Review Article
Derleme Makalesi

JOSS
Akıllı Sistemler Dergisi, 3(1): 1-17, 2024

JOSS
Journal of Smart Systems
e-ISSN: 3023-6150

METAVERSE'ÜN KARANLIK YÜZÜ: DARKVERSE

Mehmet Ali ASLAN[1,a,*]

[1]Afyonkarahisar İl Milli Eğitim Müdürlüğü, Afyonkarahisar, Türkiye
[a]mhmeta.aslan@gmail.com, ORCID: 0000-0001-8571-1773

(Geliş/Received: 02.02.2024; Kabul/Accepted: 15.05.2024)

ÖZET

Metaverse, internetin evrimi olarak tanımlanmaktadır. Metaverse'de kullanıcıları avatarlar temsil etmektedir. Metaverse içindeki avatar deneyimlerinin, gerçek dünyadaki kullanıcılar üzerinde olumlu ve olumsuz etkileri olabilmektedir. Şu anda Metaverse olarak tanımlanan oyunlar ve uygulamalar, daha yolun çok başında olduğumuzu göstermektedir. Metaverse içerisinde yasadışı faaliyetlerin gerçekleştirildiği alan, Darkverse olarak ifade edilmektedir. Derleme türündeki bu çalışmada Metaverse literatüründe güvenlik ve gizlilik konulu çalışmalar incelenmiştir. Literatür değerlendirme sonucunda ise Darkverse kavramını irdeleyen çalışmaların eksikliği tespit edilmiştir. Bu çalışmada Darkverse kavramı incelenerek literatüre bu alanda katkı sağlaması amaçlanmaktadır. Ayrıca çalışmada internetin evrimi, Metaverse ve Metaverse'ün temel bileşenleri konuları da ele alınmıştır.

Anahtar Kelimeler: Metaverse, karanlık evren, yasadışı, internet evrimi, sanal gerçeklik

THE DARK SIDE OF THE METAVERSE: DARKVERSE

ABSTRACT

The Metaverse is described as the evolution of the internet. Avatars represent users in the Metaverse. Avatar experiences within the metaverse can have positive and negative effects on real-world users. The games and applications currently defined as Metaverse show that we are only at the beginning of the journey. The area where illegal activities take place within the Metaverse is referred to as the Darkverse. In this review study, studies on security and privacy in the Metaverse literature were examined. As a result of the literature evaluation, it was determined that there was a lack of studies examining the concept of Darkverse. In this study, the concept of Darkverse is examined and it is aimed to contribute to the literature in this field. In addition, the evolution of the internet, the Metaverse and the basic components of the Metaverse were discussed in the study.

Keywords: Metaverse, dark universe, illegal, internet evolution, virtual reality

***Sorumlu Yazar (Corresponding Author)**

Atıf (Citation): Aslan, M.A., "Metaverse'ün Karanlık Yüzü: Darkverse" Akıllı Sistemler Dergisi, 3(1): 1-17, 2024

Geliş (Received): 02/02/2024
Kabul (Accepted): 15/05/2024
Yayın (Published): 30/06/2024

1. GİRİŞ (INTRODUCTION)

Teknolojinin gelişmesiyle birlikte hayatımıza birçok kavram girmiştir. Son zamanlarda adından sıkça bahsedilen bu kavramlardan birisi de Metaverse olmuştur. Metaverse, fiziksel dünyanın sanal gerçeklikle bütünleştiği çoklu kullanıcıların eş zamanlı olarak katılım sağladığı gerçek ötesi bir evrendir [1]. Metaverse terimi, ilk defa 1992 tarihinde yayınlanan "Snow Crash" isimli romanda, sanal gerçeklik evrenini ifade etmek için Neal Stephenson tarafından kullanılmıştır [2]. Metaverse'de, kullanıcıları avatarları temsil etmektedir [3]. Avatarlar Metaverse'de sosyal ilişkiler kurabilir, ekonomik ve kültürel faaliyetlerde bulunabilirler [4]. Avatar tabanlı etkileşim, sosyal varlık hissi ve imaj yönetimi üzerinde daha fazla kontrole olanak tanımaktadır, bu durum 3 boyutlu ortamda iletişim seviyesini arttırmaktadır [5].

Metaverse, Yapay Zeka, Blok Zinciri, Nesnelerin İnterneti ve Web 4.0 gibi çeşitli yeni teknolojik alanları içerisinde barındırmaktadır [6]. 2021 yılında Facebook'un Meta olarak adını değiştirmesi ve birçok şirketin Metaverse alanına büyük yatırımlar yapması, ilerleyen dönemlerde bu kavramın günlük hayatta daha fazla önem kazanacağına işaret etmektedir [7]. Zaman içerisinde Metaverse teknolojisinin gelişmesi ve kullanıcılar arasındaki ilginin artmasıyla birlikte, gizlilik ve güvenlik konuları da kritik bir hal almaktadır [8].

Metaverse literatürü incelendiğinde Metaverse konulu birçok çalışma yapılmış; ancak Metaverse'de yasadışı işlerin (sanal hırsızlık, yasadışı ticaret, fidye yazılımları, kimlik hırsızlığı, dolandırıcılık, sahtekarlık, terör eylemleri vb.) yapılmasıyla ilişkili Darkverse kavramı konusunda belirgin bir eksiklik saptanmıştır. Bu derleme kapsamındaki araştırmada, Metaverse literatüründe gizlilik ve güvenlik konuları üzerine yayınlanmış çalışmaların değerlendirilmesi yapılarak, Darkverse kavramına ilişkin öngörüler tartışılmıştır. Öngörülerin tartışılmasına konu olan bazı çalışma özetleri aşağıda verilmiştir.

Cheong (2022) yaptığı çalışmada, Metaverse ortamında kullanıcı avatarlarının karşılaşabileceği muhtemel sorunları incelemiştir. Bu sorunların çözümü için, avatarlara yapay kişilikler atfedilmesinin gerekliliği ve fikri mülkiyet hakkı ile tüketici koruma kanunlarının kullanılması önerilmektedir [9].

Mooij (2023) Metaverse ile ilişkili MLFT (Para aklama ve Terör Finansmanı) risklerini ele alan bir çalışma yapmıştır. Çalışmada MLFT'ye yönelik mevcut hukuki yaklaşımı değerlendirmek için bir çerçeve sunulmuştur. Ayrıca fon yerleştirme, kaynağın izlenmesi ve entegrasyon gibi MLFT aşamaları özelinde Metaverse'deki riskler tartışılmıştır. Çalışmada Metaverse'e özgü risklerin belirlenmesi ve mevcut yasal çerçevenin bu yeni riskleri içermesi gerektiği de vurgulanmıştır [10].

