HUKUKÇULAR İÇİN BLOKZİNCİR TEKNOLOJİSİNİN TEKNİK İŞLEYİŞİ: BİTCOİN ÖRNEĞİ*

Öğr. Gör. Osman Gazi GÜÇLÜTÜRK**

GİRİŞ

Blokzincir Bitcoin ile anılan bir dağıtılmış kayıt tutma teknolojisidir (İng. *Distributed Ledger Technology,* "**DLT**")[1]. Öncelikle belirtilmelidir ki DLT ile blokzincir aynı şey değildir, blokzincir DLT'nin sadece bir örneğidir[2]. Blokzincir genel bir kavram olduğu ve her bir uygulamasının farklı özellikleri olabileceği için üzerinde uzlaşılmış bir tanımı bulunmamaktadır[3]. Bu kitabın ilerleyen bölümlerinde farklı hukuk dalları bakımından

---

* Bu çalışma yazarın 2018'de Birmingham Üniversitesinde yürüttüğü araştırmalar sonucunda hazırlamış olduğu ve 2019'da SSRN'de yayınlanan "Blockchain: A Trustless Network or a Technologically Disguised Shift of Trust?" başlıklı raporun kısaltılmış, kısmen güncellenmiş ve Türkçeye tercüme edilmiş halidir. Eserin aslı için bkz. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3440044 (Erişim Tarihi: 05.05.2021). Bu çalışmanın Türkçeye tercüme edilmesinde ve yayına hazırlanmasındaki destekleri için Stj. Av. Mehmet Yusuf Sert'e teşekkürlerimi sunarım.

** Kırklareli Üniversitesi Hukuk Fakültesi, Bilişim Hukuku Anabilim Dalı.

1 16.04.2021 tarih 31456 sayılı Resmi Gazete'de yayımlanan Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik m. 3'te bu kavramın Türkçe karşılığı olarak "*dağıtık defter teknolojisi*" ifadesi kullanılmıştır. Çalışmanın devamında bu teknolojiye atıf yaparken "DLT" kısaltması kullanılacaktır.

2 "Final Report", **Cryptoassets Taskforce**, 2018, s. 9; GÜÇLÜTÜRK Osman G., "Blokzincir Üzerinde Depolanan Verilerin Kişisel Veri Niteliği ve Silinemezlik, Yok Edilemezlik Sorunu", **Kişisel Verileri Koruma Dergisi**, C. 1, S. 2, 2019, s. 32.

3 Blokzincir kavramına ilişkin açıklamalar için bkz. bu kitabın "Blokzincir ve Regüle Edilebilirlik" başlıklı bölümü. Ayrıca bkz. AKSOY ÇAĞLAYAN Pınar, **Akıllı Sözleşmelerin Kuruluşu ve Geçerlilik Şartları**, İstanbul, 2021, s. 17 vd.; ÖZER Yusuf Mansur, **Kişisel Verilerin Korunmasında Blok Zinciri Modeli: Vaatler ve Hukuki Engeller**, İstanbul, 2020, s. 52 vd.

blokzincirin kavramsal çerçevesi incelenmektedir. Bu çalışmada ise blokzincir teknolojisinin teknik işleyişine dair hususlara değinilecektir.

Blokzincir teknolojisi artarda eklemlenmiş matematiksel işlemlerden oluşan süreçlere dayalı olarak çalışmaktadır ve bu işlemler zaman zaman karmaşık bir hal alabilmektedir. Bu çalışmanın amacı blokzincir teknolojisi üzerine çalışan hukukçulara teknolojinin anlatılması olduğu için bu karmaşık işlemler tüm detaylarıyla anlatılmayacak, blokzincir teknolojisinin işleyişinin anlaşılmasını gerektirdiği ölçüde ilgili süreç ve işlemler basitleştirilerek aktarılacaktır. Blokzincir teknolojisinin tek somut uygulaması kripto varlıklar olmasa da, yaygın bir bilinirliğe sahip olduğu ve günlük hayatın bir parçası haline geldiği için konunun somutlaştırılmasını kolaylaştıracağı düşüncesiyle blokzincir teknolojisinin işleyişi kripto varlıklar ve bunun en bilinen örneği olan Bitcoin üzerinden anlatılacaktır.

Blokzincir teknolojisinin işleyişine ve hukuk ile etkileşimine dair çok çalışma bulunmaktadır. Ancak tespit edebildiğimiz kadarıyla doğrudan teknolojinin işleyişini hukuk perspektifinden açıklayan ve bu teknolojinin hukuk ile bağlantısını kuran bir çalışma bulunmamaktadır. İşte bu nedenle bu çalışma teknik uzmanların ve hukukçuların katkılarıyla, hukuk ile blokzincir teknolojisi arasında bir köprü kurmayı amaçlamaktadır.

I. BLOKZİNCİRİN YAPISI

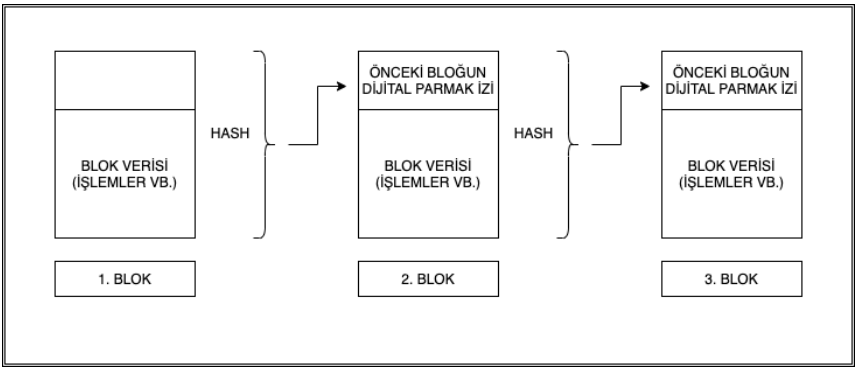
1. Blok İçeriği

Blokzincirin teknik altyapısı ve içeriği aslında temel yapı taşı olan blokların oluşturulmasından ve birbirlerine bağlanmasından meydana gelmektedir. Bu sebeple blokzincirlerin özelliklerini incelemeye geçmeden önce ileride yapılacak açıklamaların anlaşılmasını kolaylaştırmak amacıyla bir veri yapısı olan blok kavramının incelenmesi yerinde olacaktır.

Blok temelde bir grup veriyi içerisinde barındıran, sabit boyutlu bir veri yapısıdır. Bu anlamda bloklar sabit büyüklükte kutulara benzetilebilir. Bir bloğun boyutu ve içerisinde yer alan verinin niteliği her bir blokzincirde değişebilir ancak en temelde bir blokta iki tip veri depolanır. Bunlardan ilki içeriğe ilişkin, başka bir ifadeyle blokzincirin oluşturulma ve kullanılma amacıyla bağlantılı veriler, ikincisi ise bloklar arası bağlantıların kurulması için gerekli olan lojistik verilerdir. Bir kargo gönderisi ile benzetme yapmak gerekirse ilk tip veri kargo içeriğiyle ikinci tip veri ise kargonun üzerinde yer alan etiketle özdeşleştirilebilecektir.

İlk tip veriler her bir blokzincirin oluşturulma ve kullanım amacına göre çok farklı hususlar olabilir. Örneğin blokzincirler geleneksel veri tabanlarında olduğu gibi kimin neye ait olduğuna dair mülkiyet bilgilerini barındırabilirler[4]. Bitcoin gibi kripto varlıkların dayalı olduğu blokzincirlerde ise bu veri söz konusu kripto varlığın transferlerine yönelik işlemlerdir. İkinci tip verinin içeriği de bir blokzincirin teknik altyapısına göre değişiklik gösterebilir ancak bu verilerin ortak bir amacı vardır. Bu veriler sayesinde bloklar birbirine bağlanarak bir zincir oluşturulur. Buradaki en temel yöntem ise her bir blok içerisinde yer alan verilerin tamamının dijital parmak izi olarak değerlendirilebilecek bir değere bir sonraki blokta yer verilmesidir.

Bu bilgiler ışığında bir bloğun içeriği genel olarak şu şekildedir:



[4] "CATF Nihai Raporu", s. 8.

2. Blokların Bağlanması ve İz (İng. *Hash*)

Blokların birbirine bağlanması ve zincir haline getirilmesi iz (İng. *hash*) adı verilen bir veri aracılığıyla sağlanır. *Hash* hem bir bilgisayar fonksiyonunu ("iz üretme fonksiyonu") hem de bu fonksiyon sonucu üretilen çıktıyı ("iz") ifade etmek için kullanılan ifadedir[5]. Bilgisayar biliminde fonksiyon ise girdi olarak aldığı bir değeri belli işlemlere tabi tutarak bir çıktı üreten yapıyı ifade etmektedir. Örneğin toplama işlemi bilgisayar tarafından aslında bir fonksiyon olarak yerine getirilir. İki adet girdiyi alır, matematiksel değerlerini toplar ve sonucu bir çıktı olarak üretir. Benzer şekilde bilgisayar aracılığıyla yapılan her bir şifreleme aynı zamanda bir fonksiyondur. Şifrelenmesi istenen asıl değer bu şifreleme fonksiyonlarına girdi olarak verilir, bu değerler üzerinde bazı işlemler yapılır ve nihayetinde bir çıktı üretilir.

İz, belirli bir uzunluğa sahip bir sayı ve harf dizisidir ve herhangi bir veri üzerinde iz üretme fonksiyonunun gerektirdiği işlemlerin yapılmasıyla üretilir[6]. İz üretme fonksiyonlarının dayandığı algoritmaların[7]

---

[5] Akademik çalışmalarda *hash* fonksiyonu için "özetleme fonksiyonu", bu fonksiyon tarafından üretilen *hash* için ise "özet" kavramlarının kullanıldığı görülmektedir. Bkz. ONAT Fatih, "Algısal Özet Fonksiyonları Tabanlı Derin Öğrenme Yöntemleri Kullanılarak İmgelerin Sınıflandırılması", **Fırat Üniversitesi Fen Bilimleri Enstitüsü,** Doktora Tezi, 2019 (YÖK Tez Merkezi No: 539080); KARAGÖZ Emrah, "Artırımlı Özet Fonksiyonları", **Bilkent Üniversitesi Mühendislik ve Fen Bilimleri Enstitüsü,** Yüksek Lisans Tezi, 2014. *Hash* fonksiyonları uzun girdileri dahi sabit uzunlukta çıktılara dönüştürebildikleri için belli bir özetleme işlevi taşıdıkları söylenebilir. Ancak özetlemek, özetlenen asıl şeye ilişkin bilgi ve fikir veren bir çıktı üretme sürecini ifade eder. Gerçekten bir şeyin özetine baktığınızda asıl şeye ilişkin bir fikre sahip olabilirsiniz. *Hash* ise *hash* fonksiyonuna girdi olarak verilen veriyle çok alakasız olabilir. Örneğin Bitcoin'de kullanılan *hash* fonksiyonu olan SHA-256'nın "blokzincir" kelimesi için ürettiği çıktı, yani blokzincir kelimesinin SHA-256 fonksiyonu ile üretilen *hash*'i "94bddc04cf4fa84e9a76d619603421a1678048ccd439888f2d8e29a7ae6add5c". Kanımızca bu özelliği düşünüldüğünde *hash* kelimesinin Türkçe karşılığı olarak "iz" kavramının; bununla uyumlu şekilde *hash* fonksiyonunun Türkçe karşılığı olarak ise "iz üretme fonksiyonu" kavramlarının daha isabetli olduğunu düşünüyoruz. Çalışmanın devamında da bu kavramları kullanacağız.

[6] BASHIR, s. 87.

[7] Algoritma Türk Dil Kurumu sözlüğünde "*iyi tanımlanmış kuralların ve işlemlerin adım adım uygulanmasıyla bir sorunun giderilmesi veya sonuca en hızlı biçimde ulaşılması işle-*

özelliği verilen girdinin uzunluğuna bakmaksızın sabit uzunlukta sonuç üretmeleridir. Başka bir deyişle bir iz üretme algoritmasına bir kelimeyi, bir cümleyi, bir sayfayı veya bir kitabın tamamını da girdi olarak verseniz alacağınız sonuç sabit uzunlukta olacaktır. Bu önemli bir özelliktir. Bilgisayar dünyasında verilerin depolandığı alan başta olmak üzere çoğu şey deterministiktir Başka bir ifadeyle her şey belli bir kurala göre gerçekleşmektedir ve bu kuralları aşan hususları bilgisayar insan müdahalesi olmadan yorumlayamaz. Örneğin 'x = 2' ifadesi bilgisayara x değişkeninin 2 sayısına eşit olduğunu, 'x = "2"' ifadesi ise x değişkeninin tek karakterden oluşan '2' metnine eşitlenmesi gerektiğini anlatmaktadır. Değişkenin boyutu da dahil olabileceği işlemler de buna göre belirlenir. Açıkça bu durumda yapılması gerekenler kodlanmamış ise bir bilgisayar sayı olan 2 ile diğer sayıları toplayabilir, ancak metin olan '2' ile diğer sayıları doğru şekilde toplayamaz. Benzer şekilde bir bilgisayar programının ya da bir programda yer alan fonksiyonun düzgün şekilde çalışabilmesi için girdilerin, değişkenlerin, çıktıların boyutlarının yani bilgisayar depolama alanında kapladıkları yerin belirli olması gerekmektedir. Blokların da boyutu sabittir. Ancak bir blok içerisinde yer alan içeriğe ilişkin yani ilk tip verilerin boyutu her zaman bilinemeyebilir. Zira blok boyutu sabit olmakla birlikte bunun tamamını doldurmak ya da doldurmamak o bloğu zincire ekleyen kişinin takdirindedir. Diğer yandan blokların zincir şeklinde birbirine bağlanabilmesi için bahsedildiği üzere her bir blokta bir önceki bloğa ilişkin bir bilginin yer alması, bu şekilde bağlantının gösterilmesi gerekmektedir. Girdinin boyutuna bakılmaksızın sabit boyutlu çıktı üreten iz üretme algoritmalarının kullanılması işte bu boyut belirsizliği sorununu ortadan kaldırmaktadır.

---

mi" olarak tanımlanmıştır. En kısa tabirle algoritma "yöntem" demektir. Örneğin adını Roma komutanı ve lideri Sezar'dan alan ve "*Caesar Cipher*" olarak bilinen yaygın şifreleme algoritması şifrelenmek istenen metinde yer alan her bir harfi alfabedeki sırasından belirli miktar öncesindeki harfle değiştirme üzerine kuruludur. İşte soyut olarak ifade edilen bu yöntem bir algoritmadır. Bu algoritmanın alınacak bir girdi üzerinde uygulanmasını sağlayacak somutlaştırılmış kod parçacığı ise fonksiyondur. Diğer bir deyişle fonksiyonlar, çıktı üretmek için girdiler üzerinde belli algoritmaları uygularlar. Bu itibarla "iz üretme algoritmaları" da iz üretme fonksiyonları tarafından, iz üretmek için girdiler üzerinde uygulanacak işlemlerin bütününü ifade eden bir kavramdır.

İz ile kastedilenin ne olduğunu somutlaştırmak için Bitcoin Blokzinciri'nde uzlaşma mekanizmalarında ve adreslerin oluşturulmasında kullanılan SHA-256 (İng. "*Secured Hash Algorithm*") algoritması incelenebilir[8]. SHA-256 algoritması herhangi bir uzunlukta girdi için çıktı olarak 64 karakterden oluşan bir iz üretmektedir. SHA-256 ile üretilen iz sayı ve harflerden oluşan bir dizidir[9]. Farklı ifadelerin SHA-256'ya göre üretilen izleri şu şekildedir:

İfade	**SHA-256'ya göre üretilmiş izi**
Blokzincir	7a4b58bb56a4e8404e37f8e7a97c0882f424ea483d449c9514ed7a9e39e3cdee
blokzincir	94bddc04cf4fa84e9a76d619603421a1678048ccd439888f2d8e29a7ae6add5c
Blokzincir.	b562229a6d9b933ee2af6abc7578b26f2d4195a320ee11ed5ee06f41f48639d0

[8] SHA-256 algoritmasının istenilen girdilere uygulanmasını sağlayan birçok internet sitesi bulunmaktadır. Örnek olarak bkz: https://timestampgenerator.com/tools/sha256-generator/ (Erişim Tarihi: 05.05.2021).

