BLOKZİNCİR TEKNOLOJİSİ VE KİŞİSEL VERİLERİN KORUNMASI HUKUKU

Av. Müge NAZİLLİ - Av. Deniz BİLGE

GİRİŞ

Blokzincir teknolojisi, geleneksel veri kayıt sistemlerinden farklı oluşu, yeniliği ve popülerliği sebebiyle son dönemde kişisel verilerin korunması açısından büyük tartışmalara sebep olmaktadır. Teknik altyapısı ve gayri merkezi yapıda olması kişisel verilerin korunmasına ilişkin birçok sorunu beraberinde getirmektedir. Bu makalede blokzincirin teknik yapısını oluşturan *"hash"* kavramı ve *"anahtar"* kavramlarına değinilecektir. Bununla birlikte blokzincir teknolojisi açısından kişisel veri, veri sorumlusu, verinin silinmezliği/yok edilmezliği konuları ve özellikle blokzincir ağında yer alan kişisel verilerin anonimleştirme kavramı açısından niteliği değerlendirilecektir.

BLOKZİNCİR TEKNOLOJİSİ

Blokzincir, verilerin belirli kurallar çerçevesinde depolandığı bir depolama alanı olarak düşünülebilir. Bu açıdan bakıldığında bilgisayarımızın belleğinden ya da hayatımızın bir parçası haline gelen harici belleklere benzemektedir. Veri depolama alanı için verilebilecek bir diğer örnek ise bulut teknolojisidir. Bulut teknolojisinde de verilerimiz bize ait olmayan üçüncü kişilere ait olan veri depolama merkezlerinde depolanırlar. Bulut teknolojisi kullandığımızda verilerimize internet yoluyla erişiriz. Blokzincir teknolojisini bu teknolojilerden ayrılan özelliği ise depolama alanına yani blokzincire yazılan verilerin aynı anda birçok birbiri ile bağlantısı olmayan ve farklı kişilere ait bilgisayarlara kaydedilmesi ve kayıtların geçmişe dönük değiştirilmesinin neredeyse imkansız olmasıdır. Bu tür veri sistemlerine dağıtık veri sistemleri *(distributed ledger technology)* denilmektedir. Sayıca çok fazla bilgisayarda bulunan donanım ve yazılımlar sayesinde veriler daha şeffaf ve güvenli saklanırlar. Blokzincirin dağıtık yapısı sayesinde birbirine yabancı kimseler, birbirileriyle doğrudan güven ilişkisi kurmadan güven içinde işlemlerini yapabilirler. Dağıtık veri sistemlerini bir alegori ile anlatmanın zihinlerde daha net bir görüntü oluşturacağına inanmaktayız. Şöyle ki; giderek azalan bir gelenek

olmasına karşın halen yer yer varlığını koruyan mahalle bakkallarının kullandığı veresiye defteri kültürü, bu konu için güzel bir örnektir. Mahalle sakinleri, daha sonra ödemek üzere bakkaldan alışveriş yaparlar. Mahalle bakkalı bu alışverişi defterine kaydeder. Örneğin; farazi alıverişimizde Yasin'in bakkaldan iki adet çikolata aldığını düşünelim. Bakkal karşılığını almadan çikolataları Yasin'e vererek defterinde Yasin'in olduğu sayfaya iki adet çikolata ekler. Eğer Yasin de hesap konularına duyarlı bir kişiyse kendi defterine iki çikolata aldığını yazar. Ay sonunda, ya sadece bakkalın tuttuğu hesaba güvenilerek borç belirlenir ya da Yasin ve bakkalın defteri karşılaştırılır. Blokzincir teknolojisi kullanıldığı durumda ise tüm mahalle sakinleri, Yasin'in aldığı iki çikolatayı kendi defterine kaydeder. İşte bu sisteme kabaca dağıtık veri sistemi denilmektedir.

Bazı blokzincirler herkese açıkken bazıları kapalıdır. Bitcoin blokzinciri de herkese açık blokzincirlerdendir. Dileyen herkes bu yazılımı bilgisayarına indirerek inceleyerek ilk Bitcoin transferinden günümüze kadar yapılan tüm transferleri inceleyebilir.

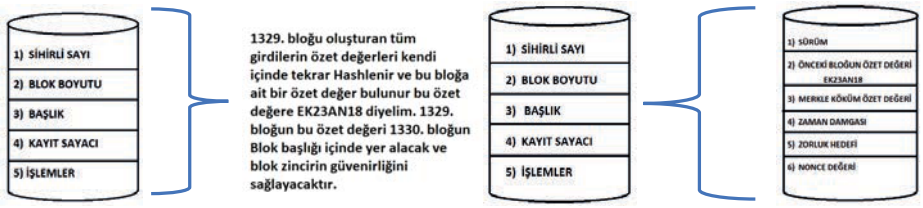
Hash Değeri

Hash bir özetleme tekniğidir. Bir verinin şifrelenerek okunmaz ve tahmin edilemez hale getirilmesi için başvurulan yollardan biridir.

Hash kavramı parmak izine benzetilebilir. Bir veriye parmak izi kazandırmak için birçok yöntem vardır. Bunlardan en bileneni SHA (*Secure Hash Algorithm*)'dir. Türkçe'ye "güvenli karma algoritma" veya "kriptografik özetleme fonksiyonu" olarak çevrilebilir.

