©2025 Published in 11th International Symposium on Intelligent Technologies in Engineering and Science 16-18 May 2025 (ISITES2025 Diyarbakır - Turkey)

Blokzincir Türlerinin Sınıflanrıdılmasında Hibrit Yaklaşım: Makina Öğrenmesi ile Elde Edilen Özniteliklerin Bulanık Mantık Modelinde Kullanımı

[1,2]Burak Ağgül, [3]Gökhan Erdemir, [4]Tayfun Acarer,
[1]Bilişim Teknolojileri Bölümü, Sakarya Uygulamalı Bilimler Üniversitesi, Sakarya, Türkiye
[2]Bilgisayar Bilimleri ve Mühendisliği Bölümü, İstanbul Sabahattin Zaim Üniversitesi, İstanbul, Türkiye
[3]Dep. of Eng. Management and Technology, The University of Tennessee at Chattanooga, Chattanooga, TN, USA
[4]Motorlu Araçlar ve Ulaştırma Teknolojileri Bölümü, Piri Reis Üniversitesi, İstanbul, Türkiye

Özet

Blokzincir platformları, güvenlik, gizlilik ve performans açısından farklı teknik özelliklere sahiptir. Doğru platform seçimi için bu özelliklerin kapsamlı ve sistematik bir şekilde değerlendirilmesi önemlidir. Bu çalışma, performans ve mimari odaklı geleneksel sınıflandırma yaklaşımlarının ötesine geçerek, teknik ve kriptografik parametreleri temel alan kapsamlı bir değerlendirme sunmaktadır. Bu kapsamda, 31 farklı blokzincir platformu; teknik (TPS, enerji tüketimi, gizlilik türü, konsensüs algoritması) ve kriptografik (şifreleme algoritması) parametreler kullanılarak sınıflandırılmıştır. Platform türlerinin belirlenmesinde Makine Öğrenmesi (Random Forest) ve Bulanık Mantık modelleri karşılaştırmalı olarak incelenmiştir. Random Forest modeli, mevcut veri setinde %100 doğruluk sağlamış ancak bu sonuç veri setine özgüdür ve genelleme yeteneğinin değerlendirilmesi gerekir. Aşırı uyum riski nedeniyle farklı veri setleri üzerinde test edilmesi önerilmektedir. Ayrıca, modelin karar verme süreci kara kutu olarak kabul edildiğinden, açıklanabilirliği sınırlıdır. Diğer yandan, klasik bulanık mantık modeli başlangıçta yalnızca %22,58 doğruluk sağlamıştır. Ancak, Random Forest modelinden elde edilen sonuçlar rehberliğinde oluşturulan hibrit bulanık mantık modeli, doğruluğunu %87,10'a yükseltmiştir. Kolay uygulanabilirliği ve hesaplama kompleksi tisinin düşük olması sebebiyle hibrit bulanık mantık modelinin doğruluğu birçok uygulama için yeterli seviyededir. Bu hibrit yapı, makine öğrenmesi sonuçlarını kullanarak bulanık mantık modelinin açıklanabilirliğini ve doğruluğunu artırmayı amaçlamaktadır.

Anahtar Kelimeler: Blokzincir, Random Forest, Bulanık Mantık, Sınıflandırma, Kriptografik Parametreler.

1. Giriş

Blokzincir teknolojileri, Bitcoin gibi kripto paraların ötesinde; sağlık sistemlerinde, tedarik zinciri izlenebilirliğinde, kimlik doğrulama altyapılarında ve IoT ağlarında geniş bir uygulama alanına sahiptir [1], [2]. Bu çeşitlilik, blokzincir teknolojisinin dağıtık yapı sunmasının yanında, gizlilik, işlem kapasitesi, veri bütünlüğü ve güvenlik gibi teknik parametreleri de etkin biçimde sağlamasıyla ilişkilidir. Bir blokzincir sisteminin kamuya açık (public), özel (private) ya da konsorsiyum tabanlı (consortium) olarak tercih edilmesi; genellikle teknik kapasite, enerji verimliliği, güvenlik mimarisi (örneğin post-quantum encryption) ve konsensüs protokolünün güvenlik-performans dengesi gibi kriterlere dayanır [3], [4].

Çalışmanın özgün katkısı olarak, platformların kullandığı şifreleme algoritmaları da modelleme sürecine dahil edilmiştir. Literatürde bu konuda sınırlı sayıda çalışma bulunmaktadır [5].

Bu çalışma, literatürde yaygın olan performans ve mimari odaklı sınıflandırmaların ötesinde, teknik ve kriptografik parametreleri temel alan sistematik bir sınıflandırma sunmaktadır. Bu amaçla makine öğrenmesi (Random Forest) ve açıklanabilir yapay zekâ (Fuzzy Logic) yöntemleri kullanılarak blokzincir platformlarının İzinsiz (Permissionless), Konsorsiyum (Consortium) ve İzinli (Permissioned) türlerinden hangisine ait olduğunun belirlenmesi hedeflenmiştir. Bu nedenle çalışma, akademik katkılarının yanında uygulamaya dönük sonuçlar da içermektedir [6].

2. Materyal ve Method

Bu çalışmada, blokzincir platformlarının sınıflandırılması için teknik ve kriptografik parametreler temel alınarak makine öğrenmesi ve bulanık mantık tabanlı hibrit bir model geliştirilmiştir. Yöntem, 31 farklı blokzincir platformunun performans, enerji verimliliği, gizlilik ve güvenlik özelliklerini sistematik olarak analiz ederek, Random Forest algoritması ile elde edilen sonuçların bulanık mantık kurallarını optimize etmesi prensibine dayanmaktadır.

2.1. Teknik Parametreler ve Veri Seti

Bu çalışmada blokzincir platformlarının sınıflandırılması için kullanılan temel teknik ve kriptografik parametreler aşağıda açıklanmıştır. Literatürde bu parametreler, platformların tasarımında ve performans-güvenlik dengesinin sağlanmasında kritik öneme sahip olarak değerlendirilir [6], [7].

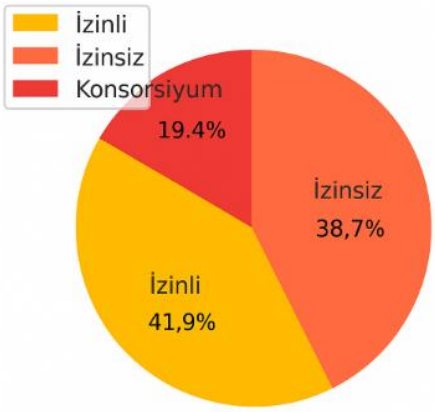
Saniye Başına İşlem Sayısı (TPS-Transaction Per Second): Blokzincirin saniyede gerçekleştirebildiği işlem sayısıdır. Ölçeklenebilirlik açısından önemli bir ölçüt olup, platformun uygulama türünü doğrudan etkiler. Örneğin, yüksek TPS değerine sahip Solana platformu (50.000 TPS), IoT veya mikro ödeme sistemleri için cazip hale gelmektedir [8].

Enerji: Konsensüs algoritmasına bağlı olarak işlem başına harcanan enerji miktarını ifade eder. Özellikle Proof-of-Work (PoW) tabanlı platformlarda (örneğin Bitcoin) enerji tüketimi yüksektir. Bu çalışmada enerji tüketimi "Low", "Medium" ve "High" olarak kategorize edilmiştir [9].

Gizlilik: Blokzincir üzerindeki verilere kimlerin erişebileceğini belirleyen mimari yapıyı ifade eder. Public (herkesin erişebildiği), Private (yetkili düğümlerin erişebildiği) ve Consortium/Hybrid (sınırlı dağıtık erişim sunan) olmak üzere üç ana tür bulunmaktadır [10].

Konsensüs Algoritması: Ağdaki düğümlerin veri bütünlüğünü sağlamak ve yeni blokları eklemek için kullanılan algoritmadır. PoW, PoS, PBFT, IBFT ve RAFT gibi çeşitli türleri bulunur ve platformun performansını, enerji tüketimini ve güvenliğini doğrudan etkiler [11].

Şifreleme Tipi: Platformların kullandığı temel şifreleme algoritmalarıdır. Yaygın olarak kullanılan algoritmalar arasında ECDSA, Ed25519, BLS, SM2 ve PQ (Post-Quantum) yer alır. Bu parametre, platformların veri bütünlüğü ve kuantum saldırılarına karşı dayanıklılığını belirlemek açısından önemlidir [12]. Bu parametreler, Bitcoin, Ethereum, Hyperledger Fabric, Algorand gibi yaygın 31 farklı blokzincir platformundan derlenmiştir.



Şekil 1: Blokzincir Türlerine Göre Yüzde Dağılımı.

Şekil 1' de görüldüğü üzere, çalışmada kullanılan veri setinde platformların çoğunluğunu İzinli (%41,9) türü oluşturmakta, ardından İzinsiz (%38,7) ve Konsorsiyum (%19,4) türleri gelmektedir. Platformlara ait özellikler ise Tablo 1' de özetlenmiştir.

Tablo 1. Blokzincir Platformlarının Teknik Özellikleri [4-14].

Platform	TPS	Gizlilik	Şifreleme	Konsensüs	Tür
Bitcoin	7	Açık	ECDSA	PoW	İzinsiz
Ethereum	15	Açık	ECDSA	PoW/PoS	İzinsiz
Hyperledger Fabric	3000	Özel	ECDSA	PBFT	İzinli
Hyperledger Sawtooth	1000	Özel	SHA256	PoET	İzinli
Hyperledger Indy	100	Özel	BLS	RBFT	İzinli
Hyperledger Iroha	400	Özel	Ed25519	YAC	İzinli
Hyperledger Burrow	500	Özel	Tendermint	Tendermint	İzinli
Hyperledger Besu	300	Özel	ECDSA	QBFT	İzinli
Quorum	2000	Konsorsiyum	ECDSA	IBFT	Konsorsiyum
R3 Corda	150	Konsorsiyum	Özel	Özel	Konsorsiyum
Cardano	250	Açık	Ed25519	Ouroboros	İzinsiz
Algorand	1000	Açık	PQ	Pure PoS	İzinsiz
Solana	50000	Açık	Ed25519	Tower BFT	İzinsiz
Stellar	1000	Açık	Ed25519	SCP	İzinsiz
Ripple	1500	Konsorsiyum	ECDSA	RPCA	Konsorsiyum
Neo	1000	Açık	dBFT	dBFT	İzinsiz
IOTA	1500	Açık	Özel	DAG	İzinsiz
Polkadot	1000	Açık	Ed25519	NPoS	İzinsiz
FISCO BCOS	2000	Özel	SM2	RAFT	İzinli
AntChain	5000	Özel	SM2	HoneybadgerBFT	İzinli
Tendermint	1000	Açık	Tendermint	Tendermint	İzinsiz
Cosmos	1000	Açık	Tendermint	Tendermint	İzinsiz

IPFS	100	Özel	SHA256	RAFT	İzinli
Private Zookeeper	100	Özel	SHA256	Paxos/Kafka	İzinli
Google Chubby	50	Özel	Paxos	Paxos	İzinli
MOBI	1000	Konsorsiyum	MOBI Konsensüsü	Özel	Konsorsiyum
TradeLens	1000	Özel	RAFT	RAFT	İzinli
Vechain	1000	Özel	PoA	PoA	İzinli
Symbiont	1200	Konsorsiyum	BFT-SMART	BFT-SMART	Konsorsiyum
Libra	1000	Konsorsiyum	LibraBFT	LibraBFT	Konsorsiyum
Hedera	10000	Açık	Hashgraph	Hashgraph	İzinsiz

2.2. Makine Öğrenmesi ile Sınıflandırma

Kurgulanan hibrit modelde, blokzincir platformlarının türlerini belirlemek amacıyla, bu çalışmada denetimli makine öğrenmesi algoritmalarından Random Forest (RF) kullanılmıştır. RF, karar ağaçları topluluğu (ensemble learning) tabanlı bir yöntem olup, sınıflandırma işlemlerinde yüksek doğruluk sağlaması ve özniteliklerin önem derecesini analiz edebilmesi nedeniyle tercih edilmiştir [13]. Ancak RF modelinin elde ettiği %100 doğruluk oranı, kullanılan veri setine özgü olup, modelin genelleme yeteneği (overfitting) konusunda risk barındırmaktadır. Bu nedenle, RF modeli tarafından elde edilen sonuçlar, bulanık mantık modelinin doğruluğunu artırmak ve modelin açıklanabilirliğini sağlamak amacıyla rehber olarak kullanılmıştır. Bu hibrit yaklaşım, makine öğrenmesi algoritmalarının güçlü sınıflandırma yeteneklerini, bulanık mantık modelinin açıklanabilirlik avantajları ile birleştirerek daha güvenilir ve açıklanabilir sonuçlar elde etmeyi amaçlamaktadır. Çalışmada kullanılan veri seti, %70 eğitim ve %30 test olacak şekilde ayrılmıştır.

2.2.1. Giriş Öznitelikleri

Bu çalışmada kullanılan ölçüm metrikleri ve kodlama şemaları şu şekildedir: Saniye Başına İşlem Sayısı (Transaction Per Second - TPS), sistem performansını değerlendirmek üzere doğrudan sayısal değerlerle ifade edilmiştir. Enerji (Energy) tüketimi, düşük (Low=0), orta (Medium=1) ve yüksek (High=2) olmak üzere üç seviyede kategorize edilerek kodlanmıştır. Gizlilik (Privacy) düzeyi ise kamuya açık (Public=0), hibrit (Hybrid=1) ve özel (Private=2) olarak üç farklı seviyede sınıflandırılmıştır. Şifreleme Türü (Encryption Type) için dört farklı algoritma tanımlanmış olup, bunlar sırasıyla ECDSA=0, Ed25519=1, SM2=2 ve PQ=3 şeklinde kodlanmıştır. Konsensüs Algoritması (Consensus Algorithm) parametresi ise her bir algoritmaya özgü sayısal etiketler atanarak nicelleştirilmiştir. Bu kodlama yöntemleri, veri analizi sürecinde kategorik değişkenlerin nicel olarak işlenebilmesine olanak sağlamaktadır.

2.2.2. Çıkış Sınıfları

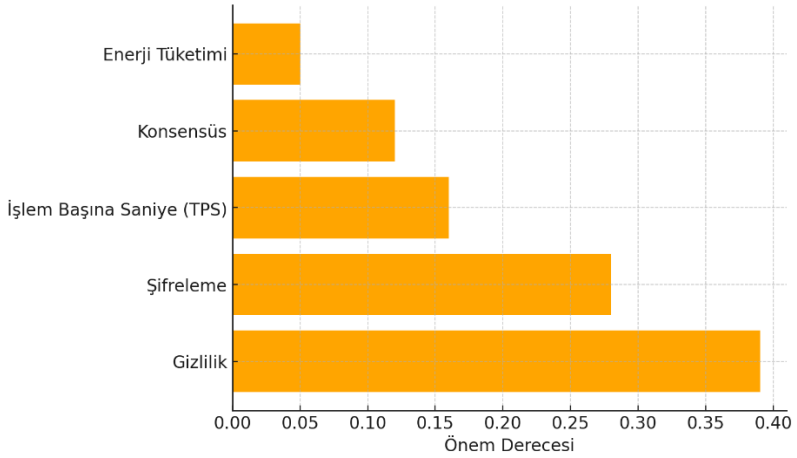
Bu çalışmada kullanılan Blok Zinciri Türü (Blockchain Type) parametresi, izinsiz (Permissionless=0), konsorsiyum (Consortium=1) ve izinli (Permissioned=2) olmak üzere üç farklı yapıyı temsil edecek şekilde sayısal olarak kodlanmıştır. Model eğitimi aşamasında bu parametrelerin yanı sıra diğer tüm özellikler değerlendirilmiş ve eğitim sonrasında elde edilen

önem sıralaması sonuçları Tablo 2' de detaylı bir şekilde sunulmuştur. Bu tablo, her bir özniteliğin model kararları üzerindeki göreceli etkisini nicel olarak ortaya koymaktadır.

Tablo 2. Öznitelik Önem Derecesi

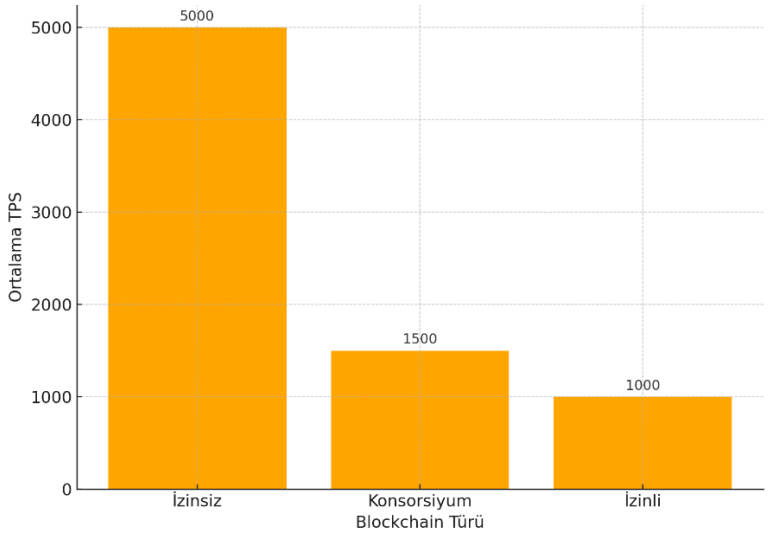
Öznitelik	Önem Derecesi
Gizlilik	0.39
Şifreleme Tipi	0.28
TPS	0.16
Konsensus	0.12
Enerji	0.05

Random Forest modelinin test verisi üzerindeki sınıflandırma başarısı kullandığımız veri setine özgü olup model üzerinde ezberleme yapması durumları da gözönünde bulundurularak başka bir yöntem ile desteklenmesi hibrit bir model oluşturmasını amaçladık. Bunu yapabilmek için gerekli olan adımlar. Bu yüksek doğruluk, seçilen özniteliklerin blokzincir türlerini ayırt etmede güçlü bir temsil gücüne sahip olduğunu göstermektedir. Özellik önem derecesi analizi sonucunda en önemli parametreler sırasıyla Gizlilik (Privacy) (%39) ve Şifreleme (Encryption) (%28) olarak belirlenmiştir. Diğer parametreler olan TPS ve Konsensus (Consensus) daha düşük oranlarda etki ederken, Enerji (Energy) parametresinin etkisi sınırlı kalmıştır (Şekil 2) [14].



Şekil 2: Random Forest Modelinde Özellik Önem Dereceleri.

Elde edilen sonuçlar, literatürdeki bulgularla da örtüşmektedir. Örneğin, izinli (Permissioned) sistemlerde genellikle Private gizlilik mimarileri tercih edilmekte ve bu yapılar daha düşük TPS değerleriyle çalışmaktadır [15]. Bu doğrultuda Şekil 3' de gösterildiği gibi "İzinsiz", "Konsorsiyum" ve "İzinli" olarak üç farklı gizlilik seviyesi incelenmiş, izinsiz (Permissionless) platformların genellikle daha yüksek TPS değerlerine sahip olduğu ve şifreleme (Encryption) parametresinin sınıflandırmada belirleyici bir role sahip olduğu görülmüştür (Şekil 3).



Şekil 3: Blokzincir Türlerine Göre Ortalama TPS Değerleri.

Kullanılan özniteliklerin ayrıştırıcı gücü, modelin genelleme yeteneğinin yüksek olduğunu göstermektedir [14]. Random Forest modelinden elde edilen öznitelik önem sıralaması sonraki aşamada oluşturulan bulanık mantık modeli için bir kılavuz olarak kullanılmıştır.

2.3. BULANIK MANTIK İLE SINIFLANDIRMA

Makine öğrenmesi tabanlı modeller genellikle yüksek doğruluk oranları sağlamakla birlikte, bazı olumsuz süreçleri de beraberinde getirmektedir. Örneğin, modelin veri setindeki kısıtlılıklar veya yetersizlikler nedeniyle ezberleme riski ortaya çıkabilir. Bir diğer olumsuz durum ise, karar süreçlerinin yorumlanabilirliğini sınırlayan ve "kara kutu" olarak tanımlanan yapıdır. Bu çalışmada, karar süreçlerinin açıklanabilirliğini artırmak amacıyla, kural tabanlı bir bulanık mantık sistemi geliştirilmiştir [16]. Model, MATLAB ortamında Fuzzy Logic Designer aracıyla tasarlanmış, analiz ve görselleştirmeler ise Python programlama dili kullanılarak gerçekleştirilmiştir.

2.3.1. Giriş Öznitelikleri ve Üyelik Fonksiyonları

Bu bölümde, Saniyede İşlem Sayısı (TPS) 0-70.000 aralığında ölçeklendirilerek düşük (0-20.000), orta (20.001-50.000) ve yüksek (50.001-70.000) olarak üç seviyeye ayrılmıştır. Enerji tüketimi 0-10 arası bir skala üzerinden değerlendirilmiş olup, 0-3 düşük, 4-6 orta ve 7-10 yüksek tüketim olarak sınıflandırılmıştır. Gizlilik seviyeleri genel (0), konsorsiyum (1) ve özel (2) şeklinde kodlanırken, şifreleme gücü ise temel (0), standart (1) ve gelişmiş (2) olarak üç kademede tanımlanmıştır. Bu sınıflandırma yaklaşımı, farklı blokzinciri konfigürasyonlarının sistematik olarak karşılaştırılabilmesi için tutarlı bir temel sağlamaktadır. Özellikle TPS ve enerji verimliliği arasındaki denge analizlerinde bu kategorik yaklaşım kritik önem taşımaktadır. Gizlilik ve şifreleme parametrelerinin sayısallaştırılması ise makine öğrenmesi algoritmalarının veriyi daha etkin işleyebilmesine olanak tanımıştır.

2.3.2. Çıkış Sınıfları

Blockchain Type (0–2) aralığında değer alırken, 0: İzinsiz (Permissionless), 1: Konsorsiyum (Consortium) ve 2: İzinli (Permissioned) olarak belirlenmiştir

2.3.3. Model Kuralları

Bulanık mantık modelinde kullanılan örnek kural yapısı şu şekildedir:

```
IF Privacy IS Private AND Encryption IS High THEN Blockchain Type IS Permissioned
IF Privacy IS Hybrid AND Encryption IS Medium THEN Blockchain Type IS Consortium
IF TPS IS High AND Energy IS Low AND Privacy IS Public THEN Blockchain Type IS
Permissionless
```

Bu tür açıkça tanımlanabilen kural setleri, özellikle yüksek güvenlik ve regülasyon uyumluluğu gerektiren uygulamalarda, karar süreçlerinin şeffaflığını ve güvenirliğini destekler niteliktedir [17]. Başlangıçta geliştirilen bulanık mantık modelinde elde edilen sınırlı doğruluk oranını artırmak amacıyla, Random Forest modeli ile elde edilen öznitelik önem sıralaması temel alınarak bulanık mantık modelindeki kural seti yeniden şekillendirilmiştir. Özellikle gizlilik (Privacy) ve şifreleme (Encryption) parametreleri merkezli olarak oluşturulan yeni kurallar, bulanık mantık modelinin sınıflandırma başarısını önemli ölçüde yükseltmiştir."

2.3.4. Önerilen Model için Kural Yapısı

```
IF Privacy IS Private THEN Blockchain Type IS Permissioned
IF Privacy IS Consortium/Hybrid THEN Blockchain Type IS Consortium
IF Privacy IS Public AND Encryption IS Low/Medium THEN Blockchain Type IS
Permissionless
```

Bulanık mantık temelli model, teknik ve kriptografik parametrelerle blokzincir türleri arasındaki ilişkileri açık, şeffaf ve yorumlanabilir bir yapı içerisinde sunmuştur. Özellikle Özel (Private) gizlilik seviyesi ve ileri seviye (Post-Quantum) şifreleme algoritmalarına sahip platformların İzinli (Permissioned) olarak sınıflandırılması mantıksal tutarlılık göstermektedir. Modelin sunduğu bu yorumlanabilir yapı, kurumsal karar alma süreçlerinde ve denetim gerektiren kritik alanlarda önemli bir avantaj olarak değerlendirilebilir.

2.4. Karşılaştırmalı Analiz

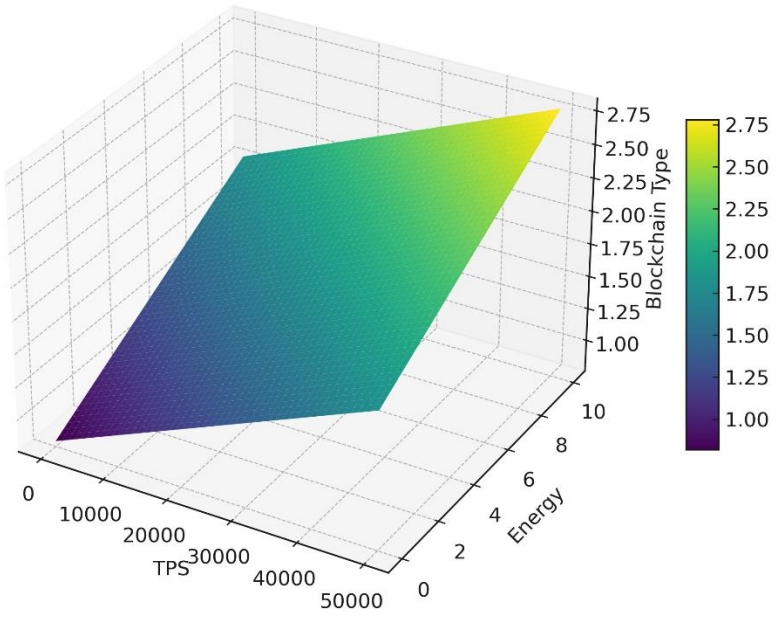
Bu bölümde, blokzincir türlerini sınıflandırmak amacıyla geliştirilen Makine Öğrenmesi (Random Forest) ve Bulanık Mantık modelleri, doğruluk ve açıklanabilirlik açısından karşılaştırmalı olarak analiz edilmiş Tablo 3’ de gösterilmiştir.

Tablo 3. Doğruluk ve Açıklanabilirlik Karşılaştırılması.

Model Türü	Doğruluk	Açıklanabilirlik
Random Forest (Makine Öğrenmesi)	%100	Düşük
Orijinal Bulanık Mantık	%22,58	Yüksek
ML ile Güncellenmiş Hibrit Bulanık Mantık	%87,10	Yüksek

Tablo 3’ de görülen ML sonuçları rehberliğinde oluşturulan hibrit bulanık mantık modeli, orijinal bulanık mantık modeline göre çok daha yüksek sınıflandırma doğruluğu sağlamıştır. Böylece bulanık mantık yönteminin açıklanabilirlik avantajıyla ML yönteminin yüksek doğruluğu etkili biçimde birleştirilmiştir.

Bulanık mantık (Fuzzy Logic) modeli, parametreleri dilsel değişkenler ve açıkça tanımlanmış kural kümeleri ile yorumlayarak sınıflandırma sağlamıştır. Bu yöntemle TPS, Enerji, Gizlilik ve şifreleme parametrelerinin Blockchain türü üzerindeki etkileri görsel olarak ortaya konmuştur (Şekil 4).



Şekil 4: TPS ve Enerji’ye Göre Blockchain Türü (Fuzzy Model Yüzey Çıkışı).

3. Sonuçlar

Bu çalışmada, blokzincir platformlarının teknik ve kriptografik parametreler temelinde sınıflandırılması amacıyla makine öğrenmesi ve bulanık mantık yöntemlerini içeren bir hibrit model geliştirilmiştir. Random Forest algoritması ile gerçekleştirilen sınıflandırma analizlerinde, özellikle Gizlilik ve Şifreleme parametrelerinin tür belirlemede yüksek etkiye sahip olduğu ve modelin %100 doğruluk oranıyla başarılı olduğu belirlenmiştir. Hibrit modelin ikinci aşamasında, Random Forest modelinin bulgularından faydalanılarak bulanık mantık kuralları yeniden oluşturulmuş ve bu sayede bulanık mantık modelinin doğruluk oranı önemli ölçüde (%22,58’den %87,10’a) artırılmıştır. Elde edilen sonuçlar, makine öğrenmesi ve bulanık mantık modellerinin birlikte kullanıldığı hibrit yaklaşımların blokzincir platformlarının sınıflandırılmasında etkin bir çözüm olduğunu ortaya koymaktadır. Gelecekteki çalışmalar için öneriler arasında; daha geniş veri setleri kullanılarak doğruluğun teyit edilmesi, derin öğrenme yöntemleriyle performansın karşılaştırılması ve şifreleme algoritmalarının matematiksel karmaşıklık seviyelerinin modellere dahil edilmesi bulunmaktadır.

References

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.

[2] W. Y. Wang et al., “Blockchain Applications in Healthcare and Supply Chains: A Survey,” IEEE Access, vol. 8, pp. 21150–21172, 2020.

[3] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, “Blockchain Technology: Beyond Bitcoin,” Applied Innovation Review, no. 2, pp. 6–10, June 2016.

[4] F. Casino, T. K. Dasaklis, and C. Patsakis, “A systematic literature review of blockchain-based applications: Current status, classification and open issues,” Telematics and Informatics, vol. 36, pp. 55–81, 2019.

[5] K. Christidis and M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things,” IEEE Access, vol. 4, pp. 2292–2303, 2016.

[6] M. Conti, C. Lal, and S. Ruj, “A Survey on Security and Privacy Issues of Bitcoin,” IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3416–3452, 2018.

[7] A. Gervais et al., “On the Security and Performance of Proof of Work Blockchains,” Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 3–16.

[8] Solana Labs, “Solana: A new architecture for a high performance blockchain,” Whitepaper, 2020.

[9] D. Yaga et al., “Blockchain Technology Overview,” NIST Interagency/Internal Report (NISTIR)- 8202, 2018.

[10] S. Rouhani and R. Deters, “Security, Performance, and Applications of Smart Contracts: A Systematic Survey,” IEEE Access, vol. 7, pp. 50759–50779, 2019.

[11] Y. Xiao et al., “A Survey of Consensus Protocols and Their Applications in Blockchain,” IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1432–1465, 2020.

[12] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, “Smart Contract-Based Access Control for the Internet of Things,” IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1594–1605, 2019.

[13] L. Breiman, “Random Forests,” Machine Learning, vol. 45, no. 1, pp. 5–32, 2001.

[14] Scikit-learn developers, “sklearn.ensemble.RandomForestClassifier documentation,” [Online] https://scikit-learn.org.

[15] Q. Zhou et al., “Performance Analysis of Consortium Blockchain for Real-Time Data,” Future Generation Computer Systems, vol. 107, pp. 841–850, 2020.

[16] R. R. Yager and L. A. Zadeh, “An Introduction to Fuzzy Logic Applications in Intelligent Systems,” Springer, 1992.

[17] L. A. Zadeh, “Fuzzy Sets,” Information and Control, vol. 8, no. 3, pp. 338–353, 1965.