MARMARA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BLOKZİNCİR UYGULAMASINDA KİŞİSEL VERİLERİN TUTULMASI

NURCAN DİRİ

YÜKSEK LİSANS TEZİ
Bilgisayar Mühendisliği Anabilim Dalı
Bilgisayar Mühendisliği Yüksek Lisans Programı

DANIŞMAN
Doç.Dr. BAHATTİN YALÇINKAYA

İSTANBUL, 2022

MARMARA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BLOKZİNCİR UYGULAMASINDA KİŞİSEL VERİLERİN TUTULMASI

NURCAN DİRİ
527319029

YÜKSEK LİSANS TEZİ
Bilgisayar Mühendisliği Anabilim Dalı
Bilgisayar Mühendisliği Yüksek Lisans Programı

DANIŞMAN
Doç.Dr. BAHATTİN YALÇINKAYA

İSTANBUL, 2022

ÖNSÖZ

Tez çalışmam süresince desteklerini, rehberliklerini, zamanlarını, yardımlarını ve sabırlarını esirgemeyen değerli hocam Doç. Dr. Bahattin YALÇINKAYA'ya,

Bana olan inançları ve koşulsuz sevgileri ile hayatımın her anında yanımda olan çok aileme ve kardeşlerime,

Yardımları ve destekleriyle yanımda olan değerli çalışma arkadaşlarıma,

Tez çalışmam süresince beni her anlamda destekleyen hocalarıma ve jüri üyesi olarak teze katılım sağlayan hocalarıma

Teşekkürü bir borç bilirim.

Aralık, 2021 Nurcan DİRİ

İÇİNDEKİLER/

ÖZET

BLOKZİNCİR UYGULAMASINDA KİŞİSEL VERİLERİN TUTULMASI

Teknolojisinin gelişmesiyle, çok miktarda kişisel veri oluşmakta, kaydedilmekte ve kullanılmaktadır. Bu kişisel veri kümeleri değerli bilgiler içerir, dolayısıyla kontrol edilmelidir. Kişiye ait verinin, güvenlik ve gizlilik bakımından çözülmesi gereken çok sayıda sorun bulunmaktadır. Blokzincir teknolojisi kişisel verilerin gizliliğini korumak ve kontrolünü sağlamak için son yıllarda önemli gelişmeler kaydeden yenilikçi teknoloji olarak görülmektedir. Merkezi olmayan ve eşler arası bir dağıtık dijital defter olan blokzincir teknolojisi, dijital varlıkların tüm işlemlerini depolayabilen, merkezi olmayan, doğrulanabilir ve değiştirilemez bir defter hizmeti sunar. Yakın zamanda tanıtılan Genel Veri Koruma Yönetmeliği (GDPR) ve Kişisel Verilerin Korunması Kanunu (KVKK), kişisel verilerin nasıl ele alınacağı konusunda büyük değişiklikler getirmektedir. Bunlar, bağlayıcı ülkelerde uygulanması gereken tek bir kurallar dizisinden oluşur. GDPR ve KVKK, veri koruma mevzuatı kapsamında birliğinin sağlanması için kişisel olarak tanımlanan verilere 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, trapdoor fonksiyonunu içeren karma değer işlevlerinin kullanımı yoluyla "düzeltilebilir blokzincir" tasarlamak vb.) küçük çaplı değişikliklerin yapılması önerilmektedir. .

ABSTRACT

STORING PERSONAL DATA IN BLOCKCHAIN APPLICATION

With the development of technology, a large amount of personal data is created, recorded and used. These personal datasets contain valuable information, so they should be checked. There are many problems that need to be solved in terms of security and privacy of personal data. 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. Blockchain technology, a decentralized and peer-to-peer distributed digital ledger, provides a decentralized, verifiable and immutable ledger service that can store all transactions of digital assets. The recently introduced General Data Protection Regulation (GDPR) and Personal Data Protection Law (KVKK) bring major changes in how personal data is handled. They consist of a single set of rules that must be applied in the binding countries. GDPR and KVKK introduce new applications such as easier access, deletion, rectification and transportation of personally defined data in order to ensure unity within the scope of data protection legislation. Within the scope of GDPR and KVKK, in a society dominated by centralized structures, 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, in the storage of personally defined data in the researches revealed on the blockchain platform; There are some inconsistencies in the implementation of the KVKK and GDPR provisions, which are prepared for central legal or natural persons to carry out applications such as data storage, processing and deletion. In this study, the basic features of the blockchain are detailed, 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 observed 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 compatible with the characteristic structure of blockchain technology. It is thought by academic circles that developments and updates in blockchain technology will contradict the technology itself and destroy the

characteristic of the blockchain, and therefore will not affect the basic structure (deletion of the private key, off-chain storage, deletion of the hash value, "correctable blockchain" through the use of hash value functions including the trapdoor function. design, etc.) minor changes are recommended.

KISALTMALAR/ABBREVIATIONS

AAA: Açık Anahtar Altyapısı (Public Key Infrastructure)

AES: Gelişmiş Şifreleme Standardı (Advanced Encryption Standard)

CA: Sertifika Yetkilisi (Certificate Authority)

CNIL: Commission Nationale de l'Informatique et des Libertés

DES: Veri Şifreleme Standardı (Data Encryption Standard)

DLT: Dağıtılmış Defter Teknolojisi (Distributed Ledger Technology)

DPoS: Yetkilendirilmiş Hisse İspatı (Delegated Proof of Stake)

ECDSA: Eliptik Eğri Dijital İmza Algoritması (Elliptic Curve Digital Signature Algorithm)

GDPR: Avrupa Birliği (AB) Genel Veri Koruma Yönetmeliği (General Data Protection Regulation)

IoT: Nesnelerin İnterneti (Internet of Things)

IPFS: Gezegenler Arası Dosya Sistemi (InterPlanetary File System)

KVKK: Kişisel Verileri Koruma Kurulu (Personal Data Protection Law)

NIST: Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology)

P2P: Eşler Arası (Peer-to-Peer)

PoS: Hisse Kanıtı (Proof of Stake)

PoW: İş Kanıtı (Proof of Work)

RPoW: Kullanılabilir İş İspatı (Reusable Proofs of Work)

SHA256: Güvenli Karma Algoritması (Secure Hash Algorithm)

3DES: Üçlü Veri Şifreleme Standardı (Triple Data Encryption Standart)