[9] SHA-256 algoritmasının isminde yer alan 256 sayısı bu algoritma çıktılarının bit uzunluğuna işaret eder. Bu bilgi bir hukukçu için detay bir bilgidir ancak özetlemek gerekirse bit bilgisayar dilinde 0 veya 1 olabilen en küçük veri tipi olarak adlandırılabilir ve ikilik sayı sistemiyle ifade edilir. Günlük hayatta onluk sayı sistemi kullanılır, 0'dan 9'a kadar 10 adet birim ile işlem yapılır. Örneğin 256 sayısı onluk sayı sisteminde basamaklarına en sağdan başlayarak 10'un kuvvetlerine göre ayrılır (6x100 + 5x101 + 2x102). İkilik sayı sisteminde bu hesaplar 10'un değil 2'nin kuvvetlerine göre yapılır; 0 ve 1 olmak üzere sadece 2 birim ile işlem yapılır. Örneğin onluk sayı sisteminde 7'nin 2'lik sayı sistemindeki karşılığı 111'dir (1x20 + 1x21 + 1x22). İzlerde ise ise sayıları ve harfleri ifade etmek için ikilik sayı sistemi ya da günlük işlemlerde kullandığımız onluk sayı sistemi değil onaltılık sayı sistemi kullanılır. Nasıl ki ikilik sayı sisteminde 2, onluk sayı sisteminde 10 adet birim ile işlem yapılıyorsa onaltılık sayı sisteminde de 16 adet birim ile işlem yapılır ancak 9'dan sonraki birimler basamak sayısı karışmaması için harflerle ifade edilir. Yani a, b, c, d, e, f sırasıyla 10, 11, 12, 13, 14, 15'e karşılık gelmektedir. 16, 2'nin dördüncü kuvvetine karşılık geldiği için her onaltılık sayı sistemindeki her bir ifade aslında 2'lik sayı sisteminde 4 basamaklı bir sayıya karşılık gelir. Örneğin 2'lik sayı sistemindeki 10011101 sayısı onluk sistemde 157 sayısına karşılık gelirken onaltılık sayı sisteminde 9d (dx160 + 9x161; d 13'e karşılık geldiğinden 13x1+9x16). Dikkatle incelendiğinde aslında 10011101 sayısının iki tane 4 basamaklı sayıya ayrılması durumunda (1001 ve 1101) bu sayıların onaltılık sayı sisteminde sırasıyla 9 ve d'ye karşılık geldiği görülebilecektir. SHA-256'nın çıktı uzunluğu aslında adından anlaşıldığı üzere 256 bittir, ikilik sayı sisteminde 256 basamaklı bir ifadye karşılık gelecektir. Ancak izler onaltılık sayı sistemine göre yazıldığından SHA-256 algoritmasının çıktılarının karakter uzunluğu 256 değil 64 olmaktadır.

Blokzincir verilerin birbirlerine kriptografik algoritmalar kullanılarak bağlanmış bloklar içerisinde depolandığı ve kural olarak sadece ekleme yapılabilen bir veri tabanıdır.	487a60c357452e7915516fcf46c8778e0dfb617b16899707e80d65484403941a

İz üretme algoritmalarının bazı genel özellikleri vardır:

1. Tabloda da görüldüğü üzere iz üretme algoritmaları hep sabit uzunlukta çıktı üretme üzerine kuruludur. Girdinin uzunluğundan bağımsız olarak SHA-256'nın ürettiği dizinin uzunluğu hep 64 karakterdir.

2. İz üretme algoritmalarında girdi olarak verilen ifadedeki en ufak değişikliğin bile çıktıyı önemli ölçüde değiştirdiğine dikkat edilmelidir. Tabloda görülebildiği gibi "Blokzincir" kelimesi sadece bir harfi küçülterek ya da sonuna bir nokta ekleyerek iz üretme algoritmasına girdi olarak verildiğinde çıktı olarak üretilen iz tamamen farklıdır.

3. Ayrıca iz üretme algoritmaları tek taraflı ve geri döndürülemez algoritmalardır. Bu ne demektir? İz üretme algoritmalarına, örneğin SHA-256'ya, istediğiniz girdiyi vererek çıktı üretebilirsiniz ancak çıktı olarak üretilmiş bir izden yola çıkılarak, tersine hesap yaparak algoritmaya girdi olarak verilen ilk ifadeye ulaşmak mümkün değildir.

4. İz üretme algoritmaları deterministiktir. Bir girdinin belirli bir iz üretme algoritmasındaki çıktısı her zaman aynı olacaktır, rastgele bir değer üretimi söz konusu değildir.

5. İz üretme algoritmalarının son önemli özelliği ise çakışmayan sonuçlar üretmeleridir. Bunun anlamı aslında her ifadenin sadece bir izinin olması, iki ayrı ifadenin izlerinin aynı olamamasıdır[10].

[10] Buna "çakışmaya dayanıklılık (İng. *collision resistance)*" denmektedir. Aslında hiçbir iz üretme algoritması çıktıların çalışma ihtimaline karşı %100 dayanıklı değildir. Bunun matematiksel çok basit bir açıklaması vardır: Teorik olarak istenen uzunlukta bir verinin girdi olarak girilebildiği sistemde çıktının uzunluğu daima sabit ise bazı girdilere ait çıktıların aynı olması matematiksel bir zorunluluktur. Buradaki mantık bir senede 365

Bütün bu özellikler bilgisayar dünyasında izlerin bir verinin dijital kimliği, deyim yerindeyse bir dijital parmak izi olarak kullanılmasını mümkün kılmıştır. İz sayesinde bir verinin değiştirilip değiştirilmediği kolayca kontrol edilebilmektedir. Üstelik bu kontrol, verinin içeriği hakkında bilgi vermeden de yapılabilmektedir. Bunun güzel bir örneği kullanıcı giriş yöntemlerinde izlerin kullanılmasıdır. Bir internet sitesi kullanıcılarının şifrelerini düz metin halinde depolamak yerine bunların izlerini depolayabilir. Bu sayede kullanıcının şifresi internet sitesinin kendi sisteminde dahi kaydedilmiş olmaz. Giriş denemesi yapıldığında ise kullanıcının o an girdiği şifre iz üretme algoritmasına girdi olarak verilir ve elde edilen çıktı sistemde kaydedilmiş olan iz ile karşılaştırılır. İz verileri birbirini tutuyorsa giriş izni verilir aksi halde verilmez.

Benzer şekilde bir blokzincirde blokların diğer blokları tanımasında ve blokların birbirlerine bağlanmasında da iz üretme algoritmaları kullanılmaktadır. Her bir blok kendisinden önceki blok içerisinde yer alan tüm verilerin yani bloğun izini içerir. Her bloğun izi o bloğa özel olduğu için önceki bir blokta değişiklik yapılmak istendiğinde içeriği değiştirilmiş olan bloğa ait iz de değişecektir. Ancak değişiklik yapılmadan önceki bloğa ait iz sonraki blokta halihazırda kayıtlıdır. Bir blokzincirde blok içeriklerine bir müdahale olup olmadığı blok içeriğinin izi ile sonraki blokta kayıtlı bulunan izin karşılaştırılmasıyla hızlıca tespit edilir ve eğer izler uyuşmazsa değiştirilmiş olan içerik sistemdeki birimler tarafından sisteme kabul edilmez, kabul edilemediği sürece de o blokzincirde ana zincirin bir parçası olamaz.

Dahası ilk bloktan itibaren kurulan iz bağlantıları düşünüldüğünde ortaya zincirin koparılmasını kelimenin tam anlamıyla imkansız kılmasa

---

gün olduğu halde dünyada 365 taneden fazla sayıda insan olduğu için en az iki insanın doğum gününün aynı gün olmasının matematiksel bir zorunluluk olmasıyla benzerdir. Ancak SHA-256 gibi etkili iz üretme algoritmalarında bu çakışma ihtimali çok düşüktür ve ihmal edilmektedir. Bir çakışmaya denk gelmek için SHA 256'nın artarda 2128 kere (39 basamaklı 340.282.366.920.938.463.463.374.607.431.768.211.456 sayısına karşılık gelmektedir) çalıştırılması ve bunların karşılaştırılması gerekmektedir ki bu durumda bile çakışma garanti değildir, buradaki hesaplar olasılık temellidir. Çakışma ihtimallerine ilişkin daha detaylı açıklamalar ve farklı iz üretme algoritmalarındaki çakışma ihtimallerine ilişkin bilgiler için bkz. BASHIR Imran, **Mastering Blockchain**, 2017, s. 89.

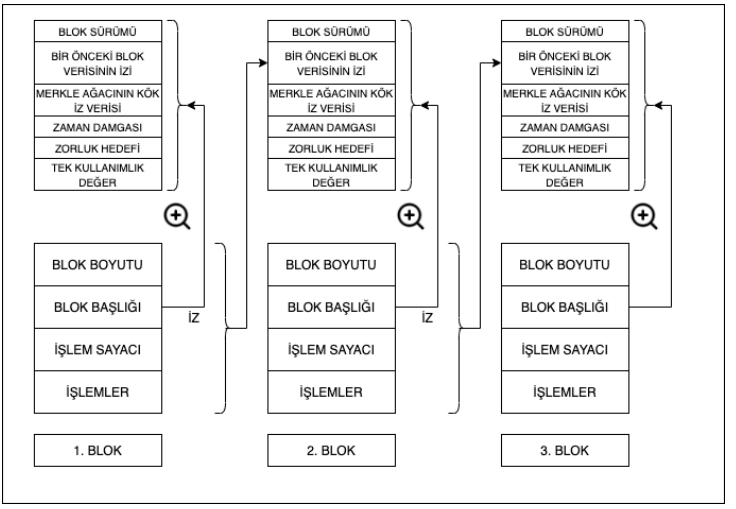
da aşırı derecede zorlaştıran bir iz bağlantıları bütünü çıkmaktadır. İlk bloğun (İng. "*genesis block*") izi ikinci blok içerisine kaydedilir. Daha sonra ikinci bloğun içeriği iz üretme algoritmasına sokularak bunun izi de üçüncü bloğun içerisine kaydedilir. Böylece ikinci bloğun izi aynı zamanda ilk bloğun izinin de dahil olduğu bir veriden üretilmiş olur. Bu itibarla ilk blokta istenmeyen bir değişiklik yapılmaya çalışıldığında ilk bloktan elde edilen iz sadece ikinci blokta değil üçüncü blokta yer alan izin de farklılık göstermesine ve kontrollerin başarısız olmasına sebep olacaktır. Başka bir deyişle bir blok içerisinde bir değişiklik yapmak ve iz zinciri kontrolünün de buna uygun olmasını sağlamak için o bloğu izleyen ilk bloktan başlayarak sonraki tüm blokların içerisindeki iz bilgilerinin sil baştan değiştirilmesi gerekecektir. Bir blokzincirde yer alan bir bloktaki verilerin ya da işlemlerin, yeni blok eklendikçe daha güvenli hale gelmesinin ve daha özel olarak Bitcoin Blokzinciri'nde yapılacak işlemlere yönelik belirli sayıda onay alınmasının sebebi budur.

Daha önce bloklar ile kutu arasında bir analoji kurulabileceğini ifade etmiştik. Aynı analojiden devam edersek her bir blok içerisinde bulunan önceki bloğa ait iz verisi de önceki bloğa ait puslu bir fotoğrafa benzetilebilir. İkinci kutuda birinci kutudaki içeriğin fotoğrafı bulunur ve eğer ilk kutuda bir şey değiştirilmeye çalışılırsa buradan kontrol edilerek değişiklik tespit edilir. Üçüncü kutuda ise ikinci kutunun ve dolayısıyla aynı zamanda da birinci kutunun fotoğrafı bulunur. Bu silsile devam ettirildiğinde ise her bir kutuda doğrudan kendinden önceki kutunun içeriğinin fotoğrafı, dolaylı olarak ise kendisinden önce gelen tüm kutuların fotoğrafı bulunmuş olacaktır. Fotoğrafa bakıldığında içeriğin ne olduğu anlaşılmasa da bir değişiklik yapıldığında bu değişikliğin fark edilmesi mümkün olacaktır.

Bu iz zincirinin blokzincir teknolojisi açısından çok temel bir sonucu vardır. Zincire eklenen her bir blok, daha önceki bloklarda yer alan verilerin değiştirilmesi için yapılması gereken işlem miktarını artırmakta ve böyle bir değişikliğin yapılmasını zorlaştırmaktadır. İşte bu sebepledir ki bir blokzincirde yer alan verilerin değiştirilmesinin pratik olarak imkansız olduğu düşünülür. Ağdaki diğer birimler yeni bir blok eklemeye çalışırken bir kişinin hem değiştirmek istediği bloktan sonra gelen tüm

blokları yeniden ekleyip hem de yeni eklenen her bloğa yetişmesi gerçekten pratik açıdan imkansıza yakındır.

Bunun yanında her bir blokzincir tipine göre bloğun yapısı ve blok içerisinde yer alan veriler değişiklik gösterebilir. Örneğin Bitcoin'de olduğu gibi blokzincirin amacına göre işlemlerin zamanlarının tutulması gerekebilir veya Ethereum'da olduğu üzere akıllı sözleşmeleri yürütecek yapılara ilişkin ek bilgilerin bulunması gerekebilir. Bitcoin Blokzinciri'nde yer alan blokların yapısı şu şekildedir[11]:



Bu şekilde yer alan kavramlar ve işlevleri daha ileride açıklanacaktır. Bitcoin özelindeki en önemli fark olan blok başlığı ise yine kutu analojisini hatırlarsak her blok üzerine yapıştırılan etiket olarak düşünülebilir. Görüldüğü üzere Bitcoin Blokzinciri'nde bir önceki bloğa ilişkin iz bilgisi de blok başlığı içerisinde yer almaktadır.

Blok yapısına ilişkin açıklamalarımız burada sona ermektedir. Bir sonraki bölümde ise blokzincirin genel özellikleri Bitcoin Blokzinciri'ne ilişkin detaylı hususlarla beraber incelenecektir.

---

[11] Bitcoin Blokzinciri'nde yer alan blokların yapısı hakkına detaylı bilgi için bkz. BASHIR, s. 127; NAKAMOTO Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008, s. 4.

II. BLOKZİNCİRİN ÖZELLİKLERİ VE İŞLEYİŞİ

Her bir blokzincirin kuruluş amacı ve kurallarına göre farklı özellikleri olabilir. Belirtmek gerekir ki tartışmalar blokzincir teknolojisinin ilk yerleşik uygulaması olan Bitcoin Blokzinciri üzerine olduğu için çoğunlukla açık ve izne tabi olmayan blokzincirler dikkate alınarak açıklamalar yapılmaktadır. Konunun anlaşılmasını kolaylaştırmak için bu çalışmada da aslında açık ve izne tabi olmayan blokzincirleri özelliği olan dört temel özellik başlıklar halinde incelenecektir ancak bu özellikler sadece açık ve izne tabi olmayan blokzincirler değil diğer blokzincir türleri için de değerlendirilecektir.

1. Dağıtılmış Olma (İng. *Distributed*)

Dağıtılmış olma ibaresi aslında İngilizce "*distributed*" kavramına karşılık olarak tercih ettiğimiz bir kavramdır[12]. Blokzincirin bu özelliğini ifade ederken İngilizce kaynaklarda "*decentralized*" (merkezi olmayan) ve "*distributed*" (dağıtılmış) terimleri kullanılmaktadır ve bu kullanımlar arasında bir uzlaşma söz konusu değildir[13]. Bu çalışma kapsamında dağıtılmış olma verilerin tek bir merkezde değil sistemde yer alan birden çok birim tarafından depolanmasını; merkezi olmama ise verinin ve veri tabanına yapılacak eklemelerin tek bir merkezi aktörün kontrolünde olmamasını ifade edecek şekilde kullanılmaktadır[14]. İkisi arasındaki farkı somutlaştırmak için Bitcoin Blokzinciri'nde madencilik işlemini gerçekleştiren işlem gücünün farklı kişilerin elinde bulunduğu senaryolar düşünülebilir. Şu an veriler ağdaki farklı düğümlere dağıldığı için dağıtılmış ve aynı zamanda blok içerisine eklenecek veriler farklı kişiler tarafından yarışma sonucu belirlendiği için merkezi olmayan bir sistemden söz edilebilir. Ancak işlem gücünün çoğunun tek bir kişinin elinde bulunması durumunda sistem dağıtılmış olmakla birlikte artak blok içerisine eklenecek veriler tek bir kişi tarafından belirleneceği için merkezi olmayan bir sistem söz konusu olacaktır. Bitcoin Blokzinciri yapısal açıdan dağıtılmış ve merkezi

---

[12] Bkz. yuk. dn.1.

[13] BARAN Paul, "On Distrubuted Communications Networks", C. S. 1962, s. 3.

[14] Aynı yönde kullanım için bkz. Cryptoassets Taskforce, s. 10.

olmayan bir yapıdır fakat teknik doğası itibariyle fiilen merkeziyetçi bir yapıya bürünebilir. Bir blokzincir oluşturulma aşamasında sadece belli kişilerin veri eklemesine izin verecek şekilde oluşturularak yapısal açıdan da merkeziyetçi olarak kurgulanabilir.

Dağıtılmış sistemler blokzincir teknolojisiyle ortaya çıkan, yeni bir şey değildir. Dağıtılmış sistemler yazılım dünyasında iki ya da daha fazla düğümün ortak bir sonuca ulaşmak için birlikte çalıştığı bir modeli ifade eder[15]. Burada düğümden kasıt ağdaki her bir katılımcıdır ve İngilizce'deki "*node*" kavramına karşılık gelir.

Dağıtılmış sistemler işlevsel açıdan hukuk ve muhasebe dünyasından alışkın olduğumuz ikili sistemlerden ayrılır. Bir sözleşme yapıldığında iki taraf da belirli haklara sahip olur ve/veya yükümlülükler altına girer. Ancak bu sözleşmenin uygulanması sırasında her iki taraf da kendi davranışlarını takip eder ve bir uyuşmazlık söz konusu olduğunda herkes kendi delillerine dayanarak yetkili yargı mercileri karşısında haklılığını ispat etmeye çalışır. Aksi açıkça kararlaştırılmadıkça tarafların tuttukları kayıtların bir diğerine üstünlüğü yoktur. Bu sebeple farklı görünüş ve işlevlerde aracı kurumlar, örneğin finansal kuruluşlar, arabulucular, mahkemeler vs., iki taraf arasındaki ilişkiye dahil olurlar.

