T.C.
GÜMÜŞHANE ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

YÖNETİM BİLİŞİM SİSTEMLERİ ANA BİLİM DALI

BLOKZİNCİR TEKNOLOJİSİNİN GÜVENLİK ZAFİYETLERİ ÜZERİNE BİR ANALİZ: KONU MODELLEME İLE İNCELEME

YÜKSEK LİSANS

Tayfur AYAS

HAZİRAN-2025
GÜMÜŞHANE

T.C.
GÜMÜŞHANE ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

YÖNETİM BİLİŞİM SİSTEMLERİ ANA BİLİM DALI

BLOKZİNCİR TEKNOLOJİSİNİN GÜVENLİK ZAFİYETLERİ ÜZERİNE BİR ANALİZ: KONU MODELLEME İLE İNCELEME

AN ANALYSIS ON SECURITY VULNERABILITIES OF BLOCKCHAIN TECHNOLOGY: EXAMINATION WITH TOPIC MODELING

YÜKSEK LİSANS

Tayfur AYAS

HAZİRAN-2025
GÜMÜŞHANE

T.C.
GÜMÜŞHANE ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

YÖNETİM BİLİŞİM SİSTEMLERİ ANA BİLİM DALI

BLOKZİNCİR TEKNOLOJİSİNİN GÜVENLİK ZAFİYETLERİ ÜZERİNE BİR ANALİZ: KONU MODELLEME İLE İNCELEME

AN ANALYSIS ON SECURITY VULNERABILITIES OF BLOCKCHAIN TECHNOLOGY: EXAMINATION WITH TOPIC MODELING

YÜKSEK LİSANS

Tayfur AYAS

Danışman: Dr. Öğr. Üyesi Uğur DEMİREL

HAZİRAN-2025
GÜMÜŞHANE

BİLİMSEL ETİĞE UYGUNLUK BEYANI

Yüksek Lisans Tezi olarak hazırlamış olduğum "**Blokzincir Teknolojisinin Güvenlik Zafiyetleri Üzerine Bir Analiz: Konu Modelleme ile İnceleme**" isimli bu tezimin, tamamen kendi çalışmam olduğunu, her alıntıya kaynak gösterdiğimi, alıntı yaptığım tüm çalışmaları kaynakçada belirtiğimi ve Gümüşhane Üniversitesi'nin lisanslı kullanıcısı olduğu intihal yazılım programı ile Lisansüstü Eğitim Enstitüsü'nün belirlediği kıstaslara uygun olarak raporladığımı taahhüt ederim. Tezimin kâğıt ve elektronik kopyalarının Gümüşhane Üniversitesi Lisansüstü Eğitim Enstitüsü arşivinde saklanmasına izin verdiğimi onaylarım.

Lisansüstü Eğitim ve Öğretim Yönetmeliği'nin ilgili maddeleri uyarınca gereğinin yapılmasını arz ederim.

19/06/2025

…….

Tayfur AYAS

TEŞEKKÜR

Lisans ve yüksek lisans öğrenimim süresince her konuda desteğini esirgemeyen, kıymetli zamanını ayırarak yol gösteren, Yönetim Bilişim Sistemleri Anabilim Dalı Başkanı ve Gümüşhane Üniversitesi Rektör Yardımcısı Sayın Prof. Dr. Handan ÇAM'a en içten teşekkürlerimi sunarım.

Tez yazım sürecinde akademik bilgisi, yönlendirmeleri ve her soruma sabırla verdiği yanıtlarla çalışmama değerli katkılar sağlayan danışmanım Dr. Öğr. Üyesi Uğur DEMİREL'e; eleştirileri ile çalışmamın bilimsel temeller ışığında şekillenmesinde yardımcı olan tez savunmasında bulunan değerli hocam Doç. Dr. Ahmet Kamil KABAKUŞ'a teşekkür ederim.

Tezin hazırlanma ve yazım aşamalarında destek olan arkadaşlarıma ve her zaman yanımda olan aileme teşekkür ederim. Bu süreçte sabır ve anlayışlarıyla yanımda olan anneme, babama ve ağabeyime minnettarım.

Ayrıca, tez sürecinin her anında bana inanan, motivasyon sağlayan ve desteğini esirgemeyen sevgili kız arkadaşıma da gönülden teşekkür ederim.

Tayfur AYAS

GÜMÜŞHANE – 2025

ÖZET

Blokzincir teknolojisi, 2008 yılında Bitcoin ile tanıtılmış ve finans başta olmak üzere birçok sektörde kullanılmaya başlanmıştır. Güvenli, şeffaf ve merkeziyetsiz yapısıyla çeşitli alanlarda yenilikçi çözümler sunan bu teknoloji, güvenlik zafiyetleri nedeniyle benimsenme sürecinde zorluklar yaşamaktadır. Literatürde blokzincir zafiyetleri üzerine yapılan çalışmalar genellikle teorik düzeyde veya vaka analizleriyle sınırlıdır. Bu çalışmada, blokzincir tabanlı uygulamalardaki güvenlik zafiyetleri incelenecek ve sosyal medya platformu Twitter'dan toplanan 8705 veri, doğal dil işleme (NLP) teknikleriyle analiz edilmiştir. LDA (Latent Dirichlet Allocation) yöntemi kullanılarak, güvenlik zafiyetlerinin türleri ve yaygınlıkları belirlenmiş, bu bulgular gelecekteki blokzincir uygulamalarının güvenliği için yol gösterici olmaktadır. Çalışmanın amacı, blokzincir sistemlerinin güvenlik risklerini daha iyi anlamak ve bu riskleri azaltmaya yönelik stratejiler geliştirmektir. Tez, veri toplama, temizleme, analiz ve sonuçların yorumlanması aşamalarından oluşmaktadır. Elde edilen sonuçların, blokzincir tabanlı teknolojilerin güvenliğine katkı sağlayacağı öngörülmektedir.

Anahtar Kelimeler: Blokzincir, Güvenlik zafiyetleri, LDA, Konu modelleme, Twitter veri tabanı

SUMMARY

Blockchain technology was introduced with Bitcoin in 2008 and has been used in many sectors, especially in finance. This technology, which offers innovative solutions in various fields with its secure, transparent and decentralized structure, has difficulties in the adoption process due to security vulnerabilities. In the literature, studies on blockchain vulnerabilities are generally limited to theoretical level or case studies. In this study, security vulnerabilities in blockchain-based applications were examined and 8705 data collected from the social media platform Twitter were analyzed with natural language processing (NLP) techniques. By using the Latent Dirichlet Allocation (LDA) method, the types and prevalence of vulnerabilities were determined and these findings have provided guidance for the security of future blockchain applications. The aim of the study is to better understand the security risks of blockchain systems and develop strategies to mitigate these risks. The thesis consists of data collection, cleaning, analysis and interpretation of the results. The results obtained are expected to contribute to the security of blockchain-based technologies.

Keywords: Blockchain, Vulnerabilities, LDA, Topic modeling, Twitter database

İÇİNDEKİLER

TABLOLAR DİZİNİ

ŞEKİLLER DİZİNİ

EKLER DİZİNİ

SİMGELER VE KISALTMALAR DİZİNİ

2FA : Two Factor Authentication (2 Faktörlü Kimlik Dogrulama)
ACM : Association for Computing Machinery (Bilgisayar Makineleri Derneği)
BFT : Byzantine Fault Tolerance (Bizans Hata Teorisi)
Bk. / bk. : Bakınız
CTM : Correlated Topic Model (İlişkili Konu Modelleme)
DApp : Decentralized Applications (Merkezi Olmayan Uygulamalar)
DDOS : Distributed Denial of Service (Dağıtık Hizmet Engelleme)
DLT : Distribute Ledger Technology (Dagıtılmış Defter Teknolojisi)
DPoS : Delegated Proof of Stake (Delege Edilen Hisse Kanıtı)
DTM : Dynamic Topic Models (Dinamik Konu Modelleme)
GDA : Gizli Dirichlet Ayrımı
İKM : İlişkisel Konu Modelleme
LDA : Latent Dirichlet Allocation (Gizli Dirichlet Tahsisi)
LSA : Latent Semantic Analysis (Gizli Anlamsal Analiz)
LSI : Latent Semantic Indexing (Gizli Anlamsal İndeksleme)
M2M : Machine to Machine (Makineden Makineye)
n-LDA : Nstage Latent Dirichlet Allocation (Nstage Gizli Dirichlet Tahsisi)
NLP : Natural Language Processing (Doğal Dil İşleme)
NMF : Non-negative Matrix Factorization (Negatif Olmayan Matris Faktörizasyonu)
P2P : Peer to peer (Eşler Arası)
PBFT : Practical Byzantine Fault Tolerance (Pratik Bizans Hata Teorisi)
PKI : Public Key Infrastructure (Açık Anahtar Altyapısı)
pLSA : Probabilistic Latent Semantic Analysis (Olasılıksal Gizli Anlamsal Analiz)
pLSI : Probabilistic Latent Semantic Indexing (Olasılıksa Gizli Anlamsal İndeksleme)
PoS : Proof of Stake (Hisse Kanıtı)
PoW : Proof of Work (Çalışma Kaniti)
SSI : Social Security İnstitution (Sosyal Güvenlik Kurumu)
STM : Structural Topc Model (Yapısal Konu Modelleme)
SVD : Singular Value Decomposition (Tekil Değer Ayrıştırması)

TF-IDF : Term Frequency-Inverse Document Frequency (Terim Frekansı-Ters Belge Frekansı)

v.d. : Ve diğerleri, ve devamı

vb. : Ve benzeri

VPN : Virtual Private Network (Sanal Özel Ağ)

YKM : Yapısal Konu Modelleme

$\sum$: Toplama Fonksiyonu

X_i : Girdi Değeri

y_i : Çıktı Değeri

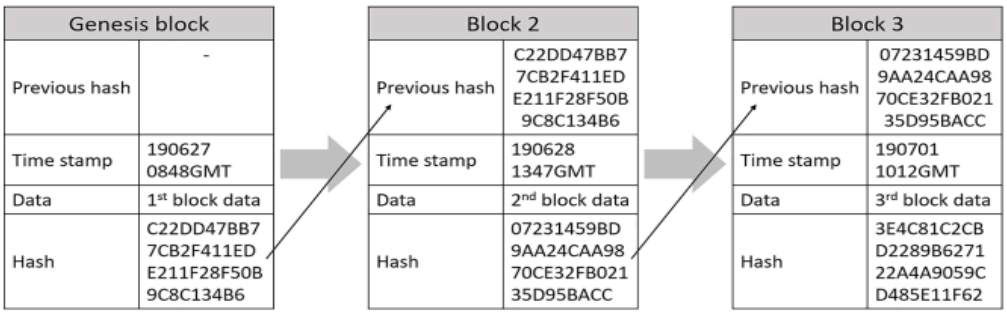
w_i : Ağırlıklar

1. GİRİŞ

Blokzincir teknolojisi, dijital çağın en yeni ve dönüştürücü teknolojileri arasında yer almaktadır. Merkeziyetsiz yapısı, şeffaflığı ve veri bütünlüğünü esas alan sistemiyle, bilgi teknolojileri için yeni bir zemin oluşturmakta ve öne çıkmaktadır. İlk olarak 2008 yılında Satoshi Nakamoto tarafında veya bir grup tarafından kripto para birimlerini tanıtan bir makalede gündem olmuştur. Kısa süre içerisinde sadece kripto para ile kalmayıp birçok sektörle de iç içe olmuştur (Nakamoto, 2008). Blokzincir teknolojisi, verilerin zaman damgalı ve sıralı bir şekilde bloklar halinde kaydedildiği, bu blokların kriptografik yöntemlerle birbirine bağlandığı bir sistem olarak çalışmaktadır. Bu özelliği sayesinde değiştirilemez ve merkeziyetsiz veri kayıtlarının oluşturulmasını sağlar. Tedarik zinciri yönetimi, eğitim ve finans gibi birçok alanda kullanım alanı bulmaktadır (Yli-Huumo vd., 2016).

Blokzincir teknolojisinin temelini oluşturan dağıtık deftere teknolojisi (DLT) sistem üzerinde yapılan işlemlerin merkezi bir otoriteye bağlı kalmaksızın tüm ağ katılımcılarının eşzamanlı bir şekilde kaydetmesini ve doğrulamalarını sağlamaktadır (Narayanan vd., 2016). Dağıtık defter teknolojisi yapısı, kriptografik algoritmalarla desteklenerek, yapılan her bir işlemin şifrelenerek ve oluşturulan zincire geri dönülemez şekilde eklenmesini sağlar. Bu şekilde, yapılan işlemler üzerinde herhangi bir değişiklik yapılmasını veyahut geçmişte kalan kayıtların silmeninin önüne geçilmiş olur. Konsensüs algoritmaları ile bu da pekiştirilip ağ üzerindeki katılımcıların hangi blokların zincire bağlanması konusunda fikir birliği oluşmasını sağlar ve güvenliği daha da pekiştirmektedir (Bonneau vd., 2015).

Halka açık bir blok zinciri, her bir katılımcının veya düğümün, işlemleri halka açık bir defterde kaydettiği merkezi olmayan bir ağ olarak oluşturulur. İşlem kümeleri toplanır ve belirli bir zamanda bu veri kümesiyle ilgili benzersiz bir karma kod oluşturmak için bir algoritmaya yerleştirilen bir gruba veya "bloğa" yerleştirilir. Bu karma kod, bir sonraki bloğu oluşturan bir sonraki işlem dizisindeki ilk veri parçasını oluşturur. İşlemler biriktikçe, “bir zincir oluşturan” bloklar eklendikçe liste büyür. Şekil 1’de bir blokzincirin yapısı gösterilmektedir (Rogerson ve Parry, 2020).



Şekil 1. Blokzincir Yapısı

Blokzincir teknolojisinin sunduğu birçok avantaja rağmen, çeşitli güvenlik zafiyetleri bu teknolojinin yaygınlaşmasının önünde önemli bir engel oluşturmaktadır. Bu zafiyetler yalnızca teknik hatalardan değil, aynı zamanda kullanıcı hatalarından da kaynaklanabilmektedir. Merkeziyetsiz yapının kötüye kullanılması ve sosyal mühendislik saldırıları gibi sorunlar da sıkça görülmektedir. Yaygın güvenlik açıkları arasında akıllı sözleşme hataları, kullanıcı cüzdanlarına yönelik saldırılar, %51 saldırıları ve Sybil saldırıları sayılabilir. Bu tür açıklar yalnızca teknik zararlar yaratmakla kalmaz, aynı zamanda kullanıcı güveni ve kamuoyu algısını da ciddi biçimde zedeler (Atzei vd., 2017; Conti vd., 2018; Douceur, 2002).

Günümüzde yapılan araştırmalar çoğunlukla bu zafiyetleri teknik çözümlerle ele almaktadır. Altyapının güçlendirilmesi, akıllı sözleşmelerin daha sıkı denetlenmesi ve konsensüs mekanizmalarının iyileştirilmesi bu çözümler arasındadır. Ancak sistemin kullanıcı tabanlı yönü derinlemesine ele alınmamaktadır. Teknik önlemler tek başına yeterli olmayabilir; sistemin başarısı aynı zamanda kullanıcı güveni ve sosyal kabul ile de doğrudan ilişkilidir. Blokzincir teknolojisinin toplumlar tarafından benimsenmesi, güvenin artması ve yaygınlaşması açısından kullanıcı algısının analiz edilmesi büyük önem taşımaktadır (Zheng vd., 2017).

Sosyal medya platformları yalnızca teknolojilerin gelişiminin paylaşıldığı ortamlar değil, aynı zamanda insanların teknolojiye yönelik algılarını, endişelerini ve tutumlarını da yansıttıkları alanlardır. Blokzincire dair güvenlik endişeleri, kullanıcıların sosyal medyada yaptıkları paylaşımlar üzerinden gözlemlenebilmektedir. Bu çalışmada, sosyal medya platformu X (eski adıyla Twitter) üzerinden toplanan 8705 tweet doğal dil işleme ve LDA konu modelleme teknikleri ile analiz edilmiştir. Amaç, kullanıcıların hangi güvenlik zafiyetlerine odaklandığını ve hangi endişeleri taşıdığını belirlemektir.

Konu modelleme, büyük veri setlerinin analizi için sıklıkla kullanılan istatistiksel bir yöntemdir. Bu tezde kullanılan ana yöntem olan Latent Dirichlet Allocation (LDA),

belgelerde saklı olan temaları ortaya çıkarmak için geliştirilmiş bir modeldir (Blei vd., 2003). LDA yöntemiyle sosyal medya kullanıcılarının paylaşımları, blokzincir güvenliğine ilişkin tematik başlıklar altında sınıflandırılmıştır.

Çalışmanın temel amacı blok zincir teknolojisine dair güvenlik zafiyetlerinin sosyal medya kullanıcıları üzerinden nasıl bir algılama yapıldığına dair analiz yapılarak bu algının sistem güvenliği üzerindeki etkilerini değerlendirmektir. Bunun için Twitter verileri üzerinde doğal dil işleme ve konu modelleme teknikleri kullanılmıştır. Bu çalışmada LDA yöntemi ile güvenlik zafiyetlerine dair tematik dağılımlar çıkartılmıştır. Sosyal medya üzerinde daha çok hangi konular üzerinde tartışılmış onlara vurgu yapılmıştır. Yapmış olduğumuz analiz sonucu elde edilen bulgular blok zincir güvenliğine hem teknik açıdan hem de sosyal açıdan değerlendirerek bütünsel bir bakış açısı sunmayı hedeflemektedir.

Sonuç olarak, blokzincir teknolojisinin kullanıcılarına sunduğu kolaylıkları, avantajları tam olarak gerçekleştirebilmesi için, sadece sistemin teknik altyapısını değil aynı zamanda kullanıcı yorumlarının ve toplum güveninin de göz önünde bulundurarak ona göre kendini daha iyi geliştirmelidir. Bu çalışma blokzincir teknolojisinde güvenlik zafiyetleri konusunda farkındalık yaratmak ve gelecekte yapılacak olan veya yapılması olası olan sistem tasarımına yön vererek bütüncül yaklaşımların geliştirilmesine katkı sağlaması ve kullanıcı odaklı güvenliklerine katkı sağlamasını hedeflemektedir. Sosyal medya platformu olan X'ten çektiğimiz veriler sonucunda oluşturduğumuz bulguların, blokzincir teknolojisinin daha güvenli ve kullanıcı dostu olarak kabul edilecek hale gelmesine katkı sağlayacağı öngörülmektedir. Araştırmanın kapsamı yalnızca blokzincir güvenlik zafiyetlerine odaklanmakta olup; analiz, X platformundan elde edilen 8.705 tweet üzerinde gerçekleştirilmiştir. Yöntem olarak doğal dil işleme ve LDA konu modelleme tekniği tercih edilmiştir.

Bu bağlamda, çalışmanın temel araştırma sorusu şu şekilde ifade edilebilir: "Sosyal medya kullanıcıları, blokzincir teknolojisinde hangi güvenlik zafiyetlerini öncelikli olarak algılamakta ve bu algılar tematik olarak nasıl sınıflandırılabilmektedir?" Araştırmada test edilen temel hipotez ise şöyledir: Sosyal medya kullanıcılarının blokzincir güvenliğine yönelik algıları belirli temalar etrafında yoğunlaşmakta ve bu temalar istatistiksel olarak LDA yöntemi ile sınıflandırılabilir niteliktedir. Çalışmanın sınırlılıkları arasında, verilerin yalnızca X platformundan elde edilmiş olması, analiz dilinin İngilizce ile sınırlı tutulması ve yalnızca kamuya açık kullanıcı verilerinin değerlendirilmesi yer almaktadır. Ayrıca, otomatik filtreleme ve önişleme süreci bazı bağlamsal ayrıntıların dışarıda kalmasına yol açmış olabilir.

2. BLOKZİNCİR (BLOCKCHAIN) VE GÜVENLİK ZAAFİYETLERİ

Bu bölümde; araştırmanın yazılmasında sunulan blokzincir teknolojisi ve güvenlik zafiyetleri hakkında kavramsal bilgiler yer almaktadır.

2.1. Blokzincir Teknolojisinin Tanımı ve Temel Kavramlar

Blokzincir teknolojisi, her ne kadar 2008 yılında Satoshi Nakamoto tarafından yayımlanan makale ile tanınmış ve yaygınlık kazanmış olsa da, kökeni daha eski çalışmalara dayanmaktadır (Narayanan vd., 2016). Örneğin, 1976 yılında yayınlanan "Kriptografide Yeni Yönelimler" başlıklı makalede, şifreleme süreçlerinde kullanılan simetrik anahtarlar yerine asimetrik anahtarlar (özel ve açık anahtar çifti) önerilmiş ve bu yaklaşım blokzincirin temel yapı taşlarından biri olmuştur (Xu vd., 2019). Ayrıca 1982 yılında ortaya konulan "Bizans Generalleri Problemi", merkezi bir otoriteye gerek duymadan güvenli karar alma mekanizmalarının geliştirilmesine yönelik önemli bir katkı sunmuştur (Lamport vd., 2019).

Blokzincir teknolojisi, genel olarak 2019 yılından bu yana ilk tanınan kripto para biriminden günümüze kadar, sosyal uygulamalardan farklı sektörlere kadar birçok alanda kullanılmaya başlanmıştır. Blokzincir teknolojisinin farklı alanlarda gelişen uygulamaları ve teknolojileri göz önünde bulundurulduğunda, bu teknolojiyi üç ana kategori altında inceleyip tartışmak mümkündür.

Birinci evre, blokzincirin gelişim evresidir. Bu evrede Bitcoin'in yanı sıra farklı kripto para birimleri de ortaya çıkmış ve aracılar olmadan finansal ödemelerin gerçekleştirilmesi sağlanmıştır. Bu dönemde işlemler gizlilik içinde yürütülmüş, gizlilik ön planda tutulmuştur.

İkinci evrede ise ilk dönemde taraflar arasında gerçekleştirilen merkeziyetsiz finansal işlemlere rağmen, süreçlerin finansal açıdan tam anlamıyla işletilemediği görülmüş ve sistemin daha gelişmiş bir haline geçilmiştir. Yazılmış olan akıllı sözleşmeler yardımıyla işlemler otomatik olarak gerçekleştirilebilmiştir. Bu dönemde tedarik zinciri, emlak, sigorta gibi birçok alanda blokzincir uygulamaları kullanılmaya başlanmıştır (Xu vd., 2019).

Üçüncü evre ise günümüzde en çok konuşulan ve popüler hâle gelen evredir. Bu evrede, teknoloji dünyasına ait maliyet sorunları büyük ölçüde giderilmiş; yapay zekâ uygulamaları yaygınlaşmış ve makineler arası iletişim (M2M) üst seviyelere ulaşmıştır. Bu ve benzeri birçok teknolojik gelişmeyle birlikte, dijital para gibi kavramların ön plana çıktığı blokzincir uygulamaları yaygınlaşmıştır (Ayberkin, 2022; Efanov ve Roschin, 2018).

2.1.1. Blokzincir'in Çalışma Presipleri

Blokzincir teknolojisinin çalışma prensiplerini anlamak, sistemin sunduğu yeniliklerin ve güvenlik yapısının kavranması açısından önemlidir. Temel olarak blokzincir, "blok" adı verilen veri yapılarının birbirine sıralı şekilde bağlanmasıyla oluşur. Her bir blok; zaman damgası, işlem verileri ve kendisinden önceki bloğa ait bir özet (hash) değeri içerir. Bu bloklar, kriptografik yöntemlerle birbirine bağlanarak zincir yapısını oluşturur. Bir kez zincire eklenen bloklar sonradan değiştirilemez, bu da sistemin bütünlüğünü ve güvenliğini artırır (Durukal, 2021).

Blokzincir sisteminde bir işlemin gerçekleşme süreci aşağıdaki adımlarla özetlenebilir:

1. Bir işlem yapmak istenilir. Bu işlemin gerçekleşmesi için bir blok oluşturulur.
2. Blok oluşturulduktan sonra süreç bitinceye kadar yer alan taraflara yayımlanır.
3. Katılımcılar kendilerine yayımlanan işlemi inceleyip onaylarlar.
4. Katılımcılar onayladıktan sonra blok oluşur.
5. Blok oluştuktan sonra algoritmik bir sistem ile blokzincire eklenir.
6. Son işlem ise üzerinde veriler bulunan bloklar blokzincire eklenir ve katılımcılar durum bildirirler.

Blokzincir teknolojisinin farklı türleri bulunmaktadır. Bu türler temel olarak ağın erişim düzeyine ve katılım koşullarına göre sınıflandırılır:

Açık (Public) Blokzincir: Herkesin katılabildiği, işlem yapabildiği ve verileri görebildiği tamamen şeffaf sistemlerdir. Bitcoin ve Ethereum gibi ağlar bu kategoriye girer. Katılımcı sayısı yüksek olduğundan güvenlik algoritmaları karmaşık olabilir ve işlem süresi uzayabilir.

Özel (Private) Blokzincir: Belirli kurum ya da kişilerce kontrol edilen ve erişim izni gerektiren blokzincir türüdür. Katılımcılar önceden belirlenir ve işlem hakları sınırlandırılabilir. Genellikle kurum içi çözümlerde tercih edilir.

Konsorsiyum (Consortium) Blokzincir: Birden fazla kurum ya da paydaşın ortaklaşa yönettiği blokzincir yapısıdır. Örneğin, birden çok bankanın dahil olduğu bir

finansal ağda kullanılabilir. Bu model, hem şeffaflık hem de gizlilik arasında bir denge sağlar (Durukal, 2021).

2.1.1.1. Dağıtık Defter Teknolojisi

Dağıtık defter teknolojisi (Distributed Ledger Technology- DLT), verilerin merkezi bir otoriteye bağlı olmadan, ağdaki tüm katılımcılar tarafından eşzamanlı olarak tutulduğu ve yönetildiği bir veri tabanı yapısını ifade eder. Bu teknoloji, işlemlerin bütünlüğünü güvence altına alırken, manipülasyonu zorlaştırarak sistem güvenliğini artırır (Swan, 2015). DLT sistemlerinde işlemler, önceden belirlenmiş bir konsensüs mekanizması aracılığıyla doğrulanır ve birden fazla blokta saklanır. Bu sistemin temel türleri şunlardır (Narayanan et al., 2016).

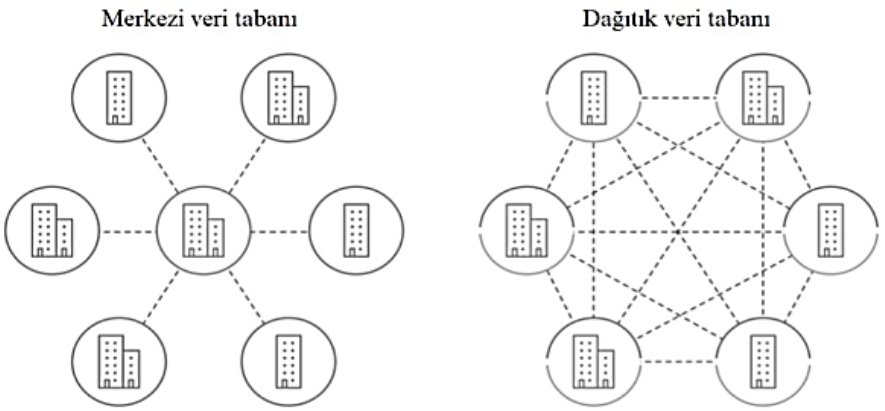
- **Blokzincir tabanlı DLT:** Veriler, bloklar halinde kriptografik olarak birbirine bağlanır. Klasik blokzincir sistemleri bu modele dayanır.
- **DAG (Directed Acyclic Graph) tabanlı DLT:** Veriler bloklar yerine yönlendirilmiş grafikler şeklinde birbirine bağlanır. Bu yapı blokzincire ihtiyaç duymadan daha yüksek işlem hacmine ulaşabilir.
- **Hashgraph tabanlı DLT:** Sanal oylama yöntemine dayanır ve işlemler ağdaki düğümler tarafından konsensüs ile onaylanır (Baird, 2016).

Dağıtık defter teknolojisi önemli avantajlara sahiptir. Bu avantajlar; şeffaf olmaları, güvenli bir ortam sağlamaları ve veri bütünlüğünü korumalarıdır. Bu defter üzerindeki kullanıcılar işlemleri görebilir ve bu da güvenliğin artmasını sağlamaktadır. Merkezi olmayan yapısı ve kriptografik yöntemler kullandığı için saldırılara karşı dayanıklıdır. Defter üzerindeki veriler değiştirilememekte birlikte, geçmişte yapılan işlemler her zaman ve her an doğrulanabilir (Joshi vd., 2018).

Bu avantajların bazı özelliklerini belirtmek gerekirse; şeffaflık konusunda, yapılan bütün işlemlerin kamuya açık olacak şekilde kaydedilmesi söz konusudur (Pilkington, 2016). Güvenlik açısından bakıldığında, dağıtık yapısı sayesinde ve kriptografi özelliğiyle saldırılara karşı dirençlidir (Yaga vd., 2019). Merkeziyetsiz olması sayesinde, sistemin tek bir bağlama bağlı kalmasının önüne geçilir. Hız ve maliyet açısından da, önceki sistemlere göre daha az maliyetle ve daha hızlı bir şekilde işlem gerçekleştirilmesini sağlamaktadır (Bonneau vd., 2015).

Blokzincir içerisinde yapılan işlemlerin gerçekleşmesi ve veri tabanı sistemi içerisinde kendine yer bulabilmesi için, ilk olarak doğrulanmış bloklar oluşturulmalı, tekrar aynı düğüm üzerinden doğrulanmış geçerli olan işlemlerin geçerli bloklara işlenmesi dahil edilmelidir. Bundan sonra ise, onaylanan blok ağ üzerindeki diğer

düğümlere yayılır. Böylelikle her bir düğüm, elde ettiği blokları doğrulayarak bloklar içerisinde oluşan işlemleri doğrulayıp çalışır hale getirir ve sonuç olarak kendi veri tabanına dâhil etmektedir.



Şekil 2. Merkezi veri tabanı ve dağıtık veri tabanı (Vurdu, 2021)

Temel olarak bakıldığında, blokzincir teknolojisi merkezi bir kontrol yapısına sahip değildir. Sisteme dâhil olan tüm kullanıcılar, "düğüm" adı verilen yapılarda açık ve özel anahtarlarla birbirleriyle etkileşim kurmaktadır. Yapmak istedikleri işlemleri ise akıllı sözleşmeler aracılığıyla otomatik olarak gerçekleştirmektedirler. Yapılan işlem kayıtlarının kopyaları, veri madenciliği sistemleri içerisinde dağıtık biçimde saklanmakta ve bu yapı, bilgi işlem altyapısının temelini oluşturmaktadır.

Dağıtık kayıt defteri teknolojisinin temelleri, ağ üzerinde bulunan tüm düğümlerin aynı verinin bir kopyasına sahip olmasını sağlayarak, merkezi bir otoriteye duyulan ihtiyacı ortadan kaldırmaktadır. Bu sistemin temel bileşenleri şu şekilde sıralanabilmektedir: Kriptografi, verilerin güvenliğini sağlamak açısından kritik bir öneme sahiptir. Konsensüs mekanizmaları, ağ üzerindeki düğümler arasında fikir birliği oluşturmaktadır. Akıllı kontratlar ise işlemlerin otomatik olarak gerçekleştirilmesini ve bu işlemlerin güvenli bir biçimde sağlanmasını temin etmektedir (Yaga vd., 2019).

Proof of Work (PoW): Anlam bakımından iş ispatı anlamına gelmektedir. Karmaşık gözüken problemleri çözüme kavuşturarak blok oluşmasını sağlamaktadır. Bu süreç, güvenlik açısından yüksek düzeyde koruma sağlamasının yanında oldukça fazla enerji de tüketmektedir. Genellikle Bitcoin gibi büyük ölçekli kripto işlemlerinde kullanılmaktadır (Nakamoto, 2008).

Proof of Stake (PoS): Hisse ispatı ile çalışmaktadır. Ağa dâhil olan düğümler üzerinde ne kadar coin miktarı varsa, bu miktara göre blok üretmeye hak kazanılmaktadır. İş ispatı anlamına gelen PoW'ye kıyasla, enerji tüketimi daha azdır (Nakamoto, 2008).

Delegated Proof of Stake (dPoS): Temsili hisse ispatı olarak da bilinen dPoS, gerçek zamanlı oylama ile kullanılan bir modelle bağlı olup, kapsayıcı bir kanıt sistemi olduğundan diğerlerine göre daha az merkezileşmiş bir fikir birliği olarak değerlendirilmektedir. Coin sahipleri, sistemdeki rolleri için oy vermektedir. Oy gücü, hesabın kaç adet coin tuttuğuna göre belirlenmektedir. Temsili hisse ispatının rolleri vardır; bu roller, düğümlerin her an açık ve çalışır durumda olmasını sağlamakta, ağ üzerinde yapılan işlemlerin bloklara taşınmasını ve toplanmasını gerçekleştirmekte, topladığı blokları yayınlamakta ve işlemleri onaylamaktadır. Herhangi bir sorun ya da sıkıntı bulunması hâlinde, bu sorunların en adil şekilde çözülmesini sağlamaktadır. PoS'a nazaran daha hızlıdır ve demokratik bir yapı sunmaktadır (Swan, 2015).

Tablo 1. Konsensüs mekanizması (Bonneau vd., 2015)

Konsensüs Mekanizması	Enerji Tüketimi	Güvenlik Seviyesi	İşlem Hızı
Proof of Work (PoW)	Yüksek	Çok Güçlü	Düşük
Proof of Stake (PoS)	Düşük	Güçlü	Orta
Delegated PoS (dPoS)	Çok Düşük	Orta	Çok Yüksek

2.1.1.2. Konsensüs Mekanizmaları

Bu mekanizmalar, dağıtılmış ağdan farklı olarak, çeşitli cihazlar arasında reddedilemeyecek bir anlaşma ortaya koymaktadır. Ayrıca, bu mekanizma sayesinde sistemin başkaları tarafından sömürülmesinin önüne geçilmektedir.

Konsensüs, yani uzlaşma terimi, sistem içerisindeki ağlarda bulunan düğümlerin, bir blokzincir merkezinde aynı fikre sahip olması ve aynı zamanda kendi kendini denetleyebilen bir sistem olması anlamına gelmektedir. Bu bahsettiğimiz iki temel işlevi sorunsuz bir şekilde yerine getirebilen teknoloji oldukça önemli kabul edilmektedir.

Şimdi ilk olarak bakacak olursak, uzlaşma protokolleri bir blokzincir sisteminin güncellenmesine olanak sağlayarak izin verirken; blokzincir içerisinde bulunan her bir bloğun doğru şekilde yapılandırılmasını, sistemi kullanacak olan kullanıcıların cesaretlendirilmesini, ilham verilmesini ve teşvik edilmesini sağlayacak bir yol izlemektedir. İkinci olarak ise, bütün blokzincir sisteminin kontrol edilmesinde rol oynamakta veya sistemin raydan çıkmasını engellemektedir. Bu protokolün kurallarının amacı, bir zincir üzerinde ilerlenmesini, bu zincirin kullanılmasını ve işlemlerin takip edilebilirliğinin garanti altına alınmasını sağlamaktır (Atabaş, 2018, s. 36).

Bu mekanizma, bazı temel işlevleri yerine getirmek açısından da oldukça yararlıdır. Bu temel işlevler ise şöyledir: sistemde bulunan ağ içerisinde dağıtık güven tesis

etmektedir. Double spending (çift harcama) gibi benzeri yolsuzlukların önüne geçmekte ve bunların yapılmasını engellemektedir. Sistem üzerinde işlem sırasını takip edip belirleyerek, bloklar arasındaki kronolojiyi düzenlemekte ve belli bir sırada dizilmesine olanak sağlamaktadır (De Filippi ve Wright, 2018; Narayanan vd., 2016). Yapılabilecek saldırılara karşı ise Bizans Hata Toleranslı (BFT) bir protokol oluşturarak sistemin sürekliliğini güvence altına almaktadır (Lamport vd., 2019).