ŞEKİL LİSTESİ/LIST OF FIGURES

TABLO LİSTESİ/LIST OF TABLES

1. GİRİŞ

Günümüzün dijitalleşen dünyasında veri miktarı olağanüstü hızda ve sürekli artmaktadır [1]. 2020'de küresel olarak oluşturulan toplam veri miktarı 64,2 zettabayta ulaştı [2]. Artan bu veriler sürekli toplanmakta ve çeşitli sistemler tarafında analiz edilmektedir, bu da ekonomik açıdan gelişmeyi sağlamaktadır. Kurum ve kuruluşlar topladıkları verileri, hizmetleri kişiselleştirmek, kurumsal karar alma sürecini optimize etmek ve gelecekteki eğilimleri tahmin etmek için kullanır [1]. Kimlik, bir bireyin kişisel seviyesini sembolize eder ve kim olduğumuzun bir sembolü haline gelir ve Bilgi İletişim Teknolojilerinde (BİT) Kimlik Yönetimi, belirli bir bireyin kimliğini doğrulamanın temelini temsil eder. Bu sebeple, kötü amaçlı kullanımlardan kaçınmak için kişisel bilgileri çok iyi korumak ve aynı zamanda kontrol etmek gerekir [3]. Kullanıcı merkezli hizmetler sağlamak için web siteleri fark edilir miktarda kişisel olarak tanımlanan veri toplar (örnek, ırk, yaş sosyal, IP adresi, güvenlik numaraları, ev ve işyeri konumu, ehliyet, pasaport, kimlik vb.). 31 Ağusto 2021 rakamlarına göre 4.021 milyar internet kullanıcısının 2.77 milyardan fazlası, çeşitli sosyal ağ sitelerini kullanıyor ve çok sayıda kişisel bilgiyi kullanıma sunuyor [4]. Bu siteler ve mobil uygulamaları yöneten kuruluşlar, premium hizmetler için oturum açma veya kayıt tutma gibi seçenekleri sunar. Kurum ve kuruluşlar, oluşturulan bu kullanıcı profilleriyle bir iş modeli oluşturarak kişisel verileri depolar. Bu depolanan kişisel veriler üzerinde dağıtım ve analiz işlemlerini yapar. Bu kurum ve kuruluşlar müşteri veri madenciliği için üçüncü bir hizmet olarak da kullanılır. Ayrıca bunun dışındaki kurum ve kuruluşlar da çok sayıda veri toplar. Kullanıcılara bu verilerin nasıl işlendiğine dair hiçbir bilgi verilmemektedir. Birçok kişi verilerin olumlu yönlerinden yararlanıyor, ancak bunların kötü yanı verilerin yasa dışı ve kullanıcının rızası olmadan işlenmesidir. Örnek olarak; Cambridge Analytica şirketinin en büyük Amazon Basit Bildirim Servisi'nden (Amazon Simple Notification Service-SNS) 87 milyon kişisel bilgiyi ihlal ettiğini açıklaması verilebilir [5]. 21. yüzyılda en çok veri ihlali yapan şirket ve kuruluşlardan bazıları; Yahoo (3 milyar), eBay (145 milyon), Adobe (38 milyon), JP Morgan (76 milyon), Personel Yönetimi Ofisi (Office of Personnel Management-OPM)[1]. (22 milyon) [6]. En

[1] Amerika Birleşik Devletleri Personel Yönetimi Ofisi (Office of Personnel Management-OPM), Birleşik Devletler Federal Hükümeti'nin ABD sivil hizmetlerini yöneten bağımsız bir kuruluşudur. Ajans, federal

büyük kullanıcı kitlesine sahip olan Facebook, başlangıçtan bu yana 300 PetaBayt (PB) üzerinde kişisel verileri toplamıştır [7].

Günümüzde kişisel veriler, dünya ekonomisi açısından değerlidir. İnsanlar veri faydalarından yararlanırken, kullanıcıya ait kişisel verilerin gizliliğiyle ilgili artan büyük bir endişe vardır. Merkezi kurum ve kuruluşlar, kamu ve özel sektörler, kişisel ve hassas veriye dayalı çokça veri toplamaktadır. Kullanıcılar, kendileriyle ilgili verilerin ne şekilde kullanıldığı ile ilgili çok az kontrol ve bilgiye sahiptir veya hiçbir bilgisi yoktur. Kişiye ait bilgilerin ihmali veya kötüye kullanımı ve güvenlik açıklarındaki artış, diğer tarafların çokça kişisel veri topladığı ve denetlendiği mevcut modeli sorgulamaktadır. Blokzincir teknolojisi, merkezi olmayan, şeffaf, güven, kimlik yönetimi, veri odaklı kararlar ile günümüz teknoloji faaliyetlerindeki kaygılara bir çözüm olarak öngörülüyor. Aynı zamanda dijital dünyada, kullanıcılar ve makineler aracılığıyla üretilen dijital verilerin miktar ve çeşidinde büyük artış olmaktadır. Büyük veri kümelerini depolama, organize etme ve işleme gibi yollar aranırken, blokzincir sistemi bu kapsamda çok önemli özellikler sağlamaktadır. Özel verilerin merkezi olmayan yönetimi, dijital mülk çözümü, Nesnelerin İnterneti (Internet of Things-IoT)[2] iletişimi ve kamu kurumları hakkında önerdiği çözüm ve reformlar, verinin nasıl gelişebileceği üzerinde önemli etkiye sahiptir. Bitcoin, finansal alanda halka açık bir defter eşliğinde merkezi olmayan bir eşler ağı kullanılarak güvenilir ve denetlenebilir bilgi işlemin mümkün olduğunu gösterdi. Kullanıcıya ait verileri sahiplenen ve bu verileri kontrol eden merkezi olmayan veri yönetim sistemi olan blokzincir, üçüncü tarafın doğrulamasını gerektirmeden otomatik olarak erişimi sağlayan bir protokol gibi görev yapar.

Blokzincir, geleneksel dijital defter bloğunda verileri tutabilen blok yapısı olarak oluşturulmuştur. Bu blok yapısı, sistemin daha güvenli olması için simetrik, asimetrik ve karma gibi kriptografik yapıları kullanılarak bağlantıyı sağlar. Kişisel veri yönetimine blokzincir uyarlaması için de zincir dışı kişisel veri depolama modelinin

---

insan kaynakları politikası için gözetim ve destek sağlar. Ayrıca, federal hükümet çalışanları, emekliler ve bakmakla yükümlü oldukları kişiler için sağlık hizmetleri, hayat sigortası ve emeklilik yardımları ile ilgilenir.

[2] Nesnelerin İnterneti (IoT), internet üzerinden diğer cihazlar ve sistemlerle veri alışverişi yapmak ve bunlara bağlanmak amacıyla sensörler, yazılımlar ve diğer teknolojilerle gömülü olan fiziksel nesnelerin ağını tanımlar.

uygulanması planlanmaktadır. Bununla, kişisel verilerin Genel Veri Koruma Yönetmeliği (General Data Protection Regulation- GDPR) [3]ve Kişisel Verileri Koruma Kurulu (Personal Data Protection Law-KVKK) [4]maddelerine uyulması için bir takım öneriler mevcuttur. GDPR ve KVKK Kanunu verileri koruma düzenlemesi, kişilere, verileri üzerinde daha detaylı kontrol imkânı sağlamak üzere tasarlanmıştır. Özellikle GDPR ve KVKK, veri koruma mevzuatı birliğinin sağlanması; kişisel olarak tanımlanan verilere daha kolay erişim, düzeltme ve silme hakkı düzenlemesi ve veri taşınabilirliği gibi birtakım haklar öngörmektedir. Bundan dolayı GDPR ve KVKK kanunları, merkezi sistemlerin hâkim olduğu bir dünyada veri işleme faaliyetlerinin çoğunlukla merkezi yapılar tarafından gerçekleştirilmesiyle, bu yapılar tarafından gerçekleştirilen veri işleme faaliyetleri sırasında uyulması gereken bir takım usul ve esasları vardır. Ne var ki, blokzincir teknolojisinde ortaya koyulan projelerde kişisel olarak tanımlanan verileri saklama, silme, işleme gibi durumlarda KVKK ve GDPR'deki hükümlerin uygulanmasında bazı uyumsuzluklar oluşmaktadır. Bunlardan biri, değişmez (immutable) olmasıdır. GDPR kapsamında getirilen silinemez (erasure) yükümlülüğüne uyumun sağlanabilmesine ilişkin; diğeri ise halka açık blokzincir (public blockchain) olarak adlandırılan herkesin verilerin kopyasını bulundurmasıdır. Genellikle yeni bloklar oluşturma yetkisine sahip düğüm (node) veya madenci (miner) olarak görev yapan, veri sorumlularının tespit edilebilmesi ve sisteme veri işleyen kişiler ile veri belirlenebilmesine ilişkindir. Şimdiye kadar, anladığımız kadarıyla, başka hiçbir çalışma denetleyicinin ve işlemcinin hassas kullanıcı verilerini nasıl biriktirdiğini ayrıntılı olarak açıklamadı. Ancak, yakın zamanda yürütülen GDPR ve KVKK'nın genel motivasyonu bireysel bilgileri korumaktır, bu nedenle kurumların kamuya açık veri paylaşımına özellikle dikkat etmesi gerekir. Kişisel veriler işlenmeden önce kişinin

[3] 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.