Dağıtılmış sistemlerde ise sistemin içerisinde bulunan aktörler belirli kurallar dahilinde bir sonuç üzerinde uzlaşırlar. Aslında bir bakıma burada dağıtılmış olan şey gerçekliktir. Herkes kendi sisteminde gerçekliğin bir versiyonunu bulundurur. Etkili çalışan bir dağıtılmış sistemde ise birimlerin bulundurduğu gerçeklik arasında farkın olmaması amaçlanır. Örneğin bir ticari ilişkide Tacir A'nın defterlerine göre B, A'ya 1000 TL borçlu gözükmekte Tacir B'nin defterlerine göre ise A, B'ye 500 TL borçlu gözükmekte olsun. Bu iki defterin kural olarak birbirine üstünlüğü olmadığından ve taraflar kendi istedikleri gibi defterleri değiştirebileceklerinden tarafların sadece defterlere bakarak bir sonuca ulaşması mümkün olmayacaktır. Ancak dağıtılmış bir yapıda tutulacak bir defter modelinde A ile B arasındaki borç dengesine dair kayıtlar deftere kaydedilmeden önce sistemdeki diğer katılımcılarının da dahil olduğu bir algoritma ta-

[15] BASHIR, s. 10.

rafından teste tabi tutulacaklar ve bu testi geçebilen kayıtların o defter açısından doğru olduğu tüm katılımcılar tarafından kabul edilecektir. A ile B'nin kayıtları arasında bir tutarsızlık olduğunda bu ağdaki diğer birimlere gönderilecek ve testler sonucunda sadece bir tanesinin kaydı gerçekliğin parçası olarak kabul edilecektir.

Buradaki gerçeklik hakikat veya objektif gerçeklik olarak anlaşılmamalıdır. Pekala sistemdeki düğümlerin bir araya gelip anlaşarak gerçeği yansıtmayan bir veri ya da işlemi bir blok içerisine koymaları ve bunu zincire eklemeleri mümkündür. Burada gerçeklik ile ifade edilmek istenen daha ziyade sistemdeki aktörlerin o sistem bakımından doğru olduğu üzerinde anlaştığı bir durumu ifade etmektedir.

A. CAP Teoremi

Dağıtılmış sistemlerde kural olarak tüm düğümler diğerlerine veri alma ve gönderme imkanına sahiptir. Böyle bir sistemde bir düğümün diğer düğümlere her zaman doğru bilgi göndereceğinin garantisi yoktur. Diğer bir deyişle, sistemde kötü niyetli düğümler olabilir ve etkili bir sistemin kötü niyetli düğümlerin davranışlarına rağmen güvenilir sonuçlar oluşturabilmesi gerekir.

Böyle bir sistemin etkili çalışmasında üç temel öğe göze çarpmaktadır. Öncelikle sistemdeki tüm birimlerin söz konusu gerçekliğin aynı versiyonuna sahip olması yani tutarlı olması (İng. "*consistency*") gerekir. İkinci olarak sistemin açık, güncel yeni bilgileri kabul edecek durumda olması yani erişilebilir olması (İng. "*availability*") önemlidir. Son olarak ise sistemin kötü niyetli düğümlerin varlığına rağmen düzgün bir şekilde çalışmaya devam edebilmesi yani düğümler arasındaki bölünmelere karşı toleranslı olması (İng. "*partition tolerance*")[16] gerekmektedir.

Ancak dağıtılmış sistemlerde bu üç özelliğin aynı anda sağlanması mümkün değildir. Bu durum CAP Teoremi -*Eric Brewer* tarafından ileri sürüldüğü için *Brewer Teorisi* olarak da adlandırılmaktadır- ile ortaya

[16] BASHIR, s. 11; GILBERT S./LYNCH N. A., "Perspectives on the CAP Theorem", **Computer** C. 45, S. 2, 2012, s. 30.

konulmuştur[17]. CAP Teoremi'nin anlaşılması için Kaushik Sathupadi tarafından kişisel internet sitesinde[18] verilen bir örnek oldukça faydalıdır.

Söz konusu örnek bir evli çiftin diğer insanlara hatırlatma hizmeti verdiği bir şirket örneği üzerinden kurgulanmıştır. Kullanıcılar bu şirketi arayarak bilgiler bırakmakta ve istedikleri zaman da talep başına ücret ödeyerek arayıp bu bilgileri sorabilmektedirler. Hizmetin rağbet gördüğü ve kullanıcı sayısının arttığı varsayımında; evli çift talebe yetişebilmek için telefonlara beraber cevap vermeye başlarlar ve her ikisi de hatırlatılacak bilgileri kendilerine ait bir deftere not alırlar. Bunun üzerine dağıtılmış sistemin sorunları baş gösterir.

Bir kullanıcı daha önce kaydettirdiği bir bilgiyi sormak için aradığında, daha önce bilgiyi kaydettirdiği eşe değil diğerine denk gelebilir. Bu ihtimalde eşler sadece kendi defterlerine baktığı ve haberleşmediği için kullanıcıya aradığı bilginin deftere kaydedilmediği söylenecektir. Buradaki temel sorun A ile B'nin defterleri arasında bir tutarlılığın, izleme ve eşleme mekanizmasının bulunmamasıdır.

Bunu çözmek için eşler kayıt tutma sisteminde bir değişiklik yaparlar ve yeni bir bilgi girilmesi için bir talep alındığında cevap veren eşin diğer eşe de söz konusu yeni bilgiyi iletmeden aramayı sonlandırmaması hususunda anlaşırlar. Bu sayede her arama her iki eşin de defterine kaydedileceği için iki defter arasındaki tutarsızlık sorunu çözülmüş, tutarlılık sağlanmış olur.

Yeni sistem tutarlılık sağlamakla birlikte başka bir sorun yaratmaktadır. Eşlerden bir tanesi işte değilken diğer eşe bir bilgi girme talebi geldiğinde o çağrı eş zamanlı olarak diğer eşe bildirilemeyeceği için bilgi girişi yeni sisteme uygun olarak sonuçlandırılamayacaktır. Dolayısıyla sistem erişilebilir olmayacaktır. Diğer eşe söylenmeden bilgi alınır, deftere kaydedilir ve çağrı kapatılırsa da bu sefer sistem erişilebilir olacak ancak tutarlılık sekteye uğrayacaktır.

---

[17] CAP Teoreminin matematiksel ve mantıksal ispatına ilişkin açıklamalar için bkz. GILBERT/LYNCH, s. 31.

[18] "*A plain English introduction to CAP Theorem*". Erişim Adresi: http://ksat.me/a-plain-english-introduction-to-cap-theorem (Erişim Tarihi: 05.05.2021).

Bunu çözmek için ise eşler yeni bir değişiklik daha yaparlar ve eğer bir bilgi ekleme talebi geldiğinde diğer eş işte değilse onun yokluğunda girilen tüm kayıtların e-posta aracılığıyla gönderilmesini ve bilgi kendisine e-posta ile gönderilen eşin işe döndüğünde ilk çağrısını almadan önce defterini yokluğunda e-posta ile gönderilen tüm yeni bilgileri girerek güncellemesini kararlaştırırlar. Bu sayede hatırlatma sistemi hem tutarlı hem de erişilebilir hale gelmiş olur.

Daha sonra eşler arasında bir anlaşmazlık çıktığını ve bu kızgınlık üzerine eşlerden biri kendisine gelen çağrıları diğer eşe bildirmemeye başladığını düşünelim. Bu durumda sistem tutarlılığını kaybedecektir. Eğer tutarlılığı sağlayıp eşler arasındaki iletişim kopukluğuna karşı toleranslı bir sistem yaratmak istenirse eşlerin arası düzelene kadar tek eş olarak kayıt yapılabilir veya kayıt alma tamamen durdurulabilir. Bu durumda sisteminiz tutarlı ve toleranslı olacak ancak erişilebilir olmayacaktır.

Alternatif bir çözüm olarak sistemin hem erişilebilir hem de eşler arasındaki iletişim kopukluğuna karşı toleranslı hale getirilmesi için üçüncü bir kişiyle defterlerin kontrol edilmesi ve farklılıkları diğer diğer deftere işlenmesi konusunda anlaşılabilir ancak bu durumda da bu kontrol yapılana kadar geçen sürede sistemde tutarlılık olmayacak, tutarlılık ancak gecikmeli şekilde sağlanabilecektir. Tutarlılığın verilerin sistemde yer alan bazı bireylerin onayına tabi tutularak sağlandığı bu duruma "nihai tutarlılık (İng. *eventual consistency*)" adı verilmektedir[19]. Ancak böyle bir kişinin yokluğunda sistemde sadece iki kişi yer aldığı için bu sistem eşlerden birinin kötü niyetli davranmasına karşı korunaklı değildir.

Örnekte de görüldüğü üzere bir dağıtılmış sistemin aynı anda hem tutarlı hem erişilebilir hem de birimler arasındaki bölünmelere karşı dayanıklı olması mümkün değildir. Bir sistem tasarlarken bunlar arasındaki denge gözetilerek sistemin ihtiyaçlarına göre bir seçim yapılması gerekir. Dağıtılmış sistemlerde verinin dağıtılmış olması temel unsur olduğundan ve sisteme veri giriş çıkışı yapıldığından sistemde birimler arasında oluşacak bölünmelere karşı dayanıklılık unsurundan vazgeçilemez. Bunun gibi güvenilir olmayan düğümllerin bulunduğu veya bulunma ihti-

[19] BASHIR, s. 30.

malinin olduğu sistemlerde tutarlılık ve erişilebilirlik arasında bir denge kurulması gerekir.

Blokzincirler de bu açıdan CAP Teoremi'nin bir istisnasını oluşturmazlar. Blokzincirlerde de tutarlılık ve erişilebilirlikten bir tanesinin diğerine nazaran daha öne çıkarılması gerekir. Erişilebilirlik öne çıkarılırsa her talebe sistemde bir cevap üretilecektir ancak bunun doğruluğuna ilişkin bir şüphe ortaya çıkacaktır. Tutarlılık öne çıkarılırsa da cevapların doğruluğundan emin olunacak ama sistem her talebe zamanında cevap veremeyebilecektir. Buradaki tercih bir tasarım tercihidir ancak en çok bilinen blokzincirlerde erişilebilirlik tutarlılığa tercih edilmiştir. Fakat bunun anlamı tutarlılığın sağlanmaması değildir zira farklı birimler tarafından tutulan bilgilerin tutarlı olmadığı bir dağıtılmış yapının işlevselliğinden de söz edilemez. Buradaki tercih zaman bakımından yapılmıştır. Yani blokzincirler çoğunlukla erişilebilirdir ve sistemdeki birimler arasındaki bölünmelere karşı toleranslıdır ancak tutarlılık bunlarla eş zamanlı olarak sağlanmaz. Farklı sistemlerle, örneğin ağdaki birimlerin davranışlarına bakılarak veya onayları alınarak tutarlılık zaman içerisinde sağlanır[20]. Yani blokzincirlerdeki durum yukarıdaki örnekte üçüncü bir kişinin dahil edildiği nihai tutarlılık örneğine benzemektedir. Bunun pratikteki sonucu ne olacaktır? Örneğin Ahmet hem Beril'e hem de Cemal'e aynı Bitcoin'i gönderdiği iki farklı işlemi sistemde dağıtıp ikisinin de farklı madenciler tarafından bir bloğa eklenmesini sağlayabilir. Ancak bunları izleyen diğer işlemler ve blokların eklenmesi sürecinde yapılan kontrollerde bu işlemlerin ikisine birden onay verilmeyeceği için nihai olarak bu işlemlerden sadece bir tanesinin bulunduğu zincir uzun zincir olarak öne çıkacak ve çoğunluk onu izleyecektir. "Çifte harcama (İng. *double spending)*" adı verilen bu durum dağıtılmış sistemlerin en önemli sorunlarından biridir ve Bitcoin özelinde nasıl aşıldığı ileride daha detaylı şekilde anlatılacaktır. Ancak CAP Teoremi'yle ilgili olarak bilinmesi gereken nokta şudur: Bitcoin Blokzinciri'nde bir işlemin güvenli gerçekleştirilmiş kabul edilmesi için o işlemin bulunduğu blok üzerine belirli sayıda bloğun -genel olarak kabul edilen sayı altıdır- eklenmiş olmasının kontrol edilmesi önerilmek-

[20] BASHIR, s. 30.

tedir[21]. Burada eklenecek blok sayısı tamamen keyfi olup önemli olan bir blok üzerine eklenen her bir bloğun, o blok içerisinde yer alan işlemlerin değiştirilmesini daha da zorlaştırmasıdır.

B. Dağıtılmış Sistemlerin Özellikleri

Geleneksel veri depolama modellerinde veriler bir ya da birkaç merkezde depolanır. Bu modellerin avantajları ve dezavantajları vardır. Avantaj olarak verilerin kontrolünün ve güvenliğinin tek bir merkezden daha kolay sağlanması, işlemlerin daha hızlı yapılması gösterilebilir. Bu bir ya da az sayıda merkeze yapılacak saldırılarla verilerin kalıcı olarak zarar görme olasılığının bulunması, şeffaflığın sağlanamaması ve sistemin işleyişinin merkezi depolamayı yürüten kişi ya da kurumlara güvenmeyi gerektirmesi gibi noktalar da dezavantajları arasında sayılabilir.

Bir sistemin dağıtılmış olma özelliğinin en önemli sonucu sistemin saldırılara karşı daha dayanıklı olmasıdır. Bütün veriler sistemdeki birçok kullanıcıda saklandığı için, sistemin tek bir hata noktası (İng. *single point of failure*) yoktur. Ağdaki tek bir düğümün uğradığı saldırı ve bunun sonucunda oluşabilecek veri kaybı diğer birimlerdeki verileri etkilemez ve saldırının etkisi tamamen geri çevrilebilir.

Diğer yandan dağıtılmış sistemlerin de dezavantajları vardır. Dağıtılmış sistemlerde veri çok sayıda birimde beraber depolandığı için bu birimler arasında bir anlaşmanın olması ve herkesin verinin son durumu üzerinde mutabakata varması gerekir. Bu sebeple tüm birimlerin tüm veriyi depolaması ve her yeni verinin yine tüm birimlere bildirilmesi gerekir. İşte bu iletişim ve mutabakat süreci, daha önce değinildiği üzere tutarlılığın gecikmeli şekilde sağlanması sonucunu doğurur.

Blokzincir teknolojisinde blokzincire eklenecek verinin kim tarafından belirleneceği sorusunun cevabı merkezi olmayan yapıda gizlidir ve bunun için daha ileride incelenecek olan uzlaşma (İng. *consensus*) protokolleri kullanılır.

---

[21] BASHIR, s. 119.

Ayrıca bir blokzincirde tutarlı bir veri tabanının oluşturulabilmesi için eklenen her yeni veride geçmişe yönelik bazı kontrollerin yapılması gereği ortaya çıkmaktadır. Örneğin Bitcoin özelinde gönderilen bir Bitcoin'in mevcut olup olmadığı, daha önce başkasına gönderilip gönderilmediği kontrolü şu ana kadarki tüm Bitcoin işlemlerinin tutulduğu bir veri tabanı üzerinde kontrol edilecektir. Bu verinin zamanla yığılması sisteme girmek isteyen her birimin depolaması gereken veri miktarını artırmaktadır. Nisan 2021 itibariyle Bitcoin Blokzinciri'nin toplam boyutu 330 GB'den[22] büyük iken Ethereum blokzincirinin tüm işlem geçmişini tutmak için gereken alan 7 TB'den büyüktür[23].

Çok büyük miktarda verinin depolanmasını ve merkezi olmayan mekanizmada gerekli kontrollerin yapılmasını kolaylaştırmak için de farklı blokzincirlerde farklı çözümler getirilebilmektedir. Bitcoin ve Ethereum örneğinde bu sorun düğümler arası farklılaştırma yoluyla çözülmüştür. Buna göre örneğin Bitcoin Blokzinciri'nde bazı düğümler tüm veriyi depolayarak sistemin dağıtılmış yapısını korurken bazı düğümler sadece onay almak için ağa bağlanabilmekte ve gerekli bilgileri bu tam birimlerden çekebilmektedir. Yine başka bir çözüm örneği olarak Ethereum blokzincirinde tüm verinin erişilebildiği iki farklı düğüm yürütülmekte ancak bir tanesi (İng. "*archive node*") tüm işlemlerin geçmişlerini tutarken bir tanesi (İng. "*full node*") tüm işlemlerin sadece son hallerini tutarak yer tasarrufu sağlamaktadır. Bu sayede en ufak işlem yapmak veya işlemi kontrol etmek için bile şu ana kadar yapılmış tüm işlemlerin kaydını içeren büyük bir veri depolanmak zorunda kalınmamaktadır. Bir işlemin gerçekleştirildiğini iddia eden kişinin söz konusu işleme dair belirli verileri paylaşması ve işlemin muhatabı olan kişinin sadece bu verileri kullanarak işlemin gerçekleştirilip gerçekleştirilmediğini kontrol etmesi mümkün olmaktadır.

Yine konunun daha iyi anlaşılması için somut bir örnek vermek adına Bitcoin tarafından kabul edilen düğüm ayrımlarını ve bir Bitcoin

---

[22] Statista, 2021. Erişim Adresi: https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/ (Erişim Tarihi: 05.05.2021).

[23] Etherscan, 2021, Erişim Adresi: https://etherscan.io/chartsync/chainarchive (Erişim Tarihi: 05.05.2021).

transfer işleminin ana zincirde kayıtlı olup olmadığına yani bir işlemin Bitcoin Blokzinciri'nin yansıttığı gerçekliğin parçası olup olmadığına ve dolayısıyla güvenilir olup olmadığında dair kontrolün daha kolay yapılması için kullanılan "Merkle Ağacı (İng. *Merkle Tree*)" yapısını incelemek faydalı olacaktır.