2.1.2. Blokzincir'in Kullanım Alanları

Blokzincir teknolojisi, halk arasında genellikle Bitcoin gibi dijital para birimlerinin altyapısında yer aldığı şeklinde bilinmekle birlikte, birçok alanda kapsamlı bir şekilde görülmektedir. Sağlık, eğitim, finans, enerji gibi birçok alanda karşımıza çıkmakta ve bu sektörlere yeni çözümler üretmekle birlikte güvenilir bir altyapı sunmaktadır (Narayanan vd., 2016).

Blokzincir teknolojisinin en yaygın kullanıldığı alanlardan biri finans sektörüdür. Özellikle para transferleri arasında aracı kurumları devre dışı bırakmak amacıyla, uluslararası para transferlerinde sıkça kullanılmaktadır. Para transferinin daha hızlı bir şekilde gerçekleştirilmesini sağlamakta ve güvenliği artırmak açısından önemli bir olanak sunmaktadır. Bankacılık sektöründe ise, dolandırıcılığın minimuma indirilmesi ve şeffaflığın artırılması amacıyla tercih edilen bir teknolojidir (Crosby vd., 2016; Nakamoto, 2008).

Tedarik zinciri yönetiminde de blokzincir teknolojisi kullanılmaktadır. Burada ürünlerin üretimden tüketiciye kadar olan yolculuğu şeffaf bir şekilde kayıt altına alınmakta ve tüketicinin bu süreci açıkça görmesine olanak sağlamaktadır. Genellikle ilaç ve gıda sektörlerinde sahteciliğin önüne geçmek amacıyla tercih edilmektedir (Francisco ve Swanson, 2018).

Sağlık hizmetlerinde de blokzincir teknolojisi kullanılmaktadır. Bu alanda, hastalara ait verilerin saklanması ve hasta mahremiyetinin korunması açısından önemli bir çözüm sunmaktadır. Bunun yanı sıra, sağlık kurumları arasında verilerin daha güvenli bir biçimde paylaşılmasına da yardımcı olmaktadır (Zhang vd., 2019).

Kamu yönetimi alanında ise blokzincir, kamu kurumlarında yapılan yolsuzluklarla mücadele etmek amacıyla kullanılan bir teknoloji olup, kamusal işlemlerde şeffaflığı artırmayı hedeflemektedir. Özellikle seçimlerde, oylama işlemlerinin doğruluğunun garanti altına alınması için blokzincir tabanlı sistemlerin kullanılması mümkündür (Swan, 2015).

Eğitim alanında da blokzincir teknolojisi çeşitli kolaylıklar sağlamaktadır. Öğrencilerin veya eğitmenlerin diploma ve sertifika gibi belgeleri blokzincir üzerinde güvenli bir biçimde saklanabilmektedir. Bu teknoloji, eğitim süreçlerinde işe alımlarda kullanılan diploma ve sertifikaların sahte olup olmadığının kolaylıkla doğrulanmasına imkân tanımaktadır (Grech ve Camilleri, 2017).

Enerji sektöründe de blokzincir teknolojisi ile karşılaşılmaktadır. Burada, kişilerin kendi imkânlarıyla ürettikleri enerjinin ticaretini yapmaları için merkezi olmayan enerji sistemlerinin mümkün hâle gelmesine olanak tanımaktadır. Böylelikle yenilenebilir enerji kaynaklarının daha etkili bir şekilde kullanılması sağlanmakta ve üreticiler için önemli faydalar sunulmaktadır (Andoni vd., 2019) .

Blokzincir teknolojisi gayrimenkul alanında da etkili bir rol oynamaktadır. Mülkiyet bilgilerinin blokzincir üzerinde saklanması sayesinde, gayrimenkul işlemleri daha güvenilir hâle gelmekte ve satışlarda şeffaflık sağlanarak işlemlerin hem daha hızlı hem de daha düşük maliyetli bir biçimde gerçekleştirilmesi mümkün olmaktadır (Zhang vd., 2019).

Blokzincir teknolojisinin sigortacılık alanında da kullanıldığı görülmektedir. Bu sektörde, son yıllarda sık karşılaşılan doğal afetler sonucunda oluşan hasarların tespit edilmesi ve tazminat süreçlerinin otomatik, şeffaf ve güvenli bir şekilde yürütülmesi hedeflenmektedir. Bu süreçlerin hızlandırılması sayesinde, dolandırıcılık riskinin minimuma indirilmesi amaçlanmaktadır (Tapscott ve Tapscott, 2016) .

Tarım sektörü de blokzincir teknolojisi ile entegre hâle gelmektedir. Bu alanda, blokzincir sayesinde gıda güvenliği sağlanmakta, mahsulün izlenebilirlik düzeyi artırılmakta ve ürünlerin üretim koşullarına dair bilgiler tüketiciyle paylaşılmaktadır. Ayrıca, ürünlerin taşınma ve depolama süreçlerine ilişkin veriler de blokzincire kaydedilerek tüketiciye güvenilir bilgi sunulmaktadır (Tian, 2016).

2.2. Blokzincir'in Teknolojisinde Güvenlik ve Riskler

Her teknolojide olduğu gibi, blokzincir teknolojisinde de belirli güvenlik açıkları ve riskler söz konusudur. Merkeziyetsiz yapısı ve kriptografik güvenlik katmanları sayesinde, dijital ortamda güvenli veri aktarımını mümkün kılan yeni bir sistem olarak karşımıza çıkar (Nakamoto, 2008). Güvenlik mimarisi ve riskler genel olarak şu şekilde sıralanabilir:

Blokzincir teknolojisinin güvenlik mimarisi, temelde Dağıtık Defter Teknolojisi (DLT) prensibine dayanır. Bu sistemlerde gerçekleştirilen her işlem, ağda yer alan tüm katılımcılar tarafından doğrulanır; sonrasında şifrelenerek bloklar hâlinde zincire eklenir

(Yli-Huumo vd., 2016). Sistemde kullanılan kriptografik hash fonksiyonları, bloklar arasındaki bağlantıyı sağlıklı şekilde kurar ve zincirin bütünlüğünü korur (Zheng vd., 2017).

Blokzincir teknolojisinde kriptografi, verilerin gizliliğini sağlamak ve kullanıcı kimliklerinin doğrulanmasında temel bir rol üstlenir. Kriptografik altyapı, genellikle Açık Anahtar Altyapısı (PKI) ve dijital imzaları temel alır. Bu sistem, kullanıcıların işlemleri güvenli biçimde tamamlamalarına yardımcı olur (Conti vd., 2018). Her kullanıcı, sahip olduğu özel anahtar ile yaptığı işlemleri imzalar; bu imza ise ilgili açık anahtar aracılığıyla doğrulanabilir.

Kuantum bilgisayarların gelişimiyle birlikte, mevcut kriptografik sistemlerin zamanla geçerliliğini yitirmesi ihtimali ortaya çıkmaktadır (Aggarwal vd., 2017). Bu nedenle, blokzincir teknolojisi post-kuantum kriptografi yaklaşımlarına adapte olmaya çalışmaktadır.

Genel olarak, "Blokzincir teknolojisi güvenli midir?" sorusu yöneltildiğinde bu soruya "evet" yanıtı verilebilir. Blokzincir, güçlü matematiksel temellere ve karmaşık algoritmalara dayalı olarak çalışır. Elle çözülmesi son derece zor olan şifreleme teknikleri kullanılır. Şifreleme sistemi, bir bireyin bir adrese sahip olduğunu doğrulamak ve bu adres üzerinden kripto varlık gönderebilmesini sağlamak amacıyla özel anahtarların kombinasyonuna dayanır. Bu adresler, rastgele sayı ve harf kombinasyonlarından oluşur ve sadece ilgili kullanıcı tarafından yönetilebilir. Bu adresler doğrudan kullanıcı kimlikleriyle ilişkilendirilmediği ve çözülmesi son derece zor olduğu için kimlik hırsızlığı gibi tehditlerin önüne geçilir. Bir adres, özel anahtar sahibi dışında kimse tarafından kontrol edilemez. Özel anahtarlar ise oldukça uzun karakter dizilerinden oluştuğundan yüksek güvenlik sağlar. Bu nedenle, blokzincir teknolojisi zayıf şifreleme ihtiyacını ve çevrim içi kimlik doğrulama gereksinimini ortadan kaldırarak bireysel kullanıcılara daha güçlü bir güvenlik sunar (Atabaş, 2018, s. 49).

Güvenliğin sağlanmasına yönelik bazı ipuçları şu şekilde sıralanabilir:

- Çevrim içi etkinliklerde VPN kullanarak şifreleme sağlanabilir.
- Her çevrim içi hesap için farklı ve güçlü parolalar kullanılmalıdır.
- Şifrelerde rakam, harf ve semboller bir arada yer almalı; parolalar karmaşık ve uzun olmalıdır.
- İki aşamalı kimlik doğrulama (2FA) mutlaka etkinleştirilmelidir (Atabaş, 2018, s. 52)

Bu öneriler, kullanıcıların kendi kullanım alışkanlıklarına göre genişletilebilir.

Blokzincir teknolojisi tasarımsal olarak güçlü ve güvenilir bir altyapı sunmakla birlikte, uygulama düzeyinde ve kullanıcı kaynaklı zafiyetler de mevcuttur. Bu zafiyetler genellikle akıllı sözleşme hataları, konsensüs protokolü zayıflıkları ve %51 saldırıları gibi teknik riskleri kapsamaktadır. Bu güvenlik açıkları, aşağıdaki alt başlıklarda ayrıntılı şekilde ele alınacaktır.

2.2.1. Güvenlik Zafiyeti Kavramı

Blokzincir teknolojisi, sistem içerisinde yer alan blokların sırasıyla birbirine bağlandığı bir yapıdır. Bu birbirine bağlı bloklar, kendisinden önce gelen bloğun hash değerini içererek yeni bir blok oluşturur ve bloklar arasındaki bütünlüğü korur. Sistem değiştirilemez ve merkeziyetsiz bir yapıya sahip olduğundan, içerdiği verilerin güvenliğini yüksek düzeyde sağlar (Zheng vd., 2017).

Güvenlik zafiyeti kavramı ise, bir sistemin dışarıdan gözle fark edilemeyen ancak kodlama veya tasarım hatalarından kaynaklanan, siber saldırılar tarafından istismar edilebilecek açıklıkları ifade eder (Conti vd., 2018). Blokzincir teknolojisinde bu tür zafiyetler çoğunlukla protokol seviyesinde ve uygulama katmanında ortaya çıkar. Uygulama katmanı ise akıllı sözleşmeler, cüzdanlar gibi bileşenleri kapsar (Atzei vd., 2017).

Blokzincir sistemi yapısal açıdan oldukça güvenli görünmesine rağmen, yazılım kaynaklı hatalar ve kriptografik zayıflıklar sistemin saldırıya açık hâle gelmesine neden olabilir. Bu tür saldırıların önlenebilmesi için sistemin yalnızca teknik düzeyde değil, aynı zamanda sosyal düzeyde de bazı önleyici tedbirler ve stratejiler benimsemesi gerekir. Ayrıca yazılım geliştiricilerin protokol iyileştirmeleri yapmaları da büyük önem taşır (Atzei vd., 2017; Bonneau vd., 2015).

Güvenlik zafiyetlerinin oluşum süreçleri bulunmaktadır. Bunlar arasında; konsensüs mekanizmasındaki açıklıklar, akıllı sözleşmelerden kaynaklanan hatalar ve %51 saldırıları yer almaktadır. Bu açıklıklar aşağıdaki alt başlıklarda daha ayrıntılı şekilde ele alınacaktır.

2.2.2. Blokzincir'de Yaygın Güvenlik Zafiyetleri

Sistem üzerinde bulunan yaygın güvenlik açıklıkları aşağıda ayrıntılı bir şekilde açıklanacaktır.

2.2.2.1. Akıllı Sözleşme Hataları

Akıllı sözleşme (smart contract) hataları, blokzincir teknolojisi tabanlı uygulamalarda çalışan, kendi kendini yürüten kodların beklenmedik ya da istenmeyen şekilde davranması sonucu ortaya çıkan yazılım temelli kusurları ifade eder (Atzei vd., 2017). Bu tür hatalar hem bireysel hem de kurumsal kullanıcılar için ciddi mali kayıplara neden olabilmektedir. Blokzincir teknolojisinin geri döndürülemez yapısı göz önünde bulundurulduğunda, bu tür hataların sonuçları telafi edilemez düzeyde olabilir (Luu vd., 2016).

Yeniden giriş (Reentrancy) hatası, iki akıllı sözleşme arasında gerçekleşen bir transfer sırasında kontrolün karşı tarafın fonksiyonlarına bırakılması ve bu fonksiyonların orijinal sözleşmeyi tekrar tekrar çağırması sonucunda ortaya çıkar. Bu durum, fonksiyonların kötüye kullanılarak sistem dışına değer aktarılması gibi ciddi güvenlik açıklarına neden olabilir (Atzei vd., 2017). Bu tür bir hataya 2016 yılında yaşanan DAO saldırısında rastlanmıştır. Saldırı sonucunda yaklaşık 60 milyon dolardan fazla bir kayıp yaşanmıştır (Batista ve Lemieux, 2019).

Taşma ve taşım (Integer Overflow and Underflow) hataları, sayısal verilerin bit uzunluklarını aşması veya altına düşmesi durumunda meydana gelen zafiyetlerdir (Luu vd., 2016). Taşma (Integer Overflow), bir tam sayının bellekte alabileceği maksimum değeri aşması durumunda ortaya çıkar. Örneğin, 8 bitlik bir tam sayı yalnızca 0 ile 255 arasında bir değer alabilir (2^8-1). Bu sınır aşıldığında değer sıfırlanır.

```
Unsigned char x= 255;
    x = x+1;
```

Bu durumda x artık 0 (sıfır) olur (Brumley vd., 2007).

Taşım (Integer underflow) hatası ise taşma hatasının tam tersi olarak düşünülebilir. Burada ise tam sayıları temsil eden minimum değerlerin altına inmesi ile oluşmaktadır. Yine aynı şekilde x= 0 olduğunu düşünüldüğünde x den 1 çıkarıldığı takdirde değer tekrar maksimum değer olan 250 sarar (Brumley vd., 2007).

Bu hataların ortaya çıkmasının başlıca nedenleri; sabit bit uzunluklarının sınır aşımına duyarlılığı, programcının kontrol eksikliği ve uygun olmayan veri tipi seçimleridir (Muntean vd., 2017).

Zamanlama bağımlı hatalar, bazı akıllı sözleşmelerin belirli zaman aralıklarına bağlı olarak çalışması gerektiğinde görülür. Ancak blokzincir yapısında mutlak bir zaman standardı bulunmadığından, bu parametreler kötü niyetli yazılımlar tarafından manipüle

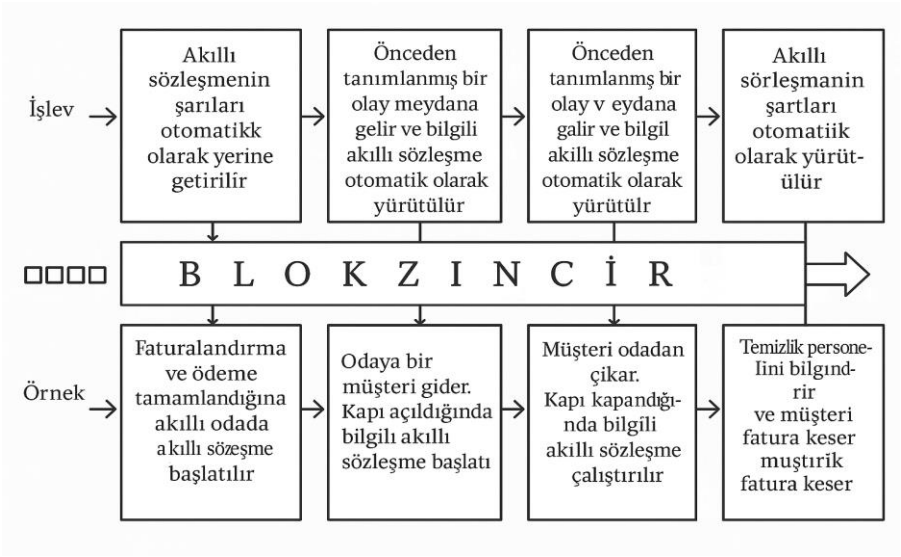
edilebilir. Bu tür saldırılar literatürde block timestamp manipulation olarak geçer (Tang vd., 2023). Kötü niyetli aktörler, işlemleri zaman manipülasyonlarıyla tetikleyerek akıllı sözleşmelerin beklenmedik sonuçlar doğurmasına neden olabilir (Hewa vd., 2021).

Selfdestruct fonksiyonu, sözleşmenin kendini kalıcı olarak silmesini sağlayan bir özelliktir. Bu fonksiyon, sözleşmenin ömrünün sona erdiği durumlarda geliştiriciler tarafından kullanılmak üzere tanımlanır. Ancak fonksiyon herkese açık şekilde yazılmışsa, kötü niyetli bir kullanıcı bu işlevi tetikleyerek sözleşmenin tamamen yok olmasına ve tüm işlevlerinin devre dışı kalmasına neden olabilir (Atzei vd., 2017). Bu fonksiyon genellikle geliştiriciler tarafından elindeki sözleşmenin tarihine göre ömrü sona erdiği düşünülen sözleşmeleri devre dışı bırakmak için kullanılır. Fakat bu fonksiyon herkesin erişebileceği şekilde tanımlanmasından dolayı aktörler arsında niyeti iyi olmayan kullanıcılar tarafından isteyerek sözleşmeyi yok etmesine neden olabilir ve sözleşmenin tüm işlevlerinin kullanılmayacak hale getirerek olumsuz sonuçlara neden olabilir (Grossman vd., 2017).

Genel olarak bu hataların ortaya çıkmasına sebep olan nedenler şöyledir;

- Denetim süreçlerinin yeterli yapılmaması.
- Kodlama alanında kodlama pratiğine uyulmaması
- Karmaşık şekilde olan iş mantıklarının hatalı olarak tasarlanıp kontrol edilmemesi (Atzei vd., 2017; Grossman vd., 2017).

Blokzincir altyapısına bağlı bir komut dosyası, akıllı sözleşme olarak bilinmektedir. Daha öncesinden tanımlanmış olan komutlar olarak ta geçen bu akıllı sözleşmelerin işlevi, blokzincir üzerinde yapılan bir işlem tarafından tekitlendiği anda yürütülür. Akıllı sözleşmelerin koşulları blokzincir tabanından saklandığından her an tüm kullanıcıların amaçladığı gibi karşılıklı bir vakit ile çalışacak ve kullanıcılar arasındaki güveni arttıracaktır. Şekil de görüldüğü gibi akıllı sözleşmelerin işlevini yere getirme sıraları gösterilmektedir (Ante, 2021).



Şekil 3. Akıllı sözleşmenin işlevini yerine getirme aşamaları (Ante, 2021)

2.2.2.2. Merkeziyetsiz Uygulama (DApp) Güvenlik Zafiyetleri

Blokzincir teknolojisinin ortaya çıkması ile merkeziyetsiz uygulamalar da gelişmekte ve birçok alanda kullanıcılar için kolaylık sağlamaktadır. Fakat merkeziyetsizliğin temel amacı manipülasyon direnci sağlasa da, merkeziyetsiz uygulamalarda (DApp) meydana gelen açıklıklar bu sistemlerin istismar edilebileceğini ortaya koymaktadır (T. Chen vd., 2017).

DApp'lerin hepsi diyebileceğimiz kadar çoğu, Ethereum gibi platformlar üzerinde çalışılan sözleşmelere dayanmaktadır. Bu akıllı sözleşmeler çoğunlukla Solidity adı verilen programlama diliyle yazılır ve bununla birlikte kod içerisinde yapılan hatalar sistemin sömürülmesine yol açmaktadır (Atzei vd., 2017).

DApp'ler, kripto çekişi ve oyunlar gibi rastgelelik gerektiren özellikleri içinde barındıran bir yapıya sahiptir. Fakat blokzincir sistemi içerisinde rastgelelik elde etmek oldukça zor bir durumdur. Bu nedenle program geliştiriciler genellikle rastgelelik için "blockhash" veya "block.timestamp" gibi bazı değişkenleri kullanmaktadır. Ancak bu değişkenler madenciler tarafından kontrol edilebilir olduğundan, manipülasyon riski de beraberinde artmaktadır (Kalodner vd., 2020).

İşlem yarışı zafiyeti diye bir durum da vardır merkeziyetsiz uygulamalarda. Bu zafiyet, kullanıcıların herhangi bir işleminin madenciler tarafından daha yüksek bir ücret ile manipüle edilerek önce o işlemin işlenmesi durumu ile ortaya çıkmaktadır. Bu tür işlemler, saldırılar "front-running" olarak bilinir. Genellikle merkeziyetsiz borsalarda daha çok görülmektedir (Daian vd., 2019).

Kötü amaçlı akıllı sözleşmelerin etkileşimi; bu gibi bazı durumlarda masum olan uygulamalarla etkileşime giren zararlı akıllı sözleşmelerin fon çekmesine ve sistem

üzerinde hiç istenmeyen davranışlara yol açmasına neden olmaktadır. Program geliştiricilerin “fallback” fonksiyonunu ve bir de “delegatecall”, “selfdestruct” gibi komutları kullanırken çok dikkatli olmaları gerekmektedir (Rodler vd., 2018).

Bir diğer yaygın zafiyet ise yetkilendirme ve erişim kontrol eksiklikleri olarak karşımıza çıkmaktadır. Bu zafiyet, akıllı sözleşmelerde belirli bazı fonksiyonlara erişim adresleri verilerek sınırlandırılmaması durumunda ortaya çıkmaktadır. “onlyOwner” gibi temel etkisi olan bu yetkilendirme kontrolü mekanizmasının eksik olması, kötü niyetli aktörler tarafından sisteme erişim yolu açılarak istenmeyen sonuçlara yol açabilir (Luu vd., 2016).

2.2.2.3. Konsensüs Protokolü Zayıflıkları

Konsensüs protokolü, blokzincirinin temel taşlarından birisidir. Ağ katılımcıları arasında güvenli bir şekilde fikir birliği sağlamaya yaramaktadır. Teorik olarak bakıldığında bu protokoller çok iyi bir şekilde görünse de, pratikte bazı zayıflıklarla karşılaşılmakta ve bazı sınırlandırmalar da içermektedir (Bonneau vd., 2015).

Bu protokollerin zayıf noktaları genellikle ağa katılım, enerji tüketimi gibi faktörlerden etkilenir. Örnek verecek olursak, Sybil saldırısını ele alabiliriz. Bu saldırılarda, bir saldırganın sahte bir kimlik ile ağa katılması sonucu konsensüs mekanizmasını manipüle etmesi kaçınılmaz bir durumdur. Kimlik doğrulamasının zor olduğu ağlarda bu tür zafiyetler önemli tehditler oluşturabilmektedir (Douceur, 2002).

Proof of Work (PoW) Zayıflıkları: Protokol, hesaplamaya dayalı olarak konsensüs sağlar. Fakat bu yapı, "%51 saldırısı" olarak bilinen saldırı çeşidine açıktır. Örneğin, bir saldırgan ağın içerisinde toplam hesaplama gücünün %51'inden fazlasını eline geçirebilirse, önceki blokları değiştirme gibi saldırılar gerçekleştirebilir (Nakamoto, 2008; Stoll vd., 2019).

Proof of Stake (PoS) Zayıflıkları: Sistem üzerindeki ağ kontrolü, yatırılan coin miktarına göre yapılır. Bu durum, "nothing at stake" problemi ile karşılaşılmasına yol açmaktadır. "Nothing at stake" dediğimiz şey, konsensüs mekanizmasının karşılaştığı bir tür güvenlik sorunudur. Bu sorun, doğrulayıcıların çatallanma durumunda hiçbir maliyet ödemeden birden fazla zincirde işlem onaylamaya çalışabilmesi durumudur. Böyle bir durumda, konsensüs dağınıklığına neden olunmaktadır (Buterin ve Griffith, 2019).

Delegated Proof of Stake (DPoS) Zayıflıkları: Temsilcilerin sayısı az olup blok üretmesiyle ilgilidir. Bu durum, merkeziyetsizlikte sapma riskini ortaya çıkarmaktadır. Delegelerin seçimi oylama ile yapılmış olsa bile, sosyal manipülasyonlara açık olmakta

ve bunun yanında oy çalma, oy satın alabilme gibi işlemlerle sistem zarar görebilmektedir (Li vd., 2020).

Practical Byzantine Fault Tolerance (PBFT) Zayıflıkları: Bu konsensüs protokolünde sistem üzerinde çok sayıda katılımcının olması ve mesaj sayısının fazla olması nedeniyle ölçeklenebilirlik sorunları ile karşılaşılmaktadır. Bunun yanında, senkronizasyonun bozulması ya da zarar görmesi durumunda sistem durabilir (Castro ve Liskov, 2002).

Konsensüs protokolü zayıflıklarını azaltmak için uygulanabilecek bazı çözümler şunlardır:

- Sybil saldırılarından korunmak için merkezi olmayan bir kimlik doğrulama sistemi uygulanabilir (Douceur, 2002).
- PoS protokollerinde, "slashing" mekanizması kullanılarak çatallama üzerinde doğrulama yapan katılımcılar değerlendirilip cezalandırılabilir (Buterin ve Griffith, 2019).
- Delegelerin seçimlerini oylama ile yapan DPoS yapısında şeffaflık artırılabilir, oy kayıtlarının denetimleri artırılmalıdır veya artırılabilir (Li vd., 2020).
- PBFT gibi sistemlerde iletişim trafiğinin fazlalığından kaynaklanan sorunlar için, bu trafiği azaltabilecek optimizasyon teknikleri geliştirilip kullanılmalıdır (Castro ve Liskov, 2002).

2.2.2.4. %51 Saldırıları ve Çift Harcama Sorunu

%51 saldırısı, blokzincir teknolojisi alanında, hesaplama gücünün toplamının %51'inden fazlasını elinde bulunduran bir kişi veya grubun sistemdeki ağ üzerinde yapılan işlemleri tek taraflı olarak değiştirebilmesi şeklinde tanımlanan bir saldırı türüdür. Bu durum genellikle Proof of Work (PoW) algoritması ile çalışan sistemlerde görülmektedir. Sistemin çoğunluğunu elinde bulunduran bu saldırganlar, sistemdeki blokları tersine çevirebilir veya alternatif bloklar oluşturabilirler. Bu alternatif bloklar sayesinde, önceden gerçekleşmiş işlemler geçersiz hale getirilebilir.

Çift harcama sorunu ise, dijital para birimlerinin aynı kopyasını birden fazla kez harcamaya yönelik bir girişimdir. Blokzincir sistemi, tam da bu sorunu önlemek amacıyla tasarlanmıştır. Ancak ağın %51'inden fazlasını kontrol eden bir kişi, blokzincir üzerinde alternatif bir blok oluşturarak daha önce gerçekleşmiş bir işlemi geri alma ve aynı kripto parayı yeniden harcama imkânına sahip olur. Bu durum, blokzincir teknolojisinin güvenliğine ciddi zararlar verebilmektedir.

%51 saldırılarına örnek olarak, 2018 yılında Bitcoin Gold (BTG) ağına gerçekleştirilen bir saldırı sonucunda yaklaşık 18 milyon dolar değerinde çift harcama yapılmıştır. Bir başka örnek ise Ethereum Classic (ETC) ağıdır. 2020 yılında bu ağ arka arkaya %51 saldırılarına maruz kalmış ve binlerce blok yeniden yazılmıştır (Nakamoto, 2008).

Eğer bir kişi veya grup, sistemdeki toplam işlem gücünün %51'inden fazlasını kontrol altına alırsa, sistem üzerinde şu işlemleri yapabilme yetkisine sahip olur:

- Sistem üzerindeki işlemleri engelleyebilir veya durdurabilirler. Yani bazı işlemleri bilinçli olarak onaylamayabilirler.
- Çift harcama yapabilirler; önceden yapılmış bir işlemi geri alarak daha önce harcanmış olan kripto parayı bir kez daha kullanabilirler.
- Zinciri yeniden yazabilirler; saldırgan, bu şekilde yeni bir blok oluşturarak alternatif zincirler yaratabilir ve bu zincirleri ana zincir haline getirebilir.

Ancak saldırganlar şu işlemleri yapamazlar:

- Başka kullanıcıların cüzdanlarına erişerek para çalamazlar.
- Yeni bir coin üretemezler (Rosenfeld, 2014).

Çözüm önerileri olarak şunlar sunulabilir:

- Konsensüs mekanizmasının geliştirilmesi, %51 saldırılarına karşı daha dirençli bir yapı sağlayabilir.
- Proof-of-Stake (PoS) gibi alternatif konsensüs mekanizmaları daha da geliştirilerek saldırılara karşı daha dayanıklı hale getirilebilir.
- Özellikle büyük işlemlerin gerçekleştiği sistemlerde, işlem süresinin uzatılması ve blok onayı sürecinin beklenmesi, çift harcama riskini azaltabilir.

Sonuç olarak, blokzincir teknolojisi kullanıcılarına büyük avantajlar sunmaktadır. Ancak %51 saldırıları ve çift harcama gibi ciddi riskler, sistemdeki zafiyetleri gözler önüne sermektedir. Bu tehditlerin en aza indirilmesi için teknik önlemlerin artırılması ve dağıtık yapının korunması büyük önem taşımaktadır.

2.2.2.5. Sybil Saldırıları

Sybil saldırısı ilk olarak John R. Douceur tarafından 2002 yılında ortaya konmuştur. Bu saldırı türünde, saldırganlar sistem üzerinde birden fazla kimlik oluşturarak bu kimliklerle sistemi kullanır. Bu durum, merkezi olmayan sistemlerde çoğunluğu ele geçirme riski doğurmaktadır (Douceur, 2002; Jetter vd., 2010). Sybil saldırısının en önemli ortaya çıkış nedeni, sistemde kimlik doğrulamasının merkezi bir otoriteye

dayanmaması ve yeni kimlikler oluşturmanın teknik açıdan oldukça kolay olmasıdır (Margolin ve Levine, 2008).

Bu saldırılar çoğunlukla, ağa yeni katılacak katılımcıların kimliklerinin kriptografik olarak doğrulanmadığı, yani merkezi bir kimlik doğrulama mekanizmasının olmadığı sistemlerde görülmektedir. Saldırganlar, kaynaklara erişim sağladıktan sonra ağ içerisindeki karar alma süreçlerini etkilemek amacıyla birçok düğüm oluşturarak, sistemde çoğunlukta oldukları izlenimini vermeye çalışırlar (Levine vd., 2006).

Blokzincir sistemlerinde Sybil saldırıları genellikle doğrulama mekanizmasını ele geçirmeyi hedeflemektedir. Örneğin PoW sisteminde, saldırgan çok sayıda sahte kimlik oluşturarak ağdaki karar alma gücünü ele geçirmeye çalışır. PoS sisteminde ise, sahte kimliklerle hisse miktarı artırılarak sistem manipüle edilebilir ve çift harcama gibi güvenlik zafiyetlerine neden olunabilir (Saleh, 2021).

2.2.2.6. Ağ Yönlendirme Saldırıları (Routing Attacks)

Ağ yönlendirme saldırıları, geleneksel IP tabanlı internet yapılarında gözlemlenmiş, bu yapıların zafiyetlerinden faydalanılarak trafik manipülasyonu gerçekleştirilmiştir (Goldberg, 2014). Bu saldırıların blokzincir gibi eşler arası (P2P) sistemlere uyarlanması, ağlar arasındaki katmanlarda siber sızmaların etkisinin daha fazla hissedilmesine yol açmaktadır (Apostolaki vd., 2017).

Blokzincir teknolojilerinin dağıtık yapısı nedeniyle çok sayıda kimliğin ağ üzerinde sürekli haberleşmesi gerekmektedir. Bu sistemlerde ağ yönlendirme saldırıları gerçekleştiğinde, saldırganlar belirli IP aralıklarını kontrol altına alarak veri trafiğini engelleyebilir. Bu durum, blokzincir sisteminin aksamasına ve gecikmelere neden olabilir.

Bu saldırı türünün bazı teknik gerçekleştirme biçimleri şunlardır:

- **BGP Hijacking (Border Gateway Protocol Hijacking):** Sınır geçidi protokolünün kaçırılması anlamına gelir. En yaygın ağ yönlendirme saldırılarından biridir. Bu saldırıda sistem, bağlı bulunduğu ağa ait olmayan IP aralıklarını duyurarak bu IP'lere giden trafiği kendi üzerine çeker (Pilosov ve Kapela, 2008).
- **Combining Redirect Attack and Eclipse Attack:** Yönlendirme saldırısı ve Eclipse saldırısının birleştirilmiş hâlidir. Bu saldırı sırasında hedef kimliğin tüm bağlantıları kontrol altına alınarak sahte bir ağa yönlendirilir. Yönlendirme seviyesi ile birleştirildiğinde, hedef kimliğin ağdaki görünümü manipüle edilir (Heilman vd., 2015).

- **Partition Attack (Bölme Saldırısı):** Yönlendirme saldırısının bir uzantısıdır. Ağ içerisindeki düğümler, IP seviyesinde ayrılıklar oluşturacak biçimde bölünerek sistemde küresel konsensüsün bozulmasına neden olabilir.

Sonuç olarak, ağ yönlendirme saldırıları blokzincir teknolojisinin altyapısındaki en kritik tehditlerden biridir. Bu saldırılar, ağın doğrulama süreçlerini etkileyerek yalnızca sistemin verimliliğini azaltmakla kalmaz, aynı zamanda güvenlik risklerini de ciddi şekilde artırır. Bu nedenle, ağ yönlendirme saldırılarına karşı çok katmanlı savunma stratejileri geliştirilip uygulanmalıdır.

2.2.2.7. Kullanıcı Cüzdan Saldırıları

Cüzdanlar iki kategoride incelenir: sıcak (hot) cüzdanlar ve soğuk (cold) cüzdanlar. Sıcak cüzdanlar internete bağlı olarak çalışırken, soğuk cüzdanlar çevrimdışı sistemler üzerinde tutulur (Eskandari vd., 2015).

Cüzdan zafiyetlerinin ortaya çıkış sebepleri ve cüzdanlara yönelik saldırıların kaynakları şu şekildedir:

- **Zayıf Anahtar Yönetimi:** Sistemi kullanan kullanıcının özel anahtarlarını yeterince güvenli şekilde kullanamaması ve zayıf anahtarlar oluşturması (Li vd., 2020).
- **Yetersiz Kimlik Doğrulama:** Web tabanlı cüzdanlarda çok faktörlü kimlik doğrulama sistemlerinin eksikliği veya yalnızca tek faktöre dayalı sistemlerin kullanılması (Feng vd., 2019).
- **Zararlı Yazılımlar:** Keylogger, trojan gibi zararlı yazılımlar aracılığıyla özel anahtarların çalınması.
- **Sosyal Mühendislik:** Kimlik avı yöntemiyle sistemdeki kullanıcılara sahte cüzdanlar yönlendirilmesi.
- **Tarayıcı Eklentileri ve Mobil Uygulama Güvenlik Açıkları:** Web tabanlı cüzdanların çeşitli yollarla manipüle edilmesi (Feng vd., 2019).

Blokzincir cüzdanlarına yönelik saldırılar giderek çeşitlenmekte ve yaygınlaşmaktadır. Bu saldırılar, genellikle kullanıcı hataları ve sistemsel zayıflıklar hedef alınarak dijital varlıkların ele geçirilmesini amaçlamaktadır. En yaygın saldırı yöntemleri şu şekildedir:

- **Kurtarma Kelime Avı (Seed Phrase):** Kripto cüzdanlar, kullanıcıların varlıklarını geri yüklemesine imkân tanıyan özel bir yedekleme mekanizmasına sahiptir. Saldırganlar, sahte internet siteleri aracılığıyla kullanıcıları bu kelimeleri paylaşmaya ikna eder. Kelimeler ele geçirildiğinde,

saldırganlar cüzdanı tamamen kontrol altına alabilir. Bu saldırı, en yaygın phishing yöntemlerinden biridir (Bonneau vd., 2015).

