PERIODICUM IURIS *Eskişehir Osmangazi Üniversitesi Hukuk Fakültesi Dergisi*
Cilt 2, Sayı 1, Ocak 2024 • ISSN: 2980-0889 • e-ISSN: 2980-0625 • ss. 33-76

BLOKZİNCİR TEKNOLOJİSİ VE AKILLI SÖZLEŞMELER: TEMEL YAPI, ÖZELLİKLER VE VERİ GÜVENLİĞİ PERSPEKTİFİ (*)

Blockchain Technology and Smart Contracts: Fundamental Structure, Features and Data Security Perspective

Aybike BERBER (**)
Emre ÖZTÜRK (***)

ÖZET

Blokzincir ve akıllı sözleşmeler; devlet sistemleri de dahil olmak üzere sistemleri dijital dönüşüm yolunda tetikleyen, bünyesinde barındırdığı multidisipliner yapılar sayesinde sözleşme süreçlerine ve iş yapma modellerine alternatif ve güvenli çözümler sunan, girift teknolojilerdir. Blokzincir teknolojisi esas ününü, Bitcoin adı verilen kripto para projesinin sunulması ile kazanmıştır. Satoshi Nakomoto rumuzlu kişi ya da kişilerce sunulan Bitcoin projesinde kişilerin elektronik para transferlerini gerçekleştirebilmek için birbirine güvenmelerine ya da banka gibi güvenilir finans kuruluşlarının sürece dahil olmasına ihtiyaç yoktur. Çünkü Satoshi Nakamoto'ya göre güven değil, kriptografik kanıt esas alınmıştır. İşte bu devrim niteliğindeki gelişme sayesinde, aslında daha önceden de literatüre kazandırılmış olan mekanizmalar ustaca bir araya getirilmiş ve blokzincir 1.0 dönemi başlamıştır. Dijital dönüşüme dair ciddi bir potansiyeli bulunan blokzincir teknolojisinin kullanımı yalnızca finans alanıyla sınırlı kalmamış, belki de geliştiricilerinin bile hayal edemediği bir şekilde evrim geçirmiştir. Blokzincirin

evrim sürecinde bir diğer dönüm noktası ise Ethereum blokzincirinin ortaya çıkmasıdır. Ethereum sayesinde, blokzincir teknolojisinin sağlık, eğitim, tedarik zinciri, sigortacılık gibi hemen hemen her alanda kullanılmasına imkân tanıyan akıllı sözleşmeler gündeme gelmiştir. Blokzincir tabanlı akıllı sözleşmeler; taraflarca kararlaştırılan edimlerin ifasını garanti altına alan, aracılara olan ihtiyacı ortadan kaldıran, değiştirilemez yapısı sayesinde gerek teknoloji dünyasının gerekse de hukuk dünyasının oldukça ilgisini çekmiştir. Türk

---

(*) Araştırma Makalesi.
Bu çalışma intihal programında kontrol edilmiş ve hakem denetiminden geçmiştir.
Gönderim Tarihi: 11.12.2023, Kabul Tarihi: 04.03.2024.
(**) Bahçeşehir Üniversitesi, Lisansüstü Eğitim Enstitüsü, Bilişim Hukuku Yüksek Lisans Programı Öğrencisi.
(***) İstanbul Okan Üniversitesi, Lisansüstü Eğitim Enstitüsü, Bilgisayar Mühendisliği Yüksek Lisans Programı Öğrencisi.

Hukuku'na göre aranan şartlara riayet eden akıllı sözleşmeler ise akıllı yasal sözleşmeler olarak adlandırılmıştır. Akıllı yasal sözleşmeler, akıllı sözleşmelerin bir alt dalı olup, sözleşme serbestisi ilkesi uyarınca geçerli ve bağlayıcı niteliktedir. Fakat akıllı sözleşmelerin, kendiliğinden ifa ve müdahalelere kapalılık başta olmak üzere, geleneksel sözleşmelerden ayrılan birtakım özellikleri mevcuttur. Bu da uygulamada sözleşmenin feshi, değiştirilmesi ya da uyarlanması gibi ihtiyaçlar karşısında pek çok soruna neden olmaktadır. Potansiyel sorunların önlenmesi için, sözleşmenin kuruluşu esnasında 'ex-ante' adı verilen hukuki ve teknik önlemlerin alınması mümkündür. Özellikle yapay zekâ ile blokzincir teknolojilerinin entegrasyonunun sağlanması, kod kaynaklı hataların ve güvenlik açıklarının en baştan önlenmesi adına faydalı olabilir. Genel itibariyle, blokzincirin bilgi güvenliğinin sağlanması için gereken güvenlik, gizlilik ve erişilebilirlik unsurlarını bünyesinde barındırdığı söylenebilir. Fakat bu durum, özellikle akıllı sözleşmelerin kodlanmasından kaynaklı hataların veya güvenlik açıklarının olmayacağı ya da siber saldırı riskinin tamamen ortadan kalktığı şeklinde yorumlanamaz. Neticeten blokzincir ve akıllı sözleşmeler; bünyesinde barındırdığı teknik ve hukuki sorunlara rağmen, dijital dönüşüm süreçlerine büyük katkı sağlama potansiyeli olan, önemli inovasyonlardır. Bu teknolojiler sayesinde, üçüncü kişi ya da kurumlara duyulan ihtiyacın önemli ölçüde azalacağı, maliyetlerin ciddi oranda düşeceği, zamandan tasarruf edileceği, efektif ve güvenilir şekilde işlemlerin gerçekleştirilebileceği söylenebilir.

Anahtar Kelimeler: Blokzincir, Bitcoin, Ethereum, Akıllı Sözleşmeler.

ABSTRACT

Blockchain and smart contracts are sophisticated technologies that trigger systems, including state systems, towards digital transformation and offer alternative and secure solutions to contract processes and business models thanks to the multidisciplinary structures they contain. Blockchain technology gained its main fame with the introduction of the cryptocurrency project called Bitcoin. In the Bitcoin project, which was presented by the person or persons with the pseudonym Satoshi Nakomoto, there is no need for people to trust each other or for reliable financial institutions such as banks to be involved in the process in order to make electronic money transfers. Because according to Satoshi Nakamoto, cryptographic proof is the basis, not trust. Thanks to this revolutionary development, mechanisms that had already been introduced to the literature were skilfully brought together and the blockchain 1.0 era began. The use of blockchain technology, which has a serious potential for digital transformation, has not only been limited to the field of finance, but has evolved in a way that perhaps even its developers could not have imagined. Another milestone in the evolution of blockchain is the emergence of the Ethereum blockchain. Thanks to Ethereum, smart contracts that allow the use of blockchain technology in almost every field such as health, education, supply chain and insurance have come to the fore. Blockchain-based smart contracts have attracted the attention of both the technology world and the legal world thanks to their unchangeable structure that guarantees the performance of the acts agreed by the parties, eliminates the need for

intermediaries. Smart contracts that comply with the conditions required under Turkish Law are called smart legal contracts. Smart legal contracts are a sub-branch of smart contracts and are valid and binding in accordance with the principle of freedom of contract. However, smart contracts have some features that distinguish them from traditional contracts, such as self-execution and closure to interventions. This causes many problems in practice in the face of needs such as termination, modification or adaptation of the contract. In order to prevent potential problems, it is possible to take legal and technical measures called 'ex-ante' during the establishment of the contract. In particular, the integration of artificial intelligence and blockchain technologies may be beneficial in order to prevent code-based errors and security vulnerabilities from the very beginning. In general, it can be said that blockchain incorporates the security, confidentiality and accessibility elements required to ensure information security. However, this situation cannot be interpreted as that there will be no errors or vulnerabilities arising from the coding of smart contracts or that the risk of cyber-attacks is completely eliminated. As a result, blockchain and smart contracts are important innovations that have the potential to make a great contribution to digital transformation processes, despite the technical and legal problems they contain. Thanks to these technologies, it can be said that the need for third parties or institutions will be significantly reduced, costs will be significantly reduced, time will be saved, and transactions can be carried out effectively and reliably.

Keywords: Blockchain, Bitcoin, Ethereum, Smart Contracts.

GİRİŞ

Blokzincir ve blokzincir tabanlı akıllı sözleşmeler, dijital dönüşümün adeta bir gereklilik haline geldiği günümüzde önemli teknolojik inovasyonlar olarak dikkat çekmiştir. Gelecekte blokzincir teknolojisinin ve akıllı sözleşmelerin de tıpkı internet gibi hayatımızın vazgeçilmez bir parçası olma potansiyeli bulunmaktadır. Ayrıca blokzincir ve akıllı sözleşmelerin kullanımı, teknoloji ve hukukun aynı potada buluşmasını sağlamıştır. Dolayısıyla hukuki çerçevede regülasyon çalışmalarının yapılmasına gerek olup olmadığı, uygulanacak hukukun tespiti, akıllı sözleşmelerin hukuki niteliği gibi pek çok konuda araştırmalar yapılmış, hukuki çalışmalar ortaya konmuştur. Bu teknolojiler hızla ve durdurulamaz şekilde gelişmeye devam etmektedir. Nasıl ki akıllı telefonlar bir günde mevcut formuna kavuşmadıysa, akıllı sözleşmelerden de tüm teknik ve hukuki sorunları tek seferde çözmesi beklenemeyecektir. Bu süreçte gerekli yasal düzenlemelerin mevzuata kazandırılması, ilgilileri aydınlatacak protokol ve rehberlerin oluşturulması ve uyumlaştırma çalışmalarının yapılması son derece önemlidir. Akıllı sözleşmeler gibi hukuk ve teknolojinin kesiştiği alanlarda; özellikle hukukçu ve yazılımcıların iş birliği halinde çalışması, hukuki bilgi ile teknik bilginin harmanlanması ihtiyacı doğmaktadır.

Bu çalışmanın amacı; blokzincir teknolojisi ve blokzincir teknolojisine dayanan akıllı sözleşmelerin güvensiz güven ortamını nasıl sağladığına, geleneksel düzende kullanılan

sözleşmelerle aralarında ne gibi farklar olduğuna dair bir anlayış sunmaktadır. Dolayısıyla ilk olarak bu teknolojilerin teknik alt yapısının detaylı şekilde incelenmesi gerekmektedir. Bu doğrultuda ilk olarak; blokzincir teknolojisinde sistem güvenliğini ve istikrarını temin etmek üzere kullanılan temel yapılar açıklanmış, bu teknolojinin öne çıkan özelliklerine yer verilmiştir. Akabinde blokzincir 2.0 dönemi olarak da ifade edilen Ethereum ağının ortaya çıkışı ve akıllı sözleşmelerle ilgisi üzerinde durulmuştur. Son olarak; akıllı sözleşmelerin tanımı, hukuken geçerliliği ve bağlayıcılığı, geleneksel uygulamalarla ayrıştığı özellikleri, bu özelliklerin sağladığı avantaj ve riskler, en nihayetinde veri güvenliği çerçevesinde değerlendirilmesine yer verilmiştir.

I. BLOCKZİNCİR TEKNLOJİSİ

A. Tarihsel Gelişimi ve Tanımı

Blokzincir teknolojisi; sistem içerisinde güvenlik ve istikrarın temin edilebilmesine hizmet eden farklı pek çok mekanizmanın bir araya gelerek oluşturduğu bir altyapı sunmaktadır. Blokzincir bünyesinde kriptografi, merkle ağacı, konsensüs mekanizmaları gibi birçok element bulunur.

Her ne kadar birinci nesil blokzincir teknolojisi olarak da bilinen bu teknolojik altyapı 2008 yılında Satoshi Nakamoto adlı kişi ya da kişilerce yayımlanan ufuk açıcı *'Bitcoin: A Peer-to-Peer Electronic Cash System'*[1] makalesi ile esas popülaritesine kavuşmuşsa da blokzincir teknolojisini bugünkü haline getiren temel yapı taşları çok daha eski tarihlerde, dönemin öncüleri tarafından ortaya atılmıştır.[2] Birinci nesil blokzincir olarak da adlandırılan[3] ve Bitcoin ile tanıtılan bu teknoloji ise, tüm bu temel elementlerin kombinasyonundan doğmuştur. Dolayısıyla blokzincir teknolojisinin teknik yönünü anlayabilmek adına, bu teknolojinin kökeninde yatan icatlardan da bahsetmek gerekmektedir.

1979 yılında, bilgisayar bilimcisi ve matematikçi Ralph C. Merkle tarafından 'Merkle Ağacı' ya da diğer adı ile 'Hash Ağacı' tanımlanmıştır. Standford Üniversitesi öğrencisi olan Merkle, doktora tezinde ağaca benzer bir veri yapısı ortaya koymuş, daha sonra kendi adını verdiği bu yapının patentini almıştır. 1988 yılında ise ağaca benzeyen bu veri yapısını açıklayan bir diğer makale yayınlamıştır. Merkle Ağacı ya da Hash Ağacı fikri, bilgi bloklarının kriptografik bir hash fonksiyonu kullanarak zincirlenmesini ve ağaca benzer bir yapı ile birbirine bağlanabileceğini öne sürer.[4] Merkle Ağacı; verilerin güvenli şekilde doğrulanmasına ve büyük veri kümelerinin tek bir kökte toplanmasına hizmet etmektedir. Bu da verimliliği arttıran ve veri bütünlüğünü sağlayan bir özellik olarak öne çıkmaktadır. Blokzincir yapısında

[1] Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System', (Bitcoin, 2008) <https://bitcoin.org/bitcoin.pdf.> Erişim Tarihi: 25.01.2024.
[2] Alan T. Sherman, Farid Javani, Haibin Zhang ve Enis Golaszewsk, 'On the Origins and Variations of Blockchain Technologies' (2019) 17(1) IEEE Security & Privacy 72,73. https://ieeexplore.ieee.org/document/8674176. Erişim Tarihi: 25.01.2024.
[3] Kaynak için bkz. <https://101blockchains.com/history-of-blockchain-timeline/> Erişim Tarihi: 25.01.2024.
[4] Sherman, Javani, Zhang, ve Golaszewsk (n3) 72,73.

iki ya da daha fazla taraf arasında yapılan işlemlere dair bilgilerin kayıtlarını içeren değiştirilemez bloklar bulunmaktadır. Merkle Ağacı, blokzincir ağını oluşturan her bir blok içerisindeki veri ve işlem kayıtlarının bütünlüğünü sağlamaktadır. Bitcoin'in icadında Merkle ağacının kullanımının katkısı büyüktür. Merkle ağaçları sayesinde belgelerin bir blokta toplanması sağlanmış ve verimliliği arttırmak hedeflenmiştir. Ayrıca Merkle ağacı hash tabanlı bir buluş olması nedeniyle, açık anahtarlı kriptografinin icadına da katkı sağlamıştır ve hash tabanlı kriptografide kullanılmaktadır.[5]

1991 yılında Stuart Haber ve W. Scott Stornetta tarafından kaleme alınan *"How to Time-Stamp a Digital Document"* adlı makale ile dijital dokümanlarda zaman damgası konusu işlenmiş, kriptografi adlı şifreleme yöntemi kullanılarak belgelerin zaman damgalarında bir değişiklik yapılmasının önlenmesi, geriye dönük bir tarihlendirme yapılamaması hedeflenmiştir.[6]

Ross Anderson tarafından hazırlanan ''*The Eternity Service*" adlı 1996 yılına ait makalede ise; merkezi olmayan bir depolama alanı önerilmiştir.[7] Bruce Schneier ve John Kelsey tarafından 1998 yılında kaleme alınan *"Cryptographic Support for Secure Logs on Untrusted Machines''* adlı makalede ise; hassas bilgileri tutmak zorunda oldukları kayıt dosyalarının saldırılara karşı korunmasız, güvenilmez bilgisayarlar üzerinde tutulduğu ve bu sorunun çözümü için şifrelemenin nasıl yapılacağı üzerinde durulmuştur.[8]

Kriptografi ve dijital mahremiyet alanlarında ortaya koyduğu vizyoner çalışmaları sayesinde bu alanlarda öncü olarak kabul edilen ve 'dijital paranın babası' olarak da anılan kriptograf, matematikçi David Chaum ise kripto para dünyasının iz bırakan mucitlerindendir. California Berkeley Üniversitesi'nden doktora derecesi bulunan David Chaum, kariyeri boyunca çok sayıda önemli yayına imza atmıştır. Chaum, doktora öğrenimi sırasında anonim iletişim metotları ve anonim şekilde gerçekleştirilebilen finansal işlemler konusunda araştırmalar yapmıştır. 1981 yılında e-posta iletişiminde tarafların kimliklerini ve mesaj içeriklerini 'genel anahtar şifrelemesi' yöntemi kullanarak kriptografik olarak gizleyen bir metodu içeren *'İzlenemeyen Elektronik Posta, İade Adresleri ve Dijital Takma Ad'* adlı makalesini

[5] Haojun Liu, Hongrui Liu, Xinbo Luo ve Xubo Xia, 'Merkle Tree: A Fundamental Component of Blockchains' (2021) 2021 International Conference on Electronic Information Engineering and Computer Science (EIECS) 556, 556-557. https://ieeexplore.ieee.org/document/9588047. Erişim Tarihi: 25.01.2024.

[6] Stuart Haber and W. Scott Stornetta, 'How to Time-Stamp a Digital Document' (1991) 3(2) Journal of Cryptology 99-111.
<https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.103.5300&rep=rep1&type=pdf.> Erişim Tarihi: 30.11.2023.

[7] Ross J. Anderson, 'The Eternity Service' (1996) Cambridge University Computer Laboratory <https://www.cl.cam.ac.uk/~rja14/Papers/eternity.pdf.> Erişim Tarihi: 30.11.2023.

[8] Bruce Schneier, and John Kelsey, 'Cryptographic Support for Secure Logs on Untrusted Machines' (1998) The Seventh USENIX Security Symposium Proceedings, USENIX Press 53–62.
<https://www.usenix.org/legacy/publications/library/proceedings/sec98/full_papers/schneier/schneier.pdf.> Erişim Tarihi: 30.11.2023

yayımlamıştır.[9] Şifrepunk grubunun önde gelen isimlerinden olan Chaum, 1982 yılında '*Karşılıklı Şüpheli Gruplar Tarafından Kurulan, Korunan ve Güvenilen Bilgisayar Sistemleri*' makalesini[10], 1983 yılında ise '*Takip Edilemeyen Ödemeler İçin Kör İmzalar*' makalesini[11] yayımlayarak anonim bir para biriminin icadındaki temelleri atmıştır. Chaum, DigiCash adıyla bir şirket kurmuş ve 'Kör İmza' yönteminden yararlanan E-Cash adını verdiği kriptografiye dayanan bir dijital para birimini üretmiştir. Ancak DigiCash uygulamada istenilen başarıyı gösterememiş ve şirket 14 Kasım 1998 tarihinde iflas başvurusunda bulunmuştur. Bunun nedeni ise; her ne kadar dijital para işlemlerinde anonimlik sağlansa da *'double spending'* de denilen çifte ödeme sorununa efektif bir çözüm sunamaması olmuştur. Şöyle ki; DigiCash bünyesinde sunulan bu sistemde çifte ödeme sorununu önlemek adına tüm işlemlerin merkezi bir noktadan (DigiCash şirketi tarafından) teyit edilmesi gerekiyordu. Dolayısıyla sistem temelde yine merkezi bir kuruluşa güven unsuruna dayalıydı. Çifte harcama sorununu çözmek adına geliştirilen en kritik adımlardan biri de 'Hashcash' projesidir. Bu proje kapsamında, yine Şifrepunk grubunda bulunan Adam Back tarafından kriptografiden temellerini alan, 'İş İspatı (Proof of Work- PoW)' adlı bir algoritma önerilmiştir. İş ispatı algoritmasını kullanan çeşitli kripto para birimleri oluşturmak için girişimlerde bulunulmuşsa da uzun ömürlü olamamıştır.[12] Esasen Satoshi Nakamoto tarafından önerilen blokzincir teknolojisine dayılı 'Bitcoin' projesinin hemen hemen her unsuru Özellikle David Chaum tarafından ortaya atılan kripto para projesi çerçevesinde önerilmiştir. Fakat blokzincir teknolojisinin temel unsurlarından biri olan ve ağdaki tüm kullanıcıların herhangi bir aracı veya merkezi otorite olmaksızın fikir birliğine varmasını sağlayan iş kanıtı algoritmasına sahip değildir. Yine de bu çalışmalar, kripto para birimlerinin evrimini doğrudan etkilemiş ve dijital mahremiyeti de odak noktasına koyacak şekilde çığır açan konseptler ortaya çıkarmış, gelecekteki çalışmalara da yön vermiştir.

