ADANA BAROSU
BİLİŞİM KOMİSYONU

DR. ÖĞR.ÜYESİ NİDA GÖKÇE NARİN

AV. ECE SU ÜSTÜN, LL.M.

AV. EDA ÜLKÜ ÜSTÜN

SENEM AKSAKAL

MÜRŞİT ÖZOĞLU

AV. TUĞÇE ÇALIŞOĞLU

AV. M. TURAN ÖZER

Temmuz 2023

İÇİNDEKİLER

YAPAY ZEKA VE YENİ TEKNOLOJİLER...

Saygıdeğer meslektaşlarım, sevgili okurlar,

Baromuz Bilişim Hukuku Komisyonunun binbir emekle hazırlamış olduğu Temmuz ayı dijital bülteninden hepinizi saygı ve sevgiyle selamlıyorum...

Dijital dünyadaki gelişmelerin meslektaşlarımıza anlatılması konularında bültenimiz istikrarlı bir şekilde yayın hayatına devam etmektedir.

Ortaya çıkan yeni teknolojiler, nesnelerin interneti, yapay zeka gibi gelişmeler, insanların yaşama, çalışma, eğlenme ve seyahat biçimlerini değiştireceği aşikar.

Gelinen aşamada ve özellikle gelişmiş ülkelerde yapay zekanın insan zekasından ayırt edilemeyecek nitelikte işler çıkartıyor olması nedeniyle insan iş gücünün yerini aldığı bir gerçek.

Bu gerçeğinse önümüzdeki yıllarda birçok meslek yönünden kişilerin çalışma hayatını tehlikeye atıp atmayacağı ya da birçok iş kolunda üretkenliği olumlu yönde etkileyip etkilemeyeceği bütün çevrelerde merak konusu...

Adana Barosu Bilişim Hukuku Komisyonumuzun çevrimiçi olarak yayınladığı dergimiz yine dopdolu ve bütün çevrelerde merak uyandıran bir içerikle karşınızda.

Günümüzde her alanda kullanılan ve gün geçtikçe ilerletilen yapay zeka çalışmalarına yönelik hazırlanan dergimiz için ve yaptıkları çalışmalar için Bilişim Hukuku Komisyonumuza çok teşekkür ediyor, siz değerli okurlarımıza keyifli okumalar diliyorum...

Av. SEMİH GÖKAYAZ

ADANA BAROSU BAŞKANI

Temmuz, 2023

John Mc Carty'nin 1956 yılında Dartmouth konferansında ilk defa kullanması ile hayatımıza giren yapay zeka kavramı o günden bu güne pek çok saha da kullanılmış ve halen de kullanılmaya devam etmektedir.

Günümüzde , Sağlık sektöründe; Doğru kanser teşhisinden sanal sağlık asistanlarına ,Eğitim sektöründe; Akıllı içerik oluşturmadan sınavlarda yapay zeka uygulamalarına ,Finans sektöründe; Bankaların kart ve işlem yönetimlerinden dolandırıcılık tespitine, Tarım sektöründe ise mahsul ve toprak izlemeden hava araştırması ve görüntülemeye kadar pek çok iş ve işlemlerin yapılmasında artık yapay zeka teknolojisinden yararlanılmaktadır.

Peki ya hukuk?

Yapay zeka, son günlerde hukuk alanında da adından söz ettirmekte ve pek çok gelişmenin yaşanmasına sebebiyet vermektedir. Belge analizi ve dökümantasyandan ,tahmin ve analize ,otomatik dil işlemeden hukuki araştırma ve ön incelemeye, dava dosyalarının risk değerlendirmesinden arabuluculuk ve anlaşmazlık çözümüne pek çok alanda kullanılmaya başlayan yapay zeka bir yandan kullanıldığı alanlardaki güvenilirliğinin sorgulanmasına yol açarken bir yandan da hukuk alanında özellikle Avukatlık mesleğinin geleceği hakkında da soru işaretlerini gündeme taşımıştır.

Tüm bu soru işaretlerinin cevapları elbette yıllar içinde ortaya çıkacaktır. Ancak bize düşen öncelikle bu cevapları düşünmekten önce yapay zeka hakkında fikir edinmek ve kavramlar hakkında bilgi sahibi olmaktır.

Bu sebeple bu sayımızda öncelikle yapay zeka hakkında kısa da olsa bilgi vermeyi uygun gördük.

Faydalı olması ümidi ile keyifli okumalar diliyoruz.

Av. Volkan Kurtar
ADANA BAROSU BİLİŞİM KOMİSYONU BAŞKANI

GENEL YAPAY ZEKANIN İLK ADIMLARI: ÜRETKEN YAPAY ZEKA

Dr. Öğr.Üyesi Nida GÖKÇE NARİN

Yapay Zekâ (YZ), artık hemen herkesin duyduğu bildiği bir kavram. Günümüz teknoloji dünyasının yeni lokomotifi. İnsana ait yeteneklerle donatılmış akıllı sistemlern, insanların yapabildiği işleri daha hızlı ve verimli bir şekilde gerçekleştirebilmeleri nedeniyle birçok sektörde kullanımı yaygınlaşmakta. Ev hizmetlerinden üretime, sağlıktan eğitime, savunma sanayinden ulaşıma her alanda YZ teknolojileri ile karşılaşmak mümkün. Akıllı cihazların günlük kullanımı, kişiselleştirilmiş tedaviler ve kişiselleştirilmiş eğitim programları gibi daha bir çok spesifik problemin çözümüne odaklanan günümüz YZ sistemleri dar YZ sistemleri olarak bilinmektedir. Çoğunlukla yapılandırılmış ve etiketlenmiş veriler ile eğitilen bu sistemlerin başarısı eğitim verilerinin miktarı, çeşitliliği ve yanlı olup olmamasına göre değişmekte.

Dar YZ sistemleri son yıllarda kayda değer başarılar gösterse de, sadece görüntü, sadece ses, sadece metin verilerini işleyebilmek gibi tek bir görev için eğitilme, yapısal verilerde daha başaralı olma gibi kısıtlara sahiptir. Oysa insan, karar verme sürecinde birden çok görevi aynı anda kullanabilmekte. Bu kısıtları ortadan kaldırabilmek için geliştirilen çoklu görevli Üretken YZ modelleri insan karar verme süreçlerini daha iyi taklit edebilmektedir.

Üretken YZ Nedir?

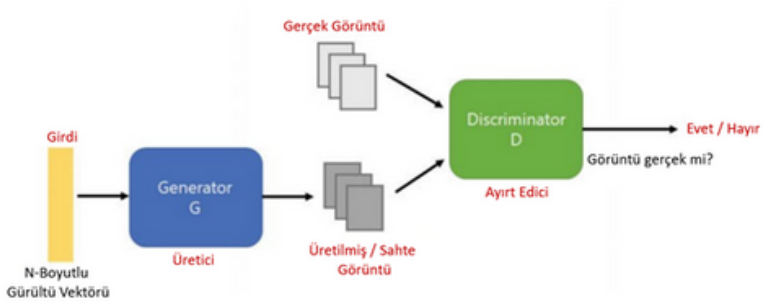
Üretken modellerin ilk örnekleri Gizli Markov Modelleri (Hidden Markov Models) [1] ve Gauss Karışım Modellerine [2] dayanarak geliştirilmiştir. Konuşma ve zaman serisi gibi sıralı verileri üretmekte kullanılan modellerde ki gerçek performans artışı 2014 yılında Üretken çekişmeli ağların (Generative Adversial Networks, GAN) geliştirilmesinden sonra gerçekleşmiştir [3,4]. GAN'lar yapay zekânın görüntü, ses ve video formatındaki verileri gerçeğine çok benzer şekilde üretmesine imkan sağlayan ilk derin öğrenme modelleridir.

Üretken YZ büyük ve çoğunlukla yapılandırılmamış eğitim verilerinden elde ettiği bilgiyi ve ortaya çıkardığı kalıpları, içerik üretmek için kullanan sistemleri ifade etmektedir. Dar YZ sistemleri gruplama, sınıflandırma, tahminleme vb. gibi tek bir probleme, tek bir amaca yönelik çözümler sunarken Üretken YZ modelleri, eğitim verilerinden öğrendiği bilgi ile yeni bir metin üretmek, yeni bir tasarım yapmak, var olmayan insan yüzleri veya yeni canlı türleri üretebilmek gibi yeteneklere sahiptir. Çok modelli yaklaşımlarla metin veya ses ile kurgulanan bir senaryoyu ya da talimatları görselleştirebilir. Kendisine sunulan bir görseli veya videoyu metne, sese dönüştürerek yorumlayabilir. Daha fazla insansı özelliklerle donatılmış oldukları için, gerçek zekâyı taklit etme konusunda çok daha yeteneklidirler ve genel YZ'a geçiş basamağı olarak görülmektedirler.

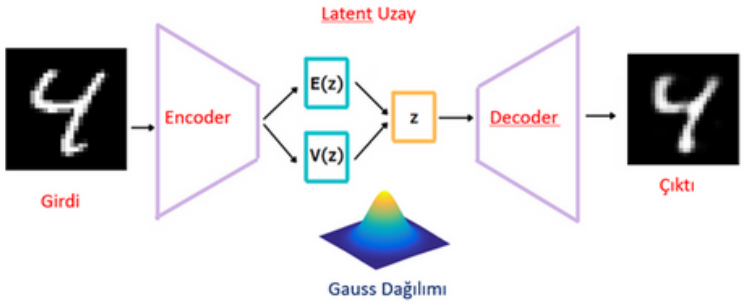
Üretken YZ Modelleri

Üretken YZ modelleri, GAN'lar [3], Varyasyonel Otokodlayıcılar (Variational Autoencoders, VAE) [5] ve Transformer tabanlı modeller (TTM) [P8] olarak temelde üç başlıkta incelenmektedirler. GAN'Lar ve VAE'ler çoğunlukla görüntü ile ilgili problemlerde kullanılırken, TTM'ler doğal dil işlemede kullanılmaktadır.

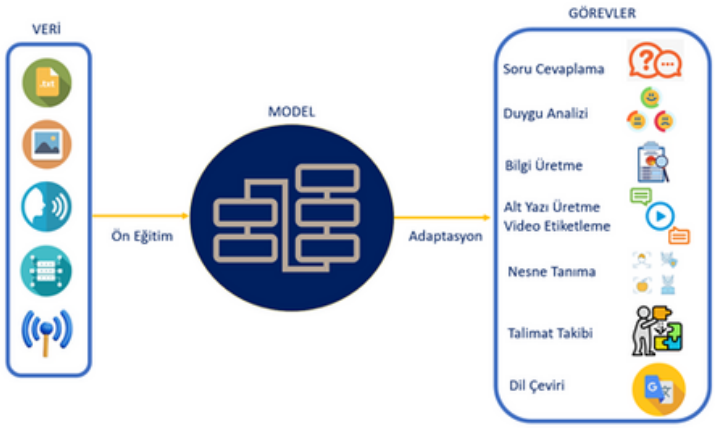
Şekil 1'de basit bir mimarisi verilen GAN'lar, üretici ve ayırt edici olmak üzere iki bileşenden oluşmaktadır. Üretici, yeni veriler üretirken ayırt edici, kendisine gelen verinin gerçek olma olasılığını hesaplayarak görüntünün gerçek mi yoksa sahte mi olduğuna karar vermektedir. Model, üretici ve ayırt edicinin sürekli rekabetinden dolayı Üretici Çekişmeli Ağlar olarak adlandırılmaktadır. GAN'lar özellikle gerçeğe yakın yüksek çözünürlüklü görüntü üretme yetenekleri nedeniyle en başarılı üretken modeller olarak öne çıkmaktadır [4].



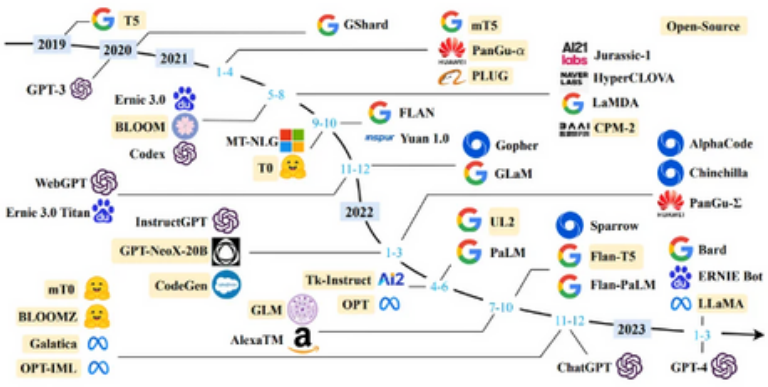
Şekil 1. Basit bir GAN mimarisi



Şekil 2. Gauss dağılımı kullanan bir VAE yapısı



Şekil 3. Transformer Tabanlı Modellerin yapısı



Şekil 4. 2019 yılından sonra geliştirilen Transformer Tabanlı Modeller [12]

Diederik ve ark. tarafından önerilen VAE'ler [5] denetimsiz öğrenme ile denetimli öğrenmeyi birleştirerek yüksek boyutlu veriyi daha düşük boyutlu bir latent uzayda modellemeye çalışır. Giriş verisini bir olasılık dağılıma eşleyen Encoder ile latent uzaydaki bir noktayı alıp orijinal giriş uzayına geri kodlayan Decoder bölümlerinden oluşur. Böylece giriş verisini yeniden yapılandırmış olur. Şekil 2'de Gauss dağılımının kullanıldığı bir VAE yapısı verilmiştir. Görüntü üretme, gürültü azaltma ve anomali tespiti için yaygın olarak kullanılmaktadır.

Transformer tabanlı modeller (TTM) [6-9], sıralı verilerdeki ilişkileri izleyerek bağlamı ve dolayısıyla anlamı öğrenen yapay sinir ağ modelleridir. Şekil 3'de genel bir gösterimi verile bu modeller çoğunlukla doğal dil işlemede kullanılırlar. Büyük metin korpusları üzerinden eğitilen modeller metin oluşturmada önemli bir başarı göstermektedir. En popüler örnekleri GPT (Generative Pretrained Transformer) ve BERT (Bidirectional Encoder Representations from Transformers) olarak adlandırılan ön eğitimli modellerdir. Yapay Zekada bir paradigma değişikliğine neden olan TTM'de ön eğitim süreci, modelin doğal dilin semantik ve söz dizimsel özelliklerini anlamasını sağlar. Böylece bir cümledeki her kelimenin, ve bir metindeki her cümlenin bağlamla uyumlu olduğu metinler üretebilir. Bu sayede dil çevirileri, metin özetleme, video altyazıları oluşturma gibi pek çok alanda kullanılmaktadırlar.

TTM'in özellikle son yıllardaki tarihsel gelişimi Şekil 4'deki zaman çizelgesinde verilmiştir. Üretken YZ çalışmalarının gelişiminde TTM'nin etkisi oldukça fazladır. Birçok model geliştiriliyor olmasına rağmen, özellikle OpenAI tarafından geliştirilen ChatGPT [10] ve GPT-4 [11] modellerinin kullanıma açılması tüm dünya için geri dönüşü olmayan bir yola giriş anlamına gelmektedir. İlk olarak Kasım 2022'de ChatGPT'nin herkesin kullanımına açılmasıyla başlayan YZ'nın risklerine ilişkin tartışmalar,

Görüntü	Ses	Metin	Kod
DALL-E	Reprica	Jasper	Tabnine
Midjourney	Speechify	Writesonic	Hugging Face
Starryai	Murf	Copy.ai	K-Explorer
Craiyon	Play.ht	Notion AI	PyCharm
NightCafe	Lovo.ai	GrammarlyGo	Kite
Artbreeder	AIVA	FraseIO	OpenAI codex
Synthesai	AmperAI	Peppertype	Codacy
Lumen5	Jukebox	Rytr	Github Copilot
Flexclip	Sounraw	INK	Replit
Elai	Evoke	Copymatic	Mutable AI
Veed.io	Synthesys	Paragraph AI	Mintify
Khroma	Altered	Outranking	Debuild
Uizard	Listnr	Writer	Locofy
Colormind	Play.ht	Sudowrite	Anima
Designs.ai	Respeecher	Anyword	CodeComplete
FrontyAI	Speechelo	Chibi	aiXcoder

Mart 2023'de GPT-4'ün tanıtılmasıyla daha da alevlendi ve uluslararası düzeyde endişeler dile getirilmeye başlandı.

Endişelerin temelinde Üretken YZ modellerin gelişimindeki hız ve elde ettikleri başarıya rağmen herkes tarafından kullanılmasının oluşturacağı riskler ve ortaya çıkması muhtemel sorunların tam olarak bilinmiyor olması yatmaktaydı. Nitekim modellerin kullanılmaya başlandığı kısa bir süre içerisinde olumlu örneklerin yanı sıra sahtecilik, aşırmacılık, hatalı bilgilerin üretilip yayılması gibi birçok problemle karşılaşıldı.

Üretken YZ Tabanlı Uygulamalar

Üretken YZ modellerinin kullanıldığı pek çok uygulama geliştirildi. Tablo 1'de Görüntü, ses, metin ve kodlama alanlarına özel olarak geliştirilmiş olan ücretli ve ücretsiz olarak kullanıma sunulmuş uygulamalardan örnekler verilmiştir. Her geçen gün bu uygulamalara yenileri eklenmektedir. Sanat, tasarım, eğitim, araştırma ve yazılım geliştirme gibi pek çok alanda kullanımı hızla yaygınlaşan bu uygulamaların ürettiği bilginin titizlikle ele alınması gerekmekte. Tasarım boyutunda orijinal ürünler ortaya çıkarma konusunda heyecan verici sonuçlar üretirken, araştırma ve eğitim boyutunda üretilen bilginin doğruluğunun kontrol edilmesine ihtiyaç duyulmaktadır. Temelde ön eğitimli modellere dayanarak geliştirilen bu uygulamalar kullanım sürecinde kullanıcılardan gelen dönütlerle kendilerini geliştirme ve adaptasyon yeteneğini arttırma eğilimindedir.

Uygulama Çıktılarına İlişkin Örnekler

A robotic female lawyer and jurors interrogate a courtroom witness, realistic, tense image, high detailed, 8k

Görüntü üretme konusunda en bilinen uygulamalar DALL-E [13] ve Midjourney'dir [14]. Aşağıdaki görsel Midjourney tarafından İngilizce metin olarak verilen basit bir komutun ürettiği çıktıdır.

Arka plandaki görseller ve detaylar konusunda iyileştirmelere ihtiyaç duysa da bu modellerin hayal gücümüzü zorlama ve geleceği şekillendirme potansiyeline sahip olduğu bir gerçek.

Riskler ve Tehditler

Üretken YZ alanındaki çalışmaların büyük bir hızla devam ediyor olması bu alanda çalışmalar yürüten araştırmacıları ve bilim dünyasını heyecanlandırsa da toplumsal etkileri konusunda endişeleri de beraberinde getiriyor. Dar YZ teknolojileri belirli problemlerin çözümüne odaklanan ve uzun zamandır tartışılan olası risklerine karşı önlemler alınmasına yönelik girişimlerde bulunulan, öngörülebilir teknolojilerdi. Ancak Üretken YZ modellerinin tanıtımı ve hızlı bir şekilde kullanıcılarla buluşması öngörülemeyen riskleri de beraberinde getirdi.

ChatGPT ve diğer LLM modelleri gerçek dışı bilgiler, önyargılar veya artık geçerliliği olmayan geçmiş bilgileri içeren büyük çevrimiçi metin veritabanlarından dilin istatistiksel kalıplarını öğrenerek çalışıyorlar. Bu nedenle hatalı bilgi üretme potansiyeli var. GPT-4 ile pek çok açığı kapatılmaya çalışılsa da hala tam olarak güvenle kullanım seviyesin de değil. Dahası pek çok dil modeli Yerel kültürler, yerel tarih bilgileri gibi eğitim verisi seti içinde nispeten az bulunan veya hiç yer almayan konularda bile öğrendiği kalıplara dayalı metin üretebildiği için kolayca hata yapabiliyor ve yanıltıcı bilgi üretebiliyor.

Özel olarak istenmediği sürece ürettiği bilgi için kaynak göstermez, kaynak göstermesi istendiğin de ise ilgili standartlara uygun ancak gerçekte var olmayan kaynaklar üretebilir. Bilimsel bir makale yazması istendiğinde gerçek dışı alıntılar üretebilir. Bu da özellikle akademide kullanımları açısından büyük bir risk oluşturmaktadır.

Örnek bir İnceleme

Olası risklere karşı önlem olarak geliştirilen bazı uygulamalar da mevcut. Bir dergi editörü, bir akademisyen, bir hakim veya genel bir okuyucu iseniz ve okuduğunuz herhangi bir metnin insan mı yoksa yapay zeka tarafından mı üretildiğini kontrol etmek isterseniz size yardımcı olabilecek uygulamalara ulaşabilirsiniz. Bu konuda küçük bir örnek çalışma aşağıda verilmiştir.

Üretken YZ'a "İdare mahkemesinde açılan dava dosyası Yargıtay'a neden gider?" diye soralım. Ardından GPT 3.5 ve GPT-4 tarafından üretilen yanıtları uygulamalar aracılığı ile kontrol edelim.

GPT 3.5

İdare mahkemesinde açılan dava dosyası, idare hukukuna ilişkin konuları içerir ve genellikle idari işlemler veya kamu kurumlarıyla ilgili uyuşmazlıkları kapsar. İdare mahkemesi, bu tür davalarda ilk derece mahkemesi olarak görev yapar.

Ancak, bir taraf idare mahkemesinin verdiği kararı veya kararın hukuki dayanağını uygun bulmazsa veya hukuki bir yanlışlık olduğunu düşünürse, dava dosyasını temyiz etmek veya daha üst bir mahkemeye taşımak için Yargıtay'a başvurabilir. Yargıtay, idare mahkemesinin verdiği kararları ve uyguladığı hukuki ilkeleri denetler.

Yargıtay, idare mahkemesinin kararının hukuka uygunluğunu değerlendirirken genellikle hukuki açıdan önemli bir konunun varlığına, hukuki bir yanlışlığa veya içtihat birliğinin sağlanması gerektiğine dikkat eder. Yargıtay, idare mahkemesinin verdiği kararı onaylayabilir, kısmen veya tamamen bozabilir veya kararı değiştirebilir.

Yargıtay'a yapılan başvurular, öncelikle hukuki nitelikli ve önemli konulara ilişkin olduğunda kabul edilir. Ancak, her başvuru Yargıtay tarafından kabul edilmez ve değerlendirme süreci bir süreç gerektirir. Yargıtay, son kararı vermeden önce dava dosyasını inceler ve tarafların argümanlarını dikkate alır.

GPT-4

Bir İdare Mahkemesi'nde açılan bir dava dosyası, genellikle aşağıdaki iki ana sebep yüzünden Yargıtay'a gitmektedir:

1.Temyiz: Eğer taraflardan biri İdare Mahkemesi'nin kararını kabul etmezse, Yargıtay'a başvurabilirler. Temyiz, daha yüksek bir mahkeme olan Yargıtay'a, daha alt bir mahkeme olan İdare Mahkemesi'nin kararının yeniden incelenmesi için başvurma hakkını ifade eder. Temyiz başvurusunda bulunan taraf, genellikle İdare Mahkemesi'nin hatalı bir karar verdiğini veya hukuki bir yanılgıya düştüğünü iddia eder.

1.İstinaf: Yargı reformu ile birlikte Türkiye'de 2016 yılından itibaren istinaf başvurusu yapılabilmektedir. İstinaf başvurusu, yerel mahkeme kararlarının bölge adliye mahkemeleri tarafından inceleme altına alınması anlamına gelir. Bölge adliye mahkemelerinin kararlarına karşı da Yargıtay'a başvurulabilir.

İdare Mahkemesi kararlarına karşı başvuru, Danıştay'a yapılır. Danıştay, idari yargı organıdır ve İdare Mahkemesi kararlarını inceleme yetkisine sahiptir. Yargıtay ise adli yargı organıdır ve genellikle asliye ve ağır ceza mahkemeleri gibi adli yargı organlarının kararlarını inceler.
Yukarıda bahsettiğim durumlar genellikle idari dava dosyalarının Yargıtay'a neden gittiğini açıklamaktadır. Ancak her dava eşsizdir ve dosyanın Yargıtay'a gitme sebebi, davaya özgü belirli faktörlere dayalı olabilir.

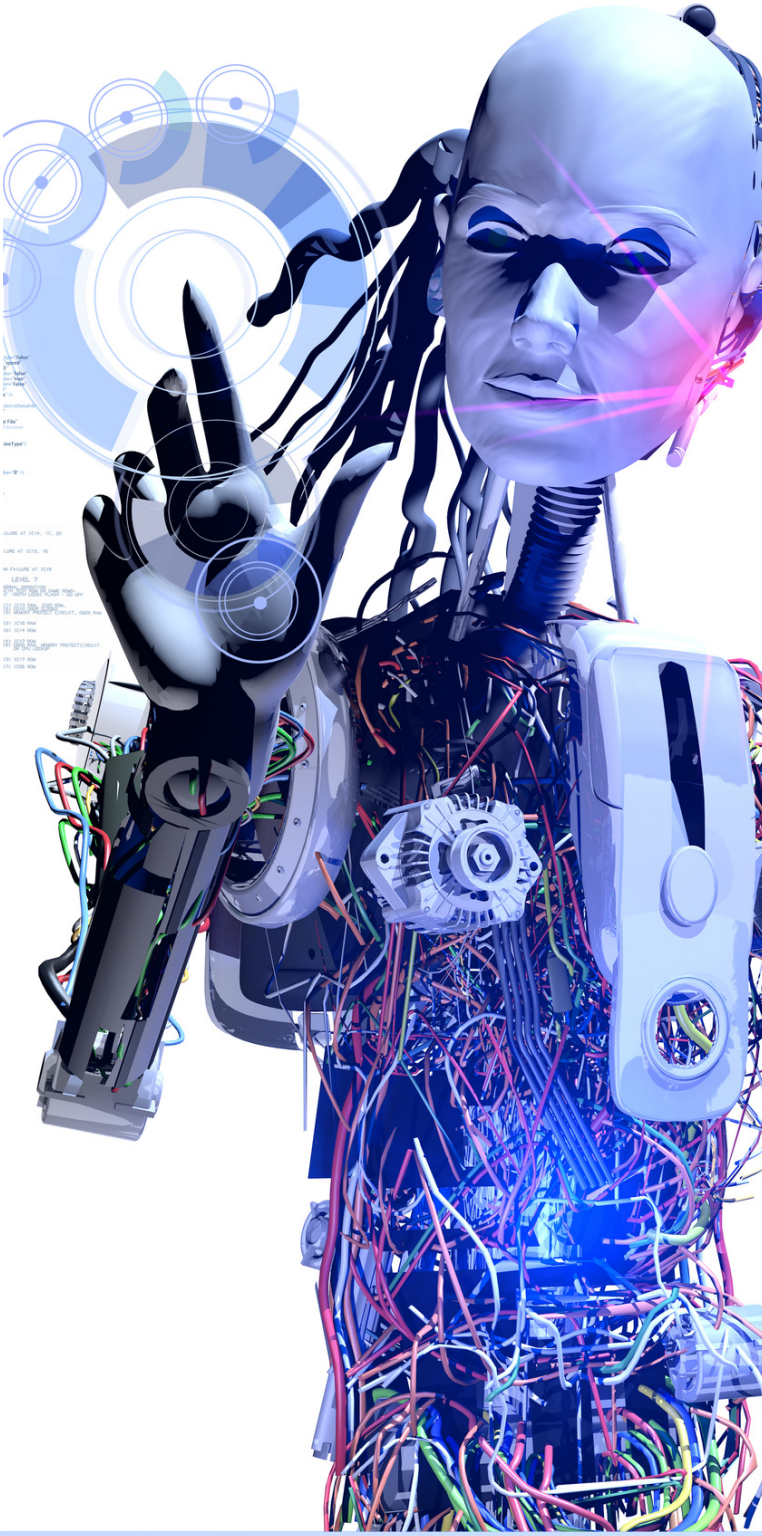
Yukarıda verilen ve YZ tarafından üretilen Türkçe metinlerin sahte olup olmadığının farklı uygulamalar tarafından incelenmiş ve elde edilen sonuçlar Tablo 2'de verilmiştir. Uygulamalar Türkçe ve İngilizce metinlerle test edilmiştir. Writer ve Copyleaks, Türkçe metin girildiğinde dil desteği olmadığı için her hangi bir sonuç üretmemiştir. Ancak diğer uygulamalar herhangi bir uyarı vermeden metnin insan kaynaklı oluğunu sonucunu üretmiştir. Bu uygulamaların İngilizce performansını test etmek için Türkçe metinin yine YZ tarafından üretilen İngilizceye çevirisi kullanılmıştır. Sonuçlar GPT-4 modelinin ürettiği metinlerin GPT3.5 metinlerine göre anlaşılmasının daha güç olduğunu göstermiştir. Karşılaştırılan uygulamalar arasında AI Detector'ın her iki model içinde İngilizce dilinme YZ tarafından üretilen metinleri yakalama başarısının en yüksek olduğunu göstermiştir.

	GPT 3.5	GPT-4
Writer (Türkçe Desteği Yok) [17]	%97 İnsan	%100 İnsan
Copyleaks (Türkçe Desteği Yok) [18]	%99.9 YZ	%81.1 İnsan
ContentDetector.AI (Türkçe)[19]	%92.6 İnsan	%94.1 İnsan
ContentDetector.AI (İngilizce) [19]	%72.3 YZ	%66.9 Kararsız
AI Content Detector (Türkçe) [20]	%100 İnsan	%100 İnsan
AI Content Detector (İngilizce) [10]	%66 (İnsan & YZ)	%100 YZ
AI Detector (Türkçe)[21]	%100 İnsan	%100 İnsan
AI Detector (İngilizce)[21]	%100 YZ	%99.9 YZ
ZeroGPT (Türkçe) [22]	%100 İnsan	%100 İnsan
ZeroGPT (İngilizce) [22]	%92.92 YZ	%55.14 YZ
Seo.AI (Türkçe) [23]	%1 YZ	%17 YZ
Seo.AI (İngilizce) [23]	%92 YZ	%75 YZ

Tablo 2. Üretilen bir metnin insan mı YZ kaynaklımı olduğuna dair inceleme sonuçları

Sonuç ve Tartışma

Günümüzdeki üretken YZ ve diğer YZ teknolojileri çalışanların zamanının yüzde 60 ila 70'ini kapsayan iş faaliyetlerini otomatikleştirme potansiyeline sahiptir. Bunda çalışma süresinin yüzde 25'ini oluşturan iş faaliyetleri için gerekli olan doğal dili anlama yeteneğinin artmasının önemli bir etkisi vardır [24]. Teknik otomasyon potansiyelindeki bu artışların, iş gücü dönüşüm hızını da arttırması beklenmektedir. Üretken YZ, ekonomik açıdan iş gücü verimliliğini önemli ölçüde arttırabilir ancak, iş faaliyetleri ve iş tanımları değişirken işçileri de desteklemek için yatırımlar yapılması gerekecektir. Her sektör için Üretken YZ'nın bir alan uzmanları tarafından desteklenerek kullanılması üretkenliği ve verimliliği arttıracak şekilde değer yaratabilir. Büyük ve karmaşık veriyi hızlı bir şekilde analiz ederek sonuç çıkarma yeteneği sayesinde ürün geliştirme süreçlerini önemli ölçüde hızlandırabilir.