Wu ve diğerlerinin (2023) yaptığı çalışmada, Metaverse ortamındaki mali suçlarla ilgili bilinç düzeyinin arttırılması ve bununla ilgili düzenlemelerin daha etkili yapılmasına katkı sağlanması amaçlanmıştır. Araştırma, Metaverse içindeki mali suçların sınıflandırılmasıyla ilgili detaylı bir

analiz sunmaktadır. Ayrıca çalışmada veriye dayalı metaveri düzenlemesinin potansiyel avantajları ve engelleri tartışılmıştır [11].

Han ve diğerlerinin (2022) yaptığı çalışmada, Metaverse ortamında yeni çıkan tehditlere karşı etkili bir şekilde korunmak için geliştirilmiş olan Paralel Zeka temelli ParaDefender isimli bir sistem tanıtılmıştır. ParaDefender yapay siber uzayı, hesaplamalı deneyler ve paralel yürütme gibi özellikleri içermektedir. Ayrıca çalışmada ParaDefender sisteminin işleyişiyle ilgili Endüstriyel Nesnelerin İnternetinin Güvenliği ve Siber-Fiziksel-Sosyal Sistemlerde (CPSS) dolandırıcılığın önlenmesi gibi iki uygulama örneği sunulmuştur [12].

Wyczik'in (2024) çalışmasında, fikri mülkiyet hakları çerçevesindeki değişim ve yeniliklere odaklanılmaktadır. Fikri mülkiyet haklarının dijital ekonomiye entegrasyonunda ortaya çıkan zorluklar ve bu hakların nasıl yeniden düzenlenmesi gerektiği üzerine detaylı bir değerlendirme yapılmaktadır. Bu düzenlemelerin hazırlanmasında derinlemesine analiz yapılması, uzmanların ve araştırmacıların katılımı, iş dünyası ve diğer paydaşlarla istişare edilmesi gerektiği önerilmektedir [13].

Huang'ın (2023) çalışmasında, sosyalleşme, sürükleyici etkileşim, gerçek dünya inşa etme ve genişletilebilirlik, Metaverse'ün dört ana özelliği olarak tanımlanmıştır. Bu özelliklerle birlikte güvenlik ve gizlilik sorunlarının da ortaya çıktığı belirtilmiştir. Çalışmada bu dört ana özelliğin güvenlik ve gizlilik sorunları genişletilerek tartışılmış ve çözüm önerileri sunulmuştur [14].

Gupta'nın (2023) çalışmasında, Metaverse'de gizlilik, güvenlik ve kontrol sorunlarının çözümünün öneminden bahsedilmiştir. Bu güvenlik sorunlarının çözümü için Sıfır Güven Mimarisi (ZTA) modelinin uygulanması önerilmektedir [15].

Liyanaarachchi ve diğerlerinin (2024) yaptıkları çalışmada geleneksel gizlilik paradoksu genişletilerek "çoklu gizlilik paradoksu" kavramı tanıtılmıştır. Bu paradoksta, mahremiyet etkisinin sanal varlıklardan yasal paydaşlara aktarımı da ele alınmıştır. Ayrıca siber suçlarla ve yanlış bilgilerle mücadele etmek için kolektif bir stratejinin gerekliliği savunulmuştur. Bu stratejiyle, tüketici gizliliğini korumak ve Metaverse'deki sanal etkileyicilerle daha sağlıklı etkileşim kurmak amaçlanmıştır [16].

Kim ve diğerlerinin (2023) yaptıkları araştırmada, merkezi olmayan sistemlerin temel özelliği olan anonimliğin, kara para aklama ve yasa dışı döviz ticareti gibi suç faaliyetlerine zemin hazırladığı belirtilmiştir. Ayrıca bu tür aktivitelerin izlenmesi ve denetlenmesinin güç olduğu da vurgulanmıştır. Bu sebeple araştırmada avatar kimlik doğrulaması ve KYC (Müşterinizi Tanıyın) sürecinin önemi üzerinde durulmuştur. Bunun yanında akıllı sözleşmeler kullanılması ve KYC sürecinin tamamlanarak, kullanıcı kimliğini doğrulayan bir strateji sunulmuştur [17].

Mandal ve diğerlerinin (2022) yaptığı çalışmada ise Metaverse tanımının ne ifade ettiğine dair bir çerçeve çizilmiş ve bu kavram içerisinde karşılaşması muhtemel güvenlik ve gizlilik meseleleri ele alınmıştır. Çalışmada gizlilik ve güvenlik sorunlarına bazı öneriler sunulmuştur. Gizlilik amacıyla kullanıcıların kendi klonlarını oluşturabileceği veya belirli bir alanda diğer

kullanıcıları engelleyebileceği ifade edilmiştir. Güvenlik bağlamında ise kullanıcı kimliğinin birden fazla kaynak tarafından yönetilmesi yerine, kullanıcının kendisinin herhangi bir kurumdan bağımsız olarak kimliği yönetmesi önerilmiştir [18].

2. İNTERNET VE METAVERSE (INTERNET AND METAVERSE)

İnternetin, Metaverse'e dönüşüm süreci, teknolojinin ilerlemesine ve kullanıcı alışkanlıklarının değişimine bağlıdır. Metaverse'ün bir katmanı olan Darkverse ile günümüzde internetin karanlık tarafını temsil eden Dark Web katmanı birbirine benzer özellikler içermektedir. Bu nedenle, Metaverse ve Darkverse terimlerini daha iyi kavramak için, internetin katmanlarını ve internetin geçmişteki gelişimini anlamak önemlidir.

2.1. İnternetin Tanımı ve Tarihçesi (Definition And History Of The Internet)

İnternet, dünya üzerindeki bilgisayarların ve elektronik aygıtların (cep telefonları, akıllı cihazlar, sensörler vd.) birbiriyle iletişim kurabildiği, veri ve bilgi alışverişi yapabildiği bir ağ sistemidir. Amerikan Savunma Bakanlığı'nın girişimleriyle 1969 yılında oluşturulan ARPA ağı olarak tanımlanan ARPANET, internetin temeli oluşturmaktadır [19]. İnternetin oluşturulmasından iki sene sonra 1971 yılında Ray TOMLİNSON tarafından e-posta geliştirilmiştir. E-posta, internet kullanıcıları arasında iletişim kurmanın kolay ve hızlı bir yoludur. 1980'li yıllara kadar ARPANET üniversiteler ve çeşitli kurumlarda ağ sistemini genişletmiştir. 1983 yılında ise özel bir ağ sistemi olan ARPANET projesi, yerini TCP/IP (Transmission Control Protocol/Internet Protocol) Protokol yapısına bırakmış ve böylelikle internetin dünya çapında yaygınlaşmasının ilk adımı atılmıştır.