- **Panoya Müdahale (Clipboard Hijacking):** Kötü amaçlı yazılımlar, kullanıcıların kopyalayıp yapıştırdıkları cüzdan adreslerini izleyebilir. Özellikle Windows sistemlerinde çalışan bu yazılımlar, kullanıcı bir adres kopyaladığında panoya müdahale ederek bu adresi saldırgana ait olanla değiştirir. Kullanıcı bu değişikliği fark etmediğinden, işlem tamamlandığında varlıklar doğrudan saldırgana gönderilmiş olur (Liao vd., 2016).
- **Sahte Cüzdan Uygulamaları:** Gerçek olmayan uygulama mağazalarında veya sahte web sitelerinde bulunan sahte cüzdan uygulamaları, kullanıcıdan özel anahtarlarını ve kurtarma kelimelerini girmesini talep eder. Bu uygulamalar, gerçek cüzdan arayüzünü taklit ederek kullanıcıların farkına varmadan kandırılmasına yol açar. Genellikle mobil cihazlar, bu tür saldırılara daha çok maruz kalmaktadır (Li vd., 2020).

2.2.3. Güvenlik Güvenliğine Yönelik Çözüm Yaklaşımları

Blokzincir teknolojisi, yapı bakımından merkeziyetsiz ve dağıtık yapısı ile güvenlik konusunda fazlasıyla önemli olmasına rağmen, bazı güvenlik zafiyetlerini de içinde barındırmaktadır. Bu bağlamda sistemin güvenliği için güvenliğe yönelik bazı yaklaşımlar geliştirilmiştir (Conti vd., 2018).

Blokzincir teknolojisinin temel açıdan bakıldığı zaman güvenlik mekanizmasının kriptografiye dayandığı görülmektedir. Merkle ağaçları, dijital imzalar ve hash fonksiyonları gibi kullanılan araçlar veriler için büyük önem taşımaktadırlar. Verinin bütünlüğünü sağlar ve verilerin kimlik doğrulamasını yapmaktadırlar (Narayanan vd., 2016).

Bu kapsamda merkle ağaçları ile sistemdeki verinin bütünlüğü kapsamlı bir şekilde doğrulanır. Bu yöntem ile veri içerisinde çok ufak bir değişiklik yapılması durumunda dahi bütün yapının bozulmasını sağlar (Narayanan vd., 2016). Diğer bir araç ise dijital imzadır, dijital imzalar kullanıldığı zaman kullanıcılar özel bir anahtar ile sitemi imzalarlar. Böylelikle işlemin gerçekleştiğini alanındaki kullanıcı tarafından yapıldığı kolaylıkla doğrulanmaktadır (Zheng vd., 2017). Bir diğer araç ise Hash fonksiyonudur. Bloklarda yer alan veriler hash fonksiyonu ile uzaklıkları sabit olacak şekilde özetlere dönüştürerek bloklar arası bağlantıyı sağlamaktadırlar. Bu yöntem sayesinde veriler üzerinde değişiklik yapmak imkansız hale gelmektedir (Bonneau vd., 2015).

Akıllı sözleşmeler blokzincir sistemi üzerinde otomatik olarak çalışan kodlardır. Fakat yazım hataları yüzünden bazı güvenlik açıklıkları ciddi derecede sistemi risk altına almaktadır (Atzei vd., 2017). Akıllı sözleşmelerin risklerini azaltmak için kod denetimi ve test araçları ile akıllı sözleşmeler dağıtılmadan önce çok önemli testlerden geçerler Mythril ve Oyente gibi araçlar bu testler için kullanılmaktadır (Luu vd., 2016). Akıllı sözleşmelerde formül tabanlı doğrulamalarda sözleşmelerin belirlenen belirli şekilde davranmalarını sağlayarak matematiksel bir doğrulama yöntemi kullanılabilir. Bu yaklaşım sayesinde sistemde beklenmedik olayların önüne geçilebilmesi için büyük katkı sağlar (Bhargavan vd., 2016).

Saldırı tespiti ve önlenmesi, bu sistem ise blokzincir teknolojisinin ağları içerisinde gerçekleşebilecek olası saldırıları klasik ağlardaki sistem gibi tespit edip önüne geçilmelidir. Bununla alakalı olarak Anomali tespit sistemleri makine öğrenmesi gibi sistemlerle normal olmayan beklenmedik olayları tespit edip o farklı davranışları bulabilir. Bu sistem ile blokzincir üzerinde gerçekleşebilecek olan saldırıları önceden algılayıp tespit edebilir (W. Chen vd., 2018). İzleme ve loglama taktiği sistemdeki ağ trafiğinin en derinine kadar incelenmesi ve bunun kayıt altına alınması, sistem için olay sonrası analizler için büyük bir önem taşır (Li vd., 2020).

Blokzincir teknolojisinde yapılmakta olan işlemlerin gerçek olup olmadığı yani gerçekliği dağıtık sistem içerisinde bulunan düğümler tarafında konsensüs algoritmaları tarafından sağlanmaktadır. Bunun için fark güvenlikleri sağlamak için farklı algoritmalar bulunur. PoW algoritması yüksek derecede hesaplama gücü gerektirerek niyeti iyi olmayan girişimler için kullanılır. Genellikle bitcoin gibi kripto paraların olduğu blokzincirlerde kullanılmaktadır (Nakamoto, 2008). PoS algoritması ise %51 saldırılarına karşı dirençli olmak için kullanılmaktadır. Sistemde sahip olunan kripto paraların miktarına göre seçim yapılmaktadır ve enerji verimliliğini de yanında sağlamaktadır (Saleh, 2021). Bir diğer algoritma ise PBFT algoritması, bu algoritma genellikle özel olan blokzincir sistemlerinde kullanılmaktadır. Ağ üzerindeki bazı düğümlerin hata yapmasına ve kötü niyetli olsa bile sistemin çalışmasını sağlamaktadır (Castro ve Liskov, 2002).

Blokzincir teknolojisindeki kullanıcıların kimliklerini ve erişimlerini sağlamak için, kimlik ve erişim sistemi kullanılmaktadır. Merkezi olmayan kimlik sistemleri (DID), bu sistem kullanıcı gizliliğini koruyarak kullanıcının kendi kimlik bilgileri üzerinde değişiklik yapmayı ve bilgileri yönetmesini sağlamaktadır (Sedlmeir vd., 2021). Erişim kontrolü (ACL) bu sistem kimlik sahiplerin hangi verilere erişim sağlayabileceklerini bu sistem aracılığı ile belirlemektedir. Genellikle izinli blokzincirlerde kullanılır (Zyskind vd., 2015).

Kuantum tabanlı bilgisayarların klasik kriptografik olan algoritmalarını kırabilme ihtimalini öngörmekte, bunun için kuantuma dirençli olan algoritmalar, kuantum güvenli yaklaşımları geliştirmektedirler (Alagic vd., 2022). Kuantum bilgisayarlar karşı güvenli, dayanıklı olduğu düşülmekte olan Lattice tabanlı algoritmalar gelecek için önemli yerlerde görülmektedir (L. Chen vd., 2016).

2.2.4. Blokzincir Zafiyetlerinin Sosyal Medyadaki Yansımaları

Blokzincir teknolojisi ile alakalı güvenlik zafiyetleri, sosyal medya üzerinde önemli sayılacak yankıları bulunmakta bunun yanı sıra hem toplumsal düzey olsun hem de teknik açıdan olsun önemli izler bırakmaktadır.

Blokzincir teknolojilerinin güvenlik zafiyetleri, sosyal medya üzerinde çeşitli yolardan ortaya çıkmaktadır. Kullanıcılar, sistem üzerinde karşılaştıkları sorunları sosyal medyada paylaşarak diğer kullanıcılara bilgi amaçlı olarak yazabiliyorlar (L. Wang vd., 2023). Bu konular üzerinde çalışma yapan blokzincir geliştiricileri de tespit ettikleri güvenlik zafiyetlerini ve bununla birlikte alınan önlemleri sosyal medya üzerinde paylaşarak kullanıcıları bilgilendirmektedirler (He vd., 2025).

Akıllı sözleşmelerde bulunan güvenlik zafiyetleri sosyal medya platformu olan X (eski adı ile twitter) üzerinde hızla artan tartışmalara yer olmaktadır. Özellikle buna benzer zafiyetler ve meydana gelen finansal düşüşler, kayıplar kullanıcılarda sıkıntı yaratmaya ve bu tarz platformlara olan güvenleri zedelenmektedir (Zhao, 2025).

Kimlik avı saldırıları, blokzincir teknolojisinde güvenlik zafiyetleri arasında en önemli tehditlerden bir olarak karşımıza çıkmaktadır. Genellikle sistemdeki kişilerin özel anahtarlarının çalınması ile gerçekleşen bu tür saldırılar sonucu kullanıcıların güveni sarsılmakta ve sosyal medya platformları üzerinde büyük bir yankı yaratmaktadır (coinmarketcap.com, 2025).

Blokzincir teknolojisinin temelinde olan karmaşık yapısı yüzünden sosyal medya platformları üzerinde bilgi kirliliği de oldukça fazla görülmektedir. Bunu fırsata çevirmek isteyen kötü niyetli kişiler sosyal medyayı kullanarak yanlış bilgi ve haberleri yayarak kullanıcıların yanlış işlemler yanlış kararlar almalarına yol açabilmektedir (He vd., 2025).

Blokzincir teknolojisinde çıkmakta olan zafiyetler sosyal medya platformlarında hızlıca yayılmakta ve bunun akabinde teknolojiye olan güven birde ekonomik dinamikler dolaylı olarak etkilenmektedir. Aynı zamanda sosyal medya platformları kullanıcılara bilgi vermek için güzel bir bilgi paylaşım merkezi haline de gelmektedir. Bu yüzden sosyal medya platformları farkındalık yaratmakta, yanlış bilinen bilgilerle mücadele

etmek ve sistem ile olana teknik düzeyleri en üste çıkarmak için önemli bir yere sahiptir (L. Wang vd., 2023; Zhao, 2025).

3. DOĞAL DİL İŞLEME KAVRAMLARI VE İLGİLİ LİTERATÜR TARAMASI

Bu bölümde doğal dil işleme kavramları olan veri madenciliği, metin madenciliği ve konu modelleme çeşitlerinden bahsedilecektir. Ayrıca konularla alakalı olarak ayrı ayrı literatür taramasına yer verilecektir.

3.1. Veri Madenciliği

Veri madenciliği, büyük ve devasa verilerden anlamlı, faydalı bilgilerin ve daha önceden bilinmesi zor olan bilgilerin otomatik yöntemlerle elde edilmesi sürecidir (Frawley vd., 1992). Bu süreçte veri madenciliği, yapay zekâ, makine öğrenmesi, veri tabanı ve istatistik gibi birçok alanın birleşiminde yer almaktadır (Han vd., 2022).

Veri madenciliği, ilk olarak 1990'ların başlarında kullanılmaya başlanmıştır. Ancak kavram olarak daha eskiye dayanır. 1960'lı yıllarda bilgisayarlarla birlikte veri analizi çalışmalarına kadar uzanabilir. O dönemlerde "örüntü tanıma" olarak adlandırılan bu çalışmalar, bilgisayarların işlem gücünün gelişmesiyle birlikte zaman içerisinde "data mining" olarak adlandırılmıştır (Witten vd., 2005).

Veri madenciliği, büyük veriler içerisinde ilerleyen zamanlardaki süreçleri tahmin etmemizi sağlar ve bu tahminlerin anlamlı, yararlı ve belirli kurallar çerçevesinde programlar aracılığıyla analiz edilmesini içerir (Coşlu, 2013). Bunun yanı sıra, veri madenciliği büyük veri kümeleri içerisindeki verileri ilişkilendirerek inceler ve veriler arasındaki bağlantıların bulunmasına yardımcı olur. Ayrıca, veri tabanı sistemi içerisinde gizli kalmış bilgilerin açığa çıkarılmasına katkı sağlayan bir veri analizi tekniğidir (Savaş vd., 2012).

Veri madenciliği, yalnızca verilerin işlenmesi ile oluşan bir analiz değildir. Bunun yanında sistematik bir süreç de içerir. Bu süreçler; veri ön işleme, veri entegrasyonu, veri seçimi, veri dönüştürme, veri madenciliği, örüntü değerlendirme ve bilginin sunumu gibi birkaç temel aşamadan oluşmaktadır (Han vd., 2022).

Veri temizleme aşamasında, verilerin analize uygun hâle getirilmesi sağlanır. Eksik veya hatalı bilgiler varsa bu bilgiler düzeltilir, eksik veriler tamamlanır, tutarsız veriler düzenlenir ve gereksiz veriler çıkarılır (Han vd., 2022).

Veri entegrasyonu, farklı kaynaklardan elde edilen verilerin birleştirilmesini ifade eder. Analiz için farklı yerlerden gelen veriler bir araya getirilerek tek bir bütünsel yapı oluşturulur. Veri entegrasyonu, büyük veri sistemlerinde önemli bir yere sahiptir çünkü farklı sistemlerden gelen verilerin biçim olarak uyumlu olması gerekmektedir (Kimball ve Ross, 2013).

Veri seçimi aşamasında, tüm veriler yerine yalnızca analizin amacına uygun olan veri kümesinin kullanılması sağlanır. Bu sayede yük azalır ve daha anlamlı sonuçlar elde edilir (Han vd., 2022).

Veri dönüştürme aşamasında, veriler veri madenciliği için uygun formata dönüştürülür. Bu süreçte öznitelik oluşturma işlemleri de gerçekleştirilir (Han vd., 2022).

Veri madenciliği aşaması, sürecin en önemli kısmıdır. Bu aşamada algoritmalar kullanılarak örüntüler ortaya konur, ilişkiler ve tahminler elde edilir. Sınıflandırma, kümeleme, regresyon gibi teknikler bu aşamada uygulanır (Witten vd., 2005).

Örüntü değerlendirme aşamasında, elde edilen örüntülerin anlamlı olup olmadıkları ve kullanılabilirlikleri değerlendirilir (Han vd., 2022). Bu aşamada eşik değerlere göre değerlendirme yapılır (P.-N. Tan vd., 2016).

Bilginin sunumu son aşamadır. Bu aşamada elde edilen bilgiler sunulacak şekilde raporlanır, görselleştirilir, tablolar hâline getirilir ve anlaşılır bir biçimde sunulur (Han vd., 2022).

Sonuç olarak baktığımızda, veri madenciliği verilerle yapmış olduğumuz analizlerin bilgiye dayalı karar almayı mümkün hâle getiren bir analiz aracıdır. Gelişen teknoloji dünyası ile birlikte veri madenciliği yöntemi daha da güçlü hâle gelmektedir. Bunun yanında yapay zekâ ve makine öğrenmesi gibi yöntemler, daha iyi sonuçlar almamızı sağlamaktadır. Şekil 4'te de görüldüğü üzere, veri madenciliğinin, gelişen teknoloji ile daha geniş ve etkili alanlara sahip olacağı görülmektedir (Kantardzic, 2011).

Şekil 4. Veri Madenciliğini Oluşturan Disiplinler (Özbay, 2015)

3.2. Metin Madenciliği

Metin madenciliği doğal dilde kaleme alınmış olan metinler içerisinde anlamlı analizler çıkartmamıza ve gizli olan bilgileri elde etmeyi sağlayan bir analiz süreci olarak tanımlanabilir (A.-H. Tan, 1999). Bu süreç, doğal dil işlemenin yanı sıra makine öğrenmesi ve istatistik gibi alanların birbiriyle entegre olmasıyla oluşmaktadır (Hotho vd., 2005).

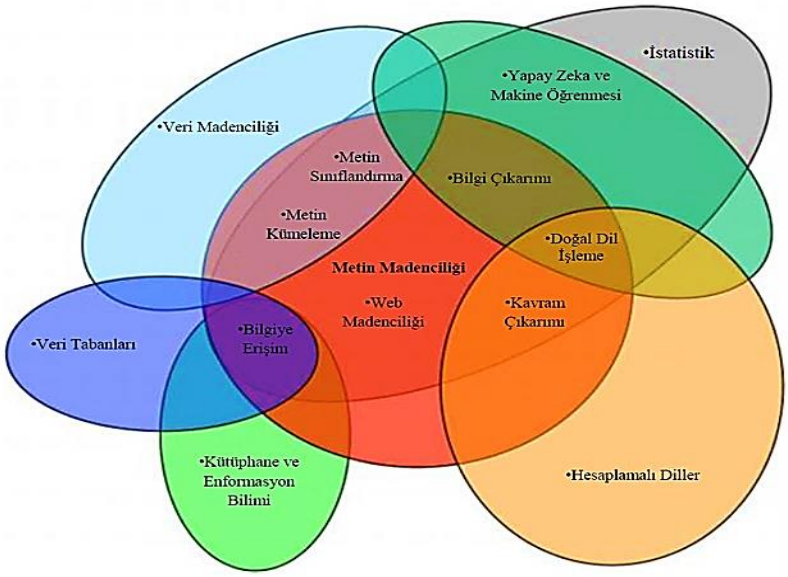
Veri madenciliğinin bir alt dalı olarak değerlendirilen metin madenciliğinin, veri madenciliğinden ayrılan özelliği; yapısal olmayan verilerle de analiz yapabilmesidir (Hearst, 1999). Bunun sebebi, metin madenciliğinde sözcük öbeklerinin köklerine inilmesi, durak kelimelerin çıkarılması ve metinlerin temizlenmesi gibi aşamalardan oluşmasıdır (Sebastiani, 2002).

Metin madenciliğinin bu kadar ön planda tutulmasının nedeni, dijital ortamların artmasından kaynaklanmaktadır. Sosyal medya ortamlarında üretilen içeriklerin çoğu, veri tabanını oluşturmakta ve bu verilerin yapılandırılmamış olması metin madenciliğinin yaygınlaşmasına olanak sağlamaktadır (Cambria ve White, 2014).

Bu uygulama alanları, metin madenciliği ile diğer altı alanın kesişim noktalarını temsil etmektedir. Metin madenciliğinin yedi uygulama alanı şu şekilde özetlenebilir (Şekil 5):

- **Arama ve Bilgi Erişimi (IR):** Anahtar kelime araması ve arama motorları da dâhil olmak üzere, metin belgelerinin depolanması ve erişilmesi süreçleri;

- **Belge Kümeleme:** Veri madenciliği kümeleme tekniklerini kullanarak, kelimeler (terimler), cümleler, paragraflar veya belgelerin gruplandırılması ve kategorize edilmesi;
- **Belge Sınıflandırma:** Etiketlenmiş örnekler üzerinde eğitim almış modellere dayalı olarak, veri madenciliği sınıflandırma yöntemlerini kullanarak cümlelerin, paragrafların veya belgelerin gruplandırılması ve kategorize edilmesi;
- **Web Madenciliği:** İnternet üzerindeki veri ve metinlerin madenciliği; özellikle web'in geniş ölçeği ve bağlantısallığı üzerinde odaklanılması;
- **Bilgi Çıkarımı (IE):** Yapılandırılmamış metinden ilgili gerçeklerin ve ilişkilerin tespit edilmesi ve çıkarılması; yapılandırılmamış ve yarı yapılandırılmış metinlerden yapılandırılmış veri oluşturma süreci;
- **Doğal Dil İşleme (NLP):** Düşük seviyeli dil işleme ve anlama görevleri (örneğin, konuşma bölümlerinin etiketlenmesi); genellikle hesaplamalı dilbilim ile eşanlamlı olarak kullanılır;
- **Kavram Çıkarımı / Topik Modelleme:** Anlamsal olarak benzer kelime ve ifadelerin gruplandırılması (Miner vd., 2012)



Şekil 5. Yedi Metin Madenciliği Uygulama Alanı, Metin Madenciliğinin Altı İlgili Alanıyla Ana Kesişme Noktaları (Miner vd., 2012)

Günümüze baktığımızda, metin madenciliği duygu analizi, konu modelleme analizleri, sosyal medya üzerinde yapılan içerik analizleri ve müşteri yorumlarının değerlendirilmesi gibi birçok alanda en etkili araçlardan biri hâline gelmiştir. Türkçe metin madenciliğinin son yıllarda oldukça sık kullanıldığı görülmektedir. Bunun nedeni,

özellikle haber metinleri ve sosyal medya içeriklerindeki yorumlar üzerinde yapılan çalışmalar sayesinde, metinlerin daha anlaşılır ve sistematik şekilde analiz edilebilmesidir.

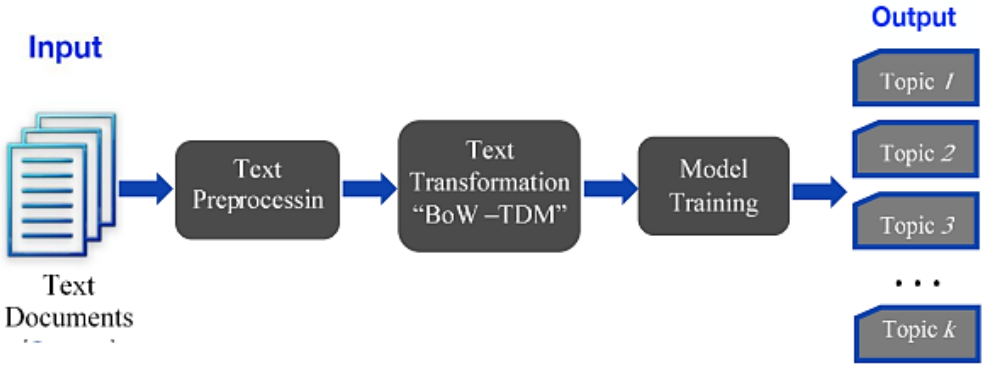
3.3. Konu Modelleme

Konu modelleme, büyük metin koleksiyonlarında belgeler arasında saklı olan tematik yapıların bilgisayar ortamında keşfedilmesini amaçlayan istatistiksel bir yöntemdir (Blei vd., 2003). Bu teknik, doğal dil işleme ve metin madenciliği alanlarının kesişiminde yer almakta; belgeleri oluşturan veriler içerisindeki konuları belirleyerek verinin içeriği hakkında özetleyici bilgiler sunmaktadır (Steyvers ve Griffiths, 2007).

Konu modelleme, özellikle günümüz büyük veri çağında; internet üzerinde yer alan haber içerikleri, sosyal medya platformlarında paylaşılan metinler gibi büyük veri yığınlarının analizinde bizlere yardımcı olmaktadır (Boyd-Graber vd., 2017). Bu tür büyük verilerin çoğu yapılandırılmamış olduğundan doğrudan analiz edilmeleri oldukça zordur. Bu noktada konu modelleme, veriler içerisindeki metinlerde gizli olan temaları ve anahtar kelimeleri otomatik olarak ortaya çıkarır. Metinleri sınıflandırma, özetleme ve bilgi çıkarımı gibi işlemlerde de büyük kolaylık sağlar (Feldman ve Sanger, 2007; Sharma vd., 2022).

Konu modelleme yönteminin temelinde, elimizdeki bir belgenin birden fazla konuya sahip olabileceği düşüncesi yer alır. Her bir konunun ise belirli bir kelime dağarcığına sahip olduğu kabul edilir. Bu durum, özellikle olasılıksal konu modelleme yöntemlerinin temelini oluşturmaktadır (Blei, 2012).

Şekil 6'da, metin madenciliği süreci içinde yer alan konu modelleme sürecinin temel adımları gösterilmektedir. Bu adımlar, analiz ve çıktı aşamalarında kullanılan modele bağlı olarak bazı farklılıklar gösterebilmekle birlikte, genellikle aynı kavramsal dizini içermektedir.



Şekil 6. Konu Modelleme Süreci (Ekin ve Algabsi, 2024)

Konu modelleme yöntemlerinin çeşitli türleri bulunmaktadır. Bunlar:

- **Latent Semantic Analysis (LSA)** – Gizli Anlamsal Analiz
- **Latent Dirichlet Allocation (LDA)** – Gizli Dirichlet Tahsisi
- **Non-negative Matrix Factorization (NMF)** – Negatif Olmayan Matris Faktörizasyonu
- **Dynamic Topic Models (DTM)** – Dinamik Konu Modellemeleri

Latent Semantic Analysis (LSA) – Gizli Anlamsal Analiz: Konu modelleme yöntemleri arasında öncülerden biri olan LSA, kelime-belge matrisini Tekil Değer Ayrıştırması (SVD) yöntemiyle çözümlemeye çalışır. Bu yöntem, belgeler içerisinde kelimeler arasındaki anlamsal ilişkileri ortaya koymayı amaçlar (Deerwester vd., 1990).

Latent Dirichlet Allocation (LDA) – Gizli Dirichlet Tahsisi: En yaygın kullanılan konu modelleme yöntemlerinden biridir (Blei vd., 2003). LDA, her bir belgenin birden fazla konudan oluştuğunu ve her bir konunun da çeşitli kelimelerden meydana geldiğini varsayan olasılıksal bir modeldir. LDA; sosyal medya analizlerinden hukuk metinlerine, akademik literatür taramalarından çeşitli dijital içeriklerin analizine kadar birçok alanda yaygın olarak kullanılmaktadır (Blei, 2012).

LDA'nın çalışma mantığı şu şekildedir: Her bir belge, Dirichlet dağılımından türetilmiş bir konu karışımı içerir. Her bir konu da yine Dirichlet dağılımı aracılığıyla belirli kelimelerden oluşur. Bu yapısıyla hem belgeler hem de kelimeler arasında yüksek boyutlu ilişkiler kurulmasına olanak sağlar. Böylece belgeler üzerinde anlamlı gruplamalar ve analizler yapılabilmektedir (Griffiths ve Steyvers, 2004).

Non-negative Matrix Factorization (NMF) – Negatif Olmayan Matris Faktörizasyonu: NMF, konu modelleme tekniklerinden biri olarak öne çıkmaktadır. Bu yöntem, veride bulunan değerlerin negatif olmaması koşuluyla belgeleri daha düşük boyutlu matrislere ayırarak içerdikleri gizli konuları ortaya çıkarır (Lee ve Seung, 1999).

Dynamic Topic Models (DTM) – Dinamik Konu Modellemeleri: Bu yöntem, zaman içinde değişim gösteren konuları analiz etmek amacıyla geliştirilmiştir. Belgelerin yayımlandığı yıllara göre zamanla konuların nasıl evrildiğini ortaya koyar. Özellikle haber arşivleri ve zaman serisi biçiminde düzenlenmiş metin koleksiyonları için oldukça uygun bir yöntemdir (Blei ve Lafferty, 2006).

3.3.1. LDA (Gizli Dirichlet Tahsisi) Yöntemi

LDA modeli, ilk olarak 2003 yılında David M. Blei, Andrew Y. Ng ve Michael I. Jordan tarafından ortaya atılmıştır (Blei vd., 2003). Bu modelin geliştirilme amacı, metin

koleksiyonları üzerindeki gizli konu yapılarını ortaya çıkarmak ve metinler içerisindeki farklı konuları belirlemektir. LDA modeli, daha önce geliştirilen Karışım Dirichlet modeli ve pLSA (Probabilistic Latent Semantic Analysis) modellerinden esinlenerek oluşturulmuştur (Hofmann, 1999).

LDA modelinin tanıtılmasının ardından, Griffiths ve Steyvers 2004 yılında yaptıkları çalışmada bu modeli Gibbs örnekleme yöntemi ile uygulayarak, büyük veri üzerinde daha etkili bir şekilde çalışmasını sağlamışlardır. Bu sayede LDA'nın verimliliği artmış ve metin madenciliği alanında yaygın olarak kullanılmasına olanak tanımıştır (Griffiths ve Steyvers, 2004).

LDA, herhangi bir belgenin belirli oranlarda birden çok konudan oluşabileceğini varsayan bir olasılıksal modeldir. Bu model, elimizdeki belgeleri kelime dağılımlarına göre uygun konulara ayırarak belgeler arasındaki gizli yapının ortaya çıkmasına yardımcı olur (Blei vd., 2003). LDA, doğal dil işleme ve veri madenciliği alanlarında gizli konuları belirlemek amacıyla yaygın olarak kullanılan konu modelleme yöntemlerinden biridir. Özellikle büyük metin koleksiyonlarında gözle görülmesi zor konuları tespit etmek için olasılıksal bir yaklaşım benimser (Blei vd., 2003).

LDA modeli birçok alanda kullanılan güçlü bir yöntemdir. Bu kullanım alanlarını şu şekilde sıralayabiliriz:

- **Metin Sınıflandırması:** Elimizdeki belgelerin belirli konulara göre sınıflandırılmasını sağlar (Blei, 2012).
- **Özetleme ve Bilgi Çıkarımı:** Büyük metinlerin içerisindeki önemli bilgilerin ayrıştırılmasında etkilidir (Boyd-Graber vd., 2017).
- **Öneri Sistemleri:** Kullanıcıların okudukları makaleler, tezler veya yaptıkları araştırmalar doğrultusunda ilgilerini çekebilecek yeni içerikler önerir (Jelodar vd., 2019).
- **Sahte Haber Tespiti:** Haber metinleri arasındaki konu dağılımlarını analiz ederek sahte haber olup olmadığını belirlemeye yardımcı olur (Shu vd., 2017).
- **E-Ticaret ve Dijital Platformlar:** Amazon veya Netflix gibi platformlarda, kullanıcıların alışveriş veya izleme geçmişlerine göre kişiselleştirilmiş öneriler sunmak için kullanılır (C. Wang ve Blei, 2011).
- **Sosyal Medya Analizi:** Twitter gibi platformlardaki gönderileri analiz ederek, kullanıcıların neye yoğunlaştığını veya hangi konuların trend olduğunu belirlemede kullanılır (L. Hong ve Davison, 2010).
- **E-Ticaret Ürün Önerileri:** Kullanıcının ilgi alanlarına uygun ürün önerileri sunmak için de LDA modeli tercih edilir (Blei ve Lafferty, 2007).

- **Bilgi Getirme Sistemleri:** Belgeler arasındaki benzerliklerin belirlenmesi ve bu sayede bilgiye erişimin daha etkili hale getirilmesi sağlanır (Ramage vd., 2010).

Tablo 2. LDA modelinin kullanım alanları

LDA	Belge Kümesi Analizi	Anahtar Konuların Belirlenmesi
	Doğal Dil İşleme (NPL)	Metin Sınıflandırma ve Kümeleme
	İçerik Öneri Sistemleri	Benzer İçerikleri Önerme
	Sosyal Medya Analizi	Gümdemdeki Konuları Belirleme

LDA, bir metin derlemesini üretken bir olasılıksal model olarak ele alır. Temel fikir; belgelerin, kelimeler üzerinde olasılıksal dağılımlarla tanımlanan gizli konuların rastgele karışımları şeklinde temsil edilmesidir (Blei vd., 2003).

LDA modeli, bir derleme D içindeki her belge w için aşağıdaki üretim sürecini varsayar:

1. N ~ Poisson (ξ)'u seçilir.
2. θ ~ Dir(α) seçilir.
3. N kelimenin her biri için:
   (a) zn ~ Multinomial(θ) seçilir.
   (b) wn, p (wn | zn, β) olasılığına göre seçilir. Burada zn, konuya bağlı olarak belirlenen çok terimli (multinomial) bir dağılımdır.

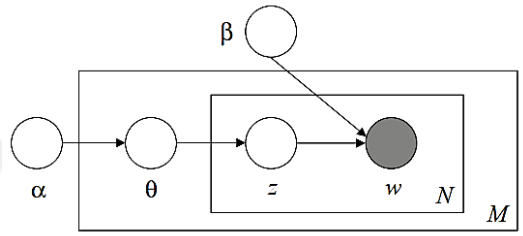
Bu temel modelde bazı basitleştirici varsayımlar yapılmıştır. İlk olarak, Dirichlet dağılımının k boyutluluğunun bilindiği ve sabit olduğu varsayılır. İkinci olarak, kelime olasılıkları k ×V matris β ile parametrelendirilir; burada βi j = p (wj = 1|zi = 1), şimdilik tahmin edilecek sabit bir miktar olarak ele alınmaktadır. Son olarak, Poisson varsayımı bundan sonraki hiçbir şey için kritik değildir ve gerektiğinde daha gerçekçi belge uzunluğu dağılımları kullanılabilir. Ayrıca, N'nin diğer tüm veri üreten değişkenlerden (θ ve z) bağımsız olduğunu unutmayın. Bu nedenle yardımcı bir değişkendir ve sonraki gelişmelerde genellikle rastlantısallığını göz ardı edeceğiz. Bir k-boyutlu Dirichlet rastgele değişkeni θ (k-1)-simpleksinde değerler alabilir (θi ≥ 0, ∑ik=1 θi = 1 ise bir k-vektörü θ (k -1)-simpleksinde yer alır) ve bu simpleks üzerinde aşağıdaki olasılık yoğunluğuna sahiptir:

$$p(\theta \mid \alpha) = \frac{\Gamma\left(\sum_{i=1}^{k} \alpha_i\right)}{\prod_{i=1}^{k} \Gamma(\alpha_i)} \theta_1^{\alpha_1 - 1} \cdots \theta_k^{\alpha_k - 1}$$

Burada α parametresi αi > 0 bileşenlerine sahip bir k-vektörüdür ve Γ(x) Gamma fonksiyonudur. Dirichlet dağılımı, simpleks üzerinde tanımlıdır, üstel aileden gelir, sonlu boyutlu yeterli istatistiklere sahiptir ve multinom dağılımın eşleniğidir.

α ve β parametreleri göz önüne alındığında, bir konu karışımı θ, bir N konu kümesi z ve bir N kelime kümesi w'nin ortak dağılımı şu şekilde verilir:

$$p(\theta, \mathbf{z}, \mathbf{w} \mid \alpha, \beta) = p(\theta \mid \alpha) \prod_{n=1}^{N} p(z_n \mid \theta) p(w_n \mid z_n, \beta)$$



Şekil 7. LDA'nın grafiksel model gösterimi

Bu grafiksel modelde kutular, tekrar eden yapıları (plaka) temsil eder. Dıştaki plaka belgeleri, içteki plaka ise bir belgedeki tekrarlanan konu ve kelime seçimlerini gösterir.

Bu yapıda, p (zn |θ), zni = 1 olacak şekilde benzersiz i için basitçe θi'dir. θ üzerinden integral alarak ve z üzerinden toplayarak bir belgenin marjinal dağılımı elde edilir:

$$p(\mathbf{w} \mid \alpha, \beta) = \int p(\theta \mid \alpha) \left(\prod_{n=1}^{N} \sum_{z_n} p(z_n \mid \theta) p(w_n \mid z_n, \beta) \right) d\theta.$$

Son olarak, tek tek belgelerin marjinal olasılıklarının çarpımını alarak bir derlemin olasılığı elde edilir:

$$p(D \mid \alpha, \beta) = \prod_{d=1}^{M} \int p(\theta_d \mid \alpha) \left(\prod_{n=1}^{N_d} \sum_{z_{dn}} p(z_{dn} \mid \theta_d) p(w_{dn} \mid z_{dn}, \beta) \right) d\theta_d.$$

LDA modeli Şekil 7'de olasılıksal bir grafik model olarak gösterilmektedir. Şekilden de anlaşılacağı üzere, LDA gösteriminin üç seviyesi vardır. α ve β parametreleri, derlem oluşturma sürecinde bir kez örneklendiği varsayılan derlem seviyesi parametreleridir. θd değişkenleri belge düzeyinde değişkenlerdir ve belge başına bir kez

örneklenirler. Son olarak, zdn ve wdn değişkenleri kelime düzeyinde değişkenlerdir ve her belgedeki her kelime için bir kez örneklenir. LDA'yı basit bir Dirichlet-multinomial kümeleme modelinden ayırmak önemlidir. Klasik bir kümeleme modeli, bir Dirichlet'in bir derlem için bir kez örneklendiği, çok terimli bir kümeleme değişkeninin derlemdeki her belge için bir kez seçildiği ve küme değişkenine bağlı olarak belge için bir dizi kelimenin seçildiği iki seviyeli bir model içerir. Birçok kümeleme modelinde olduğu gibi, böyle bir model bir belgenin tek bir konuyla ilişkilendirilmesini kısıtlar. Öte yandan LDA üç seviye içerir ve özellikle konu düğümü belge içinde tekrar tekrar örneklenir. Bu model altında, belgeler birden fazla konuyla ilişkilendirilebilir. (Blei vd., 2003)

LDA'da, kelimelerin konular tarafından üretildiğini (sabit koşullu dağılımlarla) ve bu konuların bir belge içinde sonsuza kadar değiştirilebilir olduğunu varsayıyoruz. De Finetti'nin teoremine göre, bir dizi kelime ve konunun olasılığı şu şekilde olmalıdır:

$$p(\mathbf{w},\mathbf{z}) = \int p(\theta)\left(\prod_{n=1}^{N} p(z_n|\theta)p(w_n|z_n)\right)d\theta$$

Burada θ, konular üzerinde çok terimli bir rasgele parametredir. Konu değişkenlerini marjinalleştirerek ve θ'ya bir Dirichlet dağılımı vererek belgeler üzerindeki LDA dağılımı elde edilir.