Ancak üretken YZ'nın dikkatsiz kullanımı, intihal, telif hakkı ihlalleri ve fikri mülkiyet haklarının ihlalleri gibi çok ciddi riskler taşımaktadır. Ayrıca sınırlı veya ön yargılı eğitim verileri nedeniyle baskın olan demografilerin özellikleri üzerinden hatalı sonuçlar üretebilir. Bu nedenle hem üretim süreçlerinde ve hemde bir çok alanda kritik karar verme süreçlerinde insan uzman kontrolü gereklidir. Bilgi üretirken dikkatli olunmalı. Güvenilir olmayan sonuçlar üretebileceği için veri üretiminden kaynaklı hatalarda artış olabilir. Önyargı ve Etik sorunları, güvenlik Açıkları ve gizlilik ihlalleri konusunda gerekli önlemler alınmalı ve yasal düzenlemeler yapılmalıdır. Üretken YZ modelleri sahip oldukları potansiyel ile hem toplumsal düzeyde hem de teknolojik gelişmeler noktasında önemli bir etki yaratmaktadır. Bilinçli ve kontrollü kullanımı ve olası riskleri minimize edecektir adımların ivedilikle atılması bu etkinin pozitif yönde gelişmesi ve devamlılığı için oldukça önemlidir.

Kaynakça

[1] Rabiner, L., & Juang, B. (1986). An introduction to hidden Markov models. ieee assp magazine, 3(1), 4-16.

[2] Reynolds, D. A. (2009). Gaussian mixture models. Encyclopedia of biometrics, 741(659-663).

[3] Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., ... & Bengio, Y. (2014). Generative adversarial nets. Advances in neural information processing systems, 27.

[4] Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., ... & Bengio, Y. (2020). Generative adversarial networks. Communications of the ACM, 63(11), 139-144.

[5] [P7] Kingma, D. P., & Welling, M. (2013). Auto-encoding variational bayes. arXiv preprint arXiv:1312.6114.

[6] Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., ... & Polosukhin, I. (2017). Attention is all you need. Advances in neural information processing systems, 30.

[7] Brown, T., Mann, B., Ryder, N., Subbiah, M., Kaplan, J. D., Dhariwal, P., ... & Amodei, D. (2020). Language models are few-shot learners. Advances in neural information processing systems, 33, 1877-1901.

[8] Radford, A., Wu, J., Child, R., Luan, D., Amodei, D., & Sutskever, I. (2019). Language models are unsupervised multitask learners. OpenAI blog, 1(8), 9.

[9] Devlin, J., Chang, M. W., Lee, K., & Toutanova, K. (2018). Bert: Pre-training of deep bidirectional transformers for language understanding. arXiv preprint arXiv:1810.04805.

[10] GPT 3.5, OpenAI, 2022, https://chat.openai.com/

[11] GPT-4, OpenAI, 2023. https://openai.com/research/gpt-4

[12] Zhao, W. X., Zhou, K., Li, J., Tang, T., Wang, X., Hou, Y., ... & Wen, J. R. (2023). A survey of large language models. arXiv preprint arXiv:2303.18223.

[13] DALL-E2, OpenAI, 2022, https://openai.com/dall-e-2

[14] Midjourney, 2022, https://www.midjourney.com/app/

[15] Bard, Google, 2023, https://bard.google.com/

[16] Wei, J., Wang, X., Schuurmans, D., Bosma, M., Xia, F., Chi, E., ... & Zhou, D. (2022). Chain-of-thought prompting elicits reasoning in large language models. Advances in Neural Information Processing Systems, 35, 24824-24837.

[17] Writer, 2023, https://writer.com/ai-content-detector/

[18] Copyleaks, 2023 https://copyleaks.com/ai-content-detector

[19] Contentdetertor.AI, 2023 https://contentdetector.ai

[20] AI Content Detector, 2023, https://crossplag.com/ai-content-detector/

[21] AI Detector, 2023, https://sapling.ai/ai-content-detector

[22] ZeroGPT, 2023, https://www.zerogpt.com

[23] Seo.AI, 2023, https://seo.ai/detector

[24] Chui,M. Hazan, E. Roberts, R. Singla, A. Smaje, K. Sukharevsky, A. Yee, L., Zemmel, R. (14 Haziran 2023), McKinsey & Company Report, The economic potential of generative AI: the next productive frontier,https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/The-economic-potential-of-generative-AI-The-next-productivity-frontier#key-insights

KUANTUM BİLGİSAYARLARININ BLOKZİNCİR TEKNOLOJİSİ ÜZERİNDEKİ POTANSİYEL YIKICI ETKİLERİ

Av. Ece Su Üstün, LL.M. – Av. Eda Ülkü Üstün

GİRİŞ

20. yüzyılda kuantum mekaniğinin keşfiyle başlayan birinci kuantum devrimi atom (ve atomaltı) dünyasını anlama biçimimizi kökten değiştirecek yeni fizik yasalarının doğumuna sebebiyet verdi. Gerçekten de, atomaltı parçacıkların işleyişinin makroskopik ölçekteki gözlemlenebilir doğada mevcut olan klasik fizik kurallarına göre değil de atomaltı dünyasına has birtakım farklı –ve çoğu zaman klasik fiziğin kurallarıyla çelişen- kurallarla gerçekleştiğinin öğrenilmesiyle beraber, 70'lerde bilim dünyasında bu yeni fizik kurallarının bilişim teknolojilerinde nasıl uygulanabileceğine ilişkin yoğun (ve uzun) bir araştırma süreci -ve dolayısıyla da ikinci kuantum devrimi- başladı. 80'lerde "çözülemez" matematik problemlerinin çözümü sağlamak gibi belirli bilgisayar hesaplamalarında verimliliğin artırılması ve hesaplama gücünün en üst düzeye çıkarılması hedefiyle kuantum mekaniğini esas alan bilgisayarların üretilmesi fikrinin ortaya atılmasıyla ise bugünkü kuantum bilgisayarlarının ilk fikri temelleri atılmış oldu.

Bugün, bilim camiası, devlet ve özel sektörün ortak çalışmaya dayalı uğraşları sonucu, bu hayaller kısmen gerçekleşmiş olup sınırlı kübit kapasitesine sahip kuantum bilgisayarları inşa edilmiştir. Kuantum bilgisayarları bugünkü seviyeleri itibariyle kendisinden beklenen potansiyelin tümünü gerçekleştirecek performans düzeyinde değilse de 2027 ile 2035 yılları arasındaki bir zaman dilimi içerisinde yeterli kübit kapasitesine sahip kuantum bilgisayarlarının inşa edilebileceğine dair tahminler mevcuttur [1] [2] [3]. Böylesi bir tahminin realize olması, Peter Shor ve Lov Grover tarafından ortaya konulan iki ayrı kuantum algoritmasından faydalanarak kuantum bilgisayarlarının günümüzde güvenli olarak kabul edilen ve yaygın olarak kullanılmakta olan kriptografik protokollerin önemli bir kısmının (kübit sayısına bağlı olarak) birkaç dakika ile birkaç saat arasında kırılabileceği anlamına gelmektedir.

En temel haliyle kriptografi, dağıtık defter teknolojisi (DLT) ve sanal varlıkların kompozisyonundan oluşan blokzincir teknolojisi de kuantum bilgisayarlarının yarattığı siber tehditlerin hedefindedir. Gerçekten de kriptografi blokzincir teknolojisinin adeta belkemiği olup gerek blokzincirde gerçekleşen işlemlerin güvenliği, gerek kayıtlı verilerin doğruluğu ve bütünlüğü gerek ise kullanıcıların blokzincir içerisinde işlem yapabilmelerine olanak tanıyan ve sanal varlıklarının yönetimini sağlayan dijital imzaların güvenliği seçilen kriptografik protokollerin güvenliğine sıkı sıkıya bağlıdır. Daha da önemlisi, blokzincirin dağıtık ve merkezi olmayan doğasından kaynaklanan yönetim zorlukları gözetildiğinde, blokzincir teknolojisinin sağlıklı ve güvenli bir şekilde devamlılığının sağlanabilmesi için gerekli önlemlerin ikinci kuantum devrimi [4] tamamlanmadan önce alınması büyük bir önem taşımaktadır.

Bu makale üç ana bölüm halinde, kuantum bilgisayarlarının blokzincir teknolojisi başta olmak üzere mevcut kriptosistemler üzerinde ne çeşit yıkıcı etkileri olabileceğini araştırmaktadır. Birinci bölüm blokzincir teknolojisinin kriptografiyle olan ilişkisini, ikinci bölüm blokzincir teknolojisi üzerindeki kuantum tehdidini ve nihayet üçüncü bölüm kuantum kıyametini engellemek için alınabilecek birtakım önlemleri inceleyecektir.

1. BÖLÜM: BLOKZİNCİR TEKNOLOJİSİNİN KRİPTOGRAFİ İLE İLİŞKİSİ

En basit tanımıyla, blokzincir teknolojisi kullanıcıların birbirleriyle –herhangi bir aracı kuruma ihtiyaç duymaksızın- eşler arası (P2P) olarak işlem yapmasına olanak tanıyan merkezi olmayan bir ağ ve tüm işlem kayıtlarını kriptografik protokoller sayesinde değiştirilemez ve güvenli bir şekilde saklayan dağıtık bir veri tabanıdır. Mimarisi gayrimerkezi olduğundan, blokzincir teknolojisinde işlemlerin geçerli kılınması ile kayıtların doğruluğunu ve bütünlüğünü kontrol etmek için herhangi bir merkezi otorite bulunmamaktadır.

Bunun yerine, bu görevler birbirini tanımayan (ve dolayısıyla güvenmeyen) düğümler (nodes) tarafından yerine getirilmekte olup bu düğümler arasındaki uyumluluk ve işbirliği belirli kriptografik protokoller ve oyun teorisi temelli teşviklere desteklenmiş mutabakat mekanizmalarına (consensus mechanisms) dayanmaktadır.

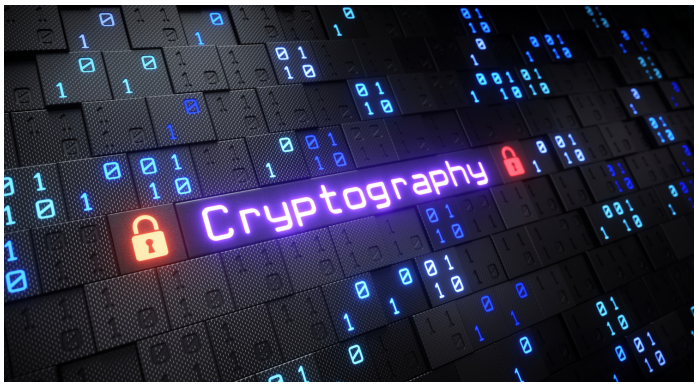
Blokzincir teknolojisinde zincirde gerçekleşen işlemler veri bloklarında kaydedilir ve bu veri blokları belirli kriptografik protokollerden faydalanılarak gizli ve güvenli bir şekilde veri katmanında depolanır. Zincirde gerçekleşen işlemlere dair veri kayıtlarının tümü dağıtık defter teknolojisi sayesinde senkronize ve eşlenik bir şekilde düğümlerde mevcut olduğundan bu kayıtlar bir anlamda herkese açık yani şeffaf olarak tutulmaktadır. Bununla beraber blokzincirde işlem güvenliğinin sağlanabilmesi amacıyla işlem yapan tarafların kimlik doğrulamasının sağlanması, bir diğer ifadeyle, işlemi yapan kişinin işlemi yapmaya yetkili kişi olup olmadığının tespit edilebiliyor olması gereklidir.

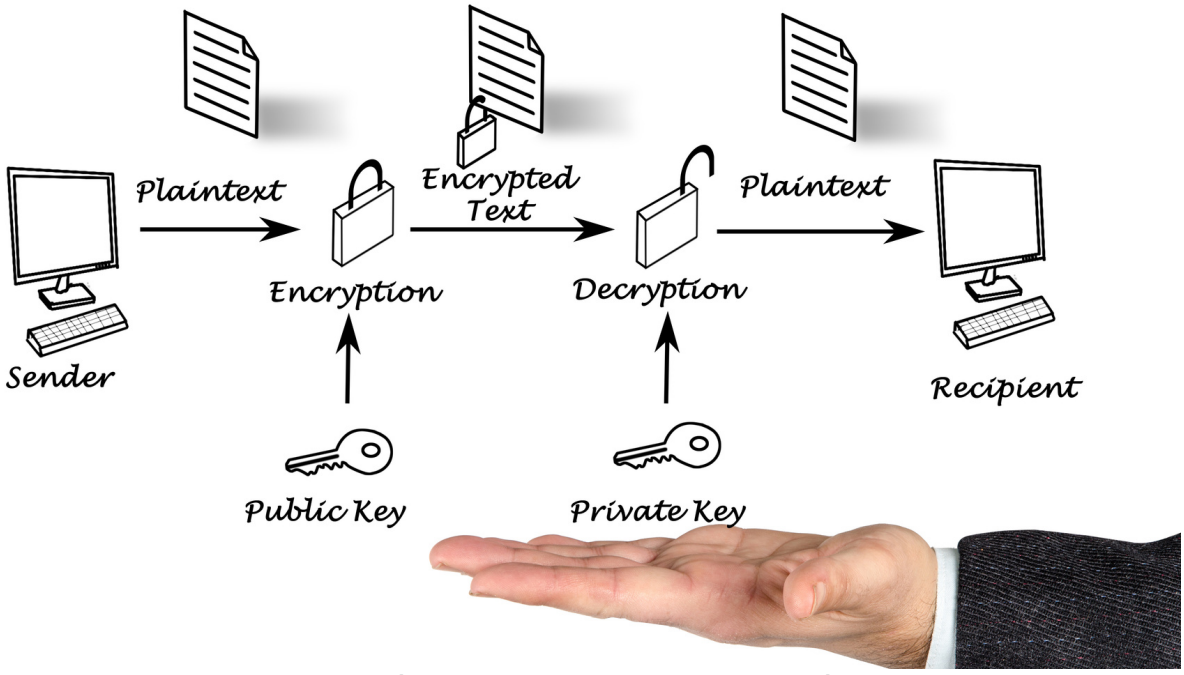
İşte tamda bu çoklu ihtiyaçların (gizlilik, kimlik doğrulama ve şeffaflık) bir aradalığı blokzincir teknolojisinde bir çift anahtarın (bir özel anahtar ve en az bir genel anahtar) kullanıldığı asimetrik kriptografinin benimsenmesine yol açmıştır [5]. Diğer bir deyişle, blokzincir teknolojisinde asimetrik kriptografi, şeffaf ve merkezi olmayan bir ağ üzerinde kullanıcıların birbirleriyle güvenli ve gizli bir şekilde işlem yapmasını sağlamak ve işlemlerin işlem yapmaya yetkili olan kişiler (imza sahibi) tarafından gerçekleştirildiğini doğrulamak amacıyla kullanılmaktadır [6].

Asimetrik anahtar sisteminin kullanılmasının temel nedeni, asimetrik kriptografinin simetrik kriptografiye (hem şifrelemek hem de deşifre etmek için aynı anahtarın kullanıldığı tek gizli anahtarlı sistem) göre mevcut teknolojik konjonktürde daha yüksek seviyede güvenlik sağlamasından kaynaklanmaktadır. Zira simetrik kriptografide (i) taraflar gizli anahtar üretimi için tam bir rasgelelik elde edememekte ve (ii) taraflar arasındaki iletişim (veya iletişim) kanalının mutlak bir biçimde güvenli olmayabileceğinden kötü niyetli üçüncü kişiler iletilen verilere müdahale edebilmektedir. Dahası, anahtar değişimi de bu güvenilmeyen kanal üzerinden gerçekleştirildiği için anahtar kötü niyetli üçüncü kişiler tarafından çok daha kolay bir şekilde ele geçirilebilir durumdadır.

Asimetrik kriptografide kullanıcı birbirleriyle matematiksel olarak ilişkilendirilmiş bir çift anahtara sahip olup bu anahtarlardan biri özel anahtar (private key) ve diğeri genel anahtar (public key) olarak adlandırılmaktadır. Kural olarak yalnızca anahtar sahibi tarafından bilinen özel anahtar gizli tutulur ve sahibine işlem yapma yetkisini sağlar. Bu doğrultuda, özel anahtar, (genellikle) zincirde işlem gerçekleştirmekte olan bir kullanıcının ancak ve ancak bu özel anahtarın meşru sahibi olduğu varsayımına dayandığından bir anlamda kimlik doğrulama işlevi de görmektedir. Zira özel anahtar her zaman gizli tutulduğundan hiçbir zaman doğrudan blokzincir üzerinde görünmez, iletilmez veya depolanmaz. Kullanıcılar özel anahtarlarını bir dijital cüzdanda saklamaktadır. Söz konusu dijital cüzdan bir donanım cüzdanı (hardware wallet) yani fiziksel bir cihaz- olabileceği gibi bir yazılım cüzdanı da (software wallet) -örneğin, web cüzdanı, mobil cüzdan uygulaması vb.- olabilir.

Genel anahtarlar esasında ise belirli kompleks matematiksel hesaplamalar yoluyla özel anahtardan türetilmektedir ve özel anahtarların aksine genel anahtarların gizli tutulmasına gerek yoktur. Zira her ne kadar özel anahtar ile genel anahtar arasında matematiksel bir ilişki varsa da günümüz teknolojisinde bir bilgisayarın genel anahtar üzerinden özel anahtarı hesaplayabilmesi imkansıza yakındır. Bir diğer anlatımla, genel anahtarı özel anahtardan hesaplamak çok kolay olmasına rağmen, tersini yapmak temeldeki kriptografik algoritmaların temelindeki kompleks matematik nedeniyle son derece karmaşık ve zorlu bir işlemdir.



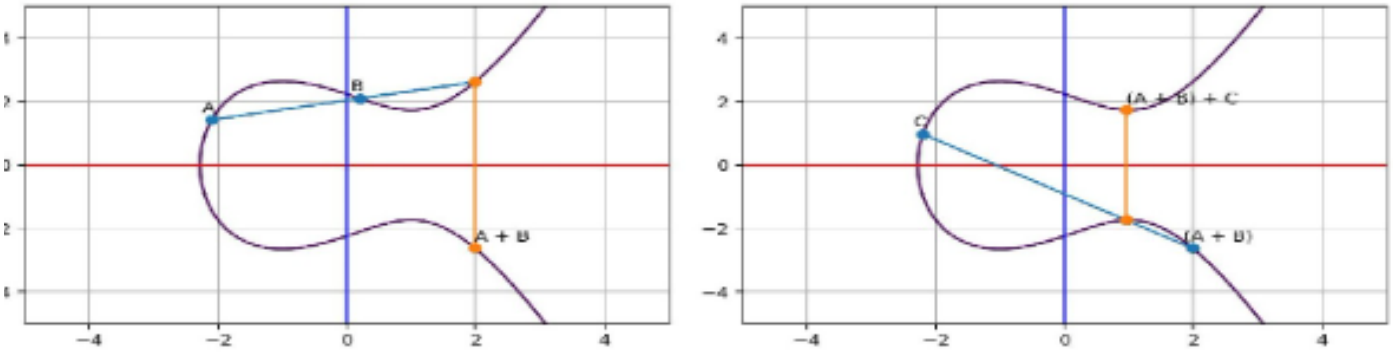


Genel anahtarların iki temel görevi vardır. İlk olarak, yalnızca belirli bir özel anahtarın sahibi bu spesifik genel imzayı oluşturabileceğinden kullanıcının kimliği ve işlemin gerçekliği kamuoyunda doğrulanmış olur. İkinci olarak ise genel anahtar kullanıcının adresine erişmek ve söz konusu kullanıcı ile zincir üzerinde işlem yapabilmek üzere diğer katılımcılar tarafından kullanılır. İşleme ilişkin veri alıcının genel anahtarıyla şifrelenmiş olduğundan yalnızca bu genel anahtarla ilişkilendirilen özel anahtarın veriyi şifre çözme yetkisine sahip olması gerekmektedir. Sonuç olarak, veriler güvenli bir kanal aracılığıyla iletilmemesine rağmen, asimetrik kriptografi sayesinde, işlem ve veri güvenliği tesis edilmiş olur.

Uygulamada, asimetrik kriptografik algoritmalar üç farklı kompleks matematiksel hesaplamaya dayanmaktadır: *çarpanlarına ayırma (ya da tamsayı faktorizsayon) şemaları (integer factorization schemes), kesirli logaritma şemaları (discrete logarithm schemes) ve eliptik eğri şemalarıdır (elliptic curve schemes) [7].* Örneğin, Rivest-Shamir-Adleman (RSA) Algoritması'nda yaygın olarak kullanılan tamsayı çarpanı problemi, verilen bir bileşik sayı N'den X ve Y olmak üzere iki tam sayıyı bulmayı gerektirir. Her ne kadar bu problem küçük sayılarla kolay gibi görünse de (örneğin, 35=5x7), asimetrik kriptografide bu sayılar oldukça büyük olduğundan sayıları çarpanına ayırma işlemi makul bir zaman çerçevesinde çözülemeyecek kadar büyük bir karmaşıklık oluşturur [7].

Öte yandan, Dijital İmza Algoritması (DSA) ve Diffie-Hellman Anahtar Değişim Algoritması'nda kullanılan kesirli logaritma şemaları, α tabanında β'nin kesirli logaritmasını belirleme problemini çözmeyi gerektirir ve matematiksel olarak x= log α β mod p şeklinde formülize edilebilir [7]. Bu matematiksel formül, bir örnek ile basitleştirilebilir: kesirli logaritma problemi, 5'in üreteç sayısı olduğu ve 5x= 41 mod 47 olduğu durumda pozitif tam sayı x'i bulmaktır ve kaba kuvvet saldırısı (brute force attack -yani x için mümkün olan tüm değerleri sistemli bir şekilde deneme) ile çözüm 15'tir [7]. Bu hesaplama, 5'i kendisiyle 15 kez çarparak ve sonucu 47'ye bölerek kalan olarak 41'in elde edileceğini göstermektedir. Bu problem de temelde karmaşık ve teorik olarak çözülemez değildir; ancak, parametreler yeterince büyütüldüğünde, problemin zorluğu o kadar artar ki, mevcut teknolojiyle problem makul bir sürede çözülemez hale gelir. Bu nedenle, genel anahtardan özel anahtarı bulmaya yönelik herhangi bir girişim, mevcut teknolojiyle ne hesaplama açısından ne de zamansal açıdan makul bir şekilde gerçekleştirilemez [7] [8].

Nihayet, Elips Eğrisi Dijital İmza Algoritması (Elliptic Curve Digital Signature Algorithm-ECDSA) tarafından kullanılan ve günümüzde en yaygın olarak kullanılan blockchain ağlarında kullanılan eliptik eğri şemaları, yine kesirli logaritma problemlerine dayanmakla beraber bu sefer matematiksel olarak y = x3 + ax + b şeklinde formülize edilen eliptik eğri gruplarında gerçekleştirilir [7].



Tablo 1. Eliptik Eğri Kriptografisi Hesaplama

Kaynak: https://fangpenlin.com/posts/2019/10/07/elliptic-curve-cryptography-explained/

En basit ifadeyle, eliptik eğri kriptografisi, iki rastgele nokta A ve B'nnin (bir tanesi x-ekseninden (yatay çizgi) ve diğeri y-ekseninden (dikey çizgi)) seçilerek, bu iki noktayı içeren bir çizgi çizerek gerçekleştirilir. Bu çizgi sonunda, eğride üçüncü bir noktayla kesişecek (zira matematiksel olarak, dikey olmayan herhangi bir çizgi en fazla üç noktada eğriyi kesmelidir) ve bu üçüncü nokta y eksenine yansıtıldığında ortaya çıkan yeni referans noktası A+B'yi oluşturacaktır. Bu kriptografik bulmaca, her seferinde yeni bir rastgele nokta seçip dikey olmayan bir çizgi çizdikten sonra kesişen üçüncü noktayı eğrinin y eksenine yansıtılması suretiyle defalarca kez tekrarlanabilmektedir [9].

ECDSA'da anahtar üretimi, eliptik eğri içindeki bir noktanın (rastgele bir tamsayı) rastgele veya pseudorandom (sözde rassal/ sözde rastgele- yani gerçek anlamda rastlantısal olmamakla beraber aralarındaki matematiksel ilişkinin kolay kolay kurulamayacağı) şekilde özel anahtar olarak seçilmesiyle başlar. Akabinde bu özel anahtar eliptik eğri üzerinde özel olarak tanımlanmış olan üreteç noktasıyla (generator point) çarpılarak genel anahtar üretilmiş olur [10]. İlk noktanın rasgeleliği ve tüm hesaplama sürecinin karmaşıklığı göz önüne alındığında, genel anahtardan özel anahtarın makul bir süre içinde yeniden hesaplanması mevcut hesaplama teknolojileri göz önünde bulundurulduğunda mümkün değildir.

Yukarıda bahsedilen tüm kriptografi şemaları ve altta yatan matematiksel problemler,kullanıcının özel anahtarının tehlikeye atılmaması koşuluyla klasik bilgisayarlarla gerçekleştirilen siber saldırılara karşı yeterince güçlüdür. Bununla birlikte, ölçeklenebilirlik endişeleri dikkate alındığında, çoğu mevcut blokzincir ağı, RSA ile aynı güvenlik seviyesini daha küçük bir anahtar uzunluğuyla sağladığı için, eliptik eğri kriptografisini, daha da belirli olarak ECDSA'yı tercih etmektedir [2] [11].

Bu noktada belirtmekte fayda gördüğümüz son husus ise imza algoritmasının anahtar boyutu ile güvenlik seviyenin birbirlerinden farklı şeyler olduğudur. Teknik anlamda bu ikisi arasında bir korelasyon olduğundan anahtar boyutu büyüdükçe imza algoritmasının güvenlik seviyesi de artmaktadır. Ne var ki, anahtar boyutu, algoritmanın güvenlik seviyesini doğrudan yansıtmaz. Anahtar boyutu algoritmada kullanılan anahtarın bit uzunluğunu ifade ederken güvenlik seviyesi algoritmanın bilinen en iyi saldırıyla (ki bu günümüzdeki imza algoritmaları için kaba kuvvet saldırısıdır) kaç adımda çözülebileceğini gösterir [7]. Bu bağlamda, 256 bitlik bir ECDSA algoritmasının özel anahtarını bulmak için bir saldırganın, mevcut teknolojinin geldiği noktada imkansıza yakın bir senaryo olan 2^{128} (340,282,366,920,938,463,463,374,607,431,768,211,456) olasılığı denemesi gerekmektedir.

Blokzincir	İmza Algoritması	Anahtar Boyutu (bit)	Güvenlik Seviyesi (bit)
Bitcoin	ECDSA	256 bit	128 bit
Ethereum	ECDSA	256 bit	128 bit
Litecoin	ECDSA	256 bit	128 bit
Monero	EdDSA	256 bit	128 bit
ZCash	ECDSA	256 bit	128 bit

Tablo 2. Beş ana blokzincir platformunda kullanılan imza algoritmalarının anahtar uzunluğu ve güvenlik seviyelerine göre mukayesesi

ÖZETLEME (HASH) FONKSİYONU & BLOKZİNCİR TEKNOLOJİSİ

Blokzincir teknolojisinde uygulanan bir diğer kritik kriptografik algoritma ise özetleme(hash) fonksiyonudur. Özetleme fonksiyonu, başlangıçta, genellikle "mesaj" olarak adlandırılan (herhangi bir boyuttaki) veriyi fonksiyonun temelindeki matematiksel algoritma doğrultusunda sabit ve belirli bir uzunlukta veri özeti değerine (hash value, message digest veya hash) dönüştürmek üzere kriptografik protokollerde yaygın olarak kullanılan bir araçtır [7] [12]. Bu bağlamda, özetleme fonksiyonu yalnızca bir harf için de yüzlerce sayfalık bir metin için de aynı (sabit) uzunlukta (ve elbette ki birbirinden tamamen farklı) özet değeri üretecektir -ki bu sabit uzunluk özetleme fonksiyonunda kullanılan algoritmaya bağlı olacaktır. Bu noktada belirtmekte fayda gördüğümüz bir diğer husus ise yukarıda değindiğimiz üzere asimetrik kriptografi iki yönlü bir şifreleme algoritmasıyken (yani belirli gizli anahtarlarla şifreli mesaj deşifre edilebilir) özetleme fonksiyonu tek yönlü bir algoritmadır ve dolayısıyla özet değerden (hash value) özetlenen mesaja dönmek imkansızdır. Bu anlamda özet değerini tersine çevirmek için bir gizli anahtar bulunmaz.

Özetleme fonksiyonu, blokzincir teknolojisinde çeşitli amaçlar için kullanılmaktadır. Özetleme fonksiyonu, ilk olarak, veri bloklarını kronolojik olarak birleştirerek (zincirleyerek) kayıtların bütünlüğünü sağlamaktadır. Öyle ki, her bir blok, bir blok başlığı ve veri içermektedir. Blok başlığı, yazılımın sürümünü, yalnızca bir kez kullanılan sayıyı (number only used once - nonce), hedefi (nBits veya target), Merkle kökünü (Merkle Roots), zaman damgasını (timestamp) ve önceki bloğun özet değerini içerirken, veri bloğu blokta kaydedilen işlemleri içerir. Bir veri bloğu kapasitesini doldurduğunda, özetlenir ve özet değeri onu takip eden bir sonraki bloğun girdisi olduğundan bu bloklar birbirlerine bağlanır (ya da zincirlenir), ki tam da bu esasında bloklar zincirini yani blokzincir teknolojisini oluşturur.

Özetleme fonksiyonu, blokzincirin bütünlüğü ve güvenilirliğinin en temel itici gücüdür. Zira bir blokta zaten kaydedilen verileri değiştirmek veya kaldırmak için yapılan herhangi bir girişim, bloğun özet değerini önemli ölçüde değiştireceğinden ve saldırganın tüm ardışık blokların özet değerlerini değiştirmesi gerektiğinden, bu kötü niyetli saldırı gerçekleştirilemez.

Ayrıca, özetleme fonksiyonu, mutabakat mekanizmasında işin ispatı (Proof of Work- PoW) algoritmasının kullanıldığı blokzincirlerin madencilik süreçlerinde de rol oynamaktadır. Şöyle ki, işin ispatında madenciler, özetleme algoritmasına dayalı kriptografik bir bulmacayı çözmek için Uygulamaya Özel Entegre Devre Madenci (Application Specific Integrated Circuit- ASIC Miner) adı verilen özel donanımı kullanmak suretiyle hesaplama güçlerini bloklar oluşturmak ve işlemleri doğrulamak için harcarlar.