İnternetin herkes tarafından kolayca kullanılabilmesini sağlayan olay, World Wide Web (WWW) isimli paylaşım sisteminin icat edilmesi olmuştur. Türkçesi Dünya Çapında Ağ olarak ifade edilen World Wide Web paylaşım sistemi, farklı bilgisayarlar ve sunucuların birbirine bağlanabildiği, bilgi ve multimedya gibi içerik alışverişinin yapılabildiği bir sistemdir. World Wide Web ile insanlar bilgiye daha hızlı ve kolay ulaşabilmektedir. İnternetin zaman içerisinde gelişimi ve değişimi kullanıcı sayılarının da hızla artmasını sağlamıştır. Dijital 2023: Küresel Genel Bakış raporuna göre; 2023 yılında dünya üzerinde 5,16 milyar internet kullanıcısı bulunmaktadır ve bu rakam dünya nüfusunun %64,4'ünü oluşturmaktadır [20].

2.2. İnternetin Katmanları (Layers Of The Internet)

İnternet, Surface Web (Yüzey Ağ), Deep Web (Derin Ağ) ve Dark Web (Karanlık Ağ) olmak üzere üç katmandan oluşmaktadır [21].

Surface Web, arama motorlarının (Google, Baidu, Yandex vd.) veri tabanına eklenmiş, genel kullanıcıların kullandığı Chrome, Firefox, Opera ve Microsoft Edge gibi tarayıcılar ile kolaylıkla ulaşılabilen web sayfalarıdır [22]. Surface Web, internetin büyük bir bölümünü kapsıyor gibi algılansa da aslında sadece %4'lük bir kısmını oluşturmaktadır.

Deep Web, internetin genel arama motorları tarafından indekslenmeyen ve doğrudan erişilemeyen kısmını ifade eder. Deep Web, internetin %90'lık bir alanını oluşturmaktadır [23]. Deep Web, çoğunlukla gazeteciler, aktivistler, araştırmacılar, ajanlar, muhbirler, terör örgütü üyeleri, silah kaçakçıları ve uyuşturucu satıcıları gibi internette anonim olmak isteyen kişiler ve gruplar tarafından kullanılmaktadır. Deep Web'e erişmek için en yaygın kullanılan araçlardan birisi Tor tarayıcısıdır [24]. Tor tarayıcısı internette gizliliği korumak için geliştirilmiş bir tarayıcıdır. Tor tarayıcısını kullanan kullanıcıların gerçek kimliği gizlidir ve takip edilmesi zordur. Tablo 1'de Tor tarayıcısını kullanan ülkelerin günlük ortalama kullanıcı sayıları verilmiştir. Rusya, İran ve Amerika Birleşik Devletleri, Tor tarayıcısını günlük kullanıcı bazında en çok tercih eden ülkeler arasında yer almaktadır.

Tablo 1. Tor tarayıcısının en yaygın olarak kullanıldığı 10 ülke (The 10 countries where the Tor browser is most widely used) [25].

ÜLKE	ORTALAMA GÜNLÜK KULLANICI
Rusya	47253 (%30,04)
İran	39164(%24,89)
Amerika Birleşik Devletleri	23115(%14,69)
Almanya	463(%2,84)
Çin	4040 (%2,57)
Fransa	2856 (%1.82)
Birleşik Krallık	2797(%1.78)
Türkmenistan	2751 (%1.75)
Hollanda	2103(%1.34)
Hindistan	1995 (%1.27)

Dark Web, Deep Web'in daha karanlık ve özel kısmıdır. Dark Web internetin %6'lık bir alanını oluşturmaktadır. Dark Web'de özel şifreler ve referans sistemi kullanılmaktadır. Dark Web'de kullanıcılar daha çok takma isimleri ile tanınmaktadır. Yasadışı işlemlerin yapıldığı bu sitelere tanıdık isimler veya referans alan kişiler girebilmektedir.

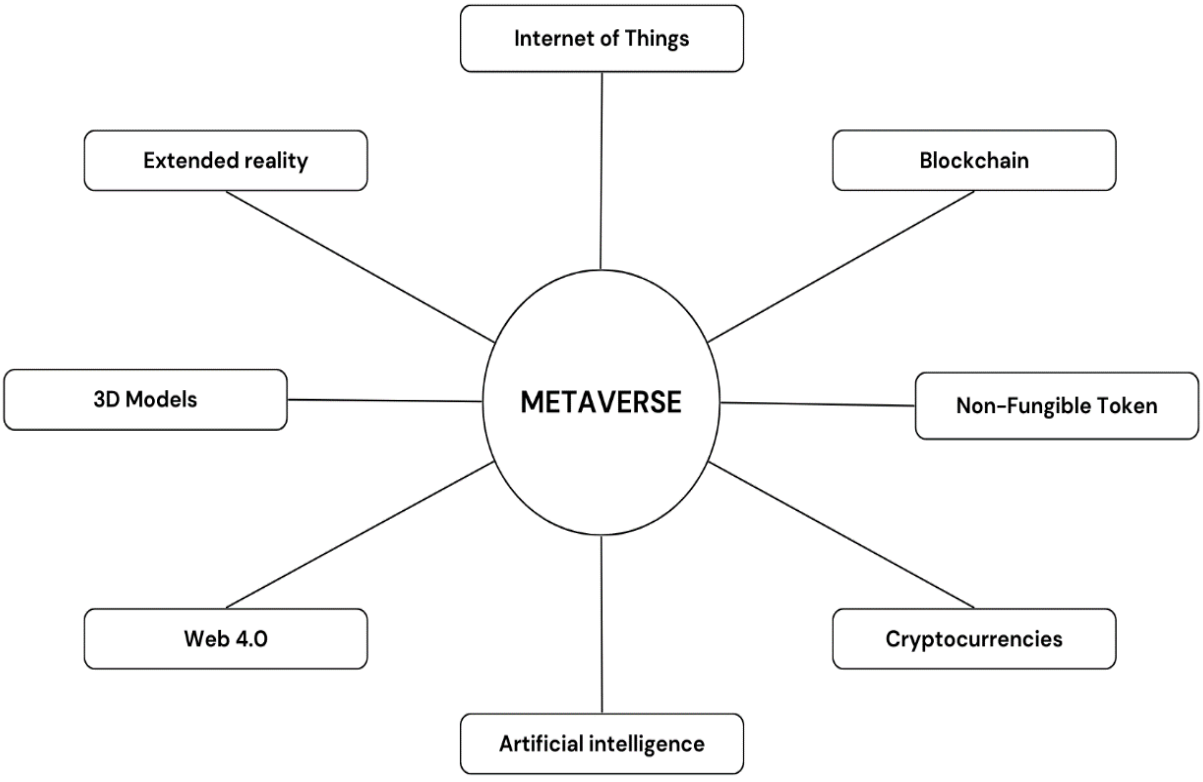
Dark Web'in dünya çapında bilinirliği Silk Road (İpek Yolu) internet sitesi sayesinde olmuştur [26]. Silk Road, Tor üzerinde çalışan uyuşturucu, silah ve yasadışı ürünlerin satışının yapıldığı bir sitedir. Bu sitede satıcıların ve alıcıların gerçek kimlikleri yerine takma isimler kullanılmaktadır. Silk Road 2011-2013 yılları arasında faaliyet göstermiş Federal Soruşturma Bürosu'nun (Fedaral Bureau of Investigation-FBI) 2013 yılında yapmış olduğu operasyon ile

kapatılmıştır. FBI'nın resmi açıklamalarına göre Silk Road üzerinden değeri 1.2 milyar dolar olan 51.000 adet Bitcoin ele geçirilmiştir [27]. Bu olay Dark Web üzerinden yapılmış en büyük bütçeli yasadışı faaliyet olarak tarihe geçmiştir. Silk Road sitesinin dünya çapında bu kadar tanınıp popüler olması, Dark Web'de yasadışı iş yapan birçok yeni web sitesinin açılmasına yol açmıştır [28].

