabileceği tartışılmaktadır.

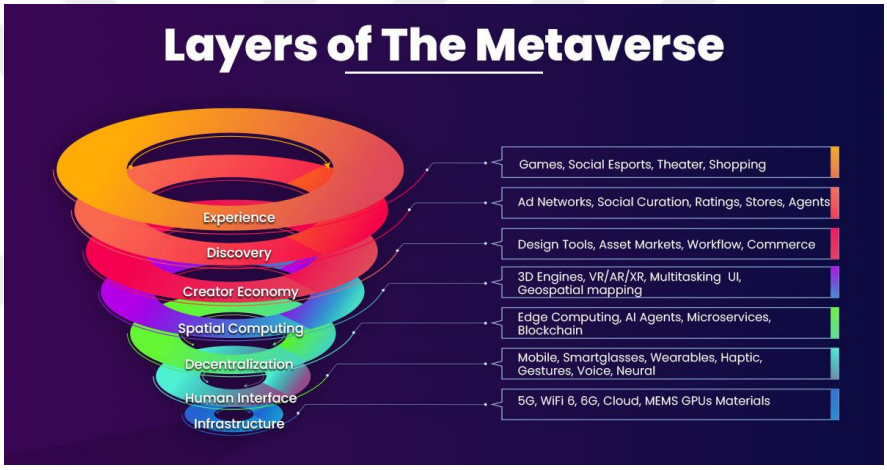
3. METAVERSE

3.1. Metaverse Tanımı ve Mimari Yapısı

Metaverse kelimesi, öte anlamına gelen “meta” ile evren anlamına gelen “verse” kelimelerinin birleşiminden oluşmaktadır. Kelime tam anlamıyla fiziksel veya gerçek dünyanın ötesindeki evren anlamına gelir. İlk defa Neal Stephenson bilim kurgu romanı Snow Crash’te (1992), bu tabiri kullanmıştır. Metaverse'te insanlar, sürükleyici bir sanal dünyada avatarlardır. Bu dünya, gerçek veya fiziksel dünyamıza paralel olarak gelişir. Kullanıcıların diğer kullanıcılarla etkileşime giren avatarlarla temsil edildiği etkileşimli bir sosyal deneyim sunar. Kullanıcılar farklı sanal sosyal dünyalar üzerinden ışınlanabilir, etkinliklere katılabilir ve kripto para birimleri kullanarak işlem yapabilir. Metaverse’te çevrimiçi/çevrimdışı, yerel/küresel ve simülasyon/gerçek hayat gibi ikilikler yoktur. Metaverse, süresiz olarak devam eden, gerçek zamanlı bir etkinliğe katılabilinen, işleyen bir ekonomiye sahip olan hem dijital hem de fiziksel dünyaları kapsayan, verilerin, dijital öğelerin/varlıkların, içeriklerin birlikte çalışabilirliği sunduğu bir yaşam alanı olarak görülebilir. Metaverse'ün çalışması için sayısız yeni teknoloji, protokol, şirket, yenilik ve keşif gerekecektir. (Sun vd., 2022a).

Metaverse, dünyadaki teknoloji devlerinin çoğu için en yeni makro hedef haline geldi. Bunda öncelikle Mart 2021’de Roblox şirketinin, Amerika Birleşik Devletleri'nde Nasdaq'ta "İlk Metaverse hissesi" olarak tanımlanan bir şekilde halka açılması, akabinde Ekim 2021'de Facebook şirketinin, adını Metaverse'ün ön ekinden alarak Meta olarak değiştirmesi, Oculus VR'yi ve yeni duyurduğu Horizon sanal dünya/toplantı alanını ve AR gözlükleri, beyinden makineye arayüzler ve iletişim gibi pek çok başka projeyi satın alması, uluslararası arenada bu teknolojiye tüm dikkatleri çekmesi adına fitili ateşleyen ilk adımlar olmuştur. (Sun vd., 2022b).

Metaverse'ün 2021 yılı itibariyle geliştirme süreci hala emekleme aşamasındadır ve bilgisayar görüşü, dijital ikiz konsepti, sanal gerçeklik, artırılmış gerçeklik, yapay zekâ ve blok zincir, makine öğrenmesi gibi çeşitli teknolojik gelişmeler yükselişine katkıda bulunmaktadır. Konsept, yeni teknolojilerin ve altyapıların ortaya çıkmasıyla yıllar içinde önemli ölçüde gelişmiştir. İlerlemeye rağmen, Metaverse'ün gelişimi hala etkileşim sorunları, bilgi işlem gücü baskıları, etik kısıtlamalar, gizlilik riskleri, güvenlik açıkları ve farklı dünyalardaki bağımlılık riskleri gibi güncel sorunlarla sınırlıdır. Zorluklara rağmen, birçok küresel şirket Metaverse'e yatırım yapıyor. Sorunsuz ve birbirine bağlı bir Metaverse deneyimi için gereken altyapıyı, teknolojileri ve standartları geliştirmek için çaba sarf ediliyor. (Wang vd., 2023).



Şekil 3.2. Metaverse mimarisi (Understanding The Value Chain of The Metaverse Priyansha Singh 2022)

Mevcut internetten Metaverse'e geçişi kolaylaştırmak için çok çeşitli temel teknolojiler gereklidir ve bunlar, Şekil 3.2.'de gösterildiği gibi Metaverse'ün yedi katmanıyla eşleştirilir. Spesifik olarak, yedinci katman, yani altyapı, gelecekteki mobil ağlar ve Wi-Fi ve grafik işleme birimleri (GPU'lar) gibi donanım bileşenleri dahil olmak üzere Metaverse'ü destekleyen temel teknolojileri temsil eder. Sanal gerçeklik (VR), artırılmış gerçeklik (AR) ve genişletilmiş gerçeklik (XR) gibi teknolojiler uzamsal bilgi işlem katmanına girerken, VR kulaklıkları gibi ilgili giyilebilir cihazlar altıncı katmana, yani insan arayüzüne aittir. Yapay Zekâ (AI), uç ve bulut bilişim gibi diğer teknolojiler birden çok katmanda yer alır ve Metaverse için önem taşır. (Wang vd., 2022).

3.2. Teknolojik Altyapı ve Güvenlik

Metaverse'ün teknolojik altyapısı, VR ve AR görüntüleme teknolojileri, AI, makine öğrenimi (ML), uç bilişim (EC), 5G altyapısı ve blok zinciri teknolojisi gibi bileşenleri içerir. Bu teknolojiler, metaverse'ün işlevselliğini ve kullanıcılarla etkileşim kurmasını sağlayarak sürükleyici deneyimler ve fiziksel çevrenin gerçek zamanlı görüntülerini sunar. Ayrıca metaverse, fiziksel dünyaya aracılar vasıtasıyla bağlı olan ancak ondan ayrı olmayan ortak altyapılar, protokoller ve standartlardan oluşur. (Pooyandeh vd., 2022).

VR teknolojisi, kullanıcıların ses takibi ve vücut hareketi gibi sürükleyici deneyimler aracılığıyla bilgisayar tarafından oluşturulmuş sanal bir ortamı deneyimlemelerine olanak tanır. Öte yandan, AR, kullanıcıların dijital nesneler ve yüzeylerle etkileşime girmesine olanak tanımak için fiziksel dünyadaki dijital bilgileri kullanır ve tamamen sanal bir ortam yaratmadan gerçek dünyayı simüle eder. (Pooyandeh vd., 2022).

EC, dağıtılmış bir bilişim topolojisinin parçası olarak uca yakın bilişimi ifade eder. VR, AR, sürücüsüz arabalar, akıllı şehirler ve otomasyon sistemleri gibi uygulamaların performansını artırmak için EC, uç sunucuların ve mobil uç bilişimin kullanılmasını içerir. EC, ağ gecikmesini, bant genişliği maliyetlerini azaltmayı ve kullanıcılar için gerçek zamanlı veri kullanılabilirliğini iyileştirmeyi amaçlamaktadır. Ayrıca 5G'de mobil AR ve VR için sis bilişim, önbelleğe alma ve uçta bilişim kullanımının yanı sıra EC ve DL yakınsamasını da içerir. Ayrıca EC, düşük gecikme süresi, yüksek verimlilik ve güvenlik sağlayarak Metaverse'ün sürdürülmesinde önemli bir rol oynamaktadır. (Xu vd., 2022).

AI, makinelerin insan zekâsını taklit etmesini sağlayan bir teknolojidir. Büyük miktarda veri kullanarak örüntü tanıma ve öğrenme yoluyla makinelerin öğrenmesini sağlar. Bu sayede insan deneyimlerinden faydalanarak çeşitli görevleri yerine getirebilir ve kararlar verebilir. (Güler ve Savaş, 2022).

ML, makinelerin deneyimlerden elde edilen bilgilerle öğrenmesini ve performansını iyileştirmesini sağlayan bir tekniktir. ML üç kategori vardır: denetlenen öğrenme, denetlenmeyen öğrenme ve takviyeli öğrenme. ML, desen sınıflandırması, regresyon, bir sıralama işlevi öğrenme, akıllı kaynak tahsisi, kanal tahmini ve iletim gücü kontrolü gibi çeşitli amaçlar için kullanılabilir. Ayrıca, daha keyifli bir kullanıcı deneyimi oluşturmak ve sanal gerçekliğe daha fazla etkileşim eklemek için verileri işleyebilir (Lee vd., 2021).

Blokzincir, dağıtık defter teknolojisi olarak bilinen ve merkezi olmayan bir yapı içerisinde veri depolama ve işlem güvenliğini sağlayan bir teknolojidir. İlk olarak Satoshi Nakamoto'nun 2008 yılında yayımladığı "Bitcoin: A Peer-to-Peer Electronic Cash System" başlıklı makalesiyle tanıtılmıştır. Blokzincir, bireyler arası işlemlerde güveni sağlamak amacıyla kullanılan bir teknolojidir ve her biri veri içeren bloklardan oluşur ve bu bloklar bir zincir şeklinde birbirine bağlanır. Her bir blok, önceki bloğun kriptografik bir özetini içerdiğinden, blok zincirindeki verilerin değiştirilmesi son derece zordur. Blokzincir, Metaverse'teki ekonomik sistemin temelini oluşturarak, varlıkların değerini ve mülkiyetini güvence altına alır. NFT (Non-Fungible Token) tabanlı blokzincir teknolojisi, Metaverse'ün daha da aktif hale gelmesini sağlar. Blokzincir teknolojisi, Metaverse'teki kaynakların ve varlıkların değerini tanımayı ve gerçek ekonomiyle eşdeğer ekonomik etkileşimler kurmayı mümkün kılar. (Jeon vd., 2022).

Metaverse, eğitimden ekonomiye, sosyal etkileşimden kültürel üretime kadar birçok alanda büyük fırsatlar sunmaktadır. Genel olarak belirtmek gerekirse eğitim alanında yapılacak inovasyonlar, kültürel üretim ve düzenlenen sosyal ve sanatsal etkinlikler, ekonomik olarak yeni iş fırsatları, markalar için reklam ve pazarlama, firmalar için ise iş birliği gibi önemli fırsatlar sunmaktadır.

Bütün bu fırsatlar, her zaman olduğu gibi tehditleri de beraberinde getirecektir. Metaverse'ün teknolojik altyapı bileşenlerinin güvenlik açıkları arasında ağ saldırıları, teknik güvenlik kusurları, kritik altyapı arızaları, veri korsanlığı, kötü amaçlı yazılım saldırıları, gizlilik sorunları, spam, blok zinciri teknolojisindeki güvenlik açıkları, finansal verileri ve kripto varlıkları hedef alan güvenlik ihlalleri,

kişisel bilgiler, biyometrik veriler, kara para aklama, kullanıcı verileri, öğrenme içeriği gibi farklı Metaverse sistemlerindeki güvenlik açıklarından yararlanma ve Metaverse'te farklı amaçlar için kullanılan teknolojilerin artan katman sayısı ve karmaşıklığı nedeniyle potansiyel siber güvenlik açıkları yer almaktadır.

4. DOLANDIRICILIK

Dolandırıcılık, insanlık tarihinin başlangıcından itibaren var olan bir olgudur. İlk insanların ticaret yapmaya başlamasıyla birlikte, dolandırıcılık da hayatın bir parçası haline gelmiştir. Bu eylem, bir kişinin diğerinin zayıflıklarından, bilgi eksikliğinden veya güveninden yararlanarak haksız kazanç elde etmesi şeklinde tanımlanabilir. Tarih boyunca farklı biçimlerde karşımıza çıkan dolandırıcılık, zamanla değişerek ve gelişerek günümüze kadar ulaşmıştır.

Para ve mal değişiminin başladığı ilk dönemlerde, sahte ürünlerin satılması, ölçü ve tartı hileleri gibi basit dolandırıcılık yöntemleri yaygın olarak kullanılmıştır. Yazının ve belgelerin icadıyla birlikte ise sahte belgelerle yapılan dolandırıcılıklar tarih sahnesinde yerini almıştır. Günümüzde ise teknolojiyle birlikte dolandırıcılık çok daha karmaşık bir hal almış, özellikle teknoloji geliştikçe yöntemleri de evrim geçirmiştir. Bugün, siber dolandırıcılık ve dijital platformlarda gerçekleştirilen sahtekarlıklar, dolandırıcılığın en yaygın ve güncel örnekleri arasında yer almaktadır.

Dolandırıcılık, sahtecilik, kredi dolandırıcılığı, içeriden bilgi ticareti ve diğer aldatıcı uygulamalar dahil olmak üzere birçok biçimde olabilir. Genellikle kurbanlar için mali kayba neden olur ve finansal sistemlerin ve kurumların bütünlüğüne önemli zararlar verebilir. (Katterbauer vd., 2022).

Dijital dolandırıcılık veya siber dolandırıcılık ise, dijital teknoloji ve internetin kullanımını içeren dolandırıcılık faaliyetlerini ifade eder. Bu dolandırıcılık biçimi, bireyleri veya kuruluşları finansal kazanç elde etmek için aldatmak amacıyla teknolojik zaafları ve dijital platformların yaygın kullanımını istismar eder. Dijital dolandırıcılık, kimlik hırsızlığı, kimlik avı, çevrimiçi dolandırıcılık ve hassas bilgilere yetkisiz erişimi içerebilir. Dijital dolandırıcılığın önemli ekonomik, itibar ve psikolojik etkileri vardır. Finansal olarak bireylere, işletmelere ve hükümetlere önemli maliyetler yükler. İtibar hasarı müşteri güveninin ve gelirinin kaybına yol açabilir. Psikolojik olarak, mağdurlar kaygı ve depresyon dahil olmak üzere önemli sıkıntılar yaşayabilir. Dolandırıcılık ve dijital

dolandırıcılık, bireyler, işletmeler ve daha geniş ekonomi için ciddi etkileri olan karmaşık olgulardır. Bu dolandırıcılık biçimlerini anlamak, etkilerini önleme ve azaltma stratejileri geliştirmek için çok önemlidir. Teknolojinin devam eden evrimi, dolandırıcılık tespiti ve önleme yöntemlerinin sürekli uyarlanmasını gerektirir (Kshetri, 2022).

4.1. Metaverse'te Dolandırıcılık Riskleri

Klasik dolandırıcılık ve dijital dolandırıcılık, kullanılan yöntemler ve faaliyetlerinin kapsamı açısından farklılık gösterir. Klasik dolandırıcılık tipik olarak sahte belgeler, kredi dolandırıcılığı ve içeriden tehditler gibi fiziksel manipülasyonları veya aldatmacaları içerir ve genellikle finansal personeli veya hizmetleri hedef alır. Öte yandan dijital dolandırıcılık, mobil telekomünikasyon dolandırıcılığı, bilgisayara izinsiz giriş ve doğal veya sentetik verilerin istismarı gibi suçları işlemek için dijitalleşme, otomasyon ve modern teknolojiden yararlanır. Dijital dolandırıcılık aynı zamanda elektronik olarak daha sofistike ve kişisel olmayan bir yaklaşım sunmakta, saldırıların kapsamı ve yaygınlığı açısından daha iddialı olmaktadır. Ayrıca, siber tehditlerin yükselişi klasik dolandırıcılık ve mali suçlar arasındaki sınırları bulanıklaştırarak dijital çağda suç faaliyetlerini daha karmaşık ve birbiriyle ilişkili hale getirmiştir. Metaverse'teki dolandırıcılığın benzersiz yönlerini anlamak çok önemlidir. Metaverse'te dolandırıcılık, sanal ortamlarda gerçekleştirilen aldatıcı uygulamaları ve dürüst olmayan faaliyetleri ifade eder. Bu, kimlik hırsızlığı, finansal dolandırıcılık, kara para aklama, kullanıcı verilerine yetkisiz erişim, siber ihlaller ve saldırılar, gizlilik ihlalleri, sahte sanal ürünler, kurumsal casusluk ve piyasa manipülasyonu gibi faaliyetler ile dijital varlıkları veya dijital para birimlerini hedef alan olumsuz işlemleri içerebilir (Wang vd., 2022). Metaverse'te dolandırıcılığın kesin tanımı ve örnekleri farklılık gösterebilmekle birlikte, Metaverse'ün dijital ve çoğu zaman merkezi olmayan doğasından yararlanan çok çeşitli yasa dışı faaliyetleri kapsayabilir.