SHA ile bir veriye (resim, müzik, roman ya da bir kelime) Hash değeri verildiğinde sabit uzunlukta bir özet değer alınır ve bu değere Türkçe'de *"özet değer"* diyebiliriz. Bu verilerde en küçük bir değişiklik olduğunda, örneğin bin sayfalık bir romanda sadece bir virgül değiştiğinde bambaşka bir özet değer ortaya çıkacaktır. Dolayısıyla tüm romanı okumaya gerek kalmaksızın iki roman verisinden hangisinin gerçek olduğunu anlamak mümkün olur. Elimizdeki verinin ne olduğu önemli değildir. Picasso'nun tablosunun data hali, bir film ya da Gençliğe Hitabe'nin data hali aynı sabit uzunlukta bir veriye dönüşür.

Bir blok 5 bölümden oluşur. Bunlar; sihirli sayı, blok boyutu, blok başlığı, kayıt sayacı ve işlemler bölümüdür. Blok başlığı da kendi içinde, önceki bloğun özet değeri, Merkle kökü özet değeri, zaman damgası, zorluk hedefi ve Nounce değerini içinde barındırır.



Blok no 1329 Blok no 1330 Başlığın Yapısı

Başlığın Yapısı

Önceki bloğun özet değeri, sonraki bloğun içindeki verilerden biridir. Önceki bloğun özet değerinin bir sonraki blokta tutulması tüm zincirin değiştirilemez olmasını da sağlar. Çünkü blokzincirde bulunan bir bloğun özet değeri değiştiğinde bundan sonraki tüm blokların da özet değeri değişecek ve bu çarpıklık, değişikliğin ortaya çıkmasına neden olacaktır. Zincirdeki Bloklar birbirlerine özet değerleri ile bağlanırlar. Bloğun özet değeri bloğu oluşturan girdilerin özet değerlerinden oluşur. Bu özet değer de bir sonraki bloğun girdilerinden biri olur. Blok zincirin güvenirliğinin temelindeki yöntem de budur. Şöyle ki 1329 numaralı blok sonradan değiştirilmek istendiğinde özet değeri değişecek ve bu bir sonraki bloğun özet değerini de etkileyecek ve bu tüm zincire sirayet edecektir. Bu durum kolayca ortaya çıkacak ve değişiklik fark edilecektir.

Hash Fonksiyonu Örneği:

Müge'nin, Deniz'e 30 Nisan 2021 tarihinde 1000 Bitcoin gönderme işleminin SHA256-2 tekniğiyle özeti alındığında ortaya çıkacak özet değer aşağıdaki gibi olacaktır. *7800e9f07ec4698cce1c97cc13887584a38bc9709178f0da1a846917c8300324*

Açık Anahtar/Kapalı Anahtar

Blokzincir güvenliği ile ilgili olan simetrik ve asimetrik şifreleme konuları açık anahtar ve kapalı anahtar sistemiyle doğrudan bağlantılıdır. Şöyle ki: Simetrik şifrelemede bir veriyi hem şifrelemek hem de çözmek için aynı anahtar kullanılır. Bir örnekle açıklamak gerekirse; avukat yazdığı dilekçeyi açık anahtarla şifreleyip müvekkile gönderdiğinde, müvekkilin şifreyi çözebilmesi için avukatın şifreleme yaparken kullandığı anahtarın aynısını müvekkiline de göndermesi gerekir. Bu durumda da kötü niyetli birisi anahtara ulaştığında şifrelenmiş veriye de ulaşabilir. Asimetrik şifrelemede ise; avukat dilekçesini açık anahtarla şifreler ve müvekkil kendi özel anahtarıyla dilekçenin şifresini çözer.

Kripto paralarda asimetrik şifreleme kullanılır. Asimetrik şifrelemede iki farklı anahtar vardır. Bu iki anahtar birbirleriyle ilişkilidir fakat aynı değillerdir. Bu anahtarlardan birine açık anahtar (*public key*), diğerine ise özel anahtar (*private key*) denir. Açık anahtar veriyi şifrelemek için, özel anahtar ise şifreyi çözmek için kullanılır. Özel anahtar, açık anahtardan türetilir ama açık anahtardan özel anahtar üretilemez. Fakat özel anahtara sahip olmak isteyen biri eğer açık anahtardan özel anahtar türetmek isterse, kripto paralar için kullanılan SHA256 protokolünde, 2^{256} kadar işlem yapması gerekir ve bu mevcut bilgisayar teknolojisiyle neredeyse imkansızdır.[1]

Özet değer dışında blokzinciri güvenli kılan enstrüman da *"iş ispatı"* tekniğidir. Blokzincir teknolojisi kullanılan sistemlerde verileri işleyen milyonlarca bilgisayar vardır. Veri işleyen kişilere madenci denilir. Bu sistemlerde, blok oluşturulduğunda bloğu oluşturana ödül verilir. Madencilerin sistemi kandırmaması ve sürekli blok üretmelerini engellemek amacıyla iş ispatı (*proof of work/PoW*) ve pay ispatı (*prof of stake/Pos*) mutabakat algoritmaları kullanılır. Birçok mutabakat sistemi söz konusudur fakat bu iki iş ispatı tekniği en popüler olanlarıdır.[2]