LDA Modelinin Avantajları;

Yorumlanabilir sonuçlar sunması: LDA, olasılıksal bir model olduğu için analiz sonuçları yorumlanabilir ve mantıklı bir yapıya sahiptir. Model, verilerdeki gizli konuları belirlerken her kelimenin hangi konuya ait olabileceğine dair olasılık hesaplamaları yapar. Bu da elde edilen çıktıları açıklanabilir kılar (Blei vd., 2003).

Büyük veri setleriyle çalışma kapasitesi: LDA, büyük ve karmaşık metin verileri üzerinde çalışırken yüksek verimlilik sağlayan algoritmalara sahiptir. Veri hacmi arttıkça modelin performansını koruyabilmesi, özellikle büyük veri analizlerinde önemli bir avantaj sunar (Griffiths ve Steyvers, 2004).

Farklı alanlara kolayca uyarlanabilir olması: Modelin esnek yapısı, doğal dil işleme, pazarlama analizi ve sosyal bilimler gibi çok çeşitli alanlarda etkili bir şekilde kullanılmasını sağlar. Bu çok yönlülük, modelin hem akademide hem de sektörde yaygın olarak benimsenmesini mümkün kılar (Blei ve Lafferty, 2007).

LDA Modelinin Dezavantajları;

Konu sayısının önceden belirlenmesi gerekliliği: LDA'da model çalıştırılmadan önce konu sayısının kullanıcı tarafından belirlenmesi gerekir. Ancak bu sayının doğru seçilmemesi durumunda, modelin çıktıları anlamlı olmayabilir ve yetersiz genellemelere neden olabilir (Blei vd., 2003).

Hesaplama maliyetinin yüksek olması: Büyük veri setleriyle çalışıldığında, modelin hesaplama maliyeti artabilir. Veri boyutu büyüdükçe model parametrelerinin güncellenmesi daha fazla işlem gücü ve zaman gerektirir. Bu durum, LDA'nın pratik uygulamalarında bir dezavantaj oluşturabilir (Griffiths ve Steyvers, 2004).

Ön işleme adımlarına duyarlılık: LDA'nın başarılı ve anlamlı sonuçlar üretmesi, metinlerin ön işleme kalitesine bağlıdır. Durak kelimelerin (stop words) çıkarılması, noktalama işaretlerinin temizlenmesi ve gereksiz bağlaçların ayıklanması gibi işlemler modelin doğruluğu açısından kritiktir. Eksik veya hatalı ön işleme, modelin kalitesini düşürebilir (Ramage vd., 2010).

3.4. İlgili Literatür Taraması

Bu bölümde, konu modelleme teknikleri ve özellikle LDA (Latent Dirichlet Allocation) yöntemi ile ilgili literatür incelenecek; ayrıca blokzincir teknolojisindeki güvenlik zafiyetleri ile bu zafiyetlerin konu modelleme yöntemleriyle analizine ilişkin çalışmalara da yer verilecektir. Amaç, konu modelleme yöntemlerinin blokzincir güvenlik açıklarının tespiti ve sınıflandırılması gibi alanlardaki kullanımını ortaya koymak ve mevcut literatürdeki yaklaşımları değerlendirmektir.

3.4.1. Konu Modelleme ile İlgili Literatür Çalışmaları

(Bozan ve Altun, 2023), bu çalışma otomotiv sektörü üzerinde faaliyet göstermekte olan bir firmanın çalışan önerileri üzerine konu modelleme yöntemiyle bir analiz yapmayı amaçlamaktadır. Metin tabanlı olan bu öneriler, metin madenciliği teknikleri için elverişli bir çalışma sunmaktadır. Çalışma 2021 yılında 2844 satır üzerinde LDA yöntemi ile kategorilere ayrılmıştır. Makalede birde doğal dil işleme yöntemleri, öznitelik seçimleri, TF-IDF hesaplamaları modelleme sürecinde anlatılmaktadır.

(Kaya ve Gülbandılar, 2022), bu çalışmada metin madenciliği için önemli bir yere sahip olan konu modelleme yöntemlerinin karşılaştırılmasının analizi yapmaktadır. LDA, İKM, YMK yöntemleri aynı veri kümesi üzerinde uygulanmıştır. Çalışma çapraşıklık, konu tutarlılığı ölçütleri üzerinde çalışılmıştır. Kullanılan veri kümesi 2019 yılında Roberts tarafından oluşturulmuş olan "poliblog5k" veri setidir. Bu seti R programlama

dili ile ilgili kütüphaneyi kullanarak uygulanmıştır. Analizler sonucu çapraşıklık açısından çıkan en iyi sonuç YKM yöntemi ile çıkmıştır ve GDA yöntemi modelleme süresinin kısalığına göre daha düşük performans göstermiştir. İKM yöntemi ise konu modelleyebilme açısında avantaj sağlasa da işlem süresi bakından çok fazladır.

(Kherwa ve Bansal, 2020), yapılan bu çalışma konu modelleme üzerine yapılan kapsamlı bir literatür taramasıdır. Yazarlar bu makale için 2003ila 2018 yıllarında yayımlanan yaklaşık olarak 300 makaleyi analiz ederler. Öte yandan LDA modelinin çeşitli uzantılarını (CTM, DTM, STM) tanımlamış ve farklı alandaki uygulamaları değerlendirmişlerdir. Bu çalışmada konu modelleme yöntemlerinin sayısal olarak değerlendirilmesini de yapmışlardır. Özellikle de kullanılan büyük verileri için şematik temaların açıklanması açısından etkili sonuçlar verdiğine değinilmiştir. Bunun yanında bu çalışma birde konu modelleme karşılaştığı temel zorlukları da ele almış ve gelecek için yapılacak olan çalışmalara öneriler sunmuştur.

(O'Callaghan vd., 2015), bu çalışma verilerden elde edilen konuların anlamsal tutarlığı üzerine bir çalışma yapmaktadır. LDA modeli ile NMF modeli karşılaştırılmıştır. Çalışmada 3 fark konu tutarlığı kullanılmış olup bu ölçütlerden 2 tanesi NMF modelinin LDA modeline kıyasla daha tutarlı yorumlar yapılabilir konular ürettiğini göstermektedir. Bunun yanında ise LDA modeli ile elde edilen konuların daha genel daha sık kullanılan terimleri içerdiği saptanmıştır. Çalışma sadece konu modelleme değerlendirmesinde sayısal ölçütlerin değil aynı zamanda anlamsal bütünlük değerlerini de incelenmesi gerektiğini savunmaktadır.

3.4.2. LDA ile İlgili Literatür Çalışmaları

(Blei vd., 2003), çalışmalarında, Latent Dirichlet Allocation (LDA) adlı olasılıksal konu modelleme yöntemi tanıtılmaktadır. LDA, geniş metin koleksiyonlarını incelemek ve belgeler arasındaki ilişkileri belirlemek için tasarlanmış bir modeldir. Bu yaklaşım, her belgeyi belirli konuların bir kombinasyonu olarak ele alır ve her konu, belirli kelimeler üzerinde olasılık dağılımı sergiler. Çalışmanın ana hedefi, LDA'nın metin madenciliği ve bilgi çıkarımı alanındaki etkinliğini analiz etmektir.

Makalede, LDA'nın temel varsayımları ve matematiksel yapısı ayrıntılı bir şekilde incelenmiştir. LDA'nın, Latent Semantic Indexing (LSI) ve Probabilistic Latent Semantic Indexing (pLSI) gibi diğer yöntemlerle karşılaştırılması da yapılmaktadır. LDA, her belgenin birden fazla konu içerebileceği varsayımına dayanırken, pLSI ve LSI belirli sınırlamalarla karşılaşmaktadır. Araştırma, LDA'nın gizli değişkenler için değişken türevleri ve EM algoritması gibi yöntemler kullanarak daha başarılı sonuçlar elde ettiğini

göstermektedir. Deneysel sonuçlar, LDA'nın belge modelleme, metin sınıflandırma ve öneri sistemleri gibi alanlarda etkili sonuçlar sağladığını ortaya koymuştur. Ayrıca, LDA'nın daha önce karşılaşılmamış belgeler üzerinde yüksek doğruluk oranları sunduğu ve genelleme yeteneğinin diğer yöntemlere kıyasla daha üstün olduğu tespit edilmiştir. Sonuç olarak, LDA'nın esnek, genişletilebilir ve farklı veri setlerine uyum sağlayabilen bir model olduğu vurgulanmaktadır. Bu model, büyük metin koleksiyonlarından anlamlı bilgiler elde etmek için güçlü bir araç olarak tanıtılmaktadır.

(Güven vd., 2020) çalışmalarında, sosyal medya platformlarında paylaşılan içerikler üzerinden duygu analizi gerçekleştirmeyi amaçlamışlardır. Bu kapsamda, Latent Dirichlet Allocation (LDA) algoritmasının n-aşamalı varyantı olan n-LDA yöntemi önerilmiş ve yöntemin başarımı test edilmiştir. LDA'nın yanı sıra Latent Semantic Analysis (LSA) ve Probabilistic Latent Semantic Analysis (P-LSA) gibi diğer konu modelleme yöntemleriyle karşılaştırmalı analizler gerçekleştirilmiştir. Araştırma, toplamda 4000 adet Türkçe tweet üzerinde yürütülmüş, veriler ön işleme süreçlerinden geçirilerek temizlenmiştir. Tweetler beş farklı duygu kategorisine — kızgınlık, korku, mutluluk, üzüntü ve şaşkınlık — göre sınıflandırılmıştır. Çalışmada düşük ağırlıklı kelimeler sözlükten çıkarılarak konu kapsamının daha isabetli biçimde belirlenmesi hedeflenmiştir. Sonuçlar, klasik LDA ve P-LSA yöntemlerine kıyasla n-LDA yönteminin daha yüksek doğruluk oranı ve daha hızlı çalışma süresi ile üstün performans sergilediğini göstermiştir. LSA yönteminin ise bu bağlamda yetersiz kaldığı gözlemlenmiştir. Geliştirilen n-LDA yöntemi, Türkçe tweetler üzerinden duygu değişimini tespit etmede umut vadeden bir yaklaşım olarak değerlendirilmekte olup, konu modelleme alanında yapılacak ileri çalışmalar için sağlam bir temel sunmaktadır.

(Ritter ve Etzioni, 2010) çalışmalarında, LDA Yöntemini kullanarak seçimsel tercihlere yönelik bir yaklaşımı, Latent Dirichlet Allocation (LDA) dağıtımını incelemektedir. En hafif tabirle, verilen yeni bir yöntem tanıtılmaktadır. LinkLDA'yı kullanarak hem gizli konuları hem de ayrı ayrı konu bölümlerini eşzamanlı bir şekilde ortaya çıkarmaktadır. Geleneksel sınıf temelli yöntemlerin insan tarafından yorumlanabilirlik özellikleri ile doğrudan metin madenciliği yaklaşımlarının yüksek tahmin gücünü bir araya getirmesini sağlar. Örneğin, LDA-SP'nin farklı dağılımının karşılaştırması yapılmış ve mevcut en iyi yöntemlere göre %85 daha yüksek bir hatırlama (geri çağırma) oran oranları. Öte yandan, LDA-SP'nin çıkarımları depolama deposunda önemli depolar sunulanlar da ortaya konmuştur. Sonuç olarak, bu makale, LDA'nın seçimsel tercihler bölümünde güçlü bir araç olduğunu ve doğal dil işleme

uygulamalarının, anlam ayırma ve öneri sistemleri gibi alanlarda önemli avantajlar sağladığını göstermektedir.

(Danler vd., 2024) çalışmalarında, hemşirelik bakım raporlarında yer alan serbest metin anlatılarını analiz etmek amacıyla Latent Dirichlet Allocation (LDA) konu modelleme yöntemini kullanmaktadırlar. Araştırmanın temel hedefi, hemşirelik anlatılarında gizli kalan temaları belirlemek ve bu temaların hasta bakımı ile sağlık hizmetleri üzerindeki etkilerini değerlendirmektir.

Araştırma kapsamında, Avusturya'daki üç farklı klinikte bir hafta süresince kaydedilen hemşirelik anlatıları incelenmiştir. Veriler, R programlama dili ve LDAvis görselleştirme aracı kullanılarak analiz edilmiştir. Elde edilen sonuçlar, hemşirelik anlatılarında üç ana temanın ön plana çıktığını göstermektedir: Hasta Refahı, Hasta Hareketliliği ve Bakım Aktiviteleri, Tedavi ve Ağrı Yönetimi. Başlangıçta "Tedavi" ve "Ağrı Yönetimi" ayrı temalar olarak değerlendirilmiş olsa da içerik açısından büyük ölçüde örtüştükleri için tek bir başlık altında birleştirilmiştir. Çalışma, LDA yönteminin hemşirelik anlatılarından anlamlı içgörüler elde etmek için etkili bir araç olduğunu ortaya koyarken, bazı zorlukları da beraberinde getirdiğini vurgulamaktadır. Özellikle modelin hiperparametre hassasiyeti, yazılım güncellemelerinin eksikliği ve analizlerin tekrarlanabilirliği konusunda karşılaşılan sorunlar dikkat çekmektedir. Gelecek çalışmaların, bu sınırlamaların aşılmasına ve daha gelişmiş metin analizi yöntemlerinin geliştirilmesine odaklanması gerektiği belirtilmiştir.

3.4.3. Blokzincir Güvenlik Zaafiyetleri ile İlgili Literatür Çalışmaları

(Li vd., 2020), yapılan bu çalışmada blokzincirin güvenlik tehditlerini sistematik bir şekilde incelemekte olup popüler saldırıları ve gerçek saldırıları araştırmaktadır. Güvenlik sorunlarına yönelik mevcut olan eksiklikleri giderip güvenlik için iyileştirme çözümlerine değinilmiştir. Güvenlik açıklıklarının çözümlerini bulmak için öneriler sunulmaktadır.

(Putz ve Pernul, 2020), yapıkları bu çalışmada blokzincirin potansiyel tehditlerine karşılık olarak korunmanın artırılması için bir tehdit izleme yaklaşımı gerçekleştirmişlerdir. Saldırılar incelenip tehditler ise genişletilmiştir. Hyperledger Fabric ile yapılan analizler ile izleme yöntemlerinin uygulanabilirliği değerlendirilmiştir.

(Tuyisenge, 2021), bu tez çalışmasında 2010 ile 2021 yılları arasındaki yayınlanmış olan 20 tane makaleyi inceleyip ve blokzincire yönelik olan güvenlik tehditlerini, etkilerini inceleyip analiz edilmiştir. Yapılan bu çalışmada blokzincirin dört farklı katmanlara göre sınıflandırılmıştır. Bunun sonucu olarak yetkisiz kod yürütme, hizmet

reddi vb. yaygın olan güvenlik risklerine haritalanmıştır. Yaptıkları çalışma sonucunda en çok güvenlik sıkıntılarının P2P ağ yapısında olduğu tespit edilmektedir. Tehditleri azaltmak için öneriler üzerinde durmuş olsalar da yeni protokollerin geliştirilmeye ihtiyaç duyulduğuna değinmişleridir.

(Cheng vd., 2021), tarafından yapılan çalışmada, blokzincir teknolojisindeki güvenlik zafiyetleri ve bu tehditlere yönelik çözümler sistematik bir şekilde özetlenmiştir. Çalışma, blokzincir'in işleyişini ve güvenlik tehditlerini ele alarak, bu tehditlerle başa çıkabilmek için çeşitli öneriler sunmuştur. Destek detayları, gizlilik koruma yöntemleri ve zafiyetlere dair farklı araştırma konuları üzerinde durulmuştur.

(Y. Chen vd., 2022), ise blokzincir'in güvenlik ve gizlilik sorunlarını kapsamlı bir şekilde incelemişlerdir. Çalışmada, saldırı teknolojileri üç kategoriye ayrılmıştır: konsensüs katmanı saldırıları, ağ iletişimi ile ilgili protokol saldırıları ve uygulama hizmeti saldırıları. Her bir kategori için ilgili savunma yöntemleri ve çözüm önerileri sunulmuştur. Özellikle, gizlilikle ilgili saldırılar ele alınmış ve bu tür zafiyetlere karşı çözüm yolları önerilmiştir.

(J. Chen, 2024), çalışmasında bitcoin gibi çok bilinen kripto paraların güvenliklerini inceleyerek blockchain teknolojisinin karşı karşıya kaldığı açıklıkları ve saldırı vektörlerini ele geçirmiştir. Bu çalışma ağ yapılarını ve uygulama katmanlarına yönelik saldırıları ele alır özellikle çatallama ve çoğunluk saldırıları gibi blockchain bütünlüğünü tehdit eden saldırılara ağırlık vermiştir. Mevcut olan savunma yapılarını değerlendirip dijital platforma da ki değerleri attırmaya yönelik stratejiler geliştirmektedir. Blockchain için güvenliğin nasıl daha güçlü savunulabilmesi için bir analiz sunmayı hedeflemektedir.

(Karahan ve Tüfekci, 2020) çalışmalarında, blokzincir teknolojisinin dijital kimlik yönetiminde kullanımını inceleyen bir sistematik haritalama uygulamışlardır. Dijital kimlik, çevrimiçi hizmetlere güvenli erişim sağlamak için gereklidir ancak mevcut sistemlerde güvenlik, mahremiyet ve veri tutarsızlığı gibi sorunlar yaşanmaktadır. Çalışma, blokzincirin merkezi otoriteye bağımlılığı azaltarak bu sorunları nasıl çözebileceğini değerlendirir. Konuyla ilgili akademik çalışmalar incelenerek blokzincir tabanlı kimlik sistemleri, kendi kendine egemen kimlikler (SSI) ve uygulama örnekleri analiz edilmiştir. Sonuç olarak, blokzincirin dijital kimlik yönetimini iyileştirme potansiyeline sahip olduğu vurgulanmaktadır.

(Dwivedi vd., 2024) çalışmalarında, blokzincir güvenliği üzerine kapsamlı bir araştırma sunulmaktadır. Çalışma, blokzincir mimarisini oluşturan katmanlar temelinde saldırı türlerini sınıflandırmakta ve her bir katmana özgü güvenlik açıklarını, bu açıklardan faydalanma yöntemlerini ve olası savunma mekanizmalarını detaylı biçimde

incelemektedir. Araştırmada, blokzincir teknolojisinin veri güvenliği açısından sahip olduğu güçlü yönlerin yanı sıra zayıf noktaları da sistematik olarak analiz edilmiştir. Ayrıca, yeni ve mevcut saldırı vektörleri değerlendirilmiş; bu doğrultuda kuantum bilişim teknolojisinin blokzincir güvenliğine olası etkileri de tartışılmıştır. Çalışmada, gelecekte ortaya çıkabilecek tehditlere karşı alınabilecek önlemlere dair öneriler sunulmaktadır. Bu yönüyle makale, blokzincir saldırılarının temel nedenlerini açıklamakta ve bu saldırılara karşı geliştirilebilecek savunma yöntemlerine ışık tutmaktadır. Elde edilen bulgular, blokzincir güvenliği alanında hem akademik literatür hem de endüstriyel uygulamalar açısından önemli katkılar sağlamaktadır.

(J. Hong, 2012), yapmış olduğu çalışmada kimlik avı (phishing) saldırılarının günümüzdeki durumunu incelemektedir. Phishing, saldırganların sahte e-postalar ve web siteleri aracılığıyla insanları kandırarak hassas bilgilerini ele geçirmeye çalıştığı bir sosyal mühendislik saldırısıdır. Çalışma, phishing saldırılarının evrimini, insanların bu saldırılara nasıl düştüğünü ve saldırganların hangi teknikleri kullandığını anlatmaktadır. Ayrıca, saldırılara karşı alınabilecek önlemler tartışılmakta ve spam filtreleme, sahte sitelerin engellenmesi, kullanıcı eğitimi gibi çeşitli savunma stratejileri önerilmektedir. Son olarak, phishing'in kurumsal güvenlik üzerindeki etkileri ve gelecekteki tehditler ele alınmaktadır.

(Zhang vd., 2019) çalışmalarında, blockchain teknolojisinin güvenlik ve gizlilik yönlerini kapsamlı bir şekilde ele almaktadırlar. Blokzincirin, merkezi olmayan güvenli veri depolama ve işlem yapma olanağı sunduğunu, ancak güvenlik açıkları ve gizlilik endişelerinin halen büyük bir tartışma konusu olduğunu belirtmektedirler. Çalışma, Bitcoin gibi kripto para sistemlerinden akıllı sözleşmelere kadar blokzincirin kullanım alanlarını inceleyerek, temel güvenlik gereksinimlerini tanımlamaktadır. Ayrıca, hash zinciri depolama, anonim imzalar, sıfır bilgi kanıtları gibi güvenlik tekniklerini ele alarak, saldırılara karşı olası savunma mekanizmalarını değerlendirmektedirler. Çalışma, blokzincirin güvenlik ve gizlilik tehditlerine karşı nasıl korunabileceğine dair derinlemesine bir analiz sunmaktadır.

(Şen ve Alnıaçık, 2024), çalışmalarında blokzincir teknolojisinin yönetim süreçlerine olası etkilerini incelemektedirler. Blokzincir, dağıtık, şeffaf ve değiştirilemez yapısıyla finans sektörü dışında da çeşitli alanlarda kullanılabilir hale gelmiştir. Çalışma, blokzincirin iş dünyasında yönetim süreçlerini nasıl dönüştürebileceğini değerlendirerek, mevcut uygulamalar ve gelecek beklentilerini ele almaktadır. Blokzincirin merkezi otoriteye duyulan ihtiyacı azaltarak daha güvenli ve verimli iş süreçleri sunabileceği belirtilmektedirler. Ancak, bu teknolojinin ölçeklenebilirliği, regülasyonlar ve teknik

sınırlamalar gibi bazı zorlukları da bulunmaktadır. İşletmeler için dijital dönüşümün temel taşlarından biri olabileceği vurgulanmaktadır.

(Conti vd., 2018), çalışmalarında Bitcoin'in güvenlik ve gizlilik bilgilerini ele alan kapsamlı bir araştırmaya yer vermişlerdir. Bitcoin'in temel seçeneği, blockchain seçenekleri ve Proof-of-Work (PoW) tabanlı konsensüs oranlarını incelerken, sistemdeki güvenlik açıklarını ve tehditleri analiz etmektedir. Çalışmada, çifte harcama, %51 saldırı, madencilik havuzu saldırıları ve ağ düzeyinde gerçekleştirilebilecek saldırılar gibi konular ele alınarak, mevcut güvenlik önlemleri ve anonimlik çözümleri değerlendirilmiştir. Ayrıca Bitcoin'in gizlilik sorunlarına ve kullanıcıların düzenlenmesini zorlaştırmak için kırılmalara de değinilmiştir. Son olarak gelecekte Bitcoin'in faydasını artırmaya yönelik açık araştırma alanları sunulmaktadır.

(Crosby vd., 2016) çalışmalarında, blockchain teknolojisinin Bitcoin'in ötesinde ele alınarak, finansal ve finans dışı olarak kayıt altına alınması inceleniyor. Blockchain, dağıtılmış bir veritabanı olarak, tüm işlemler merkezi bir otoriteye ihtiyaç duymadan güvenli ve değiştirilemez şekilde kayıt defterini alır. Çalışmada, finans sektöründe akıllı sözleşmeler, özel menkul kıymetler ve sigorta gibi kullanım alanları ele alınırken, noter hizmetleri, müzik endüstrisi, üretilen internet (IoT) ve sahtecilikle mücadele gibi finans dışı uygulamalara da değinilmektedir. Ayrıca blokzincirin benimsenmesi teknik, yasal ve ölçeklenebilirlik gibi zorluklar tartışılmış ve güncel iş fırsatları vurgulanmıştır.

(Latifa ve Omar, 2017) çalışmalarında, Bitcoin ve blockchain teknolojisinin güvenlik yönlerini, zorluklarını ve bu zorluklara karşı alınabilecek önlemleri ele almaktadırlar. Bitcoin'in 2008'den beri hızla büyüdüğü, merkezi olmayan bir yapıya sahip olduğu ve kullanıcılar arasında doğrudan işlem yapılmasına olanak sağladığı vurgulanmaktadır. Ancak, bu merkeziyetsizlik, işlem hızının sınırlı olması ve güvenlik açıkları gibi bazı dezavantajları da beraberinde getirmektedir. Yapılan bu çalışma, Bitcoin'in cüzdan yapısı, işlem süreci ve kullanılan şifreleme tekniklerini (SHA-256, ECDSA, RIPEMD-160) detaylandırarak, bunların güvenlik seviyelerini değerlendirmektedir. Ayrıca, Bitcoin cüzdanlarının çalınması, çift harcama saldırıları, kötü amaçlı yazılımlar, hizmet reddi saldırıları (DDoS) ve blockchain ağının hedef alınarak manipüle edilmesi gibi çeşitli saldırı senaryoları incelenmektedir. Son olarak, Bitcoin'in anonimlik seviyesinin tam olmadığı, kullanıcı hareketlerinin analiz edilebileceği ve gelecekte güvenlik önlemlerinin artırılması gerektiği belirtilmektedir. Araştırmacılar, güvenliği artırmak için blockchain üzerindeki düğümlerin daha etkin şekilde denetlenmesini ve saldırılara karşı ek protokoller geliştirilmesini önermektedir.

(Mosakheil, 2018) yapmış olduğu çalışmada, blockchain teknolojisinin güvenlik tehditlerini sınıflandırarak incelemektedir. Blockchain, merkeziyetsiz ve değiştirilemez bir dijital defter olarak çeşitli sektörlerde kullanım alanı bulsa da güvenlik, ölçeklenebilirlik ve gizlilik gibi sorunlarla karşı karşıyadır. Çalışmada, blockchain sistemlerinde mevcut güvenlik açıkları analiz edilerek, çift harcama (çift harcama), madencilik havuzları, ağ güvenliği, bütçeler ve akıllı sözleşmelere yönelik tehditler ayrıntılı bir şekilde ele alınmıştır. Ayrıca saldırı senaryoları ve bunlara karşı alınabilecek önlemler incelenmiş, geliştiriciler ve özellikler için güvenlik tehditlerini sınıflandıran bir taksonomi özellikleri. Bu görünümler, blockchain sistemlerinin risklerini en aza indirmek için rehber niteliğindedir.

(Aponte-Novoa vd., 2021), çalışmalarında blokzincirlerde 51% saldırısını (çoğunluk saldırısı) ve madencilik davranışlarını incelemektedirler. 51% saldırısı, bir madenci veya madenci grubunun toplam ağ işlem gücünün %51'inden fazlasını ele geçirerek blokzinciri manipüle etmesiyle gerçekleşir. Bu saldırı, çifte harcama (double-spending) yapılmasına, işlemlerin yeniden düzenlenmesine ve diğer madencilerin dışlanmasına neden olabilmektedir. Çalışma, Bitcoin ve Ethereum blokzincirlerindeki madencilerin hash gücünün dağılımını analiz ederek, bu saldırının gerçekleşme olasılığını değerlendirmektedir. Veriler, madencilik gücünün az sayıda büyük madencide yoğunlaştığını ve bunun 51% saldırısını teorik olarak mümkün kıldığını göstermektedir. Özellikle büyük madencilik havuzlarının piyasada artan hakimiyeti, merkeziyetsizlik ilkesine zarar vererek blokzincir güvenliği için risk oluşturmaktadır. Makalede ayrıca, geçmişte yaşanmış saldırı örnekleri inceleniyor ve bu tür saldırıları önlemek için farklı teknikler önerilmektedir. Alternatif konsensüs mekanizmaları, madenci davranış analizleri ve anomali tespit yöntemleri gibi çeşitli güvenlik çözümleri değerlendirilmektedir. Sonuç olarak, 51% saldırısının ciddi bir tehdit oluşturduğu vurgulanırken, blokzincirlerin güvenliğini artırmak için daha merkeziyetsiz ve güvenli sistemler geliştirilmesi gerektiği belirtilmektedir.

(Aitzhan ve Svetinovic, 2016) çalışmalarında, merkezi olmayan enerji ticaretinde güvenlik ve gizliliği sağlamak amacıyla bir sistem geliştirildiğini anlatmaktadırlar. Geleneksel enerji ticaretinde merkezi aracıların güvenlik ve ölçeklenebilirlik sorunları oluşturduğuna dikkat çekilmektedir. Çalışmada, blockchain teknolojisi, çoklu imzalar ve anonim şifreli mesajlaşma akışları kullanılarak merkeziyetsiz bir enerji ticaret sistemi olan PriWatt prototipi geliştirilmektedir. Bu sistem sayesinde kullanıcılar anonim şekilde enerji fiyatlarını müzakere edebilir ve güvenli işlemler gerçekleştirebilmektedirler

Yapılan performans analizleri ve vaka çalışmaları, sistemin güvenlik ve gizlilik gereksinimlerini karşıladığını göstermektedir.

(Rathod ve Motwani, 2018) yapmış oldukları çalışmada, blockchain teknolojisinin güvenlik tehditlerini ve bunlara karşı geliştirilen önlemleri incelemektedirler. Blockchain, merkeziyetsiz ve değiştirilemez bir dijital defter olarak birçok sektörde kullanılmaktadır. Ancak, ölçeklenebilirlik, güvenlik açıkları, gizlilik ve yönetişim gibi sorunlarla karşı karşıyadır. Makale, blockchain sistemlerini hedef alan tehditleri, örneğin çifte harcama, %51 saldırısı, yönlendirme saldırıları ve madencilikle ilgili güvenlik açıklarını ele almaktadır. Ayrıca, mevcut güvenlik önlemleri ve olası çözüm yollarını değerlendirerek, blokzincirin daha güvenli hale getirilmesi için öneriler sunmaktadır.

(Bonneau vd., 2015), yapılan bu çalışmada Bitcoin ve diğer kripto paraların araştırma alanlarını, karşılaştıkları zorlukları ve olası gelişim alanlarını ele almaktadırlar. Çalışma, Bitcoin'in teknik yapısını üç temel bileşene ayırarak incelemektedir: işlem yapısı, mutabakat (konsensüs) mekanizması ve iletişim ağı. Kripto paraların sağladığı merkeziyetsizlik, anonimlik ve güvenlik avantajlarının yanı sıra, karşı karşıya oldukları tehditler ve güvenlik açıkları değerlendirilmektedir. Çalışma, Bitcoin'in mevcut ölçeklenebilirlik sorunları, enerji tüketimi ve işlem ücretleri gibi kritik konular ele alınıyor. Ayrıca, madencilik süreçlerinin uzun vadede nasıl değişebileceği ve büyük madencilik havuzlarının (mining pools) merkeziyetsiz yapıya olan etkileri tartışılıyor. Alternatif mutabakat mekanizmaları (Proof of Stake gibi) ve Bitcoin'in mevcut konsensüs mekanizmasının zayıf yönleri araştırılmaktadır. Çalışmanın ana amacı, Bitcoin'in sürdürülebilirliğini artırmak için öneriler geliştirmek ve gelecekteki araştırmalar için yol göstermektir. Makale, kripto paraların daha güvenli, ölçeklenebilir ve verimli hale gelmesi için teknik öneriler sunarak, kripto para ekosisteminin uzun vadede nasıl gelişebileceğini tartışmaktadır.

(Taşkın ve Doğru, 2023) çalışmalarında, Blokzincir teknolojisi ve kötü amaçlı yazılımlar arasındaki ilişkiyi derinlemesine ele alan bu makale, blokzincirin sunduğu güvenilirlik, şeffaflık, değişmezlik ve kriptografik güvenlik gibi avantajların yanı sıra, siber saldırganlar tarafından kötüye kullanılma potansiyeline de dikkat çekmektedirler. Özellikle kötü amaçlı kripto madenciliği, fidye yazılımları ve oltalama saldırıları gibi tehditler üzerinde durulmuştur. Araştırmacılar, Web of Science ve Scopus gibi akademik veri tabanlarında kapsamlı bir literatür taraması yaparak, 216 makaleyi inceleyerek blokzincir tabanlı kötü amaçlı yazılımların yaygınlığını analiz etmişlerdir. Çalışmada, bu yazılımların blokzincir sistemleriyle nasıl entegre edildiği, tespit edilme yöntemleri ve bu tehditlere karşı uygulanabilecek siber güvenlik stratejileri detaylandırılmıştır. Ayrıca,

yapay zekâ ve makine öğrenmesi tekniklerinin bu tür tehditlerin belirlenmesindeki rolü de değerlendirilmiştir. Sonuç olarak, blokzincir teknolojisinin hem güvenlik açısından büyük fırsatlar sunduğu hem de siber tehditler için bir araç olarak kullanılabileceği vurgulanmış; siber güvenlik uzmanlarına yönelik çeşitli öneriler sunulmuştur. Bu çalışma, akademisyenler ve uygulayıcılar için blokzincir güvenliğini artırmaya ve kötü amaçlı yazılımlarla mücadeleye yönelik önemli bir kaynak niteliği taşımaktadır.

3.4.4. Blokzincir Güvenlik Zaafiyetleri Üzerine Konu Modelleme Çalışmaları

(Sharma vd., 2022), çalışmasında blockchain teknolojisindeki mevcut araştırma eğilimlerini belirlemek için Gizli Dirichlet Tahsisi'ne (LDA) dayalı bir konu modelleme yöntemini benimser. Çalışmanın temel amacı blockchain teknolojisinin derinlemesine araştırıldığı alanları tespit etmek ve gelecekte daha fazla araştırma yapılması gereken konuları belirlemektir. Bu amaçla IEEE, Springer ve ACM gibi çeşitli dijital veri tabanlarından 900'den fazla makale toplanmış ve bu makalelere LDA modeli uygulanmıştır. Bu model, blockchain ile ilgili anahtar kelimeleri ve literatürü analiz ederek belirli araştırma alanlarını ve bu alanlardaki eğilimleri sınıflandırır. Sonuçlar, blockchain teknolojisinin en yaygın olarak güvenlik, IoT entegrasyonu, finans sektörü, sağlık hizmetleri, akıllı sözleşmeler ve tedarik zinciri yönetimi gibi alanlarda kullanıldığını göstermektedir. Blockchain entegrasyonu, özellikle IoT sistemleri ve akıllı sözleşmeler üzerine yapılan araştırmalar dikkat çekti. Ayrıca blokzincirin veri güvenliğinin sağlanmasındaki rolü, merkezi olmayan yönetim sistemleri üzerindeki etkisi ve finansal uygulamalardaki potansiyeli gibi konular da araştırılmaktadır. Çalışma aynı zamanda blockchain teknolojisinin yeterince çalışılmamış yönlerini ortaya koyuyor ve gelecekte daha fazla araştırma yapılması için alanlar önermektedir. Makale, akademisyenler ve araştırmacılar için 15'ten fazla yeni araştırma yönü önererek blockchain teknolojisinin gelişimini teşvik etmeyi amaçlıyor. Ayrıca yıl ve yayın kaynağına göre araştırma eğilimlerini değerlendirmek için bir meta veri analizi yapılmıştır. Dolayısıyla bu çalışma, blockchain teknolojisinin akademik araştırmalardaki durumunu ve gelecekteki potansiyelini ortaya koymakta ve bu alandaki araştırmacılara yol gösterici bir kaynak oluşturmaktadır.