2.3. Metaverse ve Temel Bileşenleri (Metaverse And Basic Components)

Metaverse, internetin yeni bir evrimi olarak kabul edilen bir vizyondur. İnsanların fiziksel dünyada yaşayamayacakları deneyimleri, dijital ikizleri veya avatarlarıyla birebir eşleşerek deneyimleyebildiği, kalıcı ve üç boyutlu sanal bir dünyadır [29]. Artırılmış gerçeklik, sanal gerçeklik, karma gerçeklik ve blok zinciri teknolojisini entegre eden kompleks sanal bir dünya olan Metaverse; insanların gerçek dünyadaki faaliyetlerini, sosyal etkileşimlerini ve alışkanlıklarını sanal gözlükler, konsollar ve avatarlar gibi araçlarla dijital olarak deneyimlemelerine imkan vermektedir [30].

Metaverse teknolojisini oluşturan temel bileşenler Şekil 1'de verilmiştir.



Şekil 1. Metaverse'ün Bileşenleri (Components of Metaverse)

Metaverse'ün temel bileşenleri aşağıdaki gibidir.

Nesnelerin İnterneti (Internet of Things):

Nesnelerin interneti, internet özelliği olan cihazların birbirleriyle veri alışverişinde bulunarak iletişim kurabilmesi olarak tanımlanır. Nesnelerin interneti, insanların günlük hayatta işlerini hızlandırarak onlara yaşamdan zaman kazandıran bir teknolojidir [31]. Bu teknoloji insanların evde ve işte daha verimli olmalarını sağlayarak, yaşam kalitelerini artırmak için önemli bir araçtır.

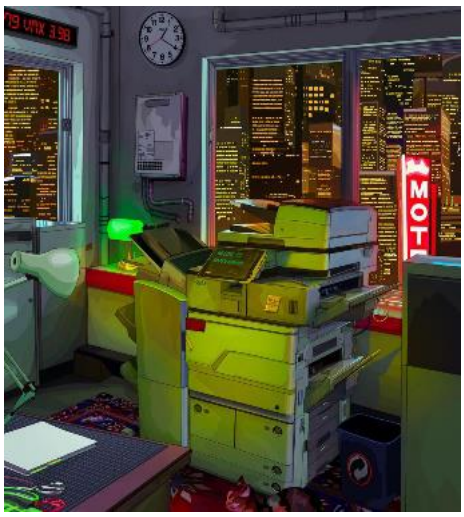
Blok zinciri (Blockchain):

Blok zinciri teknolojisi, teknolojinin yeniliklerinden biri olarak değerlendirilen ve kripto para birimleriyle ilişkilendirilerek dikkat çekmeye başlamış, ancak kendine özgü mekanizmasıyla dijital ortamlardaki herhangi bir değerin güvenli bir şekilde depolanmasını ve hızlıca taşınmasını sağlayarak dijital dönüşüm sürecinde önemli bir araç haline gelen bir teknolojidir [32].

Değiştirilemez Jeton (Non-Fungible Token):

Non Fungible Token (NFT), blok zinciri sistemini kullanarak oluşturulan eşsiz dijital varlıklar olarak tanımlanmaktadır ve Türkçe diline "değiştirilemez jeton" ismiyle çevrilmiştir. Herhangi bir tablo, resim, çizim veya bir video blok zinciri sistemine kaydedilerek NFT'ye dönüştürülebilmektedir. NFT'ler çeşitli amaçlarla kullanılabilmektedir. Örneğin; oluşturulan NFT'ler Metaverse'de bir sanat galerisinde sergilenebilmektedir. NFT'lerin yalnızca bir sanat eseri olmasının dışında parasal karşılığı olan bir varlık gibi dijital olarak alım ve satımı da yapılabilmektedir. OpenSea, Binance NFT ve Rarible gibi uygulamalarda NFT alım satımı yapılabilmektedir. Şekil 2'de NFT sanatçısı Beeple tarafından oluşturulan Ocean Front isimli NFT, 6 milyon dolara satılmıştır [33]. Şekil 3'te verilen Replicator isimli NFT'yi ise Mad Dog JONES tasarlamış ve 4.1 milyon dolara satılmıştır [34].

Şekil 2. NFT Örnek 1 (NFT Example 1) [35].



Şekil 3. NFT Örnek 2 (NFT Example 2) [36].

Kripto Paralar (Cryptocurrencies):

Kripto paralar, fiziksel karşılığı olmayan, merkezi bir otoriteye bağlı olmaksızın hareket eden, belirli bir merkeziyeti bulunmayan, elektronik platformlarda işlem gören, daha düşük maliyetli, hızlı ve güvenli para transferi aracı olarak tanımlanan sanal paralardır [37]. Satoshi Nakamoto takma isimli bir kişi tarafından 2008 yılında çıkartılan ilk kripto para Bitcoin'dir. Bitcoin teknolojisi, sanal para transferlerinde, aradaki finansal kuruluşlara gerek olmadan doğrudan kişilerin kendi aralarında para transferi yapabilmelerini sağlamıştır.

Bitcoin'in çıkışından itibaren çoğunlukla yasadışı işlerde kullanılması insanların uzun yıllar Bitcoin'e mesafeli durmasına neden olmuştur. Ancak 2017 yılında Bitcoin'in değerinde yaşanan büyük artışlar sebebiyle dünyada Bitcoin'in bilinirliği artmış ve insanlar Bitcoin'i, değeri üzerinden para kazanabilecekleri bir yatırım aracı olarak görmeye başlamışlardır. 2021 yılında 1 Bitcoin'in değeri 65 bin doları geçerek Bitcoin tarihinin en yüksek değerine ulaşmıştır [38]. Bitcoin'in tüm dünyada popülerliğinin artmasıyla birlikte birçok yeni kripto para da ortaya çıkmıştır. Günümüzde, ortaya çıkmış yirmi binden fazla kripto para olduğu tahmin edilmektedir. Bitcoin'den sonra Ethereum, Ripple (XRP), Binance Coin (BNB) gibi kripto paralar dünya borsalarında en fazla işlem yapılan ve bilinirliği olan kripto paralardan bazılarıdır.