C. Düğümler Arası Farklılaşma

Bitcoin Blokzinciri'nde farklı yetkilere sahip farklı düğümler bulunmaktadır. Bitcoin Blokzinciri'nde işlem yapmak isteyen bir kişi doğrudan sisteme katılabileceği gibi üçüncü kişiler tarafından sağlanan hizmetleri de kullanabilir. Bitcoin Blokzinciri'nde iki temel düğüm tipi vardır: Bunlar tam düğümler (İng. *full node*) ve aynı zamanda. "Basitleştirilmiş Ödeme Doğrulaması (İng. *Simplified Payment Verification*)" ifadesinin baş harflerinden yola çıkarak SPV düğümler olarak da adlandırılan hafif düğümlerdir[24].

Tam düğümler ilgili blokzincirin tüm verilerini depolayıp madencilik[25], açık-özel anahtar çiftlerini depolama[26], sistemde dolaşım sağlama gibi işlemleri gerçekleştirebilirler. SPV düğümler ise blokzincirdeki verinin sadece bir kısmını indirirler ancak özel bir mekanizma aracılığıyla tüm veriyi indirmeden de yapıldığı iddia edilen bir Bitcoin transferinin gerçekten yapılıp yapılmadığını, söz konusu transfer işleminin Bitcoin Blokzinciri'nde kayıtlı olup olmadığını tespit edebilirler[27].

D. Merkle Ağacı (İng. *Merkle Tree*)

Yukarıda gösterilen genel blok yapısında bir işlemin blokzincir üzerinde olup olmadığının tespiti için o andan geriye gidilerek tüm blokların içerisine bakılması ve dolayısıyla böyle bir işlemin yapılması için de tüm blokzincir geçmişinin depolanması gerekir. Ancak Bitcoin bir ödeme

---

[24] NAKAMOTO, s. 5. BASHIR, s. 138.

[25] Bitcoin madenciliği hakkında açıklamalar için bkz. aşa. "i. Bitcoin Madenciliği".

[26] Cüzdan sağlayıcıların yaptığı işlem aslında budur. Anahtar çiftlerine ilişkin daha detaylı bilgi için bkz. aşa. "A. Açık ve Özel Anahtar Çiftleri".

[27] NAKAMOTO, s. 5. BASHIR, s. 138.

hizmeti olmak için tasarlandığından blokzincirin teknik doğasına aşina olmayan kişilerin de kolayca onaylama işlemi yapabilmesi adına özel bir yöntem kullanmaktadır. Bu yönteme göre ise her blok başlığında, genel bilgilerin yanında bir de o blokta yer alan işlemlerin ikili işlem ağaçlarına bölünmesi ve bunların iz üretme algoritmasına sokulması ile oluşturulan Merkle Kök İzi bilgisi de depolanmaktadır[28].

A'dan H'ye kadar olan harflerle ifade edilen 8 adet işlem barındıran bir blok için Merkle Ağacı ve Mercle Kök İzi şu şekilde hesaplanmaktadır:

Bu tablo neyi ifade etmektedir? Blokzincirlerde her bir blok aslında bir veri olduğu için işlemler de aslında birer veridir. Merkle Ağacı'nda her bir işlemin izi alınır ve kaydedilir. Sonrasında tek bir iz kalana kadar her basamakta elde edilen izler birleştirilerek bunların yeniden izleri alınır ve bu şekilde tek bir ize ulaşılır. Böyle her basamakta iki dala ayrılan veri yapılarına tersten bir ağaca benzediği için ikili veri ağacı anlamında İngilizcede *"binary tree"*, bu ağaçta yer alan her bir alt veri yapısına "düğüm (İng. *node*)", ağacın en altında yer alan ve daha alt bölümlere ayrılmayan düğümlere "yaprak (İng. *leaf*)", en tepede yer alan düğüme ise "kök (İng. *root*)" adı verilir. Merkle Ağacı'nın kökünde yer alan iz değeri, Bitcoin Blokzinciri'ndeki blok yapısını gösteren şekilden de görülebileceği üzere blok başlığına kaydedilir.

Peki Merkle Ağacı bir işlemin blokzincirde kayıtlı olup olmadığının tespitini nasıl kolaylaştırmaktadır? 8 işlemli tablodaki örneğimizden giderek D işleminin blokzincirde kayıtlı olup olmadığını tespit etmek istediğimizi varsayalım. Normalde Merkle Ağacı'nın olmadığı düz bir blok yapısında önce tüm bloklar içerisindeki tüm işlemlerin teker teker taranması gerekecekti. Ancak Merkle Tree sayesinde D işleminin blokzincirde kayıtlı olup olmadığının kontrol edilebilmesi için sadece 3 adet veriye ihtiyaç duyulacaktır: HC, HAB ve HEFGH. 8 işlem söz konusu olduğunda bir bilgisayarın 3 ya da 8 arama yapması arasında bir fark olmadığı düşünülebilir ancak işlem sayısı arttıkça Merkle Ağacı'nın kolaylaştırma etkisi de artacaktır. 16 işlemin bulunduğu bir blokta 4, 32 işlemin bulunduğu bir blokta 5, 1024 işlemin bulunduğu blokta ise sadece

[28] NAKAMOTO, s. 4. BASHIR, s. 95.

10 adet veriyle söz konusu işlemin blokzincirde bulunup bulunmadığına ilişkin tarama yapılabilecektir. Matematiksel bir formül vermek gerekirse Merkle Ağacında her kademede birim sayısı yarıya düşeceğinden X adet işlem içeren bir blokta verinin mevcut olup olmadığını tespit etmek için log2X adet veri gerekecektir.

Ancak Merkle Ağacı ile ilgili bazı noktalara dikkat etmek gerekmektedir. Öncelikle Merkle Ağacı bilinmeyen bir işlemin aranması için kullanılamaz veya işlem bilinse dahi işlemin içeriğine erişim imkanı vermez. Merkle Ağacı işlemi yaptığını iddia eden kişinin vereceği bilgiler kullanılarak işlemin onaylanması için kurgulanmış olup sadece ve sadece verilen bir işlemin söz konusu blokta bulunup bulunmadığının kontrolünü sağlar. Başka bir deyişle Merkle Ağacı'na dayanarak doğrulama yapabilmek için ağdaki diğer tam birimlerden veya söz konusu işlemin taraflarından yine bir miktar veri çekmek gerekecektir ancak açıklandığı üzere bu verinin miktarı normalde gerekenden az olacaktır.

Görüldüğü üzere Merkle Ağacı Bitcoin Blokzinciri'nde hafif düğümler de denilen onaylama amaçlı SPV düğümlerinin tüm blokzincir geçmişini depolamadan bir işlemin blokzincirde kayıtlı olup olmadığını öğrenmesi için etkili bir yöntemdir. Fakat aynı zamanda söz konusu düğümlerin diğer düğümlere bağlılığını artırdığı için de geçici de olsa bazı düğümlerin yanlış şekilde bilgilendirilmesi riskini beraberinde getirmektedir.

2. Merkezi Olmayan Yapı (İng. *Decentralization*) ve Uzlaşma (İng. *Consensus*)

A. Genel Olarak

Dağıtılmış yapı verinin birden fazla birimde depolanmasını ifade ederken merkezi olmayan yapı bu verinin kontrolünün tek bir kişi ya da grubun elinde bulunmamasını ifade eder. Veri birden fazla düğümde depolanmakla birlikte tutulan kaydın bir anlamının olması için bu deüğümlerin verinin doğruluğu ve yeni verileri hangi düğümün ekleyeceği üzerinde anlaşmaları gerekmektedir. Geleneksel sistemlerde bu işlem

güvenilir üçüncü kişi konumundaki aracı kuruluşlar tarafından yerine getirilmektedir[29].

Blokzincir çoğunlukla merkezi olmayan bir yapı olarak anlatılmaktadır. Bunun anlamı, bir blokzincir üzerinde depolanacak veriyi seçme ve yönetmede tek bir merkezi kişi ya da kuruluşun bulunmamasıdır[30]. Ancak bu özellik ilgili blokzincirin tasarımına göre değişebilecektir. Özel ve izne tabi blokzincirlerde yeni verilerin eklenmesi sadece bir gruba bırakılabilir ve bu blokzincirler merkezi özellikler gösterebilirler[31]. Blokzincir teknolojisinin bir işletme içerisinde yer alan iç işleyişe ilişkin verilerin depolanması veya aktarılması için bir altyapı olarak kullanılacağı ihtimallerde durum çoğunlukla bu şekilde olacaktır. Ancak açık ve izne tabi olmayan blokzincirlerde sistem herkesin katılımına açık olduğundan ve herkes işlem ekleme talebinde bulunabileceğinden gerçekten merkezi olmayan bir yapıdan söz edilebilir. Her iki durumda da düğümler arasından hangisinin bir sonraki veriyi ekleyeceğinin belirlenmesi gerekir ancak doğal olarak merkeziyetçi özellik azaldıkça karar verme mekanizmasına katılan düğüm sayısı artacağından sorunun çözümü zorlaşacaktır.

B. Uzlaşma Mekanizmaları

Uzlaşma protokolü bir blokzincirde zincire eklenecek yeni verinin ne olacağına kimin karar vereceğini belirleyen mekanizmayı ifade eder. Farklı blokzincirler farklı uzlaşma protokolleri kullanmaktadır. Bitcoin'in uzlaşma protokolü "iş ispatı (İng. *proof-of-work,* "PoW")" iken Ethereum'un uzlaşma protokolü başta PoW olarak belirlenmiş ancak sonradan "menfaat ispatı (İng. *proof-of-stake,* "PoS")" için değişiklik çalışmaları yapılmıştır. Uzlaşma protokolleri sadece düğümler arası anlaşmayı

---

[29] MAINELLI Michael/ALISTAIR M., "The Impact and Potential of Blockchain on the Securities Transaction Lifecycle", **SWIFT Institute**, 2015, s. 46; PAECH Philipp, "The Governance of Blockchain Financial Networks", **SSRN Electronic Journal**, C. S. 2016, s 7.

[30] PETERS Gareth William/PANAYI Efstathios/CHAPELLE Ariane, "Trends in Crypto-Currencies and Blockchain Technologies: A Monetary Theory and Regulation Perspective", **SSRN Electronic Journal**, C. S. 2015, s. 2.

[31] MAINELLI/ALISTAIR, SWIFT Institute, s. 56; PAECH, s. 12.

sağlamaz, ayrıca dağıtılmış yapının devamı için düğümlerin sisteme katılmalarına yönelik olarak onları motive edici öğeler içerir. Sistemin ayakta kalması ve düğümlerin bu sürece katılmaya devam etmesi için düğümler teşvik edilmelidir. Özellikle katılımcıların tüm toplum olabildiği açık ve izne tabi olmayan blokzincirlerde uzlaşma protokolleri; toplumu, sistemin varlığını devam ettirmeye teşvik edecek şekilde dizayn edilmelidir[32]. Aksi takdirde düğümler bu verileri depolamaya devam etmeyeceğinden sistemin sürdürülebilirliği sağlanamaz.

Bu bölümde bazı uzlaşma protokolleri incelenecektir. Genel akışa uygun olarak Bitcoin Blokzinciri'nde kullanılan uzlaşma protokolü olan PoW ile başlanacak sonra detaylara inilecektir.

a. İş İspatı (Proof-of-Work)

PoW Bitcoin Blokzinciri'nde kullanılan uzlaşma protokolüdür ve Bitcoin'i kendisinden önceki dijital ödeme aracı girişimlerinden ayırarak devrimsel olarak nitelendirilmesine sebep olan temel unsur olarak düşünülebilir. Bitcoin 2008 Ekonomik Krizi'nde geleneksel güvene ve aracı kurumlara dayalı sistemin çökmesine tepki olarak, kurumlara ve geleneksel aracı kuruluşlara güven yerine kriptografiye dayalı, kullanıcıdan kullanıcıya (İng. *peer-to-peer*) doğrudan işlem sağlayan bir ödeme sistemi olarak ortaya çıkmıştır. İşte PoW, Bitcoin'in geleneksel aracı kurumlar ve güven sistemi yerine kriptografiyi koymasını sağlayan mekanizmadır.

Peki PoW'a göre sisteme bir sonraki bloğu ekleyecek kişi nasıl belirlenmektedir? PoW temelde blok eklemek için belirli bir efor harcadığını, kaynak tükettiğini yani bir iş yaptığını ispat edebilen kişilerin yeni blok eklemesine izin veren bir uzlaşma protokolüdür[33]. Bunu ispat edecek olan verinin dijital hesaplamalar yoluyla aranması olayına "madencilik (İng. *mining*)", bu işi yapan sistem katılımcılarına da "madenci (İng. *miner*)" adı verilmektedir.

---

[32] EVANS David S., "Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms", **SSRN Electronic Journal**, C. S. 2014, s. 11.

[33] Cong & Ze (2018), p. 9.

b. Bitcoin Madenciliği

Uzlaşma protokolleri anlatılırken "blokzincirde madenciler bir hesap yapmaya çalışıyor", "madenciler yarışıyor" gibi ifadeler kullanılmaktadır. İşte bu başlık altında aslında bu sürekli konuşulan hesabın, oyunun, yarışmanın ne olduğu açıklanacaktır.

Öncelikle bütün blokzincirlerin kripto varlık barındırmak zorunda olmadığı ve kripto varlık barındıran blokzincirlerde dahi tüm kripto varlıkların madencilik temeline dayanmasının gerekmediği vurgulanması gereken önemli noktalardır.

Bitcoin Blokzinciri'nde bloklar birbirine kriptografik bir işlem aracılığıyla bağlılardır. Daha önce blokların birbirine iz değerleri aracılığıyla bağlı olduğu açıklanmıştı. Ancak bu yeterli olsaydı herkes iz üretim işlemini yaparak yeni bir blok önerebilirdi çünkü Bitcoin Blokzinciri'nde blok içerikleri herkesin ulaşabileceği bir şekilde depolanmaktadır. Bu da Bitcoin Blokzinciri'nin bütünlüğünü yok ederdi çünkü bir sonraki bloğun kimin eklediği bloğun arkasına ekleneceği yani hangi zincirin asıl zincir olduğu kolay kolay tespit edilemezdi. İşte bu noktada blok eklemek isteyen düğümleri eleyebilmek için devreye İngilizcede "*nonce*" adı verilen tek kullanımlık bir değer girmektedir.

aa. Zorluk Seviyesi (İng. *Difficulty Target*) ve Tek Kullanımlık Değer (İng. *Nonce*)

Madencilerin blok ekleme işlemleri nasıl gerçekleşmektedir? Öncelikle yeni eklenecek blokta yer alması gerektiği için halihazırda zincirde yer alan son bloğun izi üretilmektedir. Bunu takiben madenci yeni ekleyeceği blok içerisine koymak istediği işlemleri sistemdeki diğer birimlerden toplamakta ve bloğa yerleştirmektedir. Sonrasında ise bloklar arası bağlantıyı kurmak için madenciler blok başlığını iki defa iz üretim sürecine tabi tutmaktadır.

Bu noktada Bitcoin Blokzinciri'nde bir blok başlığı içerisinde yer alan verileri hatırlatmak yararlı olacaktır. Bitcoin Blokzinciri'nde blok başlığı altı adet veri içermektedir. Bunlar (**i**) blok versiyonu, (**ii**) bir önce-

ki bloğun izi, (**iii**) Merkle Kök İzi, (**iv**) zaman damgası, (**v**) zorluk hedefi ve (**vi**) tek kullanımlık bir değer. Bunlardan önceki blok izi ve Merkle Kök İzi'nin neler olduğu daha önce açıklanmıştı. Blok versiyonu, Bitcoin Blokzinciri'nin temel yazılımıyla alakalı bir husustur. Zaman damgası bloğun eklendiği ana göre değişiklik gösteren bir veridir. Zorluk hedefi ve tek kullanımlık değer ise madenciler arasındaki yarışın temel unsurlarıdır.

Madenciler arasındaki yarış temelde Bitcoin temel yazılımına kodlanmış olan matematiksal bir şartı sağlayan tek kullanımlık değeri bulma yarışıdır. Daha detaylı açıklamak gerekirse madenciler içeriğini belirledikleri ve zincire eklemek istedikleri bloğun başlığındaki tüm bu verilerle bir araya getirilerek iki defa iz üretim sürecine tabi tutulduğunda çıktı olarak hali hazırda zincirdeki son blok başlığında yer alan zorluk seviyesinden daha düşük değerde bir iz üretilmesini sağlayan bir tek kullanımlık değer bulmaya çalışmaktadırlar.

Burada vurgulanması gereken ilk husus tek kullanımlık değer haricindeki değerler toplandığında madencilerin artık içeriği değiştirmeyi bırakıp sadece anılan matematiksel şartı sağlayan değeri çalışmalarıdır. Esasen Bitcoin madenciliği denilen şey zorluk hedefi şartını sağlayacak olan bir tek kullanımlık değer aramaktan ibaret. Peki bu karışık gözüken hesap aslında pratikte nasıl yürümektedir? Bitcoin Blokzinciri'nin başlangıç bloğunu ele alarak bu hususu somutlaştırmaya çalışalım. Bitcoin Blokzinciri'nin ilk bloğunun iz değeri şudur[34]:

000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

Bu metnin yazımı esnasında son sırada bulunan bloğun iz değeri ise şudur[35]:

000000000000000000055a62160a0aa5792bce91d48402b529901f54b1cbac94

---

[34] https://www.blockchain.com/btc/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f (Erişim Tarihi: 05.05.2021).