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

rıza alınmalıdır, ayrıca bu kişisel verilerin isteğe bağlı olarak geri alınma, silinme veya bu verileri doğrulama ve yetkilendirme sorumluluğu da vardır, buna kısaca unutulma hakkı da denilebilir.

Blokzincir uygulamasında kişisel verilerin depolama mimarisi, verilerin "değişmezliğine" dayanır. Ancak KVKK ve GDPR, kullanıcı talep ederse kişisel bilgilerin değiştirilmesi ve silinmesi gerekir [8]. Daha önce kullanılan kişisel veri izleme mimarisinde yalnızca üst seviyedekiler verileri nasıl izleyebileceğini bilirler. Bu çalışmada, kişisel verileri depolamak, izlemek ve korumak için blokzincir tabanlı yapılan çalışmalar tartışıldı. KVKK ve GDPR ile uyumlu şeffaf, değişmez bir şema oluşturmak için kişisel ve kişisel olmayan verilerin farklı bir şekilde saklanması ile ilgili öneriler verildi. Kişisel verilerin daha yüksek düzeyde gizlilik ve güvenlik gerektirdiği hassas veri öğeleri için veri kullanımı, saklama süresi ve analizi gibi özellikler önemli bir hale gelebilir. Bununla birlikte, hassas olarak kabul edilen veriler genellikle özneldir, kullanıcının dini, siyasi görüşlerini, kullanıcı adreslerini, bankacılık, kimlik ve sağlık gibi bilgiler içerebilir [9]. Bunu ele almak için, GDPR ve KVKK çıkarılmıştır. Kullanıcılara verilerini kontrol etme ve bu tür verilerin nasıl paylaşılıp işlendiğini kısıtlama hakkı vermek için blokzincir ortamında ele alındı. Kullanıcı gizliliğini ve güvenliğini dâhil etmek için blokzincir tabanlı tekniklerden yararlandı. Verileri güvenli bir şekilde yönetmenin ana zorluğu, tüm faaliyeti kontrol etmekten sorumlu olan insanlara ve kurumlara güvenmektir. Blokzincir teknolojisinin yükselişiyle birlikte, âdem-i merkeziyetçiliği kullanan kendi kendine egemen kimlikler ortaya çıktı; ne yazık ki, kusurlar hala devam etmektedir.

1.1. Çalışmanın Yol Haritası

Bölüm 2'de, blokzincir teknolojisi detaylandırıldı. Bölüm 3'te blokzincir ağında kullanılan kriptografik protokoller anlatıldı. Bölüm 4 kişisel bilgileri tanıtmak için ilgili çalışmaların bilgi gizliliği, GDPR ve KVKK detaylandırıldı. Bu bölümde, ayrıca veri paylaşımı, yönetimi ve izleme mekanizmalarını da detaylandırıldı, blokzincir ağında kişisel verilerin tutulması KVKK ve GDPR kapsamında tartışıldı. Bölüm 5'te GDPR ve KVKK terimleri ve blokzincir ile olan çelişkiler ve literatür taramasında önerilen modeller değerlendirildi. Bölüm 6'da gelecekteki hedefler ve sınırlamalar, gerekli referanslarla takip edilen sonuçlar değerlendirildi.

2. BLOKZİNCİR TEKNOLOJİSİ

Bu bölümde, blokzincir tarihçesi, tanımı çalışma şekli, teknolojisinin temel özellikleri dağıtılmış defterler, sözleşmeler ve konsensüs protokoller hakkında arka plan bilgileri verildi.

2.1. Blokzincir Tarihçesi

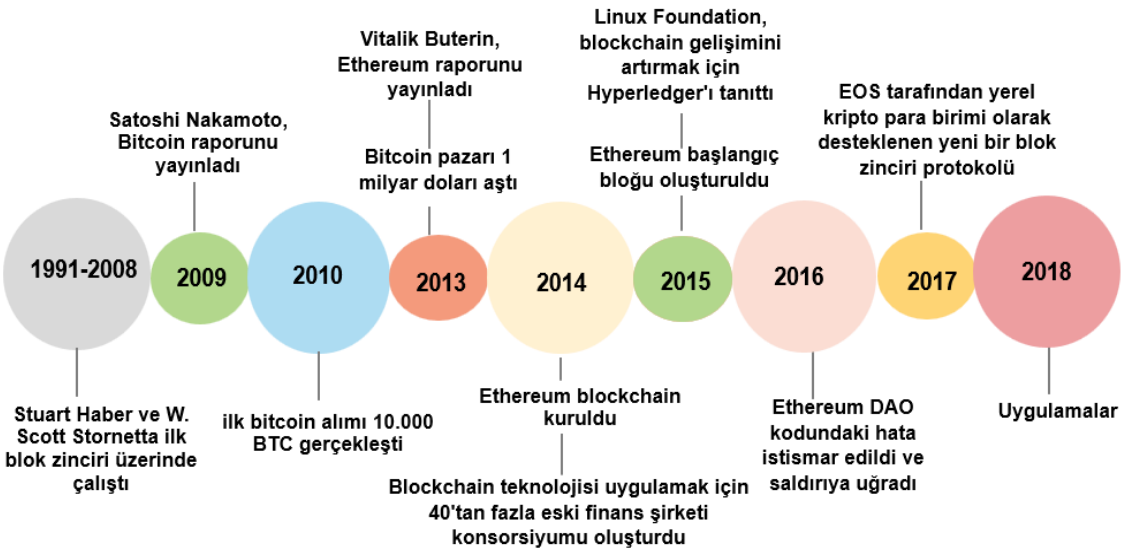
- 1983, David Chaum, Takip Edilemeyen Ödemeler için Kör İmzalar (Blind Signatures for Untraceable Payments) ve kripto para kavramını ortaya koydu.
- 1989 David Chaum, Digicash kurdu ve iflas etti.
- 1990, David Chaum, Fiat ve Naor, Takip Edilemeyen Elektronik Nakit (Untraceable Electronic Cash) ortaya koydu.
- 1991, Stuart Haber ve W. Scott Stornetta, blokzincir teknolojisinin arkasındaki fikir, hesaplama açısından kullanışlı bir çözüm ile dijital olan belgeler zaman damgasıyla kurcalanamaz veya geriye dönük olarak değiştirilemez. Zaman damgalı belgelerin saklanması için kriptolanmış güvenli bir blokzincir kullanmış ve 1992 yılında Merkle ağaç tasarıma dâhil edilmesiyle birlikte birkaç belgenin bir blok halinde toplanmasıdır.
- 1997, Adam Back, Hashcash sistemi, mail gönderimlerindeki spam ve Servis Hizmet Reddi (Denial-of-Service-DoS) saldırılarını engellemek için kriptografik hash algoritması kullandı. Hashcash'de, posta (mail) gönderen taraf başlığına Hashcash damga (stamp) ekleyerek bir süre kendi işlemcisi üzerinde hesaplamalar yaptığını kanıtladı. Mesajın başlık (header) kısmı arka arkaya birkaç bin kez hash hesaplaması ile elde edildi.
- 1998 Bilgisayar bilimi ve aynı zamanda yazar olan Nick Szabo, merkezi olmayan bir dijital para birimi olan "bit gold" ile ilgili çalışmalar yaptı.
- 1998 Wei Dai, "b-money", PoS
- 1998 Nick Szabo, Bit Gold'u yaratmak için bir teklifte bulundu (Adam Back'den PoW).