Yapay Zeka (Artificial intelligence):

Alan Turing yapay zekanın öncüsü olarak bilinse de gerçekte bu terim ilk kez 1956'da John McCarthy tarafından bir çalıştayda kullanılmıştır [39]. Yapay zeka problem çözebilme,

öğrenebilme (veri öğrenmesi), öğrendiklerini problemin çözümüne uygun şekilde kullanabilme ve genelleme yapabilme gibi insana özgü davranışları yapabilen sistemlerdir. Günümüzde yapay zeka hayatın her alanında kullanılmaya başlanmış ve çok hızlı bir şekilde gelişmeye devam etmektedir.

Web 4.0:

Web 1.0, internetin ilk halidir. Web 1.0'da kullanıcılar, sayıları çok az olan web sayfalarını yalnızca okuyabildikleri pasif tüketici konumundadır. Web 2.0'la birlikte kullanıcılar artık internette etkileşim kurabilir ve üretebilir hale gelmiştir. Forum sayfaları, sosyal medya ve içerik üretme sayfaları (video, oyun, uygulama vd.) artık kullanıcıların internette etkileşim kurabilmesini, tüketici olmasının yanında üretici olarak da internet kullanımına imkan vermiştir. Web 3.0, mevcut hizmetlerin işlevlerini iyileştirmeye odaklanıp, yapay zeka ve veri bilimi gibi yeni teknolojileri kullanarak kişiyi tanıma ve ona uygun içerikler sunma gibi hizmetlerle birlikte internetin gelişimine odaklanmaktadır [40]. Web 4.0, gelecekte kullanılacak olan web teknolojisine verilen isimdir. Web 4.0, web üzerindeki bilgileri daha anlamlı, daha güvenli ve daha hızlı kullanan bir teknolojidir. Bu teknoloji kullanıcılara kişiselleştirilmiş deneyimler sunmaktadır.

Üç boyutlu modelleme (3D Models):

Üç boyutlu modelleme, bilgisayar yazılımı kullanılarak üç boyutlu nesnelerin oluşturulması veya düzenlenmesi sürecidir. Bu süreçte tasarımcı, bir nesnenin hacmini, şeklini ve özelliklerini bilgisayar ortamında oluşturmaktadır.

Genişletilmiş gerçeklik (Extended reality):

Genişletilmiş gerçeklik, sanal dünyaları ifade eden virtual reality (sanal gerçeklik) teknolojisini, gerçek dünyadaki sanal katmanları ifade eden augmented reality (artırılmış gerçeklik) teknolojisini ve mixed reality (karma gerçeklik) teknolojisini birleştiren bütünleştirici bir kavram olarak kullanılmaktadır.

Sanal gerçeklik, kullanıcılara çeşitli yazılımlar sayesinde oluşturulmuş, gerçek olmayan sanal dünyalar sunan bir teknolojidir [41]. Bu deneyim için, sanal gözlükler, konsollar ve akıllı kulaklıklar gibi teknolojik ekipmanlar kullanılmaktadır [42].

Artırılmış gerçeklik, telefon ve bilgisayar gibi cihazlar kullanılarak gerçek dünyanın içerisinde sanal bir katman oluşturan çeşitli yazılımlardır [43]. Pokemon Go oyunu ve Google 3D uygulaması artırılmış gerçeklik teknolojisinin örneklerindendir.

Karma gerçeklik; sanal gerçeklik ve artırılmış gerçekliği aynı anda kullanabilme imkanı veren bir teknolojidir [44]. Karma gerçeklik sayesinde gerçek ve sanal dünyalar arasında geçiş yapılabilmektedir.

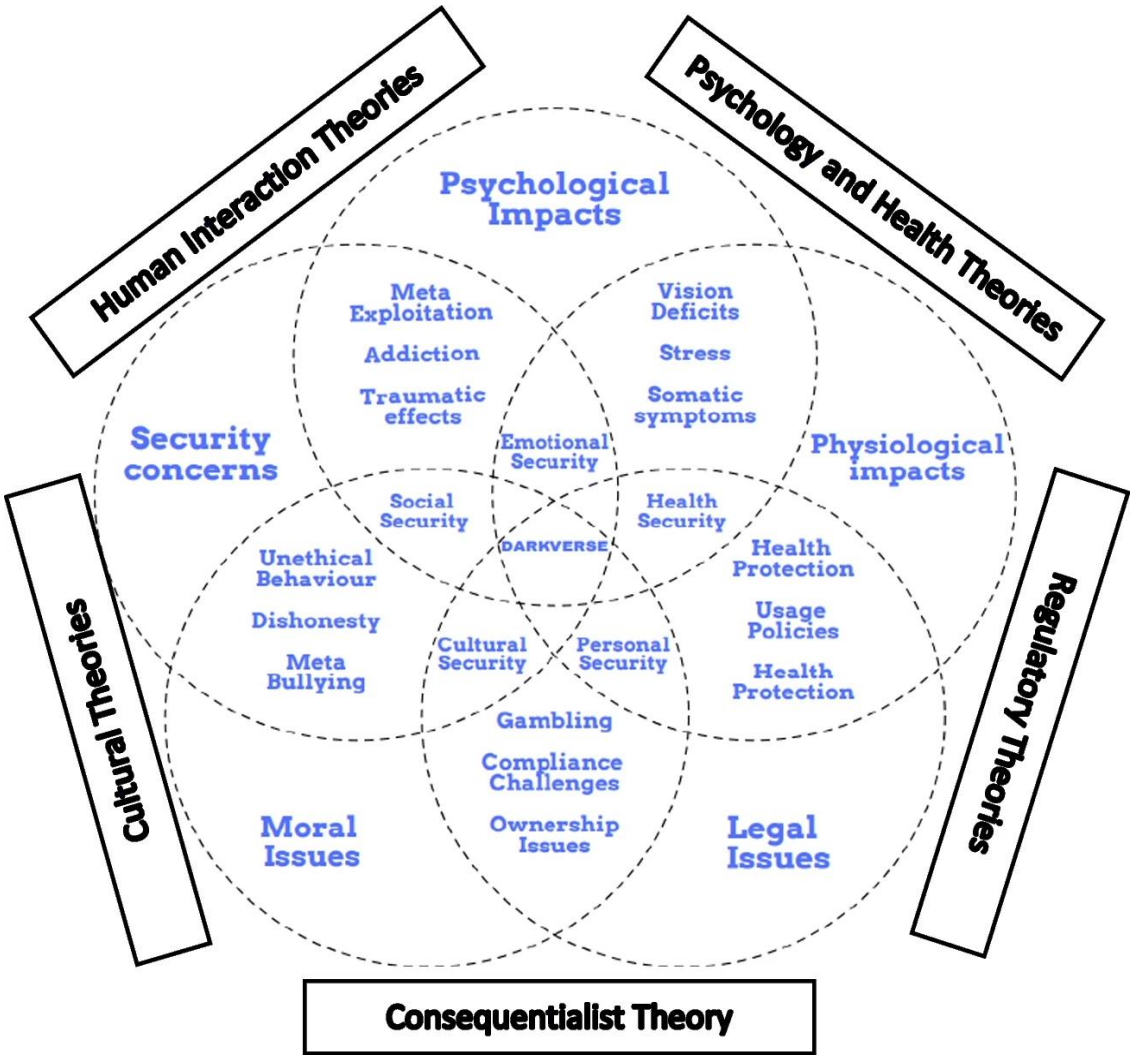
2.4. Metaverse'ün Karanlık Katmanı: Darkverse (Dark Layer of the Metaverse: Darkverse)