[35] https://www.blockchain.com/btc/block/000000000000000000055a62160a0aa5792bce91d48402b529901f54b1cbac94 (Erişim Tarihi: 05.05.2021).

Görüldüğü üzere blokların iz değerlerinde başta belirli sayıda bir sıfır yer almaktadır. Zorluk seviyesi arttıkça iz değerinin küçülmesi, yani iz değerinin başında daha çok sıfır olması gerekmektedir. Madenciler işlem gücü harcayıp değerler deneyerek eklemek istedikleri blok izinin bir önceki blokta yer alan zorluk hedefinden küçük olmasını sağlayacak değeri aramaktadırlar.

Burada bir husus vurgulanmalıdır. Blok başlığında yer alan değerler tüm madenciler için aynı değildir. Zaman damgası değişmektedir. Blok içeriğinde yer alan işlemlere bakıldığında madencilerin sistemden topladıkları işlemler farklı olduğu için Merkle Kök İz değeri de değişecektir. Yani madenciler aslında sabit bir tek kullanımlık değeri değil, kendi topladıkları işlem setiyle bir araya geldiğinde istenen blok izini ortaya çıkaran ve dolayısıyla her madenciye göre farklı olacak bir değeri aramaktadırlar. Doğru tek kullanımlık değeri bulmanın bir formülü yoktur. SHA-256 algoritmasının doğası itibariyle doğru sonucu bulmak için yapılacak tek şey teker teker denemektir.

Peki zorluk hedefi neye göre değişmektedir? Sistemde ne kadar fazla madenci varsa o kadar fazla bilgisayar gücü kendi eklemek istediği için şartı sağlayan tek kullanımlık değeri aramaktadır. Zorluk hedefinin sabit kalması durumunda katılımcı arttıkça iki bloğun eklenmesi arasında geçen zaman azalacaktır. Bu istenen bir durum değildir zira çok hızlı blok eklenebilmesi ihtimali beraberinde blokzincirin daha önce açıklandığı üzere geriye dönük şekilde manipüle edilmesi riskini de getirmektedir. Bu riske mahal vermemek adına Bitcoin Blokzinciri'nin çekirdek kodu ile iki blok arasında geçen zamanı yaklaşık 10 dakika ile sınırlanmasını sağlayacak bir kısıt getirilmiştir. Eğer iki blok eklenmesi arasındaki zaman farkı 10 dakikanın altına inerse sistem otomatik olarak zorluk seviyesini yükseltecek, baştaki sıfır sayısı artacak ve bir sonraki blok için daha küçük iz değeri üretebilecek tek kullanımlık değerin aranması gerekecektir. Bunun tam tersi de geçerlidir. Eğer iki blok eklenmesi arasında geçen süre 10 dakikanın üzerine çıkarsa o zaman da zorluk hedefi düşecek ve

tekrardan 10 dakikaya yaklaşan bir sürede bir sonraki bloğun eklenmesi sağlanacaktır[36].

Dünyanın her tarafından güçlü donanımlarla ve hatta Bitcoin madenciliği için özel olarak yapılmış cihazlarla madencilik yapılması zorluk seviyesini çok yükseltmekte ve bir Bitcoin bloğu eklenmesi için harcanması gereken zamanla birlikte elektrik tüketimi de fazlasıyla artmaktadır. Öyle ki Bitcoin madenciliği için gereken yüksek elektrik tüketimi Bitcoin Blokzinciri'nin sürdürülebilirliği konusundan önemli tartışmalara sebep olmaktadır[37].

aaa. Teşvik Mekanizması

Peki madenciler neden bu kadar yüksek oranda bilgisayar gücünü blok eklemek için harcamaya razı olurlar? Burada da Bitcoin'in teşvik mekanizması devreye girmektedir. Blok ekleme sürecinde bloğa eklenecek işlemlerin madenciler tarafından toplandığı belirtilmişti. Bu noktada madencilerin bir bloğa ekleyecekleri işlemleri seçerken tamamen keyfi davranmadıkları, bazı kriterleri dikkate aldıkları vurgulanmalıdır. Kullanıcılar madencilere sistem üzerinden bir işlem gönderirken aynı zamanda madencileri o işlemi sonraki bloğa eklemeye teşvik etmek adına bir mik-

[36] Ethereum'un PoW sisteminde bu süre 10 saniye olarak belirlenmiştir. Eğer iki blok arasındaki süre 10 saniye altına düşerse zorluk seviyesi artırılır, 10-20 saniye arasındaysa zorluk seviyesi sabit kalır, 20 saniye üzerindeyse zorluk seviyesi düşürülür. Ethereum'un PoW'unda ayrıca işlem süresinden bağımsız olarak zorluğun blok sayısına bağlı olarak artırılacağı öngörülmüştür. Bu sayede bir noktada Ethereum'da madencilik imkansız denecek kadar zorlaşacak ve tüm madencilerin PoS'a geçişi hızlanacaktı. Madencilik faaliyeti üzerindeki etkisi sebebiyle buna "saatli zorluk bombası (İng. *difficulty time bomb*)" denmektedir. Ancak Ethereum'un PoS'a geçişi geciktikçe protokol değişikliği içeren sert çatallanmalar (İng. "*hard fork*") aracılığıyla bu etki de geciktirilmiştir. Bkz. BASHIR, s. 244.

[37] Bitcoin madenciliği için tüketilen elektrik miktarının 170'ten fazla ülkenin elektrik tüketiminden fazla olduğuna dair bir çalışma için bkz. https://powercompare.co.uk/bitcoin-mining-electricity-map/ (Erişim Tarihi: 05.05.2021). Bitcoin elektrik tüketimi ile ülkelerin elektrik tüketimini karşılaştıran bir başka çalışma ve tablo için bkz. https://cbeci.org/cbeci/comparisons (Erişim Tarihi: 05.05.2021). Diğer yandan Bitcoin madenciliği için gereken enerjinin geleneksel sistemlerde işlemleri güvenli şekilde yapabilmek için harcanan aracılık, sermaye ve işçilik maliyetleri yanında düşük kaldığı yönünde bir görüş için bkz. CATALINI Christian/GANS Joshua S., "Some Simple Economics of the Blockchain", **SSRN Electronic Journal**, C. S. 2016, s. 6.

tar komisyon da belirleyebilmektedirler. Bunu da işlemin girdi ve çıktı bakiyeleri arasında bir fark bırakarak yapmaktadırlar. İlgilileri tarafından komisyonu yüksek olarak belirlenen işlemler doğal olarak madenciler tarafından öncelikli şekilde bloğa eklenecektir. Bu işlem bazlı bir teşvik mekanizması olup Bitcoin Blokzinciri'nde işlem yapılmaya devam edildiği sürece madencileri sistemi çalıştırmaya teşvik edebilecektir.

Bitcoin Blokzinciri'nde bir de blok bazlı teşvik mekanizması mevcuttur. Normalde bir Bitcoin işleminde gönderici ve alıcı adresleri bulunmaktadır. Bu sayede her Bitcoin'in o zamana kadar transfer edildiği adreslerin takibi yapılabilmektedir. Ancak her yeni blokta gönderici adresi olmayan özel bir işlem mevcuttur. Bu işlemin kaynağı Bitcoin Blokzinciri'nin çekirdek kodudur. Buna ödül işlemi ya da İngilizce olarak "*coinbase transaction*" denmektedir. Madenciler zincire eklemek istedikleri bloğu oluştururken bu işlemin alıcısını istedikleri gibi tayin edebilmektedirler[38]. Bu işlemde belirli bir sayıda Bitcoin bağlı bulunmaktadır. İşte madencileri sistemi açık tutmaya ve kaynak tüketmeye iten asıl unsur bu ödül mekanizmasıdır.

Bitcoin blok ödülü ilk başta 50 Bitcoin olarak belirlenmiştir. Ancak yine Bitcoin protokolünde yer alan bir kurala göre her 210.000 blokta bu ödül yarıya düşmektedir. Şu ana kadar üç yarılanma geride kalmış ve mevcut Bitcoin ödülü blok başına 6.25 Bitcoin'e kadar düşmüştür. Burada basit bir hesap yapmak mümkündür. Daha önce açıklandığı üzere Bitcoin protokolü her iki blok arasındaki süreyi ortalama 10 dakika tutmak üzere tasarlanmıştır. 210.000 blokta bir yarılanma olmaktadır. Bu da toplamda bir yarılanma için yaklaşık 2.100.000 dakika geçmesi gerektiğini göstermektedir. Bu süre 35.000 saate, 1458 güne ve dolayısıyla yaklaşık dört seneye tekabül etmektedir. Bitcoin ödülünün ilk yarılanması Kasım 2012'de, ikincisi Temmuz 2016'da üçüncü yarılanması ise Mayıs 2020'de gerçekleşmiştir. Bu hesaba göre bir sonraki yarılanma da Şubat-Mayıs 2024 civarında gerçekleşecektir.

---

[38] ROHR Jonathan/WRIGHT Aaron, "Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets", **SSRN Electronic Journal**, C. S. 2017, s. 9; WERBACH Kevin D., "Trust, But Verify: Why the Blockchain Needs the Law", **SSRN Electronic Journal**, C. S. 2017, s. 15.

Bitcoin blok ödülünün yarılanması başka bir soruyu daha gündeme getirmektedir. Ödülün sürekli yarılanıyor olması ödülün hiçbir zaman sıfır olmayacağı ancak kısa sürede sıfıra çok yaklaşacağı anlamına gelmektedir. Bitcoin ödülü dört yıl gibi kısa bir sürede yarılanıyorsa bu ödül kabaca bir hesapla 2024'te 3.125, 2028'de 1.5625 2032'de 0.78125 Bitcoin olacaktır. Ödül bu kadar azaldığında ise madencilerin sistemi çalışır ve güvenli tutmak için yeterli motivasyonunun kalıp kalmayacağı zamanla cevabını göreceğimiz önemli bir sorudur. Bitcoin değerindeki artışın bir süre daha yarılanmanın yaratacağı etkiyi karşılayacağı söylenebilir.

Burada bir hususa daha değinilmesi yerinde olacaktır. Yarılanmalar ile yeni bloktan elde edilecek ödül miktarı hiçbir zaman sıfıra inmeyecek olsa da yeni Bitcoin eklenmesi yine Bitcoin Blokzinciri'nin çekirdek kodunda yapılan bir ayar sebebiyle belli bir noktada duracaktır. Bu sayı 21.000.000 olarak belirlenmiştir[39]. Bu bölümün yazıldığı tarih itibariyle 19 milyona yakın Bitcoin'in halihazırda madenciler tarafından kazılmış olduğu[40], 21 milyonluk sınıra ise 2140 yılında ulaşılacağı[41] belirtilmektedir.

bbb. Yeni Bloğun Eklenmesi

Madenci zorluk seviyesini sağlayan bir tek kullanımlık değer bulduğunda hazırladığı bloğun ana zincire eklenmesini isteyecektir. Bunun için öncelikle blok bulduğuna dair haberi ağdali diğer düğümlere yayacaktır. Bir madenci tarafından gönderilen bloğun zorluk hedefini sağlayıp sağlamadığını kontrol etmek düğümler için kolay bir işlem olup sadece birkaç

---

[39] Toplam Bitcoin miktarının neden 21.000.000 adet ile sınırlandığı açık değildir. Bitcoin'in yaratıcısı Satashi Nakamato'nun her bir Bitcoin'in dünya ekonomisindeki belli parasal değerlerin belirli bir kısmına denk gelmesini istediği için bu sayıyı sınır olarak belirlemiş olabileceği yönünde açıklamalar ve farklı ihtimalleri değerlendiren bir çalışma için bkz. https://decrypt.co/34876/why-is-bitcoins-supply-limit-set-to-21-million (Erişim Tarihi: 07.05.2021).

[40] Bkz. https://www.buybitcoinworldwide.com/how-many-bitcoins-are-there/#:~:text=How%20Many%20Bitcoins%20Are%20There%20Now%20in%20Circulation%3F,adds%206.25%20bitcoins%20into%20circulation. (Erişim Tarihi: 07.05.2021).

[41] Bkz. https://decrypt.co/33124/what-will-happen-to-bitcoin-after-all-21-million-are-mined (Erişim Tarihi: 07.05.2021).

defa iz üretme fonksiyonu kullanılmasını gerektirmektedir. Diğer düğümler bu bloğun iz değerini kontrol edip içerisinde yer alan işlemlerin protokolde yer alan bazı kurallara uygunluğunu test ettikten sonra bloğu kabul ederek kendi kayıtlarını bu yeni bloğu da içerecek şekilde güncellerler ve artık bu son eklenen bloğun arkasına gelebilecek yeni blok için sil baştan tek kullanımlık değer arayışına girerler. Zincire yeni bir blok eklendiği ve bunun izi de artık hesaplamalara dahil olduğu için madenciler tek kullanımlık değer arayışlarını sıfırdan başlatmak zorundadırlar.

Peki diğer birimler bir blok üzerinde çalışırken neden başkası tarafından bulunan bir bloğu eklemeyi kabul ederler? Aslında ağdaki diğer birimler kendilerine gönderilen yeni blok bilgilerini kabul edip etmemekte özgürdürler. Yeni gönderilen blok gerçekten zorluk hedefini sağlıyorsa, bloğa eklenen işlemlerle ilgili hiçbir sıkıntı yoksa bile birimler bu bloğu eklemeyi reddedebilirler. Madenciler buradaki kararı neye göre vermektedirler?

Blokzincirler aslında düz ve tek bir zincirden oluşmazlar. Bir zincir, herhangi bir noktada farklı dallara (İng. *fork*) ayrılarak devam edebilir. Bu dallar nasıl oluşmaktadır? Toplam uzunluğu 45 blok olan bir blokzinciri örnek alarak inceleyelim:

46 numaralı blok madenci A tarafından sisteme gönderilir. Madenci B ve madenci C A tarafından gönderilen bu bloğu alıp inceleyerek kayıtlarını güncellerler. Bu durumda A, B ve C'nin blokzincir kopyalarında 46 blok bulunmaktadır, 47. blok üzerinde çalışmaya başlarlar Ancak blokzincir doğrudan kullanıcılar arası haberleşmeye dayalı olduğundan A'nın blok bulduğu haberi tüm düğümlere aynı anda gönderilmez. Bu esnada düşük de olsa muhtemel bir durum gerçekleşir ve henüz A'nın gönderdiği bloktan haberdar olmayan madenci D, neredeyse A ile eşzamanlı olarak kendi 45 blokluk zinciri için gerekli tek kullanımlık değeri bularak farklı bir 46. blok ekler, bunu diğer düğümlere gönderir. Madenci E ve madenci F de D'den gelen bloğu onaylayıp kendi kopyalarını güncelleyerek farklı bir 47.blok üzerinde çalışmaya başlarlar. Bu durumda A, B, C ile D, E, F'nin tuttuğu blokzincir kopyaları aynı değildir, diğer bir deyişle tutarlı-

lık yoktur. Bu iki farklı kopya 45.bloktan itibaren çatallanmış ve iki dala bölünmüştür.

Peki böyle bir durumda ne yapılacaktır? Doğal olarak burada sistemin hangi dal üzerinden devam edeceğinin belirlenmesi gerekir. Topluluk istediği daldan ve hatta isterlerse ikisinden de devam etmekte özgürdür ancak sistemin protokol bazında bir tercih yapması sistemin böyle durumlarda kitlenmesini önlemek açısından önem arz etmektedir. Bitcoin Blokzinciri'nde bu tercih en uzun zincir lehine yapılmıştır, en uzun zincirde yer alan bloklardaki veriler "gerçek" olarak kabul edilmektedir[42]. Protokol bu şekilde olduğu için de blok ödüllerini alma odaklı çalışan madenciler kaynaklarını boşa harcamamak adına en uzun zinciri takip etme eğilimi gösterecektir. Zira madenciler yeni blok içerisindeki ödül Bitcoin'i ancak ekledikleri ana zincirdeyse bir değer taşıyacaktır. Bu sebeple genel olarak madenciler kendilerine gönderilen yeni blokları kimin bulduğuyla ilgilenmemektedirler. Sadece yeni bloğun eklenmesi için gerekli olan kontrol ve doğrulama işlemlerini yapıp sonraki blok üzerinde çalışmaya başlamaktadırlar.

ccc. Saldırılar

Bir önceki başlıkta anlatılan mekanizma ağda yer alan düğümlerin kendilerinden beklendiği şekilde davranacağı varsayımına dayalıdır ancak gerçekte durum her zaman bu şekilde olmayabilir. Bazen ayrık davranan ve özel durumların ortaya çıkmasına neden olan madencilerle baş etmek gerekebilecektir. İşte bu bölümde bu özel durumlardan biri olan saldırılar üzerinde kısaca durulacaktır. Diğer bir özel durum olan ve aslında kısaca bir önceki bölümde değinilen dallara ayrılma ihtimali ise daha ileride değiştirilemezlik özelliği incelerken açıklanacaktır. Bitcoin Blokzinciri'nin temel amacı ödeme sistemi olarak kullanılması amacıyla bağlantılı olarak üç önemli saldırı tipi söz konusu olabilir.

---

[42] NAKAMOTO, , s. 3.