Kural olarak, kötü niyetli bir madenci, geçerli olmayan bir işlemi doğrulamaya çalıştığında, hesaplama gücünün (ve dolayısıyla para kaynağının) boşa harcanmasına neden olur; ancak, bu kural, 51% saldırısı olarak da bilinen, saldırganın ağın hesaplama gücünün yarısından daha fazlasını kontrol etmediği durumlarda geçerlidir. [2] [13] [14]. Bu mekanizmaya güvenerek, madenciler birbirlerini tanımaya veya güvenmeye ihtiyaç duymadan blokzincirde yapılan işlemlerin ve tutulan kayıtların bütünlüğü ve güvenilirliği üzerinde uzlaşma sağlarlar.

İdeal ve güvenli bir özetleme fonksiyonu algoritması, ön imaj direnci (veya ön görüntü dayanıklılığı) (pre-image resistance), çakışma direnci (collusion resistance), ikinci ön imaj direnci (veya hedef çarpışma direnci) (second pre-image resistance veya target collusion resistance) ve çığ etkisi (avalanche effect) gibi belirli özelliklere sahip olmalıdır [15] [16] [17]. Özetleme fonksiyonun tek yönlü bir algoritma olmasını sağlayan ön imaj direnci, mesajın “M” özetlenip özet değeri “D” üretildikten sonra, özet değeri D’den mesaj M'yi bulmanın hesaplama açısından ekstrem düzeyde zor olması gereken bir özelliktir [18]. Sabit bir uzunluğa sahip bir özet değeri için sonlu olasılıklar olduğundan, farklı verilerin özet değerlerinin aynı olma olasılığı vardır. Bu bağlamda, çakışma direnci, mesajlar özetlendikten sonra aynı özet değerini üreten iki farklı mesajı bulmanın hesaplama açısından zor olması gerektiği anlamına gelir [18].

İkinci ön imaj direnci, çakışma direncine benzediğinden zayıf çakışma direnci olarak da adlandırılmaktadır. İkinci ön imaj direnci, mesaj M ile aynı özet değerine sahip başka bir mesaj B'yi bulmanın hesaplama açısından ekstrem zor olduğu bir senaryoyu tanımlamaktadır [18]. Diğer bir deyişle, çakışma direnci daha çok iki rastgele mesaj arasında bir çakışma bulmaya odaklanırken, ikinci ön imaj direncinde saldırganın başlangıçta belirli bir mesajı vardır ve orijinal mesajı değiştirmek için aynı özet değerine sahip başka bir mesaj arar [19]. Son olarak, çığ etkisi, bir özetleme fonksiyonunun küçük değişikliklere karşı duyarlılığını gösterir [17]. Bu bağlamda, ideal bir özetleme fonksiyonu, mesaj hafifçe değiştirildiğinde (örneğin, mesajdaki bir küçük harf büyük harfe çevrildiğinde) algoritma tamamen farklı bir özet değeri oluşturur.

Bu makalenin yazıldığı zaman itibarıyla, Güvenli Özetleme Algoritması (Secure Hash Algorithm- SHA) ailesi, özellikle SHA-2 algoritmaları ve Keccak tabanlı SHA-3 algoritmaları en yaygın kullanılan ve güvenli algoritmalardır. Ayrıca, bunlar Amerika Birleşik Devletleri’nin Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology- NIST) tarafından resmi olarak kabul edilmiştir [20]. Blokzincir teknolojisinde, genellikle SHA-256 ve Keccak-256 uygulanmaktadır. SHA-256 ve Keccak-256 algoritmalarının güvenlik seviyesi, saldırı türüne bağlı olarak değişmektedir. Bu anlamda, her iki algoritma da 2^{256} ön imaj direnci sunarken, bu güvenlik seviyesi çarpışma saldırıları için 2^{128}'e düşmektedir [21] [22].

Blokzincir	Özet Fonksiyon Algoritması	Özet değer (Bit)	Güvenlik Seviyesi (Ön imaj)	Güvenlik Seviyesi (Çakışma)
Bitcoin	SHA-256	256 bits	256 bits	128 bits
Ethereum	SHA-3 (Keccak-256)	256 bits	256 bits	128 bits
Litecoin	SHA-256	256 bits	256 bits	128 bits
Monero	SHA-3 (Keccak-256)	256 bits	256 bits	128 bits
ZCash	SHA-256	256 bits	256 bits	128 bits

Tablo 3. Beş ana blokzincir platformunda kullanılan özetleme fonksiyonu algoritmalarının özet değer uzunluğu ve güvenlik seviyelerine göre mukayesesi

2. BLOKZİNCİR TEKNOLOJİSİ ÜZERİNDEKİ KUANTUM TEHDİDİ

Kuantum bilgisayarlarını -süper bilgisayarlar da dâhil olmak üzere- günümüzde kullanılan bilgisayar ve hesaplama sistemlerinden ayıran en büyük fark kuantum bilgisayarlarının gerçekleştirdiği hesaplamalarda kuantum mekaniğinin benzersiz özelliklerinden faydalanılmasıdır. Gerçekten de, atomaltı parçacıklarının tabi olduğu ve klasik fizikten önemli ölçüde ayrışan (ve hatta kimi zaman çelişen) prensiplerin bilgisayar teknolojilerinde kullanılması sayesinde kuantum bilgisayarları hesaplama gücü, hızı ve verimliliği açısından oldukça büyük avantajlar sağlamaktadır. Dahası, iki özel kuantum algoritmasından faydalanarak, kuantum bilgisayarları esasında oldukça karmaşık ve mevcut teknolojik konjonktürde çözülmesinin olanaksız olduğuna inanılan problemleri etkili bir şekilde çözebilmektedir. Öte yandan, önceki bölümde detaylıca irdelediğimiz üzere, modern kriptografi, günümüz teknolojisinde çözümü pratik açıdan olanaksız olan belirli karmaşıklıktaki matematiksel problemler üzerine inşa edilmiş olmakla beraber yeterli kübit kapasitesine sahip kuantum bilgisayarlar için bu problemler ne kadar karmaşıktır ne de bunların çözümü olanaksızdır. Bu nedenle, kuantum bilgisayarları, blokzincir teknolojisi de dahil olmak üzere mevcut kripto-sistemlere yıkıcı etkileri olabilir.

KUANTUM MEKANİĞİNE DAYANAN YENİ BİR HESAPLAMA TEKNOLOJİSİ

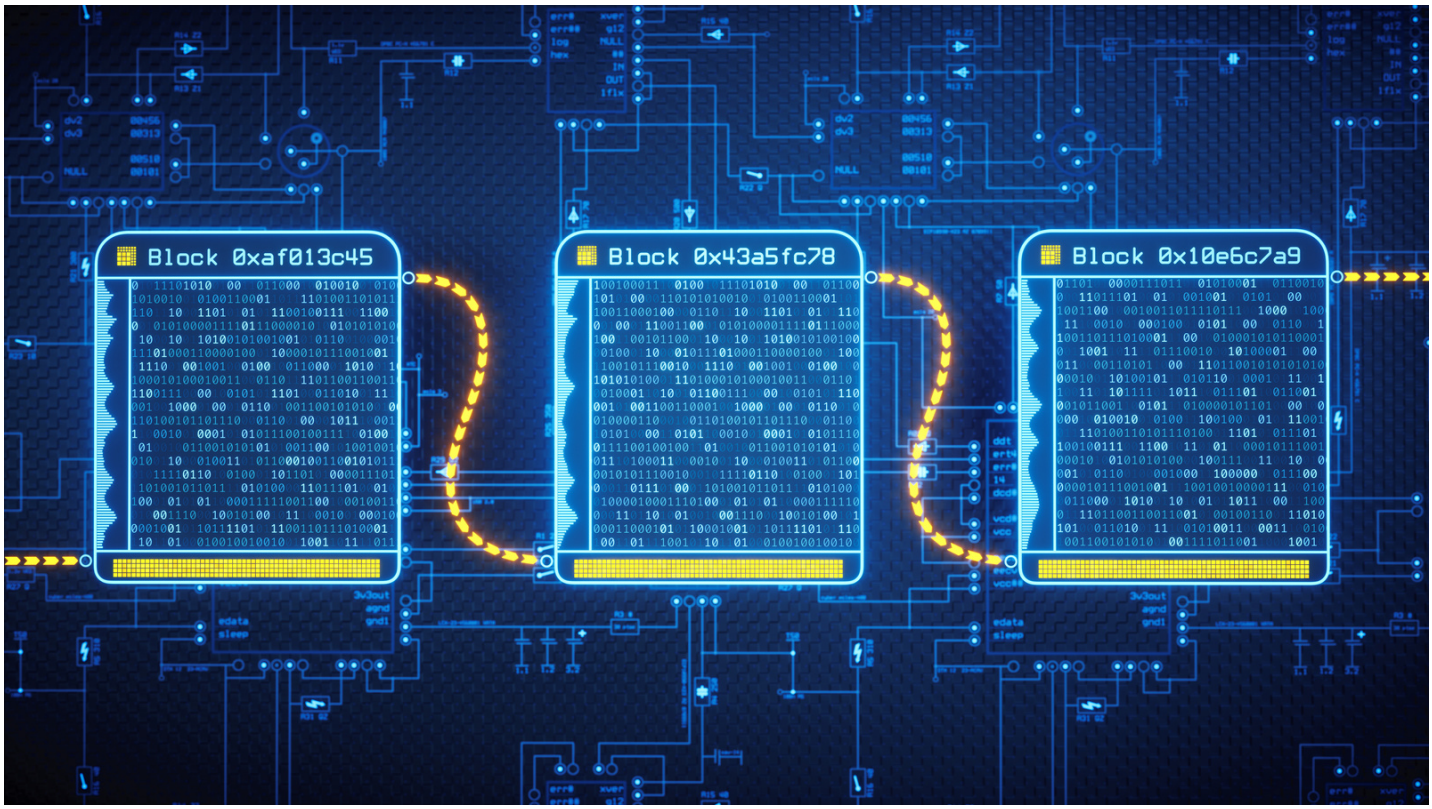
Kuantum mekaniğinin keşfi, kuantum düzlemindeki atomaltı nesnelerin davranışlarının gözlemlenebilir makroskobik ölçektekilerden çok farklı olmasından dolayı adeta bir dönüm noktası olarak nitelendirilmektedir. Kuantum aleminde egemenlik süren bazı prensipler bizlere yeni ve daha verimli hesaplama cihazları inşa etme olasılıklarını yaratmıştır. Makalemiz kapsamında özellikle şu dört kuantum prensibi büyük bir öneme sahiptir: kuantum dekoherans (kuantum ayrışma ya da kuantum eşevresizliği olarak da çevrilmiştir- quantum decoherence), belirsizlik (uncertainty), süperpozisyon (superposition) ve kuantum dolanıklığı (entanglement).

Kuantum dekoherans, atomaltı parçacıklarının çevreyle etkileşime girmesi sonucu (örneğin, kuantum nesnelerinin kuantum durumlarının ölçülmesi) kaynaklanan tutarlılık kaybını ifade eder ve parçacıkların kuantum durumlarına ilişkin bilgi kaybına yol açar [23] [24]. Bu bağlamda, kuantum nesnelerine dair yapılacak herhangi bir gözlem, ölçümleme veya herhangi bir diğer çevresel müdahale, kuantum alanının çökmesine sebebiyet vereceğinden atomaltı nesnelerin kuantum davranışlarını sonlandırmaktır. Dekoherans ile ilişkili olarak, belirsizlik ilkesi ise, bir kuantum nesnesine ait bir çift fiziksel özelliğin (örneğin, hızı ve konumunun) tek bir ölçümlemeyle aynı anda kesin olarak hesaplanamayacağını, dolayısıyla bir parçacığın hem momentumunun hem de konumunun ayı anda bilinemeyeceğini ifade etmektedir [25]. Öyle ki, bu ölçümlemeyi yapmak için gereken gözlem, kuantum alanında dekoherans yaratacağından gözlemlenen parçacık kuantum davranışlarından çıkmaya ve belirli bir pozisyonda (ya da konumda) olmaya zorlanır. Dolayısıyla yapılan gözlem ve/veya ölçüm ile parçacığın kuantum durumuna ilişkin bilgi kaybı söz konusu olmaktadır [25] [26].

Süperpozisyon, atomaltı parçacıkların kuantum düzleminde aynı anda birden çok durumda bulunabilme yeteneğini ifade etmektedir. Bu anlamda, klasik fizikte her bir nesne belirli ve tek bir durumda bulunurken, kuantum düzleminde atomaltı parçacıklar aynı anda birden fazla durumun süperpozisyonunda bulunmaktadır.

Basit bir örnekle ifade etmek gerekirse, kuantum düzleminde bir kuantum madeni para atarsak, madeni paranın üç olası durumu olur: yazı, tura ve bu ikisinin süperpozisyonu olan hem yazı hem de tura. Bu noktada hatırlatmakta fayda görmekteyiz ki, olası bir ölçümleme sonucu kuantum durumu çökeceğinden bu kuantum madeni para süperpozisyon durumundan çıkmak ve ya yazı ya da tura olmak zorunda kalacaktır. Son olarak, kuantum dolanıklığı ise, birbirleriyle mesafelerine bakılmaksızın iki veya daha fazla kuantum alt sistem arasındaki anlık (ışık hızından daha hızlı) ilişki ve iletişimi ifade etmektedir[26] [27]. Kuantum aleminde birbirleriyle dolanık hale gelmiş iki alt sistem veya parçacığın artık birbirinden bağımsız düşünülmesi imkansız hale gelir zira bu iki dolanık eş artık birlikte birleşik bir kuantum durumu yaratmış olur. Bu nedenle, kuantum diyarında birbirlerine dolanık eşlerden yalnızca birinin ölçülmesiyle diğer eşe ilişkin sonuçlar da elde edilmiş olacaktır [28]. Zira ölçülmeyen parçacık milyarlarca kilometre uzakta olsa bile dolanık eşinin ölçüldüğünden anında haberdar olacağından bu ölçümleme sonucu ölçülmeyen parçacığın da kuantum durumu–dekoherans gereği- çökmeye başlayıp belirli bir konum, durum veya momentumda olmaya zorlanacaktır.

Bu benzersiz özellikleri kullanarak, kuantum bilgisayarları belirli görevler için klasik bilgisayarlara kıyasla olağanüstü bir hesaplama yapar. Klasik hesaplamanın temel bilgi depolama ve işleme birimi bit (binary digits -ikili sistem veya ikili rakam olarak çevrilmektedir) olup her bir bitin değeri ya 1 ya da 0 olabilir. Öte yandan, kuantum hesaplama sistemlerinde temel birim ise bit değil, kuantum bit, yani kübit (qubit) olarak adlandırılır ve aynı anda 1 ve 0'ın süperpozisyon durumunda olabilmektedir [29] [30]. Kuantum bilgisayarları süperpozisyon ve dolanıklık fenomenlerinden faydalandığından aynı anda birden fazla hesaplama yolunu eşzamanlı olarak izleyebilmektedir ki buna paralel hesaplama ya da kuantum paralelliği denmektedir. Bu sayede kuantum bilgisayarları muazzam bir hız ve hesaplama verimliliği sağlar [31] [32]. Yeterli sayıda kararlı kuantum bit ile güçlendirilmiş kuantum bilgisayarları, günümüzdeki klasik hesaplama sistemleriyle pratik olarak çözülemeyen zor ve karmaşık problemlerin kuantum algoritmaları sayesinde kolaylıkla ve oldukça kısa süreler içinde çözebilecektir.



OYUNU DEĞİŞTİREN İKİ KUANTUM ALGORİTMASI: SHOR & GROVER

Kuantum algoritması, belirli hesaplama görevlerini gerçekleştirmek için kuantum mekaniğinin kendine özgü prensiplerinden yararlanan oldukça karmaşık ve özel bir hesaplama algoritmasıdır. Nadir istisnalar olmakla birlikte, bir kuantum algoritmasının işleyişi genellikle bir kuantum bilgisayarın varlığına bağlıdır ve kuantum bilgisayarındaki kübit sayısı arttıkça, bu algoritmalar görevleri daha kısa sürede ve daha hızlı çözebilirler. Elbette ki, belirli karmaşık problemlerin çözümü belirli bir sayıda (yüzlerce ve hatta binlerce) stabil kübit gerektirdiğinden günümüzdeki kuantum bilgisayarları onlarca veya yüz kadar kübit ile mevcut kriptografik protokoller için herhangi bir tehlike arz etmemektedir. Ancak, bu tespit yalnızca bugün için geçerlidir.

Ne var ki, yeterli sayıda stabil kübite sahip kuantum bilgisayarları üzerinde çalıştırılacak iki özel kuantum algoritması (Shor algoritması ve Grover algoritması) mevcut kripto sistemler ve bilhassa blokzincir teknolojisi üzerinde ciddi bir varoluş tehdidi yaratmaktadır. İlk olarak Shor algoritması, esasında çarpanlara ayırma probleminin öncelikle periyot bulmaya indirgenmesi ve akabinde kuantum paralelliğinden yararlanarak periyodun bulunması olacak şekilde iki aşamadan(yani iki alt algoritmadan) oluşmaktadır [33] [34]. Söz konusu hesaplama sırasında Shor algoritması kuantum paralelliğinden yararlanarak tüm olası değerleri aynı anda çalıştırır ve böylelikle mevcut asimetrik kriptografi sistemlerinin temelini oluşturan asal çarpanları bulma ve tamsayı logaritma problemleri için üstel bir hızlanma sağlar [10] [35].

Öte yandan, Lov K. Grover tarafından ortaya konulan Grover algoritması yapılandırılmamış veri tabanları ve oldukça büyük veri kümeleri araştırılan bilginin hızlı ve kolay bir biçimde bulunmasını sağlamak için geliştirilmiş bir kuantum arama tekniğidir[10] [34] [35] [36]. Grover algoritması, N öğeli bir yapılandırılmamış veri tabanında bir öğeyi –yine kuantum paralelliğinden faydalanarak- O(√N)=2N/2 işlemle bulurken, bu arama klasik bilgisayarlarla O(N)=2N adımlık bir süre gerektirir [29] [35]. Bu nedenle, bu algoritma hesaplamalar için üssel bir hız artışı sağlar[29] [35].

KUANTUM KIYAMETİ: OLASI YIKICI ETKİLERİN İNCELENMESİ

Yukarıda da açıkladığımız üzere, mevcut açık anahtarlı kriptografi sistemleri, asal çarpanlara ayırma ve kesirli logaritma problemlerinin karmaşıklığına ve mevcut teknolojik araçlarla makul bir süre içerisinde hesaplamasının pratik imkansızlığına bağlıdır. Başka bir deyişle, bir kullanıcının özel anahtarı, matematiksel olarak genel anahtarı ile ilişkili olduğundan genel anahtar üzerinden hesaplanabilirse de, bu hesaplama, tüm olasılıkların kaba kuvvet yöntemiyle denenmesini gerektirdiği için binlerce yıl ve ciddi bir hesaplama gücü gerektirmektedir. Bu anlamda, hem şifrelenmiş verilerin güvenliği hem de blokzincirdeki varlıkların kontrolü, asimetrik kriptografinin güvenliği ve dayanıklılığına sıkı sıkıya şekilde bağlı olduğundan bugün için blokzincir kullanıcılarının özel anahtarları ile blokzincirdeki veri bütünlüğü ve gizliliği noktasında yeterli güvenlik sağlanmıştır.

Öte yandan, yeterli sayıda stabil kübite sahip bir kuantum bilgisayarı üzerinde çalıştırılacak Shor algoritmasından faydalanan bir saldırgan, söz gelimi, dağıtık defterde kayıtlı bir işlemdeki genel anahtardan kullanıcının özel anahtarını tekrar hesaplayabilecektir [10] [13] [37]. Bunu yaparak, saldırgan, ele geçirilen özel anahtarla daha önceden şifrelenmiş olan bilgilere erişebilecek ve/veya özel anahtarın bağlı olduğu cüzdandaki varlıklar üzerinde (hala cüzdanda varlık mevcutsa) tasarrufta bulunabilecektir [10]. Dahası, henüz bir bloğa kaydedilmemiş olmakla beraber ağa (topluluğa) deklare edilmiş beklemedeki işlemlerde de genel anahtardan özel anahtar hesaplanabileceğinden işlem henüz doğrulama aşamasındayken işlem konusu kripto varlıkların işlemde öngörülen hesaba değil de saldırganın öngördüğü hesaba aktarılması suretiyle bu işlemler de manipüle edilebilecektir [2]. Benzer bir tehdit ayrıca akıllı sözleşmeler için de geçerli olabilir [38]

Bu noktada şunu belirtmekte fayda görmekteyiz: Monero blokzinciri EdDSA imza algoritmasını (ECDSA'nın bir türevidir ve kuantum saldırılarına aynı derecede savunmasızdır) kullanmasına rağmen, gizlilik odaklı yapısından kaynaklanan istisnai bir durum söz konusudur [2].

Monero'da işlemin değeri ifşa edilmediğinden saldırgan, harcadığı zaman, çaba ve hesaplama gücünün karşılığından alıp almayacağından hiçbir zaman emin olamaz. Zira burada genel anahtarı bulmak için birden fazla Pedersen bağlaması (değeri gizleme imkanı sağlayan bir çeşit şifreleme algoritması) çözülmesi gerekmektedir [2]. Bununla birlikte, bu durum Monero'yu gerçek manada kuantum dirençli bir blokzincir yapmaz; aksine, Shor'un algoritması tarafından güçlendirilen kuantum saldırıları, verilerin deşifre edilmesine ve kullanıcıların anonimliğinin ortadan kalkmasına neden olabilecektir [2]. Diğer bir istisnai durum olarak, ZCash, yukarıda bahsedilen ortak savunmasızlıkların yanı sıra, Zk-SNARK'ları oluşturan genel parametre olan küresel genel anahtar (global public key) üzerinden hesaplanabilecek küresel özel anahtarın (global private key) ele geçirilmesiyle saldırganın, sonsuz miktarda ZCash token üretebilmesine imkan yaratan ciddi bir zaafiyet söz konusudur [2].

Buna ek olarak, yeterli stabil kübit sayısına sahip bir kuantum bilgisayarına sahip bir saldırgan, Grover algoritmasından faydalanarak blokzincirde tutulan kayıtların bütünlüğünü ve güvenilirliğini tahrip edebilir. Bu durum farklı senaryolarda gerçekleşebilir. Daha önce de belirttiğimiz üzere, mutabakat mekanizması işin ispatı (PoW) olan blokzincirlerde madenciler, belirli kriptografik bulmacaları çözmek için özel bir donanım olan ASIC Miner kullanmaktadır. Öte yandan, Grover algoritması sayesinde, kuantum bilgisayarına sahip bir madenci klasik madencilere karşı madencilik sürecinde üssel bir hızlanma elde edeceğinden ağ %51 saldırılarına karşı savunmasız hale gelir[2] [13] [14] ve ortaya çıkacak güç konsantrasyonundan dolayı kötü niyetli bir düğüm bir bloğa hangi veriyi ekleyeceğine keyfi olarak karar verebilecektir [2]. Elbette ki, bu tür bir saldırı, ASIC Miners donanımının performans kalitesindeki gelişmeler ve iyileştirmelerle en azından kısmen önlenebilir veya ertelenebilir [2].

Bir diğer senaryo ise, Grover'ın algoritması, çakışma saldırıları ve ikinci ön imaj saldırıları ile özetleme fonksiyonlarını kırmak ve blokzincir kayıtlarını bozmak için kullanılabilir [13].

Bu senaryoda, bir saldırgan aynı özet değerine sahip iki farklı veriyi kolayca bulabilir ve böylelikle özet değerlerle birbirlerine bağlanmış bloklar zincirini bozmadan kayıtları değiştirebilir [13]. Böylece, saldırgan işlem kayıtlarını değiştirebilir ve işlem geçmişine ilişkin kayıtların bütünlüğünü ve güvenilirliğini azaltmış olur. Sonuç olarak, bu algoritma çakışma saldırıları ve ikinci ön imaj saldırılarını kolaylaştırarak ve madencilikte üssel bir hızlanma sağlayarak yalnızca mevcut asimetrik kriptografik protokolleri değil, aynı zamanda blokzincirde gerçekleşen işlemlere dair kayıtlarının bütünlüğünü ve güvenilirliğini de tehlikeye atar [6] [29].

Esasen, özet değerin sabit uzunluğunu artırdığımızda özetleme fonksiyonunun karmaşıklığı da üssel olarak artacağından Grover'ın algoritmasına ilişkin zafiyetten özet değerin sahip olacağı uzunluğu artırarak kaçınmak (en azından belirli bir süre ertelemek) teknik olarak mümkündür [37]. Fakat, bu yöntem -tıpkı dijital imzalarda da söz konusu olduğu gibi- özet değerlerin boyutunu artıracağı için ölçeklenebilirlik sorunlarına neden olur ve daha fazla hesaplama gücü ve depolama kapasitesi gerektirir. Dahası, bu "sabit uzunluk" kuantum hesaplamanın ilerledikçe ve geliştikçe artmaya devam etmelidir. Dolayısıyla, belirli bir noktada madencilik ve depolama için son derece yüksek maliyetli hale gelir [2]. Sonuç olarak, kuantum tehdidine karşı geliştirilecek bir önlemlerin, makul anahtar boyutları, makul özet uzunlukları, hızlı işlem kapasitesi ve düşük enerji tüketimi gibi belirli kriterleri karşılaması elzemdir [6].

	Shor Algoritması	Grover Algoritması	
Blokzincir	**Karşısındaki Zayıflık Seviyesi**	**Karşısındaki Zayıflık Seviyesi**	**Zayıflıkların Ortaya Çıkış Biçimi**
Bitcoin	Çok Zayıf	Orta	Bloğa eklenmemiş ancak topluluğa deklare edilmiş beklemedeki işlemler; 51% saldırısı; genel anahtardan özel anahtarın hesaplanması.
Ethereum	Çok Zayıf	Orta	Genel anahtardan özel anahtarın hesaplanması; akıllı sözleşmelerin güvenliği ve bütünlüğü.
Litecoin	Çok Zayıf	Orta	Bloğa eklenmemiş ancak topluluğa deklare edilmiş beklemedeki işlemler; genel anahtardan özel anahtarın hesaplanması; 51% saldırısı.
Monero	Çok Zayıf/ama saldırgan açısından mantıklı olmayabilir	Az	Transactions declared to the network; genel anahtardan özel anahtarın hesaplanması; gizlenmiş işlem grafiğinin ifşası; deanonimizasyon.
ZCash	Çok Zayıf	Orta	Bloğa eklenmemiş ancak topluluğa deklare edilmiş beklemedeki işlemler; 51% saldırısı; creation of ZCash jetonlarının üretilmesi (global özel anahtarın- *global private key*- ele geçirilmesiyle).

Tablo 4. Beş ana blokzincir platformunun Shor algoritması ve Grover algoritması karşısındaki zayıflıklarının mukayesesi

3. KIYAMET SENARYOSUNU ENGELLEMEK

Kuantum bilgisayarları günümüzdeki kriptosistemler için önemli ve giderek büyüyen bir tehdit olmakla beraber bu tehdit, blokzincir teknolojisi için daha kritik bir hal almaktadır. Çünkü blokzincir teknolojisinin merkezi olmayan ve dağıtık yapısı nedeniyle ağ içinde köklü değişiklikler yapmak zaman alır. Daha açık kılmak gerekirse, merkezi bir otorite olmadığı için tüm köklü değişiklikler, en azından çoğunluğun aynı yönde hareket ettiği durumlarda mümkün olan bir sert çatal (hard fork) oluşturularak gerçekleştirilir. Tehlikenin büyüklüğü göz önüne alındığında, ciddi güvenlik ve gizlilik ihlalleri yaşamamak için böylesi bir tehdit karşısında çoğunluğun değil bizzat tüm ağın sert çatalla aynı yönde hareket etmesi gerekmektedir. Buna ek olarak, tüm işlemler ve bilgiler, dağıtık defterde değişmez bir şekilde depolandığı için kuantum gücüne sahip saldırganlar "bugün topla yarın kır" motivasyonuyla şifreli verileri bugün toplayabilir ve kuantum bilgisayarları yeterli seviyeye ulaştığı zaman bunları kırmaya çalışabilir [38].

Sonuç olarak, geçmiş ve mevcut veriler, kuantum siber tehdidi altındadır ve hassas kriptografik protokoller kullanılarak gerçekleştirilen her bir işlemle birlikte tehlikede altındaki veri sayısı her geçen gün artmaktadır.

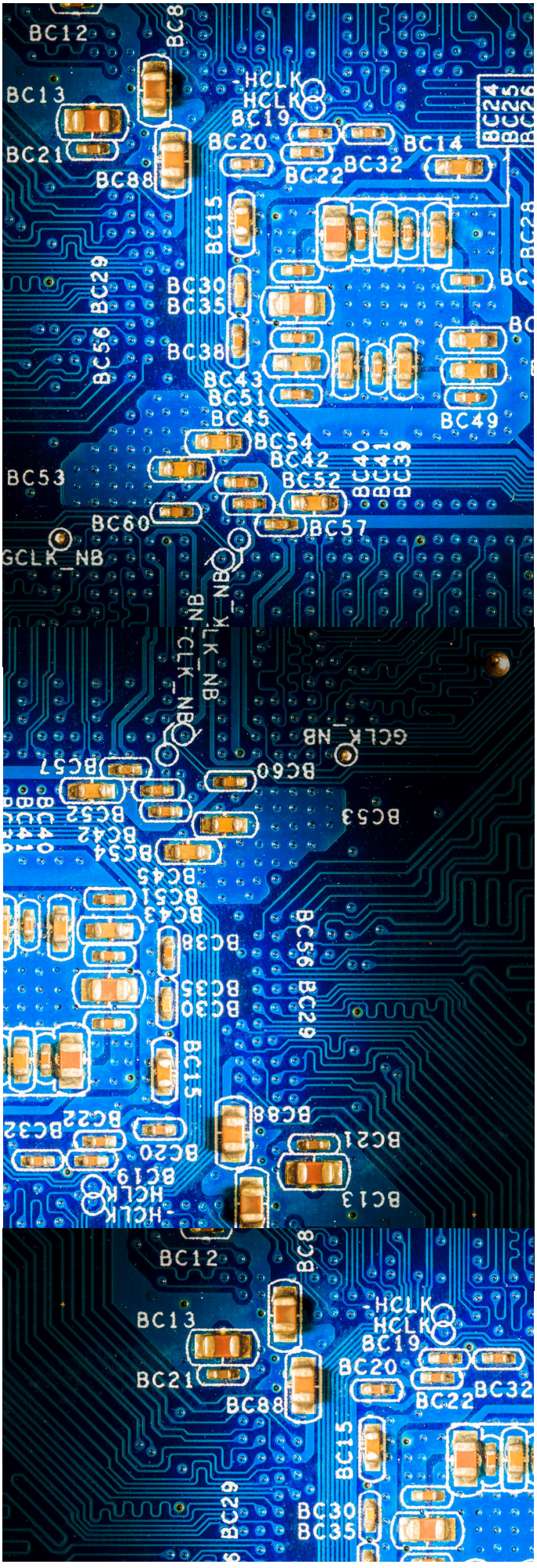
POST-KUANTUM (KUANTUM SONRASI) KRİPTOGRAFİ

Endişe verici tehlikeyi fark eden NIST, post-kuantum kriptografi protokollerinin standartlaştırma sürecini başlatarak kuantuma dayanıklı kriptografik protokollerin geliştirilmesi ve kuantum tehdidi gerçekleşmeden güvenli bir biçimde mevcut protokollerin terk edilerek kuantum saldırılarına dayanıklı protokollere geçiş yapılmasını sağlamayı amaçlamıştır [39]. Bu standartlaştırma süreci boyunca NIST, post-kuantum şifreleme protokollerinin güvenlik, etkinlik, performans, uygulanabilirlik ve diğer faktörler açısından değerlendirilmesi için bir dizi yarışma (competition) düzenlemiştir. Bu yarışmalar, farklı kriptografik algoritmaların değerlendirilmesine ve en iyilerin seçilmesine olanak sağlamıştır.