Darkverse, Metaverse ortamında yasadışı faaliyetlerin gerçekleştirilebileceği bir alanı ifade etmektedir [45]. Darkverse'de oluşabilecek suçlar arasında kimlik hırsızlığı, saldırgan pazarlama yöntemleri, manipülasyonlar, finansal suçlar, terörizm, istismar, cinsel taciz, kumar, uyuşturucu ve silah kaçakçılığı bulunmaktadır [46]. Bu yönüyle Darkverse, Dark Web ile benzer özellikler göstermektedir. Pek çok haber sitesi Darkverse'ü sadece çevrimiçi suçların gerçekleştiği ayrı bir platform olarak ele alsa da aslında Darkverse, Metaverse ortamı içinde farklı bir ekosistem olarak çok yönlü bir şekilde var olabilmektedir [47].

Mataverse'de kullanıcıların kimlik doğrulamasına ilişkin yasal bir zorunluluk bulunmadığı için, kullanıcılar Metaverse'de kolaylıkla anonim kalabilmektedir [48]. Darkverse ortamında anonim kalmak, işlenecek suçların daha kolay gerçekleştirilmesine olanak tanımaktadır.

Darkverse katmanı, Metaverse içerisinde herhangi bir bölgeye konumlandırılabilmekte ve bu özel alanlara sadece uygun kimlik kontrolü yapılmış kullanıcılar erişebilmektedir [49]. Kimlik kontrolü için kimlik doğrulama jetonları veya şifreli kapılar kullanılabilmektedir. Darkverse'de kullanıcılar, kimlik doğrulama jetonları sayesinde, yasadışı faaliyetler için oluşturulmuş bu alanlara kolaylıkla erişim sağlamaktadırlar [50]. Kimlik doğrulama jetonuna sahip olmak isteyen bir kullanıcının, belirli bir konum ve zaman diliminde, satıcılar tarafından belirlenen yerde bulunması gerekebilmektedir [51]. Bu durum Darkverse'de yasadışı faaliyet yapılan alanların ve kişilerin deşifre olmaması için satıcıların aldığı önlemlerden birisi olabilmektedir. Ayrıca kullanıcıların Darkverse'de iletişim kurabilmek için, avatarlarının birbirilerine yakın bir mesafede olmaları gibi, bir güvenlik şartı da oluşturulabilmektedir [52]. Bu gibi önlemler, güvenlik güçlerinin bu alanlara girebilmelerini çok zorlaştırmakta hatta imkansız hale getirmektedir.

Şekil 4'te Darkverse'ün bütünsel bir modeli verilmiştir. Darkverse'ün bütünsel modeli, psikolojik etkiler, fizyolojik etkiler, yasal sorunlar, ahlaki konular ve güvenlik endişeleri olmak üzere beş ana tema üzerine kurulmuştur [53]. Darkverse'e bağlı olarak ortaya çıkan sonuçlar, iki tema arasındaki kesişen konuları yansıtmaktadır [54]. Örneğin Darkverse ortamında gerçekleştirilen kumar eylemi "ahlaki konular" ve "yasal sorunlar" başlıklı temalar ile ilintilidir.



Şekil 4. Darkverse'ün Bütünsel Bir Modeli (A Holistic Model of the Darkverse) [55].

3. SONUÇ VE ÖNERİLER (CONCLUSION & SUGGESTIONS)

Metaverse, "gerçeklik" kavramına yakınlaşırken "gerçek" olandan uzaklaşılan bir mekandır. Gerçek; var olan, somut ve objektif olanı ifade etmektedir. Gerçeklik, algıladığımız veya deneyimlediğimiz dünya ve olaylar hakkındaki bilincimizi ifade etmektedir. Bu nedenle, her kullanıcının Metaverse'deki "gerçekliği" farklıdır. Metaverse ortamında yaşananlar, kullanıcıların gerçek hayattaki duygu, düşünce, davranış ve becerilerini etkileyebilmektedir. Örneğin; iş dünyasında, sanal toplantılar ve sanal iş ortamları, gerçek hayatta iletişimi ve iş ilişkilerine yön verebilmektedir. Sanal bir ortamda çalışmak, ekip çalışması becerilerini geliştirmek ve çalışanlar arası iletişimi şekillendirmek için fırsatlar sunabilmektedir. Ancak,

sanal ortamda yaşanan stres veya iletişim sorunları, gerçek hayattaki ilişkilere de yansıyabilmektedir.

Bugün bazı çevrelerce Metaverse olarak tanımlanan Roblox, Axie Infinity, Decentraland ve Fortnite gibi uygulamaların, gelecekte beklenen Metaverse dünyasının öngörülen standartlarını karşılamaktan uzak olduğunu söylemek mümkündür. Aynı ifadeyi Metaverse ortamında kullanılması beklenen teknolojik cihazlar (sanal gözlükler, akıllı kulaklıklar, konsollar vb.) içinde söyleyebiliriz. Çünkü kullanıcıların gerçek dünyadan tamamen soyutlanarak kendilerini Metaverse ortamında bambaşka bir evrendeymiş gibi hissedebilmeleri için daha gelişmiş teknolojilere ihtiyaç vardır. Ancak bu ve benzeri gelişmeleri, gelecekteki Metaverse dünyasının oluşum sürecinin birer adımı olarak nitelendirilebilmektedir.

Metaverse'ün yeni bir teknoloji olması ve birçok bileşenden oluşması yeni güvenlik zafiyetini de beraberinde getirmektedir. Bu durum Metaverse ortamını, yasadışı işlerin kolaylıkla gerçekleştirildiği bir mekana dönüştürmektedir. Metaverse içerisinde yasadışı faaliyetlerin yapıldığı alan, "Darkverse" olarak adlandırılmaktadır. Darkverse, Metaverse içerisinde herhangi bir alanda faaliyet gösterebilmektedir. Örneğin; Metaverse'deki bir NFT sergisi, bir sanatçının eserlerinin sergilendiği bir yer olmasının yanında, uyuşturucu satışının yapıldığı bir pazaryerine dönüşebilir. Darkverse alanına girebilmek için gerekli şartları (belirtilen konumda olma, kimlik doğrulama jetonu, yakın eşleşme vb.) sağlayan kullanıcılar kolaylıkla istediklerini elde edebilmektedir.