(a) Çifte Harcama

Çifte harcama aslında bir saldırıyı değil sonucu ifade eder ancak önemi itibariyle ayrı bir incelemeyi hak etmektedir çünkü sadece Bitcoin'in değil tüm dijital ödeme sistemlerinin yaşayabileceği önemli bir sorundur. Kayıtların merkezi olarak tutulmadığı blokzincir gibi dağıtılmış yapılarda ise bu sorun özel bir önem arz etmektedir çünkü merkezi bir kayıt ya da kurum olmaksızın sistemi çifte harcama yapmak için yanıltmaya çalışan aktörlerin kontrol edilmesi gereksinimi doğacaktır.

Bitcoin ekosisteminde geleneksel finansal sistemlerdeki güven ve aracı kurumlar PoW ile değiştirilmektedir. Bitcoin Blokzinciri'nin çifte harcama riskine karşı cevabı da yine PoW'da yatmaktadır. Bitcoin Blokzinciri'nde geçmişe yönelik tüm işlem kayıtları açıktır. Madenciler yeni bir blokta bulunacak işlemleri seçerken veya yeni bulunmuş bir bloğu onaylarken işlemleri otomatik bir testten geçirir ve eğer ana zincirde daha önce transfer edilmiş bir Bitcoin'i yeniden transfer etmeye çalışan bir işlem varsa bu işlemleri reddederler.

Ancak PoW'a rağmen istisnai bir ihtimalde Bitcoin Blokzinciri'nde çifte harcama durumunun gerçekleşmesi mümkün olabilecektir:

Madenci A toplam uzunluğu 12 blok olan bir blokzincir üzerinde madencilik yapmaktadır. A 13.sıraya gelecek bir blok bulur ve bu bloğun içerisine B'ye 1 Bitcoin gönderdiği bir işlem ekler. A, bloğu bulduğunda bunu sistemdeki diğer düğümlere gönderecektir ancak tüm düğümler bu mesajı aynı anda almayacaktır. Bundan hemen sonra A aynı Bitcoin'i C'ye gönderdiği başka bir işlemi yeni bir blok içerisine koyar, ancak bunu 14.blok olarak değil 13.blok olarak eklemek için yeniden faaliyete başlar. A, daha önce bulduğu bloğun arkasına yeni bir blok eklenmeden ikinci bir blok bulmayı başarırsa -ki bu daha önce bahsedildiği üzere işlem dinamikleri sebebiyle çok kolay karşımıza çıkabilecek bir durum değildir- 12.bloktan itibaren iki dala ayrılan bir blokzincir söz konusu olacaktır. İki dalın da 13.bloğunda A'nın aynı Bitcoin'i gönderdiği işlem bulunacaktır. Ancak dallardan birinde bu Bitcoin B'ye, diğerinde C'ye gönderilmiş olacaktır.

A'nın bu bloğu bulmasına rağmen B haricinde kimseye göndermemesi ya da geç göndermesi de mümkündür. Yani A daha önce kendi bulduğu bloğun yayılmasını engelleyerek kendi Bitcoin'ini iki defa kullanmaya da çalışabilir.

Kural olarak madencilerin en uzun zinciri tercih edeceklerdir ancak burada aynı uzunlukta iki farklı zincir olduğundan bir karışıklık oluşması mümkündür. Bu sorun nasıl çözülecektir? Burada katı bir kurala dayanmayan davranışsal bir çözüm kabul edilmiştir. Bitcoin Blokzinciri'nde bir işlem ancak içinde bulunduğu blok üzerine altı blok daha eklenmişse geçerli şekilde gerçekleşmiş olarak kabul edilmektedir. Bu saygı sabit bir koda dayanmayıp keyfi olarak belirlenmiş bir sayıdır. İşlemin muhatabı daha az sayıda onayla da yetinebilecektir. Her eklenen yeni blok o işlemlerin geçmişe doğru kontrol edilmesi ve bir kez daha onaylanması anlamına gelmektedir. Bu durumda çifte harcama yapılabilmesi için diğer madenciler yeni bir blok bulmadan ilgili işlemin bulunduğu bloğun içeriğini değiştirebilmek ve sistemdeki diğer birimlere kabul ettirebilmek adına altı blok bulunması gerekecektir. Bunu başarmak teorik olarak ilk denenen tek kullanımlık değerin doğru çıkması ihtimalinde mümkün olsa da pratik açıdan bunun gerçekleşmesi ihtimali imkansıza yakındır.

(b) %51 Saldırısı

Daha önce açıklandığı üzere PoW sisteminde hangi verinin zincire ekleneceği ve gerçek kabul edileceği madenciler tarafından belirlenmektedir. Madenciler seçilmiş, özel nitelikleri olan bir grup değildir. Gerekli donanıma sahip herkes sisteme girerek madencilik faaliyetine girişebilecektir. Madenciler arasında dürüst olmayan aktörler de çıkabilecektir. PoW, herhangi bir anda sistemde bulunan madencilerin belirli bir oranının üzerindekilerinin dürüst olduğu varsayımından hareket etmektedir. Bu durum Bitcoin manifestosunda şu şekilde ifade edilmiştir:

"Sistem, dürüst birimler kolektif şekilde herhangi bir saldırgan gruptan daha fazla işlemci gücü kontrol ettiği sürece güvenlidir." [43]

[43] "The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.", bkz. NAKAMOTO, , s. 1.

Buradan hareketle, sistemdeki diğer düğümlerin durumundan bağımsız olarak sistemdeki işlemci gücünün %50'sinden fazlasını kontrol eden bir kişi ya da grup aslında istediği işlemleri, kurallara uygun olup olmadığına bakmaksızın, ana zincire ekleyebilecektir.

Burada yine terminolojik bir düzeltmeye ihtiyaç vardır. %51 saldırısı iki sebeple yanıltıcı olabilecek bir ifadedir. İlk olarak burada mantıksal bir hata mevcuttur. %51 saldırısı ile anlatılmak istenen şey aslında işlemci gücünün %51'ini değil, %50'sinden fazlasını ele geçirme durumudur. Bu hata hukukçuların yeter sayılara ilişkin hukuki düzenlemelerden alışık olduğu bir durumdur. Burada %50+1 veya %50'den fazla ifadelerinden biri tercih edilmelidir. İkinci olarak bir saldırganın bu şekilde başarılı olması için toplam işlemci gücünün %50'sinden fazlasını kontrol etmesi gerekmez. Herhangi bir saldırgan aktör ya da topluluğun, dürüst düğümlerin kontrolündeki toplam işlemci gücünü geçmesi saldırının başarılı olması için yeterli olabilecektir[44].

%51 saldırısının gerçekleştirilmesi teorik olarak mümkündür. Ancak özellikle Bitcoin gibi yaygın şekilde kullanılan sistemlerde dünyanın her tarafından çok fazla düğüm sisteme dahil olduğu için bunların yarısıyla bir araya gelerek anlaşmak pratik ve ekonomik sebeplerle mümkün gözükmemektedir. Bir yazara göre Bitcoin sistemine başarılı bir %51 saldırısı gerçekleştirmek için gereken güç dünyanın en güçlü süper bilgisayarlarının yüzlercesinin durmaksızın çalıştırılmasıyla ancak elde edilebilecektir[45].

(c) Sybil Saldırısı

Sybil saldırısı saldırganların mevcut düğümlerle anlaşarak kontrol sağlamak yerine sistemde çok sayıda kimlik ve düğüm oluşturarak faaliyet göstermelerini ve bu sayede kontrolü ele geçirmeye çalışmalarını ifade eder. Çoklu kimlik oluşturma yoluyla gerçekleşecek saldırılara karşı PoW mekanizmaları dayanıklıdır çünkü önemli olan sistemde kaç adet

---

[44] ATZORI Marcella, "Blockchain Technology and Decentralized Governance: Is the State Still Necessary?", **SSRN Electronic Journal**, C. S. 2015, s. 17.

[45] WERBACH, s. 24.

aktörün olduğu değil sistemdeki işlemci gücünün ne kadarının kontrol edildiğidir[46].

c. Menfaat İspatı (İng. *Proof of Stake*) ve Türevleri

PoW'da zincire yeni bilgi ekleyecek kişinin seçiminde belirli bir iş (elektrik harcama ve hesaplama yapma gibi) yapmış olma ve bunun delilini sunma yöntemi benimsenmişken PoS'ta ise yeni eklenecek bloğu seçme ve onaylama işlemi sistemde ekonomik menfaati olan kişilere bırakılmıştır. Buradaki temel mantık sistemde ekonomik menfaati olan kişinin sistemin doğru şekilde işlemesinde de menfaatinin olduğu ve bunu kaybetmemek için dürüst davranacağı varsayımına dayanmaktadır.

PoS sistemlerinde yeni blok içeriğini belirlemek ve onaylamak için bir düğüm seçilir ve bu düğümün seçiminde farklı menfaat ölçütleri dikkate alınır. PoS'un farklı şekillerde uygulanması mümkündür ve ekonomik menfaatin ne olduğu uygulama bazında değişebilir. Genel olarak buradaki menfaat sistemde kullanılan kripto varlığa sahip olmaktır ve sahip oldukları kripto varlık miktarına oranla düğümler için madencilik işlemi kolaylaştırılır[47].

Belirli miktar kripto varlık elde bulundurmak haricinde protokol uzun süredir kripto varlık elde bulunduranların blok belirlemesi (İng. *proof of coinage*), belirli bir miktar kripto varlığı bir süre dondurmak karşılığında blok belirleme yetkisi verilmesi (İng. *proof of deposit*), kripto varlıkların yok edilmesi karşılığı blok eklenmesi (İng. *proof of burn*) veya eklenecek bloğun onaylanmasının sistemde menfaati olan birimlerin oylamasına bırakılması (İng. *delegated proof of stake*) şekillerinde de kurgulanabilir[48].

PoW ile kıyaslandığında PoS'un iki temel avantajı olduğu söylenebilir. Öncelikle kripto varlıklar işlemci gücüne göre daha dağınık olduğun-

---

[46] WERBACH, s. 12.

[47] CONG Lin William/HE Zhiguo/ZHENG Jingtao, "Blockchain Disruption and Smart Contracts", **SSRN Electronic Journal**, C. S. 2017, s. 9; BASHIR, s. 166.

[48] CONG/HE/ZHENG, s. 9; BASHIR, s. 166.

dan belirli oranda kripto varlığı toplamak işlemci gücünü tek bir odakta toplamaya göre daha zor olacaktır. İkinci olarak PoS madencilik işlemini kolaylaştırarak yüksek enerji ihtiyacını ortadan kaldırmaktadır[49].

PoS'un farklı uygulamaları farklı blokzincirlerde kullanılmaktadır. Örneğin Peercoin, kripto varlığın elde bulundurulma süresine dayalı bir uzlaşma protokolü kullanmaktadır[50]. Bitshares[51] ve Tezos[52] sistemdeki menfaat sahibi düğümlerin oylamasına dayalı bir uzlaşma protokolü kullanmaktadır. Nextcoin[53] daha fazla kripto varlığa sahip olanların blok ekleme ihtimalini artıran bir PoS kullanmaktadır. Ayrıca Ethereum da başta PoW kullanmakla birlikte PoS'a dönüşüm için bir takvimle beraber ortaya çıkmıştır ve şu an dönüşüm sürecindedir[54].

d. Geçen Süre İspatı (*ing. Proof of Elapsed Time,* "PoET")

PoET görece yeni bir uzlaşma protokolüdür. Intel tarafından *Sawtooth Lake* projesi için özel olarak geliştirilmiştir ve aslında PoW'un bir varyasyonu gibidir. PoET'te dikkate alınan ispat unsuru ise bir düğümün bekleme süresidir[55]. Bu sayede PoW'daki gibi yüksek enerjiye ihtiyaç duyulmamaktadır. Ancak bekleme süresinin doğru şekilde bildirilebilmesi için yine Intel tarafından geliştirilen özel bir donanım protokolü

---

[49] BASHIR, s. 166.

[50] Peercoin uzlaşma protokolü hakkında bkz. https://university.peercoin.net/#/9-peercoin-proof-of-stake-consensus (Erişim Tarihi: 05.05.2021).

[51] Bitshare uzlaşma protokolü hakkında bkz. https://bitshareshub.io/delegated-proof-of-stake-consensus/ (Erişim Tarihi: 05.05.2021).

[52] Tezos uzlaşma protokolü hakkında bkz. https://tezos.gitlab.io/008/proof_of_stake.html (Erişim Tarihi: 05.05.2021).

[53] Nextcoin uzlaşma protokolü hakkında bkz. https://nxtwiki.org/wiki/Whitepaper:Nxt#Nxt.E2.80.99s_Proof_of_Stake_Model (Erişim Tarihi: 05.05.2021).

[54] Bu dönüşüm bir anda değil, zaman içerisinde gerçekleşecek şekilde kurgulanmıştır. Bunun ilk adımı 01.12.2020'de atılmıştır. Bu dönüşüm süreci, etkileri ve değerlendirmeler için bkz. https://www.gemini.com/cryptopedia/what-is-ethereum-pos-proof-of-stake#section-ethereum-2-0-progress (Erişim Tarihi: 05.05.2021).

[55] *Sawtooth Lake* projesinin uzlaşma protokolü hakkında ayrıca bkz. https://sawtooth.hyperledger.org/docs/core/nightly/0-8/introduction.html (Erişim Tarihi: 05.05.2021).

olan SGX kullanılmaktadır[56]. Intel'in SGX sistemi ile PoET'in güvenli ve rastgele bir şekilde bir sonraki birimi seçmesi güvence altına alınmaya çalışılmıştır[57].

e. Seçilmiş Uzlaşma Protokolü (*ing. Federated Consensus, Federated Byzantine Agreement*)

Seçilmiş uzlaşma protokolünde ise sadece güvenilir birimler tarafından gönderilen bloklar kabul edilir ancak sistemin tasarımına göre güvenilir birimlerin nasıl seçileceği meselesi değişebilir[58]. Bu yöntem Ripple[59] ve Stellar[60] tarafından kullanılmaktadır.

3. Değiştirilemezlik (*Immutability*)

Değiştirilemezlik, bir blokzincirde yer alan verilerin değiştirilememesini, sadece yeni veriler eklenebilmesini ifade etmektedir[61]. Blokzincir teknolojisinin temelinde kayıtların tamamının tutulması ve ekleme yapılması söz konusu olduğu için değişiklik yapılabilmesi istenen bir durum değildir. Başka bir deyişle değiştirilemezliğin sağlanabilmesi, blokzincir teknolojisinin üzerine yüklenen misyonları yerine getirebilmesi açısından önem arz etmektedir. Ancak yaygın şekilde ifade edilenin aksine blokzincirler tam anlamıyla değiştirilemez değildir.

Daha önce detaylı şekilde anlatıldığı üzere blokzincir teknolojisinde her bir blokta kendisinden önce gelen bloğa ait iz değeri depolanır ve yeni bir blok eklenirken bu bağlantılar kontrol edilir. Bir blokta yer alan bir işlemin değiştirilmesi demek o bloğa ve ondan sonra gelen tüm bloklara

---

[56] BASHIR, s. 370.

[57] BASHIR, s. 29.

[58] BASHIR, s. 30.

[59] Ripple uzlaşma protokolü hakkında bkz. https://ripple.com/files/ripple_consensus_whitepaper.pdf (Erişim Tarihi: 05.05.2021).

[60] Steller uzlaşma protokolü hakkında bkz. https://www.stellar.org/papers/stellar-consensus-protocol.pdf (Erişim Tarihi: 05.05.2021).

[61] WALCH Angela, "Open-Source Operational Risk: Should Public Blockchains Serve as Financial Market Infrastructures?", **Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2** (Editör: 2018, s. 4.

ait iz değerini değiştirmek demektir. Dolayısıyla bir bloktaki bir işlemin değiştirilmesi için ondan sonraki tüm blokların değiştirilmesi gerekecektir. Bu da her yeni blok eklendiğinde, mevcut bilgilerin değiştirilmesinin daha da zorlaştığı anlamına gelecektir[62].

Bir blokzincirin durumuna ilişkin kararı blokzincirin temelinde yer alan uzlaşma protokolünün kuralları da dikkate alarak düğümlerin belirli bir çoğunluğu vermektedir. Çoğunluğa dayalı sistemlerde yeterli sayıda düğüm bir araya gelerek zincirin durumunda bazı değişiklikler yapabilirler. Ancak bu değişiklikler bir blok içerisindeki spesifik bir işlemin değişikliği şeklinde olmaz çünkü iz değeri bağlantısı sebebiyle böyle bir değişiklik sonraki tüm blokların yeniden eklenmesini ve bunun için kaynak harcanmasını gerektirecektir.

Peki o zaman nasıl bir değişiklik yapılabilir? Zincirin geçmişinden bir bloğa dönülerek o bloktan itibaren paralel bir gerçeklik yaratılması veya geriye gitmeye gerek olmaksızın mevcut bloktan itibaren zincirin bölünmesine, iki zincir halinde devam edilmesine karar verilmesi mümkündür. İki durumda da ana zincirin dallara ayrılması söz konusudur. Şimdi dallara ayrılma senaryosu incelenecektir.

A. Dallara Bölünme (İng. *Forks*)

Blokzincirler yapıları itibariyle bölünmeye müsaittir. Sistemdeki bir düğüm kendi depoladığı blokzincir versiyonunda belirli bir bloğa dönerek o andan itibaren öncekine göre farklı işlemleri zincire ekleyebilir ancak bunu sistemdeki diğer düğümlere kabul ettiremeyeceği için bu bilgiler ana zincire eklenmez. Uzlaşma protokolleri sistemde belirli oranın üzerinde düğümün zincirin tek bir versiyonu üzerinde uzlaşmasını ve bunun o blokzincir açısından gerçek kabul edilmesini sağlar. Bitcoin örneğinde daha önce açıklandığı üzere bu en uzun zincirdir.