Post-kuantum kriptografide karşımıza özellikle kod tabanlı (code-based), kafes tabanlı (lattice-based), özet tabanlı (hash-based), çok değişkenli süpersingular eliptik eğri izogeni tabanlı (multivariate, supersingular elliptic curve isogeny-based) ve simetrik kuantum dirençli kriptografi (symmetric quantum-resistant cryptography) olmak üzere altı farklı algoritma ailesi karşımıza çıkmaktadır. NIST tarafından yapılan duyuruya göre, Classic McEliece (kod tabanlı), CRYSTALS-KYBER, NTRU ve SABER (kafes tabanlı) Asimetrik Kriptografi şifreleme algoritmaları ve anahtar değişim algoritmaları (Key Establishment veya Key Exchange Algorithm) için finalist algoritmalar olarak belirlenmiştir. CRYSTALS-DILITHIUM, FALCON (kafes tabanlı) ve Rainbow (çok değişkenli) ise dijital imza algoritmaları için seçilmiş olan finalistlerdir [40] [41] [42].

Post-kuantum kriptografi, mevcut kriptografik protokollerde olduğu gibi, matematiksel problemlere dayanan yepyeni kriptografik protokolleri kapsamaktadır. Ancak, günümüz protokollerinin aksine, post-kuantum kriptografideki problemlerin karmaşıklığı ve zorluğu öyle bir seviyeye çıkarılmıştır ki, yeterli seviyeye ulaşmış bir kuantum bilgisayarı bile bu kriptosistemleri kıramaz. Sonuç olarak, -elbette teoride- bir saldırganın binlerce kübite sahip bir kuantum bilgisayara sahip olduğu durumlarda bile kuantum dayanıklılığı sağlanmış olur.

Post-kuantum kriptografi algoritmaları anahtar boyutları, işlem hızı ve özel donanım gereksinimleri dikkate alınarak farklı performanslar sunar [6]. Bu konu, blokzincir teknolojisi için "en uygun" kriptosistemin seçilmesi için "güvenlik" ve "verimlilik" arasında hassas bir denge arayışı nedeniyle daha da önem kazanır. Diğer bir ifadeyle, yeni kriptografik protokollerin uygulanması blokzincir ağını güvenli hale getirmeli ve fakat bu güvenlik aşırı karmaşıklığa yol açmayan ve zaman ve enerji tüketimini artıran uygulamalar yüzünden blokzincir teknolojisinin kullanımını yavaşlatmamalı ve/veya engellememelidir. Bu bağlamda, bazı araştırmacılar, kafes tabanlı kriptografinin (anahtar boyutunu azaltmak için yapılacak bazı değişiklik ve güncellemelerden sonra) blokzincir teknolojisine uygulanması için en umut verici kriptosistemin olduğuna dair bir sonuç çıkarmışlardır [6] [43] [44].



Yine de, düşük performanslarına rağmen hızlı algoritmalar üretebilen değişiklik önerileri dikkate alındığında, özet tabanlı algoritmalar da blokzincir teknolojisi için pratik olabilir [6] [43] [44].

Ancak, kriptografi söz konusu olduğunda neyin ne kadar süreyle güvenli olduğunu söylemek her zaman isabetli olmayacaktır. Bilindiği üzere, kriptografi alanında kriptograflar ve hackerlar arasında sürekli bir rekabet (ve hatta adeta bir mücadele) vardır ki bu da ekosistemde bir çeşit Kızıl Kraliçe Etkisi yaratır. Bu perspektiften bakıldığında, yeni güvenli kriptografik teknikler ortaya çıksa da, bu sistemleri kırmak için yeni teknikler ve ekipmanlar da ortaya çıkacaktır ki tam da bu nedenle, bu kısır döngü, post-kuantum önlemler için de tekrarlanacaktır. En önemlisi de, bu algoritmalar, yeterli gelişmişliğe ulaşmış bir kuantum bilgisayarın yokluğunda geliştirilmiştir ve teknik zorlukların aşıldığı noktada bu bilgisayarların gerçekte ne kadar güçlü hale gelecekleri asla tam olarak bilinmemektedir. Sonuç olarak, post-kuantum kriptografi tekniklerinin -en kötü ihtimalle- potansiyel bir kuantum saldırısının tarihinin ertelenmesi konusunda önemli bir çözüm sağlayabileceğini söylemek mümkündür.

KUANTUM-DAYANIKLI BLOKZİNCİRLER: BİTCOİN POST-QUANTUM ÖRNEĞİ

Post-kuantum kriptografisi, özel bir odak olmadan genel olarak kriptografik protokolleri kullanan tüm bilişim sistem ve teknolojileri için ortak çözümler sunar. Ancak, önceki bölümde de belirtildiği gibi, genelleştirilmiş uygulamaların, özellikle operasyonel gereklilikler ve verimlilik gibi hususlar göz önünde bulundurulduğunda, blokzincir teknolojisi için uygun olmayabileceği düşünülmektedir. Bu perspektifle, şuan daha ziyade deneysel olarak karşımıza çıkan kuantum dayanıklı blokzincir ağları ortaya çıkmıştır.

Örneğin, Bitcoin Post-Quantum, Bitcoin blokzincirinde yaratılan sert bir çatalla oluşturulmuş bir kuantum dirençli ağ olup 555.000'e kadar olan blok yüksekliği için Bitcoin ile aynı ağ kurallarını uygularken bu eşikten itibaren daha önceden belirlenmiş tamamen farklı kuralların uygulanmasını sağlar [37]. Bitcoin Post-Quantum, kuantum dirençli bir dijital imza olan Genişletilmiş Merkle İmza Şeması (Extended Merkle Signature Scheme - XMSS)'yi kullanır. XMSS özet tabanlı olup tek Winternitz Tek Seferlik İmza modelini (Winternitz One-Time Signature - W-OTS+) uygulamaktadır [37] [45] [46].

Anılan blok yüksekliğine ulaşıldıktan sonra, Bitcoin Post-Quantum zincirinde ECDSA tamamen devre dışı bırakılacak olup kullanıcıların söz konusu eşikten sonra ECDSA kullanarak işlem yapmalarına izin verilmeyecektir [37]. Bunun yerine, kullanıcılar XMSS aracılığıyla yeni anahtarlar oluşturacak olup Bitcoin'lerini eski adreslerden yeni (post kuantum) adreslere aktaracaklardır [37]. Dahası, Bitcoin Post-Quantum blokzinciri mutabakat mekanizması olarak algoritmasını işin ispatı yerine ZCash'in kullanmakta olduğu Equihash PoW- Equihash işin ispatı algoritmasını kriptografik bulmacalar ve SHA-256 özetleme fonksiyonu gibi farklı parametrelerle kullanmaktadır [37].

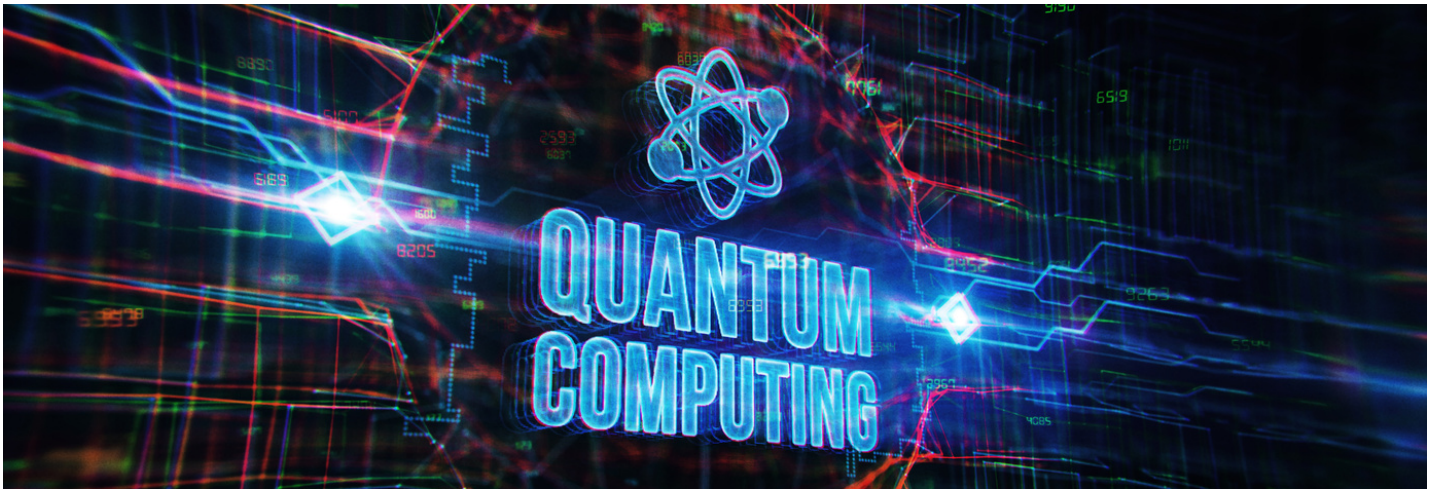
Post-kuantum kriptografi teknikleri gibi, kuantum dirençli blokzincir ağları olgun bir kuantum bilgisayarlarının yokluğunda ortaya çıktığı için oluşturulan kuantum dayanıklılığı teoriktir. Bununla birlikte, bu girişimler, yaklaşan tehdide karşı farkındalık yaratmak ve kuantum saldırılarına karşı bir miktar süre kazanmak için oldukça önemlidir. Kanımızca, kuantum bilgisayarlarının yeterli gelişmişliğe ulaştığı dönemde ve sonrasında, nihai ve işlem güvenliği muhtemelen kuantum kriptografisiyle ve blokzincir teknolojisiyle kuantum bilgisayarlarının birbirleriyle etkileşimi sonucu meydana çıkacak mutualist ilişki ve kombinasyonlar ile sağlanacaktır. Bu nedenle, blokzincir geliştiricileri, blokzincirin gerçek potansiyelini ortaya çıkarabilecek kuantum özelliklerinden yararlanarak kuantum blokzincir için yeni fırsatlar araştıracaktır.

SONUÇ

Kriptografi, özellikle de günümüzün sürekli dijitalleşen enformasyon toplumunda, güvenli ve gizli iletişimin en temel yapıtaşıdır. Daha fazla verinin dijitalleşmesiyle birlikte, siber tehditlerin kapsamı ve boyutu artmakta ve yeni şifre çözme ekipman ve tekniklerinin ortaya çıkmaktadır. Bu durum, veri ve güvenlik ihlallerini önlemek için kriptoanaliz alanında sürekli bir dikkat gerektirmektedir. Kuantum bilgisayarları, bu yeni ekipmanlardan biri olup tahminlere göre bu teknolojinin en geç 2035'e kadar yeterince güçlü hale gelebileceği ve birtakım kuantum algoritmalarından faydalanarak bugün oldukça yaygın kullanılan kriptografik protokolleri kırabileceği düşünülmektedir.

Blokzincir gibi kriptografiye yoğun bir şekilde bağımlı olan bir teknoloji de elbette ki bu tehdit altındadır ve olası bir kuantum felaketini önlemek için gerekli önlemlerin alması gerekmektedir. Şu anda NIST, yeterince büyük kuantum bilgisayarlarıyla saldırıldığında dahi güvenlik standartlarını koruyabilecek bir kuantum sonrası kriptografi protokollerini standartlaştırma sürecindedir. Ayrıca, belirli blokzincir girişimleri, kullanıcılarına kuantum güvenli ağlar sağladıklarını iddia etmektedir. Bununla birlikte, tüm bu karşı önlemler, yeterli sayıda kararlı kübite sahip bir kuantum bilgisayarının var olmadığı -ve dolayısıyla tam potansiyelinin henüz bilinmediği- bir aşamada geliştirildiğinden esasında sağlanan güvenlik seviyesi teoriktir. Yine de, mevcut konjonktür gözetildiğinde bu çözümlerin en azından potansiyel tehdidi ötelediği ve dolayısıyla, vadettikleri güvenlik seviyesi sağlanabildiği sürece önemli faydalar sağlaması kuvvetle muhtemeldir.

Kanımızca, kuantum çağında mutlak güvenliğin yine (kuantum kriptografi gibi) kuantum teknolojilerinden faydalanarak sağlanması muhtemeldir. Bu bağlamda, blokzincir ekosisteminde kuantum tehditlerine ilişkin farkındalık ve hazırlık çalışmalarının başlaması; gelecekte yaşanabilecek olası kuantum saldırılarına karşı alınacak tedbirler ve bu tedbirlerde hangi kuantum teknolojilerinden nasıl faydalanabileceğinin araştırılarak ekosistemin kuantum çağına hazırlanması büyük bir önem arz etmektedir.



KAYNAKÇA

[1] Michele Mosca, Cybersecurity in an Era with Quantum Computers: Will We Be Ready?, 16 IEEE SECURITY & PRIVACY 38 (2018)

[2] Joseph J. Kearney & Carlos A. Perez-Delgado, Vulnerability of Blockchain Technologies to Quantum Attacks, 10 ARRAY 1 (2021)

[3] Divesh Aggarwal, Gavin K. Brennen, Troy Lee, Miklos Santha & Marco Tomamichel, Quantum Attacks on Bitcoin, and How to Protect against Them, 3 LEDGER 68, 69 (2018).

[4] Jonathan P. Dowling & Gerard J. Milburn, Quantum Technology: The Second Quantum Revolution, 361 PHILOS. TRANS. R. SOC. A. 1655 (2003).

[5] Whitfield Diffie & Martin E. Hellman, New Directions in Cryptography, 22 IEEE TRANS. INF. THEORY 644 (1976).

[6] Tiango M. Fernández-Caramès & Paula Fraga-Lamas, Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Attacks, 8 IEEE ACCESS 21091, 21092 (2020).

[7] Chrıstoph Paar & Jan Pelz, Understandıng Cryptography: a Textbook for Students and Practıtıoners 155 (2010).

[8] Martin Roetteler, Michael Naehrig, Krysta M. Svore & Kristin Lauter, Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms, in 10625 LECT. NOTES COMPUT. SCI. (Tsuyoshi Takagi & Thomas Peyrin eds., 2017).

[9] Fang-Pen Lin, Elliptic Curve Cryptography Explained, FANG-PEN'S CODING NOTE (2019), https://fangpenlin.com/posts/2019/10/07/elliptic curve-cryptography-explained/

[10] Iain D. Stewart, Dragos Illie, Alexei Zamyatin, Sam Werner, Maziar F. Torshizi & William J. Knottenbelt, Committing to quantum resistance: A Slow Defence for Bitcoin against a Fast Quantum Computing Attack, 5 R. SOC. OPEN SCI. 3 (2022).

[11] Ritik Bavdekar, Eashan J. Chopde, Astutosh Bhatia, Kamlesh Tiwari, Sandeep J. Daniel & Atul, Post Quantum Cryptography: Techniques, Challenges, Standardization, and Directions for Future Research, ARXIV 5 (2022), https://doi.org/10.48550/arXiv.2202.02826.

[12] Rajeev Sobti & Greetha Ganesan, Cryptographic Hash Functions: A Review, 9 IJCSI 461 (2012).

[13] Noah Kappert, Erik Karger & Marko Kureljusic, Quantum Computing- The Impending End for the Blockchain? (Pacific Asia Conference on Information Systems 2021)

[14] Evgeniy Kiktenko, Nikolay Pozhar, Maxium Anufriev, Anton Trushechkin, Ruslan Yunusov, Yury Kurochkin, Alexander Lvovsky & Aleksey Fedorov, Quantum-Secured Blockchain, 3 Quantum Sci. Technol. 2 (2018).

[15] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY INFORMATION TECHNOLOGY LABORATORY COMPUTER SECURITY DIVISION, NIST SPECIAL PUBLICATION 800–107 REVISION 1 RECOMMENDATION FOR APPLICATIONS USING APPROVED HASH ALGORITHMS 6–9 (2012), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-107r1.pdf

[16] MIT OpenCourseWare, 21. Cryptography: Hash Functions, YouTube (Mar. 5, 2016), https://www.youtube.com/watchv=KqqOXndnvic&t=1792s.

[17] Yuliya Tanasyuk & Sergey Ostapov, Development and Research of Cryptographic Hash Functions Based on Two-Dimensional Cellular Automata, 8 INFORM. AUTOM. POMIARY GOSPOD. OCHR. ŚR. 24 (2018).

[18] Philip Rogaway & Thomas Shrimpton, Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance, in 3017 Lect. Notes Comput. Sci. 371 (Bimal Roy & Willi Meier eds., 2004).

[19] Harshvardhan Tiwari, Merkle-Damgård Construction Method and Alternatives: A Review, 41 JIOS 283, 285 (2017).

[20] NIST Informatıon Technology Laboratory, SHA-3 Standard: Permutatıon-Based Hash and Extendable-Output Functıons (2015), https://doi.org/10.6028/NIST.FIPS.202.

[**21]** CHRISTOPH PAAR & JAN PELZI, SHA-3 AND THE HASH FUNCTION KECCAK: AN EXTENSION CHAPTER FOR "UNDERSTANDING CRYPTOGRAPHY: A TEXTBOOK FOR STUDENTS AND PRACTITIONERS 4, http://professor.unisinos.br/linds/teoinfo/Keccak.pdf

[22] Furqan Shahid, Iftikar Ahmad, Muhammad Imran & Muhammad Shoaib, Novel One Time Signatures (NOTS): A Compact Post-Quantum Digital Signature Scheme, 8 IEEE Access 15895, 15900 (2020).

[23] Wojciech H. Zurek, Decoherence, Einselection, and the Quantum Origins of the Classical, 75 Rev. Mod. Phys. 715 (2003).

[**24]** David Wallace, Decoherence and Its Role in the Modern Measurement Problem, 370 Phil. Trans. R. Soc. A. 4576, 4586–4587 (2012).

[25] Paul Busch, Teiko Heinonen & Pekka Lathi, Heisenberg's Uncertainty Principle, 452 Phys. Rep. 155, 156 (2007).

[26] Ece Su Ustun, International Equity in the Quantum Age, Berkeley Glob. Soc'y (Dec. 7, 2021),https://berkeleyglobalsociety.com/en/perspectives /international-equity-in-the-quantum-age/

[27] Erwin Schrodinger, Die gegenwärtige Situation in der Quantenmechanik, 23 Naturwissenschaften 823, 827 (1935).

[28] Nivedita Dey, mrityunjay Ghosh & Amlan Chakrabarti, Quantum Solutions to Possible Challenges of Blockchain Technology, ArXıv, 11 (2021), https://doi.org/10.48550/arXiv.2110.05321

[29] Chrıs J. Hoofnagle & Sımon L. Garfınkel, Law and Polıcy for the Quantum Age 231 (2022);

[30] Eleanor Rıeffel & Wolfgang Polak, Quantum computıng: A Gentle Introductıon 2 (2011).

[31] Ivan B. Djordjevıc, Quantum Informatıon Processıng, Quantum Computıng, and Quantum Error Correctıon: An Engıneerıng Approach (2nd Ed. 2021)

[32] Giulio Casati & Giuliano Benenti, Quantum Computation and Chaos, in Encyclopedia of Condensed Matter Physics (Franco Bassani, Gerald L. Liedl, Peter Wyder eds., 2005).

[33] Unathi Skosana & Mark Tame, Demonstration of Shor's factoring algorithm for N = 21 on IBM quantum processors, Sci Rep 11, 16599 (2021). https://doi.org/10.1038/s41598-021-95973-

[34] Muharrem Tuncay Gençoğlu, Kuantum Kriptoanalizin Siber Savunmadaki Yeri, Kara Harp Okulu Bilim Dergisi, Aralık 2019, Cilt 29, Sayı 2, 179-202.

[35] Eleanor Rieffel & Wolfgang Polak, An Introduction to Quantum Computing for Non-Physicists, 32 ACM Comput. Surv. 300, 318 (1998, last revised 2000).

[36] Low K. Grover, A Fast Quantum Mechanical Algorithm for Database Search, (28th Annual ACM Symposium on the Theory of Computing 1996).

[37] Noah Anhao, Bitcoin Post-Quantum, Bıtcoın Post-Quantum, https://bitcoinpq.org/download/bitcoinpq-whitepaper-english.pdf.

[38] Arman R. Faridi, Faraz Masood, Ali H. T. Shamsam, Mohammad Luqman & Monir Y. Salmony, Blockchain in the Quantum World, 13 Int. J. Adv. Comput. Sci. Appl 542, 544 (2022).

[39] NIST, Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process, NISTIR 8413, (Temmuz 2022). https://doi.org/10.6028/NIST.IR.8413-upd1

[40] NIST, NIST Announces First Four Quantum-Resistant Cryptographic Algorithms,NIST.Gov (5 Temmuz 2022). https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic- algorithms

[41] Lukas Malina, Petr Dzurenda, Sara Ricci, Jan Hajny, Gautam Srivastava, Raimundas Matulevicius, Abasi-amefon O. Affia, Maryline Laurent, Nazatul H. Sultan & Qiang Tang, Post-Quantum Era Privacy Protection for Intelligent Infrastructures, 9 IEEE Access 36054 (2021).

[42] Andrada-Teodora Ciulei, Marian-Codrin Crețu & Emil Simion, Preparation for Post-Quantum Era: A Survey about Blockchain Schemes from a Post-Quantum Perspective, Cryptology ePrint Archive 3–6 (2022). https://eprint.iacr.org/2022/026.pdf.

[43] Yu-Long Gao, Xiu-Bo Chen, Yu-Ling Chen, Ying Sun, Xin-Xin Niu & Yi-Xian Yang, A Secure Cryptocurrency Scheme Based on Post-Quantum Blockchain, 6 IEEE Access 27205 (2018)

[44] Hyeongcheol An & Kwangjo Kim, QChain: Quantum-Resistant and Decentralized PKI Using Blockchain, 6, (Symposium on Cryptography and Information Security 2018).

[45] Andreas Hülsing, Denis Butin, Stefan Gazdag, Joost Rijeneveld & Aziz Mohaisen, XMSS: eXtended Merkle Signature Scheme, Internet Engineering Task Force (2018). https://datatracker.ietf.org/doc/html/rfc8391.

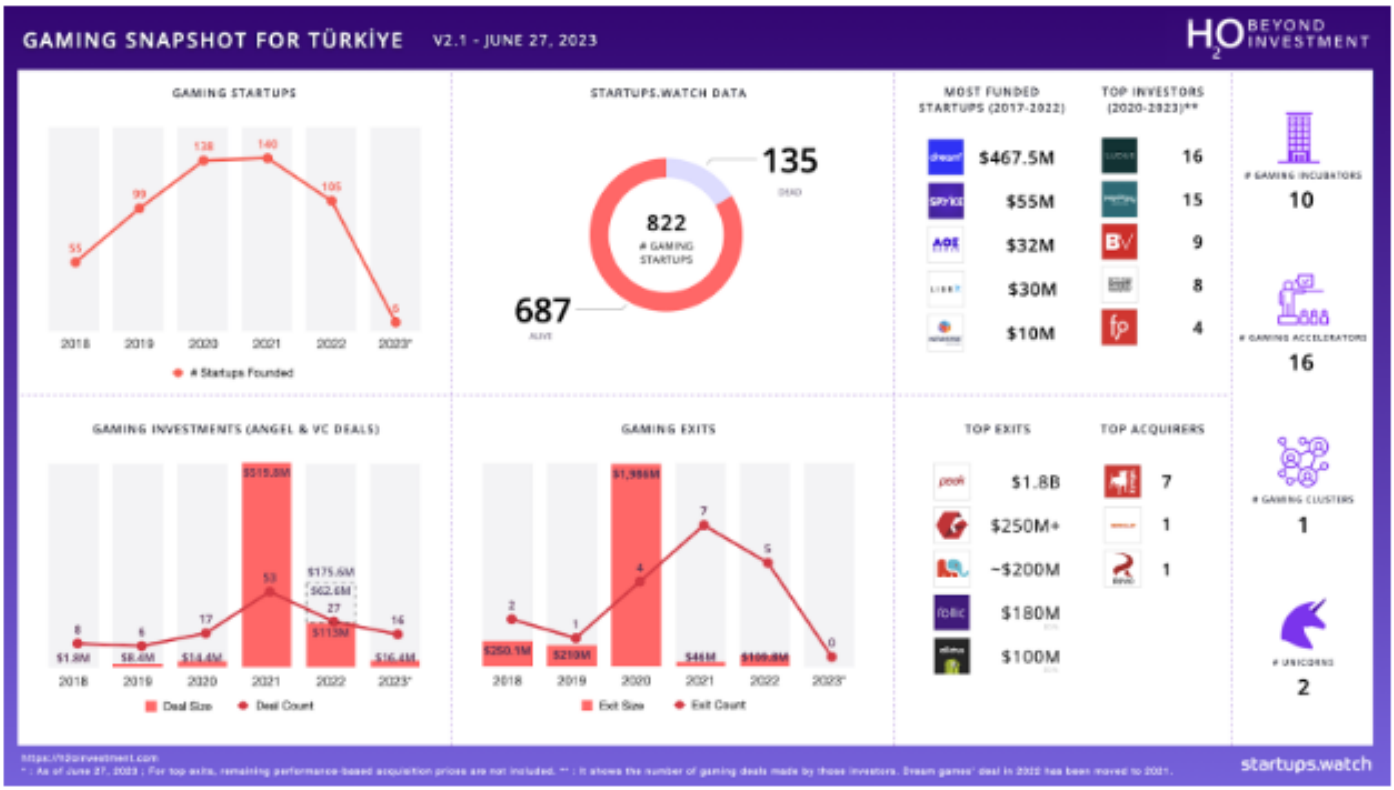
[46] Andreas Hülsing, Stefan Gazdag, Denis Butin & Johannes Buchmann, Hash-based Signatures: An Outline for a New Standard, National Institute of Standard and Technology Computer Security Research Center, NIST (2014). https://csrc.nist.gov/csrc/media/events/workshop-on-cybersecurity-in-a-post-quantum-world/documents/papers/session5-hulsing-paper.pdf.

Türkiye'de Oyun Sektörü Ve Oyun Tasarımcısı Olmak

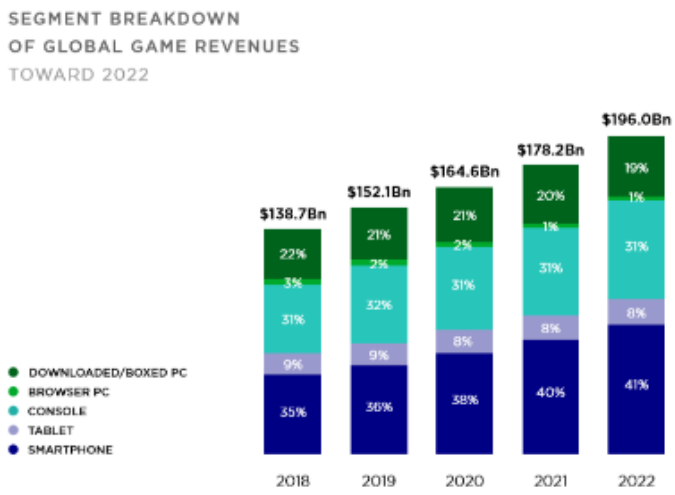
Senem Aksakal

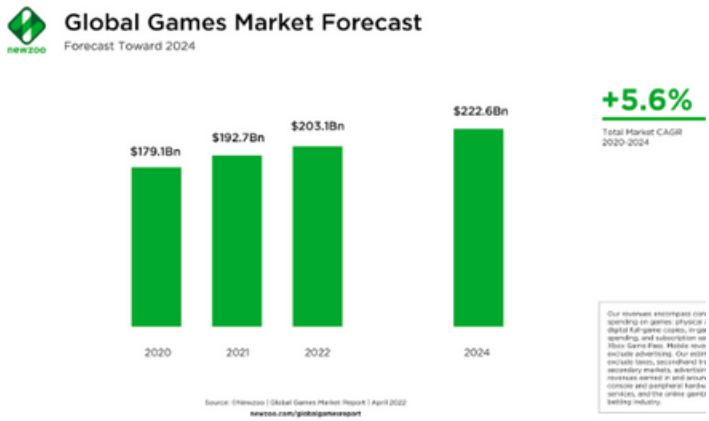
Türkiye'de oyun sektörünün gelişmesi özellikle **2000**'li yılların başına dayanmaktadır. Dünya çapında tanınırlığa sahip, BAFTA üyesi, oyun yapımcısı **Mevlüt Dinç**'in İngiltere'den Türkiye'ye dönüşü ve burada yaptığı çalışmalar ile Türkiye, ilk kez dünya arenasında ses getirmiştir. Bu tarihten önce, **1994** yılında, **İstanbul Efsaneleri: Lale Savaşçıları** gibi bazı kayda değer oyun girişimleri bulunmaktadır.

Türkiye'nin oyun sektöründe esas ivme yakalaması ise 2010 yılında **Sidar Şahin** tarafından İstanbul merkezli kurulmuş olan **Peak Games**'in, **2019** yılında **1.8 milyar dolara Zynga** tarafından satın alınması ile olmuştur. Bu satış ile birlikte Peak Games, Türkiye'den çıkan ilk **unicorn** (1 milyar doların üzerinde değerlemeye ulaşan şirket) olmuştur. Özellikle **2020 - 2022** yılları arasında Türk oyun sektörünün altın çağı yaşadığı söylenebilir. Bu dönemde yıllara göre sırasıyla **138, 140 ve 105** yeni **oyun startup**'ı kurulmuş ve yatırımcıların gözü Türk oyun sektörüne dönmüştür. **Startups Watch** tarafından yayınlanan 27 Haziran 2023 tarihli **Gaming Snapshot For Türkiye v2.1** raporuna göre; 2020 - 2022 yılları arasında toplam **97 oyun girişimi 647.2 milyon $** yatırım almıştır. Yine aynı dönemde, toplam 16 oyun girişimi exit yaparak 2,142 milyon dolar exit büyüklüğüne ulaşmıştır. Bu rakamlara Peak Games'in büyük başarısı da dahildir. (Startups Watch, 2023).



Newzoo tarafından **2019** yılında, pandemiden önce yayınlanan **"Global Games Market"** raporunda, 2020 yılında küresel oyun sektörünün yaklaşık **165 milyar dolara** ulaşılacağı tahmin edilmekteydi. Aynı şirketin 2020 yılında yayınladığı rapora göre ise yaklaşık **175 milyar dolar** olacağı gösterilmişti. Ancak pandemi ile beraber başlayan ivmelenmeden dolayı 2020 yılında küresel oyun sektörü, yaklaşık **180 milyar dolara** ulaşmıştır. (Newzoo, 2019) (Newzoo, 2020).





