Bilgi Yönetimi Dergisi

Cilt: 5 Sayı: 1 Yıl: 2022

https://dergipark.org.tr/tr/pub/by

Hakemli Makaleler

Araştırma Makalesi

Makale Bilgisi

Gönderildiği tarih: 25.09.2021
Kabul tarihi: 02.11.2021
Erken görünüm: 25.04.2022
Yayınlanma tarihi: 30.06.2022

Article Info

Date submitted: 25.09.2021
Date accepted: 02.11.2021
Date early view 25.04.2022
Date published: 30.06.2022

Anahtar sözcükler

Blokzincir, Kişisel Veri, Mahremiyet

Keywords

Blockchain, Personal Data, Privacy

DOI numarası

10.33721/by.1000702

ORCID

0000-0003-1238-6724 (1)
0000-0003-2393-5207 (2)

CC BY

Blokzincir Uygulamalarında Kişisel Veri Problemi: Depolama Riskleri ve Öneriler[1]

Personal Data Problem in Blockchain Applications: Storage Risks and Implications

Nurcan DİRİ
Marmara Üniversitesi Bilgi ve Belge Yönetimi Bölümü Yüksek Lisans Öğrencisi, *nurcan.diri.18@gmail.com*

Bahattin YALÇINKAYA
Marmara Üniversitesi Bilgi ve Belge Yönetimi Bölümü Öğretim Üyesi, *yalcinkaya@marmara.edu.tr*

Öz

Bilgi ve İletişim Teknolojilerinin (BİT) hızla gelişmesiyle birlikte, çok miktarda kişisel veri oluşmakta, kullanılmakta ve depolanmaktadır. Depolanmakta olan kişisel veriler, son kullanıcıların teknik ve hukuki yönlerden korunmalarını gerektirmektedir. Blokzincir teknolojisi kişisel verilerin gizliliğini korumak ve kontrolünü sağlamak için son yıllarda önemli gelişmeler kaydeden yenilikçi teknoloji olarak görülmektedir. Merkezi olmayan ve Eşler Arası (Peer-to-Peer-P2P)[2] bir dağıtık dijital defter olan blokzincir teknolojisi, dijital varlıkların tüm işlemlerini depolayabilen, merkezi olmayan, doğrulanabilir ve değiştirilemez bir defter hizmeti sunar. Bir ağdaki katılımcılarla onlara tam olarak güvenmeye gerek kalmadan veri paylaşma konusunda yeni bir yaklaşım sunmaktadır. Yakın zamanda tanıtılan Genel Veri Koruma Yönetmeliği (GDPR) ve Kişisel Verilerin Korunması Kanunu (KVKK), kişisel verilerin nasıl ele alınacağı konusunda büyük değişiklikler getirmektedir. GDPR ve KVKK, kişisel verilerin kullanmasıyla veri denetleyicileri ve işlemciler için yeni koruma zorunlulukları getirmiştir. GDPR ve KVKK, veri koruma mevzuatı kapsamında birliğinin sağlanması için kişisel olarak tanımlanan verilere (PII) daha kolay erişim, silme, düzeltme ve taşıma hakkı verilmesi gibi yeni uygulamalar getirmektedir. GDPR ve KVKK kapsamında, merkezi yapıların hâkim olduğu bir toplumda kişisel veri işleme faaliyetlerinin çoğunlukla merkezi yapılar tarafından gerçekleştirilmesi ve uyulması gereken bir takım usul ve esasları vardır. Ancak blokzincir platformunda ortaya koyulan araştırmalarda kişisel olarak tanımlanan verilerin saklanmasında; merkezi tüzel veya gerçek kişilerin veri saklama, işleme ve silme, gibi uygulamaları gerçekleştirmesi yönünde hazırlanan KVKK ve GDPR hükümlerinin uygulanmasında bazı uyumsuzluklar bulunmaktadır. Bu çalışmada, blokzincirin temel özellikleri detaylandırılmış, kişisel verilerinin kullanımı için blokzincir teknolojisi destekli çözümler açıklanmış ve konuya dair sorunlar ile zorlukları tartışılmıştır. Literatür incelendiğinde; kişisel verilerin günümüzde blokzincir ağında saklanmamasına yönelik tavsiyeler verildiği görülmüştür. Kişisel verilerin KVKK ve GDPR kapsamındaki birincil haklarının, blokzincir teknolojisinin karakteristik yapısına uygun olmadığı, akademik ve uygulamalı araştırmalarda gösterilmiştir. Blokzincir teknolojisindeki gelişme ve güncellemelerin, teknolojinin kendisi ile çelişeceği ve blokzincirin karakteristik özelliğini yok edeceği akademik çevrelerce düşünülmekte ve bundan dolayı temel yapıyı etkilemeyecek (özel anahtarın silinmesi, zincir dışı depolama, karma değeri silinmesi vb.) küçük çaplı değişikliklerin yapılması önerilmektedir.

[1] *Bu makalenin araştırma ve yayın süreci "Araştırma ve Yayın Etiğine" uygun şekilde yürütülmüştür. Bu çalışma, Marmara Üniversitesi Fen Bilimleri Enstitüsü, Bilgi Güvenliği Mühendisliği Bölümü yürütülen Blokzincir Uygulamasında Kişisel Verilerin Tutulması" başlıklı yüksek lisans tezine dayanarak hazırlanmıştır.*

[2] *Bilgisayar biliminde, eşler arası ağ olarak da bilinen P2P'nin tanımı, birbirleriyle bilgi paylaşmak ve depolamak için birbirine bağlı bir grup cihazdan (düğüm) oluşan merkezi olmayan bir ağ iletişim modelidir. Her düğüm veya cihaz, ayrı bir sunucu gibi davranır.*

Abstract

A large amount of personal data is created, used and stored by the rapid development of Information and Communication Technologies (ICT). The personal data being stored requires the end users to be protected from technical and legal aspects. Blockchain technology is seen as an innovative technology that has made significant progress in recent years to protect the privacy and control of personal data. As a decentralized Peer-to-Peer (P2P)[3] distributed digital ledger, Blockchain technology provides a decentralized, verifiable and immutable ledger service that can store all transactions of digital assets. It offers a new approach to sharing data with participants in a network without having to fully trust them. The recently introduced General Data Protection Regulation (GDPR) and Personal Data Protection Law (KVKK) bring major changes in how personal data is handled. GDPR and KVKK have brought new protection obligations for data controllers and processors with the use of personal data. In order to ensure unity within the scope of GDPR and KVKK data protection legislation, it brings new applications such as easier access to Personally Identifiable Information (PII), giving the right to delete and rectify and transport. In a society dominated by centralized structures within the scope of GDPR and KVKK, personal data processing activities are mostly carried out by central structures and there are a number of procedures and principles that must be followed. However, there are some inconsistencies in the implementation of the KVKK and GDPR provisions, which are prepared for the central legal or natural persons to carry out applications such as data storage, processing and deletion in the storage of personally-identified data in the researches revealed on the blockchain platform. In this study, the basic features of the blockchain are elaborated, blockchain technology supported solutions for the use of personal data are explained, and the problems and difficulties related to the subject are discussed. When the literature is examined, it has been seen that recommendations are given for not storing personal data in the blockchain network today. It has been shown in academic and applied research that the primary rights of personal data within the scope of KVKK and GDPR are not suitable for the characteristic structure of blockchain technology. Also, it is thought by academic circles that developments and updates in blockchain technology will contradict the technology itself and annihilate the characteristic feature of the blockchain, and therefore it is recommended to make minor changes that not affect the main structure (deleting the private key, off-chain storage, deleting the hash value, etc.).

1. Giriş

Günümüzün dijitalleşen dünyasında veri miktarı olağanüstü hızda ve sürekli artmaktadır. Veriler bir yandan aralıksız toplanırken diğer yandan anlık olarak analiz edilmekte; böylece sağlık, ekonomi, siyaset, uluslararası ilişkiler, finans piyasaları gibi alanlarda çeşitli ölçeklerde uygulanabilir bilgi (knowledge) üretilmekte ve tekrar kullanılmaktadır. Küresel şirketler, devletler ve veri ile çalışan diğer organizasyonlar topladıkları verileri; hizmetleri kişiselleştirmek, gelecekteki eğilimleri tahmin etmek ve uygun stratejiler oluşturmak için kullanmakta; ayrıca mevcut teknolojileri ve analiz yöntemlerini daha da geliştirmekle meşgul olmaktadır (Zyskind ve diğerleri, 2015). Örneğin; web siteleri, çeşitli oturum açma verileriyle (Sosyal güvenlik numarası, IP adresi, Konum verisi, Ehliyet, kimlik ve pasaport verileri vb.) neredeyse sonsuz sayıda Kişisel olarak Tanımlanabilir Bilgi (Personally Identifiable Information-PII)[4] toplamaktadır (Grimes, 2021). Yaklaşık beş milyar internet kullanıcısının %70'inden fazlası (3.60 milyar) sosyal ağ sitelerini (Social Network Site-SNS) kullanmakta ve çok sayıda kişisel bilgiyi platformlara kaydetmektedir. Çoğunlukla küresel şirketler, oluşturulan kullanıcı profilleriyle çeşitli iş modelleri geliştirerek kişisel verileri depolamakta ve analiz etmektedir.

Gerek elektronik ortamdaki kişisel verilerin (büyük veri bağlamında), gerekse bu verilerin kullanımını "dijital bir kaos"a meydan vermeden üçüncü taraflarca kullanımına bir sınır ve standart getirmek amacıyla geliştirilen mevzuata Genel Veri Koruma Yönetmeliği (General Data Protection Regulation-GDPR)[5] ve Kişisel Verilerin Korunması Kanunu (KVKK)[6] örnek olarak verilebilir. Her iki düzenleme

[3] *In computer science, the definition of P2P, also known as peer-to-peer networking, is a decentralized network communication model consisting of a group of interconnected devices (nodes) to share and store information with each other. Each node or device acts as a separate server.*

[4] *Kişisel olarak tanımlanabilir bilgiler veya PII, bir kişiyi doğrudan veya dolaylı olarak tanımlamak için kullanılabilecek herhangi bir bilgi parçasıdır. PII, ad, sosyal güvenlik numarası, doğum tarihi ve yeri, anne kızlık soyadı veya biyometrik kayıtlar gibi bir bireyin kimliğini ayırt etmek veya izlemek için kullanılabilecek bilgiler de dahil olmak üzere bir kişiyle ilgili her türlü bilgi ve tıbbi, eğitim, finans ve istihdam bilgileri gibi bir bireye bağlanabilen diğer bilgilerdir.*

[5] *GDPR, Avrupa Birliği'nde (AB) yaşayan bireylerden kişisel bilgilerin toplanması ve işlenmesi için yönergeler belirleyen yasal bir çerçevedir. Şirketler ve tüm bilgi sistemleri bu yeni gizlilik yasası ile başa çıkmak zorundadır. GDPR, günümüz dijital ortamında kişisel veri koruma düzeyini iyileştirmek için geliştirilmiştir.*

[6] *KVKK ise Türkiye'de kişisel verilerin korunmasını düzenleyen ve kişisel verileri işleyen kurum ve kişilerin uyması gereken yasal*

de kişisel verileri yöneten ve işleyen hizmet sağlayıcılarına daha katı kurallar getirip yükümlülükler vererek, kişisel verilerin kullanımına dair kontrolü sağlayan iki örnek mevzuat olarak karşımıza çıkmaktadır. Wirth ve Kolain (2018) kişisel verinin asıl sahibi olan son kullanıcılara, verilerin işlenmesiyle ilgili çok az bilgilendirme yapıldığı ve hatta herhangi bir bilgi verilmediğini vurgulamaktadır. Günümüzde en çok kullanıcıya sahip uygulama olan Facebook, kuruluşundan bu yana yaklaşık 300 PB[7] kişisel veri toplamıştır. Kişisel veriler, her ne kadar bir süredir dünya ekonomisi açısından değerli bir varlık olarak görülse de, verilerin asıl sahipleri olan gerçek veya tüzel kişiler açısından verilerin gizliliği ve işlenmesiyle ilgili büyük bir endişe hâkimdir (Fu ve Fang, 2016). Kişisel verilerin kötüye kullanımı ile gizlilik ve güvenlik endişeleri günümüzde geçerli olan veri kullanım modellerinin sorgulanmasına neden olmuştur.

Potansiyel olarak yüksek risk içeren kişisel verilerin kullanımında blokzincir (blockchain) mantığı, bahsedilen çekince ve sorunların çözümünde ön plana çıkan yeni bir teknoloji olarak göze çarpmaktadır. Blokzincir, kullanıcılara; kendilerine ait verilerin işlenmesi, dağıtılması ve kontrolü gibi kritik bilgileri merkezi olmayan, doğrulanabilir, şeffaf, güvenli, veri odaklı ve kimlik yönetimi özellikleriyle iletmede en iyi bilinen ve kullanılan dağıtılmış defter teknolojisi olarak görülmektedir (Danyal, 2021). Blokzincir teknolojisi; kayıtların, kanıtların ve kurumsal hafızanın korunmasına yardımcı olabilir, çünkü bir blokzincir ağına kaydedilen verilerin değiştirilmesi neredeyse imkânsız ve üçüncü bir tarafın (merkezi sunucular vb.) kontrolü altında değildir (Nayak ve Dutta, 2017). Blokzincir teknolojisinin getirdiği çözüm; verilerin şifresini kırabilmek için birçok tarafın işbirliğini gerekli kılmaktadır. Sisteme dâhil olmak isteyen bir kullanıcının kimliğini doğrulamak için kriptografik yöntemler (simetrik ve asimetrik şifreleme, karma yapıları vb.) ile ortak anahtar altyapısı kullanılarak verilerin şifrelemesi sağlanmaktadır. Böylece veri ihlal riskleri azaltabilir ve sistemin daha güvenli işlemesi sağlanır (Mamoshina ve diğerleri, 2018).