"Metaverse içerisinde avatarlara dijital kimlik verilecek mi? Avatarın işlediği bir suçun cezası olacak mı? Avatarlar hacklenebilecek mi?" gibi sorular ve çok daha fazlası çözüm beklemektedir. Metaverse, doğası gereği merkeziyetsiz ve kullanıcıların tamamen anonim kalabildiği bir yerdir. Bu merkeziyetsizlik ve anonimlik kullanıcılara bir özgürlük sağlamaktadır. Ancak bu özgürlük, kullanıcıları suça teşvik edebilmektedir. Bu nedenle avatarlara dijital kimlik verilerek herhangi bir suça karışmadığı sürece gerçekleştirdiği eylemlerde tamamen anonim kalabildiği sistemler oluşturulması önerilmektedir. Metaverse ile ilgili konular, uluslararası bir mutabakatla ele alınmalı, yasal bir zemine oturtularak tüm kullanıcıların haklarını koruyacak şekilde kapsamlı bir çerçeve çizilmesi gerekmektedir. Aksi taktirde çok sayıda kullanıcı bu durumdan olumsuz etkilenecektir. Bu durum şirketlerin, kurumların, toplulukların ve ülkelerin en kısa sürede ele alması gereken bir meseledir. Yeni çalışmalar için ise; Darkverse kavramının, Metaverse'de güvenlik ve gizlilik konuları içerisinde yer alması ve farklı yönleriyle incelenmesi önerilmektedir.

ÇIKAR ÇATIŞMASI REDDİ

Bu çalışma ile hiçbir şekilde çıkar elde edilmemiştir.

KAYNAKLAR (REFERENCES)

1. Mystakidis, S., "Metaverse", Encyclopedia, 2(1), 486-497, 2022.

2. Joshua, J., "Information bodies: computational anxiety in neal stephenson's snow crash", Interdisciplinary Literary Studies, 19(1), 17-47, 2017.

3. Di Pietro, R., & Cresci, S., "Metaverse: Security and privacy issues", In 2021 third IEEE international conference on trust, privacy and security in intelligent systems and applications (TPS-ISA), 281-288, 2021.

4. Chen, S.C., "Multimedia research toward the metaverse", IEEE MultiMedia, 29(1), 125-127, 2022.

5. Van der Land, S., Schouten, A., & Feldberg, F. "Modeling the metaverse: A theoretical model of effective team collaboration in 3D virtual environments", Journal of Virtual Worlds Research, 4(3), 2011.

6. Ali, S., Abdullah, Armand, T. P. T., Athar, A., Hussain, A., Ali, M., ... & Kim, H.C., "Metaverse in healthcare integrated with explainable ai and blockchain: Enabling immersiveness, ensuring trust, and providing patient data security", Sensors, 23(2), 565, 2023.

7. Nazlı, A.K., Beşbudak, M., & Akşit, O.O., "Metaverse Evreninde Yer Alan Bazı Uygulamalar Üzerine Tematik Bir Analiz", TRT Akademi, 7(16), 1096-1119, 2022.

8. Parlar, T., In Metaverse: Technologies, Opportunities and Threats (pp. 123-133), Singapore: Springer Nature Singapore, 2023.

9. Cheong, B.C., "Avatars in the metaverse: potential legal issues and remedie", International Cybersecurity Law Review, 3(2), 467-494, 2022.

10. Mooij, A., "Money Laundering and Financing of Terrorism via the Metaverse", In Regulating the Metaverse Economy: How to Prevent Money Laundering and the Financing of Terrorism (pp. 21-34), Cham: Springer Nature Switzerland, 2023.

11. J. Wu, K. Lin, D. Lin, Z. Zheng, H. Huang and Z. Zheng, "Financial Crimes in Web3-Empowered Metaverse: Taxonomy, Countermeasures, and Opportunities," in IEEE Open Journal of the Computer Society, vol. 4, pp. 37-49, 2023.

12. Han, J., Yang, M., Chen, X., Liu, H., Wang, Y., Li, J., ... & Ma, X. "Paradefender: A scenario-driven parallel system for defending metaverses", IEEE Transactions on Systems, Man, and Cybernetics: Systems, 53(4), 2118-2127, 2022.

13. Wyczik, J. "The rise of the metaverse: tethering effect and intellectual property of crypto tokens", Journal Of Intellectual Property Law and Practice, jpad124. 2024.

14. Huang, Y., Li, Y. J., & Cai, Z., "Security and privacy in metaverse: A comprehensive survey", Big Data Mining and Analytics, 6(2), 234-247, 2023.

15. Gupta, A., Khan, H. U., Nazir, S., Shafiq, M., & Shabaz, M., "Metaverse security: Issues, challenges and a viable ZTA model", Electronics, 12(2), 391, 2023.

16. Liyanaarachchi, G., Mifsud, M. ve Viglia, G., "Virtual performances and data privacy: An introduction to the Multiple Privacy paradox", Journal of Business Research, 176, 114584, 2024.

17. Kim, G. ve Ryou, J., "Digital Authentication System Using DID and SBT in Avatar", Math, 11 (20), 4387, 2023.

18. Mandal, T., Sağır, A. B., Öztürk, M. N. A., Uysal, M.Y., vd., "Metaverse: Sanal Dünyadan Gerçek Gizlilik ve Güvenlik Problemlerine", İstanbul Sabahattin Zaim Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 4(2), 100-106, 2022.

19. Ertan, A., "Nesnelerin İnternetinin Kişisel Verilerin Korunması Kapsamında İncelenmesi", Kişisel Verileri Koruma Dergisi, 4(2), 48-68, 2022.

20. Wearesocial. Digital 2023: Global Overview Report. https://wearesocial.com/wp-content/uploads/2023/03/Digital-2023-Global-Overview-Report.pdf. Yayın Tarihi Ocak 26, 2023. Erişim tarihi Eylül 10, 2023.

21. Sönmez, G., & Çelik, E. "Anonimlik ile İllegalite Arasında: Deep Web, Dark Web ve Devlet Dışı Silahlı Aktörlerin Uluslararası Siber Faaliyetleri", Güvenlik Çalışmaları Dergisi, 22(1), 66-88, 2020.

22. Chertoff, M., "A public policy perspective of the Dark Web", Journal of Cyber Policy, 2(1), 26-38, 2017.

23. Basheer, R., & Alkhatib, B., "Threats from the dark: a review over dark web investigation research for cyber threat intelligence", Journal of Computer Networks and Communications, 2021, 1-21, 2021.

24. Sönmez, G., & Çelik, E. "Anonimlik ile İllegalite Arasında: Deep Web, Dark Web ve Devlet Dışı Silahlı Aktörlerin Uluslararası Siber Faaliyetleri", Güvenlik Çalışmaları Dergisi, 22(1), 66-88, 2020.

25. Torproject. Top-10 countries by bridge users. https://metrics.torproject.org/userstats-bridge-table.html. Yayın Tarihi Eylül 01,2023. Erişim Tarihi Eylül 08, 2023.