(Prakash vd., 2022)'nın çalışmaları blokzincir teknolojisi ile siber güvenlik alanındaki uygulamaları derinlemesine inceleyen bir metin madenciliği analizine dayanmaktadır. Makale 2010 ile 2022 yılları arasında yazılan 1302 akademik çalışmayı analiz ederek blokzincir teknolojisinin siber güvenlik ile nasıl kullanıldığını tematik olarak sergilemektedir. Yaptıkları çalışmada en çok incelenen konular kimlik doğrulama,

metin bütünlüğü ve gizlilik yer almaktadır. Yaptıkları çalışmada yayınların zaman içerisinde artış gösterdiğini vurgulamaktadırlar. Bu da siber güvenliğin blokzincir ile giderek daha da benimsediğini ortaya koymaktadır. Çalışmada blokzincirin merkeziyetsizlik ve şeffaflık özellikleri sayesinde birçok güvenlik zafiyetleri alanlarına çözüm sunmaktalar. Bunun yanında enerji tüketimi gibi bazı zorluklarınla halen önemli engeller oluşturduklarını ifade etmektedirler.

(Taş ve Kiani, 2018) çalışmalarında, blokzincir teknolojisine yönelik olan saldırı türlerini inceleyip ve bu saldırı türlerinin potansiyel etkilerini derinlemesine incelemektedirler. Makalede özellikle üstünde durulan saldırılar %51 saldırıları, zaman damgası manipülasyonu, çift harcama ve sybil saldırısı gibi yaygın olarak karşımıza çıkan zafiyetler üzerinde daha çok durulmuştur. Makalede her saldırı çeşidi açıklanmış ve sistem üzerindeki etkileri değerlendirilmiştir. Çalışmada ayrıca ele aldıkları tehditlerin kullanılan blokzincir yapılarında nasıl ortaya çıktıklarını ve bunların ne tür zafiyetleri tetiklediklerini ve hangi önlemler alınarak bu zafiyetleri daha da minimuma indirebilmek üzerine yoğunlaşmışlardır. Blokzincir teknolojisinin sunduğu merkeziyetsizliğe rağmen dikkatli tasarım ve sürekli güvenlik analizlerinin gerektiğini söylemektedirler.

(Homoliak vd., 2021), makalede blokzincir teknolojisinin güvenlik ihtiyaçlarını sistematik bir şekilde inceleyerek ele almakta ve bunun yanında bir güvenlik referans mimarisi sunmaktadırlar. Yapılan bu çalışmada blokzincirin sahip olduğu dağıtıp yapısı ve değiştirilemezlik gibi özellikleri ile birlikte karşımıza çıkan karmaşık güvenlik sorunlarına karşı kapsamlı bir çözüm sunmayı hedeflenmektedir. Yazarlar bu çalışmada öncelik olarak literatürde bulunan blokzincir mimarilerini incelemişler ardından bu mimarilerin ve güvenlik tehditlerine karşı alabilecek güvenlikleri sınıflandırarak kendi önerdikleri mimari ile eşleştirmişlerdir. Çalışmadaki mimaride erişim kontrolü, kimlik yönetimi ve ağ güvenliği gibi temel güvenlik alanları üzerine odaklanılmıştır. Yaptıkları bu mimari hem blokzincir uygulama geliştiricileri için hem de sistem mimarileri için güvenli sistem tasarımı açısından bir kaynak niteliği taşımaktadır.

4. ANALİZ VE BULGULAR

4.1. Çalışmanın Amacı ve Kapsamı

Bu tez çalışmasının amacı, blokzincir tabanlı uygulamalarda karşılaşılan güvenlik zafiyetlerini belirlemek ve sistematik olarak sınıflandırmaktır. Bu doğrultuda, sosyal medya platformu Twitter'dan elde edilen 8.705 kullanıcı yorumu ve tartışması, Latent Dirichlet Allocation (LDA) tabanlı konu modelleme yöntemiyle analiz edilmiştir. Çalışma, blokzincir güvenliği konusunu yalnızca teknik bir çerçeveden değil, aynı zamanda kullanıcı perspektifinden ele alarak, güvenlik açıklarını daha kapsamlı ve anlamlı bir şekilde değerlendirmeyi hedeflemektedir.

Tezin temel amacı, blokzincir sistemlerinde en sık karşılaşılan güvenlik açıklarının türlerini ve yaygınlıklarını ortaya koymaktır. Bu sayede hem uzmanların hem de kullanıcıların bu zafiyetleri daha kolay tanıyabilmeleri ve gerekli önlemleri alabilmeleri hedeflenmektedir. Aynı zamanda, sosyal medya verileri üzerinden gerçekleştirilen analiz yöntemiyle literatüre yeni ve uygulanabilir bir metodolojik katkı sunulması amaçlanmaktadır.

Mevcut literatür incelendiğinde, blokzincir güvenliği konusunun genellikle teknik raporlar ve akademik makaleler üzerinden ele alındığı görülmektedir. Ancak, sosyal medya platformlarında paylaşılan kullanıcı deneyimlerinin ve şikâyetlerinin bu alandaki araştırmalara yeterince yansımadığı dikkat çekmektedir. Bu çalışma, sosyal medya verilerini dikkate alarak, blokzincir zafiyetlerinin hem kullanıcı deneyimleriyle ilişkilendirilmesini hem de konu modelleme yoluyla sistematik olarak sınıflandırılmasını sağlamaktadır.

Tezde, blokzincir teknolojisinin temel bileşenleri olan dağıtık defter yapıları, akıllı sözleşmeler ve kriptografik güvenlik mekanizmaları çerçevesinde güvenlik zafiyetleri ele alınmaktadır. Twitter üzerinden toplanan yorumlar, metin madenciliği ve doğal dil işleme (NLP) teknikleri kullanılarak analiz edilmekte; özellikle LDA yöntemi aracılığıyla metinlerdeki gizli temalar ve konular tespit edilmektedir. Böylece güvenlik açıklarının kategorize edilmesi ve bunlara yönelik çözüm önerilerinin geliştirilmesi hedeflenmektedir.

Sonuç olarak, bu çalışma, blokzincir tabanlı uygulamalardaki güvenlik risklerini hem teknik hem de kullanıcı odaklı bir yaklaşımla değerlendirerek literatüre özgün ve yenilikçi bir katkı sunmayı amaçlamaktadır.

4.2. Çalışmanın Yöntemi ve Veriler

Veri Toplama: Sosyal medya platformu Twitter, blokzincir ve güvenlik konularına ilişkin kullanıcı yorumları ile tartışmaların toplanmasında kullanılmıştır. Twitter API aracılığıyla, belirlenen anahtar kelimeler ve etiketler üzerinden ilgili veri seti oluşturulmuştur. Veri setinde en sık geçen 20 kelime aşağıda sunulmuştur. Bu kelimeler, blokzincir güvenliğiyle ilgili yaygın tartışma alanlarını yansıtmaktadır (Tablo 3).

Tablo 3. Veri Seti İçerisinde Geçen En Fazla 20 Kelime

Kelimeler	**Sayısı**
Security (Güvenlik)	1742
Blockchain (Blokzincir)	1305
Crypto (Kripto)	1295
Secure (Güvenlik)	788
Smart (Akıllı)	716
Contract (Sözleşme)	675
Key (Anahtar)	645
Decentralized (Merkezi olmayan)	549
Risk (Risk)	547
Transaction (İşlem)	465
Digital (Dijital)	442
Future (Gelecek)	425
Bitcoin	404
Asset (Varlık)	390
Network	332
Wallet (Cüzdan)	306
Protect (Korumak)	283
Vulnerability (Güvenlik açığı)	246
Attack (Saldırı)	228
Scam (Sahtekarlık)	162

Veri İşleme: Toplanan veriler, doğal dil işleme (NLP) teknikleri kullanılarak temizlenmiş ve ön işleme tabi tutulmuştur. Bu aşamada, gereksiz kelimeler (stopwords) çıkarılmış, metinler normalize edilmiş ve analiz için uygun bir formata dönüştürülmüştür.

Konu Modelleme: Temizlenmiş veriler üzerinde Latent Dirichlet Allocation (LDA) yöntemi uygulanmış; böylece güvenlik zafiyetlerine dair ana temalar ve konular belirlenmiştir. Bu adımda elde edilen temalar, blokzincir teknolojisindeki zafiyetlerin daha iyi anlaşılmasına katkı sağlamıştır.

Sonuçların Değerlendirilmesi: Analizden elde edilen bulgular, literatürdeki mevcut çalışmalarla karşılaştırılmış ve yorumlanmıştır. Bu değerlendirme, çalışmanın özgünlüğünü ve literatüre olan katkısını ortaya koymuştur.

Kullanılan Materyaller:

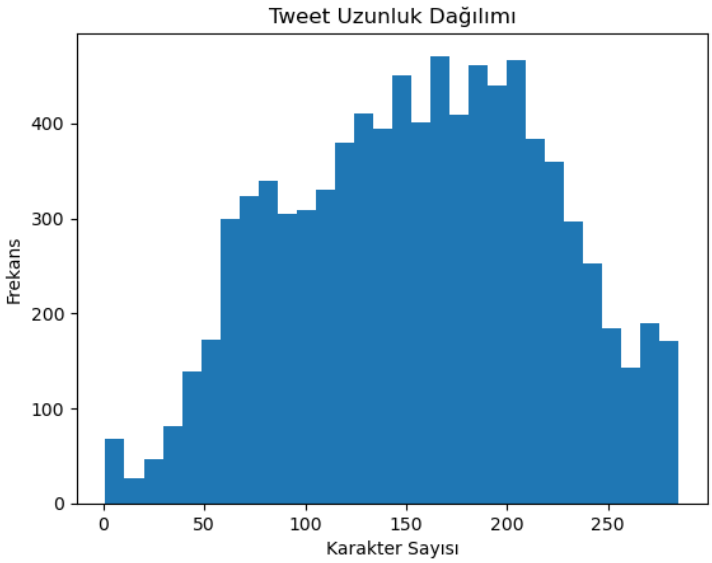
- **Twitter API:** Veri toplamak için kullanılacak birincil araçtır.
- **Twitter'dan Alınan Veri Setleri:** Blokzincir zafiyetlerini analiz etmek amacıyla kullanılmıştır.
- **Python ve Gensim Kütüphanesi:** Analiz işlemlerinde kullanılmıştır.

Bu yöntem, blokzincir tabanlı güvenlik zafiyetlerini hem kullanıcı perspektifinden hem de teknik bir yaklaşımla analiz ederek literatüre katkı sağlamıştır.

4.3. Verilerin Temizlenmesi ve Düzenlenmesi

Veriler, Twitter üzerinden çekilerek bir Excel dosyası üzerinde birleştirilmiştir. Excel dosyası daha sonra Anaconda Navigator üzerinde Jupyter Notebook ortamında analiz edilmek üzere çağrılmıştır. Twitter üzerinden elde edilen 8705 veri, uygulama tarafından ön işleme tabi tutulmuş ve veriler temizlenmiştir. Gereksiz kelimeler ve noktalama işaretleri kaldırılmış; ardından LDA analizi yapabilmek amacıyla Gensim kütüphanesi çağrılmıştır. Daha sonra, görselleştirme için pyLDAvis kütüphanesi kullanılmıştır. Çağrılan tüm veriler için toplu bir kelime bulutu oluşturulmuştur. Ayrıca, 20 adet topik oluşturularak her topik için en çok kullanılan 10 kelime belirlenmiştir.

Aşağıda yer alan görsel, Twitter platformunda paylaşılan tweet'lerin karakter uzunluklarının dağılımını göstermektedir. Şekil 8'de, X ekseni tweet'lerdeki karakter sayısını; Y ekseni ise bu karakter uzunluklarına sahip tweet'lerin frekanslarını temsil etmektedir. Verilere göre tweet'lerin çoğunluğu 100 ile 220 karakter arasında yoğunlaşmıştır. Özellikle 150–200 karakter aralığında belirgin bir frekans artışı gözlenmiştir. Bu da Twitter'ın sunduğu 280 karakterlik sınırın etkin şekilde kullanıldığını ortaya koymaktadır.



Şekil 8. Tweet Uzunluk Dağılımı

Aşağıda, modelleme öncesinde en güncel 10 tweet ve en eski 10 tweet örneklemeli olarak sunulmuştur. Bu örnekler, veri setinin zaman boyutuna ve içerik çeşitliliğine dair fikir vermektedir (Şekil 9).

Şekil 9. İlk 10 ve Son 10 Tweet

Aşağıdaki görsel, kelime bulutunu (word cloud) göstermektedir. Görselde, çok sayıda kelime yer almaktadır. Bu kelimeler, X (Twitter) platformundan çekilen tweet'ler içerisinde en sık kullanılan sözcükleri temsil etmektedir ve bir kelimenin boyutu ne kadar büyükse, o kelimenin metin içerisinde o kadar sık geçtiği anlaşılmaktadır. Görsele bakıldığında en baskın kelimelerin "blockchain", "crypto", "security", "smart contract", "secure", "risk", "twitter", "transaction", "wallet" gibi ifadeler olduğu görülmektedir

(Şekil 10). Her bir konu için ayrı ayrı kelime bulutları oluşturulmuş ve Ekler kısmında yer verilmiştir (bk. Ek 1).

Şekil 10. Kelime Bulutu

4.4. Modelin Uygulanması

Sosyal medya platformu Twitter üzerinden çekilen veriler üzerinde LDA yöntemiyle gerçekleştirilen analizler sonucunda elde edilen bilgiler, grafikler ve tablolar bu bölümde yorumlanmıştır.

LDA modeli, büyük metinler içerisinde saklı olan konuları ortaya çıkarmak için kullanılmaktadır. Elde edilen tweet'lerin belirli temalardan oluştuğu ve bu temalar içerisinde öne çıkan anahtar kelimelerin yer aldığı görülmüştür. Çalışmada yazılan kod ile 20 adet konu oluşturulmuş ve her bir konu için anahtar kelimeler ile bu kelimelere ait ağırlık değerleri elde edilmiştir. Ağırlık değeri, verilen kelimelerin o konu içerisindeki önemini yansıtmaktadır; bu değer ne kadar yüksekse kelimenin ilgili konuyu temsil etme gücü de o denli fazla olmaktadır.

Konular incelendiğinde, kelimelerin sunduğu bilgiler şu şekilde özetlenebilir: Konu 19: program, team, bug, application gibi kelimeler yazılım mühendisliği bağlamını yansıtırken; cve ve bypass gibi ifadeler güvenlik temalarına işaret etmektedir. Bu doğrultuda, bu konunun "Yazılım Geliştirme" teması altında değerlendirilebileceği anlaşılmıştır. Konu 1: problem, solve, bridge kelimeleri sistemde çözüm odaklı bir anlatımı temsil ederken; decentralize ve security kavramları merkeziyetsizlik ve güvenlik üzerine odaklanıldığını göstermektedir. Bu nedenle bu başlık, "Blokzincir Altyapısı" teması ile ilişkilendirilmiştir. Konu 5: security, dürüstlük, solution gibi ifadeler güvenli altyapıya işaret ederken; future ve technology kelimeleri güvenliğin sürdürülebilirliğini ön plana çıkarmaktadır. Bu konu, "Blokzincir Güvenliği" kapsamında değerlendirilmiştir (Tablo 4).

Tablo 4. Konulara Göre Anahtar Kelime Dağılımı

Konu	Anahtar Konu Dağılımları
Konu 1	'0.086*"security" + 0.038*"smart_contract" + 0.027*"blockchain" + "0.025*"ensure" + 0.018*"vulnerability" + 0.016*"secure" + 0.014*"code" + "0.014*"risk" + 0.013*"audit" + 0.013*"transaction"
Konu 2	'0.040*"wallet" + 0.025*"crypto" + 0.022*"safe" + 0.020*"scam" + "0.016*"protect" + 0.015*"stay" + 0.013* "asset" + 0.012*"keep" + "0.010*"user" + 0.010*"security"
Konu 3	'0.052*"blockchain" + 0.040*"secure" + 0.029*"security" + 0.024*"digital" + "0.018*"decentralize" + 0.018*"trust" + 0.016*"asset" + 0.016*"solution" + "0.015*"future" + 0.014*"technology"
Konu 4	'0.028*"attack" + 0.021*"exploit" + 0.018*"steal" + 0.017*"risk" + "0.016*"hacker" + 0.015*"fund" + 0.013* "vulnerability" + 0.013*"bitcoin" + "0.011*"defi" + 0.010*"hack"
Konu 5	'0.056*"governance" + 0.027*"community" + 0.024*"token" + 0.018*"network" + "0.018*"power" + 0.016* "future" + 0.015*"node" + 0.015*"decentralize" + "0.013*"dao" + 0.012*"platform"
Konu 6	'0.065*"crypto" + 0.055*"market" + 0.049*"resilience" + 0.043*"bitcoin" + "0.024*"strong" + 0.023*"risk" + 0.015*"volatility" + 0.014*"trading" + "0.013*"btc" + 0.013*"strategy"
Konu 7	'0.046*"let" + 0.028*"stay" + 0.023*"keep" + 0.021*"crypto" + "0.021*"together" + 0.019*"future" + 0.017* "strong" + 0.015*"build" + "0.013*"market" + 0.012*"innovation"'
Konu 8	'0.035*"crypto" + 0.017*"project" + 0.010*"long" + 0.009*"participate" + "0.008*"drive" + 0.007*"organization" + 0.007*"year" + 0.007*"big" + "0.006*"coin" + 0.006*"setback"
Konu 9	'0.024*"blockchain" + 0.023*"system" + 0.013*"problem" + 0.013*"solve" + "0.012*"crosschain" + 0.012*"node" + 0.010*"decentralize" + 0.010*"bridge" + "0.009*"network" + 0.007*"security"'
Konu 10	'0.030*"blockchain" + 0.023*"security" + 0.020*"cryptography" + "0.012*"quantum" + 0.011*"read" + 0.010*"network" + 0.010*"core" + "0.009*"threat" + 0.009*"discover" + 0.009*"encryption"
Konu 11	'0.022*"blockchain" + 0.014*"security" + 0.011*"case" + 0.009*"tough" + "0.008*"chain" + 0.007*"take" + 0.007*"learn" + 0.007*"solana" + "0.006*"well" + 0.006*"hodl"
Konu 12	'0.030*"hack" + 0.016*"crypto" + 0.015*"read" + 0.013*"day" + 0.011*"bug" + "0.011*"way" + 0.010*"exploit"+ 0.010*"defi" + 0.010*"list" + 0.009*"year"'
Konu 13	'0.035*"chain" + 0.017*"transaction" + 0.013*"npm" + 0.013*"validator" + "0.010*"supply" + 0.010*"blockchain" + 0.009*"do" + 0.009*"block" + "0.008*"begin" + 0.008*"add"
Konu 14	'0.014*"help" + 0.012*"contact" + 0.011*"support" + 0.011*"platform" + "0.010*"shape_future" + 0.008*"magic"+ 0.008*"today" + 0.008*"fuel" + "0.007*"catch" + 0.007*"money"'
Konu 15	'0.016*"follow" + 0.011*"portfolio" + 0.011*"money" + 0.011*"crypto" + "0.010*"feel" + 0.009*"event" + 0.009*"camel" + 0.008*"concept" + "0.008*"update" + 0.008*"reach"
Konu 16	'0.057*"polkadot" + 0.014*"chain" + 0.011*"bug_bounty" + 0.011*"solidity" + "0.010*"available" + 0.009*"dot"+ 0.009*"number" + 0.008*"internet" + "0.008*"share" + 0.007*"smart_contract"'

Tablo 4. (Devamı)

Konu 17	'0.032*"contract" + 0.016*"function" + 0.015*"token" + 0.013*"detail" + "0.013*"analysis" + 0.010*"believe" + 0.009*"weather" + 0.008*"owner" + "0.008*"mint" + 0.008*"know"
Konu 18	'0.021*"ever" + 0.018*"time" + 0.011*"true" + 0.011*"dip" + 0.010*"struggle" "+ 0.010*"good" + 0.008*"ultimae" + 0.008*"strength" + 0.008*"bull" + "0.008*"ve"
Konu 19	'0.024*"program" + 0.013*"team" + 0.009*"bug" + 0.008*"application" + "0.007*"join" + 0.007*"client" + 0.007*"liquidation" + 0.006*"dapp" + "0.006*"cve" + 0.006*"bypass"'),
Konu 20	'0.027*"resource" + 0.017*"comment" + 0.011*"die" + 0.010*"current" + "0.010*"medium" + 0.009*"share" + 0.008*"ease" + 0.008*"read" + 0.008*"push" "+ 0.008*"beginner"

Elde edilen 20 konuya ilişkin olarak, en baskın anahtar kelimeler dikkate alınarak konu başlıkları önerilmiştir. Bu başlıklar, kullanıcıların hangi temalar etrafında yoğunlaştığını açıklamak açısından önem arz etmektedir. Aşağıdaki tabloda önerilen konu başlıkları yer almaktadır (Tablo 5).

Tablo 5. Oluşturulan 20 Konu İçin Başlık Önerisi

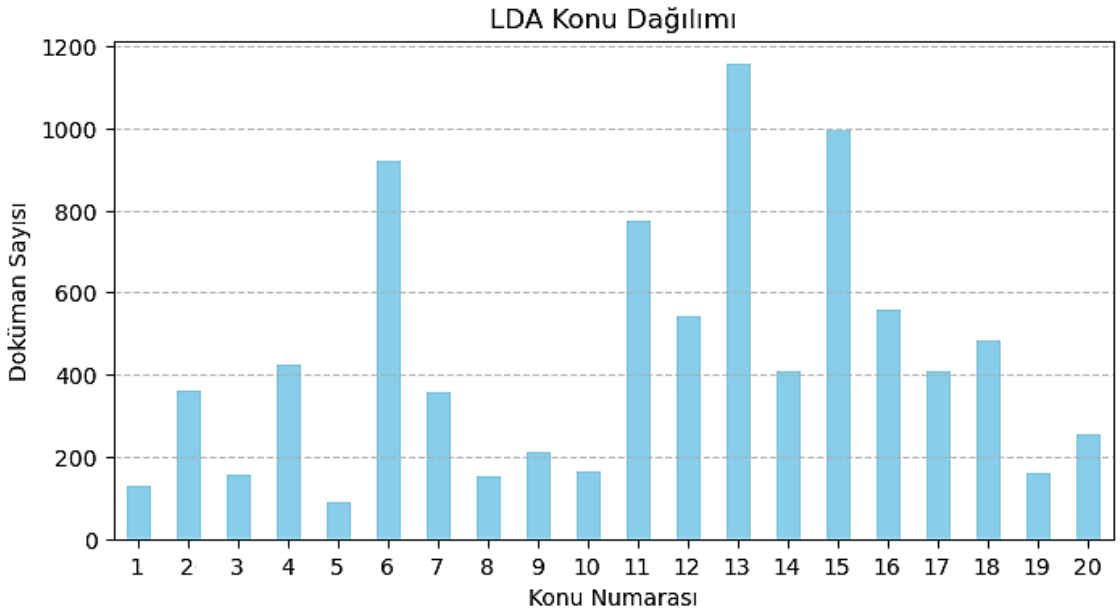
Konular	Önerilen başlık
1. Konu	Smart Contract Security (Akıllı Sözleşme Güvenliği)
2. Konu	Wallet Security (Cüzdan Güvenliği)
3. Konu	Blockchain Security (Blokzincir Güvenliği)
4. Konu	Cybersecurity (Siber Güvenlik)
5. Konu	Decentralized Governance (Merkezi Olmayan Yönetim)
6. Konu	Market Resilience (Pazar Esnekliği)
7. Konu	Crypto Future (Kripto Geleceği)
8. Konu	Crypto Governance (Kripto Yönetimi)
9. Konu	Blockchain Infrastructure (Blokzincir Altyapısı)
10. Konu	Cryptography (Kriptografi)
11. Konu	Blockchain Learning (Blokzincir Öğrenme)
12. Konu	DeFi Hacks
13. Konu	Tokenomics
14. Konu	Crypto Scams (Kripto Dolandırıcılıkları)
15. Konu	Crypto News (Kripto Haberleri)
16. Konu	Polkadot ve Smart Contracts (Polkadot ve Akıllı sözleşmeler)
17. Konu	Blockchain Development (Blokzincir Geliştirme)
18. Konu	Market Sentiment (Piyasa Duyarlılığı)
19. Konu	Software Development (Yazılım Geliştirme)
20. Konu	Bug Bounty (Hata Ödülü)

Aşağıdaki grafiğe göre, Twitter'dan çekilen tweet'lerin 20 konuya ayrıldığı görülmektedir (Şekil 11). Özellikle 1, 2, 3 ve 4 numaralı konuların diğerlerine göre daha baskın olduğu belirlenmiştir. Bu konular şu temaları temsil etmektedir:

- Akıllı Sözleşme Güvenliği

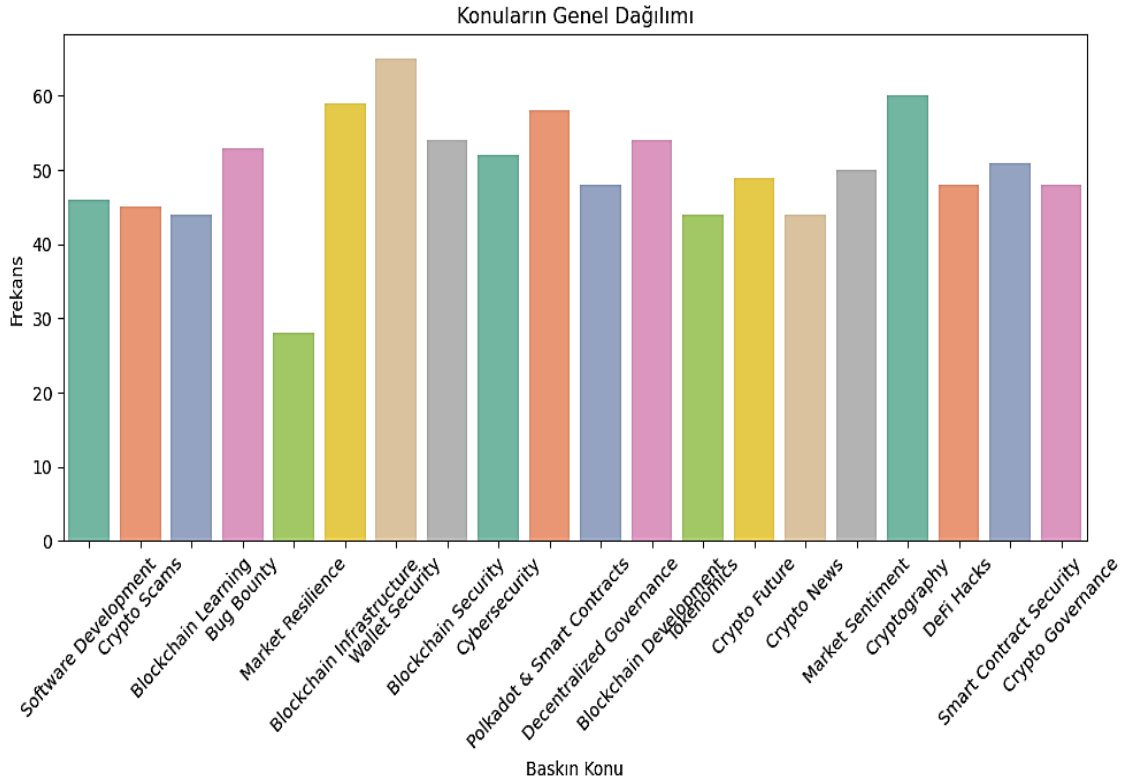
- Cüzdan Güvenliği
- Blokzincir Güvenliği
- Siber Güvenlik

Bu bulgu, analiz edilen verilerin özellikle bu dört başlık altında yoğunlaştığını ortaya koymaktadır.



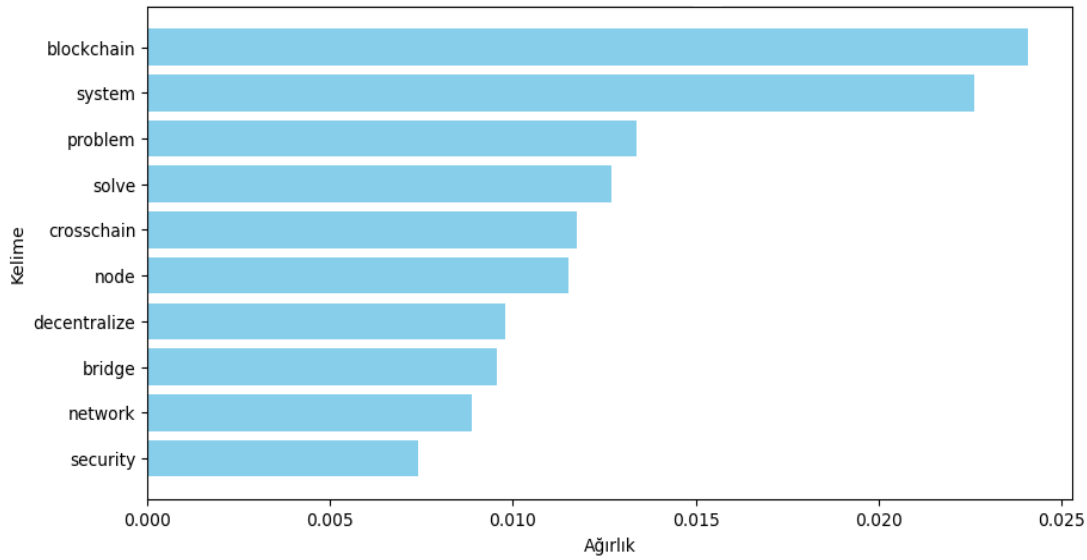
Şekil 11. LDA Modeli ile Elde Edilen Konu Dağılımı

Aşağıda yer alan grafik, 20 konu başlığının veri seti içerisindeki dağılım oranlarını göstermektedir. Bazı konuların daha sık tekrarlandığı ve daha geniş veri kümelerini temsil ettiği gözlemlenmiştir (Şekil 12).



Şekil 12. Konuların Genel Dağılımı

Şekil 13'te, Konu 9 için en çok kullanılan kelimeler görselleştirilmiştir. Bu kelimeler "blockchain", "system", "problem" ve "solve" gibi terimlerden oluşmakta ve konunun blokzincir sistemindeki sorunlar ve çözüm süreçleri üzerine odaklandığını ortaya koymaktadır. Ayrıca "crosschain" ve "decentralize" ifadeleri, farklı blokzincir ağlarının etkileşimi ve merkeziyetsizlik gibi alt temaların da analiz kapsamında olduğunu göstermektedir. Her bir konuya ait öne çıkan kelimeler grafikleri, ekler kısmında detaylı şekilde sunulmuştur. Bu grafiğe bakıldığında konular arasında heterojen bir dağılım olduğu açıkça görülmektedir. Örneğin, Konu 13 ile ilişkili yaklaşık 1150 adet doküman bulunurken, Konu 1, 3 ve 5 gibi bazı konularda ise bu sayı 100'ün altındadır. Bu durum, belirli temaların kullanıcılar tarafından daha yoğun şekilde ele alındığını göstermektedir. LDA modeli ile belirlenen diğer konulara ait öne çıkan kelimelere Ekler kısmında ayrıca yer verilmiştir (bk. Ek 2).

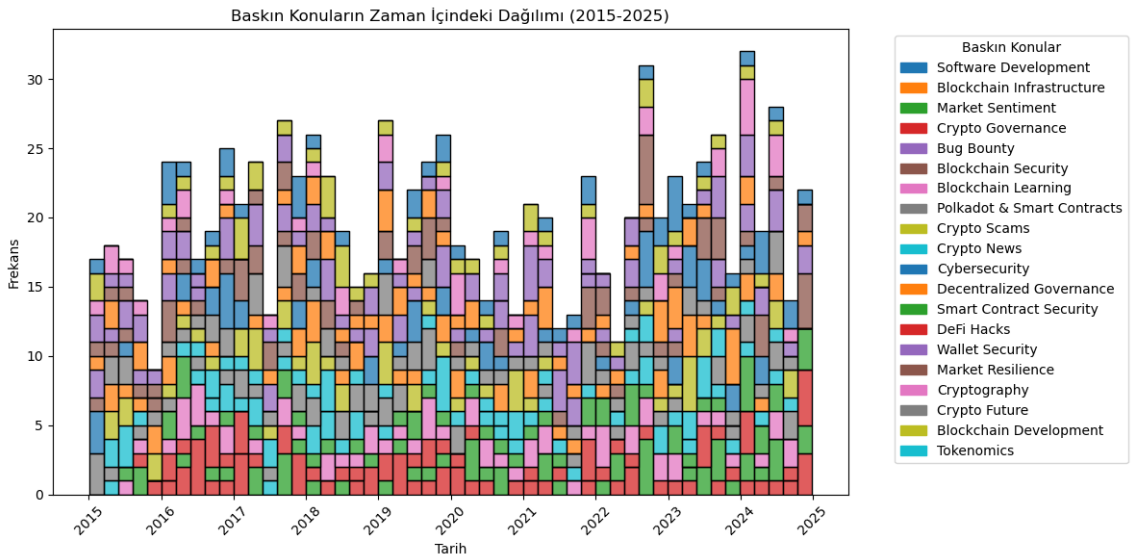


Şekil 13. LDA Modeli ile Belirlenen Konu 9'e Ait Öne Çıkan Kelimeler

4.5. Uygulama Sonuçlarının Değerlendirilmesi

Gerçekleştirilen konu modelleme uygulaması sonucunda, 8.705 adet tweet üzerinde Latent Dirichlet Allocation (LDA) yöntemi ile anlamlı konu başlıkları elde edilmiştir. Modellenen konular, blokzincir teknolojilerinde öne çıkan güvenlik zafiyetlerini temsilen belirgin kavramlar etrafında toplanmıştır. Özellikle siber saldırılar, akıllı sözleşme açıkları, kimlik doğrulama eksiklikleri, dolandırıcılık olayları ve merkeziyetsizlik ilkesine yönelik tartışmalar en çok öne çıkan konular arasında yer almıştır.

Aşağıdaki grafik, baskın konuların zaman içerisindeki dağılımını göstermektedir. Belirli dönemlerde bazı konuların öne çıktığı görülmüştür (Şekil 14). Bu durum, blokzincir güvenliğiyle ilgili gündemlerin dönemsel değişkenlik gösterdiğini ortaya koymaktadır.