İş İspatı, gerekli sıfır bit sayısı ile başlayan SHA-256 ile karma hale getirildiğinde bir karma değer üreten *"nonce"* adlı bir değer içerir. Hedef, gerekli sıfır bit sayısını ayarlar. İhtiyaç duyulan karma değer, mevcut hedef değerin altında olmalı ve hedeften daha küçük olmak için belirli sayıda baştaki sıfır biti içermelidir. Bunu yapmak için, iş ispatı tarafından doğrulamaya yüksek düzeyde hesaplama maliyeti uygulanır ve iş ispatı yapmak için madencinin yüksek düzeyde hesaplama kaynaklarına ihtiyacı vardır. Bu nedenle, bilgi işlem kaynaklarını taklit etmek çok zordur.[3]

Asimetrik şifreleme, bilginin gizlenmesi ve kaynağının doğrulanması amacıyla kullanılır. Bilgi gizlenirken şifreleme, kaynağı doğrulanırken dijital imza kullanılır. Şifrelemenin amacı gönderilen bilginin değiştirilmeden doğru ve düzgün bir şekilde gideceği yere varmasıdır. Asimetrik şifreleme yöntemi bugün kullandığımız birçok mesajlaşma programında da kullanılmaktadır. İdrakının şifreleme tekniğinin daha iyi anlaşılması için hepimizin kullandığı Whatsapp uygulaması üzerinden verilen bir örnek yararlı olacaktır. Örneğin; müvekkil Mert, boşanmak istediğini avukatıyla paylaşmak istemektedir. Bu bilgi Whatsapp programıyla gönderdiğinde

1 Güven; Şahinöz, **"Blokzincir Kripto Paralar Bitcoin",** s.45-46

2 Richard Caroll, **Bitcoin Secrets Revealed: The Complete Guide to Understanding Bitcoin, Cryptocurrency and the Blockchain**, s.42-48

3 Sandeep Kumar Panda; Ahmed A. Elngar; Valentina Emilia Balas; Muhammed Kayed, **Bitcoin and Bitcoinchain History and Current Applications**, 2020, s.7-8

sistem arka planda nasıl çalışmaktadır? Mert *"boşanma davasını açabilirsiniz"* yazdığında programın algoritması bu anlaşılır yazıyı şifreler ve ortaya karmaşık anlaşılmaz bir metin çıkar. SHA 256 algoritmasında bu şifre *ced2b2429e55404acc6ff0cda1370cc402be4e7e0625c8d480c-70d187228c1dd* şeklinde görülür.

Asimetrik şifrelemede her kullanıcının iki anahtarı olduğundan bahsetmiştik. Bunlardan biri açık anahtar diğeri özel anahtardı. Şifrelemenin amaçlarından biri mesajın doğru kişiye ulaştığından emin olunmasıdır. Bu nedenle Mert, mesajı sadece avukatın aldığından emin olmak için avukatın açık anahtarıyla şifreler dolayısıyla artık bu mesaj sadece avukatın açık anahtarıyla açılabilir hale gelir. Üçüncü bir şahıs, bizim örneğimizde Mert'in eşi Selin bu mesajı okumak istediğinde okuyacağı metin; ced2b2429e55404acc6ff0cda1370cc402be4e7e0625 c8d480c-70d187228c1dd olacaktır. Dolayısıyla selin mesajı okuyamayacaktır. Diğer yandan avukatın da mesajın Mert'ten geldiğine emin olması gerekir aksi halde başka birinden gelen *"boşanma davasını açabilirsiniz"* mesajına istinaden yanlışlıkla dava açılabilir. Asimetrik şifrelemenin bu konu içi çözümü ise Mert'in aynı zamanda mesajı kendi özel anahtarıyla imzalaması olacaktır. Avukat da Mert'in özel anahtarıyla imzaladığı mesajı yine Mert'in açık anahtarıyla açacaktır. Mert dışında başka biri Mert'in özel anahtarını bilemez. Özel anahtar gizlidir. Başka biri avukata *"boşanma davasını açabilirsiniz"* mesajını gönderdiğinde ise başka bir özel anahtarla bu metin şifrelenecek ve Mert'in açık anahtarıyla bu mesaj açılamayacaktır. Bu halde avukat, mesajın Mert'ten gelmediğini anlayacaktır. Asimetrik şifreleme sistemi Whatsapp uygulamasında gördüğümüz uçtan uca şifreleme ile çalışmaktadır.

Veriyi göndermek isteyen taraf, veriyle birlikte açık anahtarı da gönderir. Açık anahtar veriyi şifreler, veriyi alan taraf ise kendi özel anahtarı ile veriyi açıp kullanabilir. Dijital imza olduğunda ise veri özel anahtar ile şifrelenir ve karşı tarafa açık anahtar gönderilir. Karşı taraf veriyi gönderilen açık anahtar ile açabiliyorsa belgenin gönderilen kimse tarafından imzalandığına ve değiştirilmediğine emin olur.

Blokların içine kaydedilen işlemlerin değiştirilememesi, blokzincir güvenliğinde önemli rol oynamaktadır. Blokların içindeki herhangi bir kayıt değiştirildiğinde tüm bloğun Hash değerinin değiştiği yukarıda belirtilmişti. Ağdaki tüm bilgisayarlardaki blokzincir, aynı olduğundan kötü niyetli kullanım hemen fark edilecektir. Ağdaki kullanıcıların önüne iki farklı zincir gelirse, uzun olan zincir sistem tarafından kabul edilir. Kötü niyetli kullanım sonucu önceki bloklardan birinde yapılan değişiklik de-

vamındaki bloklarla olan bağı koparacağından zincir kısalacak ve sistem tarafından görmezden gelinecektir.