Yeni bir endüstri veya teknoloji etrafında, heyecan olan her yere, dolandırıcıların akın etmesi kaçınılmazdır. Metaverse de farklı değil. Metaverse'te düzenleme

eksikliği ve dünyanın herhangi bir yerinden faaliyet gösterme yeteneği, dolandırıcıların planlarını gizlemelerini kolaylaştırıyor. Buna ek olarak, gelişmekte olan platformlardaki güvenlik açıkları ve sahte metaverse deneyimleri oluşturma yeteneği, saldırılara, dolandırıcılığa veya kullanıcıların fonlarının çalınmasına yol açabilir. Kimlik hırsızlığı, finansal dolandırıcılık, kara para aklama, sanal varlık hırsızlığı, sahte sanal ürünler ve hesaplar, veri ihlalleri, kurumsal casusluk, şantaj ve sanal dünya kullanıcılarını hedef alan sosyal mühendislik teknikleri gibi Metaverse'te meydana gelebilecek farklı dolandırıcılık türleri bulunmaktadır.

4.1.1. Kimlik dolandırıcılığı

Metaverse'te kimlik dolandırıcılığı, sanal gerçeklik ortamlarında başka bir kişinin kimliğinin veya kişisel bilgilerinin hileli kullanımını ifade eder. Bu, başka bir kullanıcıyı taklit etmeyi, alışveriş yapmak için kredilerini kullanmayı, sanal kimlikleri kötüye kullanmayı ve dijital alanda başkalarını manipüle etmek veya sömürmek için aldatmayı içerebilir. Metaverse gelişmeye devam ettikçe, kimlik dolandırıcılığı, kullanıcı kimliklerinin doğrulanması ve korunması ve kötü niyetli aktörlerin kişisel bilgileri istismar etmesinin veya kötüye kullanmasının önlenmesi açısından önemli bir zorluk teşkil etmektedir (McAmis vd., 2024).

4.1.2. Sanal varlık hırsızlığı

Kshetri (2023), göre Metaverse'deki sanal varlık hırsızlığı, kötü niyetli aktörlerin kullanıcılardan dijital varlıkları ve/veya para birimini çalmak için blok zinciri teknolojisindeki güvenlik açıklarından yararlanmasını içerir. Ayrıca NFT'ler de dahil olmak üzere sahte dijital ürünler yaratabilir ve finansal kazanç elde etmek amacıyla kullanıcıların finansal bilgilerine erişmek için sahte finansal aktörler gibi davranabilirler. Ayrıca dijital varlıkların komisyoncuları gibi davranarak ve bunları farklı metaverse platformları arasında taşıyarak sahiplerini dolandırabilirler.

4.1.3. Sosyal mühendislik

Dolandırıcıların insan psikolojisini manipüle ederek kurbanları yanıltmak ve hassas bilgileri elde etmek için kullandığı bir siber saldırı türüdür. Bu tür saldırılar, teknik açıkları hedeflemek yerine, insan davranışlarını ve güvenlik bilincini hedef alır. Sosyal mühendislik saldırıları, yasadışı ekonomik kazanç için hedefi kandırmaya yönelik duygusal hitaplar, kimliğe bürünme veya ikna teknikleri şeklinde olabilir. Dolandırıcılar, kurbanlarını aldatmak için sahte bir senaryo oluşturma yöntemiyle bunu gerçekleştirebilir. Bunun için yemleme, fiziksel takip, telefon ile oltalama vb. yöntemleri tercih edebilirler. (Nicholls vd., 2021).

4.1.4. Akıllı kontrat saldırıları

Akıllı kontratlar, blokzincir teknolojisi üzerinde çalışan, belirli koşullar yerine getirildiğinde otomatik olarak yürütülen kod parçacıklarıdır. Bu kontratlar, iki taraf arasındaki işlemlerin aracısız ve güvenli bir şekilde gerçekleşmesini sağlar. Akıllı kontratların kodundaki reentrancy saldırıları, honeypot'lar ve tasarım kusurlarından yararlanma gibi farklı güvenlik açıkları ve istismar türleridir. Bu saldırılar, fonları çalmak, varlıkları dondurmak ya da blok zinciri sistemi içinde mali suçlar işlemek için akıllı sözleşmelerin işlevselliğini manipüle etmeyi amaçlamaktadır (Wu vd., 2023). Buna ek olarak, akıllı sözleşmelerin terörist faaliyetleri finanse etmek için kullanıldığı örnekler de mevcuttur ve bu durum akıllı sözleşme saldırılarının ciddi güvenlik etkilerini ortaya koymaktadır. Reentrancy saldırı türünde, bir akıllı kontratın fonksiyonları tekrar tekrar çağrılarak fonlar boşaltılır. Saldırgan, bir işlem tamamlanmadan önce aynı işlevi yeniden tetikleyerek, kontratın içindeki fonların bir kısmını sürekli olarak çekebilir. Akıllı kontratlardaki aritmetik işlemler düzgün bir şekilde kontrol edilmediğinde, sayıların değerleri aşırı derecede yükselebilir veya düşebilir.
Bu da saldırganların kontratı manipüle ederek haksız kazanç sağlamasına yol açabilir. Akıllı kontratların belirli işlemler için kimlere yetki verdiği kritik önem taşır. Yanlış yapılandırılmış izinler veya zayıf erişim kontrolü, saldırganların kontrat üzerinde istenmeyen işlemler yapmasına olanak tanıyabilir. Solidity

programlama dilini temel alan Ethereum akıllı sözleşmelerine yönelik reentrancy saldırıları, akıllı sözleşme saldırılarının yaygın bir biçimidir. (Wu vd., 2023).

4.1.5. Derin sahtecilik (deepfake)

Derin sahtecilik (deepfake), bir kişinin yüzünü, sesini veya hareketlerini taklit etmek için AI ve DL tekniklerini kullanan bir teknoloji türüdür. Bu teknoloji, bir kişinin konuşmasını, mimiklerini ve vücut dilini başka bir kişiye aitmiş gibi gösterebilir ve bu nedenle yanıltıcı ve manipülatif içerikler oluşturmak için kullanılabilir. Derin sahtecilik için öncelikle hedef kişinin bol miktarda görsel ve sesli verisine ihtiyaç vardır. Bu veri genellikle fotoğraflar, videolar ve ses kayıtları şeklinde toplanır. AI algoritmaları, hedef kişinin yüzünü, sesini ve hareketlerini analiz eder. Bu süreçte derin öğrenme modelleri kullanılarak, kişinin yüz hatları, ses tonu ve jestleri gibi ayrıntılar öğrenilir. Eğitimli model, hedef kişinin yüzünü veya sesini başka bir video ya da ses kaydına bindirir. Bu işlem sırasında, algoritmalar kişinin yüz ifadelerini, ses tonunu ve hareketlerini gerçekçi bir şekilde taklit eder. Oluşturulan sahte içerik, son derece gerçekçi görünebilir ve bu nedenle izleyicileri kolayca yanıltabilir.

4.1.6. Kripto para dolandırıcılığı

Kripto para dolandırıcılığı, bireyleri veya grupları kandırarak kripto varlıklarına yetkisiz erişim sağlamayı veya finansal kazanç elde etmek için onları dolandırmayı amaçlayan hileli planları ifade eder. Bu dolandırıcılıklar sahte kripto para borsaları, dolandırıcılık paraları, halı çekme, pompala ve boşalt, yatırım ve madencilik dolandırıcılığı gibi çeşitli şekillerde olabilir. Ayrıca, kimlik avı, saadet zinciri, avans ücreti dolandırıcılığı ve sahte hesaplar aracılığıyla manipülasyon gibi taktikleri de içerebilirler. Genel olarak kripto para dolandırıcılıkları, kripto paraların sahte ve merkezi olmayan doğasından faydalanarak haksız kazanç elde etmek amacıyla takip edilemeyen dolandırıcılık faaliyetleri gerçekleştirmektedir (Başbüyük, 2023).

4.1.7. Kara para aklama

Metaverse'te kara para aklama dijital varlıkların anonimliği, merkeziyetsiz yapısı ve denetim eksiklikleri nedeniyle artan bir endişe kaynağıdır. Bu sanal evrenler, suçluların yasa dışı gelirleri gizlemesi ve aklaması için ideal platformlar haline gelmiştir. Metaverse'teki işlemler genellikle blokzincir tabanlıdır ve bu teknolojinin sağladığı şeffaflık ve izlenebilirlik avantajlarına rağmen, kara para aklamayı önlemek zorlayıcı olabilir. Dolandırıcılık, ikincil pazar yerleri, borsalar ve diğerleri aracılığıyla gerçekleştirilebilmektedir. Kara para aklama risklerinin azaltılması için bu platformlarda para gönderen/alınan hesaplarda uyumluluk taraması yapılması gerekmektedir. Ayrıca, metaverse evrenlerinde risklerin bütünsel bir şekilde tespit edilmesi, zincirler arasında birlikte çalışabilirlik arttıkça daha da önemli hale gelmektedir. Metaverse'de kara para aklamanın en yaygın yöntemlerinden biri, sanal varlıkların alım satımıdır. Suçlular, yasa dışı yollardan elde ettikleri parayı metaverse'de sanal araziler, NFT'ler veya diğer dijital varlıkları satın alarak aklayabilirler. Bu varlıklar daha sonra farklı platformlarda veya kullanıcılar arasında tekrar satılarak kara para yasal gelir gibi gösterilebilir. Blokzincir teknolojisinin sunduğu şeffaflık, teorik olarak işlemlerin izlenebilmesine olanak tanır. Ancak, metaverse'de yapılan işlemler, farklı cüzdanlar arasında küçük miktarlara bölünerek zincirleme transferlerle izlenmesi zor hale getirilebilir (Airlangga, 2024).

4.1.8. Fiyat şişirme (pump and dump)

Metaverse'de fiyat şişirme, yani "pump and dump" yöntemi, bir piyasa manipülasyon stratejisidir ve genellikle düşük hacimli veya yeni piyasaya sürülen varlıklar üzerinde uygulanır. Bu strateji, belirli bir varlığın değerini suni olarak yükseltmeyi (pump) ve ardından bu yükselmiş fiyat üzerinden varlığı satarak kâr elde etmeyi (dump) içerir. Dolandırıcılar, düşük hacimli veya nispeten bilinmeyen bir varlığı seçerler. Bu varlık genellikle fiyatı kolayca manipüle edilebilecek bir kripto para birimi, NFT veya dijital varlık olabilir. Bu varlığı büyük miktarlarda satın almaya başlarlar. Bu alımlar, piyasa talebini yapay olarak artırır ve varlığın fiyatının hızla yükselmesine neden olur. Bu aşamada,

genellikle sosyal medya, forumlar veya diğer iletişim kanalları üzerinden bu varlığın değerinin artacağına dair yoğun bir propaganda yapılır. Fiyatın hızla yükselmesi, diğer yatırımcıların da bu varlığa ilgi duymasına neden olur. Fiyat artışı, kaçırma korkusu yaratarak daha fazla yatırımcının alım yapmasını sağlar. Bu da fiyatın daha da yükselmesine neden olur. Fiyat yeterince yükseldiğinde, dolandırıcılar ellerindeki varlıkları satmaya başlarlar. Bu aşamada, büyük miktarlarda varlık piyasaya sürülür ve arz, talebi aşar. Böylelikle varlığın fiyatı hızla düşmeye başlar. Dolandırıcılar kârlarını alırken, daha sonra alım yapan yatırımcılar büyük zararlara uğrarlar. 2021 yılında kripto para borsalarında yaşanan Squid Game Token (SQUID) adlı kripto parada yaşanmıştır (Başbüyük, 2023).

Şekil 4.1. Doldur boşalt dolandırıcılığı (wallstreetmojo.com)

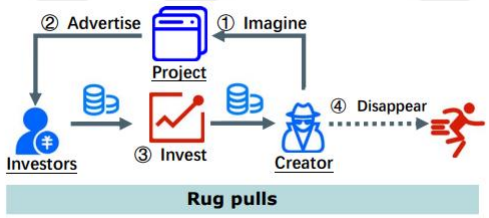
4.1.9. Yıkama ticareti (Wash Trading)

Bir piyasa katılımcısının aynı varlığı hem alıp hem de satarak, piyasada sanki varlığa yüksek bir talep varmış gibi sahte bir izlenim yaratmasıdır. Bu tür işlemler genellikle bir varlığın fiyatını yapay olarak artırmak veya işlem hacmini yüksek göstermek amacıyla yapılır. Yıkama ticareti, geleneksel finansal piyasalarda yasadışı kabul edilir, ancak merkeziyetsiz yapıdaki metaverse ve kripto para piyasalarında bu tür işlemler daha zor tespit edilmekte ve düzenleyici denetimler sınırlı olduğundan daha yaygın olabilmektedir. (Wu vd., 2023). 2022 yılında NFT pazar yeri olarak kurulan LooksRare platformu bu olayın yaşanan en büyük örneği olmuştur.

4.1.10. Halı çekme (Rug Pulls)

Rug Pulls, özellikle kripto para ve merkeziyetsiz finans (DeFi) dünyasında yaygın olarak kullanılan bir dolandırıcılık yöntemidir. Bu dolandırıcılık türünde, geliştiriciler bir kripto para veya DeFi projesi başlatır, yatırımcıları bu projeye çekmek için cazip vaatlerde bulunur ve ardından projenin arkasındaki likiditeyi veya fonları çekerek ortadan kaybolurlar. Yatırımcılar ellerinde değersiz tokenlar ile kalırken, dolandırıcılar elde ettikleri kazançlarla ortadan kaybolur.

Rug Pulls genellikle yeni ve popüler projelerde görülür. Bu projeler genellikle yüksek getiri vaat eder ve yatırımcıların ilgisini çekmek için hızlı bir şekilde büyür. Ancak, projeye dair şeffaflık eksikliği, likidite havuzunun kilitlenmemesi, anonim geliştiriciler gibi faktörler, bu tür dolandırıcılıkların gerçekleşmesine zemin hazırlar. 2021 yılında NFT alanında böyle bir dolandırıcılık olayı yaşandı. Evilved Apes NFT'lerinin yaratıcısı Evil Ape, yatırımcılardan 2,7 milyon dolar değerinde Ethereum (ETH) çalarak ortadan kayboldu (Kshetri, 2022).



Şekil 4.2. Halı çekme dolandırıcılığı (Lin, K., vd. 2023)

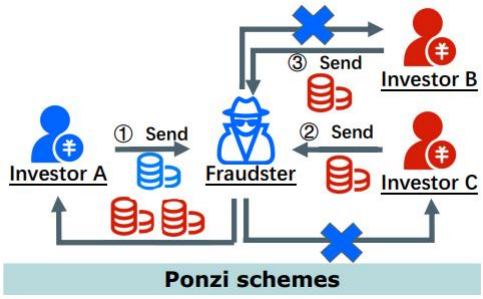
4.1.11. İçeriden bilgi alma (Inside trading)

Bir varlığın değerini etkileyebilecek kritik ve kamuya açıklanmamış bilgilere erişimi olan bireylerin bu bilgileri kullanarak kendi finansal avantajlarını maksimize etmelerini ifade eder. Bu durum genellikle adil olmayan bir avantaj yaratır ve yatırımcıların güvenini sarsabilir. Genellikle bir varlığın fiyatını etkileyebilecek büyük bir gelişmenin örneğin, yeni bir ürün lansmanı, büyük bir ortaklık veya önemli bir güncelleme gibi kamuya açıklanmadan önce öğrenilmesi ve bu bilgiye dayalı olarak varlık alım veya satımı yapılmasıyla gerçekleşir. Şirket yöneticileri, çalışanları veya projeye yakın kişiler, genellikle bu tür bilgilerin

kaynağıdır. Bu kişiler, piyasanın bu bilgiye nasıl tepki vereceğini öngörerek, kamuya açıklanmamış bilgilerle işlem yapıp, büyük karlar elde edebilir. Bilginin kamuya açıklanmasıyla birlikte varlık fiyatının artacağı veya düşeceği tahmin edilir ve buna göre pozisyon alınır. Bu konuya en güzel örnek ise popüler NFT pazarı olarak bilinen OpenSea'de 2021 yılında yaşanmıştır (Kshetri, 2022). OpenSea'nin bir çalışanının, platformda listelenmeden önce belirli NFT'leri gizlice satın aldığı ortaya çıktı. Bu çalışan, OpenSea'de listelenecek olan NFT'lerin değerinin hızla artacağını bildiği için, bu NFT'leri düşük fiyattan satın alarak listelendikten sonra kârla satıyordu.