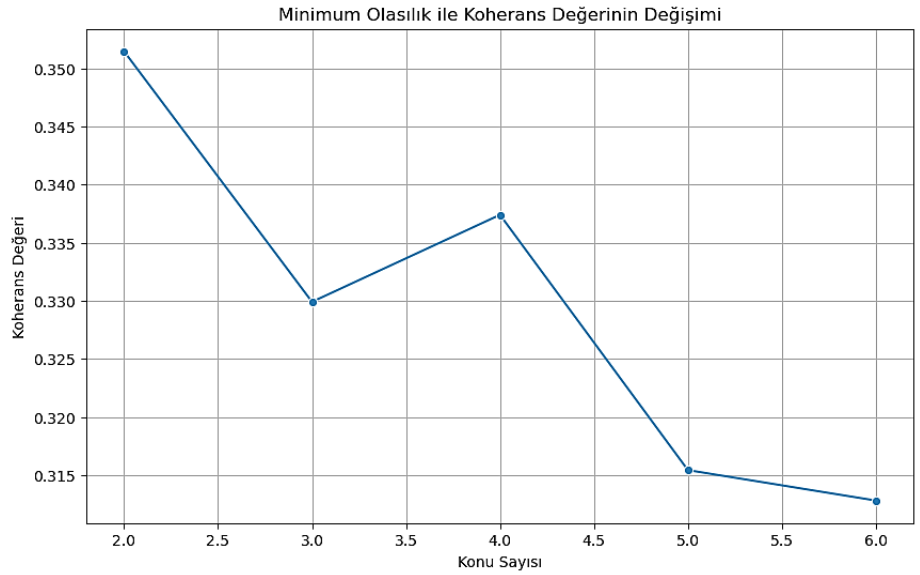


Şekil 14. Baskın Konuların Zaman İçerisinde Dağılımı

Elde edilen modeller, koherans değeri gibi ölçütlerle değerlendirildiğinde, belirlenen konu sayısının tutarlı ve anlamlı bir yapıya sahip olduğu görülmüştür. Aşağıdaki grafik, 20 konu başlığının veri setindeki dağılım oranlarını göstermektedir. Bazı konuların daha sık tekrarlandığı ve daha büyük kümeleri temsil ettiği görülmüştür (Şekil 15).

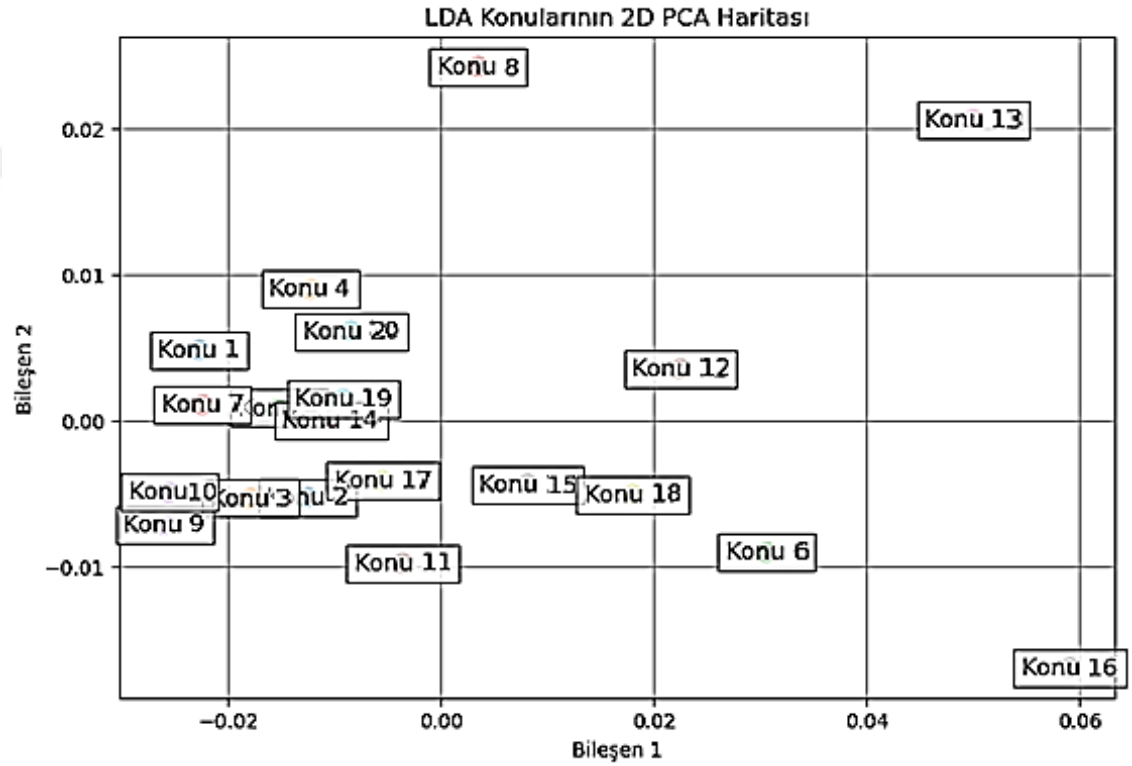
Şekil 15. Koherans Değerinin Konu Sayısına Göre Değişimi

Minimum olasılık değeri, nadir konuların model içindeki etkisini dengelemek için kullanılan bir parametredir. Aşağıdaki grafik, bu değere göre koherans değişimini göstermektedir (Şekil 16).



Şekil 16. Minimum Olasılık ile Koherans Değerinin Değişimi

PyLDAvis görselleştirmeleri üzerinden, konuların birbirinden ayrıştığı, belirgin anahtar kelimelerle temsil edildiği ve içerik tekrarlarının düşük olduğu gözlemlenmiştir. Bu bulgular, seçilen ön işleme adımlarının ve model parametrelerinin çalışmaya uygun olduğunu göstermektedir. LDA ile elde edilen 20 konu, iki boyutlu PCA haritası üzerinde görselleştirilmiştir. Bu harita, konuların birbirinden ayrışma düzeyini ve kümelenme yapısını yansıtmaktadır. Ayrışan ve örtüşen konuların dağılımı aşağıdaki şekilde sunulmuştur (Şekil 17).



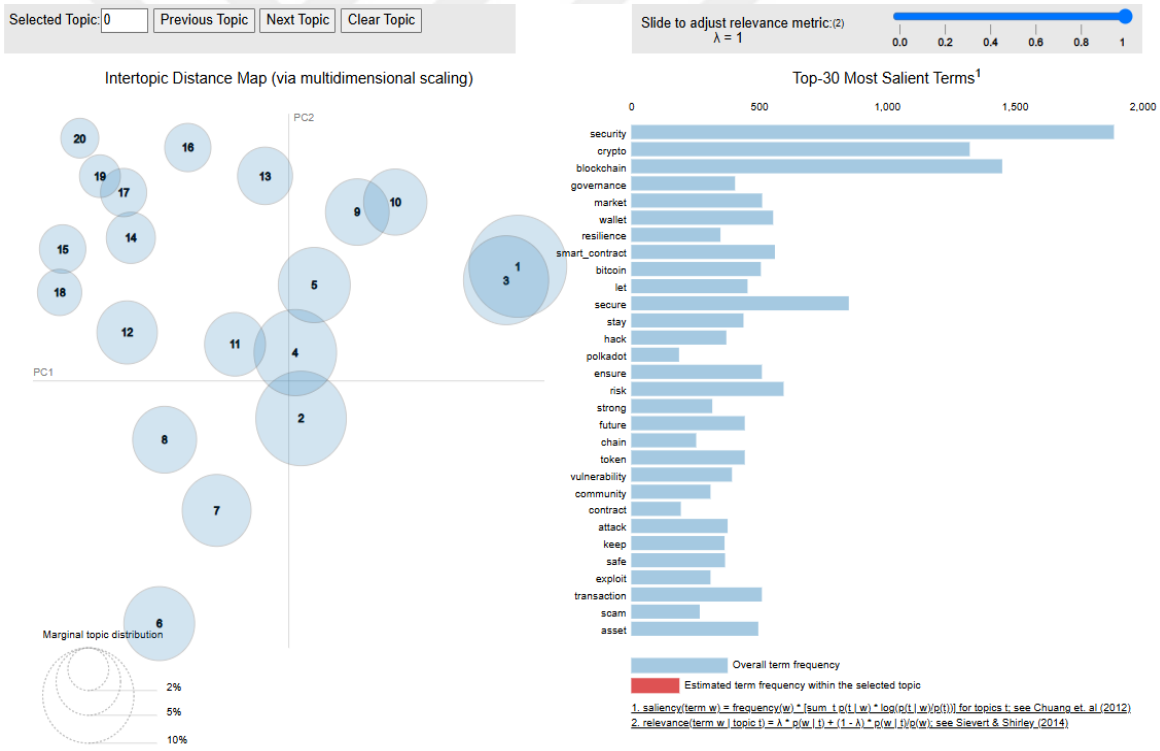
Şekil 17. LDA Konularının 2D PCA Haritası

Yapılan analiz sonucunda oluşturulan 20 konu ve bu konular içinde geçen anahtar kelimelere daha önce yer verilmişti. Şekil 18'de, LDA modeli sonuçları pyldavis ile görselleştirilmiştir. Sol taraftaki grafik, konuların birbirine olan uzaklıklarını ve büyüklüklerini gösteren bir haritadır (çok boyutlu ölçekleme ve konular arası mesafe haritası). Mavi renkteki her bir baloncuk bir konuyu temsil etmektedir. Balonların boyutları, o konunun veri setindeki oranını göstermektedir. Balonlar birbirine ne kadar yakınsa, o konular kelime içeriği bakımından birbirine o kadar benzerdir. Uzak baloncuklar ise daha özgün temaları temsil etmektedir. Örneğin, 1. ve 3. konuların birbirine oldukça yakın olması, benzer kelimeler ve benzer temaların işlendiğini göstermektedir.

Sağ tarafta ise çalışmada kullanılan en kapsamlı ve belirgin 30 kelime ile bu kelimelerin frekansları yer almaktadır. Mavi çubuklar, kelimenin veri setindeki genel frekansını, kırmızı çubuklar ise seçilen konuya ait özgün frekansı göstermektedir. Bu sayede, kelimelerin genel dağılımı ile konu içindeki dağılımı karşılaştırılabilmektedir.

Lambda (λ) değeri, sağ üst köşede yer almakta olup kullanıcı tarafından ayarlanabilir durumdadır. Lambda değeri 1'e ayarlandığında, sadece frekansa dayalı kelimeler ön plana çıkar; bu durumda en sık kullanılan kelimeler görüntülenir. Lambda değeri 0 olarak seçildiğinde ise sadece konuya ait ayırt edici kelimeler dikkate alınır. Bu ayar, konuyu en iyi temsil eden özgün kelimelerin öne çıkmasını sağlamaktadır.

Sol alt köşede yer alan yüzdelik çemberler (%2, %5 ve %10), baloncukların büyüklüklerinin veri seti içindeki temsil oranını anlamamıza yardımcı olmaktadır. Örneğin, %10 büyüklüğündeki bir baloncuk, veri setinin %10'unu temsil eden bir konuyu göstermektedir.



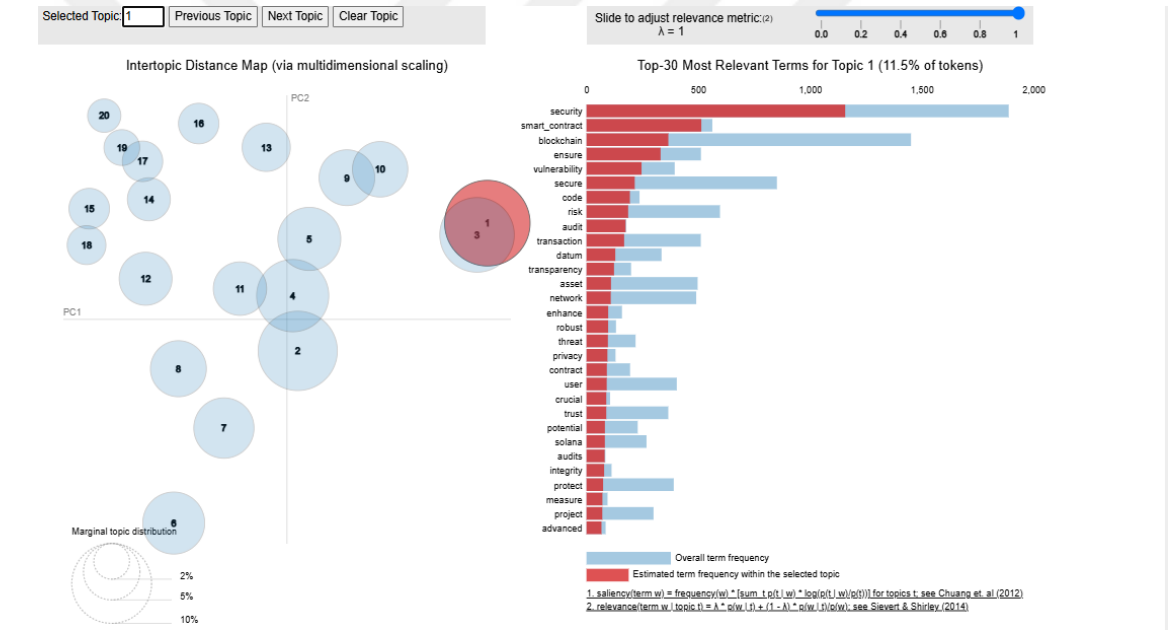
Şekil 18. LDA Modeli Sonuçlarının pyLDAvis Görselleştirmesi

Aşağıdaki görselleştirmede 1. konu seçilmiş olup, genel veri içerisindeki kelimeler ile konuya özgü kelimeler kırmızı renk ile gösterilmiştir (Şekil 19). Bu karşılaştırma, konunun anlamsal olarak ne derece belirgin olduğunu görselleştirmemize yardımcı olmaktadır. Konu 1 için en sık geçen kelimeler arasında security, smart_contract, blockchain ve vulnerability yer almaktadır. Bu kelimelerin anlamsal olarak bir bütünlük

göstermesi, model tarafından oluşturulan konunun tutarlılığını doğrulamaktadır. Her bir konu için ayrı ayrı pyLDAvis görselleştirmeleri, Ekler kısmında sunulmaktadır (bk. Ek 3).

Analiz sonucunda, sosyal medyada blokzincir güvenliği ile ilgili tartışmaların yalnızca teknik zafiyetlerle sınırlı kalmadığı; aynı zamanda kullanıcı güvenliği, regülasyon eksiklikleri ve algı boyutunu da kapsadığı anlaşılmıştır. Bu durum, blokzincir güvenliği üzerine yapılacak çalışmaların hem teknik hem de sosyal boyutları içermesi gerektiğini ortaya koymaktadır.

Genel olarak, uygulama çıktıları çalışmanın amacına uygun biçimde blokzincir güvenlik zafiyetlerine ilişkin güncel, çok boyutlu ve toplumsal yansımaları olan konuların analiz edilebildiğini göstermektedir. Modelleme sonuçları, bu alandaki akademik ve sektörel çalışmalara temel oluşturabilecek niteliktedir.



Şekil 19. 1. Konunun LDA Modeli Sonuçlarının pyLDAvis Görselleştirmesi

5. SONUÇ VE DEĞERLENDİRME

Bu tez çalışmasında, blokzincir tabanlı uygulamalarda karşılaşılan güvenlik zafiyetleri, sosyal medya platformu Twitter'dan toplanan veriler ışığında analiz edilmiştir. Toplamda 8.705 adet tweet üzerinde yapılan konu modelleme uygulaması sayesinde, kullanıcıların güvenlik zafiyetleri konusundaki algıları, öncelikleri ve kaygıları ortaya konmuştur. LDA (Latent Dirichlet Allocation) yöntemiyle gerçekleştirilen analizlerde, elde edilen konular arasında özellikle blokzincir güvenliği, akıllı sözleşme açıkları, DeFi hack'leri, cüzdan güvenliği ve kripto dolandırıcılıkları öne çıkmıştır. Bu temalar, kullanıcıların en çok tartıştığı ve endişe duyduğu başlıklar olarak dikkat çekmektedir.

Bu çalışmanın en önemli katkılarından biri, geleneksel literatürde genellikle teknik belgeler, akademik yayınlar ve teknik raporlar aracılığıyla ele alınan güvenlik zafiyetlerinin, bu kez kullanıcıların sosyal medya üzerinden yürüttüğü tartışmalar aracılığıyla değerlendirilmiş olmasıdır. Blokzincir teknolojisine yönelik algının doğrudan kullanıcı temelli ifadelerle analiz edilmesi, konunun toplumsal boyutuna da ışık tutmuştur. Yapılan analizler, (Güven vd., 2020) tarafından geliştirilen n-LDA modelinin sosyal medya verilerinde güvenlik temalarını başarılı biçimde ortaya çıkarabileceğini gösteren bulgularla örtüşmektedir. Ayrıca (Dwivedi vd., 2024)'ün blokzincir güvenliği katmanlı değerlendirmesine paralel olarak, bu çalışmada da farklı güvenlik açıklarının sistematik biçimde ayrıştırılabildiği görülmektedir.

Yapılan analizler sonucunda elde edilen konu kümeleri, sadece teknik zafiyetleri değil; aynı zamanda kullanıcı davranışlarını, algılarını ve güvenlik kültürünü de anlamaya yönelik ipuçları vermektedir. Özellikle "exploit", "vulnerability", "breach", "phishing", "wallet hacked", "exit scam" gibi ifadelerin yüksek frekansta tekrarlandığı görülmüştür. Bu ifadeler, kullanıcıların günlük yaşamlarında karşılaştıkları veya karşılaşma ihtimali taşıdıkları tehditlere karşı farkındalık geliştirdiklerini göstermektedir. Aynı zamanda, merkeziyetsiz sistemlerin şeffaflık ve güvenlik vaatlerinin, kullanıcılar nezdinde hala sorgulandığını ortaya koymaktadır.

Çalışmada elde edilen bulgular, LDA modelinin büyük ölçekli ve heterojen veri setlerinde anlamlı konu kümeleri elde etmek açısından güçlü bir yöntem olduğunu doğrulamıştır. Özellikle koherans değeri ile desteklenen model parametreleri, belirlenen 20 konunun istatistiksel olarak tutarlı olduğunu göstermektedir. Ayrıca pyLDAvis görselleştirmeleri ile konular arasındaki ayrışma, içerik benzerliği ve temsili anahtar

kelimeler net bir biçimde ortaya konmuştur. Elde edilen iki boyutlu PCA haritası, konu kümeleri arasında anlamlı bir yapısal ayrışma olduğunu da kanıtlamaktadır. Bulgular, özellikle akıllı sözleşme açıklıkları ve dolandırıcılık temalarının öne çıkması bakımından (Conti vd., 2018) ve (Atzei vd., 2017) tarafından belirtilen güvenlik riskleriyle örtüşmektedir. Bununla birlikte, sosyal medya verilerinde kullanıcıların dolandırıcılık olaylarına teknik açıklar kadar duyarlılık göstermesi, (Zheng vd., 2017)'nin ileri sürdüğü toplumsal güven algısı vurgusunu desteklemektedir. Ayrıca, elde edilen temaların çeşitliliği, (Dwivedi vd., 2024)'nin blokzincir güvenliğini çok katmanlı bir yapı olarak değerlendiren yaklaşımıyla da paralellik göstermektedir. Bu bağlamda çalışma hem mevcut literatürü destekleyen hem de sosyal boyutu güçlendiren özgün tartışmalar içermektedir.

Analiz sonucunda en çok öne çıkan zafiyet alanlarından biri akıllı sözleşme güvenliğidir. Kodlama hataları, denetlenmemiş sözleşmeler ve dış çağrıların kontrolsüz kullanımı gibi riskler, kullanıcıların ciddi kayıplar yaşamasına neden olabilmektedir. Bu durum, akıllı sözleşmelerin önceden test edilmemesi ve yeterli güvenlik protokollerine tabi tutulmamasıyla ilişkilendirilmiştir. Cüzdan güvenliği de bir diğer önemli başlık olarak öne çıkmaktadır. Özellikle "seed phrase" ve "private key" gibi kritik güvenlik öğelerinin kötü niyetli kişilerce ele geçirilmesi, bireysel kullanıcılar için büyük risk teşkil etmektedir. DeFi protokollerine yönelik yapılan saldırılar, yüksek miktarda kayıplara neden olduğu için sosyal medyada sıkça gündeme gelmektedir. Bu saldırıların sistem açıklarını ve oracle manipülasyonlarını hedef alması, kullanıcı güveninin zedelenmesine yol açmaktadır. Kripto dolandırıcılıkları ise özellikle "rug pull", "fake ICO" ve "fraud token" gibi kavramlar etrafında şekillenmiştir. Bu tür olaylar, yatırımcıların güvenini doğrudan etkilemekte ve sektöre olan inancı zayıflatmaktadır.

Bu çalışma, sadece mevcut durumu analiz etmekle kalmamış, aynı zamanda stratejik öneriler sunarak çözüm yolları da geliştirmiştir. Geliştiriciler açısından önerilen önlemler arasında açık kaynaklı kodların çok paydaşlı denetimlere açılması, statik analiz araçlarının yaygınlaştırılması ve "formal verification" uygulamalarının standartlaştırılması yer almaktadır. Kullanıcılar için ise dijital cüzdan güvenliği konusunda kamu bilgilendirme kampanyalarının düzenlenmesi, iki faktörlü kimlik doğrulamanın zorunlu hale getirilmesi ve sosyal mühendislik saldırılarına karşı eğitimlerin artırılması önerilmektedir. Düzenleyici otoriteler açısından, yeni çıkan projelere yönelik ön değerlendirme süreçlerinin sıkılaştırılması ve potansiyel dolandırıcılık projelerinin merkezi borsalar tarafından işaretlenmesi önemli adımlar olarak belirtilmiştir. Ayrıca, sosyal medya platformlarının rug pull ve benzeri olayları

otomatik tespit edebilecek algoritmalarla donatılması da sektöre ciddi katkılar sağlayacaktır.

Çalışmanın güçlü yönlerinden birisi, sosyal medya verilerinden elde edilen bulguların, akademik literatüre yeni bir perspektif sunmasıdır. Literatürde genellikle teknik belgeler ve deneysel sistem analizleri ile sınırlı kalan blokzincir güvenliği, bu çalışmada kullanıcı merkezli bir bakış açısıyla ele alınmıştır. Böylece güvenlik algısının hem teknik hem de sosyolojik boyutları birlikte değerlendirilebilmiştir. Bu yönüyle tez çalışması, dijital güvenlik araştırmalarında sosyal medya analizine dayalı yeni bir metodoloji geliştirilmesine zemin hazırlamaktadır.

Bu çalışma, literatürde sınırlı sayıda bulunan sosyal medya temelli blokzincir güvenlik analizleri arasında yer almakta ve kullanıcı algısına dayalı tematik çıkarımlar sunarak mevcut teknik odaklı yaklaşımlara yeni bir katkı sağlamaktadır. Bu yönüyle hem akademik literatür hem de uygulayıcılar için çok boyutlu bir değerlendirme zemini oluşturmuştur. Gelecek çalışmalar için önerilebilecek bazı yönler şunlardır: Farklı sosyal medya platformlarından (örneğin Reddit, GitHub) alınacak verilerle çoklu kaynaklı analizlerin yapılması, çok dilli veri setleriyle kültürel farklılıkların değerlendirilmesi ve LDA'nın yanı sıra BERT, BERTopic gibi daha güncel konu modelleme yöntemlerinin karşılaştırmalı olarak uygulanması. Ayrıca, duygu analizi ve ağ analizi tekniklerinin bu tür modellere entegre edilmesi, güvenlik algısının daha geniş bir perspektiften değerlendirilmesine olanak sağlayacaktır.

Sonuç olarak, bu tez çalışması; sosyal medya temelli veri madenciliği teknikleri ile blokzincir güvenlik zafiyetlerini kullanıcı perspektifinden sistematik olarak analiz etmiş, hem akademik literatüre hem de sektör uygulamalarına özgün katkılar sunmuştur. Çalışma çıktıları, blokzincir teknolojisinin yalnızca teknik değil, aynı zamanda toplumsal bir yapı olarak değerlendirilmesi gerektiğini bir kez daha ortaya koymuştur.

KAYNAKÇA

Aggarwal, D., Brennen, G. K., Lee, T., Santha, M., ve Tomamichel, M. (2017). Quantum attacks on bitcoin, and how to protect against them. *arXiv preprint arXiv:1710.10377*.

Aitzhan, N. Z., ve Svetinovic, D. (2016). Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE transactions on dependable and secure computing*, *15*(5), 840-852.

Alagic, G., Alagic, G., Apon, D., Cooper, D., Dang, Q., Dang, T., Kelsey, J., Lichtinger, J., Liu, Y.-K., ve Miller, C. (2022). *Status report on the third round of the NIST post-quantum cryptography standardization process*. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=934458

Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P., ve Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renewable and sustainable energy reviews*, *100*, 143-174.

Ante, L. (2021). Smart contracts on the blockchain–A bibliometric analysis and review. *Telematics and Informatics*, *57*, 101519.

Aponte-Novoa, F. A., Orozco, A. L. S., Villanueva-Polanco, R., ve Wightman, P. (2021). The 51% attack on blockchains: A mining behavior study. *IEEE access*, *9*, 140549-140564.

Apostolaki, M., Zohar, A., ve Vanbever, L. (2017). Hijacking bitcoin: Routing attacks on cryptocurrencies. *2017 IEEE Symposium on Security and Privacy (SP)*, 375-392. https://doi.org/10.1109/SP.2017.29

Atabaş, H. (2018). *Blok zinciri teknolojisi ve kripto paraların hayatımızdaki yeni yeri. İstanbul: Ceres yayınları.*

Atzei, N., Bartoletti, M., ve Cimoli, T. (2017). *A survey of attacks on ethereum smart contracts (sok)*. 164-186.

Ayberkin, D. (2022). *Blokzincir teknolojisinin dijital pazarlama sektöründe yenilikçilik ve kullanılabilirlik boyutuyla uygulanabilmesi için bir sistem mimarisinin tasarımı*.

Baird, L. (2016). The swirlds hashgraph consensus algorithm: Fair, fast, byzantine fault tolerance. *Swirlds tech reports Swırlds-TR-2016-01, Tech. Rep*, *34*, 9-11.

Batista, D., ve Lemieux, V. (2019). *Bounded and shielded: Assessing security aspects and trustworthiness of smart contracts*. Proceedings of the annual conference of CAIS/Actes du congrès annuel de l'ACSI.

Bhargavan, K., Delignat-Lavaud, A., Fournet, C., Gollamudi, A., Gonthier, G., Kobeissi, N., Kulatova, N., Rastogi, A., Sibut-Pinote, T., Swamy, N., ve Zanella-Béguelin, S. (2016). Formal verification of smart contracts: Short paper. *Proceedings of the 2016 ACM workshop on programming languages and analysis for security*, 91-96. https://doi.org/10.1145/2993600.2993611

Blei, D. M. (2012). Probabilistic topic models. *Communications of the ACM*, *55*(4), 77-84.

Blei, D. M., ve Lafferty, J. D. (2006). *Dynamic topic models*. 113-120.

Blei, D. M., ve Lafferty, J. D. (2007). A correlated topic model of science. *The annals of applied statistics*, 17-35.

Blei, D. M., Ng, A. Y., ve Jordan, M. I. (2003). Latent dirichlet allocation. *Journal of machine learning research*, *3*(Jan), 993-1022.

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., ve Felten, E. W. (2015). *Sok: Research perspectives and challenges for bitcoin and cryptocurrencies*. 104-121.

Boyd-Graber, J., Hu, Y., ve Mimno, D. (2017). Applications of topic models. *Foundations and trends in ınformation retrieval*, *11*(2-3), 143-296.

Bozan, M., ve Altun, K. (2023). Konu modelleme ile çalışan önerileri madenciliği: Bir otomotiv endüstrisi vakası. *International journal of pure and applied sciences*, *9*(1), Article 1. https://doi.org/10.29132/ijpas.1119552

Brumley, D., Chiueh, T., Johnson, R., Lin, H., ve Song, D. (2007). *RICH: Automatically protecting against integer-based vulnerabilities*.

Buterin, V., ve Griffith, V. (2019). *Casper the friendly finality gadget* (No. arXiv:1710.09437). arXiv. https://doi.org/10.48550/arXiv.1710.09437

Cambria, E., ve White, B. (2014). Jumping NLP curves: A review of natural language processing research. *IEEE Computational intelligence magazine*, *9*(2), 48-57.

Castro, M., ve Liskov, B. (2002). Practical byzantine fault tolerance and proactive recovery. *ACM trans. Comput. Syst.*, *20*(4), 398-461. https://doi.org/10.1145/571637.571640

Chen, J. (2024). Securing the chain: Comprehensive analysis of vulnerabilities and defense mechanisms in blockchain systems. *Applied and computational engineering*, *110*, 129-136.

Chen, L., Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R. A., ve Smith-Tone, D. (2016). *Report on post-quantum cryptography* (C. 12). US Department of commerce, national ınstitute of standards and technology …. https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.8105.pdf

Chen, T., Li, X., Luo, X., ve Zhang, X. (2017). *Under-optimized smart contracts devour your money*. 442-446.

Chen, W., Zheng, Z., Cui, J., Ngai, E., Zheng, P., ve Zhou, Y. (2018). Detecting ponzi schemes on ethereum: Towards healthier blockchain technology. *Proceedings of the 2018 World Wide Web Conference*, 1409-1418. https://doi.org/10.1145/3178876.3186046

Chen, Y., Chen, H., Zhang, Y., Han, M., Siddula, M., ve Cai, Z. (2022). A survey on blockchain systems: Attacks, defenses, and privacy preservation. *High-confidence computing*, *2*(2), 100048.

Cheng, J., Xie, L., Tang, X., Xiong, N., ve Liu, B. (2021). A survey of security threats and defense on blockchain. *Multimedia tools and applications*, *80*, 30623-30652.

coinmarketcap.com. (2025). *Blockchain security losses surge to $2.3B in 2024: phishing and key compromises dominate*. https://coinmarketcap.com/academy/article/1d506e3b-84e9-4acd-b623-65d20b6368a1

Conti, M., Kumar, E. S., Lal, C., ve Ruj, S. (2018). A survey on security and privacy issues of bitcoin. *IEEE communications surveys ve tutorials*, *20*(4), 3416-3452.

Coşlu, E. (2013). Veri madenciliği. *Akademik bilişim*, *23*(5).

Crosby, M., Pattanayak, P., Verma, S., ve Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied innovation*, *2*(6-10), 71.

Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., ve Juels, A. (2019). *Flash Boys 2.0: Frontrunning, transaction reordering, and consensus ınstability in decentralized exchanges* (No. arXiv:1904.05234). arXiv. https://doi.org/10.48550/arXiv.1904.05234

Danler, M., Hackl, W. O., Neururer, S. B., Huber, L., ve Pfeifer, B. (2024). Visualizing nursing narratives: An evaluation of latent dirichlet allocation topic modeling for care reports. *Digital health and informatics innovations for sustainable health care systems* (ss. 1709-1713). IOS press.

De Filippi, P., ve Wright, A. (2018). *Blockchain and the law: The rule of code*. Harvard University Press.

Deerwester, S., Dumais, S. T., Furnas, G. W., Landauer, T. K., ve Harshman, R. (1990). Indexing by latent semantic analysis. *Journal of the American society for information science*, *41*(6), 391-407.

Douceur, J. R. (2002). The sybil attack. içinde P. Druschel, F. Kaashoek, ve A. Rowstron (Ed.), *peer-to-peer systems* (ss. 251-260). Springer. https://doi.org/10.1007/3-540-45748-8_24

Durukal, O. (2021). Kamu ve özel sektörde blok zincir teknolojisi. *Nobel Yayın*.

Dwivedi, K., Agrawal, A., Bhatia, A., ve Tiwari, K. (2024). A novel classification of attacks on blockchain layers: Vulnerabilities, attacks, mitigations, and research directions. *arXiv preprint arXiv:2404.18090*.

Efanov, D., ve Roschin, P. (2018). The all-pervasiveness of the blockchain technology. *Procedia computer science*, *123*, 116-121.

Ekin, C. C., ve Algabsi, S. E. (2024). Contemporary research trends in mobile learning. Içinde X.-S. Yang, R. S. Sherratt, N. Dey, ve A. Joshi (Ed.), *Proceedings of eighth international congress on information and communication technology* (ss. 205-215). Springer Nature. https://doi.org/10.1007/978-981-99-3236-8_16

Eskandari, S., Clark, J., Barrera, D., ve Stobert, E. (2015). A first look at the usability of bitcoin key management. *Proceedings 2015 workshop on usable security*. https://doi.org/10.14722/usec.2015.23015

Feldman, R., ve Sanger, J. (2007). *The text mining handbook: Advanced approaches in analyzing unstructured data*. Cambridge university press.

Feng, Q., He, D., Zeadally, S., Khan, M. K., ve Kumar, N. (2019). A survey on privacy protection in blockchain system. *Journal of network and computer applications*, *126*, 45-58.

Francisco, K., ve Swanson, D. (2018). The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency. *Logistics*, *2*(1), 2.

Frawley, W. J., Piatetsky-Shapiro, G., ve Matheus, C. J. (1992). Knowledge discovery in databases: An overview. *AI magazine*, *13*(3), 57-57.

Goldberg, S. (2014). Why is it taking so long to secure internet routing? *Communications of the ACM*, *57*(10), 56-63. https://doi.org/10.1145/2659899

Grech, A., ve Camilleri, A. F. (2017). *Blockchain in education*. Luxembourg: Publications Office of the European Union.

Griffiths, T. L., ve Steyvers, M. (2004). Finding scientific topics. *Proceedings of the National academy of Sciences*, *101*(suppl_1), 5228-5235.

Grossman, S., Abraham, I., Golan-Gueta, G., Michalevsky, Y., Rinetzky, N., Sagiv, M., ve Zohar, Y. (2017). Online detection of effectively callback free objects with applications to smart contracts. *Proceedings of the ACM on programming languages*, *2*(POPL), 1-28.

Güven, Z., Diri, B., ve Çakaloğlu, T. (2020). Comparison of n-stage latent dirichlet allocation versus other topic modeling methods for emotion analysis. *Journal of the Faculty of Engineering and Architecture of Gazi University*, *35*(4).

Han, J., Pei, J., ve Tong, H. (2022). *Data mining: Concepts and techniques*. Morgan kaufmann.

He, Z., Li, Z., Yang, S., Ye, H., Qiao, A., Zhang, X., Luo, X., ve Chen, T. (2025). *Large language models for blockchain security: A systematic literature review* (No. arXiv:2403.14280). arXiv. https://doi.org/10.48550/arXiv.2403.14280

Hearst, M. A. (1999). *Untangling text data mining*. 3-10.

Heilman, E., Kendler, A., Zohar, A., ve Goldberg, S. (2015). Eclipse attacks on {Bitcoin's}{peer-to-peer} network. *24th USENIX security symposium (USENIX security 15)*, 129-144. https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/heilman

Hewa, T. M., Hu, Y., Liyanage, M., Kanhare, S. S., ve Ylianttila, M. (2021). Survey on blockchain-based smart contracts: Technical aspects and future research. *IEEE access*, *9*, 87643-87662.

Hofmann, T. (1999). *Probabilistic latent semantic indexing*. 50-57.

Homoliak, I., Venugopalan, S., Reijsbergen, D., Hum, Q., Schumi, R., ve Szalachowski, P. (2021). The security reference architecture for blockchains: Toward a standardized model for studying vulnerabilities, threats, and defenses. *IEEE communications surveys ve tutorials*, *23*(1), 341-390. https://doi.org/10.1109/COMST.2020.3033665

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, *55*(1), 74-81.

Hong, L., ve Davison, B. D. (2010). *Empirical study of topic modeling in twitter*. 80-88.

Hotho, A., Nürnberger, A., ve Paaß, G. (2005). A brief survey of text mining. *Journal for language technology and computational linguistics*, *20*(1), 19-62.

Jelodar, H., Wang, Y., Yuan, C., Feng, X., Jiang, X., Li, Y., ve Zhao, L. (2019). Latent dirichlet allocation (LDA) and topic modeling: Models, applications, a survey. *Multimedia tools and applications*, *78*, 15169-15211.

Jetter, O., Dinger, J., ve Hartenstein, H. (2010). Quantitative analysis of the sybil attack and effective sybil resistance in peer-to-peer systems. *2010 IEEE International Conference on Communications*, 1-6. https://doi.org/10.1109/ICC.2010.5501977

Joshi, A. P., Han, M., ve Wang, Y. (2018). A survey on security and privacy issues of blockchain technology. *Mathematical foundations of computing*, *1*(2).

Kalodner, H., Möser, M., Lee, K., Goldfeder, S., Plattner, M., Chator, A., ve Narayanan, A. (2020). *{BlockSci}: Design and applications of a blockchain analysis platform*. 2721-2738. https://www.usenix.org/conference/usenixsecurity20/presentation/kalodner

Kantardzic, M. (2011). *Data mining: Concepts, models, methods, and algorithms*. John Wiley ve Sons.