KİŞİSEL VERİ KAVRAMI

6698 sayılı Kişisel Verilerin Korunması Kanunu, 7 Nisan 2016 tarihinde 29677 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir.[4] Anılan yasa, kişisel verileri, kişisel verilerin işlenmesini ve korumasını tanımlayan, kişisel verilerin işlenmesine ve korunmasına ilişkin düzenlemeler ile bu düzenlemelere uyulmaması halinde yaptırımlar öngören bu alandaki temel düzenleyici kanundur.[5]

Avrupa Birliği Genel Veri Koruma Tüzüğü (*General Data Protection Regulation*),[6] 25 Mayıs 2018 tarihinde, 95/46/EC sayılı Yönerge'nin yerini almak üzere yürürlüğe girmiş olup günümüzle daha uyumlu, daha dinamik ve bireysel haklar açısından daha koruyucu olan bir düzenlemedir.[7]

6698 sayılı Kanunun 3. maddesinin d bendi ile kişisel veri kavramı *"kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"* şeklinde tanımlanmaktadır.[8]

GDPR m.4/1'de yer alan düzenlemeye göre ise, '*kişisel veri*' tanımlanmış veya tanımlanabilir bir gerçek kişiye ilişkin her türlü bilgidir. İlgili kişi (data *subject);* tanımlanmış bir gerçek kişi özellikle bir isim, kimlik numarası, konum verileri, çevrimiçi tanımlayıcı ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktöre atıfta bulunularak doğrudan veya dolaylı olarak tanımlanabilen bir kişidir.[9]

Görüldüğü üzere, her iki düzenlemede kişisel veri kavramının tanımı yapılmış ve kişisel veriler sınırlı sayıda sayılmamış olup tanımlar benzerlik göstermektedir. Bir verinin kişisel veri niteliğini haiz olması için üç temel unsur söz konusudur: Bir gerçek kişi; belirli veya belirlenebilirlik; ilişkinlik.

İlk unsur, kişisel verinin gerçek kişiye ilişkin olmasıdır. Burada en önemli husus tüzel kişilerin kişisel verisi olmamasıdır. Dolayısıyla tüzel kişilerin verileri 6698 Sayılı Kanun ile GDPR kapsamında koruma altında

4 29677 Sayılı Resmi Gazete, 07/04/2016

5 http://yasaizleme.org.tr/kisisel-verilerin-korunmasi-kanununun-uygulanma-sureci(s.e.t.15.10.2021)

6 General Data Protection Regulation(GDPR)

7 https://www.kisiselverilerinkorunmasi.org/mevzuat/avrupa-birligi-genel-veri-koruma-tuzugu-gdpr-turkce-ceviri(s.e.t.15.10.2021)

8 6698 sayılı Kişisel Verilerin Korunması Kanunu, m.2

9 GDPR, m.4. f.1

değildir. Yalnızca gerçek kişiye ait kişisel veriler söz konusu mevzuatlarla hukuken korunmaktadır.

İkinci unsur olan belirli veya belirlenebilir olma durumuna ilişkin olarak 6698 sayılı Kanunda bir açıklama yapılmamışsa da GDPR'da bu unsur açıklanmaya çalışılmıştır. Kişinin belirlenip belirlenememesi kişisel verinin niteliğini tanımlamada esas unsurdur. Kişisel veriden bahsedebilmek için yalnızca o kişinin isim, soyadı gibi bilgilerin bilinmesi gerekmez. Birkaç veriyi bir araya getirdiğinizde kişi belirlenebilir hale geliyor ise o halde tüm o veriler kişisel veri niteliğindedir. Nitekim GDPR, *"söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktöre atıfta bulunularak doğrudan veya dolaylı olarak tanımlanabilen bir kişidir."*[10] ifadesi ile belirlenebilirliğin tanımını yapmıştır.

Son olarak, ilişkinlik unsuru incelenmelidir. Bu unsurda önemli olan nokta, eldeki verinin ilgili kişiyi tekilleştirmesi, işaret etmesi ve onu tanımlayabilmesidir. Kişisel verinin gerçek kişiye ilişkin olması gerekmektedir. Kişinin adı soyadı, adresi, özel ve aile hayatı, sağlık geçmişi, hobileri, pasaport numarası vs. kendisine ilişkindir ve kişisel veridir. Bazı durumlarda gerçek kişiye ilişkin olma durumu bu kadar açık olmayabilir. Örneğin kişinin kullandığı telefonun IMEI numarası veya bilgisayarının MAC adresi gerçek kişiye ilişkin gibi görünmese dahi gerçek kişiyi belirli veya belirlenebilir hale getirdiği için aslında bu bilgiler de gerçek kişiye ilişkin olarak değerlendirilmelidir.[11] Nitekim Avrupa Birliği Adalet Divanı'nın (ABAD) C-434/16 sayılı 20/12/2017 tarihli Nowak Kararında, yüzlerce kişiye yönelik hazırlanan bir sınava tabi tutulan kişinin, söz konusu sınavdaki sorulara ilişkin vermiş olduğu yanıtları içeren bir cevap kâğıdı dahi ABAD tarafından kişisel veri olarak nitelendirilmiş ve bunun ilgili mevzuat kapsamında değerlendirilmesi gerektiği söylenmiştir.[12]