Blokzincir tabanlı veri paylaşım sistemi, araştırma ve ticari projeler için veri toplama sürecini önemli ölçüde basitleştirebilir. Bu durumda, kullanıcılar kendi verilerinin sahipliğini ve ayrıcalıklarını kazanma ile bunlardan yararlanma fırsatını da elde etmiş olur. Ayrıca veri sahipleri, verileri üzerinde daha iyi kontrole sahip olabilir ve tüm veri kullanım süreçlerini ayrıntılı bir şekilde izleyebilir (Mamoshina ve diğerleri, 2018). Literatürde kişisel verilerin kontrolü ve denetimine yönelik blokzincir uygulamalarını detaylandıran, KVKK ve GDPR gibi yasal düzenlemeler kapsamında bahsedilen teknolojiyle azami uyum sağlayabilecek öneriler sunan çalışmalar bulunmaktadır (Zyskind ve diğerleri, 2015; Neisse ve diğerleri, 2017; Zheng ve diğerleri, 2018; Pagallo ve diğerleri, 2018; Truong ve diğerleri, 2019; Faber ve diğerleri, 2019; Lee ve diğerleri, 2019; Desai ve diğerleri, 2020; Shrestha ve diğerleri, 2020; Ateniese ve diğerleri, 2017).

GDPR ve KVKK'nın en önemli özelliklerinin başında, veri sahiplerine verileri üzerinde daha kapsamlı kontrol imkânı sağlaması gelmektedir. KVKK ve GDPR, kişisel verileri koruma mevzuatında birliğin sağlanması için kişisel olarak tanımlanan verilere kolayca erişim, düzeltme ve silme hakkı ile veri taşınabilirliği gibi çeşitli haklar getiren yenilikçi düzenlemelerdir. Bununla birlikte, Blokzincir teknolojisinin karakteristik yapısı, kişisel verilerin korunması ve saklanması kapsamında GDPR ve KVKK ile uyumsuzluk göstermektedir (KVKK ve Blokzincir Teknolojisi Raporu, 2019). Çalışmanın ana temasını oluşturan bu uyumsuzluklar:

- ✓ Veri bütünlüğünü sağlayan blokzincir teknolojisi kullanılarak dağıtık veri tabanlarında işlenen verilerin değiştirilemez olması,
- ✓ Blokzincir teknolojisi kullanan uygulamalarda verilerin silinemez olması,
- ✓ Ağdaki tüm kullanıcıların herkesin verisini görmesi ve kopyasını barındırmasıdır.

Blokzincir teknolojisinde kişisel olarak tanımlanan verilerin depolama mimarisi, verilerin "değişmezliğine" dayanmaktadır. Ancak KVKK ve GDPR kapsamında, kullanıcılar verilerin değiştirilmesi ve silinmesi isteğinde bulunabilir (Shah ve diğerleri, 2019).

yükümlülükleri belirleyen ilk kanundur. KVKK'nın yürürlüğe girmesinden önce Türkiye'de kişisel verilerin korunmasına ilişkin özel bir kanun yoktu. GDPR ve KVKK ile ilgili detaylar Bölüm 3'te verildi.

[7] *1 Petabyte = 1024 Terabyte*

1.1. Araştırmanın Amacı, Problemi ve Hipotezi

Bu çalışmada; kişisel verilerin blokzincir üzerinde depolanması, denetlenmesi, korunması ve kontrol edilebilmesi için GDPR ve KVKK ile uyumlu blokzincir uygulamalarının nasıl kullanılacağına dair yol gösterilmesi, araştırmacılara temel bir kaynak oluşturulması ve mevcut sorulara cevap aramak açısından geleceğe ilişkin bir yön çizilmesi hedeflenmiştir. Çalışmanın temelinde, GDPR ve KVKK mevzuatı ile uyumlu blokzincir uygulamaları incelenmiş ve değerlendirilmiştir. Kişisel verilerin KVKK ve GDPR kapsamındaki "erişim veya düzenleme", "silme ve işlemeyi kısıtlama", "unutulma" ve "bilgilendirme" gibi birincil hakların blokzincir teknolojisinin karakteristik yapısına uygunluğu tartışılmıştır. Ayrıca mevcut bilgiler özetlenerek blokzincir teknolojisi ile kişisel verilerin işlenmesi ve kontrol edilmesi için GDPR ve KVKK'ya uygun kavramların derinlemesine analizi yapılmıştır. KVKK ve GDPR ile uyumlu şeffaf ve sabit bir şema oluşturmak için kişisel verilerin farklı bir şekilde saklanması ile ilgili yapılan çalışmalar incelenerek değerlendirilmiştir. Kullanıcılara, verilerini kontrol etme ve bu tür verilerin paylaşılıp işlenmesine dair bir kısıtlama hakkı vermek için örnek blokzincir ortamları ele alınarak, gizlilik ve güvenliği optimize etmek için çeşitli blokzincir tekniklerden yararlanılmıştır.

Blokzincir teknolojisi, hem tüketicilerin bilgilerini hem de işletmelerin itibarını korumak için ihtiyaç duydukları en yeni depolama teknolojilerinden biridir. Yaşamın daha fazla çevrimiçi olması, her zamankinden daha fazla veri ihlali ve saldırı olasılıklarını artırmıştır. Dolaysıyla bu çalışma, blokzincir teknolojisinin mevcut merkezi ve dağıtık veri güvenliği çözümlerini nasıl iyileştirebileceğine ve kontrolü kullanıcının kendisinde tutmasına nasıl yardımcı olabileceğini göstermek için KVKK ve GDPR uyumlu yapılan çalışmaları baz alarak, blokzincir ortamında kişisel veri probleminin nasıl çözülebileceğine dair bir yol ortaya koymuştur.

2. Literatür Değerlendirmesi

Literatür incelendiğinde; zincir dışı depolama ve kişisel verilerin blokzincir ağında GDPR uyumlu işlenmesi en çok tartışılan kavramlar olarak görülmüştür. Kişisel verilerin "zincir dışı" saklanması, kişisel veriler veya genel olarak faydalı olan verilerin blokzincir ağında tutulmadığı, ancak dışarıda, geleneksel bir veri tabanında depolandığı anlamına gelir (Esposito ve diğerleri, 2018; Ibáñez ve diğerleri, 2018). Gerçek verilerin depolandığı dış depolama konumuna ise yalnızca bir referans blokzincir ağına kaydedilir (Katuwal ve diğerleri, 2018; Zyskind ve diğerleri, 2015; Steichen ve diğerleri, 2018; Pagallo ve diğerleri, 2018; Van Humbeeck 2017). Genel olarak bir blokzincir ağının dışında daha büyük veri kümelerinin depolanması tavsiye edilmektedir, çünkü bir blokzincir üzerindeki depolama kapasitesi maliyetlidir (Zhangy ve diğerleri, 2018) ve şu anda çok yüksek performans göstermez (Jensen 2018). Bir blokzincir ağında 1 GB veri depolamanın maliyeti yaklaşık olarak 17.500 Ethereum'dur (Omaar, 2017).

Eberhardt ve Tai (2017), zincir dışı konum için dosyaları adlarına göre değil, karma değerlerine göre depolayan içerik adreslenebilir bir depolama kullanılmasını önermektedir. Bu, verilerin güvenilir bir şekilde dışarıdan temin edilmesi için bir avantaj sağlar, çünkü verilerdeki bir değişiklik, karma değerinin ve dolayısıyla depolama konumunun değişmesine yol açacaktır (Eberhardt ve Tai, 2017).

Zyskind ve diğerleri (2015), blokzinciri dağıtılmış bir dosya sistemi ile birlikte kullanmak ve merkezi bir depolama konumundan kaçınmak için yalnızca referansı zincir üzerinde depolamak için bir çözüm buldu. Uygulamada, Steichen ve diğerleri (2018), Desai ve diğerleri (2020) ve Gräther ve diğerleri (2018) uygulamalarında bu teknikten yararlanmaktadır. Hepsi de içerik adreslenebilir depolama sistemi olarak merkezi olmayan Gezegenler Arası Dosya Sistemi (InterPlanetary File System - IPFS)[8] kullanır. Bu, merkezi bir konuma ihtiyaç olmadığı ve verilerin dosya sisteminde depolanma şekliyle güvenin sağlandığı anlamına gelir. Van Humbeeck (2017) ise biraz daha farklı bir kavram sunmaktadır: Veriler de zincir dışında saklanır, ancak merkezi bir konumda veya içerik adreslenebilir bir depolamada değil, bunun yerine blokzincir ağının her bir katılımcısının arka uç sisteminde saklanır. Blokzincirin kendisi yalnızca zincir dışı konumlara ve istenen verilerin karma değerlerine bağlantılar

[8] *Gezegenler Arası Dosya Sistemi (InterPlanetary File System - IPFS), verileri dağıtılmış bir dosya sisteminde tutmak ve paylaşmak için bir protokol ve eşler arası ağdır. IPFS, tüm bilgi işlem cihazlarını birleştiren bir ad alanındaki her dosyayı benzersiz bir şekilde tanımlamak için içerik adreslemeyi kullanır.*

içerir. Bir katılımcının ayrıcalığı ve belirli bir veri kümesine erişme ihtiyacı varsa, verinin depolandığı yere referansı ve ilgili karma değeri alır. Ardından, istek sahibi, verileri depolandığı arka uç sisteminden doğrudan alabilir. GDPR bağlamında, kişisel verilerin zincir dışında saklanması, ilk bakışta birçok fayda sağlar. Bazı uzmanlar, bu prosedürle hiçbir kişisel verinin blokzincir ağında tutulmadığını ve bu nedenle GDPR gerekliliklerinin karşılanabileceğini iddia etmektedirler (Steichen ve diğerleri, 2018; Katuwal ve diğerleri, 2018; Ibáñez ve diğerleri, 2018).

Günümüzde, kişisel verilerin özet değerlerinin anonim veriler olarak kabul edilebileceği veya daha büyük olasılıkla takma adlı veriler olarak ele alınması gerektiği kesin olarak söylenememektedir (Eichler ve diğerleri, 2018). Bu itiraz, Avrupa Komisyonu'nun eski bir danışma organı olan Data Protection Working Party (2014) tarafından hazırlanan ve karma tekniklerin takma ad olarak değerlendirilmesi gerektiğini açıkça belirten bir raporuna dayanmaktadır. Özetlenmiş kişisel verilerin takma adlı veri olarak kabul edilmesi gerektiği halen yoğun bir şekilde tartışılmakta, ancak literatürde yaygın olarak kabul edildiği görülmektedir (Finck, 2018; Ibáñez ve diğerleri, 2018; Jensen, 2018). Kişisel verilerin özet değerinin takma adlı kişisel veri olarak kabul edilip edilmeyeceği önermesi, aralarındaki bağlantı kurulabilirliğe, yani özetlenmiş verinin orijinal veri ile ilişkilendirilme olasılığına bağlıdır. Data Protection Working Party (2014), bir özet tersine çevrilemese bile, girdi değerleri aralığı ve özet işlevi biliniyorsa, basitçe yeniden hesaplanabileceğini iddia eder.

Fransız Ulusal Bilişim ve Özgürlük Komisyonu, CNIL (2018), blokzincir ve kişisel verilerin sorumlu kullanımı hakkında bir rapor yayınlayarak, kişisel verilerin yalnızca bir kriptografik taahhüt olarak bir blokzincir üzerinde saklanmasını önermiştir. Bu mümkün olmadığında, kişisel veriler blokzincir ağında anahtarlanmış bir karma değer olarak saklanmalıdır. Ancak bu da mümkün değilse, son teknoloji şifreleme algoritmaları uygulanmalıdır. Özellikle ilgili kişilerin unutulma ve düzeltme haklarına bakıldığında bunların yerine getirilmesi teknik olarak mümkün değildir. Ancak CNIL (2018), son teknoloji anahtarların ve algoritmaların kullanılmasıyla istenen etkilere yaklaşmanın mümkün olduğunu savunmaktadır. Kişisel verilerin silinmesi, zincir dışı veriler ve zincirde depolanan karma değeri oluşturmak için kullanılan ilgili anahtar silinerek gerçekleştirilebilir. Bu durumda, verileri kanıtlamak veya doğrulamak mümkün değildir (CNIL 2018) ve zincirde kalan veriler anonim veriler olarak kabul edilebilir (Eichler ve diğerleri, 2018). Düzeltme hakkı göz önüne alındığında, daha önce açıklandığı gibi eski veri seti silinebilir ve düzeltilmiş verileri içeren yeni bir işlem blokzincir ağına gönderilebilir. Özetle, zincir üzerinde kişisel verilere dayalı kriptografik referanslarla çalışmanın, blokzincir kullanılarak kişisel veri işleme için GDPR uyumlu bir konsept olduğuna dair yasal bir garanti olmadığı rahatlıkla söylenebilir. Referans verilen veriler bile yasal açıdan takma adlı kişisel veriler olarak algılanabilir ve silinmesi veya düzeltilmesi teknik olarak mümkün değildir. Elbette bu koşullar, bu prosedüre ilişkin değişen yasal bakış açıları ile zaman içinde değişebilir.