4.1.12. Ponzi ve piramit şemaları

Ponzi ve piramit şemaları, finansal dolandırıcılıklar arasında en yaygın olan iki türdür. Her ikisi de yatırımcıları kandırmak ve dolandırıcıların kazanç sağlaması için kullanılan yasadışı planlardır. Ancak, bu iki şema arasında bazı temel farklar vardır. Ponzi şeması, adını 1920'lerde bu dolandırıcılığı popüler hale getiren Charles Ponzi'den alır (Trozze vd., 2022). Ponzi şemasında, dolandırıcılar yüksek getiriler vaat ederek yatırımcıları bir yatırım planına çeker. Ancak, bu getiriler aslında yeni yatırımcılardan toplanan paralarla ödenir. Ponzi şeması, sürdürülemez bir modeldir çünkü şemanın çalışabilmesi için sürekli olarak yeni yatırımcıların katılması gerekmektedir. Yeni yatırımcılar gelmediğinde veya yeterli yatırımcı bulunamadığında, şema çöker ve yatırımcılar büyük kayıplar yaşar. Piramit şeması, yatırımcıların doğrudan kazanç sağlamak yerine, daha fazla yatırımcıyı şemaya katılmaları için davet etmeleri üzerine kurulu bir dolandırıcılık modelidir. Her yeni katılımcı, üst seviyedeki kişilere ödeme yapar ve bu kişiler de kazançlarının bir kısmını üst seviyedeki kişilere aktarır. Piramit şeması, sürekli genişleyen bir yapı gerektirir ve belirli bir noktada yeni katılımcılar bulunamaz hale geldiğinde sistem çöker.



Şekil 4.3. Ponzi şeması (Lin, K., vd. 2023)

4.2. Metaverse'de Yaşanmış Dolandırıcılık Vakaları

4.2.1. LooksRare yıkama ticareti dolandırıcılığı

Metaverse'de gerçekleşen en büyük yıkama ticareti olaylarından biri, NFT (Non-Fungible Token) piyasasında yaşanmıştır. Özellikle 2021 ve 2022 yıllarında, NFT pazarlarında yıkama ticareti yaygın hale gelmiş ve bu tür olaylar dikkat çekici bir artış göstermiştir. Bu olayların en öne çıkan örneklerinden biri, LooksRare adlı NFT pazar yerinde meydana gelmiştir (Kshetri, 2022).

LooksRare, Ocak 2022'de kurulan bir NFT pazar yeri olup, kısa sürede büyük bir popülerlik kazanmıştır. Platform, kullanıcılarına sunduğu cazip ödüller ve teşviklerle tanınırken, bu teşvik sistemi aynı zamanda büyük çaplı yıkama ticaretine zemin hazırlamıştır. Yıkama ticareti, platformun işlem hacimlerinde büyük bir artışa neden olmuş, ancak bu hacmin büyük ölçüde gerçek alım satımlardan değil, yapay olarak şişirilmiş işlemlerden kaynaklandığı ortaya çıkmıştır.

LooksRare platformu, kullanıcılarına işlem hacmine dayalı olarak yüksek ödüller sunmaktaydı. Bu durum, kullanıcıları aynı NFT'leri tekrar tekrar alıp satarak işlem hacimlerini kasıtlı olarak artırmaya teşvik etti. Kullanıcılar, bu yapay işlem hacmi sayesinde platformun sunduğu teşviklerden maksimum fayda sağlamayı hedeflediler ve bu da büyük miktarda yıkama ticaretinin gerçekleşmesine yol açtı.

Yıkama ticareti LooksRare platformunda işlem hacminin büyük bir kısmını oluşturdu. Bu durum, platformun sağlıklı bir piyasa olup olmadığı konusunda soru işaretleri doğurdu ve kullanıcı güvenini sarstı. Sonuç olarak, LooksRare'deki işlem hacimleri gerçek piyasa koşullarını yansıtmaktan uzaklaştı.

Sonuçta bu durum, NFT piyasasının ne kadar kırılgan olduğunu ve düzenleyici çerçevelerin ne kadar eksik kaldığını açıkça ortaya koymuştur. LooksRare gibi platformlarda yıkama ticareti ve benzeri manipülasyonların ne kadar kolay yayılabileceğini gözler önüne seren bu durum, aynı zamanda piyasa katılımcıları için önemli bir uyarı niteliği taşımaktadır.

Bu olay, metaverse ve kripto varlık piyasalarında daha sağlam düzenleyici çerçevelerin ne kadar kritik olduğunu vurgularken, kullanıcıların da bu tür manipülasyonlara karşı daha dikkatli olmaları gerektiğini hatırlatmaktadır. Yıkama ticareti gibi olayların tekrar yaşanmasını önlemek için, platformların daha sıkı izleme mekanizmaları ve düzenleyici önlemler uygulaması kaçınılmaz hale gelmiştir. Bu tür önlemler, yalnızca piyasanın şeffaflığını artırmakla kalmayacak, aynı zamanda yatırımcı güvenini de güçlendirecektir.

4.2.2. Squid game token doldur boşalt dolandırıcılığı

Squid Game Token (SQUID), popüler Netflix dizisi Squid Game atıfta bulunarak yaratılan bir kripto para birimiydi, ancak kısa sürede bir pump and dump skandalına dönüştü.

SQUID, Ekim 2021'de piyasaya sürüldü ve Netflix dizisinin başarısından faydalanarak hızla popülerlik kazandı. Lansmanının hemen ardından, tokenın değeri astronomik seviyelere ulaştı. Geliştiriciler ve manipülatörler, sosyal medya ve çeşitli platformlar üzerinden tokenın yoğun bir şekilde tanıtarak, tokenın gelecekte büyük değer kazanacağına dair vaatlerde bulundular.

Tokenın değeri kısa süre içinde %240.000'in üzerinde arttı ve bu aşamada birçok yatırımcı SQUID tokenı satın aldı. Ancak, bu yatırımcılar tokenlarını satmakta

zorlandılar, çünkü tokenın akıllı sözleşme kodu, satış işlemlerini engelleyecek şekilde programlanmıştı.

Kasım 2021'de tokenın fiyatı zirveye ulaştığında, geliştirici ekip ellerindeki tüm tokenları satarak piyasadan çekildi. Bu ani satış işlemi, SQUID'in değerinin saniyeler içinde sıfıra inmesine neden oldu ve birçok yatırımcı büyük zararlar yaşadı.

Squid Game Token olayı, metaverse ve kripto para piyasalarının ne kadar savunmasız olabileceğini gözler önüne serdi. Pump and dump stratejilerinin ne kadar yıkıcı sonuçlar doğurabileceğini ortaya koyarak, hem yatırımcıların daha dikkatli olmaları gerektiğini hem de bu tür olayların önüne geçmek için daha sıkı düzenlemelere ihtiyaç duyulduğunu bir kere daha göstermiş oldu. Yatırımcıların, özellikle hızla popüler hale gelen ve yeterince araştırılmamış projelere yatırım yaparken çok daha temkinli olmaları gerektiği bir kez daha kanıtlandı.

4.2.3. Evolved apes halı çekme dolandırıcılığı

Evolved Apes adlı NFT projesi, metaverse alanında gerçekleşmiş en büyük halı çekme (rug pull) skandallarından biri olarak tarihe geçmiştir. Bu proje, NFT avatarlarına dayalı bir dövüş oyunu olarak tanıtıldı ve "Evil Ape" takma adıyla bilinen geliştirici tarafından büyük bir ilgiyle lanse edildi. Proje, yatırımcılar arasında hızla popülerlik kazandı ve toplamda 2,7 milyon doların üzerinde fon toplandı. Ancak, kısa bir süre sonra, geliştirici topladığı fonlarla birlikte ortadan kayboldu ve yatırımcıları büyük bir hayal kırıklığına uğrattı.

Bu skandal, NFT ve metaverse topluluklarında büyük bir şok yarattı. Projeye yatırım yapanlar, ellerinde sadece değersiz NFT' lerle kaldılar ve proje için vaat edilen oyun ve diğer geliştirmeler hiçbir zaman hayata geçirilmedi. Evolved Apes olayı, yatırımcıların metaverse projelerine yatırım yaparken çok daha temkinli olmaları gerektiğini bir kez daha gözler önüne serdi.

Halı çekme skandalları hem kripto para dünyasında hem de metaverse alanında yatırımcılar için ciddi bir risk oluşturmaktadır. Yatırımcıların, herhangi bir projeye yatırım yapmadan önce, projenin arkasındaki ekibi, teknik detaylarını, likidite kilitleme durumunu ve topluluk geri bildirimlerini dikkatlice incelemeleri son derece önemlidir. Özellikle metaverse gibi yeni ve hızla gelişen alanlarda, bu tür dolandırıcılık girişimlerine karşı dikkatli olmak hayati bir öneme sahiptir. Bu olay, yatırımcıların yalnızca vaat edilen getirilerle değil, aynı zamanda projenin gerçekliğini ve sürdürülebilirliğini de değerlendirmeleri gerektiğini net bir şekilde ortaya koymuştur.

4.2.4. OpenSea içeriden bilgi dolandırıcılığı

Eylül 2021'de, OpenSea'de bir çalışanın, platformda listelenmeden önce belirli NFT'leri gizlice satın aldığı ortaya çıkması, büyük bir skandala yol açtı. Bu çalışan, OpenSea'de listelenecek NFT'lerin değerinin hızla artacağını önceden bildiği için, bu NFT'leri düşük fiyattan alıp listelendikten sonra kârla satıyordu.

Çalışan, OpenSea'nin ana sayfasında tanıtılacak NFT'leri önceden bilme avantajını kullanarak bu NFT'leri satın alıyor ve tanıtımın ardından bu NFT'leri daha yüksek fiyatlara satarak kâr elde ediyordu. Bu durum, klasik bir içeriden bilgiye dayalı ticaret örneği olarak kabul edildi.

Olayın ortaya çıkmasıyla birlikte, OpenSea hızlı bir şekilde bir açıklama yaparak ilgili çalışanı işten çıkardı. Ayrıca, platformun gelecekte benzer olayları önlemek için ek güvenlik önlemleri alacağı belirtildi. Ancak, bu skandal NFT topluluğunda ciddi bir güvensizlik yarattı ve OpenSea'nin itibarını zedeledi.

Olay, kripto dünyasında içeriden bilgiye dayalı ticaretin nasıl gerçekleşebileceğine dair bir uyarı niteliği taşıdı. OpenSea skandalı, kripto ve metaverse dünyasında daha güçlü düzenleyici çerçevelerin gerekliliğini bir kez daha gündeme getirdi.

Yaşananlar, metaverse ve NFT pazarlarının hızla büyüdüğü bir dönemde içeriden bilgiye dayalı ticaretin ne kadar ciddi sonuçlar doğurabileceğini göstermiş oldu. OpenSea, skandalın ardından güvenlik protokollerini güçlendirdi, ancak bu olayın yarattığı güven kaybı, diğer platformlar için de önemli bir ders oldu.

4.2.5. Forsage ponzi şeması dolandırıcılığı

Forsage, Ethereum blokzinciri üzerinde çalışan bir akıllı kontrat sistemi olarak tanıtılarak, katılımcılara yüksek kazanç vaatleri sunuyordu. Bu sistem, kullanıcıların Ethereum yatırımı yaparak katılım sağladığı ve yeni katılımcılar getirmeleri durumunda daha fazla Ethereum kazanacakları vaadiyle teşvik edildiği bir yapı oluşturdu. Ancak, Forsage aslında bir ponzi şemasıydı; yani eski yatırımcılara yapılan ödemeler, yeni katılımcılardan gelen fonlarla finanse ediliyordu.

Forsage, kısa bir süre içinde milyonlarca dolarlık Ethereum toplamayı başardı. Ancak, yeni yatırımcı akışı azaldığında, sistem çöküşe geçti ve birçok katılımcı ciddi mali kayıplar yaşadı. Bu olay, blockchain ve metaverse platformlarında ponzi şemalarının ne kadar hızla yayılabileceğini ve kullanıcıların bu tür sistemlere karşı son derece dikkatli olmaları gerektiğini gösteriyordu.

ABD Menkul Kıymetler ve Borsa Komisyonu (SEC) ve diğer uluslararası düzenleyici kurumlar, Forsage'ı bir ponzi şeması olarak tanımladı ve bu sisteme karşı soruşturmalar başlattı. Forsage, metaverse ve kripto dünyasında gerçekleşen en büyük ponzi şemalarından biri olarak tarihe geçti ve bu tür olayların önüne geçmek için daha güçlü düzenleyici mekanizmaların gerekliliğini bir kez daha gündeme getirdi.

4.3. Dolandırıcılıkları Önleme Stratejileri

Metaverse'te dolandırıcılığı önlemeye yönelik stratejiler arasında ilk akla gelen blokzincir tabanlı güvenlik ve kimlik doğrulamadır. Bununla birlikte ML ve AI tabanlı tespit sistemleri gibi yeni teknolojilerin kullanılması, özellikle organize

edilecek eğitim programları ile kullanıcı farkındalığı oluşturulması, düzenleyici ve hukuk alanlarının hem hızlandırılması hem de güçlendirilmesi, gelişen yeni teknolojileri altyapılara entegre ederek, altyapıların güçlendirilmesi, metaverse platformlarına girişte kullanılan cihazların güvenliği gibi konular söylenebilir.

4.3.1. Blokzincir tabanlı güvenlik ve kimlik doğrulama

4.3.1.1. Merkeziyetsiz kimlik doğrulama

Metaverse'deki merkezi olmayan kimlik yönetimi büyük ölçüde blok zinciri teknolojisine dayanır. Güvenilir bir kimlik altyapısı oluşturmak için güven çapalarını, itibar sistemlerini, çok faktörlü kimlik doğrulamayı ve merkezi olmayan bir kimlik yönetim sistemini bir araya getirir. Bu yaklaşım, kullanıcıların dijital kimlikleri üzerinde kontrol sahibi olmalarını sağlayarak metaverse'de kimlik hırsızlığı, yetkisiz erişim ve dolandırıcılık faaliyetleri olasılığını azaltır. Ayrıca akıllı sözleşmeler, erişim kontrol politikalarının yönetilmesi ve uygulanmasında çok önemli bir rol oynayarak sistemi otomatik ve tek hata noktalarına karşı dirençli hale getirir (Rajawat vd., 2023).

4.3.1.2. Akıllı kontratlarla dolandırıcılık tespiti

Blokzincirleri üzerinde çalışan akıllı kontratlar, işlemlerin otomatik olarak ve belirli kurallara göre gerçekleşmesini sağlar. Bu kontratlar, dolandırıcılık riskini azaltmak için işlemleri önceden tanımlanmış kurallara göre izler. Örneğin, NFT satışları gibi işlemlerde akıllı kontratlar, işlemin yalnızca taraflar belirli koşulları karşıladığında tamamlanmasını sağlayarak dolandırıcılığı önleyebilir. Ayrıca, blokzincir teknolojisi ile desteklenen akıllı kontratlar finansal işlemlerde şeffaflık, güvenlik ve verimlilik sağlar ve uyumluluk kontrollerini ve düzenleyici raporlama işlevlerini otomatikleştirerek manuel çabaları azaltır ve finansal analitik ve operasyonlarda doğruluğu artırır. (Saivasan ve Lokhande., 2023).