BLOKZİNCİR TEKNOLOJİSİNDE KİŞİSEL VERİLERİN 6698 SAYILI KANUN VE GDPR AÇISINDAN DEĞERLENDİRİLMESİ

Blokzincir yapısında yer alan verilerin kişisel veri niteliğini haiz olup olmadıkları tartışılması gereken en önemli konulardan biridir. Söz konusu verilerin, kişisel veri niteliğinde oldukları kabul edildiğinde, blokzincir ağlarında depolanan kişisel verilerin işlenmesi söz konusu olacak ve 6698 sayılı Kanun ile GDPR düzenlemeleri uygulama alanı bulacaktır.

10 GDPR, m.4

11 Türkiye Bilişim Vakfı, **"Kişisel Verilerin Korunması Hukuku ve Blokzinciri Teknolojisi Raporu"**, Kasım 2019, s.26-30

12 https://www.aabghukuk.com/post/avrupa-birli%C4%9Fi-adalet-divan%C4%B1-n%C4%B1n-ki%C5%9Fisel-verileri-koruma-hukukuna-y%C3%B6n-veren-kararlar%C4%B1(s.e.t.15.10.2021)

6698 sayılı Kanunun 2. maddesi uyarınca, Kişisel verilerin işlenmesi, *"Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi*,"[13] şeklinde tanımlanmıştır.

GDPR ise 4. maddesi ile işleme faaliyetini, *"otomatik yöntemlerle olsun veya olmasın, kişisel veri veya kişisel veri setleri üzerinde gerçekleştirilen toplama, kaydetme, düzenleme, yapılandırma, saklama, uyarlama veya değiştirme, elde etme, danışma, kullanma, iletim yoluyla açıklama, yayma veya kullanıma sunma, uyumlaştırma ya da birleştirme, kısıtlama, silme veya imha gibi herhangi bir işlem veya işlem dizisidir."*[14] şeklinde tanımlamıştır.

Blokzinciri oluşturan bloklar içinde işleme ait ve bloğun teknik yapısına ait olmak üzere iki tür veri bulunur. İşleme ait veriler içinde hesap numarası, transfere ilişkin veriler, yapılan işlem eğer bir sözleşme ise sözleşmeye ilişkin veriler yer almaktadır. Sayılan bilgi ve veriler başka veriler ile ilişkilendirildiğinde ise gerçek bir kişiyi işaret etmektedir. Bu sebeple işleme ait veriler kişisel veri niteliğini haizdir.

Blokzincir yapısının başlığında yer alan verilerin amacı, söz konusu bloğun o sistem nezdinde tanınmasını sağlamaktır. Bu aşamada bir gerçek kişiyi belirli veya belirlenebilir kılan ve gerçek kişiye ilişkin herhangi bir veri söz konusu olmadığından burada kişisel veri kavramından bahsedemeyiz.[15]

Blokzincir yapısında şifreleme veya kriptografik özetleme yöntemi ile şifrelenen veriler kişisel veri midir yoksa bu veriler anonimleştirilmiş veri midir ya da blokzincir yapısında yapılan tüm işlemler kişisel veri işleme faaliyeti midir gibi tartışmalar gündemdedir. Öncelikle şifrelenen verilerin anonimleştirilmiş veri olup olmadığının değerlendirilmesi kişisel veri niteliğinin tespiti açısından isabetli olacaktır.

6698 sayılı kanunun 2. maddesi ile *"anonim hale getirme (anonimyzation)"* kavramı, *"Kişisel verilerin, başka verilerle eşleştirilerek dahi*

13 6698 sayılı Kanun, m.2

14 GDPR, m.4

15 Osman Gazi Güçlütürk, **"Blokzincir Üzerinde Depolanan Verilerin Kişisel Veri Niteliği ve Silinmezlik, Yok Edilemezlik Sorunu"** , Kişisel Verileri Koruma Dergisi, 2019, s.30-40

hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi" olarak belirtilmektedir. GDPR ise Recital 26'da açıkladığı *"anonimleştirme"* kavramına ek olarak *"takma ad kullanımı* (*psudonymizasyon*)" kavramı getirerek m.4/5'te yer alan düzenleme ile "*kişisel verilerin tanımlanmış veya tanımlanabilir bir gerçek kişiyle ilişkilendirilmemesinin sağlanması amacı ile ek bilgilerin ayrı tutulması ve teknik ve düzenlemeye ilişkin tedbirlere tabi tutulması koşuluyla, kişisel verilerin söz konusu ek bilgiler kullanılmaksızın spesifik bir veri sahibiyle artık ilişkilendirilemeyecek şekilde işlenmesidir*."[16] şeklinde tanımlama yoluna gitmiştir.

Takma ad kullanımı, anonimleştirmeden tamamen farklı bir kavram olup takma ad yönteminde kişisel verilerin ancak kendisinden ayrı olarak tutulan bazı ek bilgiler ile birleştirildiğinde gerçek kişiyi belirli veya belirlenebilir kılması söz konusudur. Dolayısıyla takma ad kullanımı gerçekleştirilmiş bir veri hala kişisel veri niteliğini korumaya devam eder. Anonim hale getirilmiş bir veri ise artık kişisel veri kapsamında korunmamaktadır.