3. Blokzincir Teknolojisi

Dağıtılmış Defter Teknolojisinden (Distributed Ledger Technology-DLT) biri olarak tanımlanabilecek Blokzincir teknolojisi, kriptografik ilkeleri kullanarak kayıtlı verilerin kurcalanmasına karşı tam koruma sağlayan, dağıtılmış ve doğrulanabilir bir veri tabanıdır (Bernabe ve diğerleri, 2019). Bu tür bir teknoloji, işlemlerde ve mesajlarda zaman damgasını kullanarak, dağıtılmış veri tabanında bir işlemin varlığı veya yokluğu için evrensel olarak doğrulanabilir kanıtlar sağlamaktadır. Ayrıca, dijital imzaları kullanan temel kriptografik ilkeler aracılığıyla kanıtların doğruluğunu garanti etme özelliğine sahiptir (Faber ve diğerleri, 2019). Doğası gereği blokzincir teknolojisi veri değişikliğine dirençlidir. Veriler ağda bir kez kaydedildikten sonra, herhangi bir bloktan geriye dönük olarak değiştirilemez. Bunun nedeni ise bir blokzincir ağındaki değişikliğin, önceden sıralanan bloklardaki tüm karmaları geçersiz kılmasıdır (Zhang ve diğerleri, 2019).

Blokzincir kavramı ilk olarak 2008 yılında Bitcoin'in kullanıldığı teknoloji olarak tanıtılmıştır (Nakamoto, 2018[9]). Bitcoin, yalnızca güvenli bir dijital para birimi olmasının yanında, üçüncü taraflara ihtiyaç duymadan uzun süredir devam eden "çifte harcama" (double spending) sorununu çözen ilk kripto para birimidir. Blokzincir teknolojisi, Bitcoin uygulamasının temelini oluşturmakta,

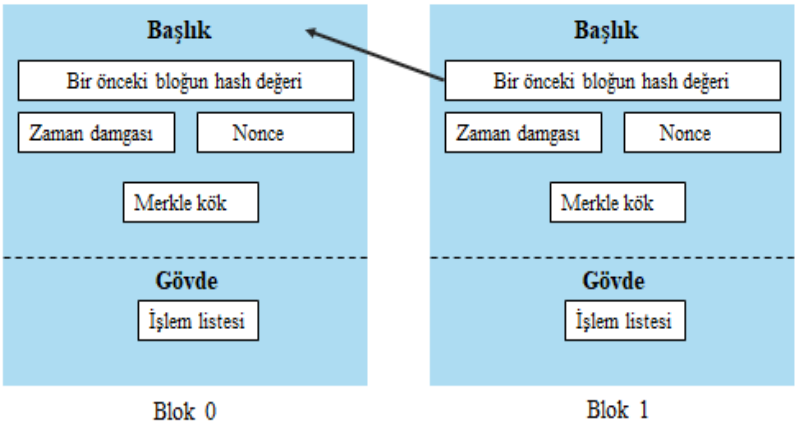
[9] *Satoshi Nakamoto, Bitcoin kripto para biriminin yaratıcıları tarafından kullanılan anonim isimdir. Kim olduğu hâlâ bilinmeyen Nakamoto'nun, 5 Nisan 1975 doğumlu Japonya'da yaşayan bir adam olduğu iddia edilmiştir. Fakat ortaya atılan iddiaların çoğu Nakamoto'nun, Amerika veya Avrupa'da yaşayan, Japon asıllı olmayan, kriptografi uzmanı ve bilgisayar bilimcilerinden biri olduğu yönündedir.*

ancak, bu teknoloji sadece Bitcoin gibi kripto para birimlerinde kullanılmamaktadır.

Blokzincir teknolojisi yapısal olarak bloklardan oluşmakta, önceki blok bir sonraki bloğa bağlı olduğu için karakteristik olarak zincir şeklinde birbirine bağlanmakta olduğundan blokzincir olarak tanımlanmaktadır. İki blok arasındaki bağlantı, bloğun kriptografik karması ile kurulur (Zheng ve diğerleri, 2017). Her bloğun kriptografik karması ile önceki bloğa bağlı olması, bir blokzincirin değişmezliğinin en önemli göstergesidir.

Şekil 1

Blokzincir Ağındaki İki Ardışık Bloğun Gösterimi.



Hâlihazırda zincir üzerinde depolanmış olan işlem adımlarındaki her bir değişiklik, kendisinden sonraki her bloğun iz (hash) değerini ve dolayısıyla tüm blokzincirin iz (hash) değerlerini değiştirmektedir (Zhang ve diğerleri, 2019). Blokzincirin önemli özelliklerinden bir diğeri ise ağdaki katılımcıların birbirlerine tam olarak güvenmelerini gerektirmemesidir. Teknoloji, her bir katılımcının ortak bir fikir birliği üzerinde anlaşmasını sağlar. Şekil 1, bahsedilen sürece genel bir bakış sağlamaktadır. Blokzincir teknolojisi ile bir kullanıcı; ağa bağlanabilir, yeni işlemler başlatılabilir ve yeni bloklar oluşturulabilir. Kullanıcının ağda yapmış olduğu işlem kayıtları ağın tümünde tutulmakta ve bu durum büyük ölçüde veri güvenliğini sağlamaktadır (Blockchain, 2019). Ağın tümünde depolanan bu veriler fikir birliğine varılmadan silinmemekte veya değiştirilmemektedir. Diğer bir deyişle blokzincir, üçüncü bir tarafa ihtiyaç duyulmadan iki taraf arasında verilerin yönetilmesi ve denetlenmesi için tasarlanmış doğrulanabilir ve şeffaf bir teknolojidir. Bir blokzincir ağında, kötü niyetli bir kullanıcıdan gelen herhangi bir zararlı eylemin, katılımcıların çoğunluğu tarafından reddedilmesini sağlamak için bir konsensüs protokolünün uygulanması gerekir (Li ve diğerleri, 2019). Protokol, Blokzincir ağındaki katılımcılar arasında hangi kullanıcının yeni bir blok ekleme iznine sahip olduğuna karar vermek anlamına gelmektedir; diğer katılımcılar izni doğrulayabilir ve yerel defterlerini buna göre güncelleyebilir (Wang, 2019).

Tablo 1

Genel ve Özel Blokzincir Arasındaki Farklar

	Genel	**Özel**
Erişim	Veri tabanına erişim için okuma/yazma izni gerekmez	Veri tabanına erişim için okuma/yazma izni gerekir
Hız	Daha yavaş	Daha hızlı
Güvenlik	Hisse Kanıtı (PoW), İş Kanıtı (PoS)	Ön onaylı katılımcılar
Kimlik	Anonim/Takma Ad	Bilinen kimlikler
Değişmezlik	Tam	Kısmî

3.1. Genel Blokzincir

Kamuya açık bir blokzincir uygulaması olarak tanımlanabilir. Herhangi bir izin gerektirmemesinden dolayı herkes blokzincir ağındaki verileri görüntüleyebilir, okuyabilir, yazabilir ve erişebilir. Tarafların genel blokzincir uygulamasında herhangi bir kontrolü yoktur. Genel blokzincir uygulamaları merkezi değildir. Bir kullanıcı blokzincir ağına katıldığında, katılım doğrulandıktan sonra bilgiler değiştirilemez veya silinemez (Mingxiao ve diğerleri, 2017).

3.2. Özel Blokzincir

Konsorsiyum Blokzincir olarak da bilinir ve sadece davetle kullanılabilir. Tek bir organizasyon tarafından yönetimi sağlanır. Katılımcıların Blokzinciri okumaları, yazmaları veya denetlemeleri için belirli izinler gerekmektedir (Mingxiao ve diğerleri, 2017). Belirli verileri gizli tutmak amacıyla çok sayıda veri erişimi katmanını barındırabilir. Bundan dolayı özel Tablo 1'de görüldüğü gibi blokzincir uygulamalarının güvenlik, gizlilik ve performansı daha yüksektir. Ağdaki işlem ve veriler kamuya açık değildir ve yalnızca üyeler erişilebilir.

3.2.1. İş Kanıtı (Proof of Work-PoW)

Kullanıcının bir blokzincir ağına katılması için çözmesi gereken kriptografik bir bulmacayı ifade eden bir protokol olup; Dwork ve Naor (1993) tarafından önerilmiştir. Birçok blokzincir uygulamasında yaygın olarak kullanılan, kamuya açık ve popüler bir fikir birliği protokolüdür. PoW bulmacasını çözebilen düğüm; blokzincir ağındaki verileri tutma, erişme ve değiştirebilme yetkisine sahip olur. Bir PoW kriptografik bulmacası çözülürken ağdaki düğümlerden doğru dönüş alınabilmesi için "Nonce" (bir kez kullanılan sayı) değerinin doğru ayarlanması gerekmektedir, bu durumda işlemler için hesaplama gücünün artışı sağlanmış olur. Ağda geçerli olan bloklar arttıkça iş yükü de artar, böylece ağdaki uzun bir zinciri bozmak ya da silmek için daha çok hesaplama gücü ve dolaysıyla elektrik enerjisi gerekmektedir (Say, 2015, s. 28). Bu yüzden, PoW'un gecikme ve verimsizliğinin üstesinden gelmek için, Hisse Kanıtı (Proof of Stake-PoS) (Kiayias ve diğerleri, 2017), Bizans Hata Toleransı (Byzantine Fault Tolerance-BFT) (Miller ve LaViola, 2014), Geçen Zamanın Kanıtı (Proof of Elapsed Time-PoET) gibi alternatif fikir birliği modelleri de önerilmiştir.

3.2.2. Hisse Kanıtı (Proof of Stake-PoS)

Bitcoin'in PoW (İş Kanıtı) protokolüne bir alternatif olarak ortaya çıkan bu kanıt, hesaplama gücüne dayanan bir sistem yerine dijital varlık sahipliğini dikkate alan bir protokoldür (Bilgi Platformu, 2020). İlk defa 2012 yılında King ve Nadal (2012) tarafından yayımlanan makalede önerilmiştir. Temel odak noktası, Bitcoin madenciliği için gerekli olan yüksek enerji tüketimi ve diğer sorunları ortadan kaldırmaktır. Ayrıca bu protokolü ilk kullanan kripto para birimi Peercoin'dir (King ve Nadal, 2012). Ağdaki bir düğümün pay miktarı arttıkça, daha fazla blok ekleme ve doğrulama yetkisine sahip olunur. Sistemdeki üyeler ise sahip oldukları bu hisselerle daha fazla söz hakkına sahip olmaktadır.

4. GDPR ve KVKK

Avrupa Birliği (AB) özelinde GDPR ve Türkiye özelinde KVKK, yakın tarihte veri gizliliği düzenlemesinde yapılan en büyük değişiklikler olarak görülmektedir. GDPR, 1995 tarihli Veri Koruma Yönergesi yerine Mayıs 2018'de yürürlüğe girmiştir (Ochôa ve diğerleri, 2019). KVKK ise 7 Nisan 2016 tarih ve 6698 sayı ile kabul edilmiştir (KVKK, 2018). Kanun, Türkiye'de kişisel olarak tanımlanan verilerin korunmasına yönelik ilk ve en önemli gelişme olup, verileri işlenen gerçek kişiler ile bu kişisel verileri kullanan gerçek ve tüzel kişiler arasında kanuna uyumluluğun sağlanmasını amaçlamaktadır. GDPR'nin 4. maddesinde kişisel veri "*tanımlanmış veya tanımlanabilir gerçek kişiyle ilgili her türlü bilgi*" olarak tanımlanmıştır (Wallace, 2018). KVKK ve GDPR incelendiğinde temel amacın, veri gizliliği ile ilgili yasaları uyumlu hale getirmek ve kişilerin verilerini ve mahremiyetini korumak olduğu rahatlıkla görülebilir. Bu bağlamda verilerin korunmasını büyük ölçüde sağlayan hizmet sağlayıcıların, kişi verdiği onaydan vazgeçerse veya kişiye ait veriler kişinin rızası dışında kullanılırsa, ilgili tüm verileri silmesi gerekmektedir. Kullanıcının isteğine bağlı olarak hizmet sağlayıcı, kişisel verilerin işlenip işlenmediğine dair bir rapor vermelidir. Hizmet sağlayıcı, tüm kişisel verileri, veri sahiplerine makine dilinde anlaşılır ve okunabilir olarak sunmalıdır. Erişim

hakkına benzer olarak veri taşınabilirliği (Right to Data Portability) hakkı da vardır; kullanıcı, kişisel verilerinin makine dilinde okunabilir biçimde denetleyiciden bir özetini alabilmeli ve verilerini başka bir denetleyiciye aktarma hakkına sahip olabilmelidir.