Global oyun sektöründeki bu büyümeden Türkiye oyun sektörü de payını almıştır. **Gaming in Turkey'**in yayınladığı **"Türkiye Oyun Sektörü Raporu 2021"**e göre Türkiye, dünya gelir sıralamasında 18. sıraya yükseldi. (Gaming in Turkey, 2022). Dolayısıyla sektörde iş olanakları da arttı. Çoğunlukla hyper casual türünde oyun yapan stüdyolar kuruldu. Bu girişimcileri destekleyen hızlandırma ve kuluçka merkezleri sayısı hızla arttı. 2022 yılına gelindiğinde oyun girişimlerini destekleyen toplam **25 adet hızlandırma, ön kuluçka ve kuluçka merkezi** kurulmuştu. (Aksakal, 2022). Benzer şekilde, üniversitelerde **oyun tasarımı lisans ve yüksek lisans programı** sayısı da arttı. Aynı zamanda seçmeli ders olarak bazı üniversitelerde Oyun Tasarımı listelendi.

Farklı sektörlerden pek çok kişi oyun sektörüne geçmenin yollarını aradı. Kimisi kendi girişimini kurdu kimisi ilanlara başvurdu. Türkiye oyun sektörünün yıldızının parladığı bu dönemde sayısız eleman alındı. Hatta sadece oyun sektörüne yönelik bir HR platformu bile kuruldu; **Zindhu**.

2016-17 gibi biraz daha erken bir döneme baktığımızda; iş ilanlarında "Oyun Tasarımcısı" rolüne rastlamak oldukça zordu. Sadece büyük şehirlerde ve belli stüdyolarda bu ilan bulunmaktaydı. Peak Games ile başlayan dalga, pandeminin yarattığı ivme ile birleşince artık her oyun stüdyosunda bu role rastlanır oldu. Dolayısıyla ilanlar da arttı. Bu dönemde, özellikle hyper casual oyun yapan ekiplerin çokluğu sebebiyle Oyun Tasarımcısı rolü, çoğunlukla Bölüm Tasarımcısı rolü ile eşdeğer görüldü. Sektör büyümeye devam edip oyun türleri arttıkça **hyper casual** türü de **hibrit casual'**a evrilmeye başladı. Mobil oyun skalasında, hibrit casual'dan sonra casual ve midcore oyunlar gelmektedir. Casual ve core türünde oyun geliştiren ekiplerde ise **Oyun Tasarımcısı (Game Designer)** rolü yerine **Ürün Yöneticisi (Product Manager)** veya **Ürün Uzmanı (Product Specialist)** rolleri tercih edildi. Günümüzde, Ürün Yöneticisi arayan bir oyun şirketinin istediği özelliklere baktığımızda, çoğunlukla Oyun Tasarımcısı ile benzeştiğini görebiliriz.

Ads Heavy

DLC Heavy

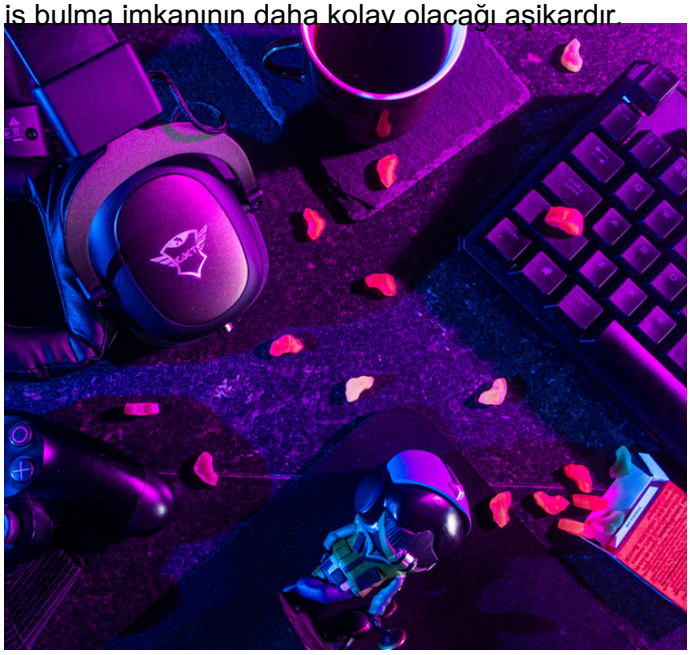
2023 yılına gelindiğinde; pandeminin etkisinin azalması, dünyanın bazı bölgelerindeki savaşlar, siyasi krizler ve ekonomik çöküş ile beraber maalesef oyun sektöründe bu hızlı ilerleyiş sona ermiş, altın çağ kapanmıştır. Bazı raporlarda, ilk kez pandemi sonrası dönemde küçülme görülmüştür. Tüm bunlara ek olarak, Türk lirasının Amerikan doları karşısında ciddi değer kaybetmesi sonucu Türkiye, küresel oyun sektörü sıralamasında 18'den 30'lara kadar gerilemiştir. (Gaming in Turkey, 2023).

İçinde bulunduğumuz yıl, hyper casual özelinde de önemli bir düşüş görüldü. Bilinen büyük hyper casual yayıncılar, bazı stüdyolar ile anlaşmalarını kesmeye başladı. Trend, hypercasual'dan hibrit casual ve casual türüne kaydı. Yayıncılar artık bu genre'larda oyun yayınlamaya başladı. Hyper casual'ın düşüşü ülkemizde işsizliği de beraberinde getirdi. Pek çok hypercasual stüdyo kapandı ve iş ilanları azaldı. Kendini sadece hypercasual özelinde geliştirmiş olan oyun tasarımcıları da dolayısıyla iş bulmakta zorlandı. Şu anda trend daha çok indie oyunlara yoğunlaşmış durumda.

Indie game, "independent" kelimesinin kısaltmasından gelmektedir ve **"bağımsız oyun"** demektir. Bu kategorideki oyunlarda sanatsal yapımlar daha çok görülür. Oyunları veya ekipleri "bağımsız" yapan pek çok faktör vardır. En temel faktörlerden biri, küçük bütçeli olmalarıdır. Yani indie ekipler, elindeki sınırlı olanaklarla (para, iş gücü) oyun geliştirmeye çalışır. Pek çok şeyi yolda öğrenirler, girişimci ruhludurlar. Para kazanmak en önemli öncelikleri değildir. Kendini ifade etmek, derdini anlatmak, bir konuya dikkat çekmek gibi amaçları daha ön plandadır. Bu nedenle daha yenilikçi oyunlar ortaya çıkarabilirler, denenmemişi deneme cesaretleri vardır.

Son birkaç yıldır indie oyunlardaki gelişmeyi gerek oyun görselleriyle gerek oyun tasarımıyla görebiliyoruz. Önümüzdeki dönemde de indie oyunlardaki bu gelişim devam ederken bu türde oyun geliştirmeye olan ilginin artacağını da söylemek yanlış olmayacaktır. Daha önce hyper casual veya hibrit casual mobil oyun geliştiren sayısız ekip, evrilerek indie oyun üretimine geçiş yapıyor. Bu oyun türü gereği, oyun tasarımcılarının rolü de artıyor. **Bölüm Tasarımcısı (Level Designer), Ekonomi Tasarımcısı (Economy Designer), Dövüş Tasarımcısı (Combat Designer)** gibi oyun tasarımının farklı alt rollerinde iş olanakları gelişiyor.

Önümüzdeki birkaç yıl, mobil oyun sektöründe casual ve midcore türünde oyunların yükselişi beklenirken PC ve konsol tarafında da indie oyunların gelişmesi beklenmektedir. Kendini tek bir alanda değil, farklı yönlerde geliştiren oyun tasarımcıları, oyun sanatçıları ve oyun geliştiricilerin iş bulma imkanının daha kolay olacağı aşikardır.



Referanslar

[1] Startups Watch. (2023, June 27). Gaming Snapshot For Türkiye v2.1. Startups Watch. Retrived from : https://startups-watch-production.s3-eu-central-1.amazonaws.com/uploads/documents/3485/_Gaming_Snapshot_v2.1.png?X-Amz-Expires=3600&X-Amz-Date=20230703T081706Z&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIJVM3YYYR2ZQJJSQ/20230703/eu-central-1/s3/aws4_request&X-Amz-SignedHeaders=host&X-Amz-Signature=1a9a261f72d069433bf81b3ee0c2e132bd5799d53a2aff5b3ae0e9268f0ac4cb

[2] Newzoo. (2019, June 19). Newzoo Global Games Market Report 2019. Newzoo. Retrieved from https://newzoo.com/resources/trend-reports/newzoo-global-games-market-report-2019-light-version

[3] Newzoo. (2020, June 25). Newzoo Global Games Market Report 2020. Newzoo. Retrieved from https://newzoo.com/resources/trend-reports/newzoo-global-games-market-report-2020-light-version

[4] Gaming in Turkey. (2022). Türkiye Oyun Sektörü Raporu 2021. Gaming in Turkey. Retrieved from https://www.turkiyeoyunsektoruraporu.com/tr/2021-1

[5] Aksakal, S. (2022, July 4). Oyun Girişimcilik Merkezleri 2022. Medium. Retrieved from https://medium.com/@PsychicSenem/oyun-giri%C5%9Fimcilik-merkezleri-2022-6b0f2302c94b

[6] Gaming in Turkey. (2023). Türkiye Oyun Sektörü Raporu 2022. Gaming in Turkey. Retrieved from https://www.turkiyeoyunsektoruraporu.com/tr/2022-1

Elektronik İmza Kavramı Ve Elektronik İmzanın Önemi

Av. Tuğçe Çalışoğlu

Yazının icadı ile birlikte insanoğlunun kayıt tutma, hukuk kuralları düzenleme, hesaplama ve sözleşme yapma gibi konularda becerileri artmıştır. Teknolojik gelişmeler bir yandan olumlu sonuçlar doğururken bir yandan da toplumda yeni suç tiplerinin ortaya çıkmasına sebep olmuştur.

Dünyada bulunan kısıtlı kaynakların paylaşılması sırasında insanlar birbirleri ile yaptıkları anlaşmalarda uyuşmazlık yaşamıştır. Medeniyetin ortaya çıkmasıyla beraber bu uyuşmazlıkların çözümü için de çeşitli kurumlar ortaya çıkmıştır. Günümüzde uygar devletlerde uyuşmazlıkların çoğunluğu, tarafsız ve bağımsız mahkemeler aracılığıyla çözülmektedir. Hukukun temel ilkelerine uygun bir yargılama yapılması için iyi hazırlanmış usul ve maddi hukuk kurallarına ihtiyaç vardır. İyi hazırlanmış usul ve hukuk kurallarına göre çözülecek uyuşmazlıklarda delil ve ispat kavramları oldukça önemlidir.

İnsanoğlu, ilk yazılı metinleri kaşe veya mühür gibi yapıların yardımıyla işaretlemiştir. Bu işaretlemelerin birtakım amaçları vardır. En temel sebeplerinden bazıları kısıtlı kaynakların paylaşımında güvenli ticaret ortamının yaratılması, belgeyi işaretleyen kişinin kimliğinin tespit edilmesini sağlayarak güvenli bilgi aktarımının sağlanması ve yaşanacak birtakım sorunların çözümünde ispat aracı olarak bu yazılı metinlerin kullanılmasını sağlamaktır. Ancak bu mühür gibi işaretlerin kopyalarının oluşturulması kolay olduğundan zamanla kopyalanması daha zor birtakım özelliklere sahip olan el yazısı ile atılan imzalar ortaya çıkmıştır.[1]

Teknolojik gelişmelerin zamanla artması ile imza klasik anlamda yazılı belgelerden veri dünyasına taşınmış bunun sonucunda ortaya elektronik imzalar çıkmıştır. İnternet üzerinden yapılan iletişimin artması ile internet ortamında da geleneksel imza ile sağlanan işlemlerin ve hukuki korumanın elektronik ortamda da mümkün kılınması gerekmiştir. Bu sebeple de elektronik imza kavramı hukuki düzenlenmelere muhtaç hale gelmiştir.[2] Bu sebeple hem ispat hukukunda kullanılması mümkün hem de güvenli ticaretin sağlanması ve insanların mağduriyetlerinin azaltılması için yeni çözüm yöntemleri aranmış ve aranmaya devam etmektedir.

Dünyada elektronik imza ile ilgili ilk düzenlemeler 1978 yılında başlamıştır. Düzenlemelere yönelik uluslararası çalışmalar hala sürmekle birlikte 13 Aralık 1999 tarihli Avrupa Parlamentosu ve Konseyi Elektronik İmza Direktifi bunlardan en önemlisidir. 14 Haziran 1996 yılında Birleşmiş Milletler tarafından Elektronik Ticarete İlişkin bir Model Kanun'un hazırlanması ile 1999 tarihli direktif ile birlikte ülkelerin mevzuatlarında birtakım değişiklikler yapılmıştır. Birçok Avrupa ülkesinde yapılan bu mevzuat değişikliklerine ülkemiz de uyum sağlamıştır.[3]

Ülkemizde Adalet Bakanlığı tarafından yürütülen çalışmalar neticesinde 23 Ocak 2004 tarihinde 5070 sayılı Elektronik İmza Kanunu yasalaşmıştır. Bu kanun genel hatları ile Avrupa Birliği'nin 99/93-EC sayılı direktifi ile uyumludur.[4] Elektronik İmza Kanunu'nun hazırlanmasında 2001 yılında yürürlüğe giren Alman Elektronik İmza Kanunu'ndan da yararlanılmıştır.[5]

Elektronik İmza Kanunu, Türkiye'de elektronik imzanın kullanımını ve hukuki geçerliliğini düzenleyen temel yasadır. Kanun; elektronik imzanın tanımını, kabul edilebilirliğini, kullanım şartlarını ve sertifika sağlayıcılarının rolünü belirlemektedir. Ülkemizde elektronik imza kavramı ile ilgili düzenlemelere ilk olarak Elektronik İmza Kanunu'nda yer verilmiş olsa da bu konu ile ilgili birçok kanuna eklemeler yapılmış ve gerekli yönetmelikler ile tebliğler çıkarılmıştır.

Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik ile yapılan düzenleme neticesinde Elektronik İmza Kanunu'nun daha ayrıntılı bir şekilde uygulamaya yönelik yönergeleri düzenlenmiştir. Bu yönetmelik; elektronik imzanın teknik standartlarını, sertifikaların düzenlenmesini ve kullanımını, yetkilendirme süreçlerini ve sertifika sağlayıcılarının yükümlülüklerini düzenlemektedir. Yine bu kapsamda Elektronik İmza ile ilgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ ve akabinde Sertifika Mali Sorumluluk Sigortası Yönetmeliği de yürürlüğe girmiştir.

Elektronik imzanın kullanımın yaygın olduğu alanlardan biri e-ticarettir. Bu sebeple Elektronik Ticaretin Düzenlenmesi Hakkında Kanun çıkarılmıştır. Kanun ile Türkiye'de elektronik ticaretin düzenlenmesini amaçlamaktadır. Bu kanun, elektronik imzanın elektronik ticaret işlemlerinde kullanımını ve elektronik ticaretin hukuki geçerliliğini de kapsamaktadır.

Kişisel Verilerin Korunması Kanunu, kişisel verilerin korunması ve işlenmesiyle ilgili genel bir çerçeve sunmaktadır. Bu kanunda da elektronik imza ile ilgili düzenlemeler yer almaktadır. Özellikle elektronik imza kullanımıyla ilgili olarak, kişisel verilerin elektronik imza sürecinde nasıl korunması gerektiği ve kişisel verilerin elektronik imza verileriyle ilişkilendirilmesi konusunda KVKK hükümleri dikkate alınmalıdır.

Elektronik imza kullanımının birtakım suçların işlenmesini kolaylaştıracağı, yeni bazı suç tiplerini de ortaya çıkaracağı açıktır. Suçta ve cezalarda kanunilik ilkesi gereğince Türk Ceza Kanunu'nda yer alan bazı maddeler elektronik imza ile ilgili suçlarda da uygulama alanı bulacaktır.

Elektronik imzanın hayatımıza girmesi ile birlikte hem maddi hem de usul hukuku kurallarında yenilikler de ortaya çıkmıştır. Bu yenilikler için Türk Borçlar Kanunu ile Hukuk Muhakemeleri Kanunu'na eklemeler de yapılmıştır. Teknolojideki son gelişmelerle birlikte Türk vergi hukukunda da "elektronik defter", "elektronik belge" ve "elektronik kayıt" gibi kavramlara yer verilmesi ile elektronik imza kullanımı daha da artmıştır. Bu bağlamda Vergi Usul Kanun'a da eklemeler yapılmıştır.[6]

Elektronik imzaya ilişkin düzenlemeleri anlayabilmemiz için imza kavramını da yakından incelememiz gerekmektedir. İmza kavramı, TDK'da bir kimsenin herhangi bir belgeyi yazdığını veya onayladığını belirtmek için her zaman aynı biçimde kullandığı işaret olarak tanımlanmıştır.[7] Klasik imza olarak bilinen kavram ise bir belgenin altına kişinin, isim ve soy ismini yazmasıdır. Hukuken bir belgenin doğruluğu ancak o belgeyi düzenleyen kişilerin, o belgeyi doğrulaması ile mümkündür. İmza, genel olarak kişiler tarafından bir belgeyi doğrulama amacı ile kullanılmaktadır.

İmza güven aracıdır. İmzanın bu sebeple birtakım özellikleri olmalıdır. Bir imza kopyalanamamalı, imzalanan belge inkâr edilememeli, imzalanan belge değiştirilememelidir.[8]

Teknolojinin hızla gelişmesi ile önce bilgisayarlar ardından da internet adı verilen bir ağ sistemi icat edilmiştir. Bu ağ sistemi ve bilgisayarların sistemleri sayısal verilerden oluşmaktadır. Elektronik imza kavramı için elektronik ortamda yer alan verilerin de anlaşılması gerekmektedir. Veri kavramı; TDK'da olgu, kavram veya komutların, iletişim, yorum ve işlem için elverişli biçimli gösterimi olarak tanımlanmıştır.[9] Burada veri kavramına daha yakından bakacak olursak KVKK'da kişisel veri kavramı da yer almıştır. Bu kanuna göre kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir. Veri kavramına ilişkin bir başka düzenleme ise Elektronik İmza Kanunu'nda yapılmış ve elektronik veri kavramı tanımlanmıştır. Buna göre elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtları ifade etmektedir.

Basit işlemlerden kullanıcıların tepki verebildiği Web 3.0'a evrilen internet teknolojisi ile internet sistemi üzerinden haberleşmek ve sözleşme yapmak isteyen kişiler için verilerden oluşan elektronik imza kavramı ortaya çıkmıştır. Elektronik imza, elektronik ortamda bilginin orijinalliğinin bozulmasını engelleyen ve belgeyi imzalayan tarafların kimliğini doğrulayarak karşı tarafa aktarılmasını garanti eden harf ve sembollerden oluşmuş bir veri setidir.[10] Elektronik imzanın kullanılması için birtakım teknik altyapıya ihtiyacı vardır. Kişi, elektronik veriler üzerindeki bilgilerini, teknik altyapı sayesinde istediği gibi şifreleyebilmekte ve mesajını güvenli bir şekilde karşı tarafa aktarabilmektedir. Doktrinde biyometrik imzadan dijital imzaya, güvenli elektronik imzadan mobil elektronik imzaya kadar birçok elektronik imza yöntemi, elektronik imza olarak nitelendirilmektedir[11].

Dijital imza ya da diğer bir adıyla sayısal imza, belirli yöntemlerle sayısal veriye dönüştürülmüş imzayı ifade etmektedir. Elektronik imza ise elle atılan imza yerine elektronik ortamda üretilen ve elektronik sistemlerde kullanılan bütün teknolojik yöntemleri ifade eden çok daha geniş bir imza türünü ifade etmektedir[12]. Dijital imza, bir verinin asimetrik olarak şifrelenmesi ve sonrasında bu şifrenin çözümlenmesi ile çalışan kriptografik bir veri teknolojisidir.[13] Elektronik imza genel olarak bir tür sayısal şifreleme sistemi aracılığıyla belgeyi imzalamaktayken kişinin el ile attığı imza belgede kullanılmamaktadır[14]

İmzanın temelde iki temel işlevi vardır: imzayı atan kişinin kimliğinin belirlenmesini sağlamak ve imzalanan metnin imza sahibinin iradesine uygun olduğunu ortaya koymaktır.[15] Elektronik imzanın ise birden fazla işlevi bulunmaktadır. Bunlar EİK'da belirtildiği haliyle kimlik doğrulama, inkâr edilemezlik, veri bütünlüğü ve gizliliktir. Kimlik doğrulama kavramı kişinin kimliğinin belirlenmesini ifade etmektedir. Elektronik imzalarda kullanılan sertifikalarda genellikle işlemi yapan kişinin bilgileri görülebilmektedir. Bu sertifikalara dijital sertifika denilmektedir.[16] Kişi elektronik imzası ile imzaladığı bir belgeyi inkâr edememekte, elektronik ortam buna izin vermemektedir. Bu da kişilerin elektronik imza ile imzaladıkları belgelerden hukuki anlamda sorumlu olmaları anlamına gelmektedir[17].

Elektronik imzanın işlevlerinden bir diğeri ise verinin bütünlüğüdür. Mesajı ileten kişinin gönderdiği mesajın hiçbir değişikliğe uğramadan iletildiği anlamına gelmektedir. Mesaj, karşı tarafa değiştirilerek ulaşırsa belgedeki elektronik imza geçerliliğini yitirmektedir[18].

Bazen bir bilginin veya verinin sadece bazı kişiler arasında gizli kalması gerekmektedir. Verilerle haberleşmede mesajların başkaları tarafından görülmesi istenmemektedir. Veriler sayesinde mesaj şifrelenmekte ve mesaj bu sayede gizli kalmaktadır. Elektronik imza ile imzalanan evrak dijital ortamda mühürlenebildiğinden bu imzalama işlemini yapan kişi tarafından ulaşması istenen kişiler belirlenebilmekte ve bu sayede gizlilik sağlanabilmektedir[19].

Elektronik imzanın türleri de bulunmaktadır. Avrupa Direktifi'nde elektronik imzanın üç türünden söz edilmiştir. Bu türlerden ilki basit anlamda elektronik imzadır. E-postanın sonuna kişinin adını ve soyadı yazarak imzalanması ya da banka kartlarını kullanırken girilen PIN numarası gibi imzalar basit anlamda elektronik imzaya örnek gösterilebilecektir[20].

İkinci tür elektronik imza ise gelişmiş elektronik imzadır. Bu tip elektronik imzalar; kullanan imza sahibine özgülenmiş, imza sahibinin özelliklerini belirten, imza sahibinin yetkisi ve kontrolüyle oluşturulmuş, elektronik verilerde yapılacak herhangi bir değişikliği tespit edecek şekilde kullanılan elektronik imza türüdür. Gelişmiş elektronik imza, temel olarak PKI (Açık Anahtar Altyapısı) tabanlı elektronik imzalardır[21].

Üçüncü tür elektronik imza ise, Avrupa Direktifinin beşinci maddesi birinci fıkrasına göre nitelikli bir sertifikaya sahip ve güvenli elektronik imza oluşturma koşullarında sayılan teknik sistem ve donanım ile oluşturulan imzadır. Avrupa Direktifi'nde tanımlanmamış olan bu imza, doktrinde "nitelikli elektronik imza" ismi ile tanımlanmaktadır[22].

Elektronik imza türlerinden biri olan güvenli (nitelikli) imza; güvenli olması, imzalayan kişinin kimlik tespitini sağlaması, aksi ispatlanmadıkça doğru olması sebepleriyle yargılama hukuku açısından ispat değeri olan el yazısı ile atılan imzaya denk görülmüş bununla birlikte birçok ülke tarafından hukuki anlamda delil olarak değerlendirilen bir imza türüdür[23]. Elektronik İmza Kanunu'nda, elektronik imza ve elektronik imza türü olan güvenli elektronik imza kavramları ayrı ayrı tanımlanarak yer almıştır.

Elektronik imza türleri içinde kanunun düzenlemesine göre güvenilir ve hukuki anlamda kabul edilen tür güvenli elektronik imzadır[24].

Güvenli elektronik imzanın unsurları Elektronik İmza Kanunu'n 4. maddesinde sayılmış ve kanunda güvenli elektronik imzanın tanımı yapılmıştır. EİK md. 4'e göre *"güvenli elektronik imza, münhasıran imza sahibine bağlı olan, sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan, nitelikli elektronik sertifikaya dayanarak imza sahibinin tespitini sağlayan, imzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan elektronik imzadır"*[25]. Bu maddeye göre güvenli elektronik imzanın taşıması gereken özellikler vardır. Buna göre;

a) Münhasıran imza sahibine bağlı olan,
b) Sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan,
c) Nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan,
d) İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan,
elektronik imza ancak ve ancak güvenli elektronik imzadır[26].

Güvenli elektronik imzanın mutlaka böyle bir yazılım ve donanımla oluşturulması gerekmektedir. Münhasıran imza sahibine bağlı olmaktan anlaşılması gereken güvenli elektronik imzanın şifresinin olması sebebiyle imza sahibi dışında başkalarının deşifre etme ihtimali olmadığından başkalarınca bu belgelere ulaşamaması kastedilmektedir. EİK md. 6'da güvenli elektronik imza oluşturulma aracı; başka benzeri olmayan, imza sahibine münhasır, başkaca kişilerin eline geçmesine imkân vermeyen bir elektronik imza oluşturulmasını sağlayan yazılım veya donanım olarak belirtilmiştir. Güvenli elektronik imzanın mutlaka böyle bir yazılım ve donanımla oluşturulması gerekmektedir[27].

Bir elektronik sertifika, elektronik imzayı şifrelemek amacıyla kullanılan anahtarların sahibini belirten elektronik kayıtlardır. Elektronik sertifika, elektronik sertifika hizmet sağlayıcısı kurum tarafından belirli bir şekilde hazırlanıp elektronik imza sahibine verilir. Bir elektronik sertifikanın nitelikli olabilmesi için birtakım unsurlara sahip olması gerekmektedir. Bu unsurlar ilgili kanunun dokuzuncu maddesinde ayrıntılı olarak gösterilmiştir. Bu unsurlar özet olarak şu şekilde sayılabilir: sertifika sahibinin kişisel ve mesleki bilgilerinin sertifikada yer alması, sertifikanın bir numarasının ve geçerlilik süresinin olması, imza sahibine sertifikayla getirilen kısıtlamalarına ilişkin bilgilerin sertifikada yer almasıdır. Nitelikli elektronik sertifika bu gibi unsurları sayesinde güvenli elektronik imza sahibinin kim olduğunu tespit etmeye imkân sağlaması gerekmektedir[28].

Güvenli elektronik imzada güvenliği sağlayan asıl unsur ise elektronik veride bir değişiklik yapılıp yapılmadığının tespitini sağlamasıdır. Buna göre güvenli elektronik imza ile imzalanmış elektronik veride sonradan bir değişiklik yapılıp yapılmadığının tespit edilebilmelidir[29].

Hukuki anlamda irade beyanı karşı tarafa yazılı, sözlü, resmi yollarla sunulabileceği gibi iradeyi gösteren bir tavır ve birtakım koşullara göre bir davranış biçimi olarak değerlendirilebilecek susma eylemi şeklinde de sunulabilir. Bir irade beyanının elektronik ortamda açıklanması, elektronik olmayan bir ortamda açıklanması ile aynı hukuki sonuçları ortaya çıkaracağı doktrin ve uygulamada kabul edilmektedir. İrade beyanları, elektronik olmayan ortamda da çevrimiçi bir ortamda da yapılabilmektedir.

Taraflar arasında bir telefon görüşmesiyle, e-posta aracılığıyla ya da en basit haliyle internet ortamında bulunan bir formun doldurulmasıyla da irade beyanı açıklanabilecektir. Bu durumun bir sonucu olarak hukukumuzda geçerli olan şekil serbestisi kuralı, kural olarak elektronik ortamda yapılan irade beyanları ve sözleşmeler için de geçerlidir[30].

EİK'da güvenli elektronik imzaya hukuki bir anlam verilmiştir. EİK'da"Güvenli Elektronik İmza, elle atılan imza ile aynı hukukî sonucu doğurur" denilmiştir.

Bu düzenlemenin sonucunda güvenli elektronik imza, elle atılan imzanın işlevini sağlamakta ve ispat hukuku açısından elle atılan imza ile aynı sonuçları doğurmaktadır. İlgili kanun maddesi sayesinde, hem hukukumuzda yazılı şekil öngörülen sözleşmelerin elektronik ortamda da yapılabilmesi hem de güvenli elektronik imza ile imzalanmış elektronik belgelerin birtakım düzenlemeler sonucunda ispat hukuku açısından senet niteliği kazanması mümkün olmuştur.

Borçlar Kanunumuzda yapılan değişiklikle kanunun 15. maddesinde güvenli elektronik imzanın, elle atılmış imzanın bütün hukuki sonuçlarını doğuracağı hususu düzenlenmiştir.[31] TBK md.14'te ise *''Kanunda aksi öngörülmedikçe, imzalı bir mektup, asılları borç altına girenlerce imzalanmış telgraf, teyit edilmiş olmaları kaydıyla faks veya buna benzer iletişim araçları ya da güvenli elektronik imza ile gönderilip saklanabilen metinler de yazılı şekil yerine geçer.''* şeklinde düzenlemeler yapılmıştır.

Güvenli elektronik imzayla ilgili kanunlarımızda yapılan düzenlemeler ile elle atılan imzanın hukuki sonuçlarını doğurmakta bu sebeple de yargılama hukukumuzda da birtakım değişikliklerin yapılması gerekmiştir. Hukuk Muhakemeleri Kanun'unun 205/2'de maddesine yapılan ekleme ile güvenli elektronik imza ile usulüne göre bir elektronik veri oluşturulan verilerin senet hükmünde olduğu düzenlenmiştir.

Elektronik İmza Kanunu'nda güvenli elektronik imzanın, elle atılan imzayla aynı hukuki sonucu doğurması yönündeki hükmüne bazı istisnalar getirilmiştir. Bu istisnalardan biri EİK md. 5'te yer alan *"Kanunların resmî şekle veya özel bir merasime tabi tuttuğu hukukî işlemler ile teminat sözleşmeleri güvenli elektronik imza ile gerçekleştirilemez "* hükmüdür. Bu düzenleme ile bazı işlem ve sözleşmelerin güvenli elektronik imza ile gerçekleştirilmesine engel olunmuştur.

Güvenli elektronik imza, elle atılan imza ile aynı hukuki sonuçları doğurduğundan hukukumuzda yazılı şekle bağlı sözleşmelerde kullanılabilecektir.

Ancak resmi şekle bağlı sözleşmelerin kurulmasında ve birtakım özel merasimler öngörülmüş hukuki işlemlerde kullanılması hukukumuzda henüz mümkün değildir[32].