- 2000 Stefan Konst, kriptografik olarak güvenli zincir teorisini ve uygulama ile ilgili fikirlerini açıkladı.
- 2004 Hal Finney, bilgisayar bilimcisi ve kriptografi aktivisti, yeniden kullanılabilir iş ispatı (Reusable Proof of Works-RPoW) değiştirilemez ve özgün bir Hashcash tabanlı PoW ile kişiden kişiye aktarılabilen bir Rivest Shamir Adleman (RSA) imzalı token oluşturmuştur. RPoW, tokenların mülkiyetini, verilerin bütünlüğünü ve doğruluğunu kontrol etmesine izin verecek şekilde tasarlanmış güvenilir bir sunucuda tutmak yoluyla, çifte harcama (double spending) sorununu çözmüştür.
- 2005 Nick Szabo sadece konseptini kamuya açıkladı, Bit Gold hiçbir zaman çalıştırılmadı.
- 2008 Nick Szabo, blogunda Bit Gold hakkında yazdı, sadece o zaman ilk gerçek uygulamayı yapmak istedi
- 2008 Aralık, Bitcoin: Eşler arası (Peer to Per-P2P) Elektronik nakit ödeme sistemi (Electronic Cash System) incelemesi, Satoshi Nakamoto adını kullanılarak kriptografi posta listesine gönderilmiştir. Bitcoin'de çifte harcama (double-spending) koruması: Hashcash PoW algoritmasına dayanmakta ancak RPoW gibi donanım tabanlı hesaplama işlevi kullanmak yerine, Bitcoin'de çifte harcama koruması, işlemleri takip eden ve doğrulayan, eşler arası dağıtık bir protokol tarafından sağlanır. Bitcoinler bireysel madenciler tarafından PoW mekanizması kullanılarak ödül için "kazılır" ve daha sonra ağdaki diğer bilgisayarlar tarafından doğrulanır.
- 2009, 3 Ocak Bitcoin blok kavramı ilk olarak Satoshi Nakamoto tarafından ortaya atıldı, (50 bitcoin kazandırdı). Bitcoin'in ilk alıcısı olan Hal Finney, (12 Ocak 2009, dünyanın ilk bitcoin işleminde Satoshi Nakamoto'dan 10 bin bitcoin aldı) (bkz: Şekil 2.1).
- 2013, bir programcı ve Bitcoin Dergisi'nin kurucularından olan Vitalik Buterin, "Bitcoin'in merkezi olmayan uygulamalar oluşturabilmesi için bir script diline ihtiyaçı var." Topluluk içinde anlaşmaya varamayan Vitalik, akıllı sözleşmeler tabanlı bir blokzincir platformu olan Ethereum'u

geliştirmeye başladı.

- 2014, NEO (Çin Ethereum, Alibaba).
- 2015, IOTA[5]. IoT ekosistemi için optimize edilmiş kripto para birimi platformu, sıfır işlem ücreti ve benzersiz doğrulama süreçleri. Blokzincir 1.0 Bitcoin ile ilişkili bazı ölçeklenebilirlik sorunlarını giderdi. Önceki blokzincir uygulamaları Monero, Zcash ve Dash blokzincirleri, Altcoin ile ilişkili bazı güvenlik ve ölçeklenebilirlik sorunlarını ele aldı.
- 2015, Açık kaynaklı blokzincir Hyperledger Linux Foundation Umbrella projesi, blokzincir ve dağıtılmış defterlerin geliştirilmesi için sektörlerde işbirliği yapıldı.
- 2017, EOS. IO EOS, EOS tarafından yerel kripto para birimi olarak desteklenen yeni bir blokzincir protokolü geliştirildi. Diğer blokzincir uygulamalardan farklı olarak EOS, CPU ve GPU dahil olmak üzere gerçek bilgisayarların özelliklerini taklit etmeye çalışır. EOS, IO, akıllı bir sözleşme platformu ve merkezi olmayan bir işletim sistemi. Ana amaç, merkezi olmayan uygulamaların özerk ve merkezi olmayan bir şirket aracılığıyla konuşlandırılmasını teşvik etmektir.

[5] Nesnelerin İnterneti (IoT) ekosistemindeki herhangi bir makine veya cihaz arasındaki işlemleri kaydetmek ve yürütmek için oluşturulan dağıtılmış bir defterdir.

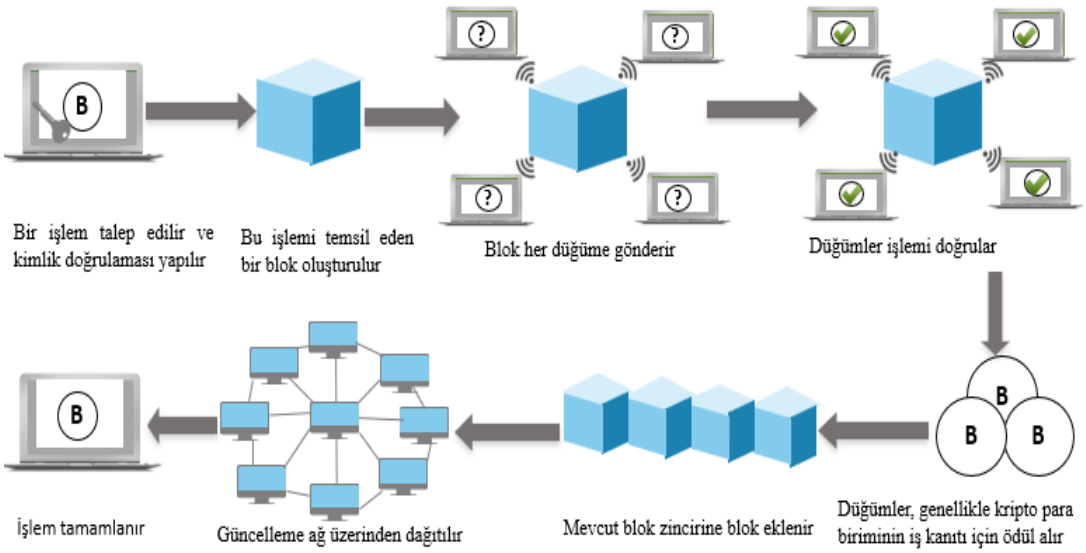


Şekil 2. 1 Blokzincir Tarihçesi. [11]

2.2. Blokzincir Tanımı

Blokzincir, dağıtılmış defter teknolojisi (Distributed Ledger Technology-DLT) olarak da isimlendirilir. Blokzincir, karma, simetrik/asimetrik şifreleme gibi kriptografik yöntemleri kullanarak işlem ve kayıtların çeşitli kişilerce çeşitli saldırılara karşı koruma sağlayan merkezi olmayan, dağıtılmış ve doğrulanabilir bir veri tabanı teknolojisidir. İşlem ve mesajlarda zaman damgası kullanılarak dağıtılmış veri tabanında bir işlemin varlığı veya yokluğu için evrensel olarak doğrulanabilir kanıtlar sağlar [11]. Hesaplama açısından da güvenli ve herhangi bir zamanda doğrulanabilir. Teknolojinin yapısı bloklardan oluşur ve bir önceki blok bir sonraki bloğa bağlı olduğu için blokzincir olarak tanımlanır. Halka açık veri tabanında (zincir) depolanan dijital bilgilerden (blok) meydana gelmektedir [12]. Bu uygulamanın avantajlarından birkaçı da kullanıcı ağa bağlanabilir yeni işlemler başlatıp, yeni bloklar oluşturabilir ve bu durumda işlemleri takip etmek kolaydır. Gerçekleştirilen işlemlerin kaydı ağın tümünde tutulur bu durumda veri güvenliği de sağlanmış olur [13]. Ağın tümünde kaydedilen veriler, fikir birliğine varılmadan değiştirilemez veya silinemez. Kısacası blokzincir, değer içeren verilerin güvenli bir şekilde depolanması, bir aracıya ihtiyaç duyulmadan iki taraf arasında verilerin yönetilmesi için tasarlanmış şeffaf ve doğrulanabilir bir teknolojidir [14]. Bu bağlamda, blokzincir, dağıtılmış, merkezi olmayan ve kamuya açık olan bir defterdir [15].