4.1. Blokzincir ile GDPR ve KVKK Arasındaki Uyumsuzluklar

4.1.1. Bilgilendirilme Hakkı

GDPR'nin 13. ve 14. maddeleri gereğince, kişisel verilerin çeşitli amaçlar için kullanılması ve toplanması ile ilgili kişilere bilgilendirilme hakkı verilmektedir (Asghar ve diğerleri, 2019). Bu hak, KVKK'nın aynı maddeleri kapsamında da çok önemli bir şeffaflık gereksinimi olarak görülmektedir. Ayrıca bireyler verilerinin işlenme amaçlarını, bu verilerin saklama sürelerini ve kimlerle nasıl paylaşılacağına dair bilgi alma hakkına da sahiptir. Bilgilendirme hakkı, GDPR ve KVKK bağlamında blokzincir teknolojisi ile uyumsuzluk gösteren alanların başında gelmektedir. Blokzincir teknolojisi, âdem-i merkeziyetçiliği sağlamaya çalışır. Bu durumda veri denetleyicisinin kim tarafından seçileceği belirsizleşir. Bu da genellikle özel ve genel blokzincir uygulamalarından etkilenir. Ayrıca, düzenleme kapsamındaki denetleyicinin belirsiz olması, hesap verebilirlik ve sorumluluğu zorlaştırır. Özel blokzincirlerin ağ üzerinde kontrole ve amacı belirleme yeteneğine sahip olduğu varsayılırsa, genellikle denetleyici olarak nitelendirilebilecek bir merkezi operatör olduğundan, denetleyicileri ve işleyicileri tanımlamayı kolaylaştırır. Açık bir denetleyici veya işleyici belirlemeden, bireyin bilgilendirilme hakkını kullanmak için kime başvuracağı genellikle belirsizdir.

4.1.2. Erişim ve Düzeltme Hakkı

GDPR'nin 15. maddesi kapsamındaki verilere erişim hakkı, verinin asıl sahiplerine verilerinin bir kopyasını alma hakkı tanımaktadır (Asghar ve diğerleri, 2019). KVKK'nın da aynı maddesinde vurgulandığı üzere veri sahiplerinin, verilere erişim için sözlü veya yazılı olarak istekte bulunduktan sonra denetleyicinin isteğe cevap vermesi için 30 gün süresi bulunmaktadır. Blokzincir uygulamasındaki veriler ve işlemler, verileri bilgisayar ağlarında tutan taraflara dağıtıldığından, blokzincir ağında verilerin tutulduğu yer çok sayıda olabilir. Bu durum, ağdaki tüm tarafların erişim hakkına uymasını gerektirecektir. Veri sahiplerinin verilere erişim hakkının yanı sıra, verilerin düzeltilmesini isteme hakkı da bulunmaktadır. Verilerin eksik olması durumunda, sahiplere eksik bilgileri tamamlama hakkı sunulur. Sonuç olarak blokzincir teknolojisinin kullanımı, bireylerin verilere erişim ve düzeltme haklarını kullanmalarını zorlaştırmaktadır.

4.1.3. Silme ve İşlemeyi Kısıtlama Hakkı

KVKK'nın 7., GDPR'nin 16. ve 17. maddeleri gereğince; veri sahiplerin isteği üzerine veriler düzenlenebilir veya silinebilir (Brown, 2020). "Unutulma hakkı" (Right to be Forgotten) olarak da tanımlanabilen bu hak mutlak değildir ve yasal gereklilikler, bilimsel araştırma, kamu politikası, halk sağlığının korunması ve talebin belirsiz olması gibi durumlarda uygulanmamaktadır. Bu hak türü, silme hakkının bir alternatifi olarak görülebilir. Böyle bir durum, bazı koşullarda silme hakkının kullanımını engeller. Veri sahipleri, istemeleri durumunda kişisel bilgilerinin kurum ve kuruluşlarca işlenmesini kısıtlama veya engelleme hakkına sahiptir. Blokzincir uygulaması, ağdaki verilerin bütünlüğünü sağlamak ve güveni artırmak için veri değişikliklerini kasıtlı olarak zahmetli hale getirir, böylece veriler kolayca değiştirilemez veya silinemez. Blokzincir uygulamasındaki dağıtık defter biçimi, kişisel veriler eklendikçe aynı olmayan düğümlerde büyüyen, sadece ekleme işlemi yapılan veri tabanlarıdır, silme ve değiştirme işlemleri için de fikir birliğine varılması gerekir. Bundan dolayı, blokzincir teknolojisi GDPR ve KVKK ile uyumlu değildir.

4.1.4. Veri Taşınabilirliği Hakkı

Veri taşınabilirliği hakkı; veri sahiplerine, talepleri üzerine kendi kişisel verilerini bir veri denetleyicisinden yapılandırılmış ve yaygın olarak kullanılan, makine dilinde anlaşılır ve okunabilir olarak alma hakkı verir. GDPR'nin en önemli yeniliklerden biridir (Hert ve diğerleri, 2018).

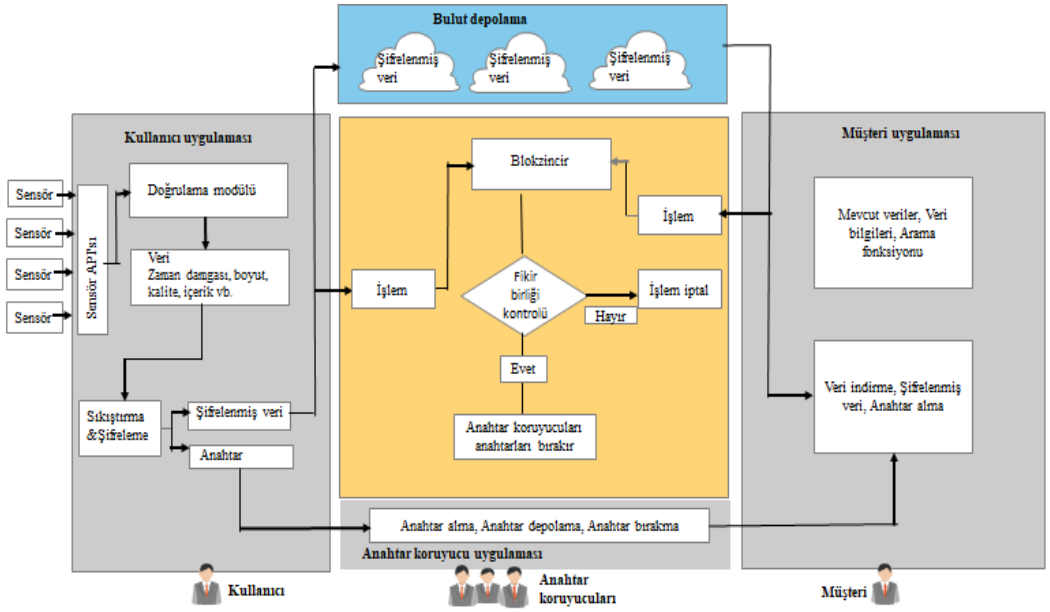
Kullanıcılara kişisel verileri üzerinde daha fazla kontrol sağlayarak, hem verilerini elde etmelerini hem de farklı bir veri denetleyicisine taşımalarını sağlayarak kullanıcıları güçlendirmeyi amaçlamaktadır. Kısacası veri sahiplerine, verileri üzerinde kontrol haklarının garantisini verir (Urquhart ve diğerleri, 2017). Kamuya açık bir blokzincir ağına eklenen verilerin taşınabilir olması gerekliliği, bu bağlamda kabul edilmelidir. Kamuya açık bir blokzincirin üzerine inşa edilen hizmetler ile kullanıcıların kendi dosyalarını indirme yeteneği göz önünde bulundurmalıdır (Eichler ve diğerleri, 2018). Bu hak yalnızca veri sahibi tarafından sağlanan kişisel verilerin işlenmesinin otomatik yollarla gerçekleştirildiği ve işlemeye onay verilen veya işlemenin kişisel veri sahibi ile veri denetleyicisi arasındaki bir sözleşmeye dayalı olarak gerçekleştirildiği durumlar ile başkalarının hak ve özgürlüklerini etkilemediği ölçüde geçerlidir.

5. Önerilen Sistemler

Zheng ve diğerleri (2018) çalışmasında, kullanıcıların kişisel sağlık verilerini kolay ve güvenli bir şekilde paylaşabilmelerini sağlamak ve verileri şeffaf ve verimli bir şekilde elde etmelerine yardımcı olmak için bulut depolama sistemine dayalı GDPR benzeri veri mevzuatına uygun olarak kişisel verilerin paylaşım sistemini önermiştir. Çalışmada kişisel verilerin paylaşım ve depolama sistemi açıklanmıştır.

Şekil 2

Bulut Depolamada Kullanılan Blokzincir Tabanlı Veri Paylaşım Sistemi (Zheng ve diğerleri, 2018)



Şekil 2'de görüldüğü gibi bahsedilen sistemde altı rol tanımlanmıştır.

- ✓ **Kullanıcılar (Users)**: Veri oluşturma, yükleme ve paylaşma hakkına sahiptir.
- ✓ **Anahtar Tutucular (Key Keepers):** Kullanıcı tarafından yüklendikten sonra verilerin şifresinin çözülmesi için özel anahtarları tutmak ve bir işlem onaylandığında anahtarları müşterilere verilmesi.
- ✓ **Müşteri (Customer):** Verilerin satın alınması ve kişilere hizmet ödülleri verilmesi.
- ✓ **Kullanıcı Uygulaması (User App):** Karma ve simetrik şifreleme algoritmasıyla sıkıştırılmış ve şifrelenmiş kişisel verilerin bir bulut sistemine kaydedilerek, verilerin şifre çözme anahtarının veri sahiplerine verilmesi. Ağda oluşturulan işlemler, blokzincir düğümlerinde yayınlanır.
- ✓ **Anahtar Koruyucu Uygulaması (Key Keeper App):** İnternet bağlantısı olan yerel bir

cihazda ya da bulut sunucusunda kaydedilir.

- ✓ **Müşteri Uygulaması (Customer App):** İnternet bağlantısı olan yerel sistemde ya da bulut sunucusunda çalışır. Müşteri mevcut tüm veri kümelerini görebilir. Ağda yapılan işlemler tüm blokzincir düğümlerinde yayınlanır. Özel anahtarla şifrelenmiş verilerin şifresi çözüldükten sonra müşteri, verileri indirebilir (Zheng ve diğerleri, 2018).

  Bu çözüm, veri kontrolü tek bir merkezde yapıldığından, blokzincirin "merkezi olmayan" ilkesine uygun değildir (Ibáñez ve diğerleri, 2018). Pagallo ve diğerleri (2018) çalışmasında, kişiye ait verilerin silinmesinde üç önemli yaklaşım sunmaktadır:

  - Kişisel veriler zincir dışı olarak veri tabanında tutulmalıdır. Blokzincir ağında, verilerin karma değeri tutulur. GDPR'nin silinme özelliğiyle, sadece zincir içi karma değeri ile bağlantılı zincir dışı verilerin silinmesi yeterlidir.
  - Anahtarlar imha edilebilir. Öneriye göre, blokzincir ağında veri şifrelemede kullanılan anahtarlar silinebilmektedir, anahtarın silinmesi durumunda şifreli veriden asıl veri çıkarılamamaktadır. Bunun nedeni şifreli verilerde kullanılan şifreli algoritmaların yetirince güçlü olmasıdır. Verilerin şifresini çözmek imkânsız olduğu için verilere artık erişilemez. Ancak, bu çözümde anahtarların yok edilmesi, kişilerin yeniden tanımlanması olasılığını ortadan kaldırmaz. Ayrıca kuantum bilgisayarlar, kaba kuvvet saldırıları[10] (brute-force attacks) ve teknolojinin evrimi de dikkate alınmalıdır.
  - Bukalemun karması kullanılmalıdır. Burada amaç; bir tuzak kapısı işlevi (Trapdoor fonksiyonunu)[11] içeren karma değerinin kullanımıyla "düzeltilebilir blokzincir" tasarlamaktır. Bukalemun karma değeri[12], blokzincir ağında düzenlenmiş verileri içeren eski başlıkları ortadan kaldırmaz ve ayrıca ağdaki madenciler de değişiklikleri onaylama konusunda takdir yetkisine sahiptir (Ateniese ve diğerleri, 2017). Kullanımlarına, işlevlerine ve hizmetlerine göre daha fazla blokzincir uygulaması göz önünde bulundurulduğunda, gelecekte silme problemine hangi çözümün hâkim olabileceğini söylemek oldukça zordur.