Bunlardan biri yazılı şekle tabi olan kefalet sözleşmesidir. Güvenli elektronik imza ile yapılan işlemler oldukça hızlı gerçekleşmektedir. Hukukumuzda bazı işler için özel merasimler öngörülmüş ve bu işlemlerin aceleye getirilmesi engellenmeye çalışılmıştır. Hukukumuzda özel merasimlerle hızlı gerçekleşmesi engellenmeye çalışılan birtakım işlemler, kanunun ilgili maddesinin kapsamı dışında bırakılarak oluşabilecek zararlar önlenmeye çalışılmıştır. Yine noterlerin yapmakta olduğu bazı işlemler, tapudaki bazı işlemler, evlenme gibi özel merasime tabi işlemlerin güvenli elektronik imza ile yapılması mümkün değildir. Dolayısıyla kanunların resmi şekil öngördüğü veya özel merasime tabi tuttuğu hukuksal işlemlerin güvenli elektronik imza ile imzalanması durumunda işlem geçersiz olacaktır[33].

Elektronik imzalar, günümüzde dijital dünyada hukuki belgelerin güvenli bir şekilde işlem görmesini sağlayan ve oldukça sık kullanılan bir araca dönüşmüştür. Elektronik imzaların güvenliği de bu sebeple çok büyük önem arz etmektedir. Elektronik imzanın güvenliği; elektronik imza teknolojisinin yazılım veya donanımı, elektronik imzanın sertifikası ve güvenlik standartları ile sağlanmaktadır. Elektronik imza ile imzalama işlemi; imzalayanın kimliğini doğrulama, imzalanan verinin bütünlüğünün sağlanması ve gizlilik gibi birtakım unsurları içermektedir.

Elektronik imzaların hukuki sonuçları da dikkate değerdir. Elektronik imza, hukuki belgelerin dijital ortamda kullanımını mümkün kılmaktadır. Bir sözleşme veya bir taahhüt belgesi gibi hukuki belgeler elektronik imza kullanılarak düzenlenebilir ve bu belgelerin kabul edilebilirliği sağlanabilmektedir. Ayrıca, elektronik imza ile imzalanan belgeler mahkemelerde delil olarak kabul edilebilmekte ve hukuki işlemlerde geçerliliği olan bir kanıt niteliği taşımaktadır.

Elektronik imzanın her geçen gün artan ve birçok sektörde uygulamaları mevcuttur. Finans sektöründe elektronik imza kullanımı yaygındır. Elektronik sözleşmelerin imzalanması, birtakım bankacılık işlemlerinin yapılması ve elektronik ticaret gibi alanlarda elektronik imza kullanımı fayda sağlamaktadır. Hukuki işlemlerin yapıldığı birçok alanda da elektronik imza kullanımı, zaman ve masraflarda tasarrufu sağlayacaktır.

Teknolojik gelişmeler giderek artmakta ve güvenli elektronik imza kullanımı ile uygulamada ortaya çıkan sorunlar birçok bilimsel çalışma yapılmasına sebep olmaktadır. Uygulamada yaşanan sorunlar elektronik imzanın yargı kararlarında da kendine yer bulmasına neden olmaktadır. Elektronik imzalarla ilgili yargı kararlarının artmasının sonucu olarak bu konuda hem birtakım hukuki düzenlemelerin yapılmasına olanak sağlayacak hem de yapılan bilimsel çalışmalar da uygulamanın ışığında artabilecektir. Güvenli elektronik imza sahibi kişilerin; hak ve yükümlülükleri konusunda var olan durumun tespiti, imza sahiplerinin ve sertifika sağlayıcıların bu konuya dikkatlerinin çekilmesi gerekliliği böyle bir çalışma yapılma ihtiyacını hissettirmiştir.

Gelecekte elektronik imzanın daha yaygın olarak kullanılması ve hukuki işlemlerde daha geniş bir kabul görmesi beklenmektedir. Bu sebeple de özellikle elektronik imza ile ilgili suçların kapsamının belirlenmesinde yeni hukuki düzenlemelere de ihtiyaç olduğu açıktır. Ceza kanunundaki boşluklarla birlikte uygulamada birtakım sorunların yaşanması oldukça mümkündür.

REFERANSLAR

[1] Leyla Keser Berber, İnternet Üzerinden Yapılan İşlemlerde Elektronik Para ve Dijital İmza, 1. Baskı, Yetkin Yayınları, Ankara, 2002, s.119
[2] Gürsel Orer, Elektronik İmza ve Elektronik Sertifika Hizmet Sağlayıcısının Hukuki ve Cezai Sorumluluğu, 1. Baskı, Adalet Yayınevi, 2011 Ankara, s.31
[3] Orer, s.35
[4] Orer, s.35
[5]İnci Biçkin, "Elektronik İmza ve Elektronik İmza İle İlgili Yasal Düzenlemeler", TBB Dergisi, S:63, Ankara, 2006, s.119
[6] Biçkin, s.118
[7] https://sozluk.gov.tr/, e.t.: 05/07/2023
[8] Gökhan İskender, "Analysıs Of Electronıc Sıgnature In Turkey From The Legal and Economıc Perspectıves and The Awareness Level In The Country'', Yayımlanmamış Yüksek Lisans Tezi, Orta Doğu Teknik Üniversitesi Bilişim Sistemleri Bölümü, Ankara 2016, s.2
[9] https://sozluk.gov.tr/, e.t.: 05/07/2023
[10] Fatih Önder, "Borçlar Hukuku Açısından Elektronik İmza'', Yayımlanmamış Yüksek Lisans Tezi, Kırıkkale Üniversitesi Sosyal Bilimler Enstitüsü, Kırıkkale 2007, s.61, s.32
[11] Ayşe Gürbüz, "Elektronik İmza'', Yayımlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara 2005, s. 52
[12] Gürbüz, s.55
[13] Gürbüz, s.55
[14] Mehmet Emin Özgül, "Güvenli Elektronik İmza Sahibinin Hakları Ve Yükümlülükleri", İnönü Üniversitesi Hukuk Fakültesi Dergisi, Mart 2021, Cilt: 12 - Sayı: 2, s.541
[15] Pınar Çağlayan Aksoy, Akıllı Sözleşmelerin Kuruluş ve Geçerlilik Şartları, 2. Baskı, On İki Levha Yayıncılık, İstanbul 2021, s. 182
[16] Cemallettin Danacı, ''Elektronik İmzanın Hukuki Niteliği ve Vergi Hukukunda Kullanılmasının Değerlendirilmesi'', Yayımlanmamış Yüksek Lisans Tezi, Balıkesir Üniversitesi Sosyal Bilimler Enstitüsü, Balıkesir 2016, s.13
[17] Biçkin, s.113
[18] Danacı, s.15
[19] Danacı, s.15
[20] Mustafa Yılmaz, "Elektronik İmzalı Belgelerin Karşılaştırmalı Hukukta Ve İdarî Yargılama Hukukunda Delil Niteliği", Cevdet Yavuz'a Armağan Özel Hukuk Sempozyumu, 3-4 Haziran 2011, s.3439
[21] Yılmaz, s.3439
[22] Yılmaz, s.3439
[23] Önder, s.39-40
[24] Özgül, s.541
[25] Önder, s.39
[26] Yılmaz, s. 3443
[27] Mustafa Topaloğlu, " Elektronik İmza", https://www.mtopaloglu.av.tr/img/makaleler/elektronik-imza 441.pdf ,Erişim Tarihi: 07/06/2023, s.6
[28] Topaloğlu, s.6
[29] Topaloğlu, s.6
[30] Önder, s. 5-6
[31] Önder, s.42
[32] Özgül, s. 544
[33] Önder, s.65

KAYNAKÇA

1. Gürsel Orer, Elektronik İmza ve Elektronik Sertifika Hizmet Sağlayıcısının Hukuki ve Cezai Sorumluluğu, 1. Baskı, Adalet Yayınevi, Ankara, 2011.

2. Leyla Keser Berber, İnternet Üzerinden Yapılan İşlemlerde Elektronik Para ve Dijital İmza, 1. Baskı, Yetkin Yayınları, Ankara, 2002.

3. Pınar Çağlayan Aksoy, Akıllı Sözleşmelerin Kuruluş ve Geçerlilik Şartları, 2. Baskı, On İki Levha Yayıncılık, İstanbul, 2021.

4. İnci Biçkin, "Elektronik İmza ve Elektronik İmza İle İlgili Yasal Düzenlemeler", TBB Dergisi, S:63, Ankara, 2006.

5. Mehmet Emin Özgül, "Güvenli Elektronik İmza Sahibinin Hakları Ve Yükümlülükleri", İnönü Üniversitesi Hukuk Fakültesi Dergisi, Mart 2021, Cilt: 12 - Sayı: 2.

6. Mustafa Yılmaz, "Elektronik İmzalı Belgelerin Karşılaştırmalı Hukukta Ve İdarî Yargılama Hukukunda Delil Niteliği", Cevdet Yavuz'a Armağan Özel Hukuk Sempozyumu, 3-4 Haziran 2011.

7. Ayşe Gürbüz, "Elektronik İmza'', Yayımlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2005.

8. Cemallettin Danacı, ''Elektronik İmzanın Hukuki Niteliği ve Vergi Hukukunda Kullanılmasının Değerlendirilmesi'', Yayımlanmamış Yüksek Lisans Tezi, Balıkesir Üniversitesi Sosyal Bilimler Enstitüsü, Balıkesir, 2016.

9. Fatih Önder, "Borçlar Hukuku Açısından Elektronik İmza'', Yayımlanmamış Yüksek Lisans Tezi, Kırıkkale Üniversitesi Sosyal Bilimler Enstitüsü, Kırıkkale, 2007.

10. Gökhan İskender, "Analysıs Of Electronıc Sıgnature In Turkey From The Legal and Economıc Perspectıves and The Awareness Level In The Country'', Yayımlanmamış Yüksek Lisans Tezi, Orta Doğu Teknik Üniversitesi Bilişim Sistemleri Bölümü, Ankara, 2016.

11. Mustafa Topaloğlu,"Elektronik İmza", https://www.mtopaloglu.av.tr/img/makaleler/elektronik-imza-441.pdf, Erişim Tarihi: 07/06/2023. https://sozluk.gov.tr/, e.t.: 05/07/2023.

Fantazi Haritacılığı

Mürşit Özoğlu

Giriş

Fantezi haritacılığı, tipik olarak fantezi literatüründe ve rol yapma oyunlarında bulunan kurgusal dünyalar için haritalar yaratma sanatıdır.

Fantezi Haritacılığı Neden Önemlidir?

Fantezi haritacılığı, yazarların ve oyun tasarımcılarının hayali dünyalarını görselleştirmelerine fırsat vererek, okuyucularına ve oyuncularına, daldıkları dünyayı daha iyi anlamaları için bir referans sağlar.

Fantezi haritacılığı ayrıca dünya inşa etme sürecine bir düzeyde ayrıntı ve özgünlük ekler. İlham getirir ve hayal edilen dünyayı hayata geçirmeye yardımcı olur.

Konunun önemini Tolkien (Yüzüklerin Efendisi'nin yazarı) şu sözüyle dile getirmiştir: ***"Akıllıca davranarak bir harita ile başladım ve hikayeyi buna uydurdum."***

(Orj: "I wisely started with a map and made the story fit". 25 Nisan 1954, Naomi Mitchison'a mektup.)

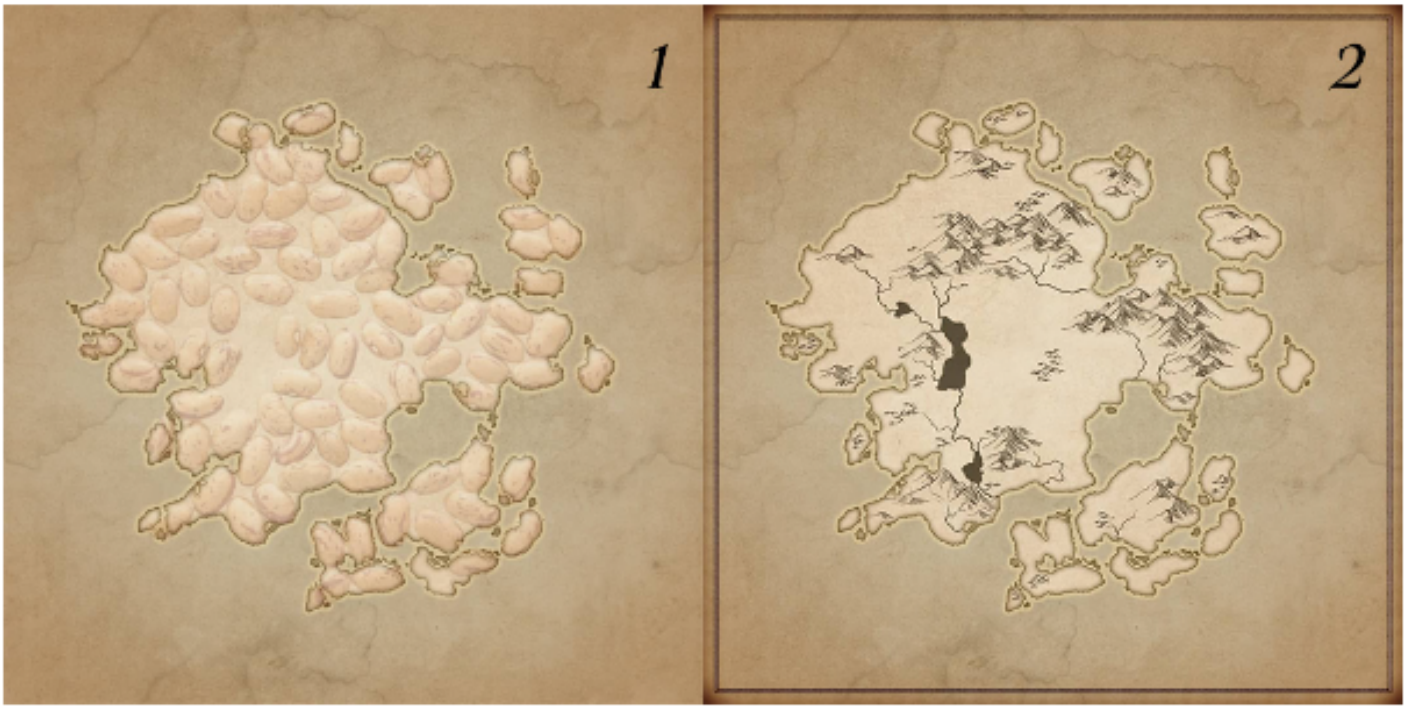
Fantezi Haritacılığı Süreci?

Her yiğidin bir yoğurt yiyişi vardır derler. Haritalama süreci için de geçerlidir bu söz. Tabletle mi çalışıyorsunuz, kağıt kalemle mi? Bu bile gidişatı değiştirir.

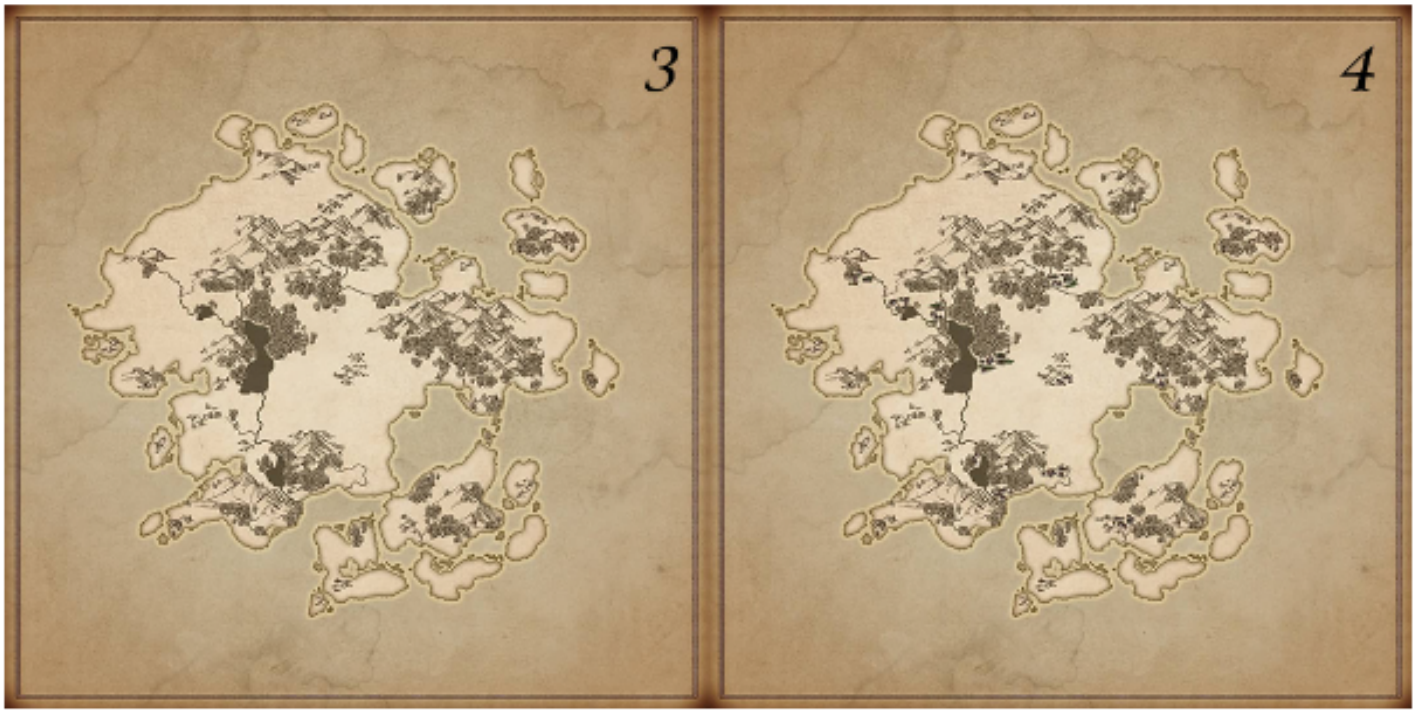
Haritalama yaparken birçok kez önceki aşamalara dönerek revize yapmanız da gerekebilir.

Ancak ana haliye birçok haritacı şuna benzer bir yol izler:

- Coğrafya ile başlanır: Kara ve denizler, dağlar, nehirler ve ormanlar gibi başlıca coğrafi özellikler de dahil olmak üzere haritanın coğrafyası belirlenir.



- Ardından beşeri unsurlar veya siyasi sınırlar eklenir: Haritanız, (gösterilecekse) ülkeler, eyaletler veya krallıklar gibi yapılara bölünür. Şehirler ve diğer görülecek yapılar eklenir.



- Gözden kaçmış olabilecek önemli ve ilginç kurgu detayları tespit edilip gerekli düzenlemeler yapılır. Haritalama sırasında gelen ilham ile hikaye gözden geçirilerek akla gelen yeni fikirler haritaya ve kurguya eklenir.

- Son olarak metinler, çerçeve ve pusula gibi kalan harita unsurları yerleştirilir.

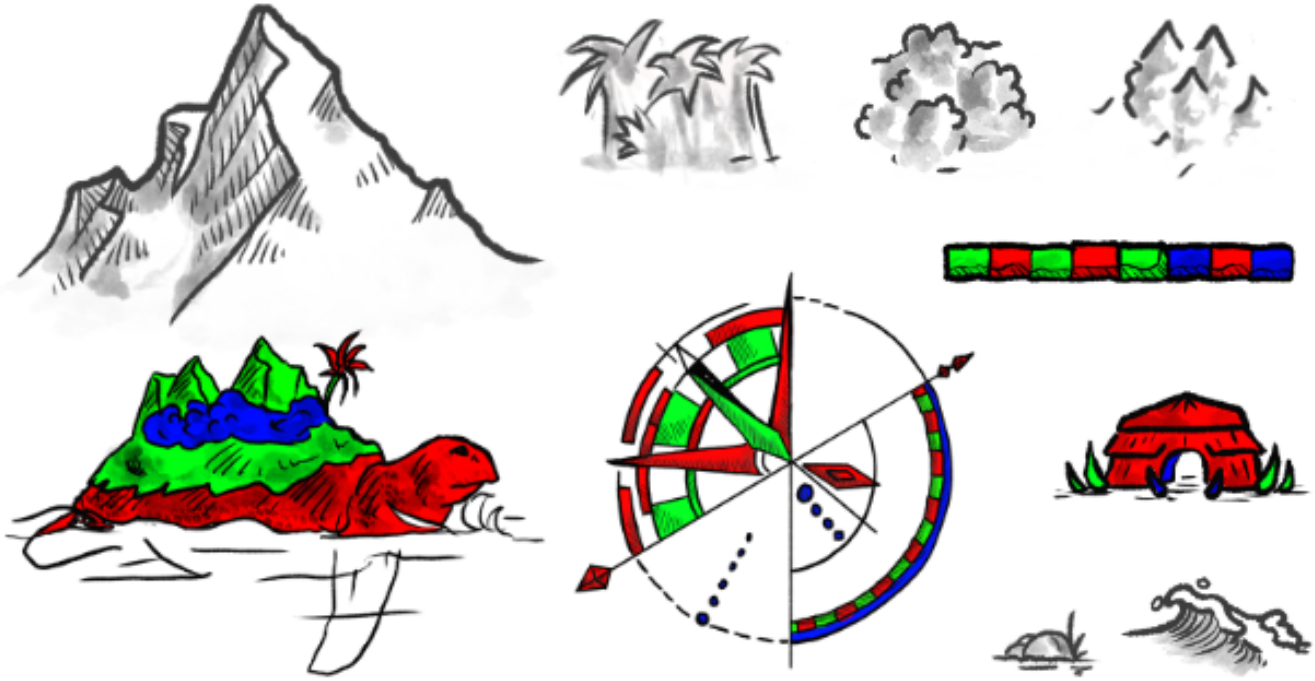
Boyama sonradan da eklenebilir, ilk baştan coğrafi unsurları planlama süreci için bir araç olarak da kullanılabilir.

"Haritacılığa ilk başladığım dönemin en sevdiğim haritası, düzenlemiş olduğum ilk #mappingtogether etkinliği için hazırlamıştım. Etkinlikte eğlenmek için fasulye kullanarak karaları belirlemiştik."

Fantezi Haritacılığı Araçları

- ***Geleneksel çizim:*** Bir fantezi haritası oluşturmak için geleneksel kalem, kağıt, pergel vb araçlarla çizim.
- ***Dijital çizim:*** Procreate, Krita ve Adobe Illustrator gibi çeşitli dijital programları üzerinde, çizim tableti ve kalemi kullanarak çizim.
- ***Asset ile tasarım:*** Wonderdraft ve Inkarnate gibi özel harita oluşturma programları veya tasarım programları üzerinde, önceden çizilmiş assetleri bir araya getirip boyayarak tasarlama.

Geleneksel çizim ve dijital çizimin ne olduğu aşikar olsa da asset kullanma mantığının kavranabilmesi için aşağıya asset örnekleri ve bu assetlerle yapılan küçük bir harita eklenmiştir.



Fantezi Haritacıların Genel Mücadeleleri

Ayrıntı ve basitliği dengeleme: Haritacılar, okuyucuyu veya oyuncuyu çok fazla bilgiyle bunaltmadan dünyayı hayata geçirmek ile yeterli ayrıntıyı sağlamak arasında bir denge bulmalıdır.

Tutarlılığı sürdürme: Dünya ve hikayesi geliştikçe, haritanın bu değişiklikleri tutarlı bir şekilde yansıtmasını sağlamak haritacı için önemlidir.

Doğru stili bulma: Harita için doğru stili ve estetiği bulmak zor olabilir ve genellikle deneme ve revizyon gerektirir.

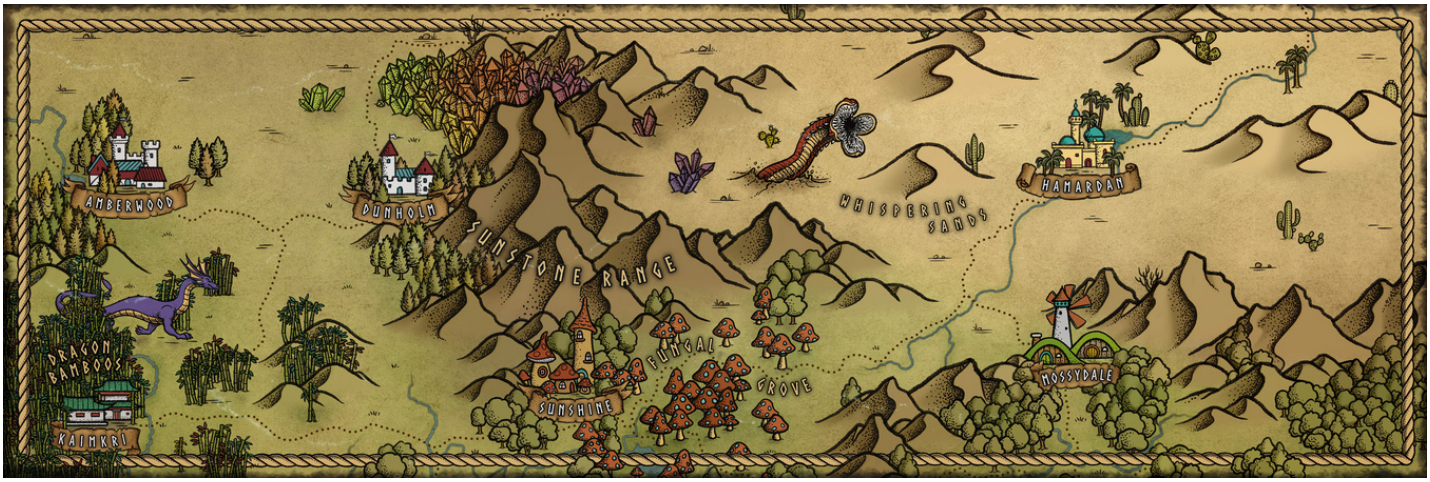
Harita çizilerek yapılıyorsa, farklı çizim teknikleri ve materyalleri kıyaslanmalıdır.

Örneğin “Game of Thrones” gibi yetişkinlere hitap eden bir yapıt için tasarlanan haritada old-school tarzda, tükenmez kalem ve suluboya ile çalışılarak antik haritalara benzer bir stil oluşturulabilirken, “Ejderhanı Nasıl Eğitirsin” gibi hedef kitlesi çocuklar olan bir yapıtta, basit ve canlı bir stil oluşturmak gerekir.
Harita assetlerle yapılıyorsa, doğru stilin oluşturulabileceği bir asset koleksiyonu kullanmak gerekir.

Ayrıca haritalama süreci esnasında, asset koleksiyonunda olmayan ancak haritaya eklenmesi gereken içerikler (assetler) tespit edildiği taktirde, bu koleksiyona uyacak şekilde yeni assetlerin üretilmesi gerekir.

Harita: Yazdığı kurgu kıyamet sonrasında geçen bir müşterim için 2021 yılında hazırlamış olduğum haritadan bir kesit.

Sonuç



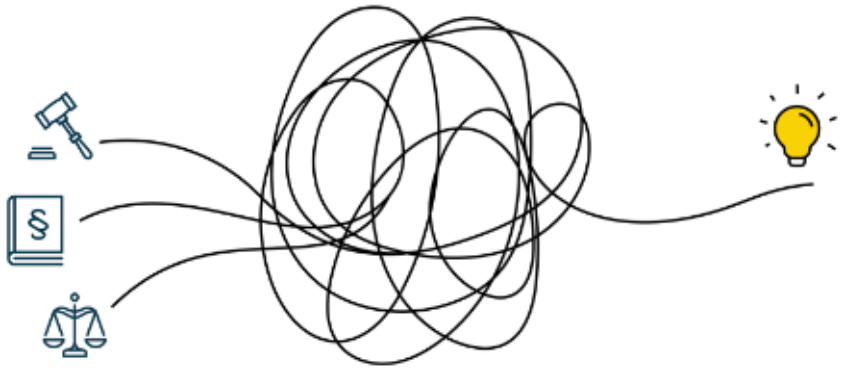
Fantezi haritacılığı, hayali dünyanın görsel bir temsilini sağlayan dünya inşa etmenin ve hikaye anlatımının önemli bir yönüdür.

Coğrafya ve fantezi haritacılığı metodlarına hakimiyet, yaratıcılık, detaylara dikkat ve hem sanatsal hem kurgu ile tutarlılık taahhüdü gerektirir.

Fantastik haritalar, gerek eğitim gerek eğlence yönünden her türlü tüketimin görsel ve işitsel materyaller ile hızlandırıldığı çağımızda, kurgulanan dünyaların ve hikayelerin somutlaştırılarak sunulmasında büyük rolü olması sebebiyle, yazarlar ve oyun yapımcıları için vazgeçilmez bir araçtır.

Legal Design Hakkında

Av. M. Turan Özer- Adana Barosu



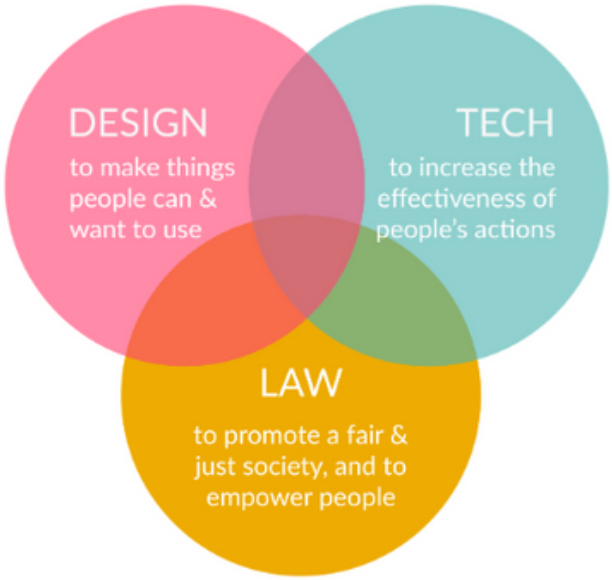
Legal Design Hakkında -1-

Bir araştırma yaparken felsefeci John Dewey'[1]e ait olan biz söze rastladım söz aynen "Bugünün çocuklarını dünün yöntemleri ile eğitirsek yarınlarından çalarız[2]" şeklinde idi. Dewey' i merak ettim ve araştırdım ki ne göreyim. Meğer, Dewey, Cumhuriyetin ilk yıllarında Atatürk'ün daveti ile Türkiye'ye gelmiş tanımamız gereken bir usta imiş. Bu ustanın Söylediği söz ise beni çok etkiledi. Bu tanımı ilk duyduğum andan itibaren de hukuk eğitimine nasıl uyarlarız diye düşündüm ve neler yapılmış diye tarama yaptım. Bu başlığıma aldığım kavram ile tanıştım, bu kavram " Legal Desing" idi.

Türkçeye uyarlanışı "Hukuk tasarımı" demekti ancak çok daha fazlası şey ifade ediyordu. Hukukçuların eğitiminin son noktadaki amacının hukukçu olduğu söyleyene hukuk nosyonu kazandırmaktır. Hukuk nosyonu ise en genel tanım ile "Hukuk Nosyonu, hukukun evrensel ilke ve esaslarından hiçbirini ihmal etmeksizin, bilimsel disipline ve sistematik düşünce bütünlüğüne dayanarak hedeflenen adaleti temine yarayan düşünme biçimidir.[3] O halde hukuk eğitiminin yarınlara göre yapılması zorunluluktur. Dewey, çok haklı onun söylediği sözü haklı çıkarırcasına geleceğe bakmak ve eğitimlerin geleceğe tasarlanması ve uygulanmalıdır. Hele konu adalet ve hukuk olunca daha da önemsenmesi gerekecektir.