---

[62] Bkz. ASLANTAŞ ATEŞ Burcu, "Kripto Para Birimleri, Bitcoin ve Muhasebesi", **Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, C. 7, S. 1, 2016, s. 356. Yazar Bitcoin Blokzinciri'nden bahsederken değişiklik için daha önceki işlemleri yapan kişilerin hesabına girilmesi gerektiğini belirtmiştir. Bitcoin Blokzinciri'nde böyle bir değişiklik şekli yoktur.

Fakat bazı önemli fikir ayrılıklarında düğümlerin tamamını aynı zinciri izlemeye devam etmeye ikna etmek kolay olmayabilir ve farklı gruplar farklı bir işlem zincirini takip etmeyi tercih edebilir. İşte bu durumlarda bir bölünmeden söz edilmektedir[63]. Dallar esasen blokzincir teknolojisinin değiştirilemezliğinin istisnasını teşkil etmektedir. Her bir yeni dal ana zincirden farklı ve bir grup birim tarafından takip edilecek alternatif bir zincir oluşturulması anlamına gelmektedir.

Temelde iki tip bölünme söz konusu olabilir. Eğer bölünme sonucunda bir dalda kalan düğümler diğer dala geçen düğümlerce üretilen verileri de okuyabiliyorlarsa, bu durumda yumuşak bölünmeden (İng. *soft fork*) söz edilir. Yumuşak bölünmelerde düğümlerin veri okuma sorunu olmadığından uzun vadede zincirde dallara bölünme gerçekleşmez ve daha fazla işlem gücüne sahip ekibin takip ettiği dal zamanla diğerine galip gelir. Ancak bölünme sonucunda bir dalda kalan düğümler yeni dala geçen düğümlerce üretilen verileri okuyamıyorlarsa o zaman sert bölünmeden (*hard fork*) söz edilir[64]. Sert bölünmeler tamamen alternatif bir dal yaratır, bu dal zamanla kendisi bağımsız bir işlem geçmişine sahip ana zincire dönüşebilir ve bu durum düğüm sayılarını etkilediği için çok istenen bir durum değildir.

Peki bölünmeler neden gerçekleşir? Bunun anlaşılabilmesi için önemli blokzincirlerin geçirdiği temel bölünmeler incelenecektir.

a. Bitcoin Blokzinciri Bölünmeleri

Normalde bir blokzincirdeki tüm düğümler aynı temel yazılım üzerinde işlem yapmaktadırlar. Bu yazılımda yapılacak önemli bir değişikliğin geçerli olması için sistemdeki düğümlerin önemli bir çoğunluğu tarafından kabul edilmesi gerekecektir. Belirli bir çoğunluk tarafından bu değişiklik kabul edildiğinde geriye kalan düğümlerin de bir karar vermesi gerekir. Bu değişikliği kabul etmeyen düğümler -tabi ki değişikliğin önemine göre- sistemde var olmayı sürdüremeyebilirler çünkü yeni özellikler bu değişikliği kabul etmeyen düğümlerce çalıştırılamayabilir. Ancak

[63] WALCH, ss. 259-260.

[64] BASHIR, s. 130.

böyle bir değişikliği kabul etmeyen kişiler zinciri kendi aralarında devam ettirecek bir güce sahiplerse o takdirde sistemden çekilmeleri gerekmez, eski sistem ile yeni sistem birbirinden ayrılarak devam eder ve ayrılma noktasından önce aynı işlem geçmişini paylaşmalarına rağmen ayrılma noktasından sonra farklı bir işlem akışına sahip olurlar. İşte bu noktada aslında iki ana zincire dönüşmüş dallardan söz edilebilir.

Bitcoin Blokzinciri'ne Mart 2013'te getirilen bir versiyon güncellemesi de tüm düğümler tarafından kabul edilmedi ve kısa bir dönem düğümler iki farklı versiyonu kullandı. Sonra 225430 numaralı blokta yer alan bir veri eski versiyonu kullanan düğümlerce okunamadı ve farklı versiyon kullanan düğümler farklı bir işlem akışı izlemeye başladı. Bu istenerek değil sistemdeki bir versiyon hatası sonucu oluşan bir bölünme örneği teşkil etmektedir[65] .

Bölünmeler genel olarak blokzincirlerde istenmez ancak Bitcoin gibi bir ödeme sistemi olmayı amaçlayan ve dolayısıyla güvenli, değiştirilemez bir işlem geçmişine sahip olması işlevsel açıdan hayati önem taşıyan blokzincirlerde bölünmeler stabilite açısından özellikle tehlikelidir. Bu sorunu çözmek için Bitcoin camiasında bilinen Bitcoin yazılımcılar bir araya geldi ve bir çözüm aradılar. Yeni versiyon daha fazla düğüm tarafından takip ediliyordu, bunu takip eden düğümler fazla işlem gücünü temsil ediyordu ve dolayısıyla söz konusu okunamayan bloktan itibaren yeni versiyon kullanan madenciler daha fazla blok eklemişti. Ancak yeni versiyonun kabul edilmesi için eski versiyonu kullanan herkesin güncelleme yapması gerekecekti çünkü ortada eski sistemin okuyamadığı bir blok söz konusuydu. Eski versiyondan devam edilmesi durumunda ise herkesin güncelleme yapmasına gerek kalmayacaktı çünkü yeni versiyondaki birimler eski versiyon bilgilerini okuyabiliyordu. Dolayısıyla yapılması gereken tek şey eski versiyonda izlenen zincirin daha uzun hale gelmesini sağlamaktı. Bitcoin yazılımcıları anlaşarak kendi versiyonlarını düşürdüler ve bir süre sonra eski versiyonu kullanan düğümlerce devam ettirilen zincir daha fazla işlem gücü tarafından temsil edilerek daha uzun

[65] Detaylı bilgi için bkz. BASHIR, s. 260.

hale geldi. Protokol gereği de bu zincir herkes tarafından takip edilmeye başlandı ve sorun çözülmüş oldu.

Bu Bitcoin Blokzinciri'ndeki tek bölünme değildir ancak en fazla problem yaratan bölünmedir. Diğer bölünmeler planlı şekilde ve Bitcoin topluluğu tarafından oylanarak gerçekleştirilmiştir. Bunlar arasından bahsedilmesi gereken iki önemli Bitcoin bölünmesi de Bitcoin Gold ve Bitcoin Cash kripto varlıklarının oluşmasına neden olan bölünmelerdir. Bunlar sert bölünmelerdir. Kural olarak kripto varlık kullanan blokzincirlerde sert bölünmeler alternatif kripto varlıklar oluştururlar. Bu durum topluluk açısından çok da olumsuz karşılanmayabilir. Aslında sert bölünme, bölünme anında mevcut olan durumun kopyalanması ve iki dalın birden farklı gelecek işlem akışıyla varlığını devam ettirmesi anlamına gelmektedir. Bu da bölünme anı itibariyle sistemdeki herkesin mevcut kripto varlığının otomatik olarak ikiye katlanması demek olacaktır. Örneğin Bitcoin, Bitcoin Cash sert bölünmesini yaşadığında hesabında 1 Bitcoin bulunan herkesin otomatik olarak 1 Bitcoin Cash'e de sahip olmuştur. Topluluk Bitcoin'i bırakmayıp ikisini de kazmaya devam ettiği için bölünme anından itibaren ise ikisi farklı blokzincirler olarak varlığını sürdürmüştür.

b. Ethereum Blokzinciri Bölünmesi ve DAO Saldırısı

Ethereum Blokzinciri yapısal olarak Bitcoin Blokzinciri'nden farklıdır. Ethereum Blokzinciri'nde Turing-destekli bir sanal makine çalışmaktadır ve bunun sayesinde Ethereum Blokzinciri üzerinde basit hesaplamaları çözen programlar çalıştırılabilir[66]. Bu programlardan bir tanesi de merkezi olmayan otonom yapılardır (İng. *decentralized autonomous organization,* "DAO"). DAO'lar yönetim işlemlerini ve işletme faaliyetlerini otomatikleştirmeyi mümkün kılan akıllı sözleşmelerden oluşmaktadır[67].

---

[66] ROHR/WRIGHT, s. 10.

[67] BASHIR, s. 64; CONG/HE/ZHENG, s. 11. Akıllı sözleşmeler hakkında daha fazla bilgi için bkz. RASKIN Max, "The Law and Legality of Smart Contracts", C. 1, S. 2017, s. 37; Ayrıca bkz. bu kitabın "Özel Hukuk Penceresinden Blokzincir: "Sanal Para (Varlık)" Değerleri ve "Akıllı Sözleşmeler" Üzerine Değerlendirmeler" başlıklı bölümü, AKSOY ÇAĞLAYAN.

En ünlü DAO projesi Slock.it firması tarafından yaratılandır ve bu aynı zamanda DAO'ların ilk örneklerinden biridir. Bu DAO, projenin yerel kripto varlığı olan *DAO Token*'larının ilk halka arzında (İng. *initial coin offering*, "ICO") 150 Milyon USD'den fazla fon toplamayı başarmış ve o zamana kadarki en büyük kitlesel fonlama projesi[68] olmuştur. Ancak DAO'nun temelinde yer alan akıllı sözleşmedeki bir hata bir saldırgan tarafından fark edilmiş ve bu sayede toplanan fonun üçte biri saldırganın kontrolünde olan bir alt DAO'ya transfer edilmiştir. Yatırımcıların şikayetlerine cevap vermek amacıyla sert bölünme yoluyla saldırının yapıldığı işlemin bulunduğu blok dahil o bloğa kadar işlem geçmişinin silinmesi teklif edilmiş ve bu da ilginç bir tartışmayı ateşlemiştir[69].

Sert bölünmeye karşı çıkanlar böyle bir işlemin Ethereum blokzincirinin felsefi temellerine uygun olmayacağını, saldırganın temelde yatan kodun izin verdiği bir işlem yaptığını ve blokzincirde aslında kurallar kod tarafından belirlediği için bu yapılanın meşru olduğunu savunmuşlardır. Ayrıca sert bölünme blokzincirin en önemli özelliklerinden olan değiştirilemezliğin de topluluk eliyle ihlal edilmesi anlamına gelmektedir ve bir grup bunun uzun vadede yarardan çok zarara sebep olacağını ifade etmiştir.

Sert bölünmeyi destekleyenler ise yapılan transferin olumsuz sonuçları üzerinde durarak saldırının çok büyük olduğunu, bu sebeple koda bağlı kalarak değil topluluğu dikkate alarak nihai kararın verilmesi gerektiğini belirtmiştir. Bu sayede topluluk eliyle bir oto-regülasyon yapılmış olacak, düzenleyici kuruluşlar ve şikayet durumunda devreye girebilecek olan mahkemeler de sistemden uzak tutulmuş olacaktır.

Sert bölünme teklifi topluluk tarafından oylanıp %89 çoğunluk ile kabul edilmiştir[70]. DAO saldırısından zarar görenler yatırımlarını blok-

---

[68] ICO'lar ve hukuki anlamda kitle fonlaması faaliyetiyle olan ilişkileri için bkz. bu kitabın "Kripto Varlıkların İlk Arzı ve Türk Hukukunda İlgili Düzenlemelerin Tespiti" başlıklı bölümü.

[69] WALCH, s. 262.

[70] Bu süreçte yaşanan gelişmeler hakkında detaylı bilgi için bkz. GÜÇLÜTÜRK Osman G., "The DAO Hack Explained: Unfortunate Take-off of Smart Contracts", **Medium**, 2018, https://medium.com/@ogucluturk/the-dao-hack-explained-unfortunate-take-

zincir teknolojisi tam anlamıyla değiştirilemez olmadığı için kurtarabilmişlerdir. Burada önemli olan nokta aslında blokzincirin simgesel özellikleri arasında gösterilen değiştirilemezliğin topluluk eliyle, çoğunluk kararıyla bir kenara bırakılmış olmasıdır[71].

Ancak bu sert bölünme sonucunda tüm birimler teklif edilen silinmeyi gerçekleştirememiş ve saldırının da içinde bulunduğu işlem grubunu koruyarak eski zincirden devam etmeyi tercih etmiştir. Burada da sert bölünme yeni bir kripto varlığın oluşumuna yol açmıştır. Ancak genel durumun aksine burada bölünmeyi kabul eden grubun izlediği zincir Ethereum ismiyle devam ederken asıl işlem geçmişinin silinmediği zincir Ethereum Classic adını almıştır.

DAO saldırısı kripto varlıkların sınıflandırılmasında önemli bir noktadır çünkü saldırıyı izleyen dönemde SEC tarafından yapılan inceleme ve yazılan rapor bazı kripto varlıklara sermaye piyasası düzenlemelerinin uygulanacağına yönelik bir kural oluşmasına sebep olmuştur[72].

4. Gizlilik ve Mahremiyet

Gizlilik kelimesi tek başına blokzincirde yer alan gizlilik kaygılarını çözmeye yeten bir ifade değildir. Zira blokzincirde tüm verilerin gizli olma zorunluluğu yoktur. Bu sebeple bu bölümde kavramsal bir ayrım yaparak bir blokzincirde yer alan verilerin diğer kişiler tarafından görülmemesi "gizlilik", blokzincir üzerinde işlem yapan kişilerin kimliklerinin tespit edilememesi ise "mahremiyet" kavramı ile ifade edilecektir.

Bir blokzincirin sağladığı gizlilik seviyesi tamamen bir tasarım tercihidir. Blokzincirin oluşturulma amacına göre hem işlemlerin hem kullanıcı kimliklerinin tamamen açıklandığı bir sistem seçilebileceği gibi her ikisinin de kriptografik algoritmalarla şifrelendiği ve kullanıcıların

off-of-smart-contracts-2bd8c8db3562 (Erişim Tarihi: 05.05.2021).

[71] WERBACH.

[72] Bu konuda bkz. bu kitabın "Kripto Varlıkların İlk Arzı (ICO) ve Türk Hukukunda İlgili Düzenlemelerin Tespiti" başlıklı bölümü.

bilgilerinin gerçek hayattaki kimliklere bağlanmasını önlemek için ek önlemlerin alındığı bir sistem de seçilebilir.

Mahremiyet, blokzincir üzerindeki işlemlerin, işlem taraflarının gerçek hayattaki bilgileriyle değil şifrelenmiş anahtarlar aracılığıyla yapılması yoluyla sağlanır. Şifrelenmiş anahtarların kullanılması ayrıca sistemin güvenliğini de sağlamaktadır. Özellikle açık blokzincirlerde tüm işlem geçmişi aslında herkesin erişimine açıktır. Bu anlamda gizlilik söz konusu değildir. Ancak işlem geçmişine bakıldığında işlemin taraflarının kimlik bilgileri değil sadece adresleri, yani açık anahtarlarının izleri görülebilir. Bu açıdan mahremiyet korunmaktadır.

Konunun daha iyi anlaşılması açısından yine Bitcoin Blokzinciri örneğinde gizlilik ve/veya mahremiyetin nasıl ve ne ölçüde sağlanabileceği incelenecektir.

A. Açık ve Özel Anahtar Çifti Sistemi

Blokzincirde işlemler için açık ve özel anahtar çiftleri (İng. *public-private key pair*) kullanılmaktadır. Özel anahtar rastgele oluşturulmuş bir karakter dizisidir. Açık anahtar ise kullanılan güvenlik algoritmasına göre farklı şekillerde oluşturulabilir ancak her durumda özel anahtarla birbirini tamamlar. Benzetme yapmak gerekirse açık anahtar bir kumbara görevi görür. Açık anahtar herkesle paylaşılır ve bunun sayesinde blokzincir ağına erişimi olan herkes bu adrese değer aktarımında bulunabilir. Ancak bir açık anahtara bağlanmış varlıklarda tasarruf etmek ancak özel anahtarla mümkündür. Dolayısıyla özel anahtar da bu kumbaranın anahtarı işlevini görür. Özel anahtar olmadan kumbara açılıp içerisindeki fon üzerinde tasarruf edilemez.

Bir Bitcoin işleminde Bitcoin göndermek isteyen kişi söz konusu işlemi kendi özel anahtarı, açık anahtarı ve alıcının açık anahtarıyla imzalar. Bu sayede hem söz konusu Bitcoin'e sahip olduğunu göstermiş olur hem de ilgili Bitcoin'i alıcının açık adresine bağlamış olur ve sadece alıcı

o açık anahtarın özel anahtar çiftine sahip ise o Bitcoin üzerinde tasarruf edebilir hale gelir[73].

Süreci daha iyi anlamak adına Bitcoin Blokzinciri'ni mercek altına alabiliriz. Bitcoin Blokzinciri'nde de açık ve özel anahtar çiftleri vardır. Bitcoin açık anahtarı, özel anahtara EC (İng. *elliptic curve*) şifrelemesinin uygulanmasıyla elde edilir. Bitcoin Blokzinciri'nde adres olarak adlandırılan şeyler aslında açık anahtarların daha önce de açıkladığımız özel bir algoritma olan *SHA-256* algoritmasıyla üretilmiş izleridir[74].