Ateniese ve diğerleri (2017) çalışmasında, her bloğu bir önceki bloğa bağlayan karma fonksiyonunun, standart bukalemun karma evrimi ile değiştirme yaklaşımı sunmuştur. Bir bukalemun karması, bir trapdoor içeren bir kriptografik karma fonksiyonudur ve bu trapdoor bilgisi, çarpışmaların verimli bir şekilde oluşturulmasına izin verir (Politou ve diğerleri, 2019). Trapdoor anahtar bilgisi ile blokların içeriğini değiştirmek mümkündür. Böylece, anahtarı bilerek, herhangi sayıda bloğun silinmesi, değiştirilmesi ve eklenmesi dahil olmak üzere blokzincirin değişimi mümkündür. Önerilen sistem ayrıca, herhangi bir bloğun ne zaman değiştirildiğini belirtmek için değişmez bir "iz" bırakır ve böylece denetlenebilirlik ve şeffaflık büyük ölçüde korunur. Araştırmacıların ana fikri, özel ve istisnai durumlarda blokzincir içeriğini yeniden düzenlemekten sorumlu bazı sabit kullanıcılar arasında gizli trapdoor anahtarının gizlice paylaşılmasını sağlamaktır. Ancak, bu anahtarların nasıl uygun bir şekilde korunacağı ve yönetileceği sorusu açık kalmaktadır. Ayrıca, blokzincir içeriklerini düzenlemek için bankalar gibi bir dizi belirli katılımcı otoriteye güvenmek zorunda olmanın, blokzincirlerin merkezi olmayan yapısını geçersiz kıldığı ve bu teknolojinin faydasını ortadan kaldırdığı iddia edilmektedir. Ek olarak, değişebilir bir blokzincirin finansal sistemleri olası dolandırıcılık faaliyetlerine açtığını, çünkü trapdoor anahtarının ifşa edilmesinin blokzinciri kötü niyetli saldırılara karşı savunmasız hale getirdiğini ve güvenliğini azalttığı da savunulmaktadır (Althauser ve diğerleri, 2017).

Desai ve diğerleri (2020) çalışmasında, blokzincir sisteminde güvenli bir Gezegenler Arası Dosya Sistemi (InterPlanetary File System - IPFS) bulut depolama mimarisi önermektedir. Bu mimaride

---

[10] Kaba kuvvet saldırısı, parolaları, oturum açma kimlik bilgilerini ve şifreleme anahtarlarını kırmak için deneme yanılma yöntemini kullanan bir bilgisayar korsanlığı yöntemidir.

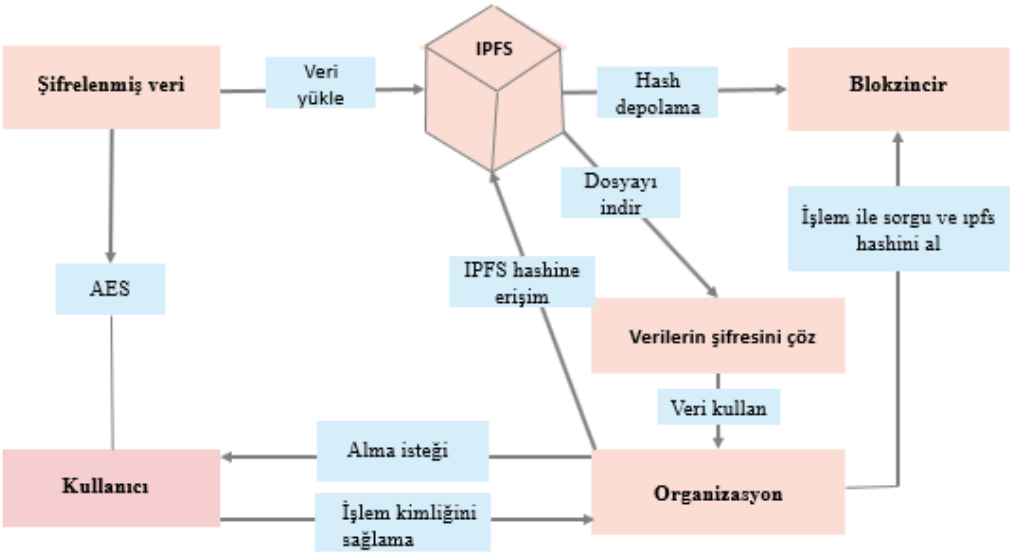
[11] Tuzak kapısı işlevi, hesaplanması kolay olan, ters işlemi hesaplamamıza yardımcı olan gizli bir anahtarı olan tek yönlü bir işlev olarak adlandırılır. İz (hash) fonksiyonu ve trapdoor fonksiyonu birbirinden farklıdır. İz (hash) fonksiyonu tersine çevrilemez. Bunun yerine tek yönlü bir işlev olarak adlandırılır. Kapı işlevi ise, tersine çevrilebilir.

[12] Bukalemun iz (hash) fonksiyonları, trapdoor anahtarı bilgisi ile verimli bir şekilde hash çarpışmaları oluşturabilen özel tip kriptografik hash fonksiyonlarıdır. Standart bir bukalemun karma işlevi, anahtar ve hash oluşturma, hash doğrulama ve hash çarpışma gibi verimli algoritmalardan oluşur.

kişisel veriler bulutta tutulmakta ve dosyayı tanımlayan bilgiler blokzincir ağında saklanarak kişisel veriler korunmaktadır.

Şekil 3

IPFS Bulut Depolama Mimarisi (Desai ve diğerleri, 2020)

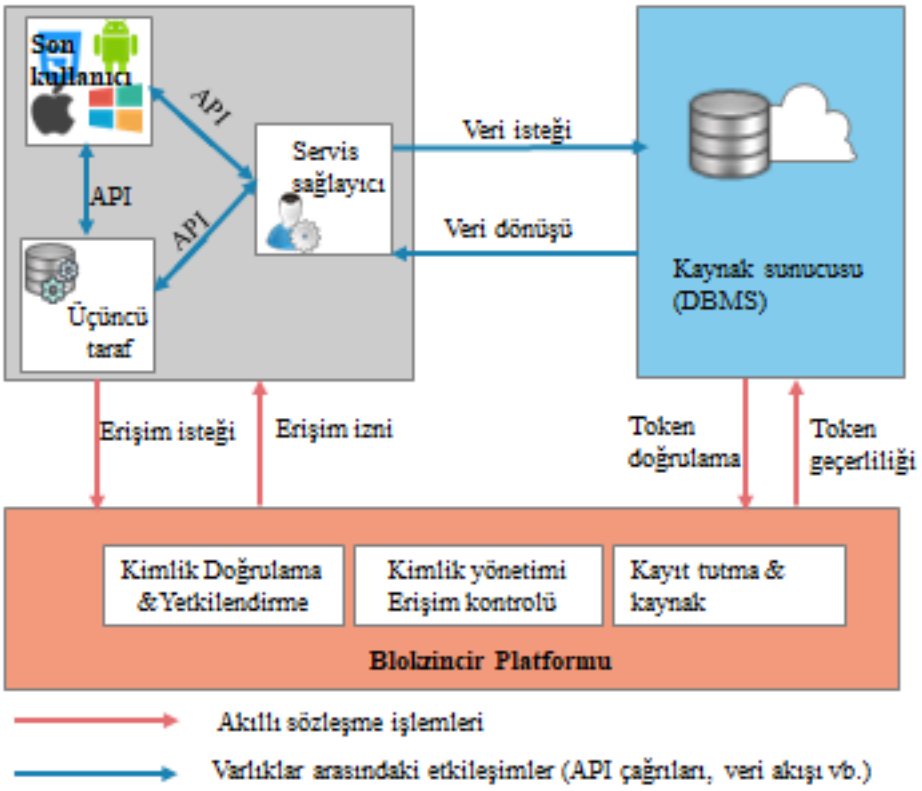


Blokzincir, Şekil 3'te görüldüğü gibi ağa kaydedilen verilere herkes erişebildiği için depolanmadan önce şifrelenmektedir. Kişinin sahip olduğu şifreleme anahtarı, verinin şifresini çözmek için kullanılır. IPFS bulut sisteminde tutulan belgelere erişmek isteyenlerin öncelikle kimlik doğrulama yapması gerekmektedir. Doğrulamadan sonra, kullanıcı sahip olduğu kimlik ile istediği verilere ulaşabilir. Kullanıcı tüm veriler için açık anahtarı yetkili kişilerce doğrulanan kurum ve kuruluşlarla paylaşır. Kurum ve kuruluşlar, kullanıcının istediği belgeyi bulursa, kullanıcıdan blokzincir ağında tutulan belgeye erişmesini isteyecektir. Kullanıcı bu talebi aldığında, belgeye erişmek isteyen kurum ve kuruluşa işlemin karma değerini (işlem kimliği) gönderir. Kurum ve kuruluşlar, işlem kimliği ile belgeleri blokzincir ağında sorgular ve verilerin karma değerini alır. Ayrıca, IPFS mimarisinde tutulan belgenin şifresini çözebilir ve talep edilen belgeyi indirebilir.

Truong ve diğerleri (2019) çalışmasında, kişisel verilerin erişim ve denetimi için, verileri fiziksel olarak tutan ve depolama katmanından ayrıştırılmasına yönelik bütünsel bir mimariyi açıklamıştır.

Şekil 4

Kişisel Veri Yönetimi ve Paylaşım Şeması (Truong ve diğerleri, 2019)



Çalışmada, GDPR uyumluluğu ile ilgili mekanizmaların geleneksel bir merkezi sunucudan bir blokzincir ağına taşınmasıdır. Özellikle yetkilendirme, kimlik doğrulama, kimlik yönetimi (Identity Managemenet-IdM), erişim kontrolü; kayıt ve kaynak bileşenleri, bir blokzincir ağında dağıtılan akılı sözleşmeler (smart contracts)13 biçiminde uygulanır. Bir blokzincir çerçevesi Turing bütünlüğü (Turing Complete)14 sunuyorsa (Ethereum ve Hyperledger Fabric (HLF)15 vb.), GDPR ile ilgili mekanizmalar akılı sözleşmeler tarafından iletilebilir. Çalışmada, özel izinli blokzincir sistemlerinde kullanılan ve verileri korumak için güvenilir kaynak hizmeti ile çalışan sosyal ağ servis sağlayıcısının GDPR gerekliliklerine tamamen uyumlu olduğu belirtilmektedir. Şekil 4'ten de görüleceği üzere, Blokzincir tabanlı ve GDPR uyumlu verilerin yönetim platformu için özel izinli bir blokzincir sistemi kullanılmıştır. Ağdaki kişisel verileri korumak için dağıtılmış defter ve asimetrik şifreleme algoritması kullanılmaktadır. Çalışmada bahsedilen yenilik; zincir dışındaki bir sunucuda tutulan verilere ulaşmak isteyenler için değişmez bir kayıt sistemi modeli oluşturulmasıdır. Böylece sistemde belirli kişilerin izinleri oluşturmasına, düzenlemesine ve silmesine izin verilebilir. Yetkili kişiler ve veri sahipleri arasında kararlaştırılan veri kullanım kurallarına göre veriler işlenebilir. Sistem, kişi hakları için mekanizmalar sağlamanın yanında, verileri işlemek ve hesap verebilirliği sağlamak amacıyla veri denetleyicisi olarak görev yapmaktadır. GDPR uyumluluğu, tehdit modelleri ve sistem performansına ilişkin analiz ve tartışmaların ardından kullanıcılara çeşitli haklar sağlar ve sosyal ağ servis sağlayıcının yükümlülüklerini kolaylaştırır.

[13] *Akıllı sözleşmeler, bir sözleşmenin tamamını veya bir kısmını otomatik olarak yürüten ve blokzincir tabanlı bir platformda depolanan bilgisayar kodunu tanımlamak için kullanılan bir terimdir. Akıllı sözleşmelerin çoğunda, Solidity programlama dili kullanılır. Akıllı sözleşmeler, normal bir sözleşme gibi kurallar tanımlayabilir ve bunları kod aracılığıyla otomatik olarak uygulayabilir. Akıllı sözleşmeler varsayılan olarak silinemez ve onlarla etkileşimler geri alınamaz.*

[14] *Turing bütünlüğü, gerekli talimatlar, yeterli zaman ve bellek verildiğinde, karmaşıklığı ne kadar olursa olsun tüm hesaplama problemini çözebilen bir makineyi ifade eder. Terim normalde modern programlama dillerini tanımlamak için kullanılır (C++, Python, JavaScript, vb.).*

[15] *Hyperledger, blokzincir tabanlı dağıtılmış defterlerin gelişimini desteklemek için Linux Vakfı tarafından geliştirilen açık kaynak kodlu blokzincir teknolojilerin bir projesidir. Blokzincir ve dağıtılmış defterler geliştirerek, teknolojilerin performansını ve güvenilirliğini iyileştirir.*

EPRS (2019) çalışmasında önerilen çözüm ise GDPR'nin 17. maddesinde belirtildiği üzere veri sahiplerinin isteği üzerine verilerin silinebileceğine ilişkin kişiye ait özel anahtarın yok edilmesidir; bu durumda, şifrelenmiş verilere genel anahtarla erişim zorlaşır. Bu çözüm, Fransız Veri Koruma Otoritesi CNIL (Commission Nationale de l'Informatique et des Libertés) [16]tarafından önerilmiş (Commission Nationale Informatique et Libertés, 2018) ve karma fonksiyondaki özel anahtarın, işlenmek üzere tutulduğu başka sistemlerden gelen verilerle silinebileceği ileri sürülmüştür. Bu da, GDPR'nin silme hakkı ile uyumluluğu göstermektedir. Ancak, burada özel anahtarın yok edilmesi uygun bir çözüm olarak görülmemeli; kuantum bilgisayarlar, kaba kuvvet saldırıları ve gelişmiş diğer araçlarla şifrelerin çözülerek verilere erişimi günümüzde büyük ölçüde olasıdır.