Blokzincirin öne çıkan özelliği şifreleme yöntemleri ve bu yöntemlerin sağladığı işlem güvenliğidir. Ağ üzerinde çeşitli ve teknik anlamda güçlü şifreleme yöntemleri kullanılarak işlemler yapılmaktadır. Ancak bu yöntemler verinin anonimleştirildiği algısını uyandırmamalıdır. Zira, söz konusu teknikler ile kişisel veriler yalnızca şifrelenmektedir. Söz konusu şifre bir şekilde çözüldüğünde ise gerçek kişiye ilişkin birtakım bilgiler açığa çıkmaktadır. Oysa anonimleştirme dediğimiz kavramda anonimleştirilmiş verinin geri döndürülemez bir hale gelmiş olması gerekmektedir. Kişisel veriye alternatif yollar ile ulaşamıyorsak ve böylelikle ilgili kişiye erişemiyorsak o zaman anonim hale getirilmiş bir kişisel veriden bahsetmek doğru olacaktır. Takma ad kullanımı olarak bildiğimiz pseudonymizasyonda ise eşleşen veriler farklı yerlerde tutulmakta ve bu veriler bir araya getirildiğinde gerçek kişiye ulaşma ihtimalini barındırdığından bu verilerin hala kişisel veri olduğundan bahsetmek yanlış olmayacaktır.

2020 yılında, Blockchain araştırma firması Elliptic'e göre, yasadışı internet pazarı olan Silk Road'a ait bir cüzdan, yaklaşık 1 milyar dolarlık Bitcoin (BTC) taşıdı. Elliptic'in kurucu ortağı Tom Robinson, gönderide Bitcoinlerin kriptografik anahtarları olduğu iddia edilen şifreli bir dosyanın hacker forumlarında dolaştığını söylemişti. Parola kırıldı ise, bir bilgisayar korsanı kripto parayı taşımış veya cüzdanın sahibinin, bu-

16 6698 sayılı Kanun, m.2

nun olmasını önlemek için onları taşımış olabileceği gündeme gelmişti.[17] Bu olayın akabinde, "*Attack of the 50 Foot Blockchain*" kitabının yazarı David Gerard, "*Bitcoin tamamen izlenebilir ve herkes bitcoinleri takip edebilir.*" ifadesinde bulunmuştur. Her ne kadar kriptografik yöntemlerle şifrelenmiş işlemlerin var olduğu bir platformdan bahsetsek de izlenebilirliği ve hacklenebilirliği bu verilerin halen kişisel veri niteliğini haiz olduğunu bizlere göstermektedir.[18]

Böylelikle blokzincir ağında *"anonimleştirmenin"* şartları sağlanmamakta ve veri, gerçek kişi ile ilişkilendirilebilecek şekle geri dönebilmektedir. Bu nedenlerle blokzincirde veri işleme faaliyetinde bulunulurken mutlaka 6698 sayılı Kanun ve GDPR ile uyumlu olunması gerektiği kanaatindeyiz.[19]

BLOKZİNCİR TEKNOLOJİSİNDE VERİ SORUMLUSU KAVRAMININ 6698 SAYILI KANUN VE GDPR AÇISINDAN DEĞERLENDİRİLMESİ

6698 sayılı kanunun 3. maddesine göre veri sorumlusu, *"Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi"* ifade eder.

GDPR'da ise 4. maddede, bu kavram *"kontrolör"* olarak karşımıza çıkmakta ve *"kontrolör"*, "*yalnız başına veya başkalarıyla birlikte kişisel verilerin işlenmesine ilişkin amaçları ve yöntemleri belirleyen gerçek veya tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organdır; söz konusu işleme amaçları ve yöntemlerinin Birlik ya da üye devlet hukukuna göre belirlenmesi durumunda, kontrolör veya kontrolörün belirlenmesine özgü kriterler Birlik ya da üye devlet hukukuna göre belirlenebilir.*" olarak tanımlanmaktadır.

Daha önce değinmiş olduğumuz üzere blokzincir merkeziyetsiz bir yapıya sahiptir. Merkezi olmayan, kontrolün tek merkezden gerçekleşmediği, dağıtık ve bağımsız yapıyı ifade eder.[20] Diğer yandan kişisel verilerin korunmasına ilişkin düzenlemelerin neredeyse hepsi merkezi sistemler esas alınarak hazırlanmıştır. Hem 6698 sayılı kanun hem de GDPR, merkezi bir veri sorumlusunun varlığı kabul edilerek düzenlenmiştir.