26. Tsuchiya, Y., & Hiramoto, N., "Dark web in the dark: Investigating when transactions take place on cryptomarkets", Forensic Science International: Digital Investigation, 36, 301093, 2021.

27. FBI. Ross William Ulbricht's Laptop. https://www.fbi.gov/history/artifacts/ross-william-ulbrichts-laptop. Yayın Tarihi Aralık 01,2020. Erişim Tarihi Ekim 15, 2023.

28. Hayes, D. R., Cappa, F., & Cardon, J., "A framework for more effective dark web marketplace investigations", Information, 9(8), 186, 2018.

29. Baltacı, Ş., "Metaverse üzerine bir değerlendirme", TRT Akademi, 8(17), 472-479, 2023.

30. Kavut, S., "Toplumsal Yaşamda Metaverse: Metaverse Haberleri Üzerine Bir Değerlendirme", TRT Akademi, 8(17), 342-367, 2023.

31. Yılmaz, R. K., "Kamu Yönetiminde Kullanılabilecek Nesnelerin İnterneti (Iot) Uygulamaları", Kamu Yönetimi ve Teknoloji Dergisi, 5(1), 87-98, 2023.

32. Selimoğlu, S., & Saldı, M. H., "İç Denetimin Blok Zincir Yoluyla Siber Güvenlik Yönetimine Adaptasyonu", Denetim ve Güvence Hizmetleri Dergisi, 2(2), 121-134, 2022.

33. https://bluecastleventures.ca/the-five-most-expensive-nfts-that-have-been-sold/ Yayın Tarihi Şubat 23,2023. Erişim Tarihi Mart 10,2024.

34. https://news.artnet.com/market/phillips-4-4m-sale-of-mad-dog-nft-1961626 Yayın Tarihi Nisan 16,2021. Erişim Tarihi Mart 10,2024.

35. https://bluecastleventures.ca/the-five-most-expensive-nfts-that-have-been-sold/ Yayın Tarihi Şubat 23,2023. Erişim Tarihi Mart 10,2024

36. https://news.artnet.com/market/phillips-4-4m-sale-of-mad-dog-nft-1961626 Yayın Tarihi Nisan 16,2021. Erişim Tarihi Mart 10,2024.

37. Güngör Karyağdı, N., & Yolci, M., "Kripto Para Kavramı ve Denetimi", Turkish Business Journal, 4(7), 1-13, 2023.

38. https://tr.investing.com/crypto/bitcoin/chart Yayın Tarihi Mart 12,2024. Erişim Tarihi Mart 12,2024.

39. Çoşkun, F., & Gülleroğlu, H. D., "Yapay Zekanın Tarih İçindeki Gelişimi ve Eğitimde Kullanılması", Ankara University Journal of Faculty of Educational Sciences (JFES), 54(3), 947-966, 2021.

40. Kapan, K., & Üncel, R., "Gelişen web teknolojilerinin (web 1.0- web 2.0- web 3.0) Türkiye turizmine etkisi", Safran Kültür ve Turizm Araştırmaları Dergisi, 3(3), 276-289, 2020.

41. Süygün, M. S., & Bozyiğit, S., "Dış Ticaret ve Lojistik Eğitiminde Dijital Oyun Tabanlı Öğrenme: Kavramsal Bir İnceleme", Çağ Üniversitesi Sosyal Bilimler Dergisi, 16(1), 36-48, 2019.

42. Özmen B, Ceyhan A., "Diş Hekimliğinde Sanal Gerçeklik Uygulamaları", NEU Dent J., 5(3), 224-3, 2023.

43. Uzun, Y., Ergün, H., & Şeker, E., "Hikayeler İçin Artırılmış Gerçeklik Yaklaşımı", Necmettin Erbakan Üniversitesi Fen ve Mühendislik Bilimleri Dergisi, 4(2), 1-7, 2022.

44. Künüçen, H. H., & Samur, S., "Dijital Çağın Gerçeklikleri Sanal, Artırılmış, Karma ve Genişletilmiş Gerçeklikler Üzerine Bir Değerlendirme", Yeni Medya, 2021(11), 38-62, 2021.

45. https://www.trendmicro.com/vinfo/tr/security/definition/darkverse Yayın Tarihi Nisan 10,2023. Erişim Tarihi Ocak 07,2024.

46. Dwivedi, Y. K., Kshetri, N., Hughes, L., Rana, N. P., Baabdullah, A. M., Kar, A. K., ... & Yan, M., "Exploring the darkverse: A multi-perspective analysis of the negative societal impacts of the metaverse", Information Systems Frontiers, 25(5), 2071-2114, 2023.

47. Dwivedi, Y. K., Kshetri, N., Hughes, L., Rana, N. P., Baabdullah, A. M., Kar, A. K., ... & Yan, M., "Exploring the darkverse: A multi-perspective analysis of the negative societal impacts of the metaverse", Information Systems Frontiers, 25(5), 2071-2114, 2023.

48. Mooij, A., "Money Laundering and Financing of Terrorism via the Metaverse", In Regulating the Metaverse Economy: How to Prevent Money Laundering and the Financing of Terrorism (pp. 21-34), Cham: Springer Nature Switzerland, 2023.

49. https://www.insurancebusinessmag.com/us/risk-management/news/the-dark-side-of-the-metaverse-423154.aspx Yayın Tarihi Ekim 06,2022. Erişim Tarihi Ocak 12,2024.

50. https://blog.polkastarter.com/metaverse-challenges-is-the-darkverse-a-real-threat/ Yayın Tarihi Nisan 10,2023. Erişim Tarihi Ocak 07,2024.

51. https://www.darkreading.com/cloud-security/metaverse-version-dark-web-nearly-impenetrable Yayın Tarihi Eylül 16,2022. Erişim Tarihi Mart 01,2024.

52. https://www.rsaconference.com/library/presentation/usa/2023/Threats%20Inside%20the%20Darkverse%20The%20Shadowy%20Underbelly%20of%20the%20Metaverse Yayın Tarihi Nisan 26,2023. Erişim Tarihi Ocak 18,2024.

53. Dwivedi, Y. K., Kshetri, N., Hughes, L., Rana, N. P., Baabdullah, A. M., Kar, A. K., ... & Yan, M., "Exploring the darkverse: A multi-perspective analysis of the negative societal impacts of the metaverse", Information Systems Frontiers, 25(5), 2071-2114, 2023.

54. Dwivedi, Y. K., Kshetri, N., Hughes, L., Rana, N. P., Baabdullah, A. M., Kar, A. K., ... & Yan, M., "Exploring the darkverse: A multi-perspective analysis of the negative societal impacts of the metaverse", Information Systems Frontiers, 25(5), 2071-2114, 2023.

55. Dwivedi, Y. K., Kshetri, N., Hughes, L., Rana, N. P., Baabdullah, A. M., Kar, A. K., ... & Yan, M., "Exploring the darkverse: A multi-perspective analysis of the negative societal impacts of the metaverse", Information Systems Frontiers, 25(5), 2071-2114, 2023.