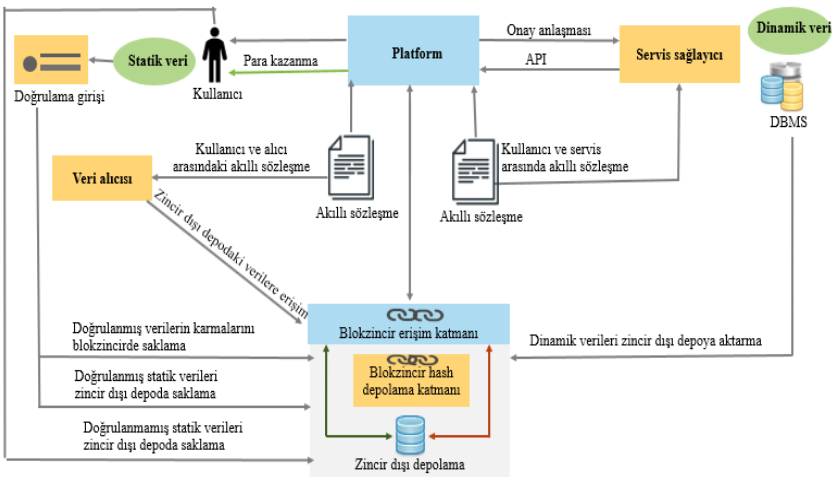
De Meijer (2018) çalışmasında, yine şifreleme anahtarlarının yok edilmesini önermiştir. Bu yöntem, genellikle küresel veri odaklı şirketler tarafından uygulanmakta ve silinme talebinde ağda depolanan verilere erişim olanaksız hale gelir. Böylece, özel (pivate) anahtar yok edildiğinde, ağdaki bilgilere erişim imkansız hale gelecektir.. GDPR uygulayan ülkelerde resmi otoritelerin bu çözümü kabul edip etmeyecekleri henüz tam olarak belli değildir (Zemler, 2019). Ayrıca, şifrelenmiş veya karma değeri alınmış veriler, geri döndürülemez şekilde anonimleştirilmeyip yalnızca takma isimli oldukları için AB yasalarına göre kişisel veri olarak nitelendirilmeye devam etmektedir.

Neisse ve diğerleri (2017) çalışmasında, verilerin kaynak takibini desteklemek amacıyla erişim ve kullanım şeffaflığını ön planda tutan bir sistem önermiştir. Bu sistem, blokzincir ağındaki sözleşmelerin denetlenebilir olması mantığına dayanmaktadır. Buradaki sorun; denetleyicilerin kişisel verilere eriştiğinde ve bu verilerin işleyicilere iletimi sonrasında, GDPR'nin hesap verebilirlik ve kaynak takibi özelliğini desteklememesidir. Denetleyiciler, kişisel verilerine doğrudan veya dolaylı olarak erişen kontrolörleri ve işleyicileri takip edebilmek, rızalarını ihlal etmeden verilere erişilip erişilmediğini, kullanılıp kullanılmadığını ve aktarılıp aktarılmadığını doğrulamak için güvenilir ve şeffaf bir çözüm kullanılarak yetkilendirilmelidir. Böylece, denetleyiciler, kişisel verileri toplamak için onay aldıklarını kanıtlamanın bir yolunu sunar. Sistemdeki denetleyiciler için kişilerin sözleşmeye katılması veya sözleşmeden ayrılması için blokzincir teknolojisini ve kullanıcıların kullanabileceği bir ara yüz önermektedir. Bu model; kullanıcı gizliliği, veri denetleyicisi ve veri izleme gibi özellikler sunmaktadır. Önerilen çözümde, ağda tutulan verilerin, GDPR gerekliliklerinden olan silme ve düzenleme hakkına dair herhangi bir bilgi verilmemektedir.

Faber ve diğerleri (2019) çalışmasında, kişisel verilerde denetim ve şeffaflık fikrini benimsemiştir.

Şekil 5

Blokzincir Tabanlı Kişisel Veri ve Kimlik Yönetim Sistem Mimarisi (Neisse ve diğerleri, 2017)



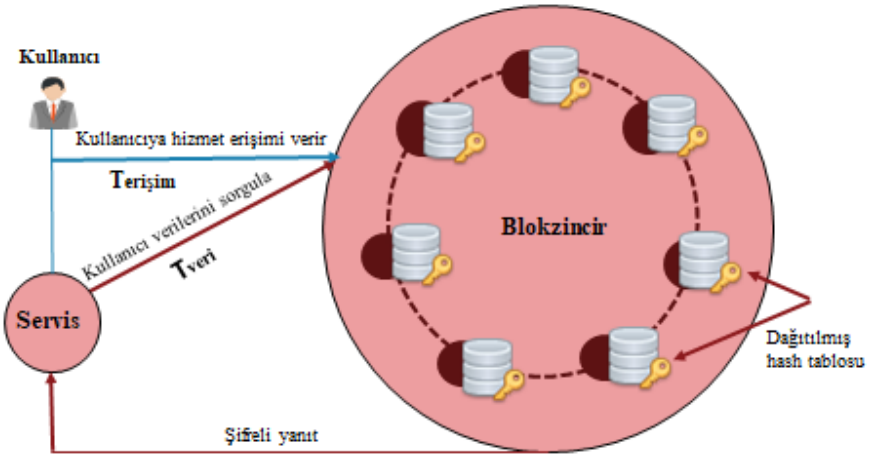
[16] *CNIL, Fransız Veri Koruma Ajansıdır. 1978'de kuruldu ve 6 Ağustos 2004'te değiştirildi. 6 Ocak 1978 tarihli veri koruma mevzuatına uygun olarak faaliyet gösteren bağımsız bir idari organdır. CNIL, bilgi teknolojisinin vatandaşların hizmetinde kalmasını sağlamaktan sorumludur.*

Şekil 5'te görüldüğü üzere modelin bileşenleri; blokzincir katmanındaki akıllı sözleşmeler, erişim ve kimlik yönetimi, ağ dışındaki veri depolama yapısı ve kullanıcı ara yüzünden oluşmaktadır. Depolanan veriler; kullanıcının adı, soyadı, yaşı, cinsiyeti, adresi gibi statik kişisel verileri içermekte ve hizmet sağlayıcısının kontrolünde dinamik verilerle birlikte tutulmaktadır. Buradaki temel odak noktası, veri sahibi olmak değil, kullanıcıya sağlanan hizmet için izinlerin kontrolünü sağlamak ve servis sağlayıcısındaki veri akışını kontrol etmektir. Blokzincir sisteminde tutulan veriler silinemediğinden, GDPR'nin unutulma hakkını uygulayabilmek için, kullanıcıya ait kişisel verileri saklamak adına zincir dışı depo kullanımı ve zincir dışı depodaki verilerin konumuna karma değerin veri işaretçisi eklenmesi önerilmektedir. Bu durumda, unutulma hakkının uygulanabilmesi için veri sahibinin isteği üzerine zincir dışında tutulan veriler silinir ve blokzincir sisteminde kaydedilen verinin değişmez karma değeri geçersiz hale getirilir. Ancak, zincir dışı ağda yer alan kişisel veriler silinse bile, blokzincir ağı üzerinde kişisel verinin zincir dışında saklandığını teyit eden kriptografik özetlenmiş veri "silinmemiş" bir şekilde kalır. Bu durum, GDPR'nin silme (veya unutulma) hakkına uygunluğu açısından tam olarak yeterli görünmemektedir.

Fu ve Fang (2016) ve Zyskind ve diğerleri (2015) çalışmalarında, şifreleme ve takma isimlendirme yöntemine dayanan bir çözüm önermiş ve GDPR'nin unutulma hakkıyla uyumsuzluk sorununu ele almıştır.

Şekil 6

Merkezi Olmayan Platforma Genel Bakış (Fu ve Fang, 2016)



Şekil 6'ya göre sistemi oluşturan üç bileşen; sistem kullanıcıları, düğümler ve servis sağlayıcılardır. Sistem kullanıcıları anonimdir. Tasarımda, erişim kontrolü için $T_{erişim}$[17] ve veri operasyonları için T_{veri}[18] kullanılmaktadır. Bu işlemler mobil uygulamalardaki geliştirmelere kolaylıkla uygulanabilir. Veri sahibi, verilerin gizliliği ve güvenliği için uygulamayı indirdikten sonra sisteme kaydolduğunda, bir hizmet kimliği oluşturulur ve veriler $T_{erişim}$ izni ile blokzincir sistemine gönderilir. Sistemdeki kullanıcı verileri (isim, güvenlik numaraları, IP adresi, yaş, ehliyet, kimlik, adresi, pasaport vb.) şifrelenir ve T_{veri} ismiyle blokzincir ağına aktarılır. Kullanıcı T_{veri} ile sahip olduğu anahtarla sorgulama yaparak dijital imzayı doğrulayabilir. Ayrıca kullanıcı, isterse sistemde tutulan verilerin erişimini iptal edilebilir. Verilerin dağıtılmış karma değer tablosu, blokzincir ağında yazma/okuma işlemlerine izin verilen bir düğümle korunmaktadır. Ağda tutulan verilerin düğümlerdeki dağılımı düzensizdir. Tüm düğümlerde kopyası bulunan verilerin kontrolü kullanıcıdadır. Blokzincir sisteminde sadece karma değeri alınmış veriler tutulduğundan, kötü niyetli bir kullanıcı için genel defterdeki veriler anlaşılır değildir. Bu durumda, kötü niyetli bir kullanıcı anahtarı alsa bile sistemde tutulan veriler hala güvendedir.

[17] *$T_{erişim}$, veriler üzerindeki kontrol ve yönetim işlemleri için kullanılır. $T_{erişim}$ işleminde bir politika seti göndererek izin ve erişim kontrollerini değiştirebilir.*

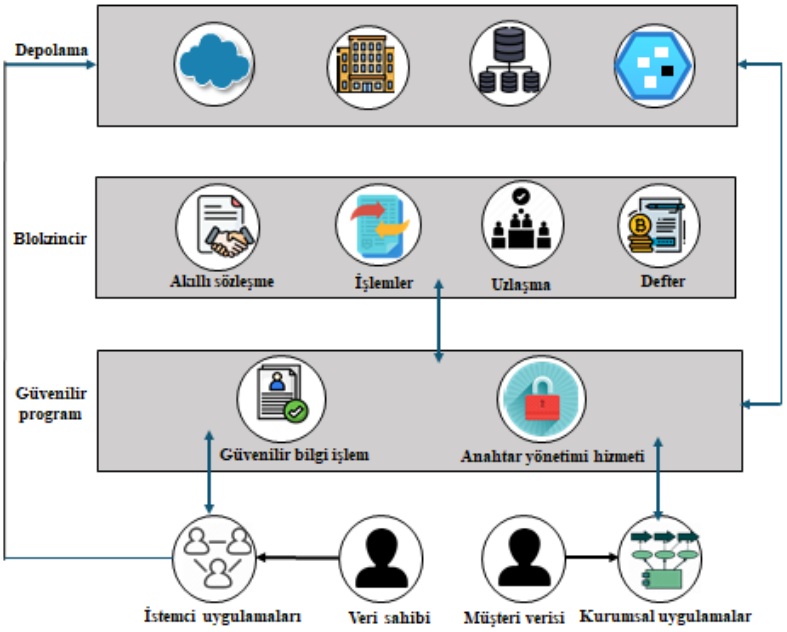
[18] *T_{veri}, veri depolama ve alma için kullanılır. Bir kullanıcı veya hizmet sağlayıcı, daha önce belirtilen politikalar karşılanırsa blokzincir düğümleri tarafından onaylanacak bir T_{veri} işlemi göndererek verilere erişebilir. Döndürülen yanıt şifrelenir; dolayısıyla yetkisiz kullanıcılar verilere erişemez.*

Shrestha ve diğerleri (2020) çalışmasında, kişisel verilerin tutulması ve denetimi için merkezi bir yapı kullanımını, verilerin başka amaçla kullanılmasını, sistemin kötü niyetli kullanıcılar tarafından saldırıya uğramasını veya kullanıcının bilgisi olmadan verilerin herhangi bir kurum veya özel kuruluşa satılması gibi riskleri vurgulamıştır. Bundan dolayı; Ethereum[19] ile birlikte blokzincir ve zincir dışı veri şifreleme, hash (iz) alma, depolama ve veri takibine çözüm olarak MultiChain[20] özel izinli blokzincir mimarisi önerilmektedir.