Yukarıda da değinildiği üzere blokzinciri oluşturan temel yapı taşları uzun bir süre boyunca literatüre farklı çalışmalar çerçevesine kazandırılmıştır. Fakat birinci nesil blokzincir olarak kabul edilen bu kavram, 'Bitcoin' adı verilen kripto paranın ilk defa duyurulmasıyla esas ününü kazanmıştır. Satoshi Nakamoto takma adını kullanan kişi ya da kişilerce 2008 yılında kaleme alınan *''Bitcoin: A Peer-to-Peer Electronic Cash System''* adlı makaleden sonra

[9] David L. Chaum, 'Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms' (1981) 24(2) Communications of the ACM 84-88 https://dl.acm.org/doi/pdf/10.1145/358549.358563 Erişim Tarihi:25.01.2024.
[10] David L. Chaum, 'Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups' (1982) <https://cdn.sanity.io/files/r000fwn3/production/e630610a9c7c3c8f950cfb5632b44ecf1b8926d2.pdf.> Erişim Tarihi: 25.01.2024.
[11] David L. Chaum, 'Blind Signatures for Untraceable Payments' in Chaum, D., Rivest, R.L., Sherman, A.T. (eds) Advances in Cryptology. (Springer, Boston, MA 1983) <https://doi.org/10.1007/978-1-4757-0602-4_18.> Erişim Tarihi: 25.01.2024.
[12] Ramesh Subramanian ve Theo Chino 'The State of Cryptocurrencies, Their Issues and Policy Interactions' (2015) 24(3) Journal of International Technology and Information Management 27 http://scholarworks.lib.csusb.edu/jitim/vol24/iss3/2 Erişim Tarihi: 25.01.2024; Yusuf Mansur Özer, *Kişisel Verilerin Korunmasında Blokzincir Modeli: Vaatler ve Hukuki Engeller* (1.Baskı, On İki Levha 2020) 58-61.

blokzincir 1.0 dönemi de başlamıştır.[13] Halbuki makale içerisinde 'blokzincir' veya literatürde blokzincir kavramını açıklamak üzere kullanılan 'dağıtık kayıt defteri' kavramlarına yer verilmemiştir. Bunun yerine teknik altyapıyı ifade etmek üzere bloklardan oluşan bir zincir denmektedir.[14] Anılan makale kapsamında; herhangi bir finansal kuruluşa veya üçüncü bir güven kuruluşuna ihtiyaç olmaksızın, elektronik paranın eşler arası doğrudan transfer edilebileceği güvenli bir ödeme sistemi sunulmaktadır. Ayrıca makale kapsamında çifte harcama sorununa da değinilmiş ve çözüm önerisi getirilmiştir. Öncelikle sistem, merkezi olmayan bir yapı üzerine inşa edilmiştir. İşlemlerin kontrolü ise her on dakikada bir iş ispatı algoritması kullanılmak suretiyle mutabakat mekanizması kullanılarak sağlanmaktadır.[15] Bu ödeme sistemi kapsamında kullanılan değişim aracı/ dijital para ise 'Bitcoin'dir. Bitcoin, yirmi bir milyon adet olmak üzere üretimi sınırlandırılan ilk kripto para birimidir.[16] Bu elektronik ödeme sisteminin temelinde yatan teknoloji ise blokzincir teknolojisidir. Bitcoin; blokzincir altyapısı kullanılarak herhangi bir aracı kuruluşa ihtiyaç olmaksızın güvenli şekilde saklanır, transfer edilir, yönetilir.[17] Dolayısıyla Bitcoin, blokzincir altyapısı olmaksızın düşünülemez. Geleneksel yöntemde para transferleri gerçekleştirirken güvenliğin sağlanması amacıyla birden fazla merkezi otorite sürece katılmaktadır. Örneğin; farklı bankalarda hesabı bulunan iki tarafın para transfer işlemini gerçekleştirebilmesi için her iki tarafın da çalıştığı bankalar, bu bankaların bağlı olduğu ulusal veya uluslararası merkez bankaları süreçlere aktif olarak katılım sağlar, kimlik doğrulama gibi aşamalardan sonra transfer işlemi gerçekleştirilir, bakiyeler güncellenir, işlemler kaydedilir. Aracı kurumlar arttıkça transfer süresi ve ücretinde de artış gözlenir. Bitcoin ile öne sürülen alternatif ödeme sisteminde ise merkezi bir otorite bulunmamaktadır. Sistemin dağıtık yapısı sayesinde her bir katılımcı işlemlerin teyit edilmesinde rol oynar ve yapılan her bir işlem zaman sıralamasına göre kriptografik olarak şifrelenerek değiştirilemez bir şekilde veri tabanına kaydedilir. Sistemin aracı kişi ya da kurumlara ihtiyaç olmaksızın güvenliği temin edebilmesi ise temelinde yatan blokzincir teknolojisi sayesinde mümkün hale gelmektedir. Uygulamada 'Bitcoin[18]' denilen kripto para birimi ile temelinde yatan teknoloji yani blokzincir teknolojisi hatalı şekilde birbiri yerine sıkça kullanılır hale gelmiştir.[19] Fakat blokzincir teknolojisi yalnızca dijital para transferlerinin

[13] Nur Şura Öz, 'Blokzinciri Teknolojisinin, Akıllı Sözleşmeler ve Kripto Paraların Karşılaştırmalı Hukuk Bakımından Değerlendirilmesi' (Yayınlanmamış Yüksek Lisans Tezi, Bahçeşehir Üniversitesi 2022) 17.

[14] Nakamoto (n 1) 1-8; Zeynep Özkan, 'Akreditifte Blokzinciri ve Akıllı Sözleşmelerin Uygulanabilirliğinin Hukuki Açıdan Değerlendirilmesi' (Yayınlanmamış Yüksek Lisans Tezi, Galatasaray Üniversitesi 2022) 46,47; Özer (n 12) 55.

[15] Özer (n 12) 60.

[16] Fatih Bilgili ve Fatih Cengil, *Blockchain ve Kripto Para Hukuku* (2. Baskı, Dora Basım-Yayın 2022) 65.

[17] Fatih Bilgili ve M. Fatih Cengil, 'Bitcoin Özelinde Kripto Paraların Ticaret Şirketlerine Sermaye Olarak Getirilmesi' (2019) 22(3) Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi 3, 5-6.

[18] Bitcoin; bireyler arasında günlük para transfer işlemlerinin daha kolay ve hızlı yapılabilmesi adına geliştirilen ilk dijital para birimidir. Kaynak için bkz. Muhammad Ashraf Fauzı, Norazha Paiman and Zarina Othman, 'Bitcoin and Cryptocurrency: Challenges, Opportunities and Future Works' (2020) 7(8) Journal of Asian Finance, Economics and Business, 695–704. Kriptografi; göndericinin mesajının şifrelenerek gizlenmesini ve alıcı tarafından şifrenin çözülerek okunmasını sağlayan bir şifreleme metodudur. Kriptografi tekniği Bitcoin gibi dijital paralarda kullanılmaktadır.

[19] Özer (n 12) 54.

aracı kurumlara ihtiyaç olmaksızın veya yüksek işlem maliyetleri doğmaksızın yapılmasına ve takibine hizmet eden bir teknoloji değildir. Blokzincir teknolojisinin ilk uygulaması finans sektörü olsa dahi, günümüzde özellikle akıllı sözleşmelerin hayatımıza girmesiyle birlikte tedarik zinciri, sağlık, eğitim gibi farklı sektörlerde, farklı kullanım alanları ortaya çıkmıştır.[20] Bitcoin ise blokzincir teknik altyapısından temellerini alan projelerden yalnızca biridir.[21] Ayrıca gelinen nokta itibariyle blokzincir teknolojisinin, nesnelerin interneti ve yapay zekâ gibi pek çok teknolojiyle de entegrasyonu da mümkün hale gelmiştir.[22] Dolayısıyla blokzincir teknolojisi; dijital dönüşüm sürecini tetikleyen, yıkıcı, dönüştürücü ve girift bir teknoloji olarak karşımıza çıkmaktadır. Her teknolojide olduğu gibi bünyesinde riskler de barındırmakla birlikte, ortaya çıkış amacını aşmış, belki de öz geliştiricilerinin dahi tahmin edemediği bir noktaya gelmiştir.

Yukarıda da izah edildiği üzere, blokzincir teknolojisinin multidisipliner yapısı nedeniyle tüm özelliklerini kapsayacak nitelikte bir tanım yapmak oldukça zordur.[23] Nitekim literatürde yerleşmiş tek bir tanım da bulunmamaktadır.[24] Blokzincir, düğüm[25] ya da İngilizce'deki kullanımı ile 'node' olarak da adlandırılan ağ katılımcıları tarafından işlemlerin onaylandığı, onaylanan tüm bu işlemlerin 'blok' adı verilen yapılara kriptografik olarak şifrelenerek kronolojik bir sıra ile kaydedildiği, dağıtık yapıda ve değiştirilemez bir veri tabanıdır.[26] Yine literatürde merkezi bir otoriteye ihtiyaç duymayan blokzinciri ifade etmek için 'dağıtık defter teknolojisi *(Distributed Ledger Technology- DLT)*' ifadesi de sıklıkla kullanılmaktadır.[27] Blokzincirin dağıtık bir defter teknolojisi olması, sistemde merkezi bir otorite bulunmayışını ve her bir düğüm ile sisteme kaydedilen verilerin paylaşıldığını ifade eder.[28]

Teknik özelliklerini ön plana alan bazı yaklaşımlarda ise blokzincir tanımlarında öne çıkan unsurlar; asimetrik kriptoloji ve mutabakat mekanizmalarının kullanılması, ağ katılımcıları

[20] Hamide Özyürek, 'Blockchaın Teknolojisinin Mevcut ve Muhtemel Kullanım Alanları' (2021) 22(4) Anadolu Üniversitesi İktisadi Ve İdari Bilimler Fakültesi Dergisi 31-50.
[21] Özkan (n 15) 48.
[22] Kaynak için bkz. https://www.geeksforgeeks.org/smart-contracts-and-iot/. Erişim Tarihi:26.01.2024.
[23] Sedanur Delioğlan, 'Akıllı Sözleşmeler' (Yayınlanmamış Yüksek Lisans Tezi, Özyeğin Üniversitesi 2023) 15.
[24] Özkan (n 15) 49; 0 Angela Walch, 'The Path of the Blockchain Lexicon (and the Law)' (2017) Review Banking & Financial Law 713, 719-723; Öz (n14) 14.
[25] Doğa Ekrem Doğancı, *Blokzincirine Dayalı Akıllı Sözleşmelerin Hukuki Nitelikleri, Kuruluşu, Yorumu, İfası ve Bazı Örnek Hukuki Uygulamalar* (1. Bası, On İki Levha 2021) 49.
[26] Bilgili ve Cengil, 'Sermaye' (n 18) 4; Ece Su Üstün, *TBK Kapsamında Geleneksel Sözleşmeler ile Mukayeseli Olarak Akıllı Sözleşmeler Blokzincir Teknolojisi* (1. Bası, Seçkin 2021) 23.
[27] Emre Şafak, Çağlar Arslan, Mesut Gözütok ve Tacettin Köprülü, 'Dağıtık Defter Teknolojileri ve Uygulama Alanları Üzerine Bir İnceleme' (2021) 29 Avrupa Bilim ve Teknoloji Dergisi 36, 38; Gökhan Ünal ve Çelebi Uluyol, 'Blok Zinciri Teknolojisi' (2020) 13(2) Bilişim Teknolojileri Dergisi 167,168; Natalia Chaudhry ve Muhammad Murtaza Yousaf, 'Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities' (2018) 12th International Conference on Open Source Systems and Technologies (ICOSST) 54,54; Özkan (n 15) 50-51; Damla Beril Çubukçu, *Teknik ve Hukuki Yönleriyle Akıllı Sözleşmeler (*1.Bası, Yetkin 2021) 10-12.
[28] Çubukçu (n 29) 10-12; Üstün (n 28) 27-28.

tarafından her bir işlemin takip edilebilmesi, eşten eşe *(Person to Person – P2P)* güvenli bir veri tabanı olması gibi özellikleri karşımıza çıkmaktadır.[29]

Özetle blokzincir; 'dağıtık' olarak adlandırılan yapısında merkezi bir otorite bulunmayan, sistemdeki katılımcılar (düğümler/nodes) tarafından işlemlerin doğrulandığı, böylelikle de birbirine bağlı 'blok' adı verilen yapılara kriptolojik olarak şifrelenmiş şekilde kaydedildiği bir veri tabanıdır.

İşlemlerin doğrulanması, bloklara kaydedilmesi ve yeni blok oluşumunda etkin rol alan bir diğer aktör ise 'madenci *(miner)*' olarak da adlandırılan ağ katılımcıları yani düğümlerdir.[30] Her düğümün madenci olması gerekmediği gibi teknik donanımları uygun olmayanların 'madencilik (mining)' işlemi yapması da mümkün değildir.[31] Çünkü madenci düğümler; yüksek kapasiteli ekran kartları kullanan, güçlü donanıma sahip, yüksek enerji kullanan bilgisayarlardır.[32] Bitcoin projesi ile kullanılan blokzincirinde 'en uzun zincir politikası' esas alınmış, böylece zincirin güvenliği ve istikrarını sağlamak amaçlanmıştır. En uzun zincir politikası daha sonra da farklı blokzincir ağları tarafından kullanılmaya devam etmiştir. Esasen blokzincirin güvenliğini korumak için öne sürülen bu doğrulama mekanizması içerisinde birtakım teşvikler bulunmaktadır. Dolayısıyla bahsi geçen mekanizma emek ve ödül unsurlarına odaklanır. Madenciler, blok başlığının hash'ini hesaplamak için karmaşık matematiksel problemler çözerler.[33] Bitcoin örneğinde; madenciler arasında bu matematik problemlerinin çözülmesi aşamasında bir bilgi işlem rekabeti oluşmaktadır. Problem çözümü için madenciler tarafından yüksek enerji kullanan güçlü kapasitedeki bilgisayarlar kullanılmak suretiyle bir çaba harcanır. Bu çaba karşılığında ise iki tür ödül toplanır; birincisi yeni bloklar oluşturmak amacıyla bir miktar kripto para, ikincisi ise bloga eklenen işlem üzerinden toplanan işlem ücretidir.[34] Dolayısıyla bu ödülleri toplamak amacıyla madenciler, hash algoritmasını içeren bir matematik sorununu çözmek için yarış halinde olurlar.[35] Bahsi geçen sistem bireysel olarak ödül toplamaya odaklandığı için 'bireysel madencilik' olarak adlandırılmaktadır. Daha sonrasında kolektif bir çabayla ödül kazanma olasılığını arttırmak amacıyla havuz sistemi *(pool mining)* denilen bir başka madencilik yöntemi daha ortaya çıkmıştır.[36] Madencilik faaliyeti ile zincir üzerine kayıtlı işlem geçmişi kontrol edilir, böylece

[29] Öz (n14) 14.

[30] Mimar Aslan ve Mustafa Cem Kasapbaşı, 'Blok Zinciri Platformları, Fikir Birliği Mekanizmaları ve Ağın Güvenlik Analizi' (2022) 5(1) Haliç Üniversitesi Fen Bilimleri Dergisi 43, 46; Doğancı (n 27) 50.

[31] Bulut Madencilik (Cloud Mining) adı verilen madencilik türü bu kapsama dahil değildir. Nitekim bulut madencilikte madencilik için gereken yüksek kapasiteli elektrik gücüne, bu donanımı çalıştırabilecek kadar güçlü bilgisayarlara ihtiyaç olmaksızın işlem gücünün kiralanması söz konusudur.
Kaynak için bkz.<https://www.btcturk.com/bilgi-platformu/bulut-madenciligi-cloud-mining-nedir-nasil-calisir/> Erişim Tarihi: 26.01.2024.

[32] Aslan ve Kasapbaşı (n 32) 46-47; Doğancı (n 27) 50.

[33] Bilgili ve Cengil, *Kripto Para Hukuku* (n 17) 77.

[34] Özer (n 12) 116.

[35] Aslan ve Kasapbaşı (n 32) 51.

[36] Bilgili ve Cengil, *Kripto Para Hukuku* (n 17) 76; Doğancı (n 27) 50-51.

çifte harcama olup olmadığı gibi hususlar denetlenir, kötü niyetli işlemler tespit edilip önlenebilir.[37]

Zincir gibi birbirine bağlı her bir bloğun kendine has bir özet değeri *(hash value)* bulunmaktadır. Bu özet değer, adeta blokların parmak izi gibi biriciktir. Aynı zamanda her bir blok, kendinden önce ağa eklenen bloğun özet değerini içerir. Böylelikle her bir blok, kendisinden sonra gelen bloğa referans olur.[38] Böylece geçmişe dönük bir işlem yapılması veya önceden bir blok üzerinde sisteme kaydedilmiş bir verinin değiştirilmesi de imkânsız hale gelir. Çünkü böyle bir müdahale olması durumunda bloğun özet değeri değişecektir. Bu da kendinden sonra gelen bütün bağlantılı blokların özet değerinin değişmesine yol açacak ve tutarsızlık oluşturacaktır.[39] Dolayısıyla değişiklik hemen anlaşılacak ve böyle bir işlem sistem tarafından doğrulanmayacaktır.

Blokzincir üzerinde yeni bir blok elde etmek için ise o ana değin üretilmemiş bir özet değer bulunması gerekir. Bu değeri bulmak için madenciler karmaşık matematik problemlerini çözer, daha önce üretilmemiş bir özet değeri bulunduğunda ise yeni bir blok ağa sunulur. En basit ifadesiyle bu süreç de madencilik işlemi olarak tariflenir. Madenciler tarafından özet değerine dayalı bu matematik problemleri çözüldükten sonra, işlemlerin yeteri kadar ağ katılımcısı(düğüm) tarafından onaylanması için bir mekanizmaya ihtiyaç duyulur. Madenciler tarafından doğrulanmak üzere yayınlanan işlemler, ancak ağ katılımcılarının (düğümlerin) çoğunluğu tarafından teyit edilirse blokzincir üzerine kaydedilebilir. Ağ katılımcılarının %51'i tarafından doğrulanması için ise 'fikir birliği mekanizması' veya 'mutabakat mekanizması *(consensus mechanism)*' olarak adlandırılan uzlaşma sistemleri kullanılmaktadır. Blokzincir ağına eklenmek istenen her bir veri ya da ağ üzerinde gerçekleştirilmek istenen her bir işlem; ağ üzerinden yayınlanır, mutabakat mekanizması sayesinde kullanıcıların çoğunluğu tarafından doğrulanır, uçtan uca şifreli şekilde bloklara kaydedilir. Ağa dahil olan her makinada (düğümde) ise bloklarda tutulan kayıtların bir kopyası bulunmaktadır. [40] Bahsi geçen ağ üzerinden yayınlanma, uygunluk denetimi, şifrelenme ve kayıt işlemleri zincire eklenen her blokta tekrar eder. Böylece sınırsız sayıda birbiriyle bağlantılı bloklardan oluşan bir zincir yapısı elde edilir.[41]

Literatürde devredilmiş hisse ispatı *(delegated proof of stake),* önem ispatı *(proof of importance)*, faaliyet ispatı *(proof of activity),* yetki ispatı *(proof of authority*), *Direct Acyclic Graph (DAG*) gibi farklı performans ve güvenlik özelliklerini barındıran çeşitli mutabakat

[37] Doğancı (n 27) 51.
[38] İbid 55-57; Üstün (n 28) 22; Arif Furkan Mendi ve Alper Çabuk, 'Bitcoin'in Arkasındaki Güç: Blockchain' (2018) 1(1), GSI Journals Serie C: Advancements In Information Sciences And Technologies 12, 15.
[39] Üstün (n 28) 22.
[40] Mesut Serdar Çekin, 'Borçlar Hukuku ile Veri Koruma Hukuku Açısından Blockchain Teknolojisi ve Akıllı Sözleşmeler: Hukuk Düzenimizde Bir Paradigma Değişimine Gerek Var Mı' (2019) 77(1) İstanbul Hukuk Mecmuası 315, 321-322; Aslan ve Kasapbaşı (n 32) 46-47.
[41] Bilgili ve Cengil, *Kripto Para Hukuku* (n 17) 49; Fikriye Ceren Sadioğlu, 'Borçlar Hukuku Çerçevesinde Akıllı Sözleşmenin İşlevleri ve İşlevlerin Yerine Getirilmesi Sırasında Karşılaşılan Sorunlar' (2021) 25(4) Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi 171, 178-179; Mendi ve Çabuk (n 40) 14-15.

mekanizmaları bulunmaktadır.[42] Bu mutabakat mekanizmaları kullanılacak uygulamaya göre, güçlü ve zayıf yönleri karşılaştırılmak suretiyle belirlenebilir.[43] İş ispatı (*Proof of Work-PoW),* blokzincir ağlarında yaygın şekilde kullanılan bir mutabakat mekanizması olmakla birlikte, ilk kez Bitcoin adlı kripto para projesi ile tanıtılmıştır. Fakat iş ispatı mutabakat mekanizması çalışırken ciddi oranda enerji harcanmasına neden olmakta, bu bağlamda da eleştirilmektedir.[44] Hayatımıza akıllı sözleşmelerin girmesini sağlayan Ethereum blokzincir ağında ise işlem kapasitesinin artması ve daha az enerji tüketiminin sağlanması gibi amaçlar doğrultusunda iş ispatından hisse ispatı *(Proof of Stake- PoS)* mutabakat mekanizmasına geçiş yapılmıştır.[45]

Ayrıca blokzincir üzerine kaydedilen her bir işlemin zaman damgası (time stamp) bulunmaktadır. Böylece işlemlerin veya her bir verinin hangi zamanda bloklara eklendiği de kayıt altına alınmış olur. Çünkü zaman damgası, bir işlemin bloğa veya bloğun blokzincir ağına eklendiği zamanı tam olarak gösterir. Böylelikle mutabakat mekanizması vasıtasıyla işlemlerin doğrulanmasında ve kayıt sonrasında da işlem geçmişinin görüntülenmesi için kullanılabilir. Zaman damgası ile kayıt altına alınan verilerin ve blokların bütünlüğü de sağlanmış olur. Böylece blokzincirin müdahaleye dayanıklı *(tamper-proof)* ve değiştilemez yapısını öne çıkartmaktadır.[46]

Blokzincirde güvenlik ve anonimlik sağlanması adına kullanılan yöntemlerden bir diğeri de asimetrik şifrelemedir. Kullanıcıların birbirleriyle doğrudan ve güvenli şekilde işlem yapabildiği blokzincir sisteminde; kullanıcılara iki anahtar atanır. Bunlar; genel anahtar *(public key)* ve özel anahtar *(private key)* olarak adlandırılır.[47] Bu anahtarlar astronomik uzunlukta bir sayı dizisinden oluşur. Blokzincir ağı üzerinden gerçekleştirilen işlemlerin güvenliğini sağlamak amacıyla her bir kullanıcıya anahtar verilmek suretiyle dijital kimlik atanmış olur. Fakat dijital kimlik atanması kişilerin belirlenebilir olduğu anlamına gelmemektedir. Nitekim blokzincir ağına katılan kullanıcılar anonim kalmayı tercih edebilir, gerçek ad soyadlarını kullanmayabilir. Dolayısıyla anahtarların esas işlevi kimlik tespiti değil, veri bütünlüğü ve gizliliğinin korunmasıdır.[48] Kullanıcıların blokzincir üzerinde işlemler yapabilmesi için her iki anahtara da ihtiyacı vardır. Genel anahtar ile şifreleme yaparken, özel anahtar ile de şifre çözme işlemi gerçekleşir. Bu çift anahtarlı sistem ise 'asimetrik şifreleme'

---

[42] Doğancı (n 27) 52; Aslan ve Kasapbaşı (n 32) 52; Elektronik Kaynak için bkz. <https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp#:~:text=What%20Are%20the%20Types%20of,authority%2C%20and%20proof%20of%20capacity.> Erişim Tarihi: 26.01.2024.

[43] Chaudhry ve Yousaf (n 29) 54.

[44] ibid 54, 55; Aslan ve Kasapbaşı (n 32) 52-53.

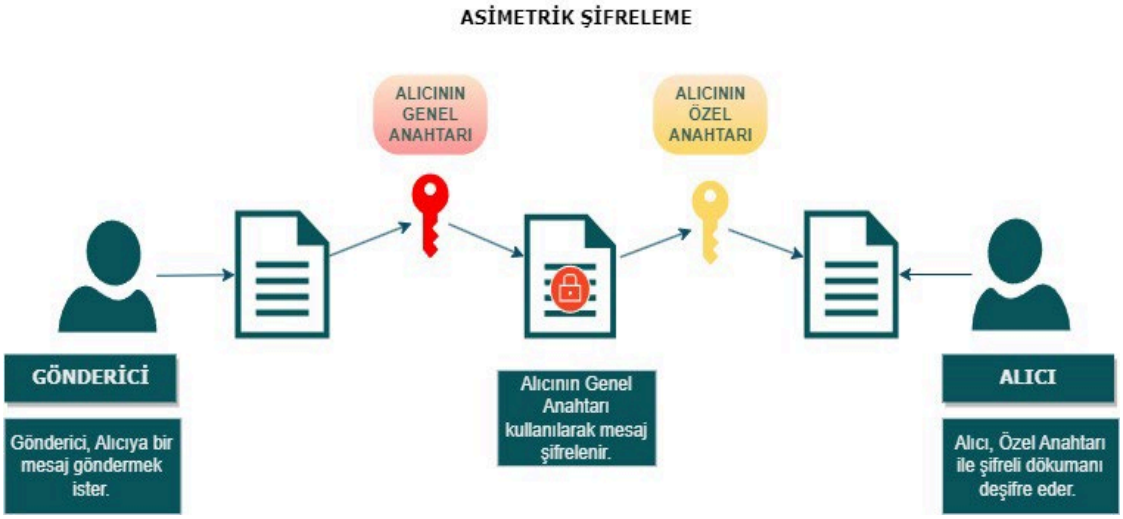
[45] Kaynak için bkz. <https://www.btcturk.com/bilgi-platformu/ethereum-2-0-the-merge/.> Erişim Tarihi: 26.01.2024

[46] Çubukçu (n 29) 14; Nakamoto (n 1) 1-2.

[47] Çekin (n 42) 321; Doğancı (n 27) 37; Üstün (n 28) 25-27; Merve Kınacı, 'Blockchain Teknolojisi ve Akıllı Sözleşmelerin Yaygınlaşmasının Önündeki Engeller' (Yayınlanmamış Yüksek Lisans Tezi, Bahçeşehir Üniversitesi 2019) 9.

[48] Üstün (n 28) 25,28,29.

olarak bilinmektedir.[49] Genel anahtar, özel anahtara bağlı olarak oluşturulur fakat tam tersi neredeyse imkansızdır. Her iki anahtar arasında aralarında matematiksel bir modelleme vardır.[50] Her iki anahtarın da amacı farklıdır. Özel anahtarlar sayesinde; imzalama gerçekleşir ve dijital kimlik sahipliği kanıtlanmış olur. Özel anahtar sayesinde şifreli bir mesaj deşifre edilir ve okunabilir hale gelir. Dolayısıyla kullanıcılar tarafından özel anahtarın diğer kişilerle paylaşılmaması ve yetkisiz erişimlerin önlenmesi gerekir. Genel anahtarlar ise; doğrulama işlevine haizdir. Genel anahtarlar literatürde daha çok IBAN numarasına ya da e-posta adresine benzetilmektedir ve işlemleri gerçekleştirmek için diğer kullanıcılarla paylaşılmasında bir sakınca bulunmamaktadır.[51]



Şekil 1: Blokzincir ağında gerçekleştirilen veri aktarımında asimetrik şifreleme ve anahtar kullanımı.[52]

Neticeten blokzincir teknolojisinde kullanıcılar (düğümler-nodes) birbiriyle bağlantılı dağıtık bir ağ üzerinde yer alırlar. Bu nedenle sistemi kontrol eden tek bir merkezi otorite bulunmaz. Dolayısıyla tek bir düğümün sistemi kontrol etmesi de mümkün değildir. Blokzincir üzerinde gerçekleştirilmek istenen işlemler, sisteme eklenmek istenen her bir veri 'blok' adı verilen yapılarda temsil edilir ve ağ üzerinde tüm düğümlerin erişebileceği şekilde

[49] Özkan (n 15) 55.
[50] Kaynak için bkz. <https://www.gemini.com/tr-TR/cryptopedia/public-private-keys-cryptography#section-what-is-a-private-key.> Erişim Tarihi:26.01.2024.
[51] Özer (n 12) 108-109; Bilgili ve Cengil, *Kripto Para Hukuku* (n 17) 161-163; Üstün (n 28) 24-27; Doğancı (n 27) 36-38; Özkan (n 15) 55; Ünal ve Uluyol (n 29) 169; Arif Furkan Mendi, 'Blokzincir Mimarisi ve Getirdiği Fırsatlar' (2021) 29 Avrupa Bilim ve Teknoloji Dergisi 181, 184.
[52] ÜSTÜN (n 28) 27; Elektronik kaynak için bkz. https://kerteriz.net/modern-sifreleme-yontemleri-simetrik-asimetrik-sifreleme/. Erişim Tarihi: 26.01.2024.

yayımlanır, işlemin doğruluğu mutabakat mekanizmaları vasıtasıyla doğrulanır, veriler veya işlemler zaman damgasıyla birlikte kriptografik olarak şifrelenerek kronolojik sırayla bloklara kaydedilir. Her bir blok, kendinden sonra gelen bloğa özet değeri ile referans olur, böylece bloklar da adeta bir zincir oluşturacak şekilde birbirine bağlanır ve sınırsız sayıda, birbiriyle bağlantılı bloklardan oluşan bir zincir yapısı elde edilir. Bahsi geçen ağ üzerinden yayımlanma, uygunluk denetimi, kriptografik olarak şifrelenme ve zaman damgası ile kayıt işlemleri zincire eklenen birbiriyle bağlantılı her bir blokta tekrar eder. Böylece sınırsız sayıda birbirine adeta bir zincir gibi bağlı bloklardan oluşan yapı elde edilir.[53] Tüm bu nedenlerle tarafların birbirine güvenmelerine ya da aracı kurumlarla işlemlerini gerçekleştirmelerine gerek kalmaz. Çünkü sistemin bizzat kendisi yukarıda da ifade edilen mekanizmalar sayesinde, güvensiz güveni oluşturmaya hizmet eder.

B. Özellikleri

Blokzincirin tarihsel gelişimi, temel elementleri ve işleyişinden yukarıda bahsedilmiştir. Blokzincir sistemi; birbirinden farklı pek çok özelliği barındıran, belli kriterlere göre oluşturulmuş, benzersiz bir yapıya sahiptir. Bu benzersiz yapısı sayesinde de blokzincir teknolojisine olan ilgi her geçen gün artmaktadır. Blokzincir teknolojisinin öne çıkan hangi özellikleri sayesinde sistemi değişikliğe zorladığı ise bu bölüm kapsamında ana hatlarıyla incelenmektedir.

1. Dağıtık Defter Teknolojisi Olması

Blokzincir teknolojisi en kısa tanımı itibariyle dağıtık bir defter teknolojisidir *(Distributed Ledger Technology- DLT)*. [54] Geleneksel olarak kullanılan merkezi veri tabanı yapısında, işlemler üçüncü bir otoritenin kontrolüne tabidir. Fakat blokzincir yapısında merkezi bir otoriteye ihtiyaç duyulmaksızın işlem güvenliği ve kontrolü sağlanır. Bu da sistemin dağıtık veri tabanı mimarisine sahip olması sayesinde gerçekleşir. Blokzincir sisteminin dağıtık veri tabanı sayesinde; yapılan tüm işlemler, sistemde kayıtlı kullanıcılara ağ üzerinden yayınlanır, doğrulanır ve bir kopyası tüm düğümlerde olacak şekilde dağıtık deftere kaydedilir. Dolayısıyla sistemde yapılan tüm işlemleri barındıran bu kayıt defterinin bir kopyası tüm düğümlerde bulunur. Böylece verinin sonradan değiştirilmesi, silinmesi gibi işlemlerin önüne geçilir. Veriler tek bir merkezi noktada tutulmak yerine, sisteme dahil olan tüm düğümlerde dağıtık şekilde saklandığı için olası siber saldırılara karşı da dayanıklıdır. Tek bir ağ katılımcısının bu verileri tahrip etmesi de mümkün değildir.[55] Tek bir ağ katılımcısı zincire yeni veriler ekleyebilir, veri girişini doğrulama sürecine katılabilir, geçmişe dönük olarak tüm işlem geçmişini takip edebilir. Fakat tek bir ağ katılımcısı tarafından sistem kontrol edilemez. Çünkü bu yetki, tüm ağ katılımcıları arasında eşit şekilde bölünmüştür. Kontrol

[53] Bilgili ve Cengil, *Kripto Para Hukuku* (n 17) 159; Sadioğlu (n 43) 178-179; Mendi ve Çabuk (n 16) 14-16.
[54] Çubukçu (n 29) 10-12; Üstün (n 28) 27-28; Şafak, Arslan, Gözütok ve Köprülü (n 29) 38.
[55] Şafak, Arslan, Gözütok ve Köprülü (n 29) 41.

mekanizmasının dağınık halde bulunması sayesinde de blokzincir teknolojisi güvenilir bir sistem olarak anılmaktadır.[56]

Dağıtık bir defter teknolojisi olan blokzincir; sisteme erişimin durdurulması, verilerin çalınması, verilerin manipüle edilmesi veya tahrip edilmesi, kişilerin şifrelerinin ele geçirilmesi gibi amaçlarla gerçekleştirilen siber saldırılar karşısında da merkezi sistemlere nazaran çok daha güçlü bir koruma sağlamaktadır.[57] Nitekim sunucuları tek bir merkezi noktada toplanan bir sistemde ağ trafiği arttırılarak sisteme erişim engellenebilir. Hizmet engelleme saldırısı (Denial of Service-Dos) ya da dağıtık hizmet engelleme saldırısı (Distributed Denial Of Service-DDos) denilen siber saldırı türü ile sistemin çalışması ve kullanıcılar tarafından ulaşılması engellenmektedir. Bir diğer ifadeyle sistemin servis dışı kalması için gerçekleştirilen, internet hizmetlerini kesintiye uğratan bir siber saldırı türüdür. Dos atağı adı verilen bu siber saldırı türünde; merkezi sunucu, sistemin durmasına yol açacak kadar aşırı yüklemeye maruz bırakılır. DDos atağında ise; saldırılar 'zombi' adı verilen ve internet korsanlarınca ele geçirilmiş elektronik cihazlar üzerinden yani farklı pek çok IP adresinden hedefe yöneltilir. Merkezi bir kaynaktan çıkan ağda, hizmet reddi saldırısı ile erişim engellenebilir. Fakat blokzincir ağının merkeziyetsiz yapısı ve sisteme yeni bir blok eklemek için kullandığı mutabakat mekanizmaları sayesinde birkaç düğüm çevrimdışı olsa dahi sistem çalışmaya devam eder.[58] Ayrıca her bir düğümde sistem kayıtlarının birebir kopyası bulunduğu için blokzincir ağına DDos atağında bulunmanın bir anlamı da olmaz.[59] Özetle; birkaç düğümün çevrimdışı olması ile sistem kesintiye uğramaz ve herhangi bir veri kaybı yaşanmaz. Keza tüm blokzincir ağının çökertilmesi için blokzincir ağındaki düğümlerin büyük bir kesiminin aynı anda çevrimdışı bırakılması gerekir ki bu risk de blokzincirin dağıtık bir defter teknolojisi olma özelliği sayesinde önlenir.[60] Blokzincir teknolojisi; sistemin sürdürülebilirliğinin tek bir ağ katılımcısına veya merkezi otoriteye bağlı olmayışı açısından siber saldırılara karşı dirençli bir yapı sunar.[61]

İçerisinde merkezi bir otorite barındırmayan bu sistem, kurcalamaya karşı dirençli bir veri tabanı sunma özelliği ile de öne çıkmaktadır. Şöyle ki; sisteme eklenen her bir veri, şifrelenerek dağıtık defter teknolojisi sayesinde kayıt altına alınır. Ayrıca her bir veri girişinin sisteme dahil olduğu an da zaman damgası (time stamp) ile değiştirilemez şekilde birbiriyle bağlantılı bloklara kaydedilir. Böylece sisteme kaydedilen tüm işlemlerin, kullanıcılar tarafından geriye dönük olarak takip edilebilmesi ve işlemlerin doğruluğunun kontrolü de mümkün hale gelir. Daha önce de ifade edildiği üzere; her bir düğüm, tüm işlemleri içeren

[56] Mendi ve Çabuk (n 40) 14-15; Ünal ve Uluyol (n 29) 168.
[57] Şafak, Arslan, Gözütok ve Köprülü (n 56) 36, 37.
[58] Nevzat Özcandan, Öznur Kalkar, Muhammed Ali Bingöl ve diğerleri, 'Blokzincirlerde Güvenlik ve Mahremiyet' (Bankalararası Kart Merkezi, Nisan 2020) 18 Elektronik kaynak için bkz. https://bkm.com.tr/wp-content/uploads/2015/06/blokzincirlerde_guvenlik_ve_mahremiyet.pdf Erişim Tarihi: 26.01.2024; Kaynak için bkz. <https://www.beyaz.net/tr/guvenlik/makaleler/dos_ve_ddos_nedir.html.> Erişim Tarihi:26.01.2024
[59] Oğuzhan Taş ve Farzad Kiani, 'Blok Zinciri Teknolojisine Yapılan Saldırılar Üzerine bir İnceleme' (2018) 11(4) Bilişim Teknolojileri Dergisi 369, 374.
[60] Nevzat Özcandan, Öznur Kalkar, Muhammed Ali Bingöl ve diğerleri (n 60) 18.
[61] Özer (n 12) 80-81; Doğancı (n 27) 34.

bu defterin bir kopyasına sahiptir. Bu da sistemin manipülasyona ve dışarıdan bir müdahaleye karşı dirençli olmasına, dolayısıyla zincirin bütünlüğünün sağlanmasına ve sistemin kendiliğinden güvenliği temin etmesine imkân tanır.[62]

2. Şeffaflık ve Dijital Kimlik Sağlama

Blokzincir ağ katılımcılarının, ağda gerçekleşen her işlemi inceleyebilmesi ise sistemin şeffaflık özelliğini ön plana çıkartmaktadır. Blokzincir, tüm kullanıcıların katılımına açık dağıtık bir kayıt defteri olması nedeniyle son derece şeffaf bir yapı sunmaktadır.[63] Burada bahsi geçen şeffaflık, kullanıcılar tarafından işlem trafiğinin izlenebiliyor oluşudur. Yoksa blokzincir ağında işlem yapan her katılımcının gerçek kimliklerinin göründüğü, işlemleri ad soyadları açık bir şekilde gerçekleştirdikleri anlamına gelmemektedir. Bu özelliği ile blokzincir, birbirine zıt anlamlar barındıran şeffaflık ve gizlilik kavramlarını aynı potada eritmeyi başaran bir sistem sunmaktadır.[64] Şöyle ki; blokzincir ağında, kullanıcılara yani sistemdeki her bir düğüme karmaşık alfanümerik dizilerden oluşan bir dijital kimlik atanır. Böylece ağ üzerindeki tüm kullanıcılar kendilerine atanan sanal adresler vasıtasıyla işlemlerini gerçekleştirebilir. Dolayısıyla blokzincir sisteminde kullanıcıların gerçek ad soyadlarını açıklayıp açıklamayacakları kendi inisiyatiflerine bırakılmıştır.[65] Fakat dijital kimlikleri ile gerçekleştirdikleri ve blokzincir üzerine kaydedilen her bir işlem, diğer kullanıcılar tarafından geriye dönük olarak izlenebilir.[66] Örneğin; iki hesap arasında Bitcoin gönderme işlemi gerçekleştirilecek olsun. Bu işlemin gerçekleştirilebilmesi için alıcının genel (açık) anahtarı alınır. Alıcı, Bitcoin gönderme işlemini gerçekleştirdiğinde bu işlem sisteme kaydedilir. Alıcı ve göndericinin gerçek ad ve soyadları sistemde gözükmeyebilir. Fakat gönderici artık alıcının genel anahtarını bilmektedir ve bu genel anahtarın ilişkili olduğu tüm işlemleri geriye dönük olarak inceleyebilir. Böylece alıcının daha önce hangi hesaplarla etkileşime girdiği, hangi hesaplara kripto para gönderdiği veya aldığı, bu işlemlerin ne zaman gerçekleştiği gibi verilere erişebilir.[67]

Bu noktada vurgulamak gerekir ki; kullanıcıların gerçek ad soyadlarını kullanmaksızın kendilerine atanan dijital kimlikle işlem yapabilmeleri, kullanıcılara yüzde yüz anonim kalma garantisi verilebileceği anlamına gelmemektedir. Zira kullanıcılar, blokzincir üzerinde kimliklerini ifşa etmemeyi tercih edebilir ve takma ad kullanarak işlemlerini gerçekleştirebilir. Fakat yapılan tüm işlemlerin şeffaf bir şekilde tüm kullanıcılara açık olması nedeniyle, takma adlarını ya da dijital kimliklerini kullanarak gerçekleştirdikleri her bir işlemin bir arada değerlendirilmesi ve ilgili kişinin davranış analizinin yapılması halinde gerçek kimliğine ulaşılması olasılık dahilindedir.[68] 6698 Sayılı Kişisel Verilerin Korunması Kanunu çerçevesinde 'anonim hale getirme' kavramı *'Kişisel verilerin, başka verilerle*

[62] Çubukçu (n 29) 12-14.
[63] Özer (n 12) 86.
[64] Doğancı (n 27) 36.
[65] Üstün (n 28) 29.
[66] Mendi ve Çabuk (n 40) 18; Üstün (n 28) 25-28; Çubukçu (n 29) 45-46.
[67] Özer (n 12) 86.
[68] İbid 86-87.

eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi' şeklinde tanımlanmıştır. Dolayısıyla farklı teknikler vasıtasıyla kullanıcının gerçek kimliğinin belirlenebilir olma olasılığının bulunması, anonim olarak kabul edilememesi için yeterlidir.

3. Eşten Eşe Güvenli İletişim

Blokzincir sisteminin en önemli vaatlerinden biri de üçüncü taraflara duyulan ihtiyacın ortadan kalkmasıdır. Kişilerin yapacakları işlemlerde mutlaka aracı bir güven kuruluşuna ihtiyaç duyması, tarafların birbirine duyduğu güven eksikliğinden kaynaklanmaktadır. Daha önce de bahsedildiği üzere, blokzincirin dağıtık yapısı, şeffaf olması, her bir işlemin kayıt altına alınması, sistemin manipüle edilememesi, verilerin silinememesi, tahrip edilememesi, geriye dönük takip edilebilirliği, değişikliklerin anında fark edilecek olması gibi özellikleri sayesinde sistem başlı başına güvenliği sağlamaya hizmet eden pek çok farklı mekanizmayı bir araya getirir. Bu da güvensiz güven ortamının oluşmasına yol açar. Güvensiz güvenin esas temeli, blokzincirin multidisipliner yapısındır.[69] Eşten eşe *(Peer to peer-P2P)* iletişim, merkezi bir sunucu ya da herhangi bir aracı üçüncü kişi olmaksızın tarafların doğrudan kendileri arasında gerçekleştirdikleri veri paylaşımıdır. Dolayısıyla aracı kişi ya da kurumlara ihtiyaç duyulmaksızın işlemler gerçekleştirilebilir, veri transferi sağlanabilir.[70] Blokzincirde ise eşler arası iletişim, ağ katılımcılarının yani düğümlerin doğrudan iletişim kurabilmesi, işlemleri herhangi bir aracı kuruma ihtiyaç duymaksızın gerçekleştirebilmesi olarak karşımıza çıkar. Blokzincirin dağıtık ağ yapısı sayesinde, sistemde aşırı yüklenme olmaksızın, büyük miktarlarda veri transferleri gerçekleştirmek de mümkün hale gelir. Ayrıca doğrudan iletişim sunan bu sistemdeki şifreleme teknikleri ve güvensiz güven ortamı oluşturmaya hizmet eden tedbirler sayesinde saldırılara dirençli bir ortam oluşturulur. Bu da özellikle yüksek seviyede gizlilik ve güvenlik gerektiren işlemler açısından tercih edilebilir bir ortam sunar.[71] Bitcoin adı verilen kripto paranın ortaya çıkışı ile ortaya koyduğu en temel farklılık, hiçbir aracı kuruma ihtiyaç olmaksızın, düğümler arası (P2P) transfer edilebiliyor oluşudur. Bu özellik ise blokzincir altyapısından kaynaklanır.[72] Geleneksel sistemde ise, kişiler gerçekleştirecekleri işlemler için karşı tarafa duyulan güven eksikliği nedeniyle kimlik tespiti, işlemin doğrulanması, kontrolü, kayıt altına alınması, uyuşmazlık halinde ispat vasıtası olarak kullanılması gibi hizmetleri alabilmek adına üçüncü bir güven kuruluşuna ihtiyaç duyar. Örneğin; Ayşe ve Mehmet arasında bir para transferi gerçekleştirilecek olsun. Ayşe ve Mehmet'in farklı banka müşterileri olduğu da kabul edilecek olursa, gerçekleştirilecek EFT işleminde her iki banka da sürece dahil olmaktadır. Bankalar, kullanıcıların yapılacak olan işleme yetkili olup olmadığını, bakiyenin yeterli olup olmadığını ve sair hususları kontrol

[69] İbid 90.
[70] Kaynak için bkz. <https://www.btcturk.com/bilgi-platformu/peer-to-peer-nedir-p2p-agi-nasil-calisir/.> Erişim Tarihi: 26.01.2024.
[71] Kaynak için bkz <https://www.blockchain-council.org/blockchain/peer-to-peer-network/. > Erişim Tarihi: 26.01.2024.
[72] Buket İşler, Mustafa Takaoğlu ve Ufuk Fatih Küçükali, 'Blokzinciri Ve Kripto Paraların İnsanlığa Etkileri' (2019) 3(2) Yeni Medya Elektronik Dergisi 71,79.

eder, belli bir işlem ücreti alınmak suretiyle transfer gerçekleştirilir, bakiyeler güncellenir. Bankalar gibi aracı kuruluşlar sayesinde çifte ödemenin önlenmesi, dolandırıcılıkların önüne geçilmesi, yetkisiz işlemlerin engellenmesi ve neticeten işlemlerin güvenliğinin sağlanması adına ciddi önlemler alınmaktadır. Bu noktada kullanıcılar açısından bankalar, merkezi bir otorite konumunda olup, müşterilerinin tüm kayıtları bu kuruluşlarda saklanmaktadır. Fakat banka müşterileri, diğer müşterilere ait hesap hareketlerine ulaşamaz. İşte bu merkezi yapılarda güvenliğin temini için pek çok ciddi tedbirin alınması, yedekleme yapılması, yüksek maliyetli bir ana bilgisayar kurulması ve sürekli olarak bu tedbirlerin yinelenmesi, teknik bakımların yapılması gerekir. Böylece geleneksel sistemde maliyet de artar ve kullanıcılara yükletilir. Blokzincir sistemi ise; aracı kuruluşları devreden çıkartarak sistemin doğrudan kimlik doğrulama, kayıt altına alma, değiştirilemez şekilde saklama, geçmişe dönük işlemleri izleyebilme gibi özellikleri sayesinde güvensiz güven ortamını oluşturmayı ve maliyetleri düşürerek alternatif bir sistem sunmayı hedefler.[73] Bitcoin gibi kripto para birimleri; ödemeler, fon transferleri gibi işlemlerdeki işlem maliyetlerini azaltmak, ödeme verimliliğini arttırmak, uluslararası para transferlerini kolaylaştırmak konularında ciddi bir potansiyel barındırmaktadır. Ayrıca üretimi, işlem görmesi veya saklanması için de herhangi bir banka ve sair merkezi otoriteye ihtiyaç duyulmaz.[74] Bitcoin adlı kripto para biriminin yaratıcısı Satoshi Nakamoto, asıl olanın kriptografik kanıt olduğunu, kişilerin birbirine veya üçüncü kişi ya da kurumlara güvenmesine ihtiyaç olmadığını ileri sürmüş ve geriye döndürülmesi neredeyse imkânsız işlemler vasıtasıyla kişilerin dolandırıcılıktan korunabileceği işlemler yapabileceği, eşten eşe iletişimi esas alan bu alternatif ödeme sistemini sunmuştur.[75]

3. Değiştirilemezlik

Blokzincir sisteminde zincire eklenen hiçbir veri sonradan güncellenemez ve silinemez. Tıpkı numaralandırılmış bir kitap gibi araya yeni bir sayfa eklenemez, aksi halde değişiklik anında anlaşılır. Numaralandırılmış bir kitaba ancak son sayfadan itibaren devam edilebildiği gibi zincire de ancak son bloktan dahil olunabilir, geçmişe dönük bir işlem yapılamaz. Her yeni veri girişi zaman sıralamasına göre bloklara şifrelenerek kaydedilmeye devam edilir. Bazı saldırı tipleri ayrık olmak üzere kaydın değiştirilebilmesi mümkün değildir.[76] İşlemler devam ettikçe bloklar üzerine yazılmaya devam eder, bloklara kaydedilen bu veriler ise değiştirilemez niteliktedir. Bloklar üzerinde geçmişe dönük bir değişiklik yapılmaya kalkıldığında, sistem ağ bütünlüğünü korur ve önceki kayıtlarla ve zincirle uyuşmayan bu müdahalelere izin vermez. Yukarıda her bloğun adeta parmak izi gibi biricik bir özet değeri

[73] Ali Nizamettin Yıldırım, 'Türk Borçlar Hukuku Bakımından 'Akıllı Sözleşmeler'' (Yayınlanmamış Yüksek Lisans Tezi, Koç Üniversitesi 2022) 21-22.
[74] İşler, Takaoğlu ve Küçükali (n 74) 80; Murat Ali Dulupçu, Mehmet Yiyit ve Asena Gizem Genç, 'Dijital Ekonominin Yükselen Yüzü: Bitcoin'in Değeri ile Bilinirliği Arasındaki İlişkinin Analizi' 2017 22(15) Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi 2241, 2248.
[75] Dulupçu, Yiyit ve Genç (n 76) 2245; Nakamoto (n 1) 1.
[76] Ünal ve Uluyol (n 29) 168; Hiroki Watanabe, Shigeru Fujimura ve diğerleri "Blockchain Contract: A Complete Consensus Using Blockchain" (2015) IEEE 4th Global Conference on Consumer Electronics (GCCE) 577, 578.

(hash value) içerdiğinden ve her bir özet değerin kendisinden sonra gelen bloğa referans olacak şekilde blokları birbirine bağladığından bahsedilmiştir. Bir blok üzerinde işlem geçmişe dönük bir işlem yapılması halinde bloğun özet değeri yani sabit sayıda bit'e sıkıştırılan değeri değişir, bu da kendisinden sonra gelen tüm blokların özet değerinin değişmesini gerektirir. Blokzincir ise devamlı olarak üzerinde işlem yapılan bir altyapı olduğu için zincir sürekli olarak uzamakta ve sistem bu değişiklik riskine izin vermemektedir. Böylece zincirin güvenliği ve blok bütünlüğü korunur. Blokzincir üzerinde geçmişe dönük bir değişiklik yapılması için bloktaki ve onu takip eden tüm bloklardaki özet değerinin hesaplanması ve değiştirilmesi gerekmektedir ki bu da mevcut blokzincirden başka bir blokzincirin çok daha hızlı şekilde oluşturulması ile gerçekleşebilecek bir senaryodur. Ayrıca değişiklik yapılmış ve özet değerleri değişmiş olan blokları içeren bu alternatif blokzincir oluşturulurken bir yandan mevcut blokzincir ağında da sürekli işlem yapıldığı unutulmamalıdır. Dolayısıyla böyle bir senaryonun gerçekleşebilmesi için tüm ağdaki işlem gücünün büyük bir çoğunluğuna sahip olunması gerekir.[77] Aksi halde zaten yapılmak istenen tüm geçmişe dönük değişiklikler anında anlaşılacak ve dürüst olmayan bu değişiklik talepleri sistem tarafından reddedilecektir. Değişikliğe dirençli yapısı da blokzincirin güven veren bir sistem oluşunu destekleyen en önemli özelliklerindendir.

II. ETHEREUM ALTYAPISI

A. Genel Olarak

Akıllı sözleşmelerin daha iyi anlaşılabilmesi için öncelikle sözleşme ilişkisindeki karşılıklı edimlerin otomatik şekilde ifa edilebilmesine olanak sağlayan teknolojinin, bir diğer ifadeyle teknik altyapının anlaşılması gerekmektedir. Bu nedenle, makalenin bu bölümünde akıllı sözleşmelerin oluşmasına olanak sağlayan Ethereum kavramı, bağlantılı teknik kavramlar ve bu teknoloji sayesinde akıllı sözleşmeleri geleneksel sözleşmeden ayıran özelliklere değinilecektir.

B. Tanımı ve Akıllı Sözleşmeler ile İlişkisi

Ethereum ilk defa Kuzey Amerika Bitcoin Konferansında, 2013 yılında program geliştiricisi ve Bitcoin araştırmacısı Vitalik Buterin tarafından tanıtılmıştır.[78] Vitalik Buterin ve ekibi tarafından, Bitcoin ile birlikte gerçekleştirilen merkezi olmayan güvenli ödeme sisteminin geliştirilmesi, sistemin bir adım daha ileri taşınması amaçlanmıştır. Vitalik Buterin, blokzincir teknolojisinin yalnızca parasal işlemlerde değil, daha pek çok alanda kullanılabileceğine değinmiştir. Ethereum protokolü, başlangıçta bir kripto para biriminin yükseltilmiş bir versiyonu olarak tasarlanmışsa da çıkış noktasının çok daha ötesine geçmiş ve bünyesinde pek çok uygulamaya izin veren bir altyapı sağlamıştır.[79]

[77] İşler, Takaoğlu ve Küçükali (n 74) 79.
[78] Kaynak için bkz. https://ethereum.org/en/whitepaper/. Erişim Tarihi: 25.11.2023.
[79] Vitalik Buterin, 'A Next Generation Smart Contract & Decentralized Application Platform' (2015). Kaynak için bkz. https://blockchainlab.com/pdf/Ethereum_white_paper-

Ethereum blokzincirinin geliştirilmesiyle adeta Bitcoin ile tanıtılan blokzincir teknolojisine yenilikçi bir soluk getirilmiştir. Ethereum'dan önce blokzincir sistemleri yalnızca belli amaçlara hizmet ederken, Ethereum blokzinciri sayesinde çok farklı yazılımlar geliştirme imkânı da ortaya çıkmıştır. Ethereum ve Bitcoin aynı temele yani blokzincir teknolojisine dayanmasına rağmen, Ethereum blokzincir teknolojisini geliştirmiş ve her geçen gün de bu teknolojinin hızla gelişmesine imkân sağlayan bir altyapı sunmuştur. Ethereum blokzinciri sayesinde, önceden kararlaştırılan kurallara göre edimlerin otomatik olarak ifa edilmesini sağlayan sistemler, yani bugünkü kullanımıyla 'akıllı sözleşmeler' literatüre kazandırılmıştır. Akıllı sözleşmeler, blokzincirin evrimleşmesine yol açmış ve blokzincir 2.0 olarak ifade edilen dönemi başlatmıştır.[80] Akıllı sözleşmeler ile amaçlanan, tıpkı Bitcoin'in finansal işlemlerde aracısız güven ortamı yaratma amacı gibi, sözleşme ilişkilerinde de tarafların birbirine güvenmesine ya da aracı kurumlara başvurmasına gerek olmaksızın ifanın güvensiz güven ortamında kendiliğinden ifa edilebilmesidir. Otonom ifa kabiliyeti olan ve 'akıllı sözleşme' olarak uygulamada bilinen bu sistemleri uygulamaya kazandıran ise Ethereum blokzinciri olmuştur.[81]

Ethereum kısaca; Açık kaynaklı, zincirleme modellemesini kullanan, akıllı sözleşme protokolü özelliğine haiz, kamuya açık bir işletim sistemidir.[82] Ether (ETH) ise; aynı Bitcoin gibi bir kripto para birimidir. Ether, Ethereum işletim sistemi üzerinde uygulamaların çalışması için zorunludur. Ethereum blokzincirinde, akıllı sözleşmelerin çalıştırılması için ise Ether'e ihtiyaç vardır.[83] Ethereum, 'Solidity[84]' adlı nesne yönelimli, üst düzey bir yazılım dilini kullanır. Ayrıca Buterin tarafından Bitcoin blokzincirinde kullanılan sertifika değiştirilmiş ve SHA-256 olarak adlandırılan bir algoritmayı kullanılmıştır. Secure Hash Algorithm(SHA), herhangi bir uzunlukta olan girdiyi, sabit bir çıktıya yani özet değere (hash value) çeviren algoritmadır.[85] Dolayısıyla Ethereum blokzincirinde Solidity sayesinde kodlamada ve SHA-256 güvenlik sertifikası ile algoritmada ortaya konan farklılıklar neticesinde, edimlerin otonom ifasına imkân veren akıllı sözleşmeler kodlanabilir ve uygulanabilir hale gelmiştir.[86]

---

a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf. Erişim Tarihi: 25.11.2023.

[80] Kaynak için bkz. <https://digicentralized.com/blockchainin-evrimi/.> Erişim Tarihi:26.01.2024; Kaynak için bkz. https://academy.binance.com/tr/articles/what-is-ethereum. Erişim Tarihi:26.01.2024; Delioğlan (n 25) 22-23.

[81] Mete Tevetoğlu, 'Ethereum ve Akıllı Sözleşmeler' (2021) 12(1) İnönü Üniversitesi Hukuk Fakültesi Dergisi 193, 194.

[82] İbid 193, 196.

[83] ibid 196; Elektronik kaynak için bkz. <https://ethereum.org/en/eth/> Erişim Tarihi: 25.11.2023; Elektronik kaynak için bkz. <https://lorentlabs.com/ethereum-nedir-nasil-ortaya-cikmistir-ethereum-hakkinda-her-sey/> Erişim Tarihi: 25.11.2023.

[84] Kaynak için bkz. <https://docs.soliditylang.org/en/v0.5.3/.> Erişim Tarihi: 25.11.2023.

[85] Özkan (n 15) 52.

[86] Tevetoğlu (n 83) 196,200; Elektronik kaynak için bkz. <https://docs.soliditylang.org/en/v0.5.3/.> Erişim Tarihi: 25.11.2023.

Akıllı sözleşmelerin uygulanabildiği tek platform Ethereum blokzinciri olmamakla birlikte, ilk defa blokzincir tabanlı akıllı sözleşmeleri sunan ve en bilineni Ethereum'dur.[87]

Böylece adeta, teknoloji ve hukuk bir kez daha aynı paydada buluşmuş olur. Günümüzde akıllı sözleşmelerin niteliği, avantajları, riskleri gibi konularda pek çok tartışma bulunsa da akıllı sözleşmelerin hukuku ve teknolojiyi aynı potada erittiği, birlikte var olmaya devam ettiği ve sistemleri değişime zorladığı yadsınamaz bir gerçektir.

III. AKILLI SÖZLEŞMELER

A. Tanımı

Akıllı sözleşmeler, blokzincir teknolojisinden bağımsız şekilde ilk defa şifreleme uzmanı, bilgisayar bilimci ve hukukçu Nick Szabo tarafından tanımlanmıştır. Nick Szabo'ya göre; akıllı sözleşmeler, kâğıt üzerinde hazırlanan geleneksel sözleşmelere göre çok daha güvenilir ve işlevsel yollar sunan, dijital ilişkileri resmi hale getirebilen, içerisinde protokoller barındıran, edimlerin ifasına kadar süren tüm sözleşme sürecini çok daha kolay hale getiren araçlardır.[88]

Szabo, akıllı sözleşmeleri basit şekilde otomatlarla açıklamaktadır.[89] Bu açıklamaya göre; içerisinde çeşitli yiyecek veya içecekler barındıran bir otomatta, her bir ürünün fiyatı ve numaraları bellidir. Otomata para atılır, seçilen ürünün numarasına basılır ve ürün teslim alınır. Yani belli kurallara göre oluşturulmuş sözleşme, otomatik olarak ifa edilmekle sonuçlanır. Basitçe akıllı sözleşmelerin mantığı ''x olursa y olur'' şeklinde özetleyerek açıklansa da akıllı blokzincir teknolojisi ve Ethereum altyapısı sayesinde akıllı sözleşmeler, günümüzde son derece karmaşık ilişkilerde de kullanılabilir hale gelmiştir.[90] Bu gelişim sayesinde özellikle tedarik zinciri, sağlık, sigortacılık, oylama sistemleri, sanat ve müzik endüstrisi dahil pek çok alanda akıllı sözleşmelerden yararlanılmaya başlanmıştır.[91]

Blokzincir tabanlı akıllı sözleşmeleri bir kalıba dahil etmenin zorluğu bir yana çok kesin bir tanım yapılması halinde hızla gelişen teknoloji karşısında yetersiz kalma riski de oldukça fazladır.[92] Ayrıca kesin bir tanım yapılmasının, blokzincir tabanlı akıllı sözleşmelerin

[87] Pınar Çağlayan Aksoy,'Dijital Sözleşmelerin Yeni Yüzü Akıllı Sözleşmeler' (Arksigner, 30 Mart 2023) Kaynak için bkz. https://blog.arksigner.com/blokzinciri-teknolojisi/dijital-sozlesmelerin-yeni-yuzu-akilli-sozlesmeler. Erişim Tarihi: 26.01.2024.

[88] Nick Szabo, 'Formalizing and Securing Relationships on Public Networks' (1997) 2(9) First Monday Kaynak için bkz. <https://firstmonday.org/ojs/index.php/fm/article/view/548.> Erişim Tarihi: 25.11.2023.

[89] Szabo (n34) s.;Tevetoğlu (n 83) 198.

[90] Stuart D. Levi, Alex B. Lipton ve diğerleri, 'An Introduction to Smart Contracts and Their Potential and Inherent Limitations' (Harvard Law School Forum on Corporate Governance 26 Mayıs 2018) Kaynak için bkz. <https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/.> Erişim Tarihi:26.01.2024.

[91] Kaynak için bkz. <https://hedera.com/learning/smart-contracts/smart-contract-use-cases.> Erişim Tarihi:26.01.2024; Kaynak için bkz. <https://www.lawdistrict.com/legal-dictionary/smart-contracts.> Erişim Tarihi:26.01.2024.

[92] Riccardo de Caria, 'Law and Autonomous Systems Series: Defining Smart Contracts - The Search for Workable Legal Categories' (Oxford Business Law Blog, 25 Mayıs 2018) Kaynak için bkz.

uygulama alanlarını hatalı şekilde sınırlama ihtimali de göz ardı edilmemelidir. [93] Literatürdeki tanım çeşitliliğine değindikten sonra, blokzincir tabanlı akıllı sözleşmeler; önceden belirlenen ve kodlanan şartların gerçekleşmesi ile tetiklenen, yine önceden belirlenen ve bireyselleştirilebilen içeriğin otomatik olarak uygulanabildiği bilgisayar programları şeklinde açıklanabilir. [94] Blokzincir teknolojisine dayanan akıllı sözleşmeler, blokzincirin karakteristik özelliklerini bünyesinde barındırmakla, sözleşme süreçlerini edimin ifasını da kapsayacak şekilde otonom hale getirmeyi, süreçlerin daha hızlı ve daha az maliyetle yürütülmesini amaçlar. Ayrıca blokzincir tabanlı olması nedeniyle aracısızlaştırma, eşten eşe güvenli etkileşim, şeffaflık, kendiliğinden ifa, değiştirilemezlik gibi özellikleri de ihtiva eder.[95] Neticeten geleneksel sözleşmelerden ayrılan en büyük farkının; edimin ifasının doğrudan sistem tarafından garanti altına alınması olduğu söylenebilir.

Belirtmek gerekir ki, akıllı sözleşme tanımındaki 'akıllı' ibaresi, sistemin yapay zekâ teknolojileriyle desteklendiği anlamına gelmez. Günümüzde gelişen teknolojilerle birlikte blokzincir temelli akıllı sözleşmeler ile yapay zekâ teknolojisinin entegrasyonu mümkün hale gelmişse de temel kullanımımı itibariyle her akıllı sözleşmenin yapay zekâ teknolojisini de içerdiği çıkarımında bulunulamaz. [96] Aynı şekilde 'sözleşme' ibaresi de hukuki anlamda kullanılan ve yaptırımlara tabi sözleşme kavramını her durumda karşılamaz.[97]

Günümüzde akıllı sözleşmelere dair pek çok tanım yapılmıştır. Kimi tanımlar teknik yönünü kimi ise hukuki niteliğini ön planda tutmaktadır.[98] Dijital dünyanın regüle edilmesinde lider rolü bulunan Avrupa Birliği de bu alanda çalışmalarını sürdürmektedir. Nitekim Avrupa Komisyonu AB Veri Yasası (The Data Act) teklifi çerçevesinde akıllı sözleşmeleri ''*bir elektronik defter sisteminde saklanan ve programın yürütülmesinin sonucunun elektronik deftere kaydedildiği bilgisayar programı*'' [99] şeklinde tanımlamışsa da Avrupa Parlamentosu tarafından değişiklik yapılan metinde bahsi geçen tanım kabul görmemiş ve kaldırılmıştır.[100] Daha sonra Avrupa Parlamentosu ve Avrupa Konseyi Veri Kanunu üzerinde anlaşmaya

<https://blogs.law.ox.ac.uk/business-law-blog/blog/2018/05/law-and-autonomous-systems-series-defining-smart-contracts-search.> Erişim Tarihi:26.01.2024

[93] Doğancı (n 27) 87.

[94] İbid 88.

[95] Blockchain Türkiye, 'Akıllı Sözleşme Raporu', (Blockchain Türkiye, Temmuz 2021) 6. Kaynak için bkz. <https://bctr.org/dokumanlar/Akilli_Sozlesme_Raporu.pdf.> Erişim Tarihi:26.01.2024

[96] Pınar Çağlayan Aksoy, 'Akıllı Sözleşmelerin Dünü, Bugünü ve Yarını: Karşılaştırmalı Bir Değerlendirme' (2022) 42(494) Vergi Dünyası 17, 19; Mükerrem Onur Başar, 'Akıllı Sözleşmeler ve Özel Hukuk Uygulamasında Ortaya Çıkması Muhtemel Sorunlar' (2022) 80 (4) İstanbul Hukuk Mecmuası 1067, 1073.

[97] Pınar Çağlayan AKSOY, 'Akıllı Sözleşmeler: Temel Hukuki Problemler ve Regülasyon' (Hukuk ve Bilişim Dergisi, 26 Mart 2023) Kaynak için bkz. https://www.hukukvebilisimdergisi.com/akilli-sozlesmeler-temel-hukuki-problemler-ve-regulasyon/ Erişim Tarihi:26.01.2024.

[98] Doğancı (n 27) 76-82; Delioğlan (n 25) 9- 12.

[99] Commission, 'Proposal For A Regulation Of The European Parliament and of the Council On Harmonised Rules on Fair Access to and Use Of Data (Data Act)' Com (2022) 68 Final, Ch I, Art 2.

[100] European Parliament, 'Amendments adopted by the European Parliament on 14 March 2023 on the proposal for a regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)' 2022/0047(COD).

varmış ve Veri Yasası Konsey tarafından resmen kabul edilmiştir. Kabul edilen metinde ise akıllı sözleşmeler; '*bir dizi elektronik veri kaydı kullanarak ve bunların bütünlüğünü ve kronolojik sıralamalarının doğruluğunu sağlayarak bir sözleşmenin veya bir kısmının otomatik olarak yürütülmesi için kullanılan bilgisayar programı*''[101] şeklinde ifade edilmiştir.

B. Akıllı Yasal Sözleşmelerin Hukuken Geçerliliği

Bir önceki başlık altında da ifade edildiği üzere; akıllı sözleşmeler kendiliğinden ifayı mümkün kılan bilgisayar programlarıdır. Uygulamada yerleşik olarak 'akıllı sözleşme' kavramının kullanılması, birtakım karışıklıklara yol açmaktadır. Şöyle ki; sözleşme ibaresi başta hukukçular olmak üzere kişilere hukuken bir etki doğurmaya ehil, bağlayıcı sözleşmeleri çağrıştırmaktadır. Fakat bu anlayış, akıllı sözleşmelerin dahil olduğu her durumda geçerli değildir.[102] Akıllı sözleşmelerin hangi hallerde hukuken bağlayıcı sözleşme niteliğine haiz olduğu, yani 'akıllı yasal sözleşme' olarak kabul edilebileceği somut olay nezdinde değerlendirilmeli, akıllı sözleşmenin işlem gördüğü blokzincir türüne, taraflara, menfaatlere ve uygulanacak hukuk kurallarına göre inceleme yapılmalıdır. Nitekim bazı hallerde akıllı sözleşmeler vasıtasıyla bir sürecin yalnızca otomasyonu sağlanabilir ya da akıllı sözleşmeler yalnızca koddan oluşan teknik bir işlemi içerebilir. Dolayısıyla ortada hukuken bir sözleşme bulunmayabilir. [103] Merkezi Olmayan Özerk Kuruluşlarda *(Decentralised Autonomous Organisation-DAO)* gerçekleştirilen oylama şekli bu kullanıma örnek teşkil eder. Teknik anlamda gerçekleştirilen oylama akıllı sözleşmeler vasıtasıyla gerçekleştirildiğinden, tamamen işlemseldir ve hukuki niteliği itibariyle bir sözleşme kurulmamaktadır. Bir diğer türde ise sözleşme zincir dışında (off-chain) kurulur, doğal dillerde kurulan bu sözleşmenin yalnızca icrası için akıllı sözleşmelere başvurulur. Bu halde akıllı sözleşmeler, doğal dilde akdedilen sözleşmenin yalnızca otonom ifasını gerçekleştirmek üzere sözleşme sürecine dahil edilen araçlardır. Zincir dışı (off-chain) akdedilen bir uçuş sigorta sözleşmesinin yalnızca icrasının akıllı sözleşmeler vasıtasıyla gerçekleştirilmesi bu duruma bir örnek teşkil eder. Şöyle ki; müşteriler tarafından internet sitesi üzerinden (off-chain şekilde) uçuş gecikmelerine karşın sigorta yaptırılmaktadır. Böylece Müşteri/yolcu ve sigortacı arasında, poliçe hükümleri incelendikten sonra, zincir dışı olacak şekilde, uçuş gecikmelerine dair bir sigorta sözleşmesi akdedilmiş olur. Akıllı sözleşme ise sigorta sözleşmesinin icrası

[101] Regulation of the European Parliament and of the Council on Harmonised Rules On Fair Access to and Use Of Data and Amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act)

[102] Çağlayan Aksoy, 'Akıllı Sözleşmelerin Dünü, Bugünü ve Yarını' (n 98) 26.

[103] Fikriye Ceren Sadioğlu, 'Borçlar Hukuku Çerçevesinde Akıllı Sözleşmenin İşlevleri ve İşlevlerin Yerine Getirilmesi Sırasında Karşılaşılan Sorunlar' (2021) 25(4) Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi 171, 182-184; Çağlayan Aksoy, 'Akıllı Sözleşmelerin Dünü, Bugünü ve Yarını' (n 98) 25-26; Avrupa Hukuk Enstitüsü, 'Blokzincir Teknolojisi, Akıllı Sözleşmeler ve Tüketicinin Korunması Hakkında ELI İlkeleri' Raporu, 26-33. Kaynak için bkz. <https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_Blockchain_Technology__Smart_Contracts_and_Consumer_Protection.pdf.> Raporun çevirisi için bkz. <https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/Blokzinciri_Teknolojisi__Akilli_So__zles__meler_ve_Tu__keticinin_Korunmasi_Hakkinda_ELI_I__lkeleri_-_Avrupa_Hukuk_Enstitu__su___Raporu_-_Nesli_S__en_O__zc__elik_O__zer.pdf.> Erişim Tarihi: 26.01.2024.

aşamasında devreye girmektedir. Zincir dışı akdedilen sözleşmenin hükümleri akıllı sözleşmeye kodlanmıştır. Böylece sigorta edilen uçuşta bir gecikme yaşanması halinde, akıllı sözleşme tetiklenmekte ve önceden poliçe hükümleri çerçevesinde belirli olan sigorta teminat tutarı, müşterilerin başkaca bir işlem yapmasına gerek kalmaksızın hesaplarına aktarılmaktadır. Uçuşun gecikmesini konu alan bu sigorta sözleşmesi uyarınca, sigortalanan uçuşta 2 saat üzeri bir rötar yaşanması halinde, önceden belirlenen bedel müşterilerin hesabına otomatik olarak yatırılmış olur.[104] Bu durumda akıllı sözleşmelerin yasal sözleşme sürecinin yalnızca belli bir kısmına da dahil olabileceği söylenebilir. Bahsi geçen sigorta sözleşmesi örneğinde, akıllı sözleşmeler vasıtasıyla otomatikleştirilen kısım yalnızca sözleşmenin icrasıdır. Son olarak incelenecek tür ise müzakere süreci dahil tüm sözleşme sürecinin zincir içinde gerçekleştirildiği uygulamadır. Bu halde akıllı sözleşme yalnızca zincir içi kurulabilir ya da hem zincir içi hem de zincir dışında bulunacak şekilde düzenlenebilir. Sözleşmeye uygulanacak hukuk kuralları çerçevesinde değerlendirildiğinde, zincir içi akıllı sözleşmelerin hukuken geçerli ve bağlayıcı nitelikte olduğu kabul edilebilir.[105] İşte yasalar uyarınca, hukuken geçerlilik atfedilen bu akıllı sözleşmeler bakımından bir ayrım yapmak adına 'akıllı yasal sözleşmeler' ifadesi de kullanılmaktadır.[106]

6098 Sayılı Türk Borçlar Kanunu (TBK) uyarınca[107]; tarafların icap(öneri) ve kabulden oluşan, karşılıklı ve birbirine uygun iradelerini açıklamaları ile hukuken geçerli ve bağlayıcı nitelikte bir sözleşme kurulmaktadır. Ayrıca Türk Hukuku'nda şekil şartı getirilen haller ayrık tutulmakla beraber, sözleşme serbestisi ilkesi esas alınmaktadır. Kanunda ayrıca bir şekil şartı öngörülmeyen, kanunun emredici hükümlerine, ahlaka, kamu düzenine, kişilik haklarına aykırı olmayan veya konusu imkânsız olmayan sözleşmelerin, geleneksel yollarla kurulması ile programlama dilleri kullanılarak blokzincir üzerinde akıllı yasal sözleşme olarak kurulması arasında da bir fark bulunmamaktadır.[108] TBK uyarınca, sözleşmenin hukuken bağlayıcı ve geçerli olduğunun kabulü için ayrıca tarafların hak ve fiil ehliyetlerinin mevcut olması ve hata, hile ya da korkutma gibi irade bozukluklarının bulunmaması gerekmektedir.[109] Nitekim akıllı sözleşmeler çerçevesinde kişilerin gerçek ad soyadlarını

[104] Sezai Tunca ve Bülent Sezen, 'Sigorta İşlemlerinde Blokzincir (Blockchain) Teknolojisi Uygulamaları' (2020) (14) Bankacılık ve Sigortacılık Araştırmaları Dergisi 13, 20; Elektronik kaynak için bkz.< https://webrazzi.com/2017/10/06/axa-fizzy/.> Erişim Tarihi: 26.01.2024; Doğancı (n 27) 147,148; Avrupa Hukuk Enstitüsü, 'Blokzincir Teknolojisi, Akıllı Sözleşmeler ve Tüketicinin Korunması Hakkında ELI İlkeleri' Raporu, 29; Andrea Stazi,' Smart Contracts and Comparative Law, A Western Perspective' (Springer Cham, 2022) 84-86. https://doi.org/10.1007/978-3-030-83240-7.

[105] Avrupa Hukuk Enstitüsü, 'Blokzincir Teknolojisi, Akıllı Sözleşmeler ve Tüketicinin Korunması Hakkında ELI İlkeleri' Raporu, 29; Çağlayan Aksoy, 'Akıllı Sözleşmelerin Dünü, Bugünü ve Yarını' (n 98) 9-10.

[106]Çağlayan Aksoy, 'Regülasyon' (n 99) Elektronik kaynak için bkz. https://www.hukukvebilisimdergisi.com/akilli-sozlesmeler-temel-hukuki-problemler-ve-regulasyon/ Erişim Tarihi:26.01.2024; Stazi (n 107) 84-86.

[107] Türk Borçlar Kanunu, Kanun Numarası: 6089, Kabul Tarihi: 11.01.2011, RG 04.02.2011/ 27836.

[108] Blockchain Türkiye, 'Akıllı Sözleşme Raporu', (Blockchain Türkiye, Temmuz 2021) 16. Kaynak için bkz. <https://bctr.org/dokumanlar/Akilli_Sozlesme_Raporu.pdf.> Erişim Tarihi:26.01.2024

[109] Türk Borçlar Kanunu, Kanun Numarası: 6089, Kabul Tarihi: 11.01.2011, RG 04.02.2011/ 27836.

kullanarak işlem yapması bir zorunluluk değildir. Bu durumda sözleşmenin bir tarafında küçük ya da kısıtlı bir kimsenin bulunması da ihtimal dahilindedir.[110]

Sonuç itibariyle, Türk Hukuku çerçevesinde belirtilen şartlara riayet eden akıllı sözleşmelerin hukuken geçerli ve bağlayıcı olacağı kabul edilir.[111] Yine de akıllı sözleşmeler ve temelinde yatan blokzincir teknolojisinde programlama dillerinin kullanılması nedeniyle, bu sistemlerin teknik boyutunun herkes tarafından kolaylıkla anlaşılamama ihtimali bulunmaktadır. Bu nedenle taraflar arası akdedilmiş zincir dışı bir sözleşme de var ise ve taraflarca aksi kararlaştırılmamışsa, zincir dışı sözleşmeye öncelik atfedileceği kabul edilmektedir.[112]

O halde akıllı sözleşmelerin yasal anlamda sözleşme olup olmadığının, o sözleşmeye uygulanacak hukuk kuralları çerçevesinde ve somut olay özelinde değerlendirilmesi gerekir. Her akıllı sözleşmenin yasal anlamda hukuki sonuç doğurmaya ehil, geçerli ve bağlayıcı bir sözleşme niteliğinde olduğu kabul edilemez. Akıllı sözleşme, bir tetikleyicinin aktif olması ile otomatik olarak çalışan bilgisayar programları iken; akıllı yasal sözleşmeler, sözleşme şart ve yükümlülüklerinin yerine getirilmesi adına harici yazılımlar veya veri kaynaklarıyla çalışabilen, hukuken bağlayıcı olan anlaşmalardır.[113] Bu durumda akıllı sözleşmeler bir üst kavram, akıllı yasal sözleşmeler ise onun bir alt dalı olarak kabul edilebilir.[114]

C. Özellikleri ve Geleneksel Uygulamalarla Karşılaştırılması

Akıllı sözleşmeler, geleneksel yöntemlerle uzun ve zahmetli iş süreçlerine karşı hızlı ve güvenilir bir iş yapma metodu vadetmektedir. Akıllı sözleşmelerin bu etkisi hemen hemen tüm sektörleri etkileyebilecek niteliktedir. Bu bölümde, akıllı sözleşmelerin geleneksel düzenden ayrışan özelliklerinin neden sistemde köklü bir değişiklik yaratabilecek potansiyelde olduğu ve bünyesinde barındırdığı risklerin neler olduğu açıklanmıştır.

1. Kendiliğinden İfa Edilebilirlik

Akıllı sözleşmelerin kendi kendine ifa edilebilirlik, diğer bir ifadeyle otonom olma özelliği; kanımızca akıllı sözleşmelerin değerini yaratan en kritik özelliktir. Bu nedenle akıllı sözleşmelere kendiliğinden ifa edilebilen sözleşmeler *(self-executing contracts)* de

[110] Doğancı (n 27) 106.
[111] Üstün (n 28) 81.
[112] Avrupa Hukuk Enstitüsü, 'Blokzincir Teknolojisi, Akıllı Sözleşmeler ve Tüketicinin Korunması Hakkında ELI İlkeleri' Raporu, 40.
[113] Tim Sloane, 'The Difference between a Smart Contract and a Smart Legal Contract Explained' (PaymentsJournal, 24 Eylül 2021) Kaynak için bkz. https://www.paymentsjournal.com/the-difference-between-a-smart-contract-and-a-smart-legal-contract-explained/ Erişim Tarihi: 25.01.2024.
[114] Harriet Jones-Fenleigh, Adam Sanitt ve Jonathan Hawkins, ' Smart legal contracts under English law - Part 1: Introduction' (Norton Rose Fulbright, 1 Şubat 2022) Kaynak için bkz. https://www.nortonrosefulbright.com/en/inside-disputes/blog/202202-smart-legal-contracts-under-english-law-introduction#:~:text=Smart%20legal%20contracts%20are%20a,or%20partly%2C%20without%20human%20assistance. Erişim Tarihi: 25.01.2024.

denilmektedir.[115] Geleneksel sözleşmelerde; taraflar karşılıklı olarak hak ve yükümlülüklerini belirler, hangi şartlar altında hangi edimlerin taraflara yükletildiği detaylarıyla açıklanır ve karşılıklı iradelerin uyuşması ile sözleşmeler kurulur. Fakat tarafların bir kez sözleşmeyi akdetmesi; her iki tarafın da edimlerini yerine getireceği anlamına gelmez.[116] Dolayısıyla geleneksel anlamda çok detaylı olarak hazırlanmış bir sözleşme dahi; uyuşmazlık çıkmasını engelleyemeyebilir. Akdin tarafları arasında uyuşmazlık çıktığı durumda, şayet sözleşmede cezai şart, tazminat, uyuşmazlık çözüm yeri ve sair haller düzenlenmişse, tarafların hangi taleplerde bulunabileceği ya da hangi mahkemelerin yetkili olduğu gibi hususlar belirli olabilir. Fakat söz gelimi temerrüt halinde bir cezai şart düzenlenmişse, geleneksel yöntemde ilgili tarafın bu tutarı otomatik olarak karşı tarafa ödemesini zorunlu kılan bir sistem bulunmamaktadır. Bu durumda somut olayın özelliklerine göre, taraflar mahkemelere başvurarak hak arama yoluna gidebilir. Dolayısıyla geleneksel yöntemlerin özünde yine karşı tarafa güven ya da üçüncü kişi ya da kurumlara başvuru esas alınmaktadır. İşte bu noktada akıllı sözleşmelerin otomatik olarak edimlerin ifasını sağlaması, geleneksel sözleşmelerden ayrıldığı bir özellik olarak ortaya çıkmaktadır. Nitekim akıllı sözleşmelerde, sözleşme hükümleri ve karşılıklı edimler belirlenip blokzincir üzerine kaydedildiği takdirde, artık sözleşmenin tarafları dahil hiç kimse tarafından müdahaleye izin verilmez ve karşılıklı edimler otomatik olarak başkaca bir işleme gerek olmaksızın gerçekleşir. Dolayısıyla ifa aşamasında, tarafların bir etkisi bulunmamaktadır. Zaten akıllı sözleşmeler, önceden sisteme kodlanan talimatlar doğrultusunda işlemleri kendiliğinden gerçekleştirmektedir.[117]

Otonom ifa, bazen avantaj bazense dezavantaj olarak algılanabilir. Akıllı sözleşmelerde taraflar; üzerlerinde anlaştıkları sözleşme maddelerini kodlarla ifade ederek sisteme yükler ve önceden kararlaştırılan bu edimler sistemin kendisi tarafından, herhangi bir başvuru ya da talebe gerek olmaksızın, şartlar gerçekleştiği anda otomatik olarak ifa edilir. Böylece akıllı sözleşmeler ile, geleneksel sözleşmelerin aksine, edimin yerine getirilmesini de garanti eden bir sistem oluşturulması amaçlanmıştır.[118] Fakat blokzincir tabanlı akıllı sözleşmelerin değişmezlik özelliği neticesinde, sonuç doğurması istenmeyen veya üzerinde değişiklik yapılmaya ihtiyaç duyulan sözleşmeler de sisteme ilk kaydedildiği haliyle çalışmaya devam eder. Örneğin; sözleşmenin kodlanması aşamasında bir hata yapılması halinde, sisteme yüklenen ve fakat sonuç doğurması talep edilmeyen akıllı sözleşmedeki edimler de otonom olarak ifa edilir. Yine TBK Madde 27 uyarınca düzenlenen kesin hükümsüzlük hallerinin ya da TBK Madde 30, 36 ve 37. Maddelerinde düzenlenen yanılma, aldatma, korkutma gibi irade sakatlıklarının somut olayda mevcut olması, sözleşmelerin taraf iradelerini doğru bir şekilde yansıtmaması, sözleşmenin haksız şartlar barındırıyor oluşu gibi hallerde de akıllı sözleşmelerin ifa sürecine müdahale edilemeyeceğinden, hukuki düzlemde ortaya çıkabilecek sorunlara gebe bir sistem olduğu ve her zaman tarafların arzu ettiği sonuçları

[115] Elektronik kaynak için bkz. <https://www.investopedia.com/terms/s/smart-contracts.asp.> Erişim Tarihi: 25.11.2023.
[116] Çubukçu (n 29) 38-39.
[117] İbid 38-43.
[118] Üstün (n 28) 50.

garanti etmediği söylenebilir.[119] Bu gibi risklerin en aza indirgenmesi amacıyla sözleşmenin başlangıcında; temerrüt, kötü ifa, imkânsızlık halleri ve ifa etmeme durumlarının öngörülmesi ve tarafların iradelerinin örtüştüğü tüm bu hususların kodlanarak sisteme doğru bir şekilde yüklenmesi gerekmektedir.[120] Ayrıca otonom ifadan doğan sakıncaların önüne geçmek adına, bir takım teknik çareler de zaman içinde düşünülmüştür. Fakat belirtmek gerekir ki, akıllı sözleşmelerin esas amacı; taraflarca belirlenen sözleşme edimlerinin hiçbir müdahaleye ihtiyaç duyulmaksızın yerine getirilmesini teminat altına almaktır. Dolayısıyla akıllı sözleşmeler ile temelde odaklanılan hedef; sözleşme öncesi veya sözleşme süresince ortaya çıkabilecek sorunlara çözüm sağlamak değil, geçerli bir şekilde taraflar arasında kurulan sözleşmenin işlevini yerine getirmesini aracısız, güvenilir ve otomatik olarak sağlamaktır.[121] Borçlar hukukuna göre geçerli ve bağlayıcı bir akıllı yasal sözleşme çerçevesinde, kendiliğinden ifa özelliği ifayı da garanti altına alacağından büyük fayda sağlayacağı söylenebilir. Fakat daha önce de belirtildiği üzere, akıllı sözleşmenin geçerli ve taraflar arasında bağlayıcı olup olmadığına borçlar hukuku kuralları uyarınca karar verilir. Nitekim akıllı sözleşmeler de borçlar hukukuna tabidir. Sonuç olarak, kendiliğinden ifa özelliğinin uygulamada problem yaratma potansiyeli olduğu bir gerçektir. Aynı zamanda akıllı sözleşmelerin bu özellik doğrultusunda nihai hedefi; uygulamaya konan bir sözleşmenin taraflarca ihlal edilmesinin önlenmesi ve hiçbir müdahaleye gerek kalmaksızın ifanın yerine getirilmesinin sistem dinamikleri sayesinde teminat altına alınmasıdır.[122]

2. Değişmezlik

Akıllı sözleşmelerin öne çıkan bir diğer özelliği ise; değişmezliktir. Yukarıda detaylı olarak açıklandığı üzere; bugünkü kullanımı itibariyle akıllı sözleşmeler, blokzincir teknolojisinden temellerini almaktadır. Blokzincir teknolojisi; akıllı sözleşmelerin saklanması ve ifası bakımından, değişmezlik özelliği ile sözleşmeleri güvenli hale getirmektedir. Nasıl ki bloklar üzerine kriptografik olarak şifrelenerek kaydedilen bir verinin geriye dönük olarak kurcalanması ve değiştirilmesine karşı sistem dayanıklı ise blokzincir ağına kaydedilen bir akıllı sözleşmeye de sonradan müdahale edilmesi mümkün değildir. Böylece tarafların üzerinde anlaştıkları ve kodlarla ifade ettikleri sözleşme koşullarının manipülasyonu engellenmiş olur. Böylece akıllı sözleşmeler ve geleneksel sözleşmeler arasındaki ayrımda, akıllı sözleşmelerin değişikliğe dirençli yapısı da öne çıkan bir unsur olarak kabul edilir. Keza geleneksel sözleşmelerde; sözleşme şartları üzerinde değişiklik yapılabilir, tarafların iradesi doğrultusunda veya mahkemeye başvuru yoluyla sözleşme yeni şartlara uygun düşecek şekilde uyarlanabilir veya sözleşme feshedilebilir. Akıllı sözleşmelerde ise; taraflar dahil, herhangi bir kişi ya da kurumun yürürlüğe girmiş sözleşmeye müdahale etmesi mümkün değildir. Dolayısıyla değişmezlik özelliği, akıllı sözleşmenin yürürlüğünü kapsamaktadır.[123]

[119]Çağlayan Aksoy, 'Regülasyon' (n 99) Elektronik kaynak için bkz. https://www.hukukvebilisimdergisi.com/akilli-sozlesmeler-temel-hukuki-problemler-ve-regulasyon/ Erişim Tarihi:26.01.2024; Başar (n 98) 1077-1078.
[120] Sadioğlu (n 43) 186.
[121] Başar (n 98) 1077.
[122] İbid 1073,1074, 1078.
[123] Çubukçu (n 29) 33.

Akıllı sözleşmelerin kendiliğinden ifa özelliğinin değerlendirildiği bölümde de işaret edildiği üzere, sözleşmenin kuruluşu veya yürürlüğü aşamasında ortaya çıkabilecek ihtilaflarda, hukuka aykırılık hallerinde veya teknik aksaklıklarda sözleşmeye müdahale edilmek istense dahi kural olarak edimin otomatik olarak gerçekleştirilmesi durdurulamamaktadır. Akıllı sözleşmeler ile sunulan bu katı sistemde ortaya çıkması muhtemel müdahale sorununa çare olabilecek birtakım mekanizmalar öngörülmüştür.[124]

Nitekim Avrupa Birliği Veri Yasası Madde 36 uyarınca, veri paylaşım anlaşmaları için kullanılan akıllı sözleşmeleri sunan kişilerin sağlaması gereken temel gereksinimler düzenlenmiştir. Buna göre; işlevsel hataların engellenmesi amacıyla akıllı sözleşmelere erişim mekanizmaları eklenmesi vasıtasıyla erişim kontrolünün sağlanması, istenmeyen sonuçların engellenebilmesi veya sözleşmenin yürütülmesinin talep edildiği takdirde durdurulması amacıyla akıllı sözleşmelere güvenli sonlandırma *(safe termination)* ya da sözleşmeyi kesintiye uğratma*(interruption)* talimatını verecek dahili mekanizmaların *(kill switch)* eklenmesi, denetlenebilirliğin temini amacıyla akıllı sözleşmenin feshi ya da devre dışı bırakılması durumlarında işlem geçmişinin ve kodun arşivlenmesi, sürekliliğin sağlanması bu temel gereksinimler arasında sayılmıştır.[125] Esasen bu durumda, sözleşmeye müdahale edilmesi ya da sözleşmenin feshedilmesi gerektiği takdirde erişimi mümkün kılan mekanizmaların akıllı sözleşmeye kuruluş aşamasında eklenmesinden bahsedilmektedir. Dolayısıyla bu durum, akıllı sözleşmelerin kodlandıktan ve sisteme yüklendikten sonra değişikliğe izin veren bir yapıya dönüştürülebileceği anlamına gelmez. Akıllı sözleşmeler, blokzincir temelli yapısı nedeniyle değişmezlik özelliğini ihtiva etmeye devam eder. Fakat taraflarca akıllı sözleşmelerin kodlanması aşamasında, sözleşmenin feshi veya uyarlanması gereken haller tespit edilip, bu durumda nasıl bir yöntem izleneceği hususu da koda eklenebilir. Bu nevi önlemler de kuruluş aşamasında gerçekleştirilmesi nedeniyle *'ex-ante'* önlemler olarak kabul edilmektedir. Örneğin, taraflardan birinin müzik dosyası sağladığı diğerinin ise bir bedel karşılığında bu müzik dosyasını edindiği akıllı sözleşmede, müşteri ücretini ödemesine rağmen müzik dosyasını indiremiyor ise akıllı sözleşme içine kodlama aşamasında eklenen iade komutu tetiklenerek para iadesi gerçekleştirilebilir.[126] Bu durumda akıllı sözleşmelerin kodlanması aşamasında; istenmeyen sonuçları önleyebilmek adına

[124] Aybüke Uzunpınar Tüfek, 'Akıllı Sözleşmelerde Esneklik İhtiyacı: Akıllı Sözleşmelerin Değiştirilmesi ve Sona Ermesi' (Akıllı Sözleşmeler Bilkent, 25 Kasım 2023) Elektronik kaynak için bkz. https://akillisozlesmeler.bilkent.edu.tr/2023/12/akilli-sozlesmelerde-esneklik-ihtiyaci-akilli-sozlesmelerin-degistirilmesi-ve-sona-ermesi/. Erişim Tarihi: 26.01.2023.

[125] Regulation of the European Parliament and of the Council on Harmonised Rules On Fair Access to and Use Of Data and Amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act); EU Blockchain Observatory and Forum, 'Smart Contracts' Raporu için bkz. https://www.eublockchainforum.eu/sites/default/files/reports/SmartContractsReport_Final.pdf. Erişim Tarihi: 26.01.2026; Furkan Güven Taştan, 'AB, Akıllı Sözleşmeleri Düzenlemenin Eşiğinde: Veri Kanunu Teklifi,Parlamento'dan Geçti' (Akıllı Sözleşmeler Bilkent, 27 Mart 2023) Elektronik kaynak için bkz.<https://akillisozlesmeler.bilkent.edu.tr/2023/03/ab-akilli-sozlesmeleri-duzenlemenin-esiginde-veri-kanunu-parlamentoda-kabul-edildi/.> Erişim Tarihi: 26.01.2024.

[126] Pınar Çağlayan Aksoy, *Akıllı Sözleşmelerin Kuruluşu ve Geçerlilik Şartları* (2. Baskı, On İki Levha 2021) 316-318.

sözleşmenin sonlandırılacağı ve kesintiye uğrayacağı hallerin açıkça belirlenmesi gerekmektedir.

Ayrıca akıllı sözleşmelerin değişmezlik özelliği nedeniyle karşılaşılabilecek sorunların çözümü için yapay zekâ destekli sistemlere de başvurulabilir. Şayet akıllı sözleşmelerin kodlanmasında teknik hatalar yapılması, güvenlik açıklarının bulunması ya da içerik itibariyle taraf iradelerinin doğru şekilde yansıtılmaması ihtimal dahilindedir.[127] Yapay zekâ ise, akıllı sözleşme kodlarının incelenmesi ve hata *(bug)* tespitinde devreye girebilir. Koddaki hatalar ve güvenlik açıkları en baştan tespit edilir, ortak kusurların tespiti ve düzeltilmesi için büyük miktarda akıllı sözleşme kodu incelenebilir ve düzeltilebilir.[128] Akıllı sözleşmelerde sonradan ortaya çıkabilecek sorunların engellenmesi amacıyla başvurulabilecek bir diğer yapay zekâ destekli yöntem ise; bilgisayarların insan dilini anlamasına, yorumlamasına, analiz etmesine ve işlemesine imkân veren, bir makine öğrenimi teknolojisi olan doğal dil işleme *(Natural Language Processing – NLP [129]) yöntemidir*. Buna göre doğal dil işleme yöntemi sayesinde akıllı sözleşmelerin dili analiz edilip, belirsizlikler kuruluş aşamasında düzeltilebilir. Blokzincir ekosistemindeki aktörlerden olan geliştiriciler; akıllı sözleşmelerin kodlanması aşamasında, koddaki hataların ve güvenlik açıklarının tespiti ve giderilmesi, NLP vasıtasıyla dil bakımından muğlaklık ya da tutarsızlıkların en baştan önlenmesi amacıyla yapay zekâ teknolojilerinden yararlanabilirler.[130] Ayrıca akıllı sözleşmeler ve yapay zekâ teknolojilerinin entegrasyonu sayesinde; zincir dışı bir sözleşmenin akıllı sözleşmeye çevrilmesi için gereken kod oluşturabilir, bilgisayar dilinde yazılı akıllı sözleşmelerin ise amacı, konusu, işlevi gibi konularda doğal dilde okunabilir ve anlaşılabilir bir kaynak sunabilir. Böylelikle blokzincir ağına eklendikten sonra, akıllı sözleşmelerin işleyişine dair potansiyel sorunlar en baştan önlenebilir.[131] Gelecekte özellikle karmaşık akıllı sözleşmelerin kullanıldığı süreçlerde yapay zekâ teknolojilerinden sıkça yararlanılması mümkündür.

Akıllı sözleşmelerin değişmezlik ve otonom ifa özelliklerinden doğan risklerin minimalize edilmesi adına bulunan teknik çözümlerden bir diğeri ise güncellenebilir veya revize edilebilir (*upgradable)* akıllı sözleşmelerdir.[132] Hataların düzeltilmesi, işlevselliğin, verimin, güvenliğin arttırılması ve değişen taleplerin karşılanması gibi nedenlerle akıllı sözleşmelerde güncelleme yapma ihtiyacı doğabilir. Bu durumda akıllı sözleşmeyi güncellemek; geliştirme yapılmak istenen akıllı sözleşmenin zincirde adeta terk edilmesi ve

[127] Pınar Çağlayan Aksoy, 'Yapay Zekadan Yararlanan Akıllı Sözleşmeler' (Arksigner, 30 Ekim 2023) Elektronik kaynak için bkz. https://blog.arksigner.com/blokzinciri-teknolojisi/yapay-zekadan-yararlanan-akilli-sozlesmeler. Erişim Tarihi: 26.01.2024.

[128] Moez Krichen, 'Strengthening the Security of Smart Contracts through the Power of Artificial Intelligence' (2023) 12(5)107 *Computers* 10,11.

[129] Elektronik kaynak için bkz. https://aws.amazon.com/tr/what-is/nlp/#:~:text=Do%C4%9Fal%20dil%20i%C5%9Fleme%20(NLP)%2C,ses%20ve%20metin%20verilerine%20sahiptir. Erişim Tarihi: 26.01.2024

[130] Krichen (n 131) 10.

[131] Çağlayan Aksoy, 'Yapay Zekâ' (n 130) Elektronik kaynak için bkz. https://blog.arksigner.com/blokzinciri-teknolojisi/yapay-zekadan-yararlanan-akilli-sozlesmeler. Erişim Tarihi: 26.01.2024.

[132] Doğancı (n 27) 527.

onun yerine farklı bir akıllı sözleşmenin konulması anlamına gelir.[133] Bu halde de akıllı sözleşmenin değişmezlik özelliğine halel gelmemektedir. Nitekim ilk olarak kodlanarak sisteme eklenen akıllı sözleşmede herhangi bir değişiklik yapılamamakta, yalnızca bu sözleşmenin etkisiz hale getirilmesi ile yeni bir versiyonun sisteme eklenmesi söz konusu olmaktadır. Bir diğer ifadeyle; güncellenmiş versiyon, ilk olarak kodlanan ve sisteme eklenen akıllı sözleşmenin yerini almaktadır.[134]

Hızla gelişen teknolojiyle birlikte, yukarıda ifade edilenler dışında daha pek çok alternatif yöntem üretildiğini söylemek mümkündür. Kanımızca değişmezlik ve kendiliğinden ifa gibi akıllı sözleşmelere asıl değerini katan özelliklerin esnetilmesi ve bu teknolojinin geleneksel sistemlere uygun hale getirilmesi inovasyonu engelleme tehlikesini barındırmaktadır. Nitekim blokzincir teknolojisi ve bu teknolojiye dayanan akıllı sözleşmeler, bünyesinde barındırdığı multidisipliner yapılar sayesinde sistemleri ve süreçleri dijital dönüşüme zorlayan, önemli inovasyonlardır. Fikrimizce, değişmezlik özelliği nedeniyle doğabilecek sorunların çözümü için geliştirilen teknik çarelerde akıllı sözleşmelerin temel prensiplerinden feragat edilmemesi daha doğru bir yaklaşım olur.

3. Aracılara Duyulan İhtiyaç Bakımından

Akıllı sözleşmeler, güvensiz güven ortamının kurulması ile işlemlerin aracısız şekilde gerçekleştirilebilmesini sağlar. Böylece tarafların birbirine güvenmesine ya da banka, sigorta şirketleri, noterler gibi güven duydukları aracı kurumları sürece dahil etmelerine gerek kalmaz. Üçüncü kişilerin akıllı sözleşme sürecinde bulunmamasının; işlem hızının artması ve masrafları azaltması gibi faydaları da bulunmaktadır.[135]

Örneğin; akıllı sözleşmeler vasıtasıyla bir tapu devri gerçekleşecek olsun. E-devlet hizmeti olarak blokzincir altyapısının kullanıldığı ve tarafların e-devlet şifreleri ile kimliklerini doğrulayarak sisteme girdiğini düşünelim. Taşınmazını satmak isteyen A'nın tapuda malik olup olmadığı ve taşınmazı satın almak isteyen B'nin banka hesabındaki tutarın yeterli olup olmadığının kontrolü sistem tarafından gerçekleşsin. Gerekli denetim ve doğrulama işlemleri yapıldıktan ve taraflarca onay verildikten sonra, eş zamanlı olarak; B'nin hesabından gayrimenkul satışı için belirlenen para A'ya aktarılır, tapuda malik olarak da B kaydedilir. Yapılan bu işlem de tapu devrine dair akıllı sözleşmenin bulunduğu blokzincir ağına zaman damgasıyla kaydedilir. Ayrıca bu gibi süreçlerde, insan müdahalesinden kaynaklı sorunlar da bertaraf edilmiş olur ve sistemler arası iletişim sağlanarak hızlı şekilde işlemler gerçekleştirilebilir.[136] Elbette ki bu işlemlerin gerçekleşmesi için gerekli teknolojik altyapının kurulması ve devlet kurumları tarafından bu teknolojilerin kullanılmaya

[133] Elektronik kaynak için bkz. https://blog.chain.link/upgradable-smart-contracts/. Erişim Tarihi: 26.01.2024
[134] Doğancı (n 27) 527.
[135] Çubukçu (n 29) 34,35; Çağlayan Aksoy, 'Akıllı Sözleşmelerin Kuruluşu' (n 129) 56; Üstün (n 28) 61-62.
[136] Ahmet Usta ve Serkan Doğantekin, 'Blockchain 101' (Bankalararası Kart Merkezi, 30 Nisan 2018) 37-38. Elektronik kaynak için bkz. https://bkm.com.tr/wp-content/uploads/2019/08/15082019_kitap.pdf. Erişim Tarihi: 30.11.2023.

başlanması gerekmektedir.[137] Blokzincir ve akıllı sözleşmeler gibi sistemleri değişime iten teknolojilere karşı her devletin tutumu farklıdır. Keza tapu sicilinde blokzincir teknolojisinin kullanımı açısından; Gürcistan, İsveç, Amerika Birleşik Devletleri gibi bazı devletlerde birtakım projeler yürütülmüştür.[138] Dijital dönüşümü süreçlerine uygulamada öncü rolü bulunan ülkelerden biri de Estonya'dır. Estonya'da kullanılan KSI Blokzincir altyapısı sayesinde vatandaşlar e-kimlik adı verilen bir dijital kimliğe sahip olur. Vatandaşlar kendilerine atanan dijital kimlik sayesinde; oy vermek, tıbbi kayıtlarına erişmek, sağlık veya eğitim hizmetlerinden yararlanmak, fatura ödemek, sözleşme imzalamak gibi işlemlerini de blokzincir destekli bu sistem vasıtasıyla efektif ve güvenilir şekilde gerçekleştirme imkânı elde etmiştir.[139] Böylece Estonya, oy vermek gibi vatandaşlık hizmetlerini de içeren blokzincir uygulamalarını kullanmak konusunda lider ülkelerden biri haline gelmiştir.[140] Sonuç itibariyle, bu teknolojilerin kullanılmaya başlanması halinde, üçüncü kişi ve kurumlara duyulan ihtiyacın büyük oranda azalacağı, maliyetlerin düşeceği, hızlı ve efektif şekilde işlemlerin gerçekleştirilebileceği söylenebilir.

4. Veri Sağlayıcılar Yoluyla Dış Dünyayla Etkileşim

Akıllı sözleşmelerin öne çıkan özellikleri; kendiliğinden ifayı sağlaması, sonradan değişiklik yapılmasının mümkün olmaması ve sistemin dinamikleri sayesinde güven ortamını oluşturması sayesinde aracı kişi ya da kurumlara duyulan ihtiyacı ortadan kaldırmasıdır. Akıllı sözleşmeler, harici müdahalelere kapalı bir yapıdadır. Fakat bazı hallerde, akıllı sözleşmeler kapsamında belirlenen edimlerin gerçekleşip gerçekleşmediğinin kontrolü, dış dünyadan alınacak verilere bağlı olabilir. Akıllı sözleşmeler bu verileri kendiliğinden elde edemez. Çünkü blokzincir ağları internete bağlı değildir. Dolayısıyla akıllı sözleşmelerin gerçek dünya ile etkileşimi bulunmamaktadır. Bu durumda harici veri sağlayıcısına *(oracle)* ihtiyaç duyulmaktadır.[141] Harici veri sağlayıcısı da bir nevi dış dünya ile blokzincir ağında var olan akıllı sözleşme arasında köprü görevi gören bir aracıdır.[142] Harici veri sağlayıcıları, blokzincir dışından akıllı sözleşmelerin ihtiyaç duyduğu verileri iletme görevini üstlenir. Harici veri sağlayıcılar; bir kişi, kurum, algoritma, cihaz, internet sitesi ve hatta yapay zekâ olabilir.[143] Akıllı sözleşmeler, belirlenen işlemleri yerine getirmek için veri sağlayıcılarını kullanarak

[137] Parmila Kargar, 'Akıllı Sözleşme Tabanlı Tapu Kayıt Sistemi' (Yayınlanmamış Yüksek Lisans Tezi, Süleyman Demirel Üniversitesi 2019) 41.
[138] Numan Tekelioğlu, 'Dijital Tapu Sicili: Blokzinciri Teknolojisinin Tapu Sicilinde Kullanılmasına Dair Karşılaştırmalı Bir İnceleme' (2021) 80(1) İstanbul Hukuk Mecmuası, 1, 7-11.
[139] Kaynak için bkz. https://e-estonia.com/solutions/. Erişim Tarihi: 30.11.2023.
[140] Aslıhan Tüfekci ve Çetin Karahan, 'Blokzincir Teknolojisi ve Kamu Kurumlarınca Verilen Hizmetlerde Blokzincirin Kullanım Durumu' (2019) (4) Verimlilik Dergisi (T. C. Sanayi ve Teknoloji Bakanlığı Yayını) 169.
[141] Çağlayan Aksoy, 'Akıllı Sözleşmelerin Kuruluşu' (n 129) 63.
[142] Üstün (n 28) 55-56; Çubukçu (n 29) 36-38; Doğancı (n 27) 43; Elektronik kaynak için bkz. https://www.oracle.com/tr/blockchain/ Erişim Tarihi: 26.11.2023; Ezgi Elife Pilavcı, 'The Regulation of Smart Contracts: Law, Governance And Practice' Yayınlanmamış Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi 2019) 27-28.
[143] Delioğlan (n 25) 32-33.

fiziksel sensörlerden, uydu görüntülerinden, web API'lerinden ya da gerçek kişi ya da kurumlardan gerek duyduğu fiyat, hava durumu, istatistik gibi verileri çekebilir.[144]

Uçuş gecikmelerine ilişkin sigorta sözleşmesinin akıllı sözleşmeler üzerinden yapıldığı örnekte; akıllı sözleşmenin tetiklenmesi ve teminat bedelinin müşteriye ödenmesi için, akıllı sözleşmeye uçuşta rötar olup olmadığı ve olduysa kaç saat gecikme yaşandığı bilgisinin alınması gerekir. Ancak bu veri sisteme girildiği takdirde, önceden belirlenen şartları sağlıyorsa doğrultusunda ödeme gerçekleştirilir. Günümüzde internet üzerinden tüm uçuş bilgilerine, uçakların canlı konumlarına ve rötar durumuna dair bilgilere kolaylıkla ulaşılabilmektedir. Bu durumda, söz gelimi sigortalanan uçuşta 2 saat gecikme olduğu verisi, internet sitesinden çekilip harici veri sağlayıcı ile akıllı sözleşmeye iletildiğinde, akıllı sözleşme tetiklenir ve poliçe hükümleri uyarınca önceden belirlenen bedel müşterinin hesabına aktarılır. Ayrıca veri sağlayıcılarından, akıllı sözleşmelerin bir diğer kullanım alanı olan tedarik zinciri yönetiminde de yararlanılabilir. Nitekim tedarik zincirine ilişkin taraflar arasında bir sözleşme akdedildiğinde, ifanın doğru ve gerektiği gibi gerçekleşip gerçekleşmediğinin kontrolü amacıyla; ürünün doğru miktarda gönderilip gönderilmediği, doğru ısıda muhafaza edilip edilmediği, teslimin süresinde yapılıp yapılmadığı, gecikme halinde ödenecek cezai şart tutarı gibi hususların bilinmesi gerekir. Blokzincir üzerine kaydedilen bir tedarik zinciri uygulamasında, yapılan tüm işlemler eş zamanlı olarak takip edilebilecektir. Tüm bu aşamalarda ise oracle adı verilen dış veri sağlayıcılarına ihtiyaç duyulmaktadır. Teslimat gerektiği gibi yapıldığı takdirde, para transferi de gerçekleştirilir. Aynı şekilde teslimatta gecikme olması halinde de bu bilgi sisteme aktarılır, şayet sözleşme şartlarında bulunuyorsa bu durumda gecikmeden kaynaklı cezai şart miktarı da doğrudan alıcının hesabına aktarılabilir.

Ayrıca akıllı sözleşmelerdeki değişmezlik unsuruna bir çare olarak da harici veri sağlayıcılarından yararlanılabilir. Keza harici veri sağlayıcıları ile mahkemeler ya da hakem kurullarından alınan bilgiler de akıllı sözleşmenin işleyişini etkileyebilir.[145]

Özetle, dış kaynaktan alınan verilerin akıllı sözleşmeye aktarılması sayesinde, akıllı sözleşmelerin kullanım alanı da ciddi ölçüde artmaktadır. Uluslararası ticaret, sigorta, tedarik zinciri ve daha pek çok alanda veri sağlayıcıları vasıtasıyla akıllı sözleşmelerin uygulanması mümkün hale gelir. Fakat akıllı sözleşmelerin dış kaynaktan aldığı veri doğrultusunda çalışması, beraberinde birtakım riskleri de getirmektedir. Bunların başında veri girişinin hatalı olma riski bulunmaktadır. Dış dünya ile bir köprü görevi gören veri sağlayıcılarının siber saldırılara uğrama riski de mevcuttur. Ayrıca veri sağlayıcılarının manipüle edilmesi *(oracle manipulation)* riski de vardır. Bu durumda saldırganlar, girdileri hatalı verilerle

[144] Kaynak için bkz. https://chain.link/education/blockchain-oracles. Erişim Tarihi: 30.11.2023.

[145] Aybüke Uzunpınar Tüfek (n 127) Elektronik kaynak için bkz. https://akillisozlesmeler.bilkent.edu.tr/2023/12/akilli-sozlesmelerde-esneklik-ihtiyaci-akilli-sozlesmelerin-degistirilmesi-ve-sona-ermesi/. Erişim Tarihi: 26.01.2023; Çağlayan Aksoy, 'Akıllı Sözleşmelerin Kuruluşu' (n 129) 64.

değiştirip, kendi lehine olacak şekilde akıllı sözleşmelerin yürütülmesine sebebiyet verebilir.[146]

D. Akıllı Sözleşmelerin Veri Güvenliği Çerçevesinde İncelenmesi

Teknolojinin inanılmaz bir hızla gelişmesi nedeniyle hayatımıza akıllı sözleşmeler gibi kavramlar girmekte, beraberinde de pek çok tartışmayı getirmektedir. Elbette ki bu gibi yeni teknolojilerin faydaları olduğu gibi riskleri de vardır.

Veri; bilginin işlenmemiş, ham halidir. Diğer bir ifadeyle bilgi; verilerin anlamlandırılması suretiyle ortaya çıkan değerdir. Bilgi güvenliği ise temel olarak; gizlilik, bütünlük ve erişilebilirlik unsurlarının bir bütün halinde sağlanması halinde söz konusu olur.[147] Yine güvenliğin temini için; kimlik doğrulama, inkâr edememe, erişim denetimi, güvenilirlik gibi diğer hususların da sağlanmış olması gerekir.[148] Akıllı sözleşmeler bakımından güvenlik ise; akıllı sözleşmeler oluşturulurken veya yürürlüğü sırasında kullanılan güvenlik prensipleri ve uygulamalarıdır.[149]

Genel anlamda blokzincir teknolojisi ve bu teknolojiden dallanan Ethereum ağında düzenlenen akıllı sözleşmeler ile güvensiz güven ortamı yaratılmak istenmiştir. Gerçekten de blokzincir tabanlı uygulamalarda; kriptografi, dağıtık ağ yapısı, özet değer ve sair pek çok girift mekanizma, sistemin güvenliğini sağlamak için bir araya getirilmiştir. Fakat sistem açıklarını bulmaya odaklanan karşı teknolojilerin de bir o kadar sofistike ve karmaşık olabileceği göz ardı edilmemelidir. Blokzincir teknolojisi, son derece güvenli bir sistem sunmaktadır. Fakat bu özellik, siber saldırı riskinin tamamen ortadan kalktığını göstermeyecektir. Nasıl ki internet ortamında güvenlik açıkları olan sitelerin siber saldırılara maruz kalması ve çökertilmesi mümkünse, akıllı sözleşmeler de bu siber saldırılardan etkilenecek kod hatalarını veya güvenlik açıklarını barındırıyor olabilir. Sistemin kendisinin güvenli oluşu, sistem üzerinde çalıştırılan her akıllı sözleşmenin de siber güvenlik tehditlerine kapalı olduğunu göstermemektedir. Aslında bu güvenlik açıkları, sistemin doğrudan kendisinin güvenli olmadığı sonucunu doğurmamakta, akıllı sözleşmenin kodlanmasından kaynaklı hatalar olarak ortaya çıkmaktadır.

Akıllı sözleşmelerdeki her güvenlik zafiyeti Ethereum altyapısına mal edilemese de söz konusu kod hataları ya da güvenlik açıkları ciddi kayıplara yol açabilmektedir. Örneğin; 2016 yılında bir internet korsanı, Ethereum üzerinde akıllı sözleşme ile inşa edilen ve tarihin en büyük kitle fonlaması olan Decentralized Autonomous Organization (DAO) adlı topluluktan başka hesaba para aktarılmasına izin veren kod tabanlı bir güvenlik açığı bulmuştur. Akıllı

[146] Kaynak için bkz.https://www.immunebytes.com/blog/what-are-oracle-manipulation-attacks-in-blockchain/. Erişim Tarihi: 26.01.2023; Kaynak için bkz. https://coinmarketcap.com/academy/glossary/oracle-manipulation. Erişim Tarihi: 26.01.2023

[147] Gürol Canbek ve Şeref Sağıroğlu, 'Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme' (2006) 9(3) Politeknik Dergisi 165, 170.

[148] ibid 170.

[149] Kaynak için bkz. <https://hedera.com/learning/smart-contracts/smart-contract-security> Erişim Tarihi: 26.11.2023.

sözleşmedeki bu kodlama hatasından yararlanarak gerçekleştirdiği siber saldırı ile yaklaşık 50 milyon Amerikan dolarına eşdeğer tutarda olan 3.6 milyon Ether'i çalmayı başarmıştır.[150] Bu siber saldırıya karşı Vitalik Buterin tarafından 'hard fork' adı verilen çatallaşma önerisi sunulmuştur. Bu hamle de blokzincirin değişmezlik özelliğini etkilemesi nedeniyle tartışma yaratmıştır. DAO siber saldırısı olayının, Ethereum blokzincirinde de büyük bir etki yarattığı söylenebilir. Kimilerine göre yaşanan bu olay; Ethereum'un bugünkü halini almasına ve akıllı sözleşmelerdeki güvenlik açığı sorununa odaklanılmasına yol açmıştır. Sonrasında akıllı sözleşmelere dair teknik denetim standardizasyonları da geliştirilmiştir. [151] Ayrıca CyberNews tarafından yapılan bir araştırmada, Ethereum platformundaki yaklaşık 3.800 akıllı sözleşmede güvenlik açığı bulunduğu ve bunlara "saatli bomba" dendiği de tespit edilmiştir.[152]

Akıllı sözleşmeler vasıtasıyla çok büyük miktarda veri ve varlık kontrol edilebilmekte, blokzincir tabanlı proje ve uygulamalarda yüksek miktarda para sirkülasyonu gerçekleştirilmektedir. Dolayısıyla her geçen gün gelişmekte olan bu yeni, dijital ekosistem içerisinde potansiyel saldırı riski de artmaktadır. Bu da varlıkların çalınmasının yanı sıra sistemin tamamına karşı güven kaybına da yol açar.[153] Değiştirilemez yapısı ile ön plana çıkan bu sistem içerisinde, güvenli bir akıllı sözleşmeye yönelik atılacak ilk adım ise; kodun kendisidir.[154] Bu nedenle geliştiricilerin bazı temel akıllı sözleşme prensiplerini anlaması ve uygulaması son derece önemlidir. Siber saldırı riskinin tamamen biteceği söylenemediğinden; geliştiricilerin akıllı sözleşmelerin kodlanması aşamasında birtakım önlemleri alması, teknik olarak sağlam ve güvenilir akıllı sözleşmeler oluşturmak için çaba göstermeleri gerekmektedir. Daha önce de bahsedildiği üzere, akıllı sözleşmelerdeki hataların tespiti ve güvenlik açıklarının önlenmesi adına yapay zekâ teknolojilerinden de yararlanılabilir.

1. Gizlilik Unsuru Bakımından Değerlendirilmesi

Gizlilik, veriye yalnızca yetkili kişiler tarafından ulaşılabilmesi anlamına gelmektedir.[155] Akıllı sözleşmelerin blokzincir tabanlı yapısı sayesinde; kullanıcılara biri genel biri özel olmak üzere iki anahtar atandığından bahsedilmiştir. Bu anahtarlar sayesinde; her kullanıcıya tıpkı

[150] Çubukçu (n 29) 53; Kaynak için bkz. https://www.gemini.com/tr-TR/cryptopedia/the-dao-hack-makerdao#section-the-dao-hack-remedy-forks-ethereum. Erişim Tarihi: 26.01.2024.

[151] Kaynak için bkz. https://www.coindesk.com/consensus-magazine/2023/05/09/coindesk-turns-10-how-the-dao-hack-changed-ethereum-and-crypto/ Erişim Tarihi: 26.01.2024; Kaynak için bkz. https://medium.com/@iublocktech/ethereum-ve-dao-hack-daba3f215205 Erişim Tarihi: 26.01.2024; Kaynak için bkz. https://www.gemini.com/tr-TR/cryptopedia/the-dao-hack-makerdao#section-the-dao-hack-remedy-forks-ethereum. Erişim Tarihi: 26.01.2024.

[152] Elektronik kaynak için bkz. https://www.forbes.com/sites/davidbirch/2021/09/04/theyre-not-smart-and-theyre-not-contacts/?sh=1d983ad6397e Erişim Tarihi: 26.11.2023.

[153] Elektronik kaynak için bkz. https://101blockchains.com/smart-contract-security-guide Erişim Tarihi: 26.11.2023.

[154] Elektronik kaynak için bkz. https://www.alchemy.com/overviews/smart-contract-security-best-practices Erişim Tarihi: 26.11.2023.

[155] Canbek ve Sağıroğlu (n 152) 170.

vatandaşlık numarası gibi sanal kimlikler atanır.[156] Ayrıca akıllı sözleşmeler ile aracılara ihtiyaç olmaksızın eşten eşe işlem yapılabilmesi de yetkisiz erişim riskini azaltır. Bu minvalde, blokzincirde gizlilik özelliğinin yüksek olduğu söylenebilir.

2. Bütünlük Unsuru Bakımından Değerlendirilmesi

Bütünlük; verinin her türlü müdahaleden korunması, boyutlarında veya içeriğinde değişiklik yapılmaması, silinmemesi, herhangi bir değişikliğe uğramadan korunabilmesi anlamına gelmektedir.[157] Akıllı sözleşmelerin blokzincir tabanlı yapısı; bütünlük unsurunu sağlamaktadır. Çünkü kural olarak bir kez zaman damgasıyla sisteme kaydedilen veri; artık hiç kimse tarafından geriye dönük olarak değiştirilemez veya yok edilemez.[158] Ayrıca blokzincirin dağıtık bir hesap defteri teknolojisi olması nedeniyle, işlem geçmişinin kopyaları her bir düğümde tutulmakta, yedeklenmektedir. Blokzincir sisteminde yapılan her işlemin kriptografik olarak şifrelenerek zaman damgası ile kayıt altına alınması ve özet değerleri sayesinde birbirine bağlı bloklarda muhafaza edilmesi işlem güvenliğini sağlamaktadır. Yine blokzincir üzerinde kayıtlı tüm işlem trafiğinin düğümler tarafından geriye dönük olarak izlenebiliyor olması da sistemin şeffaflığını sağlamaktadır. Tüm bu özellikleri sayesinde blokzincirin değişikliğe dirençli *(tamper-proof)* bir yapı sunduğu kabul edilmektedir.[159] Sonuç olarak; akıllı sözleşmelerde veri güvenliği bakımından bütünlük unsurunun birçok mekanizma sayesinde sağlandığı söylenebilir.

3. Erişilebilirlik Unsuru Bakımından Değerlendirilmesi

Erişilebilirlik; verinin yetkili kimselerce istenildiği anda ulaşılabilir olması anlamına gelmektedir.[160] Akıllı sözleşmelerin çalıştırılmasında ilk olarak Ethereum platformunun kullandığını, Ethereum platformunun altında yatan teknolojinin de blokzincir teknolojisi olduğundan bahsedilmiştir. Dolayısıyla sistemin kendisinin bir siber saldırıyla çökertilmesi, sisteme erişimin engellenmesi pratikte neredeyse imkânsız bir senaryonun gerçekleşmesine bağlıdır. Daha önce de ifade edildiği üzere, blokzincirin dağıtık ağ yapısı sayesinde merkezi sistemlere nazaran verilerin değiştirilmesi, manipüle edilmesi ya da tahrip edilmesi bakımından çok daha güçlü bir koruma sağlamaktadır. Keza merkezi yapılarda, hizmet reddi saldırılarına maruz kalınması halinde, tek bir kritik merkez bulunduğu için ağ trafiğinin arttırılması ve yetkili kişilerce sisteme girişin engellenmesi daha olasıdır. Fakat blokzincirin dağıtık ağ yapısı, bir defter teknolojisi olması ve kullanılan mutabakat mekanizmaları sayesinde birkaç düğümün çevrimdışı olması sağlansa dahi sistem çalışmaya devam eder ve herhangi bir veri kaybı yaşanmaz.[161] Neticeten sistemin sürdürülebilirliği, tek bir kritik

[156] Üstün (n 28) 28.
[157] Canbek ve Sağıroğlu (n 46) 170.
[158] Çubukçu (n 29) 14.
[159] Çekin (n 42) 321-322; Aslan ve Kasapbaşı (n 32) 46-47; Çubukçu (n 29) 33,34,44-45.
[160] ibid 170.
[161] Şafak, Arslan, Gözütok ve Köprülü (n 29) 37; Nevzat Özcandan, Öznur Kalkar, Muhammed Ali Bingöl ve diğerleri, 'Blokzincirlerde Güvenlik ve Mahremiyet' (Bankalararası Kart Merkezi, Nisan 2020) 18 Elektronik kaynak için bkz. https://bkm.com.tr/wp-content/uploads/2015/06/blokzincirlerde_guvenlik_ve_mahremiyet.pdf Erişim

noktanın güvenliğine bağlı değildir. Dolayısıyla ağ katılımcıları diledikleri zaman sisteme giriş yapabilir, işlemlerini gerçekleştirebilir veya yapılan diğer işlemleri kontrol edilebilir. Bununla birlikte belirtmek gerekir ki, kişilere atanan özel anahtarın kaybedilmesi gibi bireysel erişilebilirlik sorunları yaşanması mümkündür.[162] Genel çerçevede ise blokzincir, erişilebilirlik unsuru bakımından güçlü bir yapı sunmaktadır.

SONUÇ VE DEĞERLENDİRMELERİMİZ

Blokzincir ve blokzincire dayalı akıllı sözleşmeler, bünyesinde taşıdıkları multidisipliner mekanizmalar sayesinde, sözleşme süreçlerinde ve işlemlerde güven unsurunu bir zorunluluk olmaktan çıkartmaktadır. Blokzincir ve akıllı sözleşmeler, dijital dönüşüm yolunda devrim niteliği taşıyan inovasyonlardır. Dijital dönüşüm ise, günümüzde adeta kaçınılmaz hale gelmiştir. Bu teknolojiler ise başlı başına sistemin güveni temin ettiği, daha az maliyetle, daha hızlı işlemlerin gerçekleştirilebildiği, ifanın garanti altına alındığı, dış müdahalelere kapalı, hemen hemen her sektörde kullanılabilir, alternatif bir çözüm yolu önermektedir.

Bu yeni ve her an gelişmeye devam eden teknolojilerin uygulama alanının artması ile birtakım sorunlar da gün yüzüne çıkmıştır. Teknik açıdan bu sorunlar; akıllı sözleşmelerin kuruluşu aşamasında oluşabilecek kod kaynaklı hatalar ve güvenlik açıkları olabilir. Hukuki açıdan ise; kendiliğinden ifa ve değişmezlik özellikleri nedeniyle hükümsüz bir sözleşmenin ifasının durdurulamaması ya da tarafların uyarlama, değişiklik, fesih gibi taleplerine cevap verilememesi olarak karşımıza çıkabilir. Bu sorunların önlenmesi için, sözleşmenin kuruluşu aşamasında, ex-ante tedbirlerin alınması son derece önemlidir. Potansiyel sorunların çözümü için her geçen gün yeni çareler üretilmektedir. Özellikle yapay zekâ teknolojileri, akıllı sözleşmelerdeki hataların ve güvenlik açıklarının en baştan tespiti ve engellenmesi adına son derece faydalı olabilir. Fikrimizce bu teknolojilere esas değerini katan, kendiliğinden ifa veya değişmezlik gibi temel prensiplerinden feragat edilmeksizin, uyumu sağlamak adına teknik çareler geliştirilmesi daha doğru bir yaklaşım olur.

Akıllı sözleşmeler, sözleşme süreçlerinin bir kısmına ya da tamamına katılabileceği gibi sözleşmesel bir ilişki barındırmıyor, yalnızca işlemsel bir otomasyon sağlamak için kullanılıyor da olabilir. Her ihtimalde yapılmak istenen işlemin icrası, önceden belirlenen şartlara göre, kendiliğinden gerçekleşir. Dolayısıyla akıllı sözleşmelerin yasal zeminde bir sözleşme niteliğine haiz olup olmadığının tespiti için önce somut olay nezdinde bir değerlendirme yapılması gerekir. Akabinde uygulanacak hukukun tespiti ve bu hukuk kuralları uyarınca gerekli şartları taşıyıp taşımadığının incelenmesi gerekir. Akıllı sözleşmeler de Türk Borçlar Kanunu'na tabidir ve borçlar hukuku uyarınca gerekli şartları taşıyan bir akıllı sözleşmenin hukuken geçerli ve bağlayıcı olduğunun kabulü gerekmektedir.

Tarihi: 26.01.2024; Kaynak için bkz. <https://www.beyaz.net/tr/guvenlik/makaleler/dos_ve_ddos_nedir.html.> Erişim Tarihi:26.01.2024.

[162] Üstün (n 28) 54-56.

Günümüzde Avrupa Birliği kurumları başta olmak üzere, dijital dünyanın risklerini en aza indirmek adına önemli regülasyon çalışmaları yürütülmektedir. Her ne kadar üçüncü taraf ve kişilere duyulan ihtiyacın ortadan kalkması, blokzincirin temel vaatlerinden olsa da bu teknolojilerin tıpkı internet gibi hayatımızın vazgeçilmez bir parçası haline gelmesi için uzun bir yol olduğunu söylemek mümkündür. Blokzincir ve akıllı sözleşmeler adeta hukuk ve teknolojinin kesişim noktasındadır. Bu nedenle konunun teknik ve hukuki boyutunun birlikte değerlendirilmesi gerekmektedir. Bu süreçte de gri alanların düzenlenmesinde, yazılımcılar ve hukukçuların iş birliği halinde çalışmasının önem arz edeceğini söylemek mümkündür.

Sonuç olarak blokzincir teknolojisi ve akıllı sözleşmeler, dijital dünyanın taşıdığı riskleri bünyesinde barındırmakla birlikte, hayatımızı önemli derecede etkileyebilecek bir potansiyele sahiptir. Akıllı sözleşmeler konusunda gerekli hukuki ve teknik çalışmaların yapılması, özellikle de yapay zekâ, nesnelerin interneti gibi teknolojilerle desteklenmesi halinde; uluslararası ticaret ve finans sektörü başta olmak üzere, tapu, sigorta, fikir ve sanat eserleri gibi pek çok alanda gerçek bir dijital dönüşüm yaratmaya aday olduğu; veri odaklı yeni dijital toplum düzeninin vazgeçilmez bir parçası olabileceği söylenebilir.

KAYNAKÇA

Anderson RJ, 'The Eternity Service' (1996) Cambridge University Computer Laboratory

Aslan M ve Kasapbaşı MC, 'Blok Zinciri Platformları, Fikir Birliği Mekanizmaları ve Ağın Güvenlik Analizi' (2022) 5(1) Haliç Üniversitesi Fen Bilimleri Dergisi 43-72

Başar MO, 'Akıllı Sözleşmeler ve Özel Hukuk Uygulamasında Ortaya Çıkması Muhtemel Sorunlar' (2022) 80 (4) İstanbul Hukuk Mecmuası 1067 – 1103

Bilgili F ve Cengil F, *Blockchain ve Kripto Para Hukuku* (2. Baskı, Dora Basım-Yayın 2022)

—— 'Bitcoin Özelinde Kripto Paraların Ticaret Şirketlerine Sermaye Olarak Getirilmesi' (2019) 22(3) Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi 3, 23

Blockchain Türkiye, 'Akıllı Sözleşme Raporu', (Blockchain Türkiye, Temmuz 2021)

Buterin V, 'A Next Generation Smart Contract & Decentralized Application Platform' (2015)

Caria RD, 'Law and Autonomous Systems Series: Defining Smart Contracts- The Search for Workable Legal Categories' (Oxford Business Law Blog, 25 Mayıs 2018)

Chaudhry N ve Yousaf MM, 'Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities' (2018) 12th International Conference on Open Source Systems and Technologies (ICOSST) 54-63

Chaum DL, 'Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms' (1981) 24(2) Communications of the ACM 84-88

—— 'Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups' (1982)

—— ' Blind Signatures for Untraceable Payments' in Chaum, D., Rivest, R.L., Sherman, A.T. (eds) Advances in Cryptology. (Springer, Boston, MA 1983)

Çağlayan Aksoy P, *Akıllı Sözleşmelerin Kuruluşu ve Geçerlilik Şartları* (2. Baskı, On İki Levha 2021)

—— 'Akıllı Sözleşmelerin Dünü, Bugünü ve Yarını: Karşılaştırmalı Bir Değerlendirme' (2022) 42(494) Vergi Dünyası 17-38

—— 'Akıllı Sözleşmeler: Temel Hukuki Problemler ve Regülasyon' (Hukuk ve Bilişim Dergisi, 26 Mart 2023)

—— 'Yapay Zekadan Yararlanan Akıllı Sözleşmeler' (Arksigner, 30 Ekim 2023)

—— 'Dijital Sözleşmelerin Yeni Yüzü Akıllı Sözleşmeler' (Arksigner, 30 Mart 2023)

Çekin MS, 'Borçlar Hukuku ile Veri Koruma Hukuku Açısından Blockchain Teknolojisi ve Akıllı Sözleşmeler: Hukuk Düzenimizde Bir Paradigma Değişimine Gerek Var Mı' (2019) 77(1) İstanbul Hukuk Mecmuası 315-341

Çubukçu DB, *Teknik ve Hukuki Yönleriyle Akıllı Sözleşmeler (*1.Bası, Yetkin 2021)

Delioğlan S, 'Akıllı Sözleşmeler' (Yayınlanmamış Yüksek Lisans Tezi, Özyeğin Üniversitesi 2023)

Doğancı DE, *Blokzincirine Dayalı Akıllı Sözleşmelerin Hukuki Nitelikleri, Kuruluşu, Yorumu, İfası ve Bazı Örnek Hukuki Uygulamalar* (1. Bası, On İki Levha 2021)

Dulupçu MA, Yiyit M ve Genç AG, 'Dijital Ekonominin Yükselen Yüzü: Bitcoin'in Değeri ile Bilinirliği Arasındaki İlişkinin Analizi' 2017 22(15) Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi 2241- 2259

Fauzı MA, Paiman N and Othman Z, 'Bitcoin and Cryptocurrency: Challenges, Opportunities and Future Works' (2020) 7(8) Journal of Asian Finance, Economics and Business, 695–704

Gürol Canbek ve Şeref Sağıroğlu, 'Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme' (2006) 9(3) Politeknik Dergisi 165-174

Güven Taştan F, 'AB, Akıllı Sözleşmeleri Düzenlemenin Eşiğinde: Veri Kanunu Teklifi, Parlamento'dan Geçti' (Akıllı Sözleşmeler Bilkent, 27 Mart 2023)

Haber S ve Stornetta WS, 'How to Time-Stamp a Digital Document' (1991) 3(2) Journal of Cryptology 99-111

İşler B, Mustafa Takaoğlu ve Ufuk Fatih Küçükali, 'Blokzinciri Ve Kripto Paraların İnsanlığa Etkileri' (2019) 3(2) Yeni Medya Elektronik Dergisi 71 – 83

Kargar P, 'Akıllı Sözleşme Tabanlı Tapu Kayıt Sistemi' (Yayınlanmamış Yüksek Lisans Tezi, Süleyman Demirel Üniversitesi 2019)

Kınacı M, 'Blockchain Teknolojisi ve Akıllı Sözleşmelerin Yaygınlaşmasının Önündeki Engeller' (Yayınlanmamış Yüksek Lisans Tezi, Bahçeşehir Üniversitesi 2019)

Krichen M, 'Strengthening the Security of Smart Contracts through the Power of Artificial Intelligence' (2023) 12(5) Computers 107

Levi SD, Lipton AB ve diğerleri, 'An Introduction to Smart Contracts and Their Potential and Inherent Limitations' (Harvard Law School Forum on Corporate Governance 26 Mayıs 2018)

Liu H, Liu H, Luo X ve Xia X, 'Merkle Tree: A Fundamental Component of Blockchains' (2021) 2021 International Conference on Electronic Information Engineering and Computer Science (EIECS) 556-561

Mendi AF, 'Blokzincir Mimarisi ve Getirdiği Fırsatlar' (2021) 29 Avrupa Bilim ve Teknoloji Dergisi 181- 186

——ve Çabuk A, 'Bitcoin'in Arkasındaki Güç: Blockchain' (2018) 1(1), GSI Journals Serie C: Advancements In Information Sciences And Technologies 12-2

Nakamoto S, 'Bitcoin: A Peer-to-Peer Electronic Cash System', (Bitcoin, 2008)

Öz NŞ, 'Blokzinciri Teknolojisinin, Akıllı Sözleşmeler ve Kripto Paraların Karşılaştırmalı Hukuk Bakımından Değerlendirilmesi' (Yayınlanmamış Yüksek Lisans Tezi, Bahçeşehir Üniversitesi 2022)

Özcandan N, Kalkar Ö, Bingöl MA ve diğerleri, 'Blokzincirlerde Güvenlik ve Mahremiyet' (Bankalararası Kart Merkezi, Nisan 2020)

Özer YM, *Kişisel Verilerin Korunmasında Blokzincir Modeli: Vaatler ve Hukuki Engeller* (1.Baskı, On İki Levha 2020)

Özkan Z, 'Akreditifte Blokzinciri ve Akıllı Sözleşmelerin Uygulanabilirliğinin Hukuki Açıdan Değerlendirilmesi' (Yayınlanmamış Yüksek Lisans Tezi, Galatasaray Üniversitesi 2022)

Özyürek H, 'Blockchaın Teknolojisinin Mevcut ve Muhtemel Kullanım Alanları' (2021) 22(4) Anadolu Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi 31-50

Pilavcı EE, 'The Regulation of Smart Contracts: Law, Governance And Practice' Yayınlanmamış Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi 2019)

Sadioğlu FC, 'Borçlar Hukuku Çerçevesinde Akıllı Sözleşmenin İşlevleri ve İşlevlerin Yerine Getirilmesi Sırasında Karşılaşılan Sorunlar' (2021) 25(4) Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi, 171–216

Schneier B ve Kelsey J, 'Cryptographic Support for Secure Logs on Untrusted Machines' (1998) The Seventh USENIX Security Symposium Proceedings, USENIX Press 53–62

Sherman AT, Javani F, Zhang H, ve Golaszewsk E, 'On the Origins and Variations of Blockchain Technologies' (2019) 17(1) IEEE Security & Privacy 72-77

Stazi A, 'Smart Contracts and Comparative Law, A Western Perspective' (Springer Cham, 2022)

Stuart D. Levi, Alex B. Lipton ve diğerleri, 'An Introduction to Smart Contracts and Their Potential and Inherent Limitations' (Harvard Law School Forum on Corporate Governance 26 Mayıs 2018)

Subramanian R ve Chino T 'The State of Cryptocurrencies, Their Issues and Policy Interactions' (2015) 24(3) Journal of International Technology and Information Management 25-40

Szabo N, 'Formalizing and Securing Relationships on Public Networks' (1997) 2(9) First Monda

Şafak E, Arslan Ç, Gözütok M ve Köprülü T, 'Dağıtık Defter Teknolojileri ve Uygulama Alanları Üzerine Bir İnceleme' (2021) 29 Avrupa Bilim ve Teknoloji Dergisi 36-45

Taş O ve Kiani F, 'Blok Zinciri Teknolojisine Yapılan Saldırılar Üzerine bir İnceleme' (2018) 11(4) Bilişim Teknolojileri Dergisi 369–382

Taştan FG, 'AB, Akıllı Sözleşmeleri Düzenlemenin Eşiğinde: Veri Kanunu Teklifi, Parlamento'dan Geçti' (Akıllı Sözleşmeler Bilkent, 27 Mart 2023)

Tekelioğlu N, 'Dijital Tapu Sicili: Blokzinciri Teknolojisinin Tapu Sicilinde Kullanılmasına Dair Karşılaştırmalı Bir İnceleme' (2021) 80(1) İstanbul Hukuk Mecmuası, 1 – 39

Tevetoğlu M, 'Ethereum ve Akıllı Sözleşmeler' (2021) 12(1) İnönü Üniversitesi Hukuk Fakültesi Dergisi, 193–208

Tunca S ve Sezen B, 'Sigorta İşlemlerinde Blokzincir (Blockchain) Teknolojisi Uygulamaları' (2020) (14) Bankacılık ve Sigortacılık Araştırmaları Dergisi 13 – 25

Tüfekci A ve Karahan Ç, 'Blokzincir Teknolojisi ve Kamu Kurumlarınca Verilen Hizmetlerde Blokzincirin Kullanım Durumu' (2019) (4) Verimlilik Dergisi (T. C. Sanayi ve Teknoloji Bakanlığı Yayını) 157–193

Türk Borçlar Kanunu, Kanun Numarası: 6089, Kabul Tarihi: 11.01.2011, RG 04.02.2011/27836

Usta A ve Doğantekin S, 'Blockchain 101' (Bankalararası Kart Merkezi, 30 Nisan 2018)

Uzunpınar Tüfek A, 'Akıllı Sözleşmelerde Esneklik İhtiyacı: Akıllı Sözleşmelerin Değiştirilmesi ve Sona Ermesi' (Akıllı Sözleşmeler Bilkent, 25 Kasım 2023)

Ünal G ve Uluyol Ç, 'Blok Zinciri Teknolojisi' (2020) 13(2) Bilişim Teknolojileri Dergisi 167–175

Üstün ES, *TBK Kapsamında Geleneksel Sözleşmeler ile Mukayeseli Olarak Akıllı Sözleşmeler Blokzincir Teknolojisi* (1. Bası, Seçkin 2021)

Yıldırım AN, 'Türk Borçlar Hukuku Bakımından 'Akıllı Sözleşmeler'' (Yayınlanmamış Yüksek Lisans Tezi, Koç Üniversitesi 2022)

Walch OA, 'The Path of the Blockchain Lexicon (and the Law)' (2017) Review Banking & Financial Law 713- 765

Watanabe H, Fujimura S ve diğerleri "Blockchain Contract: A Complete Consensus Using Blockchain" (2015) IEEE 4th Global Conference on Consumer Electronics (GCCE) 577-578

Avrupa Birliği Kaynakları:

Commission, 'Proposal For A Regulation Of The European Parliament and of the Council On Harmonised Rules on Fair Access to and Use Of Data (Data Act)' Com (2022) 68 Final, Ch I, Art 2

European Parliament, 'Amendments adopted by the European Parliament on 14 March 2023 on the proposal for a regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)' 2022/0047(COD)

Regulation of the European Parliament and of the Council on Harmonised Rules On Fair Access to and Use Of Data and Amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act)

Avrupa Hukuk Enstitüsü, 'Blokzincir Teknolojisi, Akıllı Sözleşmeler ve Tüketicinin Korunması Hakkında ELI İlkeleri' Raporu; <https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_Blockchain_Technology__Smart_Contracts_and_Consumer_Protection.pdf.>

Raporun çevirisi; <https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/Blokzinciri_Teknolojisi__Akilli_So__zles__meler_ve_Tu__keticinin_Korunmasi_Hakkinda_ELI_I__lkeleri_-_Avrupa_Hukuk_Enstitu__su___Raporu_-_Nesli_S__en_O__zc__elik_O__zer.pdf.> Erişim Tarihi: 26.01.2024.

EU Blockchain Observatory and Forum, 'Smart Contracts' Raporu için bkz. <https://www.eublockchainforum.eu/sites/default/files/reports/SmartContractsReport_Final.pdf>Erişim Tarihi: 26.01.2026.

Elektronik Kaynaklar:

https://bkm.com.tr/wp-content/uploads/2015/06/blokzincirlerde_guvenlik_ve_mahremiyet.pdf Erişim Tarihi: 26.01.2024; Kaynak için bkz. <https://www.beyaz.net/tr/guvenlik/makaleler/dos_ve_ddos_nedir.html.> Erişim Tarihi:26.01.2024

https://hedera.com/learning/smart-contracts/smart-contract-security. Erişim Tarihi: 26.11.2023

https://www.gemini.com/tr-TR/cryptopedia/the-dao-hack-makerdao#section-the-dao-hack-remedy-forks-ethereum. Erişim Tarihi: 26.01.2024.

https://www.coindesk.com/consensus-magazine/2023/05/09/coindesk-turns-10-how-the-dao-hack-changed-ethereum-and-crypto/ Erişim Tarihi: 26.01.2024

https://medium.com/@iublocktech/ethereum-ve-dao-hack-daba3f215205 Erişim Tarihi: 26.01.2024.

https://www.gemini.com/tr-TR/cryptopedia/the-dao-hack-makerdao#section-the-dao-hack-remedy-forks-ethereum. Erişim Tarihi: 26.01.2024

https://www.forbes.com/sites/davidbirch/2021/09/04/theyre-not-smart-and-theyre-not-contacts/?sh=1d983ad6397e. Erişim Tarihi: 26.11.2023

https://101blockchains.com/smart-contract-security-guide Erişim Tarihi: 26.11.2023

https://www.alchemy.com/overviews/smart-contract-security-best-practices Erişim Tarihi: 26.11.2023

https://www.immunebytes.com/blog/what-are-oracle-manipulation-attacks-in-blockchain/. Erişim Tarihi: 26.01.2023

https://coinmarketcap.com/academy/glossary/oracle-manipulation. Erişim Tarihi: 26.01.2023

https://chain.link/education/blockchain-oracles. Erişim Tarihi: 30.11.2023

https://www.oracle.com/tr/blockchain/ Erişim Tarihi: 26.11.2023

https://bkm.com.tr/wp-content/uploads/2019/08/15082019_kitap.pdf. Erişim Tarihi: 30.11.2023

https://e-estonia.com/solutions/. Erişim Tarihi: 30.11.2023

https://aws.amazon.com/tr/what-is/nlp/#:~:text=Do%C4%9Fal%20dil%20i%C5%9Fleme%20(NLP)%2C,ses%20ve%20metin%20verilerine%20sahiptir. Erişim Tarihi: 26.01.2024

https://blog.chain.link/upgradable-smart-contracts/. Erişim Tarihi: 26.01.2024

https://akillisozlesmeler.bilkent.edu.tr/2023/03/ab-akilli-sozlesmeleri-duzenlemenin-esiginde-veri-kanunu-parlamentoda-kabul-edildi/. Erişim Tarihi: 26.01.2024

https://blog.arksigner.com/blokzinciri-teknolojisi/yapay-zekadan-yararlanan-akilli-sozlesmeler. Erişim Tarihi: 26.01.2024

https://akillisozlesmeler.bilkent.edu.tr/2023/12/akilli-sozlesmelerde-esneklik-ihtiyaci-akilli-sozlesmelerin-degistirilmesi-ve-sona-ermesi/. Erişim Tarihi: 26.01.2023

https://www.investopedia.com/terms/s/smart-contracts.asp. Erişim Tarihi: 25.11.2023

https://www.nortonrosefulbright.com/en/inside-disputes/blog/202202-smart-legal-contracts-under-english-law-introduction#:~:text=Smart%20legal%20contracts%20are%20a,or%20partly%2C%20without%20human%20assistance. Erişim Tarihi: 25.01.2024

https://www.paymentsjournal.com/the-difference-between-a-smart-contract-and-a-smart-legal-contract-explained/ Erişim Tarihi: 25.01.2024

https://bctr.org/dokumanlar/Akilli_Sozlesme_Raporu.pdf.> Erişim Tarihi:26.01.2024

https://webrazzi.com/2017/10/06/axa-fizzy/. Erişim Tarihi: 26.01.2024

https://cbddo.gov.tr/sss/blokzincir-sozlugu/. Erişim Tarihi: 26.01.2024

https://www.hukukvebilisimdergisi.com/akilli-sozlesmeler-temel-hukuki-problemler-ve-regulasyon/ Erişim Tarihi:26.01.2024

https://bctr.org/dokumanlar/Akilli_Sozlesme_Raporu.pdf. Erişim Tarihi:26.01.2024

https://blogs.law.ox.ac.uk/business-law-blog/blog/2018/05/law-and-autonomous-systems-series-defining-smart-contracts-search. Erişim Tarihi:26.01.2024

https://hedera.com/learning/smart-contracts/smart-contract-use-cases Erişim Tarihi:26.01.2024

https://www.lawdistrict.com/legal-dictionary/smart-contracts. Erişim Tarihi:26.01.2024

https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/. Erişim Tarihi:26.01.2024

https://firstmonday.org/ojs/index.php/fm/article/view/548. Erişim Tarihi: 25.11.2023

https://ethereum.org/en/eth/> Erişim Tarihi: 25.11.2023

https://lorentlabs.com/ethereum-nedir-nasil-ortaya-cikmistir-ethereum-hakkinda-her-sey/> Erişim Tarihi: 25.11.2023

https://docs.soliditylang.org/en/v0.5.3/. Erişim Tarihi: 25.11.2023

https://docs.soliditylang.org/en/v0.5.3/. Erişim Tarihi: 25.11.2023

https://blog.arksigner.com/blokzinciri-teknolojisi/dijital-sozlesmelerin-yeni-yuzu-akilli-sozlesmeler. Erişim Tarihi: 26.01.2024

https://academy.binance.com/tr/articles/what-is-ethereum. Erişim Tarihi:26.01.2024

https://digicentralized.com/blockchainin-evrimi/.> Erişim Tarihi:26.01.2024

https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf. Erişim Tarihi: 25.11.2023

https://ethereum.org/en/whitepaper/ Erişim Tarihi: 25.11.2023

https://www.btcturk.com/bilgi-platformu/peer-to-peer-nedir-p2p-agi-nasil-calisir/. Erişim Tarihi: 26.01.2024

https://www.blockchain-council.org/blockchain/peer-to-peer-network/. Erişim Tarihi: 26.01.2024

https://bkm.com.tr/wp-content/uploads/2015/06/blokzincirlerde_guvenlik_ve_mahremiyet.pdf Erişim Tarihi: 26.01.2024

<https://www.beyaz.net/tr/guvenlik/makaleler/dos_ve_ddos_nedir.html.> Erişim Tarihi: 26.01.2024

https://kerteriz.net/modern-sifreleme-yontemleri-simetrik-asimetrik-sifreleme/. Erişim Tarihi: 26.01.2024

https://www.gemini.com/tr-TR/cryptopedia/public-private-keys-cryptography#section-what-is-a-private-key. Erişim Tarihi:26.01.2024

https://www.btcturk.com/bilgi-platformu/ethereum-2-0-the-merge/. Erişim Tarihi: 26.01.2024

https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp#:~:text=What%20Are%20the%20Types%20of,authority%2C%20and%20proof%20of%20capacity. Erişim Tarihi: 26.01.2024

https://www.btcturk.com/bilgi-platformu/bulut-madenciligi-cloud-mining-nedir-nasil-calisir/ Erişim Tarihi: 26.01.2024

https://www.geeksforgeeks.org/smart-contracts-and-iot/. Erişim Tarihi:26.01.2024

https://101blockchains.com/history-of-blockchain-timeline/ Erişim Tarihi: 25.01.2024