Bu aşamada iz değeri bir kimlik gibi kullanılır. A, B'ye bir Bitcoin göndermek istediği zaman yapacağı şey bu Bitcoini B'nin verdiği adrese bağlayan bir işlem (İng. *transaction*) oluşturup bunu kendi özel anahtarıyla imzalamaktır[75]. İşlem içerisinde A'nın özel anahtarı gözükmez, A ve B'nin adresleri ile işleme konu olan Bitcoin miktarı gözükür. Bu bilgiler sayesinde ağdaki diğer katılımcılar tüm işlem geçmişini tarayarak A'nın verdiği adrese bağlı bulunan Bitcoin miktarını görebilir ve işlemin geçerliliğini denetleyebilirler. Ancak o Bitcoin'i sadece gönderilen adrese bağlı özel anahtara sahip olan kişi, yani B, tekrar başkasına gönderebilir.

Bitcoin Blokzinciri'nde bir blok içerisinde bir işleme üzerinde bu hususlar daha da somutlaştırılabilir. Örnek olarak 682161 numaralı bloğu inceleyebiliriz[76]. Bu blok içerisine 2489 işlem kaydedilmiştir. Bu işlemlerden bir tanesine ait bilgiler ise şu şekildedir:

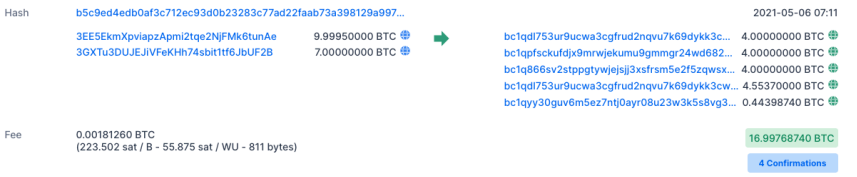
---

[73] AGGARWAL Divesh/BRENNEN Gavin/LEE Troyvd., "Quantum Attacks on Bitcoin, and How to Protect Against Them", **Ledger**, C. 3, S. 2018, s. 3.

[74] İlk başlarda açık anahtarın değiştirilmiş hali (*hash*) değil doğrudan açık anahtarın kendisi kullanılıyordu ancak daha sonra güvenlik protokollerinde yapılan değişikliklerle şimdiki hali kabul edildi. Bkz. AGGARWAL/BRENNEN/LEE/SANTHA/TOMAMICHEL, s. 3.

[75] BASHIR, s. 69.

[76] https://www.blockchain.com/btc/block/000000000000000000618f119cb31a3e03ff153a31cd544098d6e33bd80dac5 (Erişim Tarihi: 05.05.2021).



Bitcoin işleminin içeriği (Kaynak: Blockchain.com[77])

Bu resimde üstte yer alan uzun dizi bu işleme özel iz değeridir. Aynı bloklarda olduğu gibi blok içerisindeki her bir işlem için de ayrı bir iz değeri üretilmektedir. İz değerinin hemen altında okun sol tarafında yer alan iki adet dizi gönderilen Bitcoin'lerin çıkacağı iki adresi göstermektedir. İşte bu adresler aslında birer açık adresin izidir. Sağ tarafta ise bu Bitcoin'leri alacak kişiler tarafından verilmiş adresler mevcuttur ve hemen yanlarında gönderilen miktarlar gösterilmektedir. İşlemde 4 adet onay olduğuna dair mavi kutucukta yer alan bilgi bu işlemin bulunduğu bloğun arkasına 3 adet daha blok eklendiği gelmektedir. Görüldüğü üzere onay sayısının hesabında işlemin bulunduğu blok ilk onay olarak değerlendirilmektedir. Hemen altta sol tarafta yer alan Bitcoin miktarları ise sırasıyla toplam girdi ve çıktı miktarları ile bunlar arasındaki farkı, yani bu işlemi bloğa ekleyerek ana zincire girmesini sağlayan birime ödenecek olan işlem komisyonunu göstermektedir.

B. Anahtar Çiftleri Kullanımının Etkileri

Öncelikle belirtmek gerekir ki anahtar çiftleri şu anki teknolojik gelişme seviyesinde yüksek güvenlikli kabul edilebilecek algoritmalar kullanılarak üretildikleri için sistemin güvenliğini sağlamaktadır. Ancak gizliliğe ilişkin iki temel sorun ortaya çıkmaktadır.

İlk olarak işlemler tarafların gerçek kimliklerine dair bilgilerini içermiyorsa da işlemde kullanılacak adres bilgisi paylaşılmaktadır. Bir Bitcoin adresi üzerinden yapılan işlemlerin oluşturduğu mantıksal bağlantılara bakılarak o adresi kullanan kişinin gerçek kimliği hakkında

[77] https://www.blockchain.com/btc/tx/b5c9ed4edb0af3c712ec93d0b23283c77ad22faab73a398129a997edc66228a7 (Erişim Tarihi: 05.05.2021).

çıkarımlar yapılması mümkündür. Bu sebeple aslında tam bir anonimlik (İng. *anonimity*) değil, mahremiyet benzeri bir durum (İng. *pseudo-anonimity*) söz konusudur[78]. Burada adresin ait olduğu kişinin ifşa edilmesi riskini azaltmak adına bir kişinin her bir işlem için yeni bir anahtar çifti üretmesi ve kullanması[79] ya da farklı işlemlerin tek bir işlem içerisinde birleştirilmesi[80] tavsiye edilmektedir. Ancak bu hamleler de düzenleyici kurumlar devreye girdiğinde özellikle kara para aklama ve terörist finansmanı düzenlemeleri açısından sıkıntı çıkarabilecektir.

İkinci olarak gerçek bilgilerin değil sadece anahtarların kullanılması özel anahtara sahip olan kişinin işlemi gerçekten yapan kişi olup olmadığına bakılmaksızın söz konusu anahtara bağlı kripto varlıklar üzerinde tasarruf edebilmesi sonucunu doğurmaktadır. Bu da kripto varlıklar üzerindeki hak sahipliğine dair belirsizlikler yaratmaktadır. Bu anlamda kripto varlıklar ile bağlı bulundukları adreslere ait özel anahtarlar arasındaki ilişki, hamiline yazılı kıymetli evraklardaki dolaşıma benzemektedir. Üstelik ciro silsilesinin yerini alan işlem kaydı burada otomatik olarak blokzincir üzerinde tutulmaktadır.

Ancak belirtmek gerekir ki kripto varlıkların günlük hayatta kullanımları ve dolaşıma sokulmaları çok yüksek oranda kripto varlık borsaları üzerinden olmakta ve bu borsalar da dünyada birçok ülkede düzenleyici kurumlar tarafından doğrudan bir statüye sokulmasalar da kara para aklamanın engellenmesi (İng. *anti money laundering*) ve "müşterini tanı" (İng. *know-your-customer, KYC*) kurallarına tabi tutulmaktadırlar. Dolayısıyla bu borsalar üzerinden yapılan işlemlerde anahtarlar borsalar tarafından tedarik edilmekte ve tutulmakta, kolaylıkla gerçek kimliklere bağlanabilmekte, ayrıca hangi anda kimin tasarruf hakkı olduğu kolaylıkla tespit edilebilmektedir. Ancak kripto varlıkları borsalar üzerinden değil doğru-

---

[78] PILKINGTON Marc, "Blockchain Technology: Principles and Applications", **SSRN Electronic Journal**, https://ssrn.com/abstract=2662660 (Erişim Tarihi: 05.05.2021), s. 5.

[79] NAKAMOTO, , s. 6.

[80] TASCA Paolo, "Digital Currencies: Principles, Trends, Opportunities, and Risks", **SSRN Electronic Journal**, 2015, http://www.ssrn.com/abstract=2657598 (Erişim Tarihi: 05.05.2021), s. 19.

dan madencilik yoluyla elde eden kullanıcılar için yukarıda bahsedilen meseleler geçerliliğini korumaktadır.

Anahtarlardan bahsederken kripto varlık transferlerinde standart bir model halini alan cüzdanlardan da söz etmek gerekecektir. Cüzdan İng. (*wallet*) denilen şey bir kripto varlığı tasarruf etmeye izin verecek ve özel anahtar ve ona bağlı açık anahtarı depolayan üçüncü-parti bir uygulamadır. Genelde borsalar aynı zamanda cüzdan hizmetleri de vermektedirler. Bitcoin kullanılması için bir cüzdan kullanılması gerekmez[81], isteyen kendi özel-açık anahtar çiftlerini ve adreslerini istediği şekilde saklayabilir. Cüzdan sadece bunun için geliştirilmiş ve kullanımı kolaylaştıran bir uygulamadır. Cüzdanın her durumda internete erişimi olan bir depolama olması gerekmez. İnternete bağlı olan, yazılımsal tabanlı cüzdanlara "sıcak cüzdan (İng. *hot wallet*)" adı verilirken internete erişimi olmayan cüzdanlara ise "soğuk cüzdan (İng. *cold wallet*)" adı verilmektedir.

III. BLOKZİNCİRLERİN HUKUKİ DEĞERLENDİRİLMESİNİN YAPILMASI

Çalışmanın bundan önceki bölümlerinde blokzincir teknolojisine ilişkin teknik hususlar açıklanmış ve Bitcoin Blokzinciri temel alınarak detaylı şekilde incelenmiştir. Peki bunların blokzincir teknolojisinin

[81] Bkz. **Aslantaş Ateş** (2016), 356. Yazar Bitcoin kullanmak için cüzdan gerektiğini ve bu süreçte kişisel adresler oluşturulduğunu ifade etmiştir ancak bu doğru değildir. Bitcoin kullanımı için cüzdan kullanmak gerekmediği gibi oluşturan adresler kişiye özel değildir, hatta kişilerin gerçek kimlikleriyle ilgili hiçbir bağlantı içermezler. Benzer bir hata **Hepkorucu/Genç** tarafından da yapılmıştır, bkz. **Hepkorucu/Genç** (2017), s. 48. Yazarlar Bitcoin blockchaininden bahsederken sanal paraların Bitcoin açık kaynak yazılımda oluşturulan dijital cüzdanlar üzerinde saklandığını ve geçmiş tüm transferlerin de kullanıcı bilgisiyle bağlantılı olarak bir blockchain üzerinde saklandığını belirtmiştir. Cüzdan servisleri Bitcoin'in açık kaynak yazılımı üzerinde oluşturulmaz, zorunlu değillerdir. Ayrıca geçmiş tüm transfer bilgileri blockchain üzerinde kullanıcı bilgileriyle bağlantılı olarak saklanmaz. Tam aksine kullanıcıların gerçek bilgileriyle blockchain üzerinde depolanan adresler arasında bir bağ olmaması Bitcoin'de gizliliği sağlayan unsurlardan biridir. Adresler ve anahtar çiftleri kişilere bağlı değildir, bir kişi her bir işlem için farklı bir adres ve anahtar çifti kullanabilir.

değerlendirilmesi açısından bir hukukçuya nasıl faydası dokunacaktır? Burada birkaç temel nokta öne çıkmaktadır.

Hukukçular geleneksel olarak teknolojileri geliştiren gruplardan farklı bir dil ve çalışma kültürüne sahiptir. Ancak teknolojik gelişmelerin yaygınlaşması ve farklı alanlarda uygulama bulması hukukçuların alışık oldukları sistemden farklı bir yapıya sahip olan bu alanlarda çalışmalarını zorunlu kılmaktadır. Blokzincir teknolojisinin özellikle bu alanda çalışmamış bir hukukçu için bile karmaşık olarak değerlendirilebilecek finans hukuku alanındaki etkisi ve yarattığı tartışmalar durumun ciddiyetini ortaya koyduğu gibi bu tartışmaların çözülebilmesi için gerekli olan teknik okur yazarlığı yüksek hukukçu ihtiyacını da gözler önüne sermektedir.

Bu çalışmadaki açıklamaların en önemli katkılarından biri hukukçuların blokzincir teknolojisinin hukuk ile etkileşimine dair değerlendirmeler yaparken sadece dışarıdan görünene değil, "blokzincir" etiketinin altında olup bitene dair bir temel bilgilendirme sağlamasıdır. Zira hukuki nitelendirmeler temelde adlandırmaya ya da görünüme değil, esasa bakılarak yapılmalıdır. Teknolojinin işleyişi dikkate alınmaksızın yapılan değerlendirmelerin hatalı olabildiği görülmektedir.

İkinci önemli husus, çalışmada sürekli vurgulandığı üzere blokzincir teknolojisiyle ilgili hukuki değerlendirmelerde basmakalıp ifadelere dayanılmaksızın sistemin esnekliğinin ve her somut uygulamanın özel şartlarının dikkate alınmasıdır. Blokzincir, üzerine çok fazla konuşulan ve sürekli belli özelliklerle eşleştirilen bir teknoloji olmakla birlikte somut blokzincir uygulamaları özelinde bu özellikler geçerli olmayabilecektir. Özellik değerlendirmesinin yapılmasında blokzincirin türü, kullanım amacı, uzlaşma protokolü gibi hususlar incelenmeden bir sonuca ulaşılmamalıdır.

SONUÇ YERİNE

Bu çalışma niteliği itibariyle bir hukuki argümantasyon ortaya koymayı değil blokzincir teknolojisinin işleyişini açıklamayı amaç edindiğinden bir sonuç bölümü yerine bir açıklama bölümünün daha uygun olduğu kanaatindeyiz.

Kitabın devamındaki kısımlar okunurken blokzincir teknolojisinin işleyişine ilişkin bu bölümde yer alan açıklamaların hatırlanması faydalı olabilecektir. Bununla birlikte bu bölümdeki açıklamalar blokzincirin sadece bir uygulaması olan kripto varlıkların sadece bir tane örneği olan Bitcoin dikkate alınarak yapılmıştır. Blokzincir platformlarının ve kripto varlıkların farklı şekillerde kurgulanabileceği, esnek bir niteliğe sahip olduğu unutulmadan değerlendirmeler her uygulamanın somut özellikleri dikkate alınarak yapılmalıdır.

KAYNAKÇA

"Final Report", **Cryptoassets Taskforce**, 2018

AGGARWAL Divesh/BRENNEN Gavin/LEE Troy/SANTHA Miklos/TOMAMICHEL Marco, "Quantum Attacks on Bitcoin, and How to Protect Against Them", **Ledger**, C. 3, S. 2018, ss.

AKSOY ÇAĞLAYAN Pınar, **Akıllı Sözleşmelerin Kuruluşu ve Geçerlilik Şartları**, İstanbul, 2021

ASLANTAŞ ATEŞ Burcu, "Kripto Para Birimleri, Bitcoin ve Muhasebesi", **Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, C. 7, S. 1, 2016, ss. 349-366

ATZORI Marcella, "Blockchain Technology and Decentralized Governance: Is the State Still Necessary?", **SSRN Electronic Journal**, C. S. 2015, ss.

BARAN Paul, "On Distrubuted Communications Networks", C. S. 1962, ss.

BASHIR Imran, **Mastering Blockchain**, 2017

CATALINI Christian/GANS Joshua S., "Some Simple Economics of the Blockchain", **SSRN Electronic Journal**, C. S. 2016, ss.

CONG Lin William/HE Zhiguo/ZHENG Jingtao, "Blockchain Disruption and Smart Contracts", **SSRN Electronic Journal**, C. S. 2017, ss.

EVANS David S., "Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms", **SSRN Electronic Journal**, C. S. 2014, ss.

GILBERT S./LYNCH N. A., "Perspectives on the CAP Theorem", **Computer** C. 45, S. 2, 2012, ss. 30-36

GÜÇLÜTÜRK Osman G., "The DAO Hack Explained: Unfortunate Take-off of Smart Contracts", Medium, 2018, https://medium.com/@ogucluturk/the-dao-hack-explained-unfortunate-take-off-of-smart-contracts-2bd8c8db3562 (Erişim Tarihi: 05.05.2021)

GÜÇLÜTÜRK Osman G., "Blokzincir Üzerinde Depolanan Verilerin Kişisel Veri Niteliği ve Silinemezlik, Yok Edilemezlik Sorunu", **Kişisel Verileri Koruma Dergisi**, C. 1, S. 2, 2019, ss. 30-40

MAINELLI Michael/ALISTAIR M., "The Impact and Potential of Blockchain on the Securities Transaction Lifecycle", **SWIFT Institute**, 2015

NAKAMOTO Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008

ÖZER Yusuf Mansur, **Kişisel Verilerin Korunmasında Blok Zinciri Modeli: Vaatler ve Hukuki Engeller**, İstanbul, 2020

PAECH Philipp, "The Governance of Blockchain Financial Networks", **SSRN Electronic Journal**, C. S. 2016, ss.

PETERS Gareth William/PANAYI Efstathios/CHAPELLE Ariane, "Trends in Crypto-Currencies and Blockchain Technologies: A Monetary Theory and Regulation Perspective", **SSRN Electronic Journal**, C. S. 2015, ss.

PILKINGTON Marc, "Blockchain Technology: Principles and Applications", SSRN Electronic Journal, https://ssrn.com/abstract=2662660 (Erişim Tarihi: 05.05.2021)

RASKIN Max, "The Law and Legality of Smart Contracts", C. 1, S. 2017, ss. 37

ROHR Jonathan/WRIGHT Aaron, "Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets", **SSRN Electronic Journal**, C. S. 2017, ss.

TASCA Paolo, "Digital Currencies: Principles, Trends, Opportunities, and Risks", SSRN Electronic Journal, 2015, http://www.ssrn.com/abstract=2657598 (Erişim Tarihi: 05.05.2021)

WALCH Angela, "Open-Source Operational Risk: Should Public Blockchains Serve as Financial Market Infrastructures?", **Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2** (Editör: 2018, ss.

WERBACH Kevin D., "Trust, But Verify: Why the Blockchain Needs the Law", **SSRN Electronic Journal**, C. S. 2017, ss.