Şekil 7

Kullanıcı Kontrolü ve Gizliliği Koruyan Veri Paylaşım Sistemi

(Shrestha ve diğerleri, 2020)



Şekil 7'ye göre, kullanıcı verilerinin blokzincir ağının dışında depolanmadan önce karma değeri alınmakta ve şifrelenmektedir. Verilerin çoğu özel MultiChain'de depolanıp paylaşılır. Bu durumda, kullanıcı verileri blokzincir sisteminde tutulmaz. Akıllı sözleşmelerde, verilerin karma değeri ve üst verileri kodlanır ve blokzincir ağında yayılır. Kurum ve özel kuruluşlar, kişisel verilere erişmek için akıllı sözleşmeleri kullanır. Blokzincir teknolojisi ve akıllı sözleşmeler, kullanıcılara kimin, ne zaman ve ne gibi amaçlarla verilerine ulaştığı ile ilgili şeffaflık sağlayarak, kişilerin veri paylaşımı amacıyla, paylaşılabilecek veri türü ve uygulama gruplarını belirleyerek sistemdeki kullanıcıları destekler. Ağ dışında tutulan verilere MultiChain ile erişim sağlanır ve buradaki düğümlerde; kullanıcı verilerinin iz (hash) değerinin alınması ve şifrelenmesi, şifrelenmiş dosyanın zincir dışında saklanması, dosyanın iz (hash) değerinin blokzincir ağında uygulanması, verilerin aranması, doğrulanması ve teslim edilmesi gibi önemli operasyonlar da gerçekleştirilir.

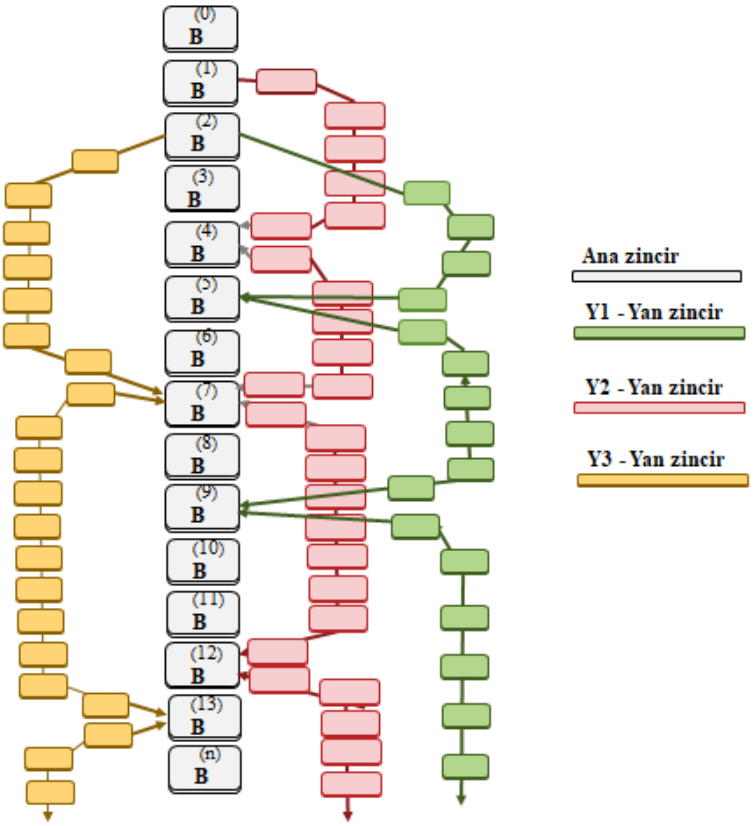
Lee ve diğerleri (2019) çalışmasında, yan zincir modelinin kullanılarak işlemlerin onaylanabileceği ve değiştirilebileceği bir blokzincir oluşturma yöntemi önermektedir. Blokzincir sistemindeki ana zincir, işlemleri tutmak ve yan zincirlerin başlatılma ve sonlandırılma süreçlerini takip eder.

[19] *Ethereum, Ether (ETH) veya Ethereum adlı kendi kripto para birimine ve Solidity programlama diline sahip bir blokzincir teknolojisidir. Ethereum, akıllı sözleşmeleri ve kripto para ticaretini üçüncü bir taraf olmadan güvenli bir şekilde kolaylaştırmak için blokzincir teknolojisini kullanan açık kaynaklı bir kamu hizmetidir. Bir Blokzincir platformu olarak Ethereum, işlemleri kaydetmek ve doğrulamak için merkezi olmayan bir defter sunar.*

[20] *MultiChain, Bitcoin'in genişletilmiş açık kaynak kodlu çatalıdır. Özel ve genel blokzincir teknolojilerini başlatmak için kullanılabilir. MultiChain kolayca yapılandırılabilir ve aynı anda farklı blokzincirlerle çalışabilir. API ve komut satırı arayüzüne sahiptir. MultiChain, kullanıcı izinlerinin entegre yönetimi yoluyla madencilik, gizlilik ve açıklık sorununu çözer.*

Şekil 8

Ana Zincir ve Yan Zincir Mimarisi (Lee ve *diğerleri, 2019)*



Şekil 8'e göre, her yan zincir işlemleri ana zincir ve diğer yan zincirlerinkinden neredeyse bağımsızdır. Ağdaki blokların uzunluk ve özelliklerine göre verimlilik değişkenlik göstermektedir. İzinli model tabanlı yöntemlere kıyasla, herhangi bir merkezi veya yarı merkezi otoriteye ve güvene dayalı olmayan bir ortamda işlem değiştirme konusunda daha kolay genel bir fikir birliğine varılabilmektedir. Model, işlem düzeyinde değişiklik sağlar ve veri sahiplerine işlemlerin zorluk seviyesini seçmelerine olanak tanır. İşlem değişikliğinin kötü amaçlarla yapılmasını önlemek için çeşitli şifreleme teknikleri kullanır (Advanced Encryption Standard-AES[21] ve Rivest–Shamir–Adleman-RSA[22]). Mimari, Bitcoin gibi geleneksel genel blokzincir uygulamalarına benzemekte, dolayısıyla mevcut genel blokzincir modeline kolayca uyarlanabilmektedir. Ayrıca, 'düzeltme hakkı', 'rızayı geri çekme hakkı' ve 'unutulma hakkı' vb. gibi veri koruma düzenlemelerinin temel taleplerine de uygundur.

6. Sonuç

AB özelinde GDPR ve Türkiye özelinde KVKK, kişilerin başta sosyal medya olmak üzere kamu hizmetlerinde (belediye, bankacılık, sağlık vb.) ve diğer çeşitli işlemler boyunca dijital ortamda bıraktıkları her türlü veri ve bilginin; kişilik haklarını (gizlilik) katı kurallarla koruyacak bir çerçeve olarak görülmelidir. Bahsedilen mevzuat, özellikle hizmet sağlayıcılara potansiyel veri ihlalleri olması durumunda yüksek bir sorumluluk ve yaptırım getirmektedir. Hizmet sağlayıcılar ise, çeşitli bilgilendirme formları oluşturarak, bu sorumluluklarını ya sürecin başında ya da sonunda kullanıcılara sunmakta ve kullanıcıların da bu metni kabul etmelerini istemektedir.

Yapısal düzenlemelere rağmen kullanıcı gizliliğiyle ilgili kamuoyunda artan bir endişe

[21] *AES, güvenli ve sınıflandırılmış veri şifreleme ve şifre çözme için bir simetrik anahtar blok şifreleme algoritması standardıdır.*

[22] *RSA, yaygın olarak kullanılan asimetrik bir şifreleme algoritmasıdır. Asimetrik şifreleme, verileri şifrelemek ve şifresini çözmek için matematiksel olarak bağlantılı bir anahtar çifti (özel ve genel anahtar) kullanır. RSA algoritması, çok büyük sayıları çarpanlarına ayırmanın zorluğuna dayanmaktadır.*

gözlenmektedir. Organizasyonların elinde olan kişisel ve dolayısıyla hassas veriler, doğal olarak verinin asıl sahipleri olan son kullanıcıların büyük çoğunlukla kontrolünde değildir. Başka bir deyişle, artan endişelerin temel kaynağı kişisel verilerin asıl sahipliğinin organizasyonlara geçmiş olmasıdır. Bu durum ise çeşitli çevrelerce mevcut iş modellerinin sorgulanmasına neden olmaktadır. Veri ihlali sonucu kişisel verilerin ele geçirilmesiyle edinilen bazı bilgiler (örneğin cep telefonu numaraları) kullanılarak, kullanıcılara SMS, Whatsapp mesajı ve telefon araması gibi yollarla ulaşılmakta ve çoğunlukla ticari içerikler iletilmektedir. Son zamanlarda bazı büyük işletmelerde yaşanan veri ihlalleri sonucunda milyonlarca kişinin ad, soyad, e-posta, cep telefonu numarası ve adres gibi çeşitli bilgilerin ele geçirildiği bilinmektedir. Yetkili otoriteler tarafından yapılan teknik ve idari incelemeler neticesinde süreçte hatası olan işletmelere yüksek boyutlu cezalar kesilmektedir.

Veri ihlallerinin mümkün olan şekilde en aza çekilmesinde, blokzincir teknolojisi yeni bir alan olarak görünse de, literatürde konu ile ilgili çok sayıda araştırma bulunmaktadır. Teknik ve idari gerekliliklerin yanında hukuki düzenlemelerin odak noktasını oluşturan "teknoloji ile uyumluluk", blokzincir uygulamalarında birtakım tartışmalara yol açmış görünmektedir. Kişisel verilerinin hassasiyeti göz önüne alındığında, çalışmalarda çoğunlukla GDPR ile uyumlu işleyebilecek çeşitli mimariler önerildiği ve verilerin silinmesinin genellikle mümkün olmadığı bilindiğinden, veri ile alakalı hash (iz) değerlerinin silinerek kısmi önlem alınmaya çalışıldığı görülmektedir. Çözüm olarak sunulan mimariler, verilerin GDPR kapsamında "düzenleme", "silme", ve "unutulma" gibi temel yasal yükümlülükleri göz ardı etmeyecek şekilde kurgulanmıştır.

Diğer bir konu ise blokzincirin kişisel verileri depolamada ne kadar uygun olduğudur. Blokzincir, genellikle küçük boyutlu ve doğrusal işlem verilerini kaydetmek için tasarlanmıştır. Başka bir deyişle, kullanıcı yalnızca mevcut işlemin orijinal "anlaşmaya" kadar geriye doğru izlenip izlenemeyeceğiyle ilgilenmektedir. Blokzincirin kişisel verileri depolamada optimum bir seçenek (veya kaçış noktası) olduğu halen belirsizliğini korumaktadır. Denilebilir ki kişisel verilerin yönetiminde "düzenleme", "silme", "unutulma" gibi birincil hakların, blokzincir teknolojisinin karakteristik yapısına uygun olmadığı, akademik ve uygulamalı araştırmalarda kendini göstermiş; uyumsuzlukların giderilmesinin, ilgili teknolojinin kendisinde saklı olduğu, ancak, mevzuata uyumluluk adına blokzincir teknolojisinde yapılması olası güncellemelerin, teknolojinin kendisi ile çelişeceği ve blokzincirin karakteristik özelliğini yok edeceği düşünülmekte ve bu yüzden ana yapıyı etkilemeyecek (örneğin; özel anahtarın yok edilmesi, zincir dışı depolama, iz değeri silinmesi vb.) küçük çaplı değişikliklerin yapılması önerilmektedir. Bu durumda, gelecekte ortaya çıkabilecek en önemli sorunlardan birisi de hukuki-teknolojik uyumluluğun sağlanması noktasında bir gereklilik olup olmayacağıdır.

Blokzincir uygulamaları yerine gelecekte ortaya çıkması muhtemel yeni yöntemlerin tartışılacağı ve bu bağlamda yeniliklerin uygulamalı olarak değerlendirilebileceği öngörülebilir. Blokzincir teknolojisi ile kişisel verilerin korunması konusunun literatür bağlamında ilişkilendirilmeye çalışıldığı bu makalenin gelecekteki çalışmalara; hukuki ve teknoloji alanlarındaki değerlendirmeye ve mevzuat uyumunun gerekip gerekmeyeceği yönünden katkı sağlayacağı düşünülmektedir.

Etik Standartlar ile Uyumluluk

Çıkar Çatışması: Yazar herhangi bir çıkar çatışmasının olmadığını beyan eder.

Etik Kurul İzni: Bu çalışma için etik kurul iznine gerek yoktur.

Yazar Katkı Beyanı: Yazarlar makale için eşit oranda katkıda bulunduklarını beyan ederler.

Finansal Destek: Yoktur.

Kaynakça

Althauser, J. (2017). Accenture Secures Patent for its' Editable Blockchain Technology. https://cointelegraph.com/news/accenture-secures-patent-for-its-editable-blockchain-technology.

Asghar, M.N., Kanwal, N., Lee, B., Fleury, M., Herbst, M. ve Qiao, Y. (2019). Visual Surveillance within the EU General Data Protection Regulation: A Technology Perspective. https://doi.org/10.1109/ACCESS.2019.2934226.

Ateniese, G., Magri, B., Venturi, D. ve Andrade, E. (2017). Redactable Blockchain–or–rewriting History in Bitcoin and Friends. https://doi.org/10.1109/EuroSP.2017.37.