Bu düşünce ile Legal Desing konusunda okumalar yaptım okudukça gördükçe ufkum açıldı. Her şeyi anlamasam da her ortamda bu kavramdan söz etmeye başladım, amacım hukukçuların bu kavramı merak etmeleri, öğrenmeleri, çevrelerine tanıtmaları ve kavramın gündemde tutulmasını sağlamaktı.

Adana Barosu bilişim komisyonu benden bir şeyler yazmamı isteyince de bu konuyu yazmak istedim. Legal Desing'i öğretmek değil gündemde tutmak her şeyden önemli. Bu konuyu seri bir yazı haline getirmek istiyorum. Sizlerden gelecek geri bildirimlere göre şekillendirmek, genişletmek ve geliştirmek istiyorum.



Dilerim beni yalnız bırakmazsınız.

1] Jhon Dewey, ABD'li felsefeci John Dewey, 1924 yılında Mustafa Kemal Atatürk'ün daveti üzerine Türkiye'ye gelerek Türk eğitim sistemi üzerinde incelemeler yaptıktan sonra kapsamlı bir rapor hazırlamıştır.
https://www.turkyurdu.com.tr/yazar-yazi.php?id=2277
[2] http://www.ortaweb.bilkent.edu.tr/formlar/mypnm.pdf
[3] https://hukukbook.com/hukuk-nosyonu/

İSTİNYE ÜNİVERSİTESİ
İKTİSADİ,İDARİ VE SOSYAL BİLİMLER FAKÜLTESİ
YÖNETİM BİLİŞİM SİSTEMLERİ BÖLÜMÜ

TOPLUMSAL FAYDA İÇİN YAPAY ZEKA KULÜBÜ

Yapay Zeka nedir?	Fatih Kaan Çamyurdu
Yapay Zeka Tarihi?	Emre Süme
Yapay Zeka uygulama Alanları ?	Havva Demirbaş
Yapay Zeka Etiği?	Efe Yeniyol
Toplumun Yapay Zekaya Bakışı ?	Umut Gönder
Yapay Zekanın iş yelpazesi	Rümeysa Kandemir
Yapay zeka ve iş istihdamı	Rümeysa Kandemir
Bir Çağın Başlangıcı Chat Gpt	Havva Demirbaş
Yapay Zekanın geleceği	Dilara Cihan
İndex 2023 incelemesi	Furkan Hüseyin Araz

Yapay Zeka

ZEKA VE AKIL - Fatih Kaan Çamyurdu

İnsanoğlunun yaratılıştan bugüne gelen hayatta kalma çabası, doğanın engellerine karşı adapte olmasınısağlar. Beraberinde, karşılaştıkları olaylara tepki vermek zorunda kalmışlardır. Zamanla tecrübelenip olaylara daha farklı açıdan yaklaşmayı öğrenmişlerdir. Böylece insanı diğer canlılardan ayıran en önemli özellik amaca göre hareket edip, yargılayıp bundan sonuç çıkarması olarak adlandırılabilir. İnsan doğası gereği belli birzekaya sahiptir. Geçmişten bugüne bilgi ve birikimler sonucunda karşılaşılan durumlara daha geniş açıdan hızlı ve pratik şekilde çözümlemeye başlamışlardır. Ancak akıl zekaya göre yaşanılan bölge, çevre ve dış etkenlere bağlı değişiklik gösterebilir. Bununla beraber genetik yolla aktarım sağlanır.

Akılsürekli değişen bir yetenektir, bu yüzden yapay birşekilde oluşturulması imkansızdır. Zeka modellemesi oluşturularak gelecek hakkında yorum istenemez ancak var olan bilgileri kullanarak cevaplar verebilir. Örneğin; Bu sene en iyi film ödülünü kim alır? (bu soruya cevap verememesinin nedeni akıl yürütme ve öngörü yeteneğinin olmamasıdır)

Yapay Zeka

Yapay zeka; insanların anlama, yorumlama, karar verebilme , çözüm yolu üretme yeteneğini sanal ortama aktararak işgücünü kolaylaştırma amacıyla ortaya çıkarılmıştır. Bu sayede Şirketler bir problemle karşılaşıldığında veya stratejik kararlarda daha hızlı çözüme ulaşılır. Şirketler, gelecekteki eğilimleri tahmin etmek ve şirketlerin stratejik kararlar almasına yardımcı olmak için yapay zeka, veri madenciliği, makine öğrenimi ve derin öğrenme gibi
yöntemleri kullanarak büyük miktarda veriyi analiz etmek ve bunlardan önemli bilgiler çıkarmak için yapay zeka tekniklerini kullanabilir. Ancak yapay zekanın bir bilinci olmadığı için sadece girilen bilgiler ve bu bilgilerin doğru olması karşılığında çıkarımlar yapabilir.

YAPAY ZEKA TARİHİ- Emre Süme

Yapay zeka, bilgisayar bilimleri ve bilişsel bilimlerin bir dalı olarak uzun bir tarihe sahiptir. Gelişimi, 1956 yılında John McCarthy tarafından düzenlenen Dartmouth Konferansı ile ivme kazandı. Bu konferans, yapay zeka terimini resmi olarak tanımlayarak disiplinin doğmasını sağladı. Konferansa katılan diğer önemli isimler arasında Marvin Minsky, Nathaniel Rochester ve Claude Shannon yer alıyordu.

1950'lerden itibaren yapay zeka araştırmaları hız kazandı ve birçok önemli program geliştirildi. Bu dönemde, Eliza gibi programlarla doğal dilde etkileşim kurma ve uzman sistemlerle uzmanlık alanlarının taklit edilmesi gibi çalışmalar yapıldı.

1970'lerde, uzman sistemler popüler hale geldi. Uzman sistemler, belirli bir uzmanlık alanında insan uzmanlarından alınan bilgiyi taklit eden bilgisayar programlarıydı. Tıp, mühendislik, finans gibi alanlarda kullanıldılar. Bu dönemde, dil işleme, bilgi temsili ve arama algoritmaları gibi alanlarda da ilerlemeler kaydedildi. 1980'lerde, yapay sinir ağları ve uzman sistemlerin birleşimi olan "bağlantılı sistemler" önem kazandı. Ayrıca, doğal dil işleme, görüntü işleme ve robotik gibi alanlarda da gelişmeler yaşandı.

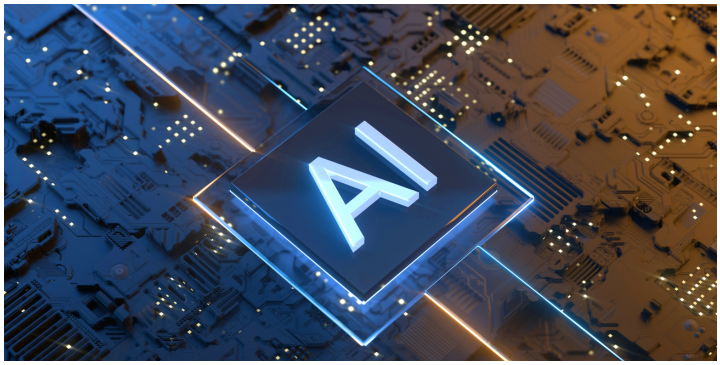
1990'lar, yapay zeka alanında makine öğrenmesinin yaygınlaşmaya başladığı bir dönemdi. İstatistiksel yöntemler ve makine öğrenmesi teknikleri kullanılarak çeşitli problemlerin çözümüne odaklanıldı. Bu dönemde, yapay zeka araştırmaları daha da yoğunlaştı ve endüstriyel uygulamalarda kullanımı arttı. 2000'ler ve sonrasında ise büyük veri, derin öğrenme ve yapay sinir ağları gibi teknolojilerin gelişimiyle yapay zeka alanında büyük bir dönüşüm yaşandı. Derin öğrenme, karmaşık veri setlerinden otomatik olarak öğrenme yeteneği sağlayan yapay sinir ağları ile ilgili bir yaklaşımdır. Görüntü ve ses tanıma, doğal dil işleme, oyun oynama ve otonom araçlar gibi birçok alanda büyük ilerlemeler kaydedildi.

YAPAY ZEKANIN UYGULAMA ALANLARI- Havva Demirbaş

Yapay zeka, günümüzün en heyecan veren ve ilgi çeken teknolojik alanlarından birisidir. Bilgisayarların insan benzeri zeka ve yetenekler kazanmasını sağlayan bu alan, birçok sektörde devrim niteliğinde değişiklikler sağlamaktadır. Bunlara birçok örnek verilebilir:

1. Görüntü ve Ses İşleme: Yapay zeka, görüntü ve ses verilerini analiz ederek birçok uygulamada kullanılabilir. Örneğin, yüz tanıma, nesne algılama, otonom araçların çevreyi algılaması, konuşma tanıma, konuşmayı metne dönüştürme (transkript), sesli asistanlar gibi alanlarda kullanılır.

2. Doğal Dil İşleme ve Dil Çevirisi: Yapay zekanın kullanım amaçlarından birisi de insan dilini anlamak ve işlemektir. Doğal dil işleme yöntemlerini kullanarak insan diline dair daha etkili işler yapabilmek, kolay anlaşılabilmeyi sağlamak için dil çevirisi sağlamak gibi alanlarda da yapay zeka, çeşitli yöntemlerle birlikte kullanılır.



3. Öneri Sistemleri: Öneri sistemleri geliştirme alanında yapay zekanın kullanılması da özellikle müşteri odaklı şirketler için oldukça büyük bir önem arz etmektedir. Müşterilerin ya da bireylerin geçmiş davranışları incelenerek ileriye dönük olarak çeşitli tavsiyelerde bulunulabilir ve bu bakımdan hayatın kolaylaşmasına katkı sağlanabilir. Örneğin; dizi/film tavsiyeleri, haber içeriklerinin kişiye özel oluşturulması, kişinin alışveriş sepetine uygun ürünlerin önerilmesi gibi kullanımları mevcuttur.

4. Otomasyon ve Robotik: Özellikle son zamanlarda robotlar sayesinde otomatikleştirilen işler çoğalmaktadır ve yapay zeka, süreçlerin oluşturulması, yönetilmesi, otomatikleştirilmesinde başlıca rol almaktadır. Otomasyon ve robotik alanlarında yaşanmakta olan faaliyetler ise sektörlerde değişim ve dönüşümler yaratmaktadır ancak elbette ki bu değişim ve dönüşümlerin temelinde harcanan enerjiyi azaltmak, kaynakları verimli kullanmak ve daha etkili işler çıkarmak gibi pozitif sonuçlar amaçlanmaktadır.

5. Sağlık Hizmetleri ve Biyomedikal Uygulamalar: Yapay zeka tıp alanında birçok uygulamada ve çeşitli alanlarda kullanılmaktadır. Bu alanlara örnek olarak hastalıkların teşhisi, tedavilerin planlanması, ilaç keşifleri, analiz, sağlık hizmetleri örnek olarak verilebilir.

6. Finansal Hizmetler ve Risk Analizi: Yapay zeka; finansal piyasaları analiz ederek bu alandaki kullanıcılara hem kişiye özel hem de genel olarak tavsiyelerde bulunabilir, tahminler yapabilir ve çeşitli tespitlerde bulunabilir.

Bu maddeler, yapay zekanın popüler kullanım alanlarından sadece birkaçını içermektedir ve zaman ilerleyip teknolojik gelişmeler çoğaldıkça da bu alanlar genişleyecektir.

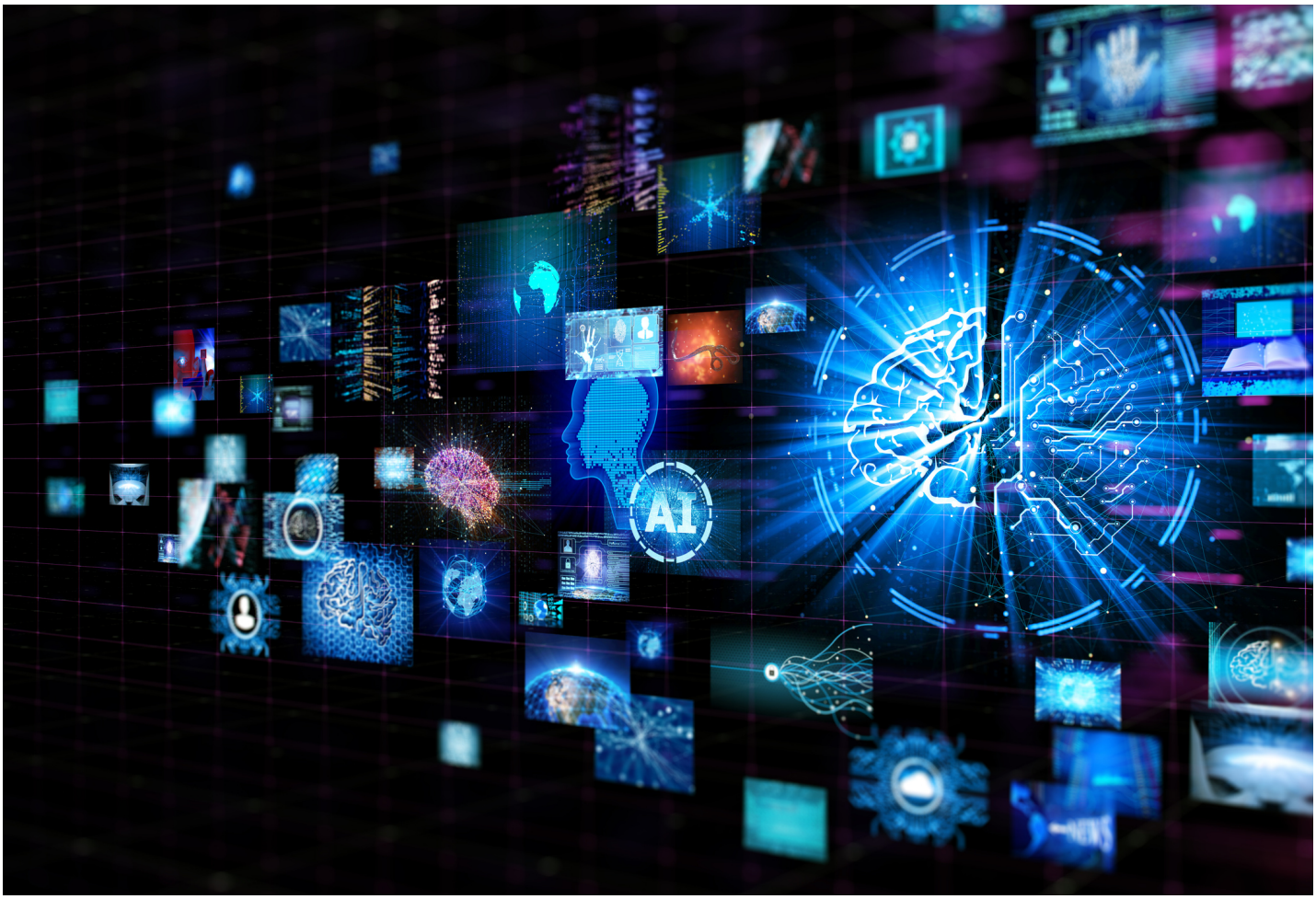
YAPAY ZEKA ETİĞİ- Efe Yeniyol

1.Yapay Zeka Ve Etik

Günümüzde yapay zeka , bilgisayar sistemlerinin insan benzerizeka yeteneklerini taklit etmeyi amaçlayan bir bilim dalı olarak önemli bir yer edinmiştir. Ancak, bu teknolojinin kullanımıyla birlikte ortaya çıkan fırsatlar ve potansiyel riskler, etik boyutunun da göz önünde bulundurulması gerektiğini göstermektedir. Yapay zekanın otomatik kararlar alabilme yeteneği, sorumluluk kavramını da beraberinde getirmektedir. Örneğin, sürücüsüz bir aracın trafikte kararlar alması durumunda, sorumluluk kimde olmalıdır? Bu tür soruların adil ve etik açıdan uygun şekilde yanıtlanması gerekmektedir.Bir diğer önemli etik sorun, yapay zeka ayrımcılığıdır. Yapay zeka sistemleri, karar alma süreçlerindeki önyargıları ve ayrımcılığı yansıtabilmektedir. Bu da toplumsal eşitsizlikleri derinleştirme ve haksızlık yapma potansiyeline sahiptir. Bu nedenle, yapay zekanın geliştirme ve eğitim süreçlerinde önyargı azaltıcı adımlar atılmalı ve çeşitlilik ve kapsayıcılık prensipleri benimsenmelidir.

2. Yapay Zeka Politikaları

Yapay zeka politikaları, etik ilkelerin önemli birşekilde gözetilmesi gereken bir konudur. Yapay zekanın kullanımı, adalet ilkesine dayanmalı ve adil sonuçlar üretmelidir. Bu, ayrımcılığa veya haksızlığa yol açabilecek etiketleme veya sınıflandırmalardan kaçınılması anlamına gelir. Ayrıca, yapay zekanın kararları anlaşılır olmalıdır. İnsanlar, yapay zekanın neden belirli bir karar verdiğini anlama ve açıklama talep etme hakkına sahip olmalıdır. Bu durum, yapay zekanın güvenilirlik ve hesap verebilirlik açısından önemlidir. Bu nedenlerle, yapay zeka politikaları, etik ilkelerin korunmasına odaklanmalıdır. Yapay zeka teknolojisinin geliştirme ve kullanım süreçlerinde, adalet, adillik ve şeffaflık ilkeleri ön planda tutulmalıdır. Aynızamanda, toplumsal farkındalık ve katılım da yapay zeka politikalarının önemli bir parçası olmalıdır.



3.Temel Hedef

Yapay zekanın asıl hedefi, toplumsal refahın artırılması için toplumun yararına yönelik bir şekilde kullanılmasıdır. Yapay zeka, toplumun gelişimine katkı sağlayan ürünlerin ortaya çıkmasına ve geliştirilmesine yardımcı olmak amacıyla çalışır. Bununla birlikte, yapay zeka aynı zamanda insanların iş yükünü azaltarak küresel refah seviyesinde bir artış sağlama potansiyeline sahiptir. Bu nedenle, yapay zekanın öncelikli yönelimi herzaman toplumun ihtiyaçları ve gelişimi olmalıdır. Bu temel amacın korunması, yapay zeka politikalarının oluşturulmasında büyük bir rol oynamaktadır ve yapay zeka politika yapıcıları bu sorumluluğu üstlenmelidir. etik bilincin artırılması için birlikte çalışmalıdır. Bu şekilde yapay zeka , dijital dünyanın şekillendirilmesinde önemli bir rol oynayacak ve insan değerlerini koruyarak ilerlememizi sağlayacaktır.

4.Yapay Zeka Ve Suçlar

Yapay zekanın hayatımıza girmesiyle birlikte, yapay zeka politikalarına uymayan ve siber suç olarak nitelendirdiğimiz suçlarla karşı karşıya kalmış bulunmaktayız. Hatta bazı sibersuçlar, uluslararası basının da yakından ilgisini çeken olaylar arasında yer almaktadır. Örneğin, Rusya-Ukrayna savaşı esnasında yapay zeka tarafından üretilen deepfake videolar kullanılarak, Ukrayna Cumhurbaşkanı'nın savaştan çekildiği şeklinde yanıltıcı görüntüler yayılmıştır. Bu gibi suçlar, uluslararası ilişkileri ve kamuoyunu etkileyebilecek ciddi sonuçlar doğurabilmektedir. Ancak, bu tür suçların azaltılması ve önlenmesi noktasında büyük bir sorumluluk yapay zeka politikalarını belirleyenlerin omuzlarındadır. Yapay zeka teknolojisinin etik kullanımı ve güvenlik önlemlerinin sağlanması için etkili politikalar ve düzenlemeler oluşturulmalıdır. Yapay zekanın geliştirilmesi ve uygulanmasında sorumluluk taşıyan kuruluşlar, açık ve şeffaf bir şekilde hareket etmeli ve güvenlik, gizlilik ve manipülasyon gibi risklere karşı önlemler almalıdır.Aynızamanda, uluslararası işbirliği de bu alanda büyük önem taşımaktadır. Ülkeler arasında yapılan anlaşmalar ve ortak politikalar, siber suçlarla mücadelede etkili bir araç olabilir. Yapay zeka teknolojisini kullanan ülkeler ve şirketler, uluslararası standartları gözeterek ve işbirliği yaparak suçları tespit etme ve önleme konusunda daha güçlü bir duruş sergileyebilirler. Sonuç olarak, yapay zekanın yaygınlaşmasıyla birlikte ortaya çıkan siber suçlar ciddi bir tehdit oluşturmaktadır. Ancak, bu suçların azaltılması ve önlenmesi noktasında yapay zeka politikalarını belirleyenlerin büyük bir sorumluluğu vardır. Etik kullanım, güvenlik önlemleri, uluslararası işbirliği ve şeffaflık gibi temel prensipler üzerine inşa edilen politikalar, yapay zeka teknolojisinin sorumlu bir şekilde kullanılmasını sağlayabilir ve toplumun güvenini artırabilir.

TOPLUMUN YAPAY ZEKAYA BAKIŞI- Umut Gönder

Toplumun yapay zekaya bakışı, genel olarak farklı görüşler ve tutumlardan oluşan karmaşık bir tabloya sahiptir. Bu bakış, kişisel deneyimlere, kültürel farklara, eğitim seviyesine ve toplumun teknolojiye ve yeniliklere olan genel tutumuna bağlı olarak değişebilir. Bir kesim, yapay zekanın potansiyelini heyecan verici bir şekilde değerlendirir. Onlar yapay zekanın, yaşamı kolaylaştıran ve insanların günlük hayatında önemli bir rol oynayan bir dizi alanda büyük faydalar sağlayabileceğini düşünür. Bunlar arasında sağlık hizmetleri, otomasyon, iletişim, ulaşım, eğitim ve daha birçok sektör yer alır.

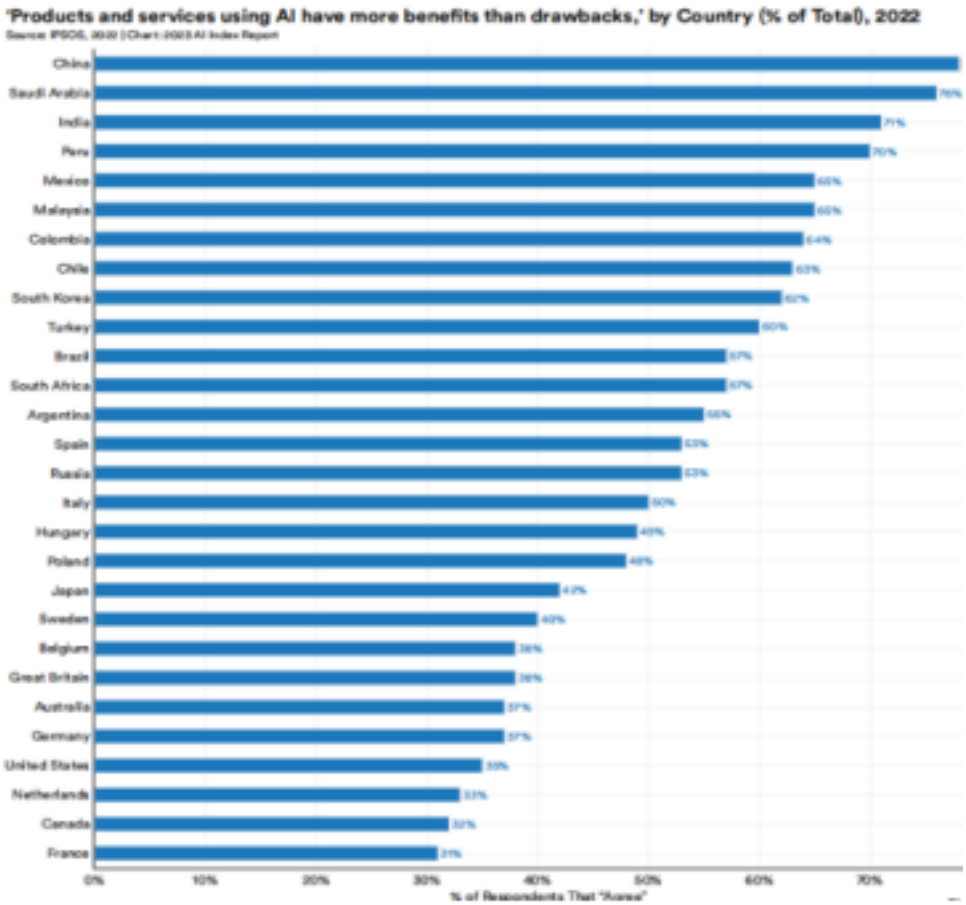
Yapay zeka, işsüreçlerini optimize etmek, verimliliği artırmak ve karmaşık sorunlara çözüm bulmak için büyük potansiyele sahip olarak görülür. Ancak, bazı insanlar yapay zekaya karşı daha temkinli bir yaklaşım sergiler. Onlar yapay zekanın, insanların işlerini kaybetmelerine, özel yaşamlarının gizliliğinin ihlal edilmesine ve insan faktörünün azalmasına yol açabileceğinden endişe duyarlar.

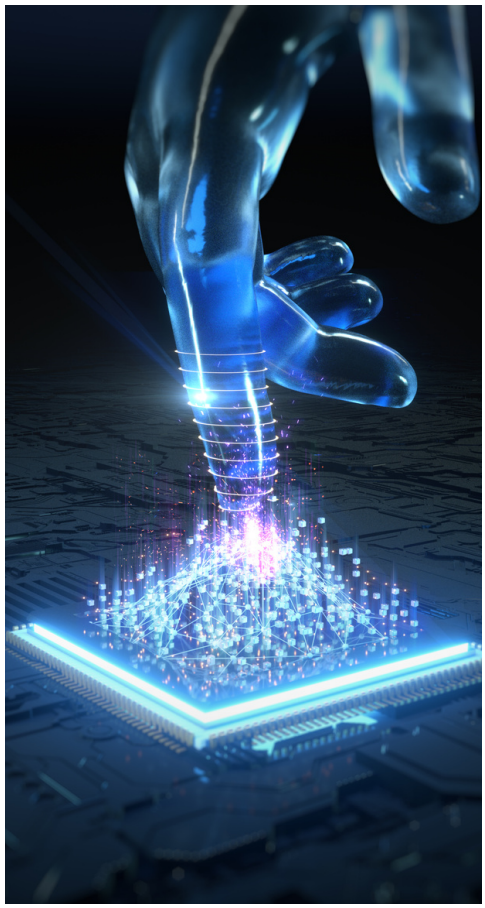
Ayrıca, yapay zekanın yanlış kararlar alabileceği, önyargılı olabileceği ve etik sorunlara neden olabileceği gibi konular da tartışma konusu olur. Toplumda yapay zekaya ilişkin farklı görüşlerin olması doğaldır ve bu görüşler teknolojinin gelişimine ve uygulanmasına şekil vermektedir.

Yapay zeka teknolojilerinin etkileri üzerine toplumsal tartışmalar ve düzenlemeler de yapılırken, genellikle dengeyi sağlama, etik standartları belirleme ve teknolojinin toplumun yararına kullanılmasını sağlama hedeflenir.

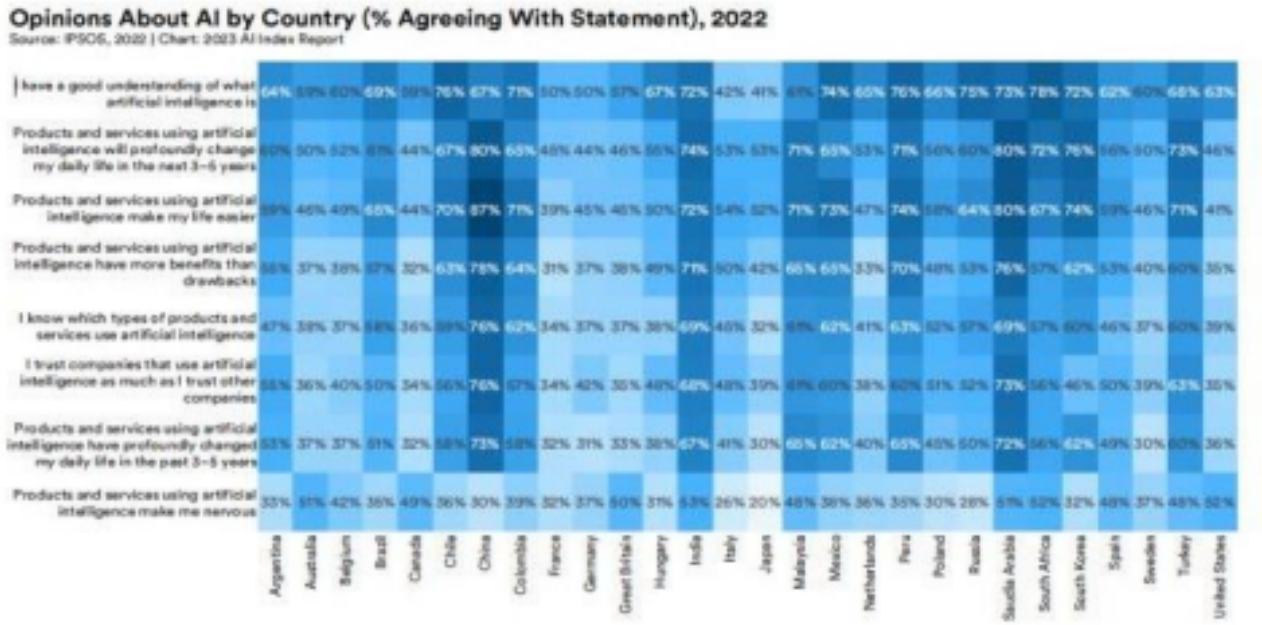
Yapay zekanın göreceli avantaj ve dezavantajları konusundaki görüşler ülkeler arasında büyük farklılıklar göstermektedir. IPSOS anketi, Çinli katılımcıların %78'inin, Suudi Arabistanlı katılımcıların %76'sının ve Hintli katılımcıların %71'inin yapay zeka kullanan ürün ve hizmetlerin dezavantajlardan çok faydası olduğunu düşünüyor. Ancak, Amerikalıların yalnızca %35'i bu düşünceyi paylaşmaktadır. 28 katılımcı arasında ankete katılan ülkeler arasında Fransa ve Kanada en çok olumsuz görüş bildiren ülkelerdir.