Karahan, Ç., ve Tüfekci, A. (2020). Blokzincir teknolojisinin dijital kimlik yönetiminde kullanımı: Bir sistematik haritalama çalışması. *Politeknik Dergisi*, *23*(2), 483-496.

Kaya, A., ve Gülbandılar, E. (2022). Konu modelleme yöntemlerinin karşılaştırılması. *Eskişehir Türk Dünyası Uygulama ve Araştırma Merkezi Bilişim Dergisi*, *3*(2), Article 2. https://doi.org/10.53608/estudambilisim.1097978

Kherwa, P., ve Bansal, P. (2020). Topic modeling: A comprehensive review. *EAI Endorsed Trans. Scalable Inf. Syst.*, *7*(24), e2.

Kimball, R., ve Ross, M. (2013). *The data warehouse toolkit: The definitive guide to dimensional modeling*. John Wiley ve Sons.

Lamport, L., Shostak, R., ve Pease, M. (2019). The Byzantine generals problem. İçinde *Concurrency: The works of leslie lamport* (ss. 203-226).

Latifa, E.-R., ve Omar, A. (2017). Blockchain: Bitcoin wallet cryptography security, challenges and countermeasures. *Journal of Internet Banking and Commerce*, *22*(3), 1-29.

Lee, D. D., ve Seung, H. S. (1999). Learning the parts of objects by non-negative matrix factorization. *nature*, *401*(6755), 788-791.

Levine, B. N., Shields, C., ve Margolin, N. B. (2006). A survey of solutions to the sybil attack. *University of Massachusetts Amherst, Amherst, MA*, *7*, 224.

Li, X., Jiang, P., Chen, T., Luo, X., ve Wen, Q. (2020). A survey on the security of blockchain systems. *Future generation computer systems*, *107*, 841-853.

Liao, K., Zhao, Z., Doupe, A., ve Ahn, G.-J. (2016). Behind closed doors: Measurement and analysis of cryptoLocker ransoms in bitcoin. *2016 APWG symposium on Electronic Crime Research (eCrime)*, 1-13. https://doi.org/10.1109/ECRIME.2016.7487938

Luu, L., Chu, D.-H., Olickel, H., Saxena, P., ve Hobor, A. (2016). *Making smart contracts smarter*. 254-269.

Margolin, N. B., ve Levine, B. N. (2008). Quantifying resistance to the sybil attack. içinde G. Tsudik (Ed.), *Financial cryptography and data security* (ss. 1-15). Springer. https://doi.org/10.1007/978-3-540-85230-8_1

Miner, G. D., Elder, J., Fast, A., Hill, T., Nisbet, R., ve Delen, D. (2012). *Practical text mining and statistical analysis for non-structured text data applications*. academic press.

Mosakheil, J. H. (2018). *Security threats classification in blockchains*.

Muntean, P., Grossklags, J., ve Eckert, C. (2017). Practical integer overflow prevention. *arXiv preprint arXiv:1710.03720*.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., ve Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies*. Princeton University Press.

O'Callaghan, D., Greene, D., Carthy, J., ve Cunningham, P. (2015). An analysis of the coherence of descriptors in topic modeling. *Expert systems with applications*, *42*(13), 5645-5657. https://doi.org/10.1016/j.eswa.2015.02.055

Özbay, Ö. (2015). Veri madenciliği kavramı ve eğitimde veri madenciliği uygulamaları. *uluslararası eğitim bilimleri dergisi*, *5*, Article 5.

Pilkington, M. (2016). Blockchain technology: Principles and applications. İçinde *Research handbook on digital transformations* (ss. 225-253). Edward Elgar Publishing.

Pilosov, A., ve Kapela, T. (2008). Stealing the Internet: An Internet-scale man in the middle attack. *NANOG-44, Los Angeles, October*, 12-15.

Prakash, R., Anoop, V. S., ve Asharaf, S. (2022). Blockchain technology for cybersecurity: A text mining literature analysis. *International Journal of Information Management Data Insights*, *2*(2), 100112. https://doi.org/10.1016/j.jjimei.2022.100112

Putz, B., ve Pernul, G. (2020). *Detecting blockchain security threats*. 313-320.

Ramage, D., Dumais, S., ve Liebling, D. (2010). *Characterizing microblogs with topic models*. *4*, 130-137.

Rathod, N., ve Motwani, D. (2018). Security threats on blockchain and its countermeasures. *Int. Res. J. Eng. Technol*, *5*(11), 1636-1642.

Ritter, A., ve Etzioni, O. (2010). *A latent dirichlet allocation method for selectional preferences*. 424-434.

Rodler, M., Li, W., Karame, G. O., ve Davi, L. (2018). *Sereum: Protecting Existing Smart Contracts Against Re-Entrancy Attacks* (No. arXiv:1812.05934). arXiv. https://doi.org/10.48550/arXiv.1812.05934

Rogerson, M., ve Parry, G. C. (2020). Blockchain: Case studies in food supply chain visibility. *Supply Chain Management: An International Journal*, *25*(5), 601-614. https://doi.org/10.1108/SCM-08-2019-0300

Rosenfeld, M. (2014). *Analysis of Hashrate-Based Double Spending* (No. arXiv:1402.2009). arXiv. https://doi.org/10.48550/arXiv.1402.2009

Saleh, F. (2021). Blockchain without Waste: Proof-of-Stake. *The Review of Financial Studies*, *34*(3), 1156-1190. https://doi.org/10.1093/rfs/hhaa075

Savaş, S., Topaloğlu, N., ve Yılmaz, M. (2012). Veri madenciliği ve Türkiye'deki uygulama örnekleri. *İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi*, *11*(21), 1-23.

Sebastiani, F. (2002). Machine learning in automated text categorization. *ACM Computing Surveys (CSUR)*, *34*(1), 1-47.

Sedlmeir, J., Smethurst, R., Rieger, A., ve Fridgen, G. (2021). Digital Identities and Verifiable Credentials. *Business ve Information Systems Engineering*, *63*(5), 603-613. https://doi.org/10.1007/s12599-021-00722-y

Sharma, C., Sharma, S., ve Sakshi. (2022). Latent dırıchlet allocation (LDA) based information modelling on blockchaın technology: A review of trends and research patterns used in integration. *Multimedia tools and applications*, *81*(25), 36805-36831.

Shu, K., Sliva, A., Wang, S., Tang, J., ve Liu, H. (2017). Fake news detection on social media: A data mining perspective. *acm sıgkdd explorations newsletter*, *19*(1), 22-36.

Steyvers, M., ve Griffiths, T. (2007). Probabilistic topic models. İçinde *Handbook of latent semantic analysis* (ss. 439-460). Psychology Press.

Stoll, C., Klaaßen, L., ve Gallersdörfer, U. (2019). The carbon footprint of bitcoin. *joule*, *3*(7), 1647-1661. https://doi.org/10.1016/j.joule.2019.05.012

Swan, M. (2015). *Blockchain: Blueprint for a new economy*. O'Reilly Media, Inc.

Şen, E., ve Alnıaçık, B. (2024). Blokzincir teknolojisinin yönetim süreçlerine olası etkileri üzerine inceleme. *The Journal of Social Sciences*, *34*(34), 660-673.

Tan, A.-H. (1999). *Text mining: The state of the art and the challenges*. *8*, 65-70.

Tan, P.-N., Steinbach, M., ve Kumar, V. (2016). *Introduction to data mining*. Pearson Education India.

Tang, X., Du, Y., Lai, A., Zhang, Z., ve Shi, L. (2023). Deep learning-based solution for smart contract vulnerabilities detection. *Scientific Reports*, *13*(1), 20106.

Tapscott, D., ve Tapscott, A. (2016). *Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world*. Penguin.

Taş, O., ve Kiani, F. (2018). Blok zinciri teknolojisine yapılan saldırılar üzerine bir inceleme. *Bilişim teknolojileri dergisi*, *11*(4), Article 4. https://doi.org/10.17671/gazibtd.451695

Taşkın, E., ve Doğru, İ. A. (2023). Blokzincir ve kötü amaçlı yazılımların kesişimi: kapsamlı bir inceleme ve analiz. *Gazi mühendislik bilimleri dergisi*, *9*(4), 58-69.

Tian, F. (2016). *An agri-food supply chain traceability system for China based on RFID ve blockchain technology*. 1-6.

Tuyisenge, M. J. (2021). *Blockchain technology security concerns: Literature review*.

Vurdu, S. A. (2021). Dış ticarette blokzincir uygulamaları. *Sosyal, Beşeri ve İdari Bilimler Dergisi*, *4*(9), 924-936.

Wang, C., ve Blei, D. M. (2011). *Collaborative topic modeling for recommending scientific articles*. 448-456.

Wang, L., Sheng, V. S., Düdder, B., Wu, H., ve Zhu, H. (2023). Security and privacy issues in blockchain and its applications. *IET Blockchain*, *3*(4), 169-171. https://doi.org/10.1049/blc2.12051

Witten, I. H., Frank, E., Hall, M. A., Pal, C. J., ve Data, M. (2005). *Practical machine learning tools and techniques*. *2*, 403-413.

Xu, M., Chen, X., ve Kou, G. (2019). A systematic review of blockchain. *Financial innovation*, *5*(1), 1-14.

Yaga, D., Mell, P., Roby, N., ve Scarfone, K. (2019). Blockchain technology overview. *arXiv preprint arXiv:1906.11078*.

Yli-Huumo, J., Ko, D., Choi, S., Park, S., ve Smolander, K. (2016). Where is current research on blockchain technology?—A systematic review. *PloS one*, *11*(10), e0163477.

Zhang, R., Xue, R., ve Liu, L. (2019). Security and privacy on blockchain. *ACM Computing Surveys (CSUR)*, *52*(3), 1-34.

Zhao, B. (2025). Towards a secure blockchain ecosystem: Current vulnerabilities and future directions in smart contract security. *ITM Web of Conferences, 73*, 03014. https://doi.org/10.1051/itmconf/20257303014

Zheng, Z., Xie, S., Dai, H., Chen, X., ve Wang, H. (2017). *An overview of blockchain technology: Architecture, consensus, and future trends*. 557-564.

Zyskind, G., Nathan, O., ve Pentland, A. "Sandy". (2015). Decentralizing privacy: using blockchain to protect personal data. *2015 IEEE Security and Privacy Workshops*, 180-184. https://doi.org/10.1109/SPW.2015.27

EKLER

Ek 1. LDA Modeli ile Belirlenen Konulara Ait Kelime Bulutları

Şekil 20. Konu 1 Kelime Bulutu

Şekil 21. Konu 2 Kelime Bulutu

Şekil 22.Konu 3 Kelime Bulutu

Şekil 23.Konu 4 Kelime Bulutu

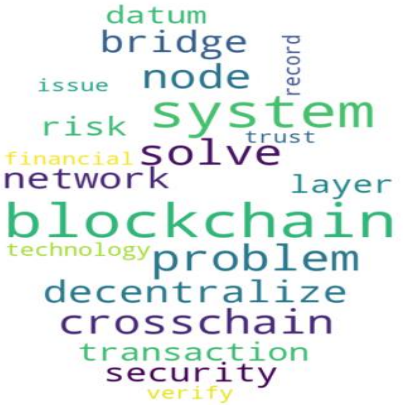
Şekil 24. Konu 5 Kelime Bulutu

Şekil 25. Konu 6 Kelime Bulutu

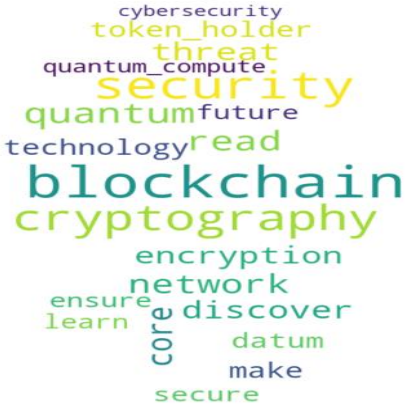
Şekil 26. Konu 7 Kelime Bulutu

Şekil 27. Konu 8 Kelime Bulutu

Şekil 28. Konu 9 Kelime Bulutu



Şekil 29. Konu 10 Kelime Bulutu



Şekil 30. Konu 11 Kelime Bulutu

Şekil 31. Konu 12 Kelime Bulutu

Şekil 32. Konu 13 Kelime Bulutu

Şekil 33. Konu 14 Kelime Bulutu

Şekil 34. Konu 15 Kelime Bulutu

Şekil 35. Konu 16 Kelime Bulutu

Şekil 36. Konu 17 Kelime Bulutu

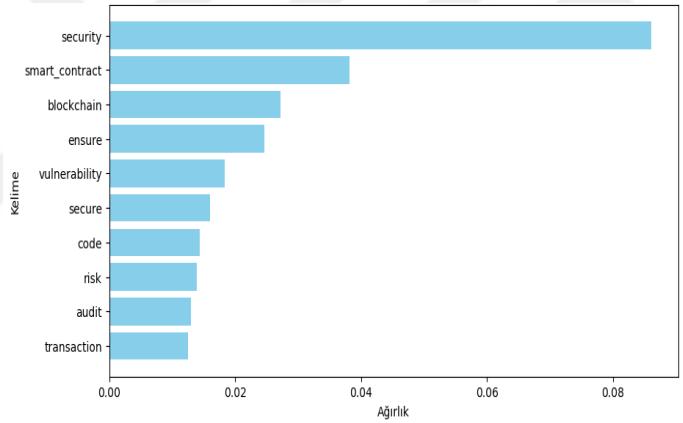
Şekil 37. Konu 18 Kelime Bulutu

Şekil 38.Konu 19 Kelime Bulutu

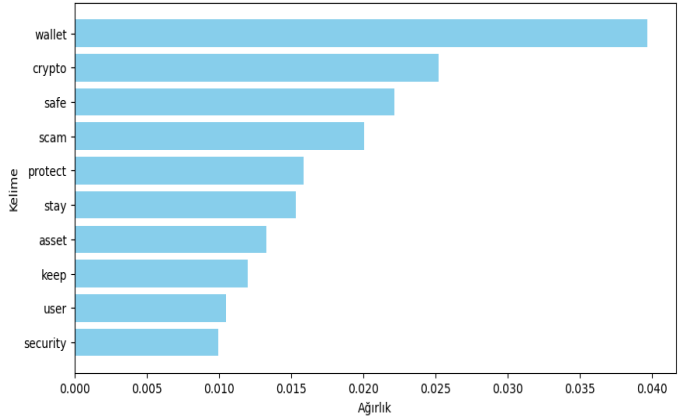
Şekil 39. Konu 20 Kelime Bulutu

Ek 2. LDA Modeli ile Belirlenen Konulara Ait Öne Çıkan Kelimeler

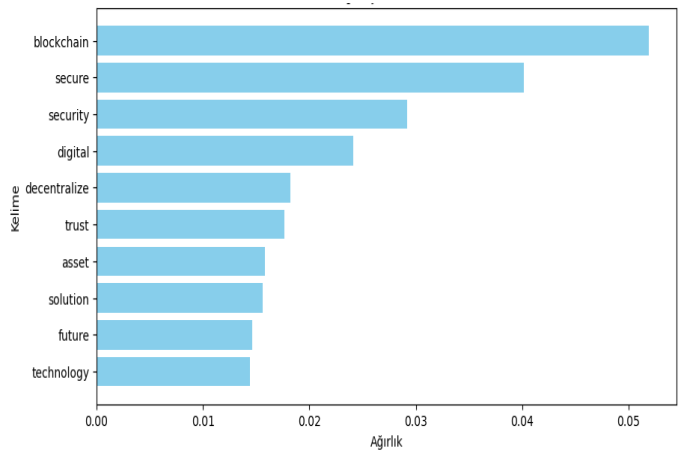
Şekil 40. Konu 1 İçin Önemli Kelimeler



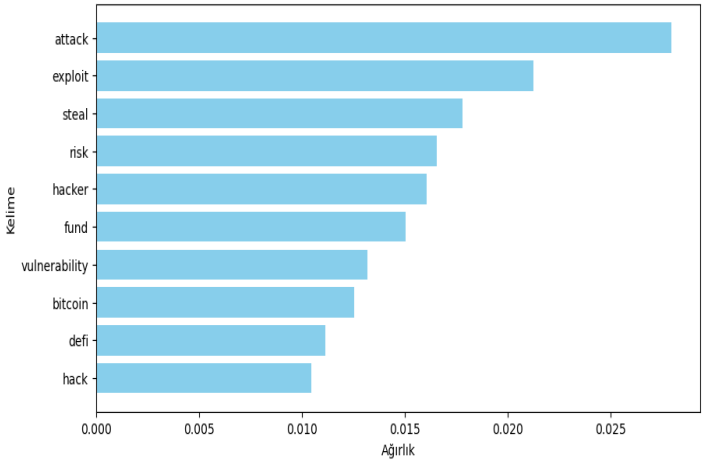
Şekil 41. Konu 2 İçin Önemli Kelimeler



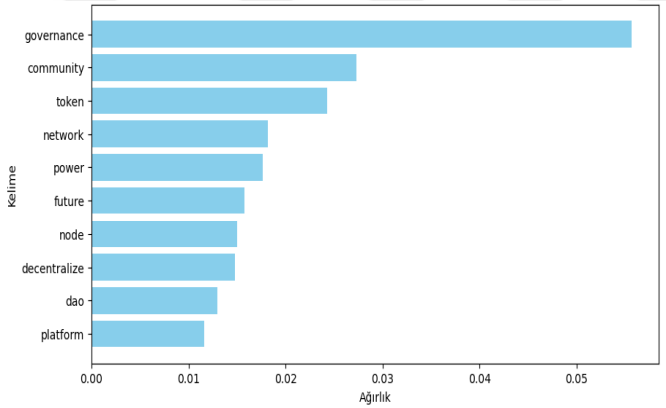
Şekil 42. Konu 3 İçin Önemli Kelimeler



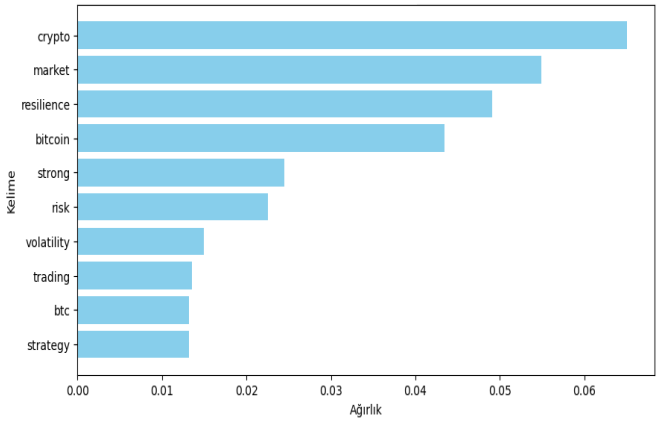
Şekil 43. Konu 4 İçin Önemli Kelimeler



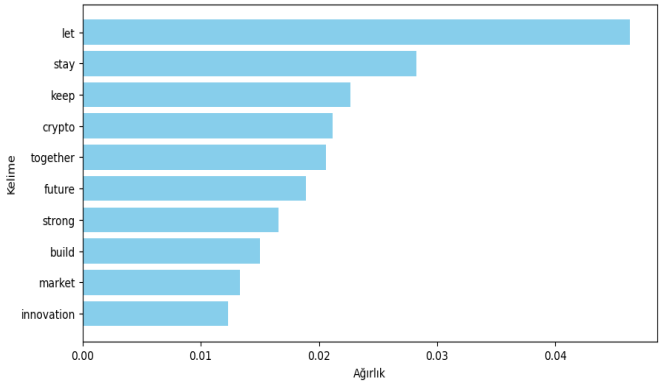
Şekil 44. Konu 5 İçin Önemli Kelimeler



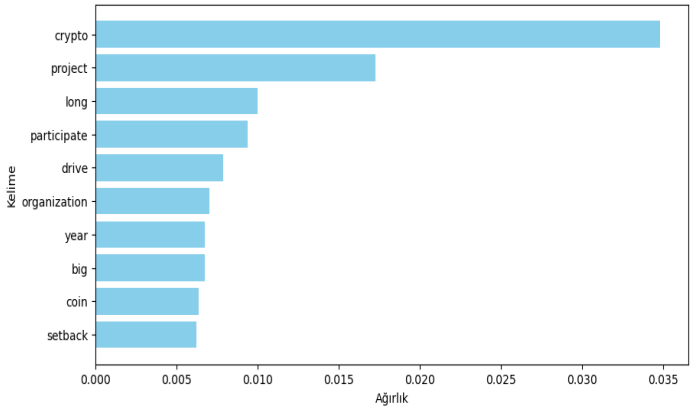
Şekil 45. Konu 6 İçin Önemli Kelimeler



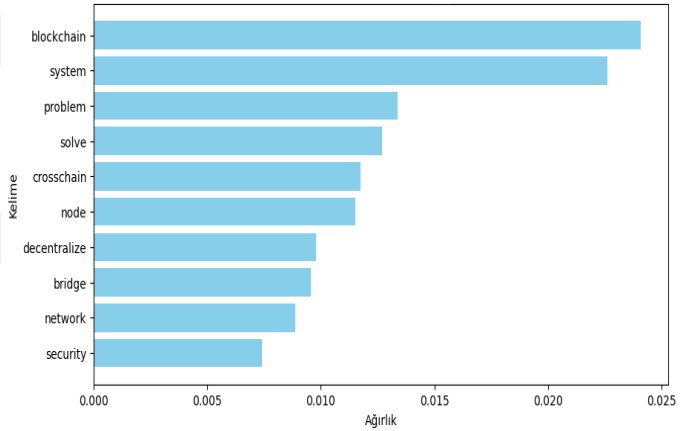
Şekil 46. Konu 7 İçin Önemli Kelimeler



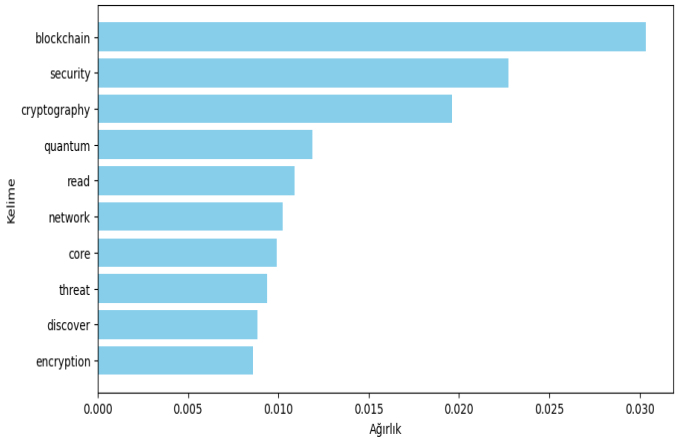
Şekil 47. Konu 8 İçin Önemli Kelimeler



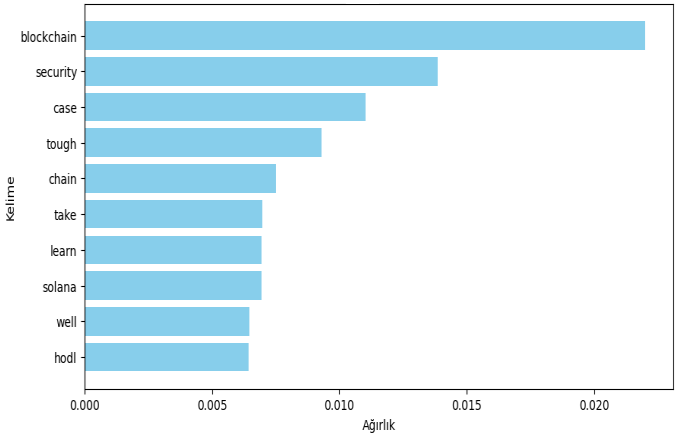
Şekil 48. Konu 9 İçin Önemli Kelimeler



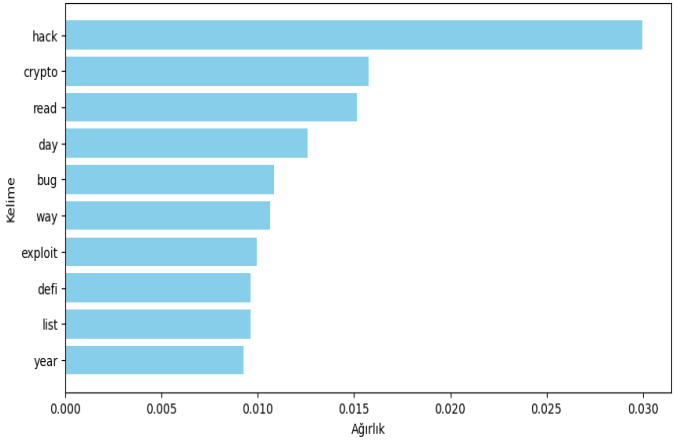
Şekil 49. Konu 10 İçin Önemli Kelimeler



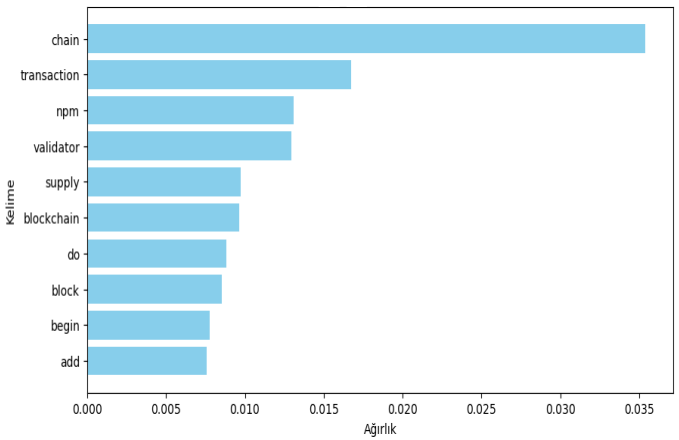
Şekil 50. Konu 11 İçin Önemli Kelimeler



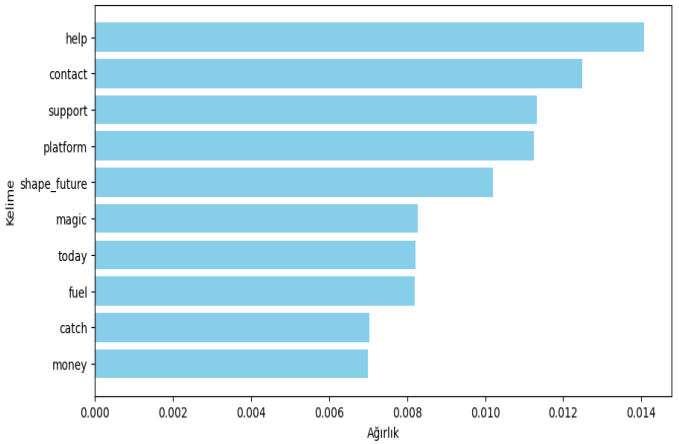
Şekil 51. Konu 12 İçin Önemli Kelimeler



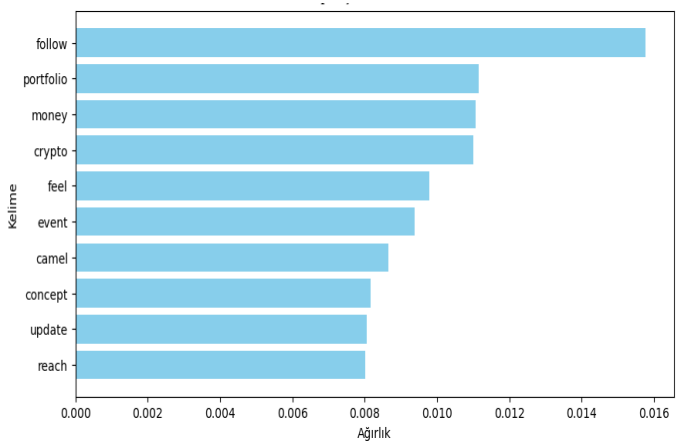
Şekil 52.Konu 13 İçin Önemli Kelimeler



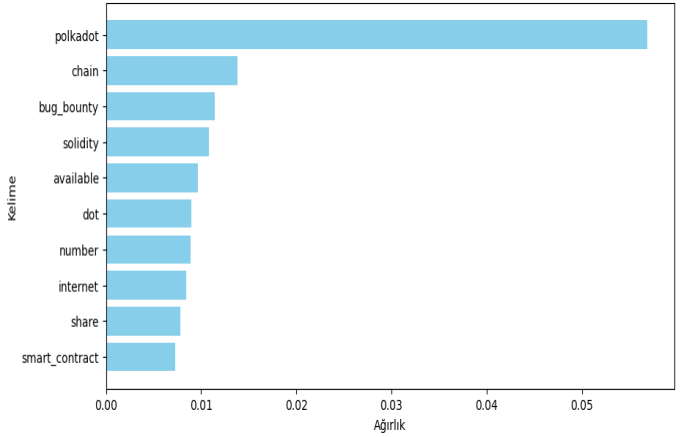
Şekil 53. Konu 14 İçin Önemli Kelimeler



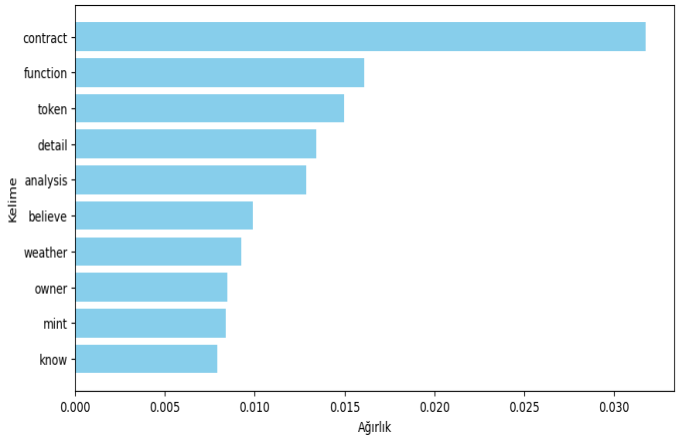
Şekil 54. Konu 15 İçin Önemli Kelimeler



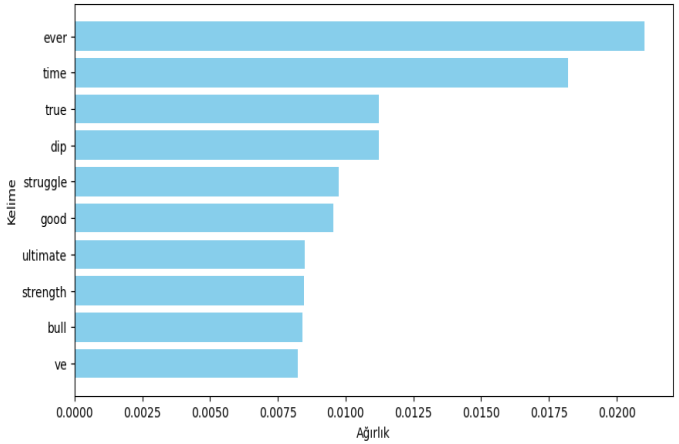
Şekil 55.Konu 16 İçin Önemli Kelimeler



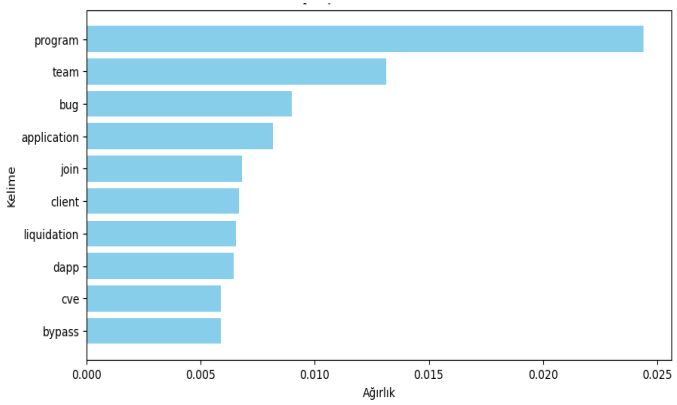
Şekil 56. Konu 17 İçin Önemli Kelimeler



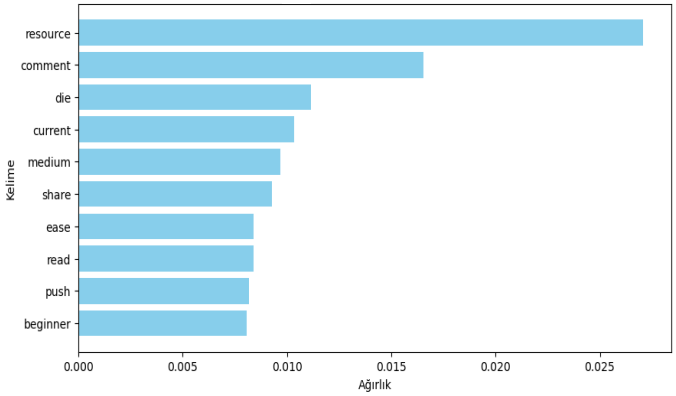
Şekil 57. Konu 18 İçin Önemli Kelimeler



Şekil 58. Konu 19 İçin Önemli Kelimeler

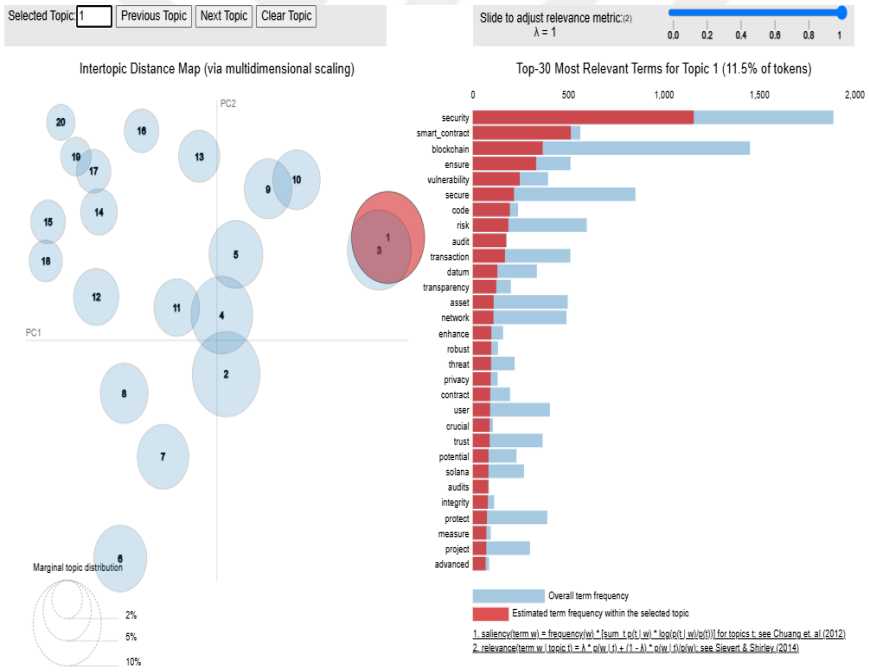


Şekil 59. Konu 20 İçin Önemli Kelimeler

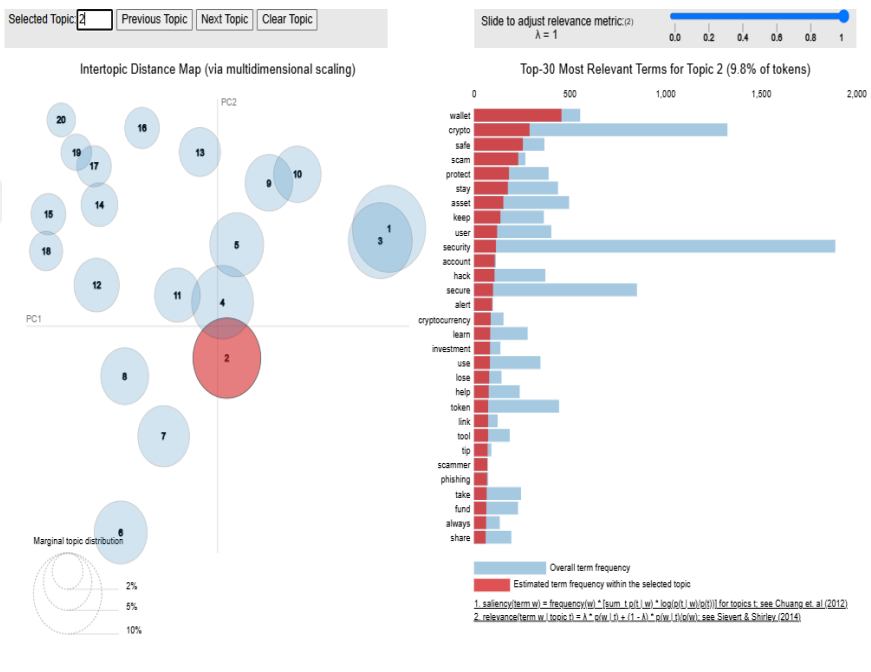


Ek 3. LDA Modeli Sonuçlarının pyLDAvis Görselleştirmesi

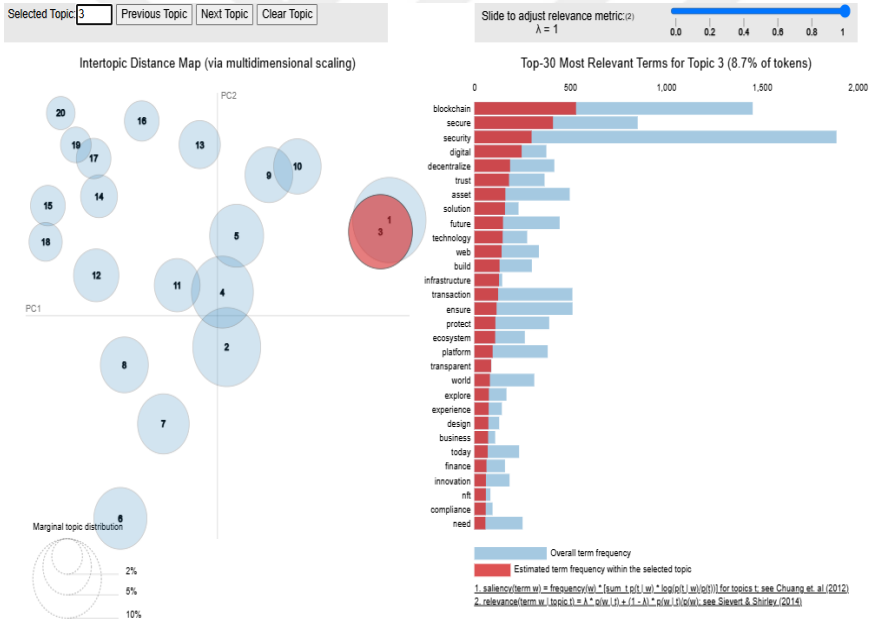
Şekil 60. Konular Arası Mesafe Haritası ve Konu 1 İçin En Alakalı 30 Terim



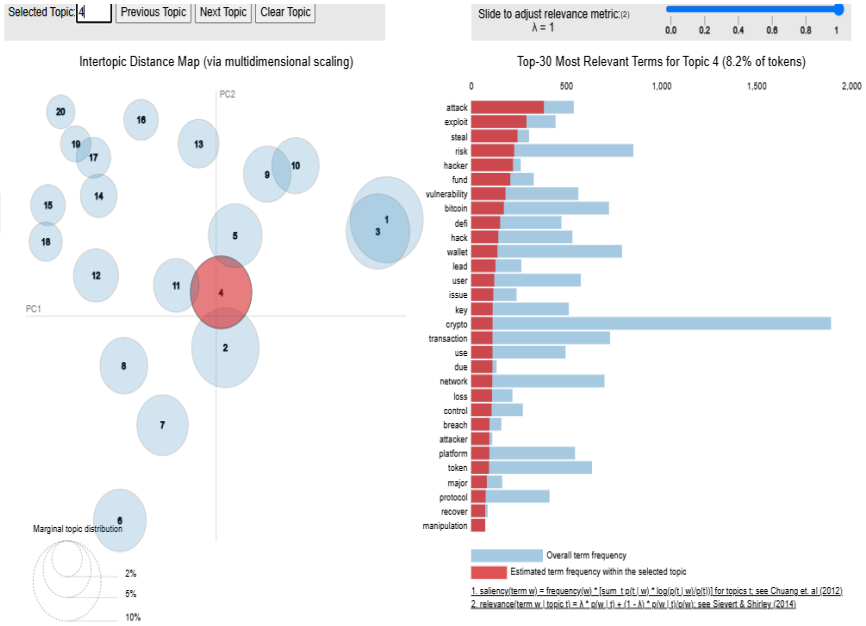
Şekil 61. Konular Arası Mesafe Haritası ve Konu 2 İçin En Alakalı 30 Terim



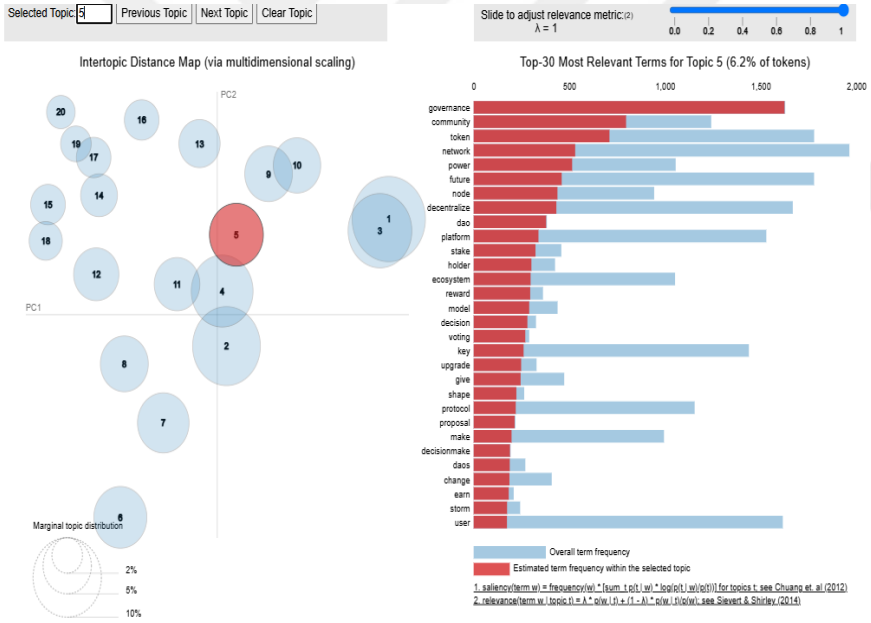
Şekil 62. Konular Arası Mesafe Haritası ve Konu 3 İçin En Alakalı 30 Terim



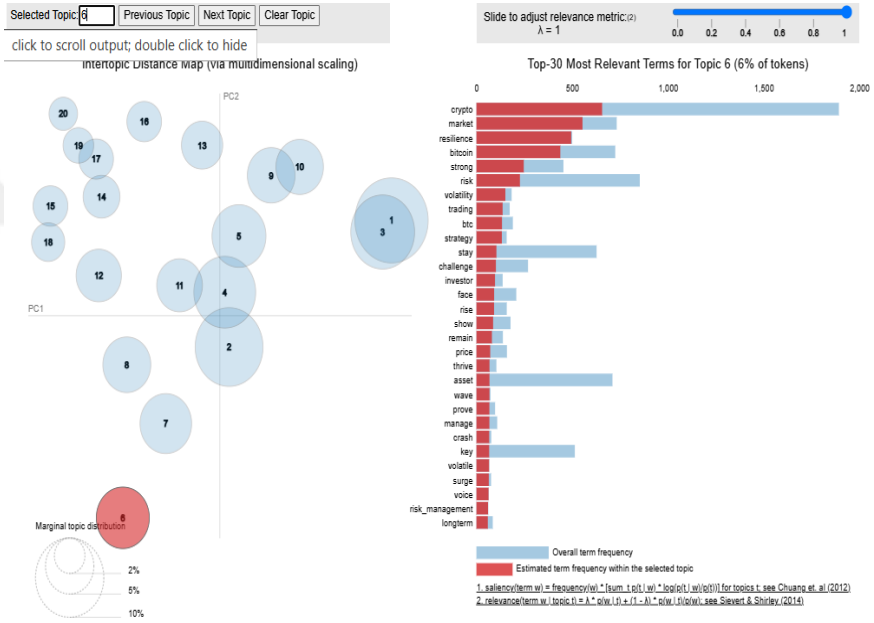
Şekil 63. Konular Arası Mesafe Haritası ve Konu 4 İçin En Alakalı 30 Terim



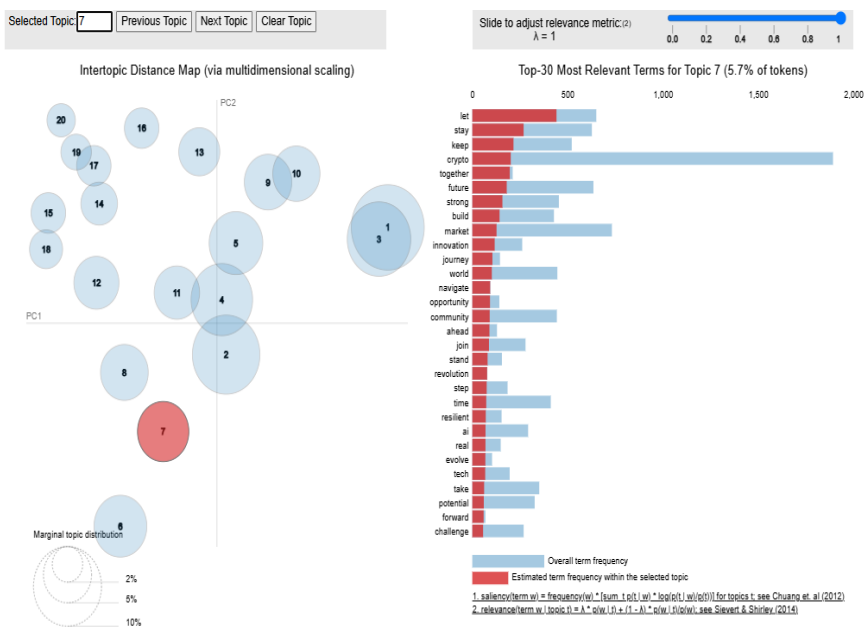
Şekil 64. Konular Arası Mesafe Haritası ve Konu 5 İçin En Alakalı 30 Terim



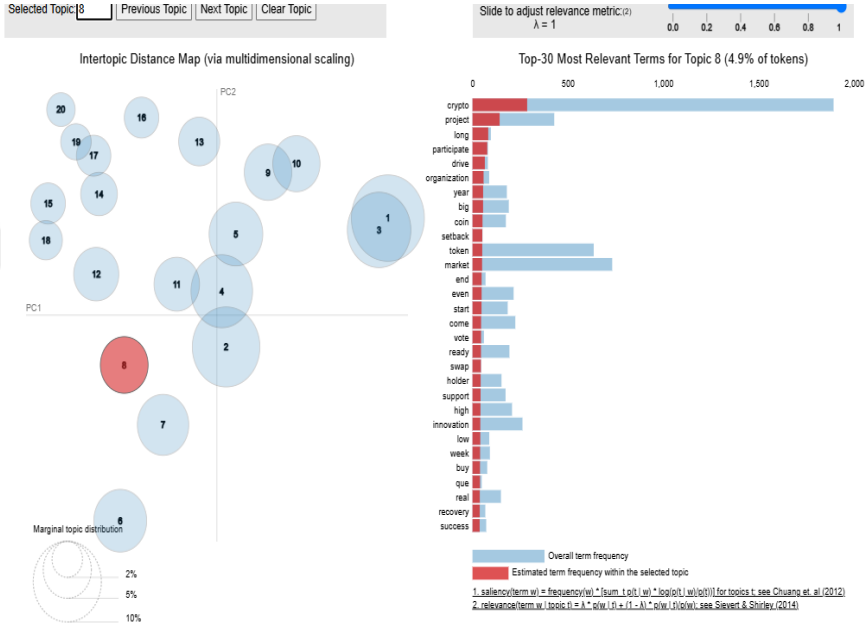
Şekil 65. Konular Arası Mesafe Haritası ve Konu 6 İçin En Alakalı 30 Terim



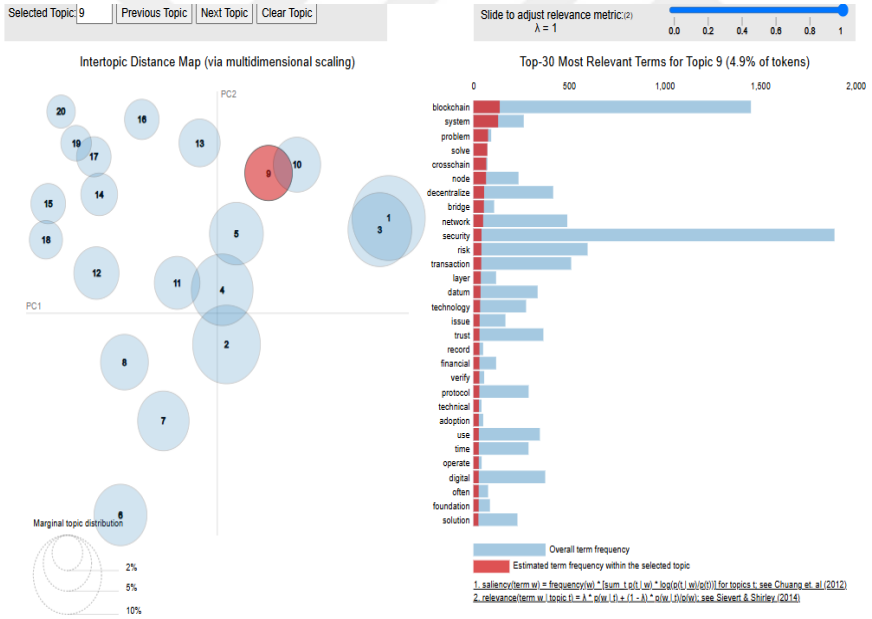
Şekil 66. Konular Arası Mesafe Haritası ve Konu 7 İçin En Alakalı 30 Terim



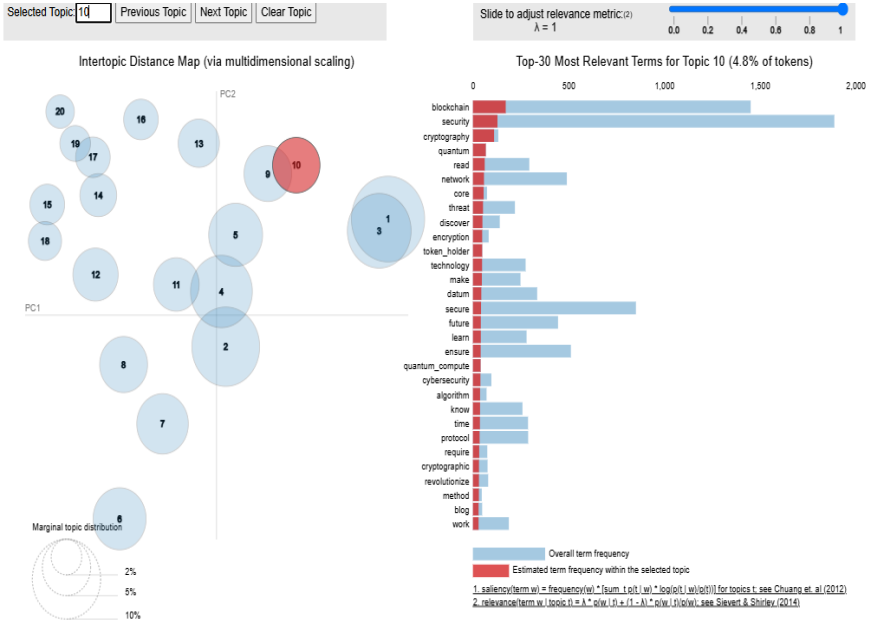
Şekil 67. Konular Arası Mesafe Haritası ve Konu 8 İçin En Alakalı 30 Terim



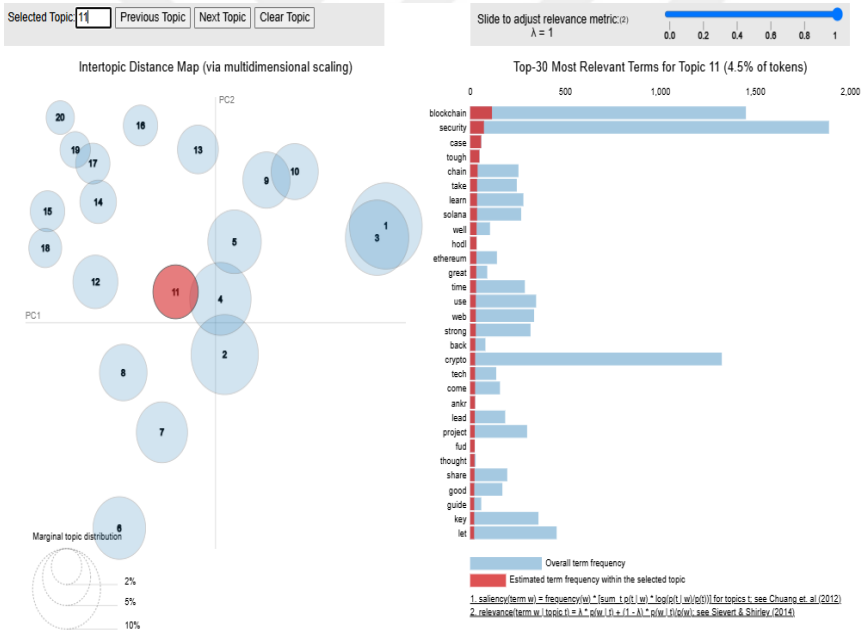
Şekil 68. Konular Arası Mesafe Haritası ve Konu 9 İçin En Alakalı 30 Terim



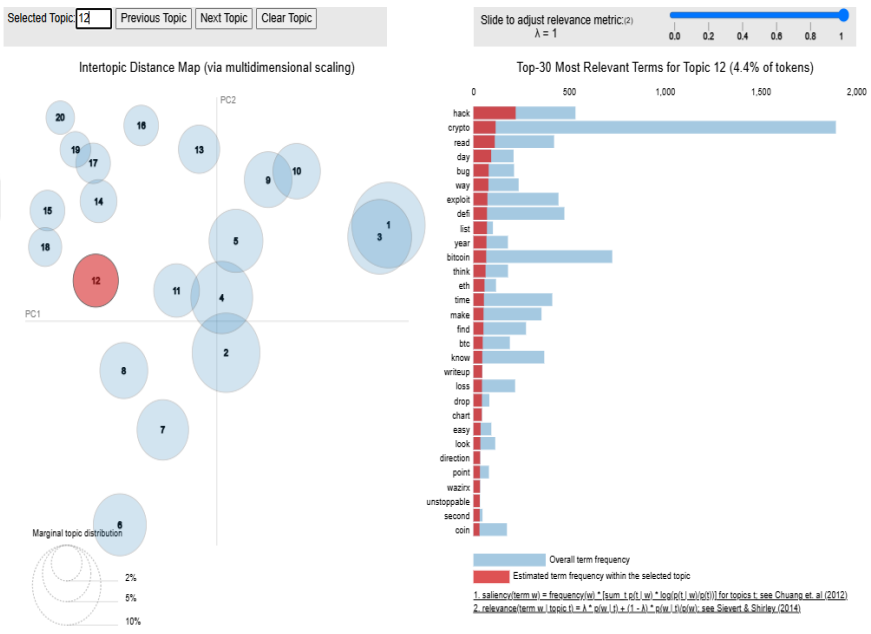
Şekil 69. Konular Arası Mesafe Haritası ve Konu 10 İçin En Alakalı 30 Terim



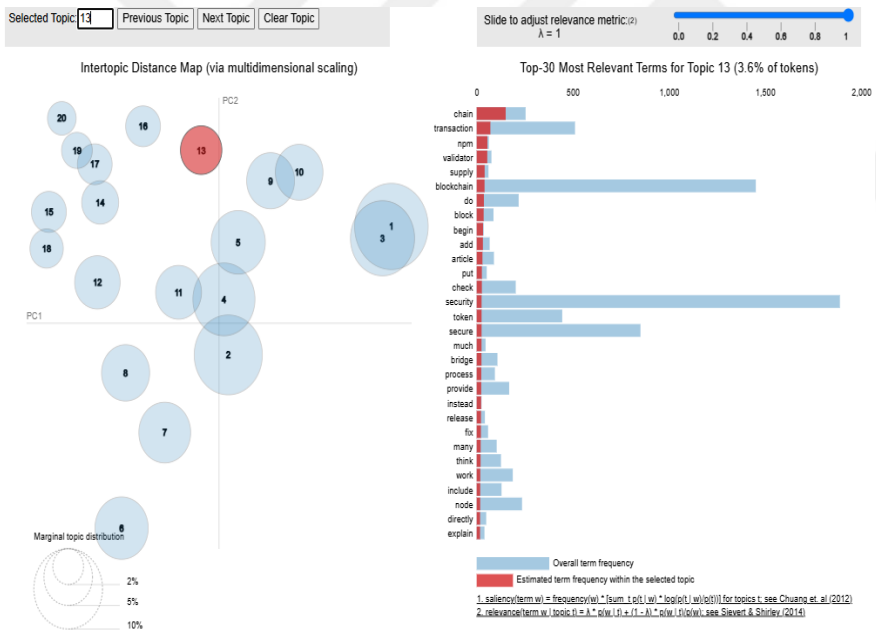
Şekil 70. Konular Arası Mesafe Haritası ve Konu 11 İçin En Alakalı 30 Terim



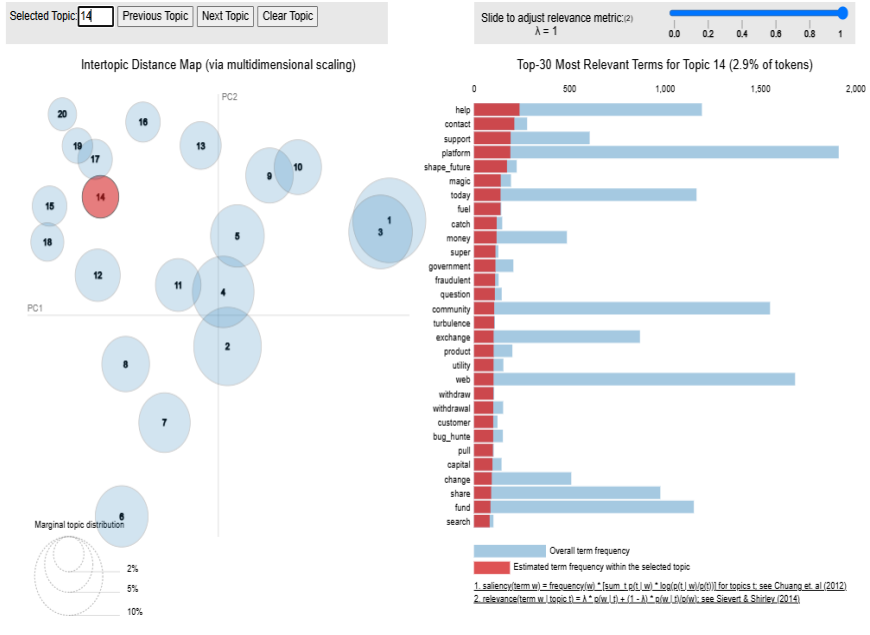
Şekil 71. Konular Arası Mesafe Haritası ve Konu 12 İçin En Alakalı 30 Terim



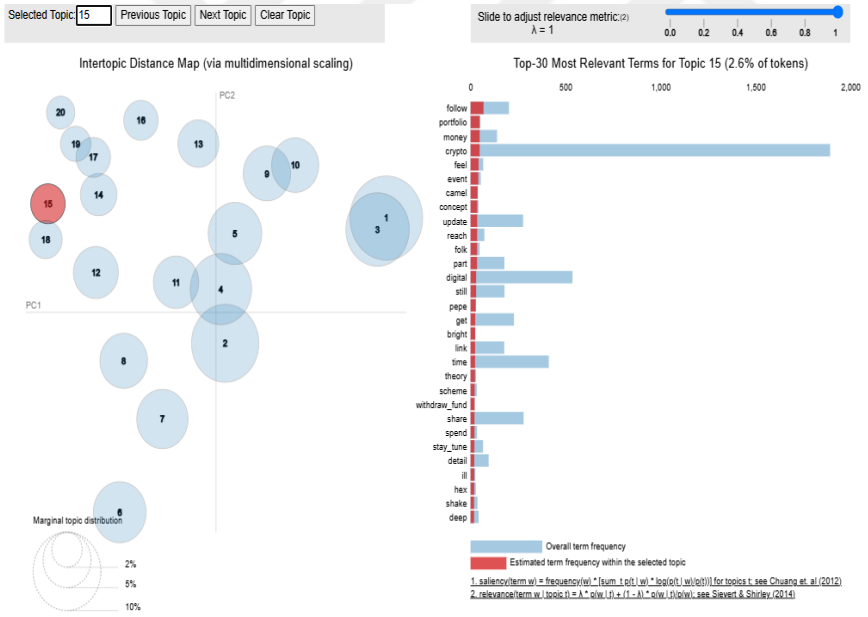
Şekil 72. Konular Arası Mesafe Haritası ve Konu 13 İçin En Alakalı 30 Terim



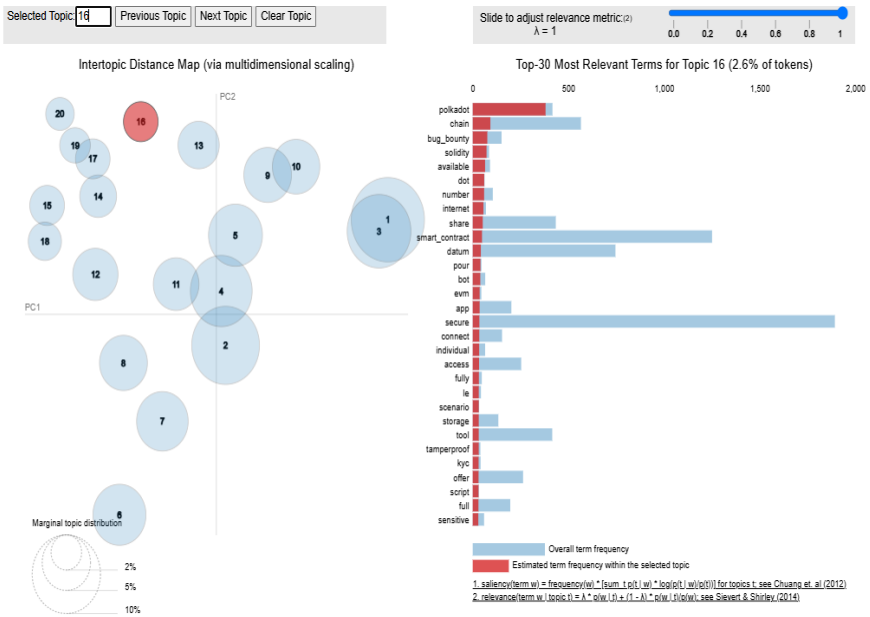
Şekil 73. Konular Arası Mesafe Haritası ve Konu 14 İçin En Alakalı 30 Terim



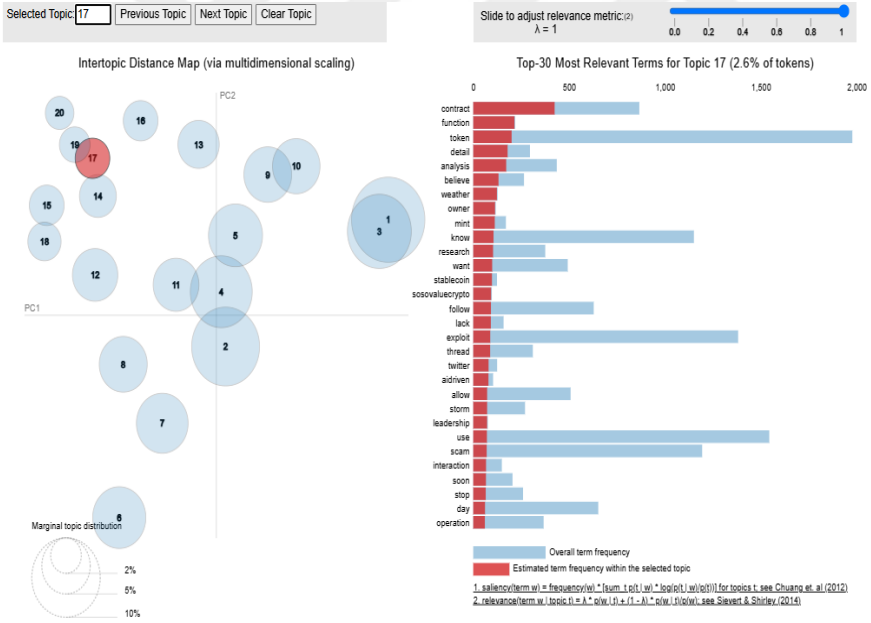
Şekil 74. Konular Arası Mesafe Haritası ve Konu 15 İçin En Alakalı 30 Terim



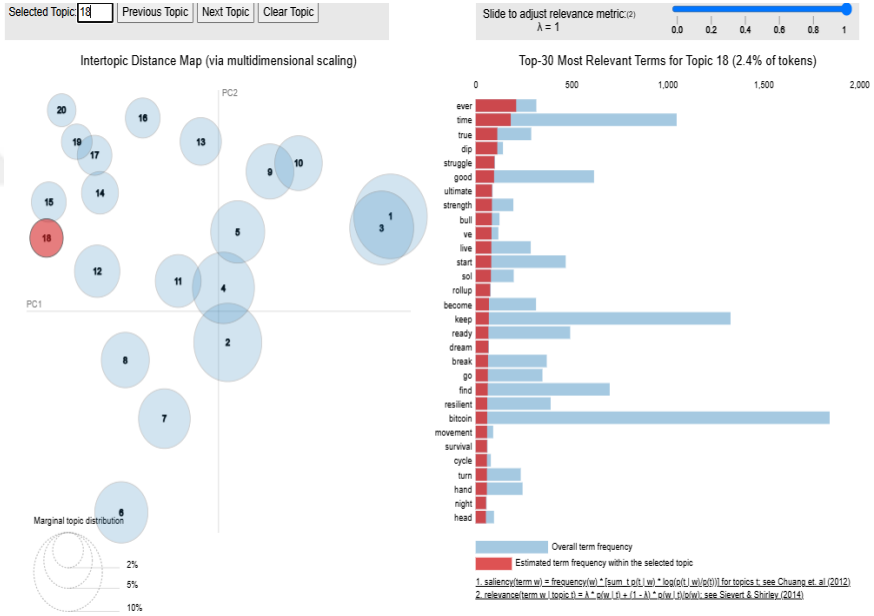
Şekil 75. Konular Arası Mesafe Haritası ve Konu 16 İçin En Alakalı 30 Terim



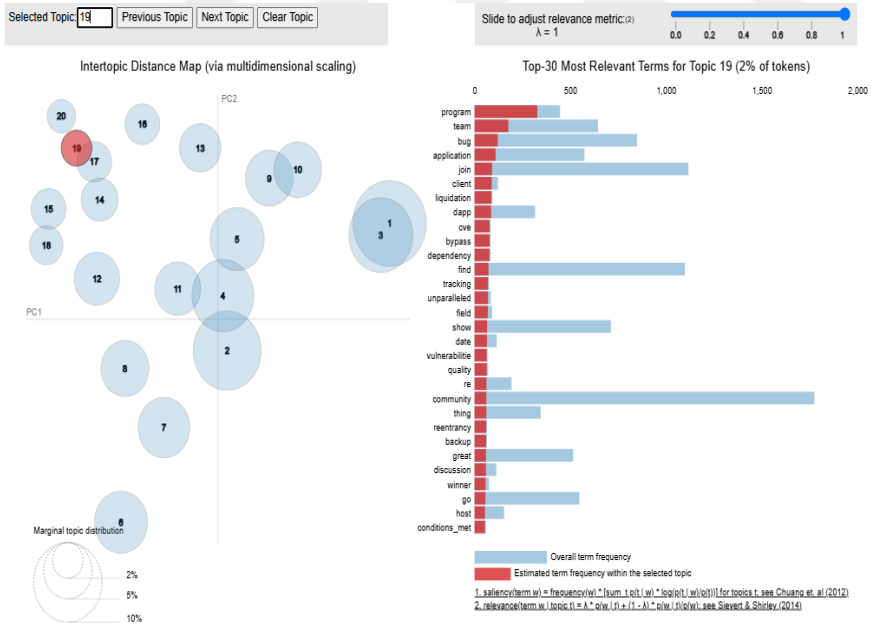
Şekil 76. Konular Arası Mesafe Haritası ve Konu 17 İçin En Alakalı 30 Terim



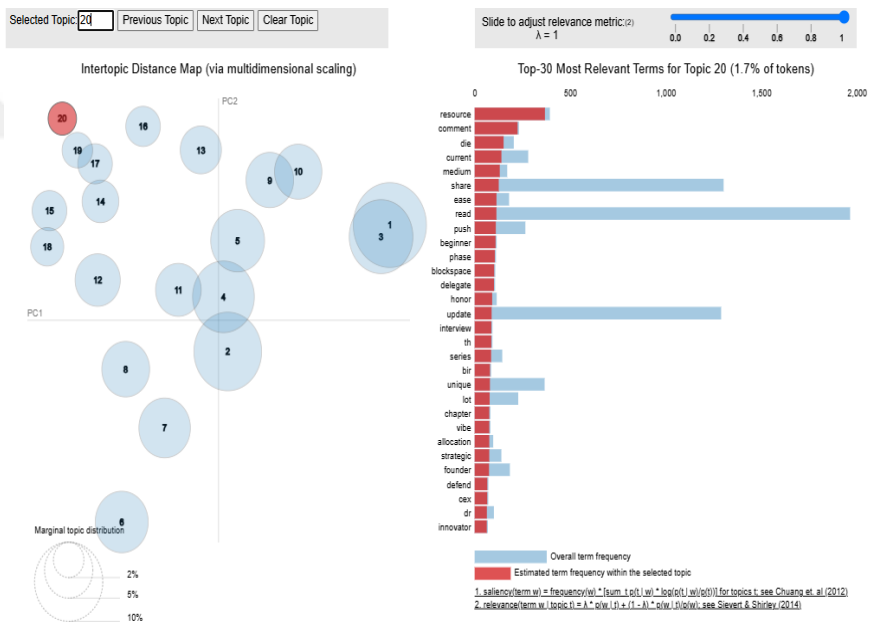
Şekil 77. Konular Arası Mesafe Haritası ve Konu 18 İçin En Alakalı 30 Terim



Şekil 78. Konular Arası Mesafe Haritası ve Konu 19 İçin En Alakalı 30 Terim



Şekil 79. Konular Arası Mesafe Haritası ve Konu 20 İçin En Alakalı 30 Terim



ÖZGEÇMİŞ

Tayfur AYAS, Lise eğitimini Elazığ'ın Baskil ilçesinde Baskil Lisesinde tamamlamıştır. 2018 2020 yılları arasında Mehmet Akif Ersoy Üniversitesi Bucak Emin Gülmez Teknik Bilimler Meslek Yüksek Okulundan Bilgi Yönetimi bölümünü tamamladı. Ardından DGS sınavı ile 2020 2023 yılları arasında Gümüşhane Üniversitesi Yönetim Bilişim Sistemleri bölümünü tamamladı. 2023 yılında başladığı Gümüşhane Üniversitesi Yönetim Bilişim Sitemleri Anabilim dalında halen Lisansüstü eğitimine devam etmektedir. Lisans eğitimi devam ederken 2209-A kapsamında bir TÜBİTAK projesi vardır.