Bernabe, J.B., Canovas, J.L., Herhandez-Ramos, J.L., Moreno, R.T. ve Skarmeta, A. (2019). Privacy-Preserving Solutions for Blockchain: Review and Challenges. https://doi.org/10.1109/ACCESS.2019.2950872.

Bilgi Platformu (2020). Proof of Stake (Hisse Kanıtı) Nedir? Nasıl Çalışır? https://www.btcturk.com/bilgi-platformu/proof-of-stake-hisse-kaniti-nedir-nasil-calisir/.

Brown, M. (Ağustos 2020). Blockchain and the GDPR: Can the Conflicts be Resolved? https://compliancecosmos.org/blockchain-and-gdpr-can-conflicts-be-resolved.

CNIL. (2018). Premiers Éléments d'Analyse de la CNIL: Blockchain. https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf.

Danyal, D. (2021, Ocak 24). Blockchain ve Dağıtılmış Defter Teknolojilerinin Temel Avantajları, https://devrimdanyal.medium.com/blockchain-ve-da%C4%9F%C4%B1t%C4%B1lm%C4%B1%C5%9F-defter-teknolojilerinin-temel-avantajlar%C4%B1-6490828bb18a.

Data Protection Working Party (2014). Opinion 05/2014 on anonymisation techniques. 0829/14/EN WP216. Edited by Article 29 Data Protection Working Party. https://ec.europa.eu/justice/article9/documentation/opinionrecommendation/files/2014/wp216_en.pdf.

De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L. ve Sanchez Martin, J.I. (2018). The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services, *Computer Law & Security Review*, 34(2), 93-203. https://doi.org/10.1016/j.clsr.2017.10.003 .

De Meijer, C.R.W. (2018, Ocotober 9). Blockchain versus GDPR and Who Should Adjust Most, 01.09.2021 tarihinde https://www.finextra.com/blogposting/16102/blockchain-versus-gdpr-and-who-should-adjust-most adresinden erişildi.

Desai, S., Shelke, R., Deshmukh, O., Choudhary, H. ve Sambare, S.S. (2020). Blockchain Based Secure Data Storage and Access Control System Using IPFS, *Journal of Critical Reviews*, 7(19), 1254-1260. https://doi.org/10.1109/ICCUBEA47591.2019.9129015.

Dwork, C. ve Naor, M. (1993). Pricing via Processing or Combatting Junk Mail. Brickell E.F. (eds), *Advances in Cryptology-CRYPTO '92 Lecture Notes in Computer Science* içinde (ss. 139-147), 740, Springer: Berlin. https://doi.org/10.1007/3-540-48071-4_10.

Eberhardt J. ve Tai S. (2017). On or off the Blockchain? Insights on off-chaining computation and data. https://link.springer.com/chapter/10.1007/978-3-319-67262-5_1.

Eichler, N., Jongerius, S., McMullen, G., Naegele, O., Liz, S. ve Wagner, K. (2018). Blockchain, data protection, and the GDPR. https://www.crowdfundinsider.com/wpcontent/uploads/2018/06/GDPR_Position_Paper_v1.0.pdf.

EPRS. (2019). Blockchain and the General Data Protection Regulation. https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf.

Esposito, C., Santis, A.D., Tortora, G., Chang, H. ve Choo, K-K. R. (2018). Blockchain: A Panacea for healthcare cloud-based data security and privacy? In IEEE Cloud Comput. 5 (1), pp. 31–37. https://fardapaper.ir/mohavaha/uploads/2019/03/Fardapaper-Blockchain-A-Panacea-for-Healthcare-Cloud-Based-Data-Security-and-Privacy.pdf.

Faber, B., Michelet, G., Weidmann, N., Mukkamala, R. ve Vatrapu, R. (2019). BPDIMS: A Blockchain-based Personal Data and Identity Management System. https://scholarspace.manoa.hawaii.edu/bitstream/10125/60121/0681.pdf.

Finck, M. (2018). Blockchains and data protection in the European Union. In European Data

Protection Law Review 4 (1), pp. 17–35. https://edpl.lexxion.eu/article/edpl/2018/1/6.

Fu, D. ve Fang, L. (2016). Blockchain-Based Trusted Computing in Social Network. https://doi.org/10.1109/CompComm.2016.7924656.

Gräther, W., Kolvenbach, S., Ruland, R., Schütte, J. Torres, C., Wendland, F. (2018). Blockchain for education: Lifelong learning passport. In W. Prinz & P. Hoschka (Ed.): Proceedings of the 1st ERCIM Blockchain Workshop 2018, Reports of the European Society for Socially Embedded Technologies. https://www.dotmagazine.online/issues/blockchain-e-government/blockchain-e-government-citizen-control-of-data/blockchain-for-education.

Grimes, R.A. (2021). What is personally identifiable information (PII)? How to protect it under GDPR. https://www.csoonline.com/article/3215864/how-to-protect-pii-under-gdpr.html .

Ibáñez, L.D., O'Hara, K. ve Simperl, E. (2018). On Blockchains and the General Data Protection Regulation. https://eprints.soton.ac.uk/422879/1/BLockchains_GDPR_4.pdf.

Jensen, G. (2018). Reconciling GDPR rights to erasure and rectification of personal data with Blockchain. https://blogs.oracle.com/cloudsecurity/reconcilinggdpr-rights-to-erasure-and-rectification-of-personaldata-with-blockchain.

Katuwal, G.J., Pandey, S., Hennessey, M. ve Lamichhane, B. (2018). Applications of Blockchain in healthcare: Current landscape & challenges. http://arxiv.org/pdf/1812.02776v1.

Kiayias, A., Russell, A., David, B., Oliynykov, R. (2017). Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol. Katz J., Shacham H. (eds), Advances in Cryptology - CRYPTO 2017 Lecture Notes in Computer Science, içinde (ss. 357-388), 10401. Springer. https://doi.org/10.1007/978-3-319-63688-7_12.

KVKK ve Blokzinciri Teknolojisi Raporu (Kasım 2019). https://bctr.org/dokumanlar/KVKK_ve_Blokzincir_Teknolojisi.pdf.

KVKK (2018, Temmuz 02). Data Protection in Turkey. https://www.kvkk.gov.tr/Icerik/5389/Data-Protection-in-Turkey.

Lee, D., ve Park, N. (2020). Blockchain Based Privacy Preserving Multimedia Intelligent Video Surveillance Using Secure Merkle Tree, *Multimedia Tools and Applications*, 1-18. https://doi.org/10.1007/s11042-020-08776-y.

Li, R., Song, T., Mei, B., Li, H., Cheng, X. ve Sun, L. (2019). Blockchain for Large-Scale Internet of Things Data Storage and Protection, *IEEE Transactions on Services Computing*, 12(5), 762-771. https://doi.org/10.1109/TSC.2018.2853167.

Mamoshina, P., Ojomoko, L., Yanovich, Y., Ostrovski, A.,Botezatu, A., Prikhodko, P., Izumchenko, E., Aliper, A., Romantsov, K., Zhebrak, A., Ogu, I. O. ve Zhavoronkov, A. (2018). Converging Blockchain and Next-Generation Artificial Intelligence Technologies to Decentralize and Accelerate Biomedical Research and Healthcare. *Oncotarget*, 9(5). https://doi.org/10.18632/oncotarget.22345.

Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W. ve Qijun, C.A (2017). Review on Consensus Algorithm of Blockchain. https://doi.org/10.1109/SMC.2017.8123011.

Miller, A.K. ve LaViola, J. (2014). Anonymous Byzantine Consensus from Moderately-Hard Puzzles: A Model for Bitcoin. http://diyhpl.us/~bryan/papers2/bitcoin/Anonymous%20byzantine%20consensus%20from%20moderately-hard%20puzzles:%20a%20model%20for%20Bitcoin.pdf.

Nakamoto, S. (2018). Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf.

Nayak, A. ve Dutta, K. (2017). Blockchain: The Perfect Data Protection Tool. https://doi.org/10.1109/I2C2.2017.8321932.

Neisse, R., Steri, G. ve Fovino, I.N. (2017). A Blockchain-Based Approach for Data Accountability and Provenance Tracking, *ARES '17: Proceedings of the 12th International Conference on*

Availability, Reliability and Security içinde (ss. 1-10), Association for Computing Machinery: New York. https://doi.org/10.1145/3098954.3098958.

Ochôa, I., Calbusch, L., Viecelli, K., Paz, J.D., Leithardt, V. ve Zeferino, C. (2019). Privacy in the Internet of Things: A Study to Protect User's Data in LPR Systems Using Blockchain. https://doi.org/10.1109/PST47121.2019.8949076.

Omaar, J. (2017). Forever isn't free: The cost of storage on a Blockchain database. https://medium.com/ipdb-blog/forever-isnt-freethe-cost-of-storage-on-a-blockchain-database59003f63e01.

Pagallo, U., Bassi, E., Crepaldi, M. ve Durante, M. (2018). Chronicle of a Clash Foretold: Blockchains and the GDPR's Right to Erasure, M. Palmirani (Ed.), *Legal Knowledge and Information Systems* içinde (ss. 81-90), IOS Press, Amsterdam. https://doi.org/10.3233/978-1-61499-935-5-81.

Politou, E., Casino, F., Alepis, E. ve Patsakis, C. (2019). Blockchain Mutability: Challenges and Proposed Solutions. http://dx.doi.org/10.1109/TETC.2019.2949510.

Say, C. (2015). *5 Soruda Blokzinciri*, Bankalararası Kart Merkezi: İstanbul.

Shah, P., Forester, D., Berberich, M. ve Raspé, C. (2019). Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies. *Thomson Reuters The Practical Law*, 1-8. https://www.davispolk.com/sites/default/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf.

Shrestha, A.K., Vassileva, J. ve Deters, R. (2020). A Blockchain Platform for User Data Sharing Ensuring User Control and Incentives, *Frontiers in Blockchain*, 3, 1-22. https://doi.org/10.3389/fbloc.2020.497985.

Steichen, M., Fiz, B., Norvill, R., Shbair, W. ve State, R. (2018). Blockchain-based, decentralized access control for IPFS. https://www.researchgate.net/publication/327034734_BlockchainBased_Decentralized_Access_Control_for_IPFS.

Truong, N.B. ve Lee, G.M. (2019). GDPR-Compliant Personal Data Management: A Blockchain-Based Solution, *IEEE Transactions on Information Forensics and Security*, 15, 1746-1761. http://dx.doi.org/10.1109/TIFS.2019.2948287.

Urquhart, L., Sailaja, N. ve McAuley, D. (2017). Realising the Right to Data Portability for the Domestic Internet of Things, *Personal and Ubiquitous Computing*, 22, 317-332. https://link.springer.com/article/10.1007/s00779-017-1069-2.

Van Humbeeck, A. (2017). The Blockchain-GDPR paradox. https://medium.com/wearetheledger/the-blockchaingdpr-paradox-fc51e663d047.

Wallace, A. (2018). Protection of Personal Data in Blockchain Technology: An investigation on the Compatibility of the General Data Protection Regulation and the Public Blockchain (Yüksek Lisans Tezi). Stockholm Üniversitesi. http://su.diva-portal.org/smash/get/diva2:1298747/FULLTEXT01.pdf.

Wang, W., Hoang, D. T., Hu, P., Xiong, Z., Niyato, D., Wang, P., Wen, Y. ve Dong, D. I. (2019). A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks. *IEEE Access*,7, 22328-22370. https://arxiv.org/pdf/1805.02707.pdf.

Wirth, C. ve Kolain, M. (2018) GDPR-compliant Approach for Handling Personal Data. http://dx.doi.org/10.18420/blockchain2018_03.

Zemler, F. (2019). Concepts for GDPR-Compliant Processing of Personal Data on Blockchain: A Literature Review, *Anwendungen und Konzepte der Wirtschaftsinformatik*, 9, 96-107. https://www.researchgate.net/publication/338117615_Concepts_for_GDPR-Compliant_Processing_of_Personal_Data_on_Blockchain_A_Literature_Review.

Zhang, R., Xue, R. ve Liu, L. (2019). Security and Privacy on Blockchain. *ACM Computing Surveys*, 52(3), 51-85. https://doi.org/10.1145/3316481.

Zhang, S., Kim, A., Liu, D., Nuckchady, S. C., Huang, L., Masurkar, A., Zhang, J., Karnati, L., Martinez, L., Hardjono, T., Kellis, M. ve Zhang, Z. (2018). Genie: A secure, transparent sharing and services platform for genetic and health data. http://arxiv.org/pdf/1811.01431v1.

Zheng, Z., Xie, S., Dai H., Chen, X., ve Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus and Future Trends. https://doi.org/10.1109/BigDataCongress.2017.85.

Zheng, X., Mukkamala, R., Vatrapu, R. ve Ordieres-Mere, J. (2018). Blockchain-Based Personal Health Data Sharing System Using Cloud Storage. https://doi.org/10.1109/HealthCom.2018.8531125.

Zyskind, G., Nathan, O. ve Pentland, A.S. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. https://doi.org/10.1109/SPW.2015.27.