4.3.2. Makine öğrenimi ve yapay zekâ tabanlı tespit sistemleri

4.3.2.1. Anomali tespiti ile dolandırıcılık önleme

Anomali tespiti, finansal işlemlerdeki düzensiz ve potansiyel olarak hileli modellerin belirlenmesine yardımcı olduğu için dolandırıcılığın önlenmesinde çok önemli bir yöntemdir. Grafikler, derin öğrenme ve özellik mühendisliğinin bir kombinasyonunu kullanarak, anomali tespit teknikleri kötü niyetli davranışları etkili bir şekilde belirleyebilir ve kullanıcıların varlıklarını koruyabilir. Ayrıca, son zamanlarda yapılan çalışmalar dijital işlemlerdeki anormallikleri tespit etme ve dolandırıcılığı önleme konusunda veri odaklı yaklaşımların, ML ve AI potansiyelini vurgulamıştır. Bu nedenle, anomali tespit yöntemlerinden yararlanmak dolandırıcılığın önlenmesini önemli ölçüde artırabilir (Airlangga, 2024). ML algoritmaları, büyük veri kümeleri üzerinde anomali tespiti yaparak, normal kullanıcı davranışlarından sapma gösteren dolandırıcılık faaliyetlerini tespit edebilir. Kullanıcı işlemleri ve davranışları sürekli olarak izlenir ve anormal etkinlikler tespit edildiğinde sistem uyarı verir. Örneğin, bir kullanıcının aniden çok sayıda farklı cüzdandan NFT alması, olası bir yıkama ticareti (wash trading) faaliyeti olarak tespit edilebilir.

4.3.2.2. Birleştirilmiş öğrenme (federated learning) ile dolandırıcılık tespiti

Birleştirilmiş öğrenme ile merkezi olmayan dolandırıcılık tespiti, finansal hizmetlerin güvenliğini artırmak için umut verici bir yaklaşımdır. Birleştirilmiş öğrenmeden yararlanarak, dolandırıcılık tespiti için kullanılan veriler merkezi bir sunucuya aktarılmadan uç cihazlarda kalabilir ve böylece güvenlik ihlali riskini azaltır. Ayrıca, blok zinciri teknolojisinin federe öğrenme ile entegre edilmesi, güvenli ve özel veri paylaşım gereksinimlerine olanak tanıyarak dolandırıcılık tespit sürecinin güvenliğini daha da artırır. Kullanıcıların işlem verileri merkezi bir noktada toplanmadan, her kullanıcının cihazında model eğitimi yapılır. Bu sayede gizlilik korunur ve model, daha geniş bir veri seti

üzerinde eğitilmiş olur, bu da dolandırıcılık tespitini daha etkin hale getirir (Chatterjee vd., 2023).

4.3.3. Kullanıcı farkındalığı ve eğitim programları

4.3.3.1. Farkındalık eğitimleri

Kullanıcı farkındalığı ve eğitim programları, metaverse'deki bireylerin emniyeti ve güvenliği için çok önemlidir. Şirketlerin ve hükümetlerin dijital okuryazarlığı artırmaya yönelik araçlar ve kaynaklar geliştirmesi ve suçların kolayca bildirilmesine yönelik destek mekanizmaları sağlaması önemlidir. Ayrıca, kullanıcıların metaverse'ü güvenli bir şekilde kullanabilmelerini sağlamak için eğitim programlarının farklı demografik kategorilere ve durumlara göre uyarlanması gerekmektedir. Düzenli olarak güncellenen eğitim materyalleri, web seminerleri ve etkileşimli öğrenme modülleri aracılığıyla kullanıcılar, kimlik avı saldırıları, sahte projeler ve sosyal mühendislik teknikleri gibi tehditlere karşı bilinçlendirilmelidir (Al-Tkhayneh, K2023).

4.3.3.2. Davranış ödüllendirme

Kullanıcıların güvenli davranışlarını teşvik etmek amacıyla bir ödüllendirme sistemi oluşturmak. Kullanıcılar, güvenli işlemler yaptıklarında veya dolandırıcılık girişimlerini bildirdiklerinde ödüller kazanabilirler. Bu, kullanıcıların daha dikkatli olmasını sağlar ve dolandırıcılık girişimlerinin hızla tespit edilmesine katkıda bulunabilir.

4.3.4. Düzenleyici ve hukuki çerçevenin güçlendirilmesi

4.3.4.1. Uluslararası iş birliği

Metaverse ortamındaki dolandırıcılık faaliyetleri, ulusal sınırları aştığından, uluslararası iş birliği gereklidir. Uluslararası düzenleyici çerçeveler geliştirilmelidir. Metaverse'deki dolandırıcılıklarla mücadele için küresel polis iş

birliği stratejileri geliştirebilir. Bu, ulusal yasaların ötesine geçen bir düzenleyici çerçeve ile desteklenmelidir.

4.3.4.2. Yasal düzenlemelerin güncellenmesi

Düzenleyici ve yasal çerçeve, düzenleme ve yönetişim boşlukları ele alınarak, yeni lisanslama gereklilikleri getirilerek, sektörde fikir birliği sağlanarak ve düzenleyici plan optimize edilerek güçlendirilebilir. Ayrıca, savunmasız grupları korumak için proaktif yönetişim ve düzenleme uygulanmalıdır. Daha küçük sağlayıcıların pazar dışına itilmesini önlemek için de düzenleyici çerçeveye üçüncü bir kategori eklenmelidir. Bu, yasal çerçevenin etkinliğini korurken metaverse'de kara para aklama ve terörizmin finansmanının önlenmesine yardımcı olacaktır.

4.3.5. Teknolojik altyapının güçlendirilmesi

4.3.5.1. Güvenli ağ altyapısı

Teknolojik altyapının güçlendirilmesi için hızlı teknolojik ilerlemelere sürekli uyum sağlanması, yenilikçi finansal ürünlerin geliştirilmesi ve aktif keşif ve iş birliğine ihtiyaç duyulduğu açıktır. Dijital dünyanın etkin bir şekilde kullanılabilmesi için son derece güvenli ve emniyetli internet erişiminin, ölçeklenebilir ağların ve tahmine dayalı analizlerin sağlanması önemlidir. Bununla birlikte, ileri teknolojilerin benimsenmesi ve güvenlik açıklarının giderilmesine yönelik politikaların geliştirilmesi, teknolojik altyapının güçlendirilmesi açısından büyük önem taşımaktadır.

4.3.5.2. VR/AR cihazlarının güvenliği

VR/AR cihazlarının güvenliği, bu teknolojilerle ilişkili potansiyel gizlilik ihlalleri ve güvenlik ihlalleri nedeniyle çok önemli bir endişe kaynağıdır. Cihazlar bağlamsal verileri, biyometrik bilgileri ve kişisel verileri toplayabilir, bu da onları bilgi sızıntısı, şifre hırsızlığı ve yetkisiz veri ihlalleri gibi tehditlere karşı

savunmasız hale getirir. Metaverse'ün güvenliğini güçlendirmek için cihaz üreticilerinin güvenlik hükümlerini donanıma entegre etmeleri önemlidir. Gömülü sistem güvenliği ve güvenilir yürütme ortamlarının uygulanması, kötü niyetli davranışlara karşı korunmaya yardımcı olabilir ve cihazlardaki verilerin güvenli bir şekilde işlenmesini sağlayabilir. Ayrıca, yeterli güvenlik özelliklerine sahip cihazların dikkatli bir şekilde seçilmesi ve etkili kimlik doğrulama yöntemlerinin geliştirilmesi, kullanıcı gizliliğini korumak ve siber saldırıları önlemek için gerekliliktir.

5. YÖNTEM

Yöntem bölümünde; araştırmanın modeli, çalışma grubu, veri toplama araçlarından kişisel bilgi formu, verilerin toplanma süreci, analiz süreci detaylı biçimde ele alınmış ve ek olarak araştırmanın geçerliliği ve güvenirliği başlığı altında araştırma sürecine dair detaylara değinilmiştir.

5.1. Araştırmanın Modeli

Bu araştırmada, Metaverse'te dolandırıcılık riskleri, güvenlik açıkları ve firmaların bu konudaki algılarını ve çözüm yaklaşımlarını anlamak için betimsel bir araştırma modeli benimsenmiştir. Çalışma hem nitel hem de nicel veri toplama yöntemlerini kullanarak karma bir yaklaşımı benimsemektedir.

Araştırmanın teorik çerçevesi, Metaverse ortamında karşılaşılan dolandırıcılık türlerinin ve bu ortamın güvenlik açıklarının kapsamlı bir şekilde anlaşılmasını hedefleyen literatür taramasına dayanmaktadır. Bu çerçevede, dolandırıcılık tespitine yönelik önlemler, teknolojik altyapı gereksinimleri ve düzenleyici çerçevelerle ilgili varsayımlar test edilmiştir.

5.2. Çalışma Grubu

Araştırma kapsamında, Metaverse teknolojileriyle ilişkili farklı sektörlerden profesyoneller hedeflenmiştir. Çalışma grubu, bilgi teknolojileri, finans, telekomünikasyon ve reklam gibi sektörlerden 53 katılımcıdan oluşmaktadır. Katılımcılar, yaş aralıkları, eğitim durumları ve sektörel pozisyonları gibi demografik değişkenler açısından çeşitlilik göstermektedir.

Örneklem seçiminde kolayda örnekleme yöntemi kullanılmıştır. Katılımcıların Metaverse hakkında temel bilgiye sahip olmaları ve bu alanda belirli bir süre faaliyet göstermiş olmaları, seçimin temel kriterlerini oluşturmuştur. Çalışmaya katılan bireyler arasında eğitim uzmanları, iş geliştirme uzmanları, teknik

uzmanlar ve çeşitli sektörlerde uzun yıllar deneyime sahip yöneticiler bulunmaktadır.

5.3. Veri Toplama Aracı

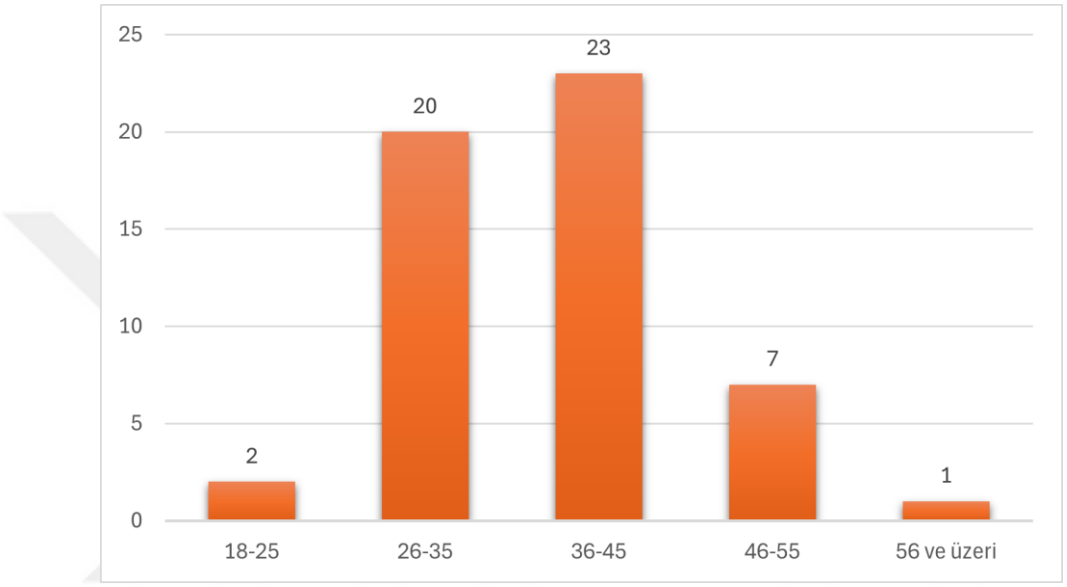
Veri toplama aracı olarak, Metaverse ve dolandırıcılık konularını ele alan 29 sorudan oluşan bir anket kullanılmıştır. Anket hem kapalı uçlu hem de açık uçlu soruları içermektedir. Kapalı uçlu sorular, katılımcıların dolandırıcılık riskleri, karşılaşılan zorluklar ve dolandırıcılık önleme stratejilerine ilişkin tutumlarını ölçmek amacıyla tasarlanmıştır.

Açık uçlu sorular, katılımcıların kendi deneyimlerini, görüşlerini ve önerilerini daha ayrıntılı bir şekilde ifade etmelerine olanak tanımıştır. Anket soruları, literatür taraması ve uzman görüşleri doğrultusunda geliştirilmiş ve geçerlilik açısından bir ön test uygulanmıştır. Anket, çevrim içi bir platform üzerinden uygulanmış ve bu yöntemle katılımcıların rahatlıkla erişim sağlaması hedeflenmiştir.

6. BULGULAR

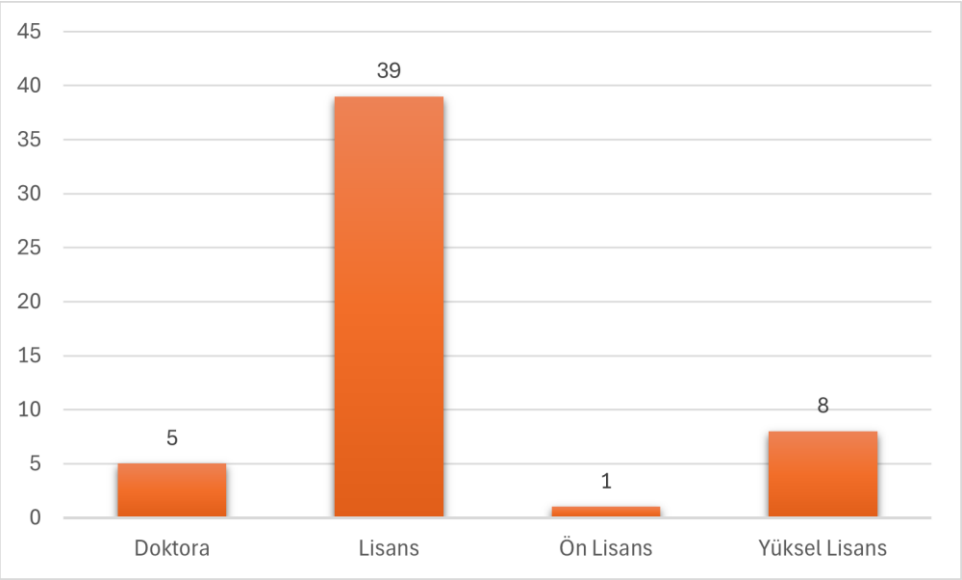
Bu bölümde, anket sonuçlarına dayanarak Metaverse'te dolandırıcılık algıları, karşılaşılan zorluklar ve çözüm önerilerine ilişkin bulgular sunulmuştur.

6.1 Demografik Bulgular



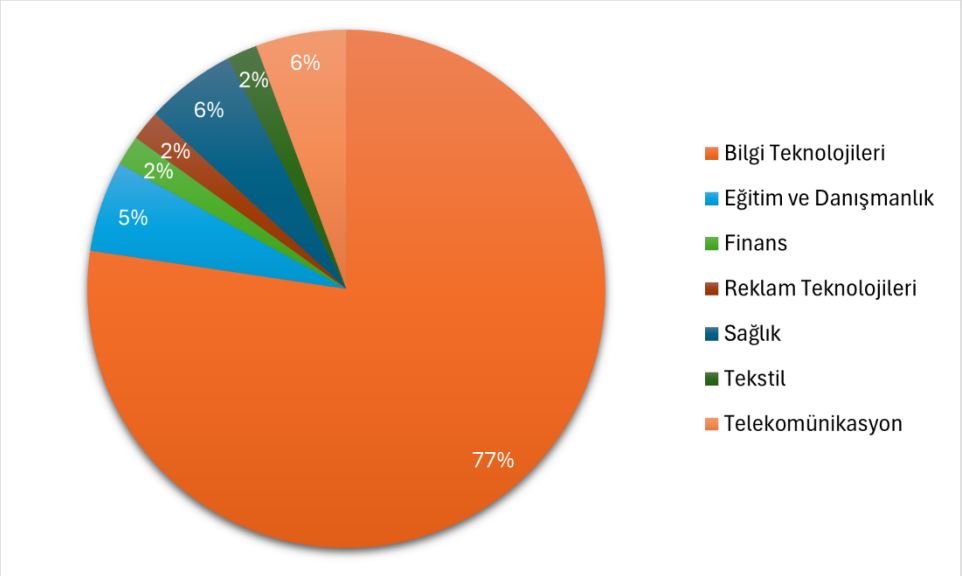
Şekil 6.1. Katılımcı yaş aralığı

Anket katılımcılarının yaş dağılımı incelendiğinde, %40'tan fazlasının 36-45 yaş aralığında olduğu görülmektedir. Bunu sırasıyla 26-35 yaş aralığı %35 ve 46-55 yaş aralığı %12 takip etmektedir. Katılımcılar arasında en düşük temsil oranı, 56 yaş ve üzeri ile 18-25 yaş aralığındadır. Bu dağılım, çalışma grubunun genel olarak kariyerlerinin orta seviyesinde olan bireylerden oluştuğunu göstermektedir.