---

17 https://kriptokoin.com/silk-road-ile-baglantili-1-milyar-dolarlik-bitcoin-5-yil-sonra-harekete-gecti(s.e.t.15.10.2021)

18 https://www.bbc.com/news/technology-54810976(s.e.t.15.10.2021)

19 Türkiye Bilişim Vakfı, **"Kişisel Verilerin Korunması Hukuku ve Blokzinciri Teknolojisi Raporu"**, s.59-63

20 Türkiye Bilişim Vakfı, **"Blokzinciri Teknolojisi Terminoloji Çalışması"** , Haziran, 2019, s.22-24

Veri sorumlusu kavramı hem kişisel verilerin korunmasına ilişkin yasal düzenlemeler açısından hem de blokzincir ağı bakımından kilit bir konumdadır. Yasal düzenlemelerin veri sorumlusuna yüklediği birtakım yükümlülükler söz konusudur. Bunlar; ilgili kişinin verilerinin mevzuata uygun işlenmesi, ilgili kişinin talebi halinde cevap verme yükümlülüğü, veri sorumlusunun aydınlatma yükümlülüğü ve kişisel veriler için gerekli idari ve teknik tedbirleri alma yükümlülükleridir. Bu sebeple, bir sistemde veri sorumlusu tespit edilemediğinde kişisel verilerin korunması mevzuatının anlamsız hale geldiğini söylemek yanlış olmayacaktır. Diğer yandan, blokzincir ağında veri sorumlusunun tespiti oldukça zordur. Bu sebeple blokzincir gibi merkeziyetsiz bir yapıda veri sorumlusu kavramı çeşitli tartışmalara yol açmaktadır.[21]

Bilindiği üzere, kapalı blokzincir ile izin gerektirmeyen ve açık blokzincir ağı olmak üzere iki tür ağ bulunmaktadır. Kapalı sistemde veri sorumlusunun tespiti daha kolaydır. Bunun sebebi, ağa erişime izin veren kişiler ile sistemin sorumlularının aynı kişiler olmasıdır.[22]

Açık sistemde ise merkeziyetsiz yapı göz önünde bulundurulduğunda tek bir veri sorumlusunun tespiti neredeyse imkansızdır. Fransız Veri Koruma Otoritesi (CNIL) en kısa sürede veri sorumlusu veya ortak veri sorumlularının kim olacağının tespit edilmesine ilişkin çağrıda bulunmuştur.[23] Ancak böyle bir durum söz konusu olduğunda blokzincirin merkeziyetsizlik yapısı zedelenecektir.

BLOKZİNCİR TEKNOLOJİSİNDE KİŞİSEL VERİLERİN SİLİNEMEZLİK VE YOK EDİLEMEZLİK SORUNUNUN 6698 SAYILI KANUN VE GDPR AÇISINDAN DEĞERLENDİRİLMESİ

Blokzincir teknolojisi ile Kişisel Verilerin Korunması Kanunu'nun ters düştüğü noktalardan biri de kişisel verilerin *"işlenme amacına uygun olan süre kadar muhafaza edilmesi"* ilkesi ile *"doğru ve gerektiğinde güncel olma"* ilkesidir.

Kişisel verinin *"işlenme amacına uygun olan sure kadar muhafaza edilmesi"* ilkesi, 6698 sayılı Kanunun 7. maddesi ile *"Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel ve-*

21 Türkiye Bilişim Vakfı, **"Kişisel Verilerin Korunması Hukuku ve Blokzinciri Teknolojisi Raporu",** s.40-42

22 Güçlütürk**, "Blokzincir Üzerinde Depolanan Verilerin Kişisel Veri Niteliği ve Silinmezlik, Yok Edilemezlik Sorunu, Kişisel Verileri Koruma Dergisi"** , s.30-40

23 https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data (s.e.t.15.10.2021)

riler re'sen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir." şeklinde düzenlenmiştir.

Veri sorumlusu tarafından kişisel verinin amaçla sınırlı olarak muhafaza edileceği süre veya veri sorumlusunun tabi olduğu mevzuat uyarınca kişisel verinin muhafaza edileceği süre belirlenmiş olabilir. Her iki halde de zamanı geldiğinde kişisel veri silinmeli, yok edilmeli veya anonim hale getirilmelidir.[24]

Kişisel verinin *"doğru ve gerektiğinde güncel olma"* ilkesi ise 6698 sayılı Kanunun *"İlgili Kişinin Hakları"* başlıklı 11. Maddesi ve GDPR'ın *"Düzeltme ve Silme (Unutulma) Hakkı"* başlıklı 16. ve 17. maddeleri ile düzenlenmiş olup ilgili maddelerde sayılan hallerde ilgili kişinin düzeltme talep hakkı ve veri sorumlusunun silme yükümlülüğü bulunmaktadır.

Blokzincir ağında veriler dağıtık defter teknolojisi üzerinden birden çok birimde depolandığından merkezi sistemlerin aksine merkezi olmayan sistem üzerinden veriyi silmek yoluyla diğer birimlerin erişimini engellemek mümkün değildir. Nitekim her birim isteğe bağlı olarak tüm blokzincir üzerindeki veri tabanının bir kopyasını cihazına indirebilmektedir. Birimler tarafından indirilen kopyalar blokzincirin temelinde yer alan yazılım tarafından belirlenmiş kurallara tabidir. Yeni eklenecek verilerin seçimi de yine tek bir kişi ya da kurumun tekelinde olmadığından bir emir ya da talimat yoluyla kişisel verilere erişimin engellenmesi, kişisel verilerin silinmesi ve yok edilmesi de mümkün olmamaktadır. Blokzincir sistemine yanlış bir veri girildiğinde bunun silinebilirliği ve düzeltilmesi de neredeyse imkansızdır.[25]