2.3. Blokzincir Çalışma Şekli



Şekil 2. 2 Blokzincir Çalışma Şekli. [16]

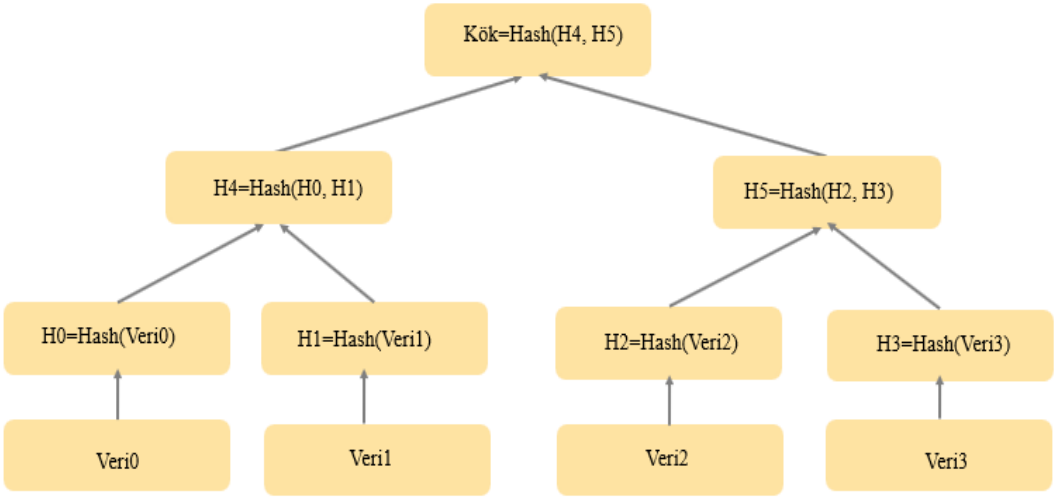
Blokzincir ağında, X kişisi başka bir Y kişisine blokzincirdeki Bitcoin ağını kullanarak cüzdan üzerinden para göndermek isterse X kişisi tarafından Bitcoin ağında işlem başlatılır. Madencilik sürecini başlatmak için işlem ağdaki her düğüme yayınlanır. Madenci olan bu düğümler, işlemleri bir blokta toplayarak bloktaki işlemleri doğrulayacak ve ağdan onay almak için bir konsensüs protokolü kullanarak bloğu ve doğrulamasını yayınlayacaktır. Şekil 2.2'de gösterildiği gibi diğer düğümler, blokta yer alan tüm işlemlerin geçerli olduğunu doğruladığında, blok blokzincir ağına eklenebilir. Bitcoin'deki blokzincir uygulaması tarafından desteklenen üç temel özellik şunlardır: Karma zincir depolama, dijital imza ve küresel zincir depolamaya yeni bir blok eklemek için taahhüt konsensüsü. Karma zinciri, Merkle ağacı, dijital imza gibi bir dizi popüler güvenlik tekniğinin fikir birliği mekanizmalarıyla zarif bir kombinasyonu ile Bitcoin'lerin çifte harcama (double spending) problemi önlenebilir.

2.3.1. Karma Zincir Depolama

Karma zincir ve Merkle ağacı, karma zincir depolama modelini kullanarak Bitcoin ağındaki blokzinciri kullanmak için temel özelliklerin ilkidir. Blokzincir uygulamasında depolanan tüm verilerin karması ile depolanan veriler değiştirilmez ve silinemez. Tüm zincirdeki herhangi bir bloktaki veriler değiştirilirse önceki tüm blokların karma işaretçilerin değiştirilmesi gerekir. Başlangıç bloğunun kök iz işaretçisi kaydedilerek

tüm zincir etkili bir şekilde kurcalamaya karşı dayanıklılık özelliğine sahip olabilir.

2.3.2. Merkle Ağacı (Merkle Tree)

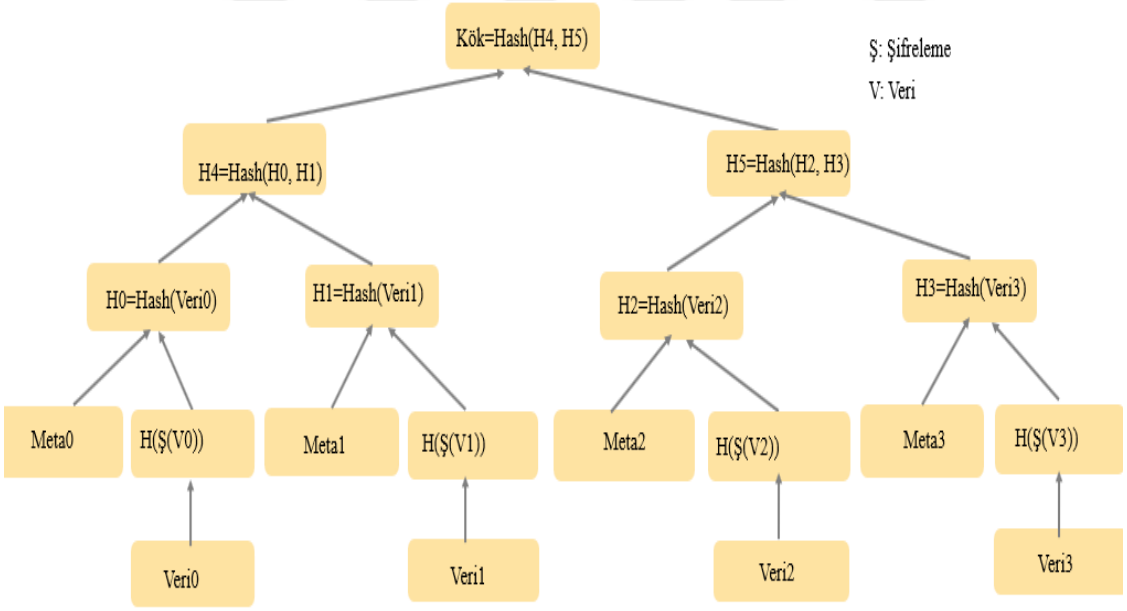


Şekil 2. 3 Merkle Ağaç Yapısı. [17]

Merkle ağaç ile ilgili öneriler ilk olarak 1979 yılında Merkle tarafından ortaya atılmıştır [18]. Bu önerilen yöntemle kaydedilen verileri bloklarda parçalara ayrılır. Merkle ağaç yapısında bulunan tüm bloklara Şekil 2.3'te gösterildiği gibi hash uygulanır, kökten başlayıp yapraklardaki her düğüme girer ve tek hash değeri oluşturulana kadar Merkle ağacı hashlemeyi tekrarlar. Bu yapının kökündeki hash değeri sistemin imzası olarak kullanılabilir. Bu yöntem, verilerin bütünlüğünü ve sürekliliğini kontrol etmek için uygundur. Blokzincir uygulamasında, Merkle ağaçta uygulanan hash ile bloktaki verilerinin bütünlüğünü, güvenliğini ve sürekliliğini sağlamak için kullanılır. Ayrıca, kontrolü zor verilerin bütünlüğünü yönetmek için kullanılabilir. Bu veriler başka bir düğümde kullanılacaksa, veri iletim işleminden sonra verilerden Merkle ağacın kökü çıkarılır ve diğer düğümlerdeki değerler karşılaştırılarak iletimi yapılan verilerin doğruluğu ve bütünlüğü sağlanır. İletim aşamasında bayt veride herhangi bir hata bile oluşursa, düğümlere uygulanan (hash değerleri) ile hatayı kolayca bulup çözebilir. Böylece, bloklardaki verilerin özet değerleri doğrulama için karşılaştırılır, değerler aynı değilse verimli olarak tespit edilen ilgili verilerin güncellenmesiyle senkronizasyon sağlanabilir.

Merkle ağaç açık blokzincir uygulamasında verilerin bütünlüğünü ve doğruluğunu sağlamak için kullanılır. Şekil 2.3'te tipik bir Merkle ağaç yapısını göstermektedir.