Şekil 6.2. Katılımcı eğitim durumu

Katılımcıların eğitim düzeylerine ilişkin dağılım, büyük çoğunluğun lisans derecesine sahip olduğunu %74 göstermektedir. Ayrıca, katılımcıların %15'i yüksek lisans, %9'u ise doktora düzeyinde eğitim almıştır. Bu durum, Metaverse gibi altyapısı ileri düzey teknolojilerle ilgili bilgi ve tecrübe gerektiren kişilerin genellikle yüksek bir akademik yeterliliğe sahip olduğunu ortaya koymaktadır.



Şekil 6.3. Katılımcı sektör grafiği

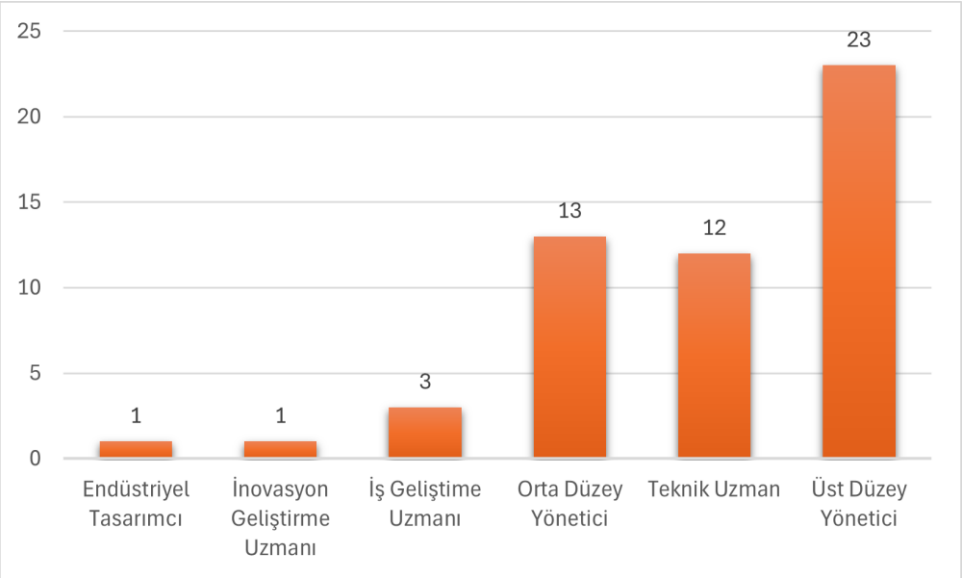
Katılımcıların, bilgi teknolojisi sektöründe çalışma oranı %77 ile en yüksek seviyede olması, bu sektörün Metaverse teknolojilerinin gelişiminde öncü rol oynayan bir alan olarak öne çıkmasını sağlamaktadır.

Katılımcıların önemli bir kısmını ise %6 telekomünikasyon, %6 sağlık, %5 eğitim ve danışmanlık, sektörleri oluşturmaktadır.

Telekomünikasyon sektörü altyapı sağlayıcıları arasında yer almaktadır ve Metaverse uygulamalarının teknik gereklilikleriyle doğrudan ilişkilidir. Metaverse, sağlık sektöründeki hizmetleri iyileştirmek, daha erişilebilir hale getirmek ve yenilikçi yöntemlerle sunmak için bir fırsat olabilir. Eğitim ve danışmanlık firmaları ise Metaverse'te müşterileri için sanal ticaret çözümleri, dijital kimlik yönetimi veya Metaverse platformlarının adaptasyonu konusunda rehberlik sağlayabilir.

Bu dağılım, Metaverse teknolojilerinin yalnızca teknik sektörlerle sınırlı olmadığını, aynı zamanda reklam, tekstil, finans ve telekomünikasyon gibi daha geniş bir endüstriyel yelpazede benimsenmeye başladığını göstermektedir.

Bilgi teknolojileri sektörünün bu alanda öncü olması beklenen bir bulgu olmasına karşın, diğer sektörlerden katılımcıların da bu alana ilgisinin olması, Metaverse'ün farklı uygulama alanlarında hızla yaygınlaşmakta olduğunun bir göstergesidir.

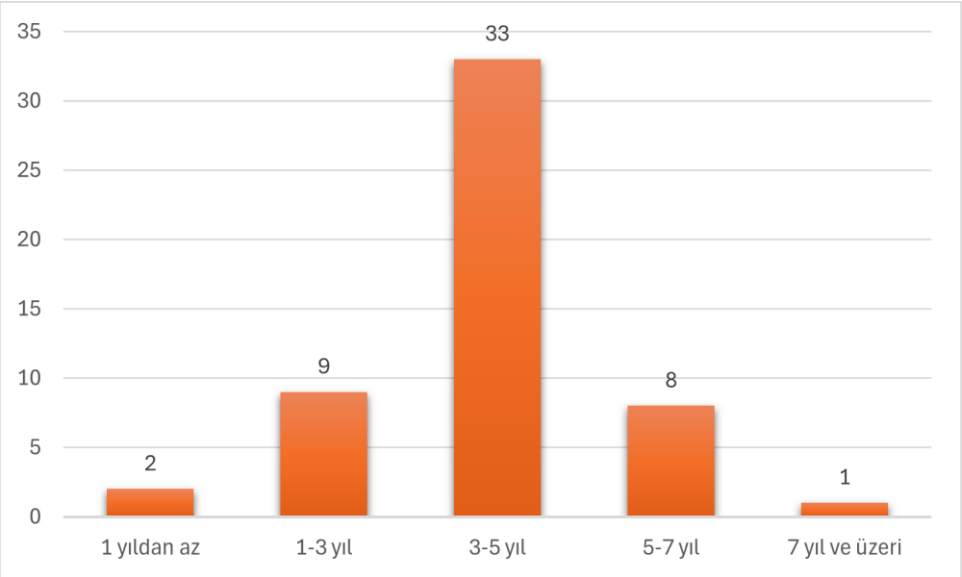


Şekil 6.4. Katılımcı çalışma pozisyonu

Üst ve orta düzey yöneticilerden oluşan %67'lik kesim, Metaverse ile ilgili stratejik kararlar ve güvenlik politikaları oluşturma sürecinde etkili bir rol oynamaktadır. Bu durum, katılımcıların büyük çoğunluğunun organizasyonlarında karar alıcı pozisyonlarda bulunduğunu ve Metaverse güvenlik algılarını daha geniş bir perspektiften değerlendirme eğiliminde olduklarını göstermektedir. 12 katılımcı, teknik uzman olarak anketi cevaplamıştır. Teknik uzmanların katılım oranı, Metaverse platformlarının güvenlik altyapısına dair teknik bilgilerin analize entegre edilmesine olanak tanımaktadır. Bu grup, dolandırıcılık tespit sistemlerinin tasarımı ve uygulanmasında doğrudan rol oynadığını göstermektedir. İş geliştirme uzmanları, endüstriyel tasarımcılar ve inovasyon geliştirme uzmanlarından oluşan %10'luk kesim, Metaverse platformlarının ticari fırsatlarını ve yenilikçi yönlerini değerlendiren bir perspektif sunmaktadır. Bu gruptan gelen veriler, güvenlik önlemlerinin yalnızca teknik değil, aynı zamanda ticari sürdürülebilirlik açısından da ele alınması gerektiğini vurgulamaktadır.

Çeşitli pozisyonlardan gelen katılımcılar, Metaverse güvenlik algısının çok boyutlu bir şekilde incelenmesini sağlamaktadır. Yönetim, teknik altyapı, iş geliştirme ve tasarım gibi farklı alanlardan gelen geri bildirimler, Metaverse

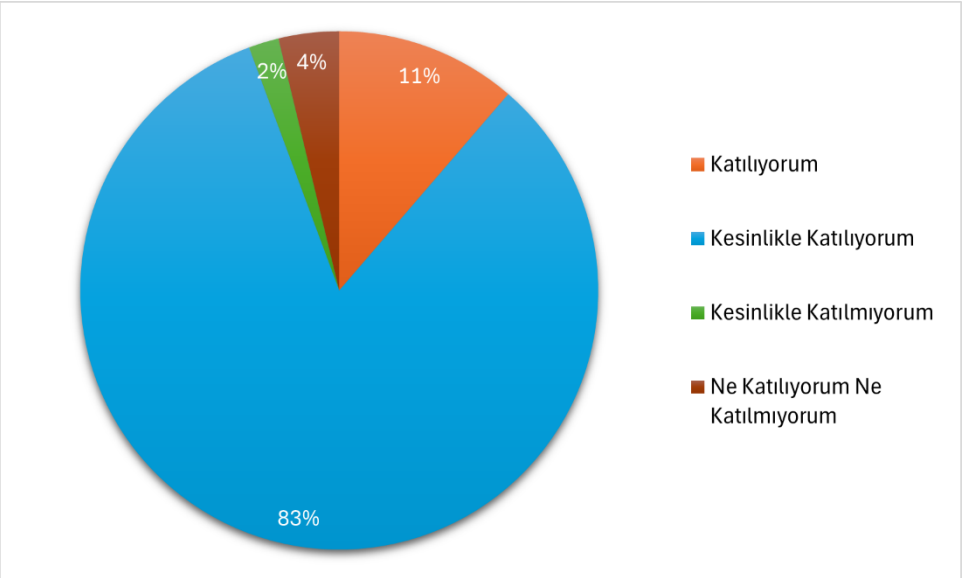
ekosisteminde dolandırıcılık risklerinin ve güvenlik ihtiyaçlarının kapsamlı bir şekilde anlaşılmasını kolaylaştırmaktadır.



Şekil 6.5. Firma faaliyet süresi

3-5 yıl cevabını veren katılımcıların %62'sini oluşturan grup, Metaverse platformlarının yaygınlaşmaya başladığı dönemde kurulan firmaları temsil etmektedir. Metaverse'ün yaygınlaşmasının başlangıcı, yaklaşık olarak son 5 yıl içinde hızlanmıştır. Bu durum, 3-5 yıl arası faaliyet gösteren firmaların (%62) bu süreçte öncü oyuncular haline geldiğini göstermektedir. Bu firmalar, sektörde sağlam bir yer edinmeye çalışırken Metaverse'teki güvenlik açıklarıyla mücadele etmek zorunda kalabilir. Daha önce kurulan firmalar (5 yıl ve üzeri) ise, bu teknolojilere adaptasyonda ilk dalgayı temsil etmektedir. 1-3 yıl arası faaliyet gösteren firmalar ise, yenilikçi iş modellerini benimseyip hızlı bir başlangıç yapmış ve son dalgayı temsil etmektedir.

6.2 Metaverse Güvenlik Risklerine İlişkin Algılar

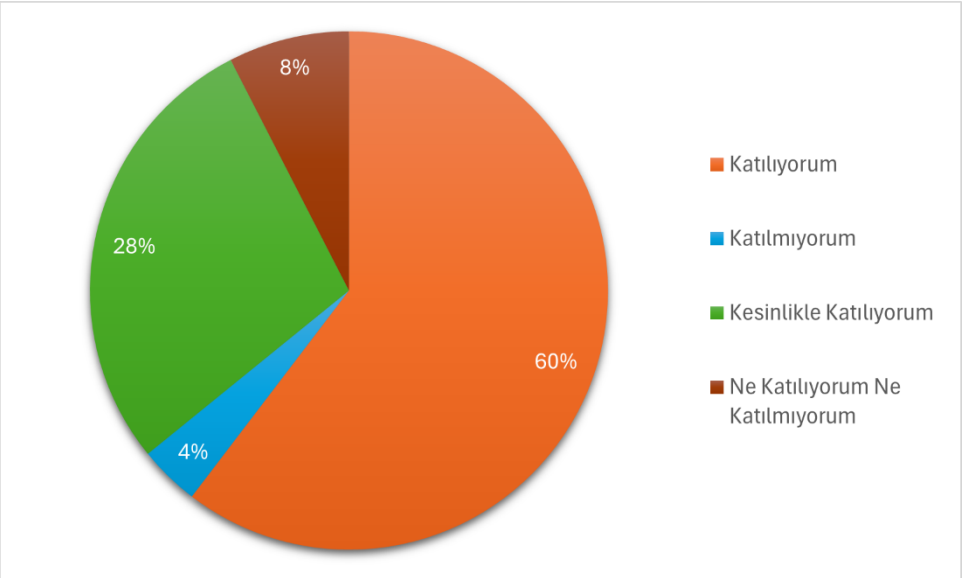


Şekil 6.6. Katılımcı metaverse teknolojileri bilgi düzeyi

Katılımcıların %94'lük kısmı, Metaverse teknolojileri hakkında bilgi sahibi olduklarını ifade etmiştir. Bu, katılımcıların büyük bir kısmının Metaverse teknolojileriyle profesyonel düzeyde ilgilendiğini ve bu alandaki kavramları iyi bir şekilde anladığını göstermektedir. Güçlü bilgi düzeyi, Metaverse platformlarında dolandırıcılık risklerini ve güvenlik ihtiyaçlarını doğru bir şekilde analiz etme ve çözüm üretme potansiyelini artırmaktadır.

Kararsızım ve katılmıyorum yanıtlarını veren katılımcılar, Metaverse teknolojileri konusunda daha düşük bilgi düzeyine sahiptir. Bu durum, bilgiye erişim eksikliği, teknolojilere maruz kalma süresinin kısalığı veya eğitim fırsatlarının yetersizliğinden kaynaklanabilir.

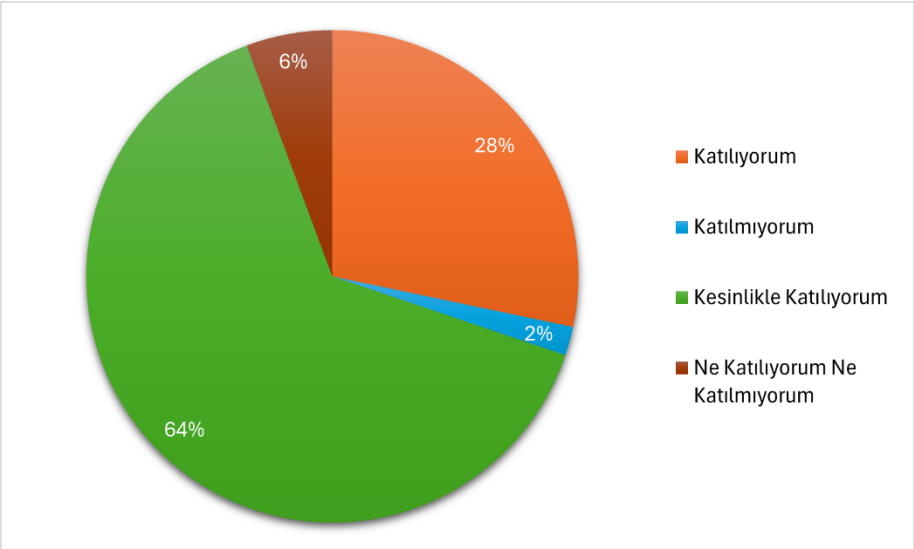
Bu grup, Metaverse ekosistemindeki dolandırıcılık tespiti ve güvenliğiyle ilgili farkındalık artırıcı programlara ve teknik eğitimlere ihtiyaç duymaktadır.



Şekil 6.7. Katılımcı güvenlik ve dolandırıcılık riskleri bilgi düzeyi

Anket sonuçlarına göre, katılımcıların büyük bir kısmı %88, Metaverse güvenlik riskleri ve dolandırıcılık konularında bilgi sahibi olduklarını ifade etmiştir. Katılımcıların %8'i bu konuda tarafsız bir duruş sergilerken, yalnızca %4'ü bu riskler hakkında yeterli bilgiye sahip olmadıklarını belirtmiştir.

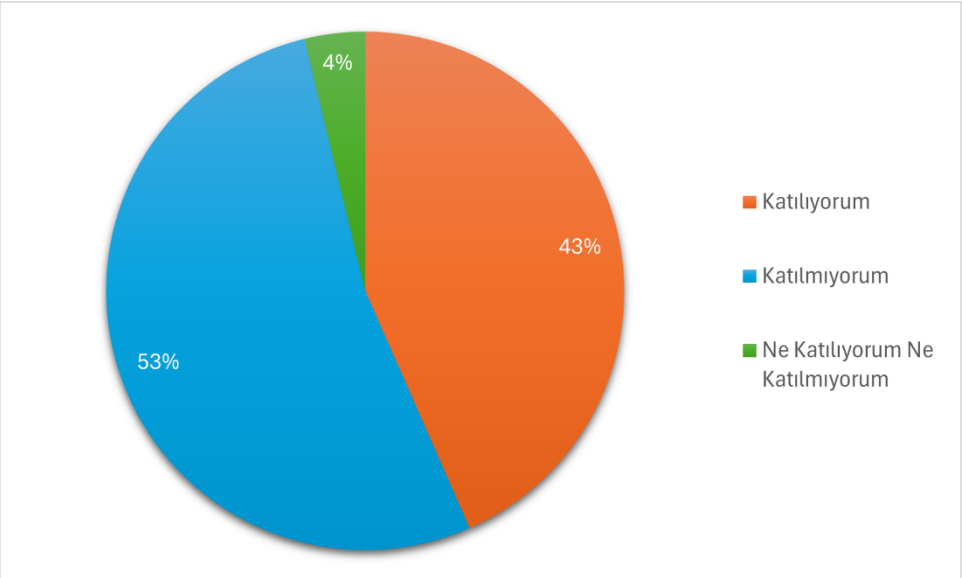
Bu bulgu, Metaverse ile ilgilenen profesyonellerin, güvenlik risklerinin farkında olduğunu ve bu risklerin yönetimi konusunda bilinçlendirilmeye uygun bir grubu temsil ettiğini göstermektedir. Ancak, tarafsız veya bilgi eksikliği bildiren bir kesimin bulunması, farkındalık eğitimlerinin önemini vurgulamaktadır.



Şekil 6.8. Platformların dolandırıcılığa karşı savunmasızlığı

Metaverse platformlarının dolandırıcılığa karşı savunmasız olduğuna ilişkin algılar incelendiğinde ise, katılımcıların %92'si bu görüşe "katılıyorum" veya "kesinlikle katılıyorum" ifadeleriyle destek vermiştir. Katılımcıların yalnızca %8'i, bu savunmasızlığın bir sorun teşkil etmediğini düşünmektedir.

Bu sonuç, platformların mevcut güvenlik altyapılarının, kullanıcılar tarafından yeterli görülmediğine işaret etmektedir. Özellikle, teknolojik altyapının geliştirilmesi ve düzenleyici çerçevelerin güçlendirilmesi gerektiği, bu algılar doğrultusunda önemli bir ihtiyaç olarak öne çıkmaktadır.

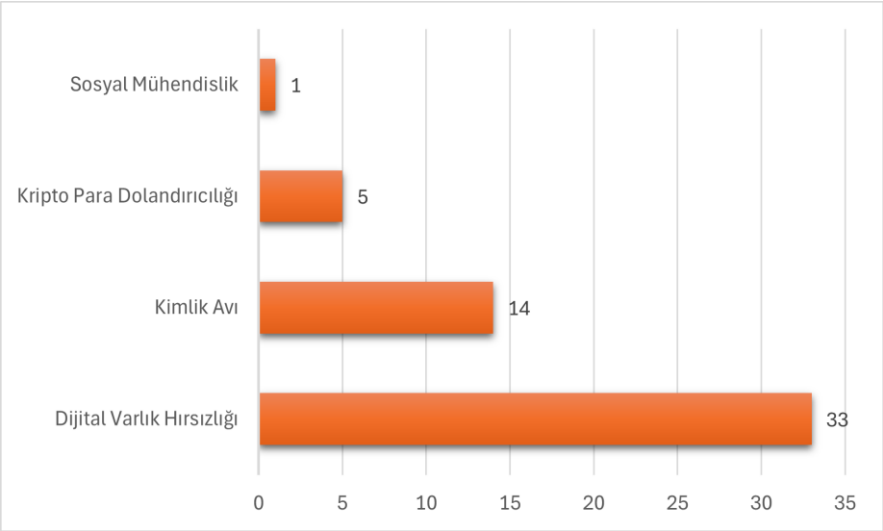


Şekil 6.9. Firmaların dolandırıcılık vakaları ile karşılaşma oranı

Firmaların yarısından fazlası dolandırıcılık vakalarıyla karşılaşmadıklarını belirtmiştir. Bu durum, bu firmaların güçlü güvenlik önlemleri almış olabileceğini veya Metaverse platformlarını daha sınırlı bir şekilde kullandıklarını gösterebilir. Bununla birlikte, bu oran, bazı firmaların dolandırıcılık faaliyetlerini algılayamamış veya raporlamamış olabileceğine de işaret edebilir.

Dolandırıcılık vakalarıyla karşılaştığını belirten firmaların oranı oldukça yüksektir. Bu, Metaverse platformlarının dolandırıcılık açısından hâlâ önemli riskler içerdiğini ve güvenlik önlemlerinin her durumda etkili olmadığını ortaya koymaktadır. Bu gruptaki firmalar, özellikle dijital kimlik sahteciliği, sanal varlık hırsızlığı veya kimlik avı gibi dolandırıcılık türlerinden etkilenmiş olabilir.

Anket sonuçlarına göre, dolandırıcılık vakalarıyla karşılaşan firmaların %43'lük oranı, Metaverse platformlarında güvenlik açıklarının hâlâ ciddi bir tehdit oluşturduğunu göstermektedir. Kararsız kalan %4'lük kesim ise, dolandırıcılık tespiti ve raporlamasında farkındalık artırıcı programların gerekliliğine işaret etmektedir.



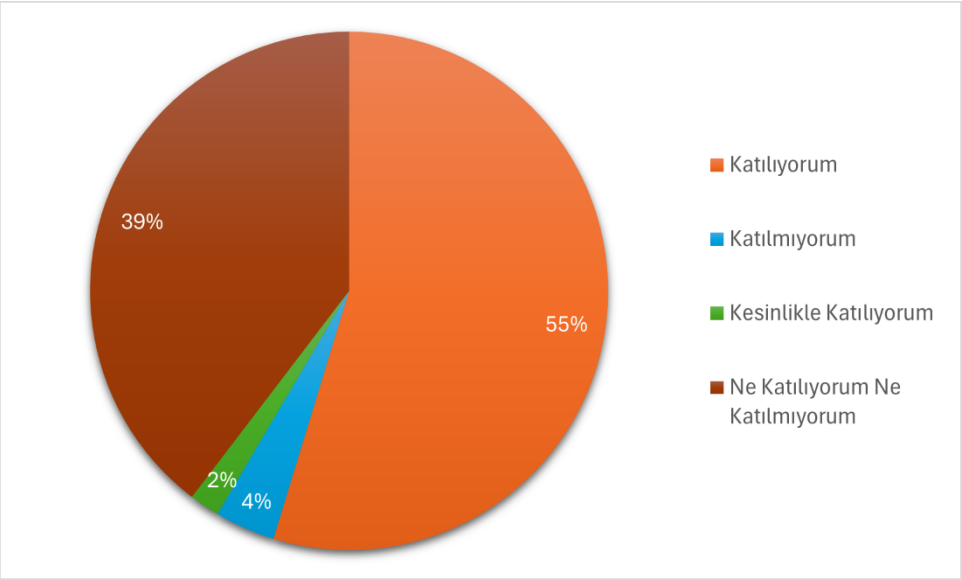
Şekil 6.10. En yaygın dolandırıcılık türleri

Dijital varlık hırsızlığının en yaygın dolandırıcılık türü olarak belirtilmesi, Metaverse platformlarında dijital varlıkların değerinin hızla artmasıyla ilişkilendirilebilir. NFT'ler, oyun içi varlıklar ve diğer dijital mülkler, dolandırıcılar için cazip hedefler haline gelmiştir. Bu durum, sanal varlıkların güvenliğini sağlamak için daha güçlü koruma önlemlerine ihtiyaç olduğunu göstermektedir. Özellikle, blokzincir tabanlı güvenlik sistemleri ve akıllı sözleşmelerin bu tür tehditleri önlemede etkili bir çözüm olabileceği değerlendirilmektedir.

Kimlik avı saldırılarının yaygınlığı, Metaverse kullanıcılarının dolandırıcılar tarafından sahte kimliklerle kandırılması veya hassas bilgilerin çalınması riskini ortaya koymaktadır. Bu saldırılar, genellikle kullanıcıların kişisel verilerini veya hesap bilgilerini ele geçirmek amacıyla gerçekleştirilir. Kimlik avı tehditlerini azaltmak için kullanıcı eğitimi ve iki faktörlü kimlik doğrulama gibi güvenlik mekanizmalarının yaygınlaştırılması kritik önem taşımaktadır.

Kripto para dolandırıcılıkları, Metaverse platformlarında finansal işlemlerin önemli bir kısmının kripto varlıklar üzerinden gerçekleştirilmesiyle bağlantılıdır. Sahte kripto para projeleri, dolandırıcılar tarafından yatırımcıları yanıltmak için kullanılabilir. Bu tür dolandırıcılıklara karşı daha sıkı düzenlemeler ve kullanıcıların finansal işlemler konusunda bilinçlendirilmesi gerekmektedir.

Sosyal mühendislik yöntemlerinin düşük bir oranla belirtilmesi, bu tür dolandırıcılıkların daha az algılandığını veya daha az raporlandığını gösterebilir. Ancak sosyal mühendislik, özellikle dolandırıcıların kullanıcıların güvenini kötüye kullanarak hassas bilgileri ele geçirmesi açısından hala ciddi bir tehdittir.

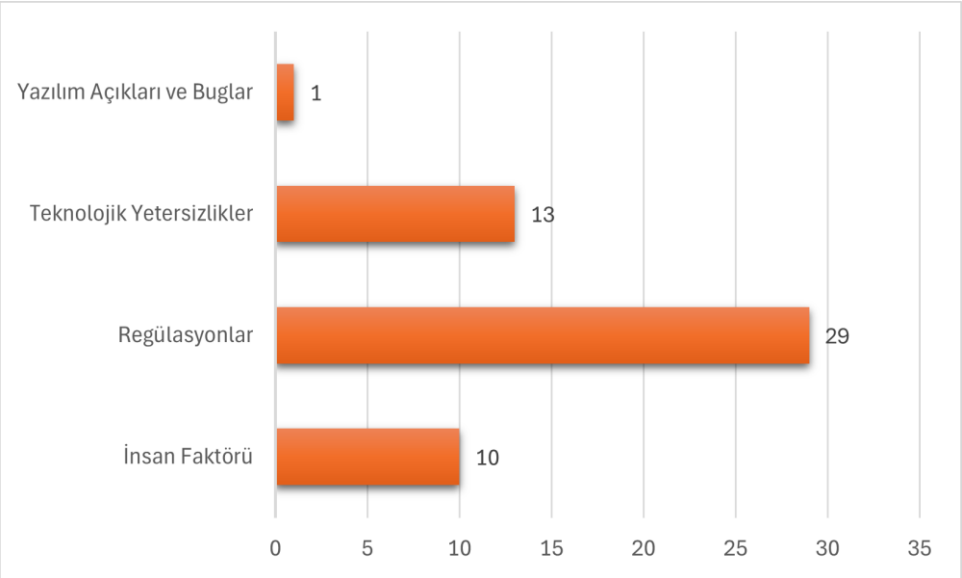


Şekil 6.11. Mevcut güvenlik sistemlerinin yeterlilik oranı

Katılımcıların yarısından fazlası, dolandırıcılık tespit sistemlerinin yeterli olduğunu düşünmektedir. Bu durum, bazı firmaların dolandırıcılıkla mücadelede güçlü teknolojik altyapılara ve iyi tanımlanmış süreçlere sahip olduğunu gösterebilir. Ancak, bu güven, tüm firmalar için yaygın olmamakla birlikte, sektörel farklılıklardan veya kullanılan sistemlerin çeşitliliğinden kaynaklanabilir.

Yüksek bir kararsızlık oranı ile birlikte küçük bir kesim, tespit sistemlerinin yetersiz olduğunu belirtmiştir. Mevcut sistemlerin yeterliliği konusunda kullanıcılar arasında net bir güven oluşmadığını göstermektedir. Bu belirsizlik, sistemlerin etkisinin tam olarak anlaşılamamasından veya iletişim eksikliğinden kaynaklanabilir. Kararsızlık, aynı zamanda sistemlerin tutarsız performansı veya kullanıcı deneyiminin yetersizliğiyle ilişkilendirilebilir.

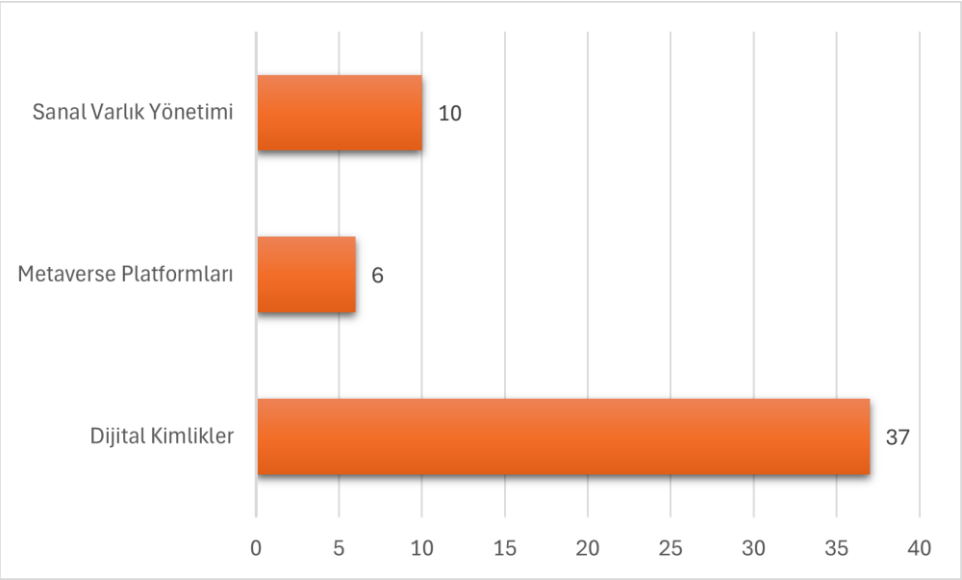
6.3 Karşılaşılan Zorluklar



Şekil 6.12. Dolandırıcılık tespitindeki zorluklar

Anket katılımcılarının %58'i, Metaverse dolandırıcılık tespitiyle ilgili en büyük zorluk olarak regülasyon eksikliğini belirtmiştir. Bunu %26 oranıyla teknolojik yetersizlikler takip etmektedir. 10 katılımcı, dolandırıcılık tespitiyle ilgili zorluklarda insan faktörünü öncelikli olarak görmüştür. Daha az sıklıkla ifade edilen diğer zorluklar arasında, yazılım açıkları yer almaktadır.

Bu bulgular, Metaverse ortamında dolandırıcılığı önleme ve tespit etme konularında iki anahtar faktörün öne çıktığını göstermektedir; düzenleyici altyapıların oluşturulması ve teknolojik gelişmelerin hızlandırılması. Katılımcıların bu iki alanı vurgulaması, Metaverse'ün henüz olgunlaşmamış bir ekosistem olduğunu ve bu eksikliklerin dolandırıcılık faaliyetleri için bir fırsat oluşturduğunu ortaya koymaktadır. İnsan faktörünün önemli bir zorluk olarak belirtilmesi hem kullanıcıların bilinçsizliği hem de dolandırıcıların sosyal mühendislik yöntemlerini kullanarak insan hatalarından faydalanması şeklinde iki yönlü bir tehdit oluşturabilir.



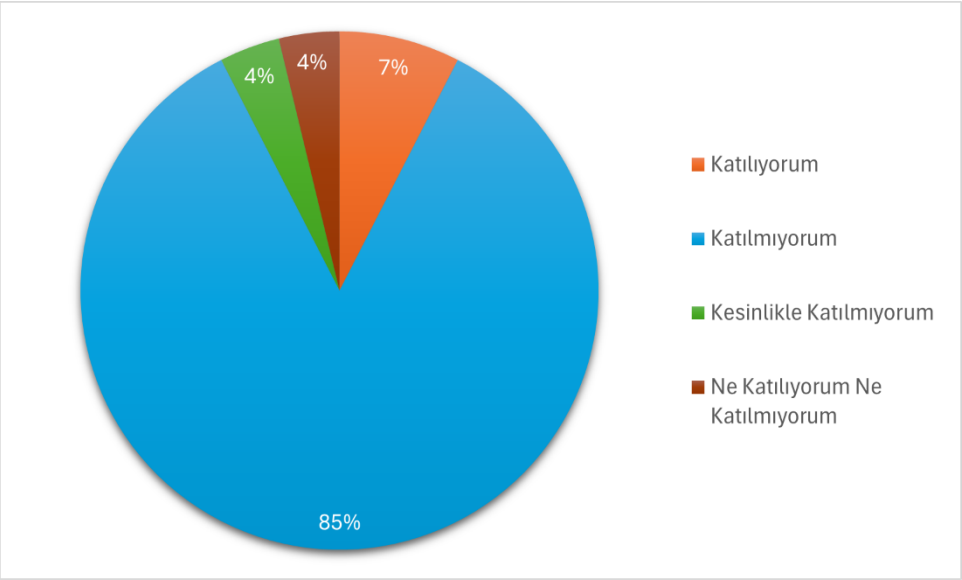
Şekil 6.13. Dolandırıcılık tespitindeki en büyük riskler

Katılımcılara Metaverse'te dolandırıcılığı tespit etmede en büyük riski hangi alanlarda görüyorsunuz? sorusu yöneltilmiştir. Dijital kimliklerin güvenliği, katılımcılar tarafından en kritik risk alanı olarak belirtilmiştir. Özellikle kimlik sahtekârlığı, hesap ele geçirme ve sahte kimlik oluşturma gibi tehditler, Metaverse ekosisteminde dolandırıcılık faaliyetlerini kolaylaştırmaktadır. Bu durum, kimlik doğrulama sistemlerinin yetersizliğini ve bu alandaki teknolojik çözümlere duyulan ihtiyacı ortaya koymaktadır.

Dijital varlıkların çalınması, sahte varlıkların üretilmesi ve finansal dolandırıcılık, katılımcılar tarafından ikinci en büyük risk alanı olarak görülmektedir. Özellikle NFT'ler ve kripto para gibi yüksek değerli dijital varlıklar, dolandırıcılar için cazip hedefler haline gelmiştir. Dijital varlıkların güvenliği, özellikle yüksek değere sahip varlıklar nedeniyle dolandırıcılığa karşı savunmasız kalmaktadır. Blokzincir tabanlı çözümlerin bu alanda etkin rol oynayabileceği değerlendirilmektedir.

Metaverse platformlarının altyapısal güvenlik açıkları, dolandırıcılık faaliyetlerinin kolayca gerçekleştirilmesine neden olabilmektedir. Katılımcılar, platformların özellikle kullanıcı bilgilerini koruma ve sahte hesapları tespit etme konularında yetersiz olduğunu düşünmektedir. Bu bulguya göre Metaverse

platformlarının dolandırıcılık tespitinde daha güçlü araçlara ihtiyaç duyduğu anlaşılmaktadır. Kullanıcı verilerinin korunması ve sahte hesapların engellenmesi bu alandaki kritik gelişim alanlarıdır.

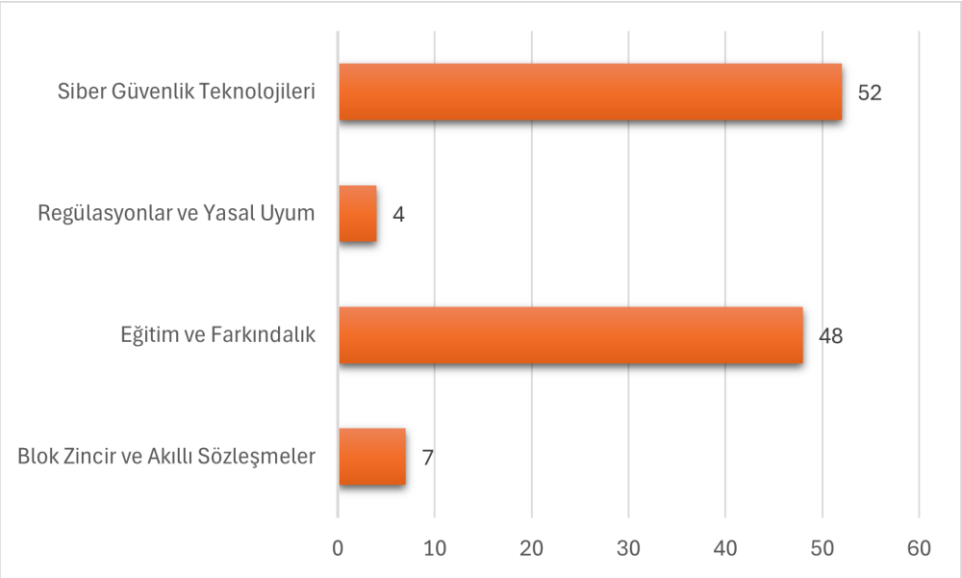


Şekil 6.14. Regülasyonların yeterliliği bilgisi

Katılımcıların büyük çoğunluğu, Metaverse platformlarında dolandırıcılık tespiti için mevcut regülasyonların yetersiz olduğunu ifade etmiştir. Bir kısım katılımcı ise regülasyonların dolandırıcılık tespitinde tamamen yetersiz olduğunu belirtmiştir. Az sayıda katılımcı, regülasyonların dolandırıcılığı tespitte yeterli olduğunu düşünmektedir.

Katılımcıların %89'unun regülasyonları yetersiz bulması, Metaverse ekosisteminde dolandırıcılıkla mücadele için gerekli düzenleyici çerçevelerin büyük bir eksikliğe işaret ettiğini göstermektedir.
Bu durum, dolandırıcılık tespit ve önleme süreçlerinde firmaların yalnız bırakıldığını ve sektörde standart bir uygulama veya güvenlik prosedürü olmadığını ortaya koymaktadır. Özellikle ulusal ve uluslararası düzeyde koordinasyonsuzluk, bu algının ana nedenlerinden biri olabilir.

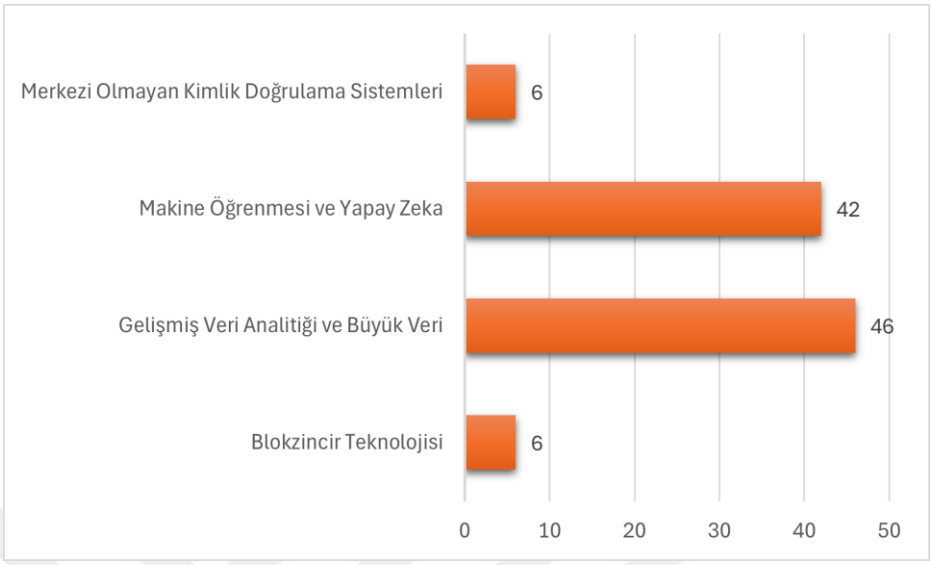
6.4 Kritik Teknolojiler ve Stratejiler



Şekil 6.15. Dolandırıcılığı önlemek için yatırım yapılması gereken alanlar

Katılımcılara yöneltilen Metaverse'te dolandırıcılığı önlemek için daha fazla yatırım yapılması gereken alanların hangisi olduğunu düşünüyorsunuz? Sorusuna katılımcıların büyük bir çoğunluğu, siber güvenlik teknolojilerinin dolandırıcılığı önlemede kritik bir yatırım alanı olduğunu düşünmektedir. Bu oran, Metaverse platformlarının karşı karşıya olduğu siber tehditlerin farkındalığının oldukça yüksek olduğunu göstermektedir. Bu bulgu, Metaverse'teki güvenlik açıklarının giderilmesi için sağlam bir siber güvenlik altyapısına ihtiyaç olduğunu vurgular. Verilerin şifrelenmesi, güvenli oturum açma sistemleri ve gerçek zamanlı tehdit algılama gibi teknolojilere yatırım öncelikli olmalıdır. Katılımcılar bir sonraki aşama için kullanıcıların bilinçlendirilmesinin dolandırıcılığı önlemek için önemli bir faktör olduğunu belirtmiştir. Teknoloji ne kadar güçlü olursa olsun, insan faktörü dolandırıcılık faaliyetlerinde önemli bir rol oynar. Kullanıcılara dolandırıcılık yöntemlerini tanıma, güçlü parola kullanımı, kimlik avı saldırılarından korunma gibi konularda eğitim verilmesi gerekmektedir. Blokzincir teknolojisi ve akıllı sözleşmeler, dolandırıcılık önlemede %13'lük bir destek oranına sahiptir. Bu teknolojiye yönelik farkındalık, siber güvenlik ve eğitim gibi alanlara göre daha düşük kalmıştır. Blokzincir ve akıllı sözleşmeler, dolandırıcılığı önlemek için önemli bir

potansiyele sahiptir. Ancak bu alanın daha fazla tanıtıma ve kullanım senaryolarının genişletilmesine ihtiyacı vardır.

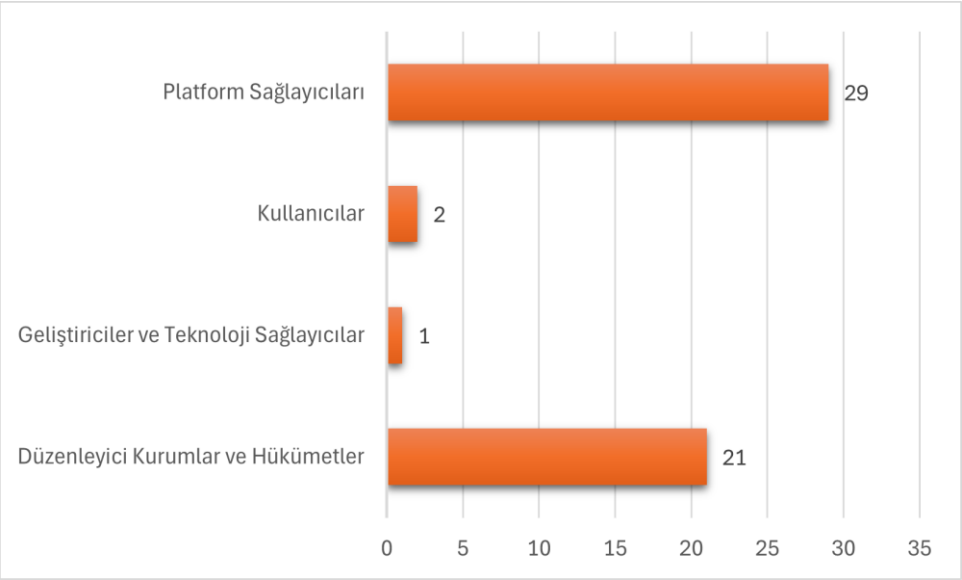


Şekil 6.16. Dolandırıcılığı önlemek için ihtiyaç duyulan yeni teknolojiler

Hangi yeni teknolojilere ihtiyaç duyulduğu sorusuna katılımcılar arasında en yüksek öncelik, büyük veri analitiği ve gelişmiş veri işleme teknolojilerine verilmiştir. Dolandırıcılık tespiti için büyük veri analizleri, geçmiş verilerden örüntüleri çıkararak olası dolandırıcılık faaliyetlerini tespit edebilir. Bu teknoloji, özellikle Metaverse'teki büyük miktarda veri akışını anlamlandırmak ve anomalileri belirlemek için kritik öneme sahiptir.

Yapay zeka ve makine öğrenimi, dolandırıcılığı gerçek zamanlı olarak tespit etmek için ikinci en çok tercih edilen teknoloji olmuştur. Makine öğrenimi algoritmaları, dolandırıcılık desenlerini öğrenerek sürekli gelişebilir ve kullanıcı davranışlarındaki anormallikleri tespit edebilir. Bu, proaktif bir savunma mekanizması sağlar.

Daha düşük bir oran olsa da katılımcılar blokzincir teknolojisini önemli bir teknoloji olarak görmektedir. Blokzincir, işlemlerin şeffaf ve değişmez olmasını sağlar. Ancak dolandırıcılık tespiti için tek başına yeterli olmayabilir ve diğer teknolojilerle entegre edilmesi gerekebilir.



Şekil 6.17. Dolandırıcılıkla mücadelede sorumluluk

Katılımcılara yöneltilen Metaverse'te dolandırıcılıkla mücadelede en büyük sorumluluğun kime ait olduğunu düşünüyorsunuz? sorusuna çoğunluk, platformların güvenlik ve dolandırıcılıkla mücadele için daha fazla önlem alması gerektiğini düşünmektedir. Özellikle kullanıcı verilerinin korunması ve dolandırıcılık girişimlerini tespit etmede bu aktörlerin kilit rol oynadığı belirtilmiştir. Katılımcılar, ulusal ve uluslararası düzenleyici kurumların daha katı regülasyonlar oluşturmasını talep etmekte ve dolandırıcılıkla mücadelede kullanıcıların bilinçlendirilmesi ve sorumluluk alması gerektiği görüşü ortaya çıkmaktadır.

7. SONUÇ VE ÖNERİLER

Metaverse, dijital dünyanın yeni sınırlarını belirleyen bir ekosistem olarak, kullanıcıların sanal dünyada etkileşimde bulunma biçimini köklü bir şekilde değiştirmektedir. Bu yeni dijital evren, büyük fırsatlar sunarken aynı zamanda ciddi güvenlik tehditlerini ve dolandırıcılık risklerini de beraberinde getirmektedir. Metaverse'ün merkeziyetsiz yapısı, kimlik sahtekarlığı, sanal varlık hırsızlığı, NFT dolandırıcılığı ve kripto para dolandırıcılığı gibi çeşitli dolandırıcılık türlerinin yaygınlaşmasına zemin hazırlamaktadır.

Bu çalışma, Metaverse'teki dolandırıcılık risklerini, bu risklerin ortaya çıkış biçimlerini ve bu tehditlere karşı geliştirilen stratejileri ayrıntılı bir şekilde ele almıştır. Elde edilen bulgular, dolandırıcılık risklerinin bireysel kullanıcılar kadar kurumlar, finansal sistemler ve uluslararası düzenleyici çerçeveler üzerinde de ciddi etkiler yarattığını göstermektedir.

Metaverse'ün altyapısına entegre edilmesi gereken teknolojiler, güvenlik risklerini azaltmada kritik rol oynamaktadır. Blokzincirin merkeziyetsiz yapısı, veri bütünlüğü ve işlem şeffaflığı sağlarken; yapay zeka ve makine öğrenimi tabanlı sistemler, anormal kullanıcı davranışlarını izleyerek dolandırıcılığı önlemektedir.

Kullanıcı gizliliğini korurken dolandırıcılık tespit süreçlerini daha etkili hale getiren gizlilik odaklı teknolojiler, Metaverse'ün güvenliği için yenilikçi bir yaklaşım sunmaktadır.

Metaverse'ün sınır tanımayan yapısı, küresel düzeyde düzenlemelerin ve iş birliğinin zorunluluğunu ortaya koymaktadır. Bu düzenlemeler, dijital varlık yönetimi, kimlik doğrulama süreçleri ve veri güvenliği gibi konularda standartlar oluşturmalıdır.

Kullanıcıların dolandırıcılık riskleri hakkında bilinçlendirilmesi, güvenli davranışları teşvik eden programlarla desteklenmeli ve hatta ortaöğretim ve üniversite müfredatlarına da entegre edilerek dijital okuryazarlık düzeyleri artırılmalıdır.

Kripto varlıklar ve dijital ekonominin Metaverse'ün temel yapı taşları olacağı göz önüne alındığında, bu varlıkların güvenliği ve denetimi için gelişmiş teknolojik çözümler geliştirilmelidir. Aynı zamanda, Metaverse'ün sosyal yönleri, olumsuz davranışların tespitine yönelik yapay zeka tabanlı sosyal denetim mekanizmaları ile güvence altına alınmalıdır.

Metaverse, teknolojik yeniliklerin sunduğu büyük fırsatlarla birlikte önemli güvenlik zorluklarını da beraberinde getirmektedir. Bu çalışmada incelenen stratejiler ve öneriler, Metaverse'teki dolandırıcılık risklerini azaltmak ve bu dijital ortamı daha güvenli hale getirmek için somut adımlar sunmaktadır. Gelecekte, Metaverse'ün sürdürülebilir bir platform olarak gelişmesi, bu stratejilerin etkin bir şekilde uygulanmasına bağlı olacaktır.

Bu bağlamda, teknolojik çözümler, düzenleyici çerçeveler ve kullanıcı farkındalığı programlarının entegre edilmesi, Metaverse'ün potansiyelini tam anlamıyla gerçekleştirmesi için kritik öneme sahiptir. Kullanıcılar, teknoloji sağlayıcıları ve düzenleyiciler arasında geliştirilecek çok paydaşlı bir iş birliği, bu yeni dijital evrenin güvenliğini ve bütünlüğünü sağlamada önemli bir rol oynayacaktır.

KAYNAKLAR

Airlangga, G. (2024). Deep learning for anomaly detection and fraud analysis in blockchain transactions of the open metaverse. *Jurnal Informatika Ekonomi Bisnis*, 324-329.

Al-Tkhayneh, K. M., Olowoselu, A., & Alkrisheh, M. A. (2023). The crime in metaverse (the future scenarios for crime patterns and the prospective legal challenges). *Tenth International Conference on Social Networks Analysis, Management and Security,* 1-6.

Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., ... & Saif, A. (2022). Financial fraud detection based on machine learning: a systematic literature review. *Applied Sciences,* 12-19.

Başbüyük, İ. (2023). Blokzincir-kripto varlık bağlantılı yaygın sahtekarlık türlerinin dolandırıcılık ve ilişkili suçlar yönünden analizi. *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, 25:805-846.

Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. *Statistical Science*, 17:235-255.

Chatterjee, P., Das, D., & Rawat, D. B. (2023). Next generation financial services: Role of blockchain enabled federated learning and metaverse. *23rd International Symposium on Cluster, Cloud and Internet Computing Workshops*, 69-74.

Gartner,Inc. (2022, February 07). Gartner predicts 25% of people will spend at least one hour per day in the metaverse by 2026. Gartner. https://www.gartner.com/en/newsroom/press-releases/2022-02-07-gartner-predicts-25-percent-of-people-will-spend-at-least-one-hour-per-day-in-the-metaverse-by-2026

Güler, O., & Savaş, S. (2022). Tüm yönleriyle metaverse çalışmaları, teknolojileri ve geleceği. *Gazi Mühendislik Bilimleri Dergisi*, 8:292-319.

Hasham, S., Joshi, S., & Mikkelsen, D. (2019). Financial crime and fraud in the age of cybersecurity. *McKinsey & Company*, 2019.

Hudnurkar, M., Singh, K., Ambekar, S., Sahu, G., & Yecho, H. (2024). Legalities in metaverse–ethereum fraud detection. *Ninth International Conference on Science Technology Engineering and Mathematics*, 1-14.

Jeon, H. J., Youn, H. C., Ko, S. M., & Kim, T. H. (2022). Blockchain and AI meet in the metaverse. *Advances in the Convergence of Blockchain and Artificial Intelligence*, 73:73-82.

Katterbauer, K., Syed, H., & Cleenewerck, L. (2022). Financial cybercrime in the Islamic finance metaverse. *Journal of Metaverse*, 2:56-61.

Kou, Y., Lu, C. T., Sirwongwattana, S., & Huang, Y. P. (2004). Survey of fraud detection techniques. *In IEEE International Conference on Networking, Sensing and Control*, 749-754.

Kshetri, N. (2023). Privacy violations, security breaches and other threats of Web3 and the metaverse.

Kshetri, N. (2022). Scams, frauds, and crimes in the nonfungible token market. *Computer*, 55.4:60-64.

Lee, L. H., Braud, T., Zhou, P., Wang, L., Xu, D., Lin, Z., ... & Hui, P. (2021). All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda. *ArXiv Preprint arXiv:2110.05352.*

Lin, K., Wu, J., Lin, D., & Zheng, Z. (2023). A survey on metaverse: applications, crimes and governance. *In 2023 IEEE International Conference on Metaverse Computing, Networking and Applications,* 541-549.

Mackenzie, S. (2022). Criminology towards the metaverse: Cryptocurrency scams, grey economy and the technosocial. *The British Journal of Criminology*, 62.6:1537-1552.

McAmis, R., Durak, B., Chase, M., Laine, K., Roesner, F., & Kohno, T. (2024). Handling identity and fraud in the metaverse. *IEEE Security & Privacy.*

Mooij, A. (2024). Regulating the metaverse economy: How to prevent money laundering and the financing of terrorism. *Springer Nature,* 112.

Nicholls, J., Kuppa, A., & Le-Khac, N. A. (2021). Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. *Ieee Access,* 9:163965-163986.

Pooyandeh, M., Han, K. J., & Sohn, I. (2022). Cybersecurity in the AI-based metaverse: A survey. *Applied Sciences*, 12,24:12993.

Rajawat, A. S., Goyal, S. B., Solanki, R., Raboaca, M. S., Mihaltan, T. C., Illés, Z., & Verma, C. (2023). Blockchain-based security framework for metaverse: A decentralized approach. *In 2023 15th International Conference on Electronics, Computers and Artificial Intelligence,* 01-06.

Saivasan, R., & Lokhande, M. (2023). Exploring use cases of generative AI and metaverse in financial analytics: Unveiling the synergies of advanced technologies. *International Journal of Global Business and Competitiveness,* 18:77-86.

Smaili, N., & de Rancourt-Raymond, A. (2022). Metaverse: Welcome to the new fraud marketplace. *Journal of Financial Crime*, 31,1:188-200.

Stephenson, Neal. (1992). *Snow crash*. Bantam Books.

Sun, J., Gan, W., Chen, Z., Li, J., & Yu, P. S. (2022). Big data meets metaverse: A survey. *ArXiv Preprint arXiv:2210.16282.*

Sun, J., Gan, W., Chao, H. C., & Yu, P. S. (2022). Metaverse: Survey, applications, security, and opportunities. *ArXiv Preprint arXiv:2210.07990.*

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.

Wang, H., Ning, H., Lin, Y., Wang, W., Dhelim, S., Farha, F., ... & Daneshmand, M. (2023). A survey on the metaverse: The state-of-the-art, technologies, applications, and challenges. *IEEE Internet of Things Journal,* 10,16: 14671-14688.

Wang, X., Wang, J., Wu, C., Xu, S., & Ma, W. (2022). Engineering brain: Metaverse for future engineering. *AI in Civil Engineering*, 1,1:2.

Wu, J., Lin, K., Lin, D., Zheng, Z., Huang, H., & Zheng, Z. (2023). Financial crimes in web3-empowered metaverse: Taxonomy, countermeasures, and opportunities. *IEEE Open Journal of the Computer Society*, 4:37-49.

Xu, C., Liang, X., Sun, Y., & He, X. (2023). Fraudsters beware: Unleashing the power of metaverse technology to uncover financial fraud. *International Journal of Human–Computer Interaction*, 1-16

Xu, M., Ng, W. C., Lim, W. Y. B., Kang, J., Xiong, Z., Niyato, D., ... & Miao, C. (2022). A full dive into realizing the edge-enabled metaverse: Visions, enabling technologies, and challenges. *IEEE Communications Surveys & Tutorials*, 25,1:656-700.

EKLER

EK A. Anket Soruları

EK A. Anket Soruları

1. Yaş aralığınız nedir?

    a. 18-25
    b. 26-35
    c. 36-45
    d. 46-55
    e. 56 ve üzeri

2. Eğitim durumunuz nedir?

    a. Lise
    b. Ön Lisans
    c. Lisans
    d. Yüksek Lisans
    e. Diğer: _____

3. Firmanızın sektörü nedir?

    a. Bilgi Teknolojileri
    b. Finans
    c. Sağlık
    d. Eğitim
    e. Diğer: _____

4. Firmanızda hangi pozisyonda çalışıyorsunuz?

    a. Üst Düzey Yönetici
    b. Orta Düzey Yönetici
    c. Güvenlik Uzmanı
    d. Teknik Uzman
    e. Diğer: _____

5. Firmanızın büyüklüğü nedir? (Çalışan Sayısı)

    a. 1-50
    b. 51-100
    c. 101-250

d. 251 - 500
e. 501 ve üzeri

6. Metaverse alanında ne kadar süredir faaliyet gösteriyorsunuz?

a. 1 yıldan az
b. 1-3 yıl
c. 3-5 yıl
d. 5-7 yıl
e. 7 yıl ve üzeri

7. Metaverse teknolojileri hakkında bilgi sahibi olduğunuzu düşünüyor musunuz?

a. Kesinlikle Katılmıyorum
b. Katılmıyorum
c. Ne Katılıyorum Ne Katılmıyorum
d. Katılıyorum
e. Kesinlikle Katılıyorum

8. Metaverse güvenlik ve dolandırıcılık riskleri hakkında bilgi sahibi olduğunuzu düşünüyor musunuz?

a. Kesinlikle Katılmıyorum
b. Katılmıyorum
c. Ne Katılıyorum Ne Katılmıyorum
d. Katılıyorum
e. Kesinlikle Katılıyorum

9. Metaverse platformlarının genel olarak dolandırıcılığa karşı savunmasız olduğunu düşünüyor musunuz?

a. Kesinlikle Katılmıyorum
b. Katılmıyorum
c. Ne Katılıyorum Ne Katılmıyorum
d. Katılıyorum
e. Kesinlikle Katılıyorum

10. Firmanızın Metaverse'te dolandırıcılık vakalarıyla karşılaştığını düşünüyor musunuz?

    a. Kesinlikle Katılmıyorum
    b. Katılmıyorum
    c. Ne Katılıyorum Ne Katılmıyorum
    d. Katılıyorum
    e. Kesinlikle Katılıyorum

11. Metaverse dolandırıcılıklarının en yaygın türünün hangisi olduğunu düşünüyorsunuz?

    a. Kimlik Avı (Phishing)
    b. Sosyal Mühendislik
    c. Dijital Varlık Hırsızlığı
    d. Kripto Para Dolandırıcılığı
    e. Diğer: _____

12. Firmanızın Metaverse platformlarında dolandırıcılığı önlemek için özel güvenlik önlemleri aldığını düşünüyor musunuz?

    a. Kesinlikle Katılmıyorum
    b. Katılmıyorum
    c. Ne Katılıyorum Ne Katılmıyorum
    d. Katılıyorum
    e. Kesinlikle Katılıyorum

13. Firmanız güvenlik önlemleri alıyorsa bu önlemlerin etkili olduğunu düşünüyor musunuz?

    a. Kesinlikle Katılmıyorum
    b. Katılmıyorum
    c. Ne Katılıyorum Ne Katılmıyorum
    d. Katılıyorum
    e. Kesinlikle Katılıyorum

14. Firmanız dolandırıcılık tespit sistemleri (örneğin, yapay zekâ destekli izleme sistemleri) kullanıyor mu?

    a. Kesinlikle Katılmıyorum
    b. Katılmıyorum
    c. Ne Katılıyorum Ne Katılmıyorum
    d. Katılıyorum
    e. Kesinlikle Katılıyorum

15. Dolandırıcılık tespitine yönelik mevcut sistemlerin yeterli olduğunu düşünüyor musunuz?

    a. Kesinlikle Katılmıyorum
    b. Katılmıyorum
    c. Ne Katılıyorum Ne Katılmıyorum
    d. Katılıyorum
    e. Kesinlikle Katılıyorum

16. Firmanızın dolandırıcılık vakalarına karşı kullanıcı farkındalığını artırmak amacıyla eğitimler düzenlediğini düşünüyor musunuz?

    a. Kesinlikle Katılmıyorum
    b. Katılmıyorum
    c. Ne Katılıyorum Ne Katılmıyorum
    d. Katılıyorum
    e. Kesinlikle Katılıyorum

17. Firmanız dolandırıcılığı tespit etmek için hangi teknolojileri kullanıyor?

    a. Makine Öğrenimi ve Yapay Zekâ
    b. Blokzincir Teknolojisi
    c. Merkezi Olmayan Kimlik Doğrulama Sistemleri
    d. Gelişmiş Veri Analitiği ve Büyük Veri
    e. Diğer: _____

18. Kullanılan teknolojilerin dolandırıcılık tespitinde ne kadar etkili olduğunu düşünüyorsunuz?

    a. Çok etkili
    b. Etkili
    c. Ne Etkili Ne Etkisiz
    d. Az etkili
    e. Hiç etkili değil

19. Dolandırıcılık tespiti için hangi teknolojilerin gelecekte daha fazla önem kazanacağını düşünüyorsunuz?

    a. Makine Öğrenimi ve Yapay Zekâ
    b. Blokzincir Teknolojisi
    c. Merkezi Olmayan Kimlik Doğrulama Sistemleri
    d. Gelişmiş Veri Analitiği ve Büyük Veri
    e. Diğer: _____

20. Metaverse'te dolandırıcılık tespiti ile ilgili karşılaştığınız en büyük zorluk nedir?

    a. Teknolojik Yetersizlikler
    b. İnsan Faktörü
    c. Maliyetler
    d. Regülasyonlar
    e. Diğer: _____

21. Metaverse'te dolandırıcılığı tespit etmede en büyük riski hangi alanlarda görüyorsunuz?

    a. Sanal Varlık Yönetimi
    b. Dijital Kimlikler
    c. Kullanıcı Etkileşimleri
    d. Metaverse Platformları
    e. Diğer: _____

22. Metaverse'te dolandırıcılık tespiti için regülasyonların yeterli olduğunu düşünüyor musunuz?

    a. Kesinlikle Katılmıyorum
    b. Katılmıyorum
    c. Ne Katılıyorum Ne Katılmıyorum
    d. Katılıyorum
    e. Kesinlikle Katılıyorum

23. Metaverse'te dolandırıcılığı önlemek için daha fazla yatırım yapılması gereken alanların hangisi olduğunu düşünüyorsunuz?

    a. Siber Güvenlik Teknolojileri
    b. Blokzincir ve Akıllı Sözleşmeler
    c. Eğitim ve Farkındalık
    d. Regülasyonlar ve Yasal Uyumluluk
    e. Diğer: _____

24. Firmanızın, dolandırıcılık vakalarının tespitini geliştirmek için yeni çözümler üzerinde çalıştığını düşünüyor musunuz?

    a. Kesinlikle Katılmıyorum
    b. Katılmıyorum
    c. Ne Katılıyorum Ne Katılmıyorum
    d. Katılıyorum
    e. Kesinlikle Katılıyorum

25. Metaverse platformlarında dolandırıcılığı tespit etmek için hangi yeni teknolojilere ihtiyaç olduğunu düşünüyorsunuz?

    a. Makine Öğrenimi ve Yapay Zekâ
    b. Blokzincir Teknolojisi
    c. Merkezi Olmayan Kimlik Doğrulama Sistemleri
    d. Gelişmiş Veri Analitiği ve Büyük Veri
    e. Diğer: _____

26. Metaverse'te dolandırıcılık tespiti hakkında firmanızın güvenlik politikalarının ne derece etkili olduğunu düşünüyorsunuz?

    a. Çok etkili
    b. Etkili
    c. Ne Etkili Ne Etkisiz
    d. Etkisiz
    e. Çok etkisiz

27. Metaverse'te dolandırıcılık tespiti konusunda firmanızda en fazla gelişmesi gereken alanın hangisi olduğunu düşünüyorsunuz?

    a. Siber Güvenlik Altyapısı
    b. Makine Öğrenmesi ve Yapay Zekâ
    c. Blokzincir Teknolojisi
    d. Kullanıcı Eğitimi Farkındalığı
    e. Diğer: _____

28. Metaverse'te dolandırıcılıkla mücadelede en büyük sorumluluğun kime ait olduğunu düşünüyorsunuz?

    a. Platform Sağlayıcıları
    b. Kullanıcılar
    c. Geliştiriciler ve Teknoloji Sağlayıcılar
    d. Düzenleyici Kurumlar ve Hükümetler
    e. Diğer: _____

29. Metaverse'te dolandırıcılık tespitiyle ilgili eklemek istediğiniz herhangi bir görüş veya öneriniz var mı?

TEZ SÜRECİNDE ÜRETİLMİŞ YAYINLAR

Demirtaş, A.H., Aydın, M.A., Zaim, A.H. (2024). The Future and Security of The Metaverse, *İstanbul Ticaret Üniversitesi Teknoloji ve Uygulamalı Bilimler Dergisi,* Basımda.