Blokzincir teknolojisi ise *"silinemezlik"* ve *"değiştirilemezlik"* ilkeleri üzerine kurulu bir sistem olması sebebi ile ilgili yasal düzenlemeler arasında çatışma yaşanmakta olup bu durumun çözülmesi için çeşitli öneriler ortaya atılmaktadır. Bunlardan biri özel anahtarın yok edilmesinin silinme olarak değerlendirilmesi iken bir diğeri de kişisel veri niteliğindeki verilerin blokzincir dışında bir yerde depolanması, blokzincirde ise sadece Hash değerinin depolanması şeklindedir. Ancak hem blokzincirin temel ilkeleri ile ters düşmeyip hem de kişisel verilerin korunması mevzuatı ile uyumlu bir çözüm henüz bulunamamıştır.[26]

SONUÇ

Blokzincir teknolojisinin teknik alt yapısı ve genel prensipleri ile kişisel verilerin korunmasına ilişkin yasal mevzuat bu araştırma kapsamında incelenen dört noktaya ters düşmektedir. Bunlar, anonimleştirmenin

24 Elif Küzeci, **Kişisel Verilerin Korunması**, 4. Baskı, Mayıs, 2020, s.200-275

25 Güçlütürk, **"Blokzincir Üzerinde Depolanan Verilerin Kişisel Veri Niteliği ve Silinmezlik, Yok Edilemezlik Sorunu",** Kişisel Verileri Koruma Dergisi, s.35-40

26 Türkiye Bilişim Vakfı, **"Blokzinciri Teknolojisi Terminoloji Çalışması"**

zorluğu, silinemezlik, değiştirilemezlik ve veri sorumlusunun belirsizliğidir. Blokzincir ağında bulunan veriler şifrelenmiş olsalar dahi kişisel veri niteliğinde olduklarından hem 6698 sayılı kanuna hem de GDPR'a tabidirler. Bu yasal mevzuata tabi olmak için bir veri sorumlusunun tespiti gerekirken blokzincirin merkeziyetsiz yapısı nedeniyle veri sorumlusunun tespiti mümkün olmamaktadır. Bu nedenle veri sorumlusuna ait yükümlülüklerin kim tarafından yerine getirileceği belli olmadığı gibi ilgili kişi de mağdur olmaktadır. Bunun yanında yine veri sorumlusuna yüklenen yükümlülüklerden kişisel veriyi *"işlenme amacı ile sınırlı süre kadar muhafaza etme" ve kişisel verinin "doğru ve gerektiğinde güncel olma"* ilkeleri gereği kişisel verinin belli zamanlarda silinmesi, yok edilmesi veya anonim hale getirilmesi gerekmektedir. Ancak blokzincirin dağıtık defter teknolojisi kişisel verinin silinmesine, değiştirilmesine ve yok edilmesine izin vermemektedir. Bu sorunları aşmak için birtakım önerilerde bulunulsa da henüz hem blokzincirin hem de kişisel verilerin korunması ilkeleriyle örtüşen ortak bir çözüme kavuşulamamıştır.

KAYNAKÇA

CAROLL, Richard, ,Bitcoin Secrets Revealed: The Complete Guide to Understanding Bitcoin, Cryptocurrency, and the Blockchain.

DEDEOĞLU, Daron, A'dan Z'ye Blockchain, Kodlab, 2019.General Data Protection Law. General Data Protection Regulation(GDPR).

GÜÇLÜTÜRK, Osman Gazi, Blokzincir Üzerinde Depolanan Verilerin Kişisel Veri Niteliği ve Silinmezlik, Yok Edilemezlik Sorunu, Kişisel Verileri Koruma Dergisi, 2019, s.30-40.

GÜVEN, Vedat; ŞAHİNÖZ, Erkin, Blokzincir Kripto Paralar Bitcoin, Kronik, İstanbul, 2020.

KÜZECİ, Elif, Kişisel Verilerin Korunması, 4. Baskı, Mayıs, 2020.

PANDA, Sandeep Kumar; ELNGAR, Ahmed A.; BALAS, Valentina Emilia; KAYED Muhammed, Bitcoin and Bitcoinchain History and Current Applications, 2020.

Türkiye Bilişim Vakfı, Kişisel Verilerin Korunması Hukuku ve Blokzinciri Teknolojisi Raporu, Kasım 2019.

Türkiye Bilişim Vakfı, Blokzinciri Teknolojisi Terminoloji Çalışması, Haziran, 2019.

6698 sayılı Kişisel Verilerin Korunması Kanunu.

http://yasaizleme.org.tr/kisisel-verilerin-korunmasi-kanununun-uygulanma-sureci/(s.e.t.15.10.2021)

https://www.kisiselverilerinkorunmasi.org/mevzuat/avrupa-birligi-genel-veri-koruma-tuzugu-gdpr-turkce-ceviri/(s.e.t.15.10.2021)

https://www.aabghukuk.com/post/avrupa-birli%C4%9Fi-adalet-(s.e.t.15.10.2021)

https://kriptokoin.com/silk-road-ile-baglantili-1-milyar-dolarlik-bitcoin-5-yil-sonra-harekete-gecti/(s.e.t.15.10.2021)

https://www.bbc.com/news/technology-54810976(s.e.t.15.10.2021)

https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data(s.e.t.15.10.2021)

divan%C4%B1-n%C4%B1n-ki%C5%9Fisel-verileri-koruma-hukukuna-y%C3%B6n-veren-kararlar%C4%B1(s.e.t.15.10.2021)