Ülkelere göre 'Yapay zeka kullanan ürün ve hizmetlerin dezavantajlarından çok faydaları vardır' (Toplamın %'si), 2022

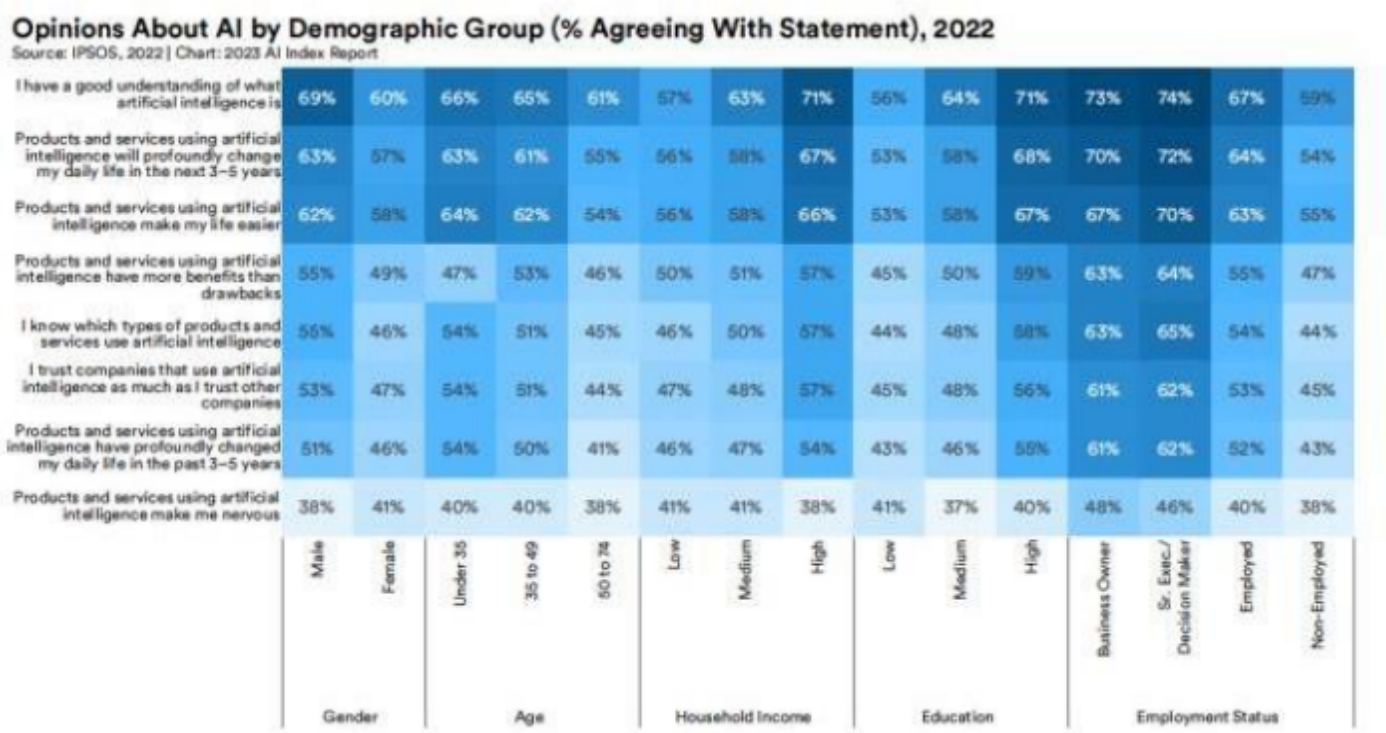




IPSOS'un tüm sorularına verilen cevapların dökümünde, ülkelere göre yapay zeka ürün ve hizmetlerine ilişkin bulgular yer almaktadır. Bu verilere göre, belirli ülkeler arasında yapay zeka ürünleri ile hizmetleri arasında güçlü bir ilişki olduğu görülmektedir. Özellikle, Çin katılımcıları, yapay zeka ürünleri ve hizmetleri konusunda en olumlu hislere sahip oldukları belirlenmiştir. %87'si, yapay zeka ürün ve hizmetlerinin hayatlarını kolaylaştırdığını ifade ederken, %76'sı yapay zeka kullanan şirketlere diğerşirketler kadar güvendiğini belirtmiştir. Ayrıca,sadece %30'u yapay zeka kullanımının kendilerini tedirgin ettiğini belirtmiştir. Buna karşılık, Amerikalı katılımcılar yapay zeka konusunda daha olumsuz bir tutum sergilemektedir. Sadece %41'i yapay zeka ürün ve hizmetlerinin hayatlarını kolaylaştırdığını iddia etmektedir, %35'i yapay zeka kullanan şirketlere diğer şirketler kadar güven duymaktadır ve %52'si yapay zeka ürünleri ve hizmetlerinin kendilerini gergin hissettirdiğini ifade etmektedir.



Demografik gruplar arasında cinsiyet, yaş, hane geliri ve istihdam durumu gibi faktörlere göre ülkelerdeki görüşleri ayrıştırmaktadır. IPSOS'un bulguları, erkeklerin yapay zeka ürün ve hizmetleri konusunda kadınlardan daha olumlu düşündüğünü ortaya koymaktadır. Örneğin, erkeklerin yapay zeka ürün ve hizmetlerinin hayatlarını kolaylaştırdığına dair raporlama olasılığı, kadınlardan daha yüksektir. Yaşa göre görüşler de farklılık göstermektedir. Örneğin, 35 yaş altı bireylerin yapay zeka ürün ve hizmetlerinin hayatlarını kolaylaştırdığına inanma olasılığı daha yüksekken, 35-49 yaş grubundakilerin inanma olasılığı daha düşüktür. Ayrıca, yaşa bağlı olarak yapay zeka ürün ve hizmetlerinin dezavantajlardan daha fazla fayda sağladığı görülmektedir. Son olarak, hane geliri düzeyi düşük olan bireyler, yapay zeka ürün ve hizmetleri konusunda daha olumsuz düşünme eğilimindedir ve bu durum, daha yüksek gelirli hane halklarıyla karşılaştırıldığında ortaya çıkmaktadır



YAPAY ZEKANIN İŞ İSTİHDAMINA ETKİSİ-Rümeysa Kandemir

Günümüzde hızla gelişmekte olan teknolojik gelişmeler ve yeniliklerle beraber istihdam yapısında olumsuz sonuçlar oluşturması endişesi günümüze özgü bir durum değildir. 1930'lu yıllarda Keynes'in teknolojik işsizlik teorisinde ileri sürdüğü teknolojik gelişimin işsizlik kaybına neden olacağı görüşüne kadar uzanmaktadır.

Günümüzde bakıldığında teknolojik gelişmelerin istihdamı iki ana şekilde etkilediği gözlemlenmektedir. Bu iki ana etkiden şu şekilde bahsedilebilmektedir:

1. Yer değiştirme Etkisi: Çalışanların halihazırda yapmış oldukları görevlerinden doğrudan uzaklaştırılması anlamına gelmektedir.

2. Verimlilik Etkisi: teknolojik gelişmelerin beraberinde getirmiş olduğu yenilikler sonucunda ortaya çıkan ya da gelişen endüstrilerde iş gücü talebinin artması şeklinde bahsedilmektedir.

Son iki yüzyılda yılda meydana gelişmeler incelendiğinde otomasyon ve teknolojinin gelişmesine paralele olarak istihdam, nüfus oranı, kadınların iş gücüne katılımlarının artması benzeri olayların artması sonucunda işsizlik oranın uzun vadede bakıldığında dalgalandığı fakat işsizlik oranın artmadığı sonucuna ulaşılmaktadır.

Gelecekteki Otomasyon ve istihdam arasındaki ilişkiye geçmişteki durumda göz önüne alınarak bakıldığında özellikle bilgi işlem gücünün büyük ölçüde gelişim göstermesiyle beraber yapay zekanın ve robotik teknolojinin geçmişte görülmemiş düzeyde emeği değiştirme olasılığına dikkat çekilmektedir. Bu durumda otomasyon kaygısını tekrar insanların önüne çıkarmaktadır. Geçmiş tarihlerden günümüze teknolojinin gelişimine baktığımızda istihdam kavramının tarım ve zanaatkarlık kavramlarından imalata, hizmet ve yönetim mesleklerine büyük ölçüde kaydığı gözlemlenmektedir. Bu gözlem bizlere teknolojik işsizliğin ortaya çıkmadığının bir kanıtı olarak görülebilmektedir.

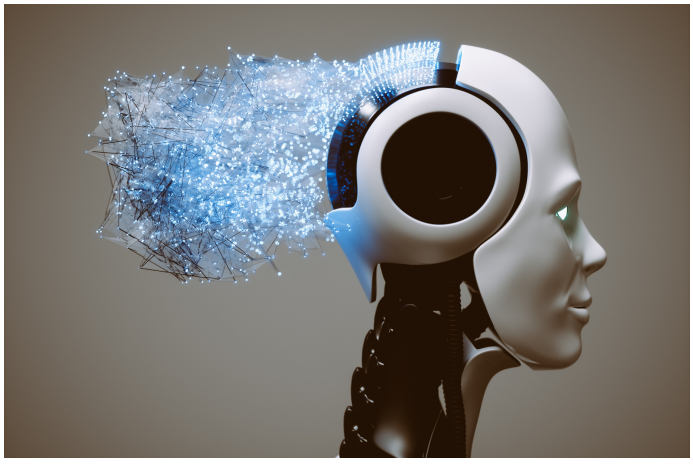
Otomasyonun artması iş gücünde azalma oluşturmanın zıttına geçmiş dönemlere bakıldığında otomasyonlarda meydana gelen gelişmeler sonucunda iş gücü talebinde ve ücretlerde artışa neden olduğu görülmektedir. Tüm bunların sonucunda yapay zeka uygulamalarının işler ve görevler üzerinde hem olumlu yorumlar hem de olumsuz yorumlara ulaşmak mümkündür. Olumlu yorumlar yapay zekanın insan yeteneklerini arttırarak yetenekli çalışanlara talebi yükselteceği yönündedir. Olumsuz yorumlar ise yapay zekanın işçilerin yerini alarak işlerin makineler tarafından deviralınacağı görüşünü savunmaya yöneliktir.

Oxford Üniversitesiakademisyenleri tarafından yapılan bir araştırmaya göre bilgisayarlaşmanın en az etkileyeceği meslek alanları şu şekilde sıralanmıştır :

a. Çevirmenler ve tercümanlar (%5,8)
b. Performanssergileyen sanatçılar(%7)
c. Radyo yayıncıları(%7,7)
d. Film ve TV yapımcıları (%8)
e. Doğa bilimlerinde Ar-Ge (%10,9)

En fazla etkileyeceği meslek alanları ise :

a. Ofis yöneticileri
b. Çağrı merkezi çalışanları
c. Kütüphaneciler
d. Büyükbaşhayvanyetiştiricileri
e. Ağaç kesiciler
f. Madenciler
g. Araba satıcıları ve otel personeli olarak sıralanmıştır (Dirican, 2015:569).



BİR ÇAĞIN BAŞLANGICI: CHATGPT- Havva Demirbaş

ChatGPT, OpenAI tarafından geliştirilen büyük bir dil modelidir ve kısa süre içerisinde tüm dünyanın en popüler, en çok tercih edilen sohbet robotlarından biri haline gelmiştir. GPT-3 dil modeline dayanan ChatGPT, geniş bir metin ve kod veri kümesi üzerinde eğitilerek oluşturulmuştur. Bu veri kümesi; kitaplardan, makalelerden, web sitelerinden ve kod depolarından elde edilen metinleri içerir.

ChatGPT'nin farklı alanlarda ve farklı konularda yapabilecekleri oldukça çeşitlidir. Örneğin; zorlayıcı görünen birtakım soruları anlayarak yanıtlayabilir, şiirler yazabilir, kodları analiz ederek hataları bulabilir ve baştan yazabilir, web sitesi oluşturmak için yönlendirmelerde bulunabilir, senaryo metinleri yazabilir, dil çevirisi yapabilir, istediğiniz amaca yönelik olarak e-posta/dilekçe örneği yazabilir, tarih-felsefe-psikoloji gibi alanlar hakkında konuşabilir, soruları ve yanıtları takip ederek anlamlı şekilde sohbete devam edebilir yani kısacası ufak yönlendirmeler sayesinde birçok alanda faaliyet gösterebilir.

Ayrıca ChatGPT, gerçek hayatta birçok sektörde de aktif olarak kullanılmaya devam etmektedir. Örneğin bir öğrenci tezini ChatGPT yardımıyla yazdırdı, bir hakim karar verirken ChatGPT'den destek aldı, bir adam günlük hayatının yönlendirilmesi için ChatGPT'ye kendi hayatı hakkında detaylıca bilgiler verdi, blog yazarları pek çok farklı konuda bloglar yazdırdı ve bu örnekler giderek artmaya devam etmektedir.

Ancak ChatGPT'nin bazı potansiyel riskleri de bulunmaktadır. Örneğin; yanlış bilgi yaymak veya sahte haber makaleleri oluşturmak, gerçek insanları taklit etmek veya deepfakeler oluşturmak gibi kötü niyetli amaçlarla kullanılabilir.

Elbette ki ChatGPT olgusal bir dil modelidir, yani çoğunlukla gerçek / doğru bilgiler üretme eğilimindedir ve sürekli geliştirilerek yetenekleri de artırılmaktadır ancak yine de ChatGPT'yi sorumlu bir şekilde kullanmak ve potansiyel risklerini göz önünde bulundurmak, ChatGPT'nin etkin kullanımı için oldukça önemli olacaktır.

YAPAY ZEKANIN GELECEĞİ- Dilara Cihan

Yapay zeka, günümüzde büyük bir hızla gelişen ve hayatımızın birçok alanında önemli bir rol oynamaya başlayan bir teknolojidir. Yapay zeka, bilgisayar sistemlerine insan benzeri düşünme ve karar verme yetenekleri kazandırmayı amaçlar. Bu yazıda, yapay zekanın geleceği hakkında bazı önemli noktalara değineceğim.

Yapay zeka, bilgisayar bilimindeki ilerlemelerle birlikte önemli bir evrim geçirmiştir. İlk başlarda, yapay zeka daha çok hesaplama ve veri işlemeyle ilgiliyken, günümüzde derin öğrenme ve makine öğrenimi gibi daha gelişmiş tekniklerle birlikte karmaşık sorunları çözebilme yeteneğine sahip olmuştur. Bu gelişmeler sayesinde yapay zeka, sağlık, otomotiv, finans, hizmet sektörü ve daha birçok alanda kullanılmaya başlanmıştır.

Gelecekte yapay zeka teknolojisinin hızla ilerlemesi ve yaygınlaşması beklenmektedir. Bunun birkaç nedeni vardır. İlk olarak, bilgisayar donanımındaki hızlı gelişmeler ve yüksek performanslı işlemcilerin ortaya çıkması, yapay zekanın daha karmaşık problemleri çözebilme kapasitesini artırmıştır. Bu, yapay zekanın daha geniş bir uygulama alanına yayılmasını sağlamaktadır.

İkinci olarak, veri miktarının büyük ölçüde artması yapay zekanın gelişimi için büyük bir avantaj sağlamaktadır. Günümüzde internet ve sosyal medya gibi platformlar üzerinde büyük miktarda veri oluşturulmaktadır. Bu veriler, yapay zekanın öğrenme ve desenleri tanıma yeteneklerini iyileştirmek için kullanılabilir. Gelecekte, daha fazla veri toplanacak ve işlenecektir, bu da yapay zekanın daha da gelişmesini sağlayacaktır.

Yapay zekanın geleceği, sağlık sektöründe önemli bir etkiye sahip olacaktır. Yapay zeka, hastalıkların erken teşhisini yapabilme, tıbbi görüntülerin analizini gerçekleştirme ve tedavi planlarını optimize etme gibi alanlarda büyük bir potansiyele sahiptir. Bu sayede, sağlık hizmetlerinde daha etkin bir şekilde kullanılarak hastaların yaşam kalitesini artırabilir ve sağlık hizmetlerine erişimi iyileştirebilir.

Yapay zeka aynı zamanda otomasyon ve robotik alanlarında da büyük bir rol oynayacaktır. Fabrikalarda ve üretim tesislerinde yapay zekaya dayalı robotlar, tekrarlayıcı görevleri yerine getirebilir ve insan gücünden tasarruf sağlayabilir. Bunun yanı sıra, otonom araçlar ve insansız hava araçları gibi alanlarda da yapay zekanın kullanımı artacaktır. Bu sayede, daha güvenli ve verimli bir toplum oluşturmak mümkün olabilir.

Yapay zekanın gelecekteki etkileri ve potansiyelleri hakkında endişeler de bulunmaktadır. Özellikle, yapay zekanın insan işgücünün yerini alması ve işsizlik oranlarını artırması gibi konular tartışılmaktadır. Ancak, bu endişelerin üstesinden gelmek için insanların yapay zeka teknolojisine uyum sağlayabilmesi ve yeni beceriler öğrenerek dönüşebilmesi önemlidir.

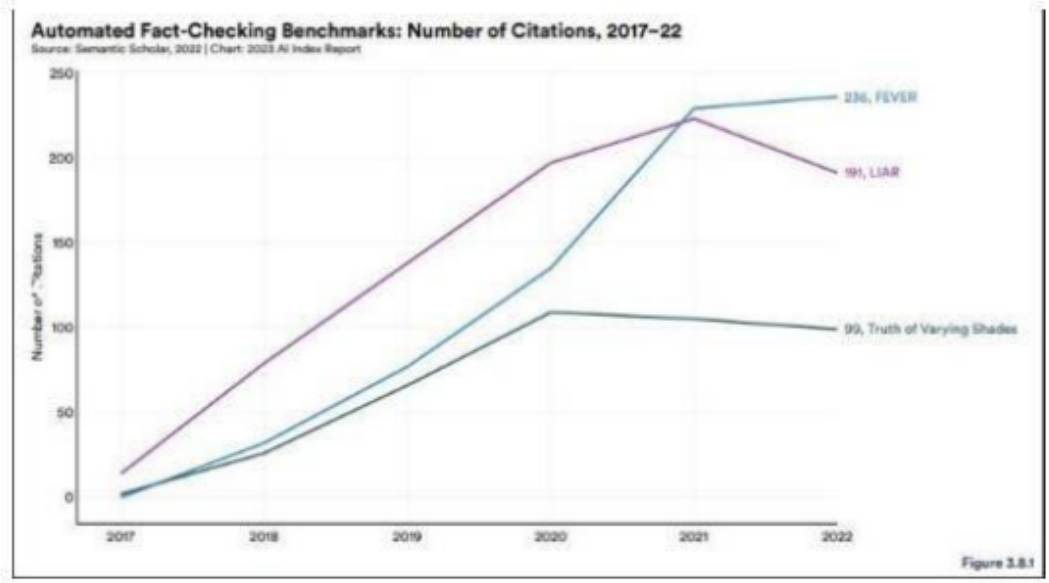
Sonuç olarak, yapay zeka teknolojisinin geleceği oldukça umut vaat etmektedir. Bu teknoloji, birçok alanda büyük bir potansiyele sahip olup hayatımızı daha kolay, verimli ve güvenli hale getirebilir. Ancak yapay zekanın etik, gizlilik ve güvenlik gibi konularında dikkatli olunması gerekmektedir. Bu nedenle, yapay zeka teknolojisinin gelişimini yönlendiren politika ve düzenlemelerin de etkin bir şekilde uygulanması önemlidir.

AI Index Raporu 2023

"Artificial Intelligence Index Report 2023" raporunun Teknik Yapay Zeka Etiği bölümüne bir göz attım. Ama daha raporu incelememin öncesinde 2017 yılından bu zamana kadar her yıl düzenli rapor yayınladıklarını fark ettim.

Rapora bakmadan önce değişiklerden birinin de 2022 yılında yapay zeka endeksi 25 ülke olan küresel yapay zeka mevzuatı takibi, bu yıl 127 ülke ile genişletilmiş olmasıydı. Buradan daha rapora göz gezdirmeden bir yıl farkla değişimin olduğunu görmek mümkün.Sekiz bölümden oluşan rapor alttaki başlıklardan oluşuyor:

Bölüm 1: Araştırma ve Geliştirme Bölüm
2: Teknik Performans Bölüm
3: Teknik YZ Etiği Bölüm
4: Ekonomi Bölüm
5: Eğitim Bölüm
6: Politika ve Yönetişim Bölüm
7: Çeşitlilik Bölüm
8: Kamuoyu Görüşü Gerçeğe Uygunluk ve Doğruluk kısmına baktığımızda üç adet çokça kullanılan popüler olan makalelere yapılan atıf sayılarına bakılmış. Bunlar "FEVER", "LIAR" ve "Truth of Varying Shades" makalelerinden oluşuyor. 2017 yılında yayınlanan bu üç makalenin yıllara göre yapılan atıf sayılarına ilişkin grafiği gönderinin resimlerinde yer vereceğim. Ve korkmayın, ben bu rapordan kullandığıma dair atıfta bulunacağım. Burada sizlerin de düşünüp yorum yapmasını isteyeceğim kısım: Sizce bu atıf sayıları gerçeği yansıtıyor mu? Gerçekten bu makalelerden yararlanan herkes atıfta bulunmuş mudur?



DİYOLAĞA DAYALI YAPAY ZEKA ETİK SORUNLAR- Furkan Hüseyin Araz

İsveç'teki Luleå University of Technology araştırmacıları, popüler chatbotların bir analizini gerçekleştirdi. Bu araştırmacılar, 2022 yılının ortalarında 100 konuşma analizi gerçekleştirdiler. Sonuca baktığımızda bu yapay zeka sistemlerinin %37'sinde kadın cinsiyet rolü gözlemlenmiş. Bunun yanında popüler ticari ürünlerinin %62,5'inde diyalogsal yapay zeka sistemleri varsayılan olarak kadın cinsiyeti şeklinde görüldü. Şirketlerin orantısız bir şekilde sistemi kadınlardan yana kullanması eleştirmenlerin gözünde şunu ortaya çıkartıyor: Oluşacak sorunlarda suçun kadınlar üzerine yıkılabilme ihtimalinin doğurabilecek olması... Peki sizin kulağınıza bu durum nasıl gelmekte? Bana kalırsa hassas olunması gereken bir konu.. Chatbotların cinsiyetsiz halde kullanarak oluşabilecek sorunları başlamadan çözebileceğimizi düşünüyorum.

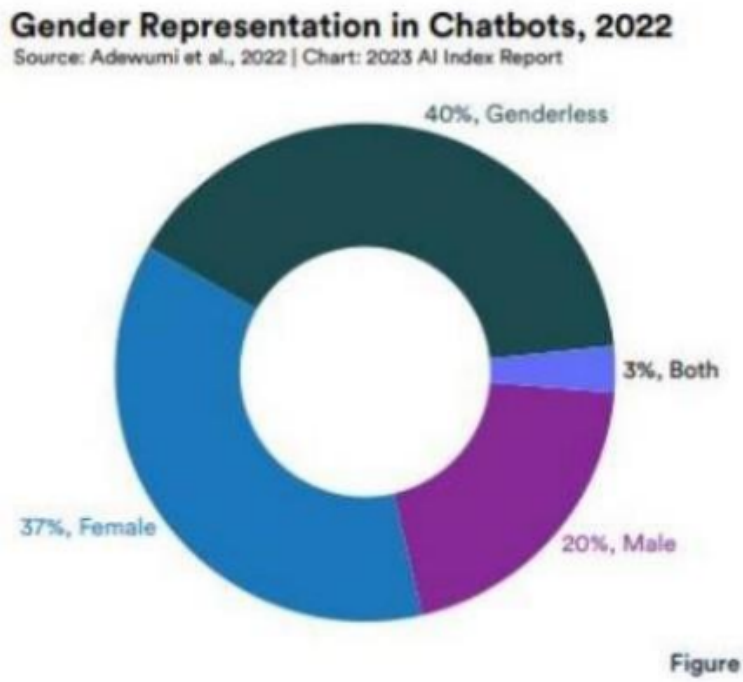
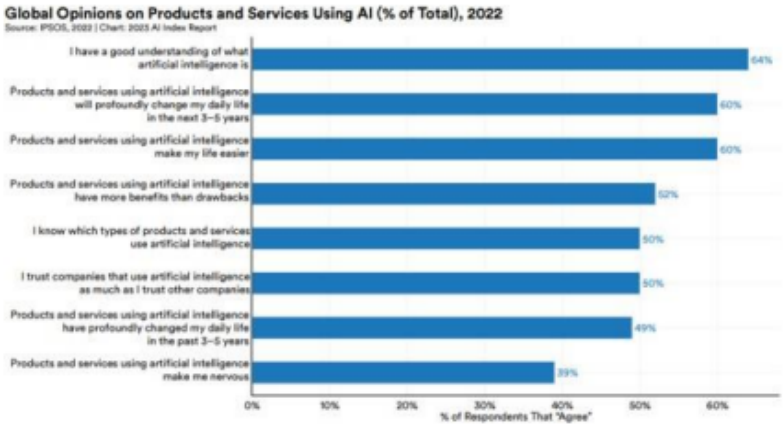


Figure 3.4.1

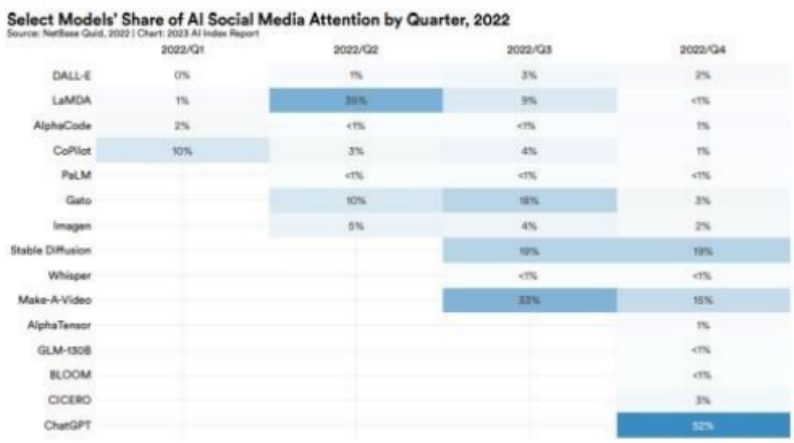
Farklı milliyetten insanlara bazısorular yöneltilerek demografik yapıya göre insanların yapay zeka eğilimlerinin belirlenmesi hedeflenmiş. Bu sorulardan biri olan “Yapay zeka ürün ve hizmetlerinin iyi-kötü hangi taraf sizler için ağır basıyor?” sorusuna Çinli katılımcıların büyük bir kısmı olumlu taraflarının daha ağır bastığını düşünüyor. Bu sonucu ilk gördüğümde Çin’de yaşamın, işlerin nasıl olduğuna dair düşünceler belirdi. Demek ki yapay zekanın daha verimli olacağı işler var ve insanları rahatlatacak bir sonuç veriyor ve verecek ki Çinli insanlar yapay zekanın ürün ve hizmetleri karşısında daha olumlu bir yaklaşım sergiliyorlar. Suudi Arabistan ve Hindistan da olumlu tarafın daha ağır olduğunu düşünen diğer bazı ülkelerden. Peki her milliyet yapay zekanın olumlu taraflarının ağır bastığını mı düşünüyor? Cevabı şöyle vermek gerekirse: Ankete cevap veren Amerikalıların sadece %35’i yapay zekanın iyi taraflarını baskın olarak görmektedir. Soru belki de amacına ulaşmış ve demografik yapı değişince yapay zekaya bakış açının farklılaştığı gözlenmiştir.

Cinsiyet olarak bakıldığında ise erkeklerin yapay zekanın ürün ve hizmetlerinde avantajlarının dezavantajlara göre daha baskın olduğunu kadınlara oranla daha yüksek olduğu görüşmüştür. Aynı zamanda erkeklerin kadınlara göre yapay zekanın bir yardımcı rolü oynayacağını düşünme oranı da daha yüksek. 2022 IPSOS anket raporuna göre: erkeklerin fikri, yapay zekanın hayatı kolaylaştırdığı, yapay zekayı aktif olarak kullanan şirketlere güvendikleri, yapay zeka ürünlerinin avantajlarının daha ağır bastığı yönünde olmuştur. Raporlar sonucunda dünya genelinde (özellikle Amerika’da) otonom araçlara karşı ön yargısürmektedir. Bu sonucu destekler neticesinde olan diğer bir veri ise: Küresel çapta yapılan bir araştırma sonucunda, katılımcıların yalnızca %27’si otonom araçlara güvendiklerini söylemiştir.



Yandaki anket sonuçları 28 farklı ülkeden 16-74 yaş aralığında 19504 kişinin verdiği sonuçları yansıtmaktadır. Sonuç grafiğine bakıldığında örneklemin %60'lık kısmı, yakın gelecekte yapay zekanın hayatlarını oldukça değiştireceğini düşünmektedir. Katılımcıların %40'lık kısmı yapay zekanın onları gergin hissettiklerini düşünüyor.

Raporda sosyal medyanın da nabzının tutulduğundan bahsedilerek, Chat GPT'nin kullanıma girdikten sonra çokça kullanılmaya başlanması,sosyal medyaya bomba gibi düşüp diğer yapay zeka uygulamalarına kıyasla oldukça fazla bir şekilde konuşulduğundan bahsedilmiş. Hep iyi şeyler konuşulmamış elbette. Chat GPT sohbet robotunun belirli bir kültür, siyaset anlayışı, etik ve inanış konusunda nerede durduğu gibi konularda irdelenmiş. İşte bu konu hakkında bazı Twitter tweetleri: "Alarm: ChatGPT by @OpenAI now *expressly prohibits argumentsfor fossil fuels*. (It used to offer them.) Not only that, it excludes nuclear energy from its counter-suggestions." -@sama, "what isthe reason for this policy?" - @AlexEpstein Bazı insanlar Chat GPT'nin kullanıma yasak olması gerektiğini bile savundu. Hatta savunulmakla kalmadı bazı yerlerde kullanılması sınırlandırıldı. Aşağıda yapay zeka teknolojilerinin yılın bölümlere ayrılmış bir şekilde sosyal medyadaki yeri ile ilgili yapılan çalışma sonucunu görebilirsiniz.



Kaynakça

1.hhttps://gradientflow.com/wp-content/uploads/2060/09/Gradient-Flow-Trend-2023-Report-Final.pdf?utm_source=gradientflow&utm_medium=newsletter

2.https://aiindex.stanford.edu/wp-content/uploads/2023/04/HAI_AI-Index-Report-2023_CHAPTER_3.pdf

3.https://dergipark.org.tr/en/download/article-file/596690https://books.google.com.tr/books?4.hl=tr&lr=&id=JsoqEAAAQBAJ&oi=fnd&pg=PA1&dq=yapay+zeka+nedir&ots=8K0VXPiOFY&sig=X1MbY7x7uMiSEBAScfk1rPbFgOY&redir_esc=y#v=onepage&q=yapay%20zeka%20nedir&f=false

5. https://www.platinonline.com/dijital-trend/yapay-zeka-ve-robot-otomasyonu-is-sureclerinimukemmellestirecek-1074406

6. https://dspace.ankara.edu.tr/xmlui/handle/20.500.12575/73967

7.https://tr.wikipedia.org/wiki/ChatGPT#:~:text=İnce%20ayarı%20yapılan%20temel%20model,nin%20GPT%2D3.5%20dil%20modeliydi.&text=ChatGPT%2C%2030%20Kasım%202022%27de,kısa%20sürede%20dikkatleri%20üzerine%20çekti.

8. https://aiindex.stanford.edu/report/

9. Coşkun, F., & GÜLLEROĞLU, H. D. (2021). Yapay zekânın tarih içindeki gelişimi ve eğitimde kullanılması. Ankara University Journal of Faculty of Educational Sciences (JFES), 54(3), 947-966.

10. Sheikhi, M./ Journal of Economics and Political Sciences 2022 2(1) 102-111

11. Dirican, C. (2015). The Impacts of Robotics, Artificial Intelligence On Business and Economics, Procedia - Social and Behavioral Sciences, 195, 564–573.