Ancak, Merkle ağaç yalnızca bütünlüğü dikkate alır ve varsayılan olarak güvenliği dikkate almaz. Uygulanan karma değer kişinin isteğiyle değiştirilirse veya silinirse, bütünlüğü sağlamak amacıyla bu yöntem kullanılabilir. Ancak, verinin özgün bir kısmı sahte veya bozuksa ve karma değeri sahte veya bozuk verilere dayalı tekrar oluşturulmuşsa ve verinin oluşum aşamasında imza değeri yoksa bütünlük ile ilgili kontrol yapılamaz. Ayrıca verilerin eklenmesi veya silinmesi durumunda delta güncelleme işlemi desteklenmemektedir. Bu durumda, Merkle ağacın dezavantajlarını ortadan kaldıran yeni bir Merkle ağaç yöntemi olan bir Güvenli Merkle Ağacı (Security Merkle Tree-SM-Tree) yöntemi önerilmiştir [19]. Bu yöntem, düz metni şifrelenmiş verilere ve meta verilere böler ve bir karma ağacı oluşturur ve veri bloğunun değişken boyutunu yönetebilir (bkz Şekil 2.4). Ayrıca, senkronize edilen verileri meta veri değerleriyle karşılaştırarak verilerin sahte veya tahrip edilip edilmediğini bütünlük kontrolü ile görmek mümkündür. Ayrıca, verilerin yalnızca ağacın kendisi tarafından kontrol edilebildiği ve orijinalin kurcalanmasının önlendiği blokzincir tabanlı video izleme ortamı için uygundur.



Şekil 2. 4 Güvenli Merkle Ağaç (SM) Yapısı. [17]

2.3.3. Dijital İmza

Dijital imza, bir şifreleme algoritması kullanarak bir veri parçasının geçerliliğini belirler. Aynı zamanda, bir veri parçasının tahrip edilmediğini doğrulamak için bir şemadır. Dijital imza ile ilgili üç önemli özellik vardır. Bunlardan birincisi, çift anahtar

oluşturan simetrik ve asimetrik anahtar oluşturma algoritmasıdır. Anahtarlardan biri mesajları imzalamak için kullanılır ve özel olarak saklanıp özel (private) anahtar olarak isimlendirilir. Diğeri ise geneldir, genel (public) anahtar olarak da bilinir, imzanın özel anahtar imzalamayı doğrulamak için kullanılır. Diğer önemli özellik, imzalama algoritmasıdır. Verilen özel anahtarı kullanarak onaylanan giriş mesajında bir imza niteliği oluşturur. Son olarak, doğrulama algoritmasıdır. Veri girişi olarak bir mesajın imzasını ve bir genel anahtarı alır ve bu genel anahtarı kullanarak mesajın imzasını doğrular buna bağlı olarak doğru veya yanlış değeri döndürür. Güvenilir bir imza algoritmasının iki önemli özeliği olmalıdır. Birincisi, kullanılan imzaların doğrulanmasıdır. İkinci özellik ise imzaların taklit edilemez olmasıdır. Bu da, genel anahtarınıza sahip bir kötü niyetli kullanıcının bazı mesajlarda oturum açamayacağı anlamına gelir.

Bitcoin'deki blokzincir uygulamasında, imzalama için dijital imza için Eliptik Eğri Dijital İmza Algoritması (Elliptic Curve Digital Signature Algorithm-ECDSA) algoritması kullanır. Eliptik eğri "secp256k1" [6]üzerinde ECDSA kullanılarak, Bitcoin blokzincir için 128 bitlik güvenlik sağlanır [20]. ECDSA, jenerik bir gruba ve çarpışmaya dirençli hash fonksiyonuna dayalı bir seçilmiş mesaj saldırısının mevcudiyetinde sahteciliğe karşı dirençli olduğunu kanıtlamaktadır (Bölüm 2.8.3 anlatıldı). Dijital imza kullanmanın avantajı, Açık Anahtar Altyapısı-AAA (Public Key Infrastructure-PKI)[7] kullanarak mesajın gerçekliği etkin bir şekilde doğrulanabilmektedir, öyle ki mesajı yazan kişi mesajı göndermeden önce kendi özel anahtarıyla imzalar; bu imzalı mesajın alıcısı, mesajın geçerliliğini kanıtlamak için gönderenin genel anahtarını kullanabilir. Çoğu uygulama senaryosunda güvenilir bir üçüncü taraftan anahtar çifti elde edilebilir. Bir AAA, varlıkların ilgili kimlikleri (ad, e-posta ve kimlik, pasaport vb.) ile ortak anahtarları arasında bağlayıcı bir anlaşma oluşturarak ortak anahtarları yönetmek için kullanılır. Sertifikaların bir sertifika

[6] Secp256k1, Bitcoin tarafından ortak anahtar şifrelemesini uygulamak için kullanılan eliptik eğrinin adıdır. Bu eğri üzerindeki tüm noktalar geçerli Bitcoin ortak anahtarlarıdır.

[7] Açık anahtar altyapısı (PKI), ortak anahtarları ve dijital sertifikaları oluşturmak, dağıtmak, yönetmek, depolamak, kullanmak ve iptal etmek için gereken donanım, yazılım, ilkeler, süreçler ve prosedürler kümesidir. Ayrıca, ortak anahtarın güvencesini sağlar. Ortak anahtarların tanımlanmasını ve dağıtımını sağlar.

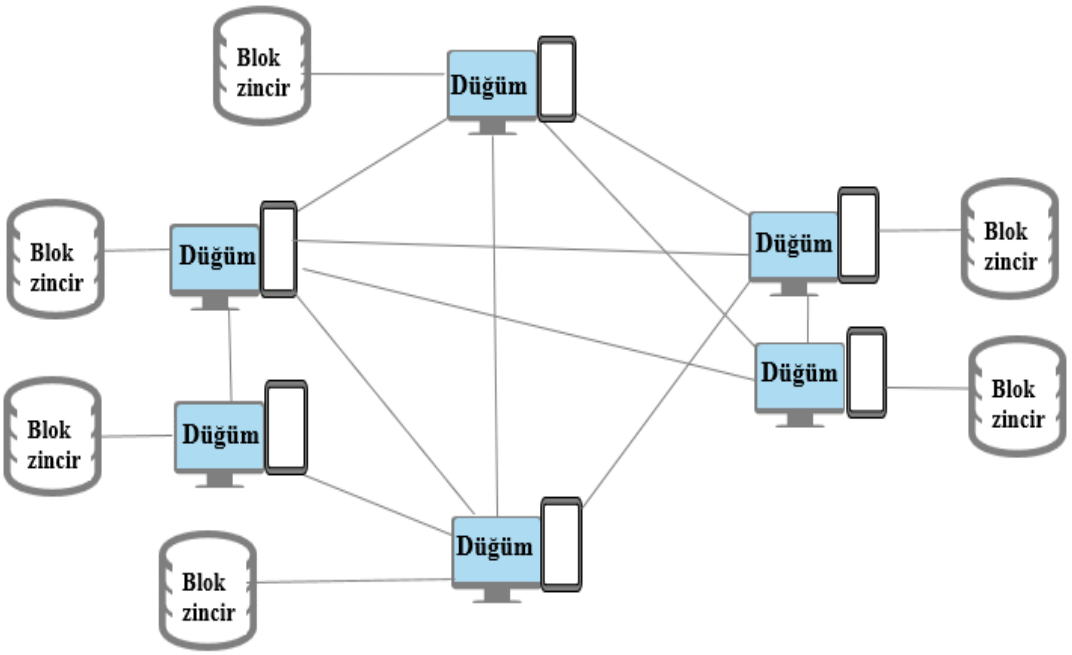
merkezine depolanması ve sertifikaya yetki verilerek yapılır. İmza doğrulama süreci, bağlayıcının güvence düzeyine bağlı olarak otomatik olarak imzalayanın kimlik doğrulamasına çevrilir.

2.3.4. Dağıtılmış Defter Teknolojisi (DLT)

Blokzincir, merkezileştirilmiş altyapıyı dağıtılmış bir altyapıyla değiştirerek bir yönetim mekanizmasını önerir. Yetki birçok güvenilir aktör arasında dağıtılır [21]. Dağıtımda P2P teknolojisi kullanılır. Dağıtılmış bir defter, işlemleri doğrulamak için merkezi bir otorite veya aracıya olan ihtiyacı ortadan kaldırmak için merkezi olmayan bir yapı sağlar (bkz: Şekil 2.5). Kurum ve kuruluşlar, işlemleri veya diğer veri alışverişi türlerini işlemek ve doğrulamak için dağıtılmış bir defter teknolojisini kullanır. Tipik olarak bu kayıtlar sadece ilgili taraflarca fikir birliğine varıldığında defterde saklanır. Dağıtılmış defterdeki tüm dosyalara zaman damgası eklenir ve sadece o dosyada kullanılacak bir şifreleme imzası verilir [22].

Dağıtılmış defterde bulunan katılımcılar söz konusu kayıtları izin yönetimine göre görüntüleyebilir. DLT, söz konusu veri kümesinde depolanan bütün bilgilerin doğrulanabilir ve denetlenebilir bir geçmiş sağlar. DLT, kullanıcılara tüm bilgilerinin ve işlemlerinin kontrolünü verir ve şeffaflığı teşvik eder, aynı zamanda verimlilik ve otomasyonu da kolaylaştırır. Blokzincir gibi dağıtılmış defterler, finansal işlemler için fazlasıyla faydalıdır. İşlemsel verimsizlikleri azaltır. Merkezi olmayan yapıları ve defterlerin değişmez olması nedeniyle daha fazla güvenlik ve gizlilik sağlar. Bir blokzincir uygulamasına veri eklendiğinde değişmez bir şekilde ağa kaydedilir. Zaman içinde bir dizi işleminiz olduğunda, doğru ve değişmez bir denetim elde edilir. Verilerin tek bir varlığın sahibi olmadığı veya kontrol etmediği ve hiç kimsenin önceden yazılmış olanı değiştiremeyeceği bir yerde saklanması, çift girişli defter tutma gibi avantajlar sağlar. Bu durumda, hata ve dolandırıcılık oranı düşer [22].

2.3.5. Eşler Arası (P2P)



Şekil 2. 5 Eşler Arası (P2P) Yapısı. [23]

P2P, blokzincirin tamamında veya belli bir kısmında depolanan dağıtılmış ve yedekli eşler arası bir düğüm sistemidir (bkz: Şekil 2.5). Kriptografik algoritmalarla bir araya gelmiş ekonomik destek mekanizmalarına dayalı dağıtılmış fikir birliği algoritması ile işlemlerin güvenli P2P doğrulamasını sağlar, bu da geleneksel ve merkezi yapılardaki güvenilir üçüncü taraflara olan ihtiyacı ortadan kaldırarak daha şeffaf, doğrulanabilir ve merkezi olmayan bir çözüm sağlar. İlk olarak Ekim 2008'de, bankalar olmadan P2P para yaratma amacıyla Bitcoin teklifinin bir parçası olarak ün kazandı [24].

Tüm ağ işlemleri blokzincir ağında depolanır. Blokzincir, P2P ağları fikri üzerine kuruludur ve birbirlerini tanımasalar veya güvenmeseler bile her aktörün güvenebileceği evrensel bir veri seti sağlar. Değişmez ve şifreli bilgi kopyaları ağdaki her düğümde depolandığı için güvenilir bir işlem defteri sağlar [13]. Ağı hataya dayanıklı, saldırı ve gizli anlaşmalara karşı dirençli hale getirmek için yerel ağ belirteçleri biçimindeki ekonomik teşvikler uygulanır.

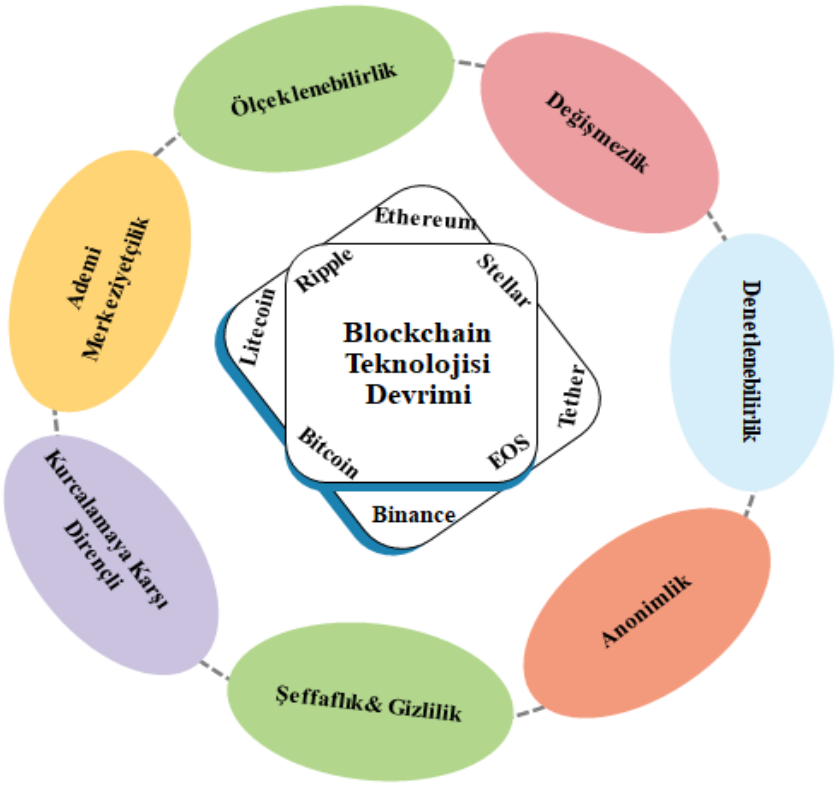
2.3.6. Uzlaşma

Merkezi olmayan blokzincir bağlamında, ağa geniş yayın yoluyla yeni bir blok gönderildiğinde her düğümün bu bloğu kendi yerel defter kopyasına ekleme veya yok

sayma seçeneği vardır. Konsensüs, blokzincir genişlemesini güvence altına almak ve dürüst olmayan girişimleri veya kötü niyetli saldırıları önlemek için ağın çoğunluğunu tek bir durum güncellemesi üzerinde anlaşmaya varmasını sağlamak için kullanılır. Bir düğüm, kendi genel muhasebe defter kopyasının durumunu değiştirmeye karar vermesi veya birkaç düğümün gizlice bu tür kurcalamaya teşebbüs etmesi bir suç olabilir. Örneğin, Alice cüzdanından Bob'a 10 Bitcoin gönderiyorsa, ağdaki hiç kimsenin işlem içeriğini kurcalayamayacağından ve 10 Bitcoin'i 100 Bitcoin'e değiştiremeyeceğinden emin olmak ister. Blokzincirin güvenlik ve doğruluk garantisi ile küresel ölçekte çalışmasını sağlamak için paylaşılan ortak defterin, hataya dayanıklı olması gereken ve tüm düğümlerin aynı anda aynı zinciri sürdürmesini sağlayan verimli ve güvenli bir fikir birliği algoritmasına ihtiyacı vardır. İyi niyetli olmayan kişilerin uzlaşmanın ihlâlini önlemek için mevcut olan merkezi bir yapıya güvenmez. Aynı şekilde, ağdaki düğümler arasında gönderilen herhangi bir mesajın ya da metnin fikir birliğine bağlı bir anlaşma sağlanması için ağdaki katılımcılarının çoğu (en az %51) tarafından onaylanması gerekir. Buna ek olarak, ağdaki bazı kötü niyetli düğümlerin olması veya iletilen bir mesaj ya da metnin bozulması gibi hatalara ve olası saldırılara karşı çok dayanıklı olmalıdır.

Blokzincir mimarisinde kullanılan fikir birliği algoritmasının sağlam olması kalıcılık ve canlılık açısından iyi dağıtılmış işlem defteri sağlar. Kalıcılık ile yapılan işlemin durumuyla ilgili mimariden tutarlı cevap almayı garantiler. Canlılık ise tüm düğümlerin veya süreçlerin sonunda bir karar veya değer üzerinde anlaşmaya vardığını belirtir. Blokzincir uygulamasında dağıtılmış deftere bazı veriler depolandıktan sonra blokzincir ağına kaydedilen verilerin değiştirilmesi ve silinmesi imkânsız olmalıdır ve güncelleme ve silme işlemi için çoğunluk (en az %51) fikir birliği uygulanmalıdır. Konsensüs algoritmaları Bölüm 2.5'de açıklandı ve karşılaştırıldı.

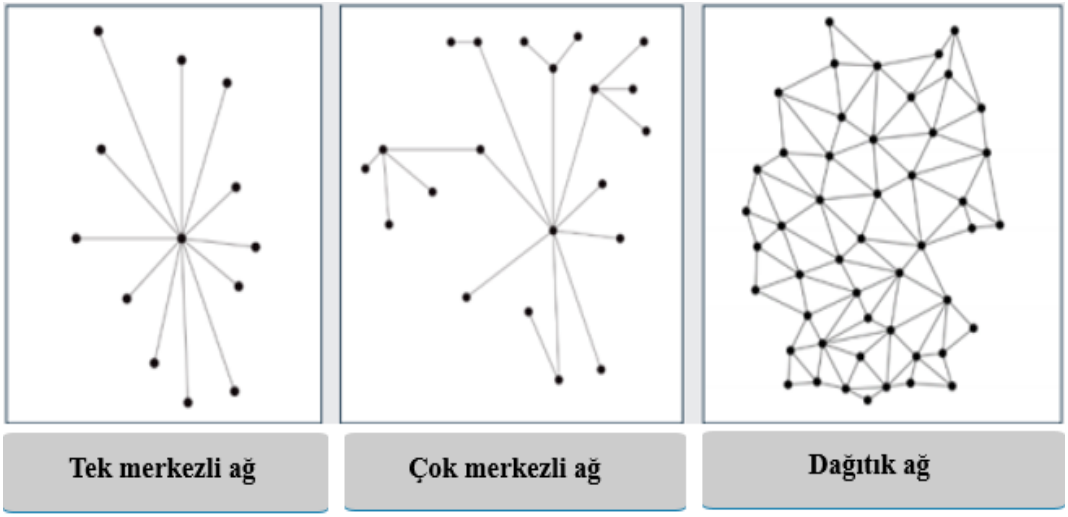
2.4. Blokzincir Teknolojisinin Temel Özellikleri



Şekil 2. 6 Blokzincirin Temel Özellikleri. [25]

Şekil 2.6'da gösterildiği gibi blokzincir teknolojisi genellikle yedi temel unsurdan oluşur.

2.4.1. Adem-i Merkeziyetçilik (Decentralization)



Şekil 2. 7 Ağların Karşılaştırılması. [7]

Adem-i merkeziyetçiliğin mevcut kullanımı merkezi yapıdan çok daha farklıdır.

Merkezi uygulamaya göre daha fazla güvenlik ve esneklik sağlar [7]. Merkezi olmayan bir blokzincir ağında hiç kimse kimseyi tanımak veya güvenmek zorunda değildir. Blokzincir uygulamasındaki tüm üyeler, ağdaki dağıtılmış bir defter ile aynı veri kümelerin bir kopyasını bulundurur. Uygulamadaki dağıtılmış bilgilerde uzlaşma sağlanırsa herhangi bir şekilde değiştirilebilir, silinebilir ya da veri bozulursa, ağda bulunan üyelerin çoğunluğu tarafından iptal edilebilir. Şekil 2.7'de gösterildiği gibi merkezileştirilmiş bir yapıda tüm işlemler aynı yerde yapılır, merkezi olmayan yapıda ise işlemler farklı yerlerde yapılır. Merkezi olmayan yapı daha çok verimlilik ve yenilik sağlar. Verimlilik ve yenilik de daha iyi maliyet ve zaman tasarrufu sağlar [26].

Tablo 2. 1 Merkezi Olmayan, Merkezi ve Dağıtılmış Ağların Karşılaştırılması

	Merkezileştirilmiş	Dağıtılmış	Merkezi olmayan
• Ağ/donanım kaynakları	• Merkezi bir konumda tek bir varlık tarafından sürdürülür ve kontrol edilir	• Birden çok veri merkezi ve coğrafyaya yayılmış; ağ sağlayıcısına ait	• Kaynaklar, ağ üyeleri tarafından sahiplenilir ve paylaşılır; kimsenin sahibi olmadığı için bakımı zor
• Çözüm bileşenleri	• Merkezi kuruluş tarafından sürdürülür ve kontrol edilir	• Çözüm sağlayıcı tarafından bakım ve kontrol	• Her üye, dağıtılmış defterin tam olarak aynı kopyasına sahiptir
• Veri	• Merkezi kuruluş tarafından sürdürülür ve kontrol edilir	• Genellikle müşteri tarafından sahip olunan ve yönetilen	• Yalnızca grup fikir birliği yoluyla eklendi
• Kontrol	• Merkezi kuruluş tarafından kontrol edilir	• Tipik olarak, ağ sağlayıcı, çözüm sağlayıcı ve müşteri arasında paylaşılan bir sorumluluk	• Kimse veriye sahip değil ve herkes veriye sahip
• Tek hata noktası	• Evet	• Hayır	• Hayır
• Hata toleransı	• Düşük	• Yüksek	• Son derece yüksek
• Güvenlik	• Merkezi kuruluş tarafından sürdürülür ve kontrol edilir	• Tipik olarak, ağ sağlayıcı, çözüm sağlayıcı ve müşteri arasında paylaşılan bir sorumluluk	• Ağ üyesi sayısı arttıkça artar
• Verim	• Merkezi kuruluş tarafından sürdürülür ve kontrol edilir	• Ağ/donanım kaynakları büyüdükçe ve büyüdükçe artar	• Ağ üyesi sayısı arttıkça azalır
• Örnek	• ERP sistemi	• Bulut bilişim	• Blokzinciri

Her blokzincir protokolü, merkezi olmayan uygulama (dApp), Merkezi Olmayan ve Otonom Organizasyon (Decentralized Autonomous Organization-DAO)[8] değişen düzeylerde ademi merkeziyetçiliği benimser. Ademi merkeziyetçilik mantıklı olduğu yerde uygulanmalıdır. Uygulanan bir blokzincir mimarisi olması, %100 merkezi olmayan bir yapı olduğu anlamına gelmez. Uygulanan blokzincir çözümünün temel amacı, kullanıcıların ihtiyaç duyduğu güveni sağlamaktır ve bu, belirli seviyede ademi merkeziyetçiliği sağlayabilir veya sağlamayabilir. Merkezi olmayan ağ yapılarını daha iyi anlamak için Tablo 2.1'de merkezi olmayan, daha yaygın merkezi ve dağıtılmış ağların karşılaştırılması gösterilmektedir.

2.4.1.1. Merkezden Yönetilmemenin Avantajları

- **Güvensiz bir ortam sağlar**

Merkezi olmayan bir blokzincir ağında kimse kimseyi tanımak veya güvenmek zorunda değildir. Ağdaki her düğüm, kaydedilen verilerin dağıtılmış bir defter biçiminde kopyasına sahiptir. Bir düğümün dağıtılmış defteri herhangi bir şekilde değiştirilir, silinmeye çalışılırsa veya bozulursa ağdaki diğer düğümler tarafından reddedilecektir [68].

- **Verilerin mutabakatını iyileştirir**

Şirketler, kurum ve kuruluşlar genellikle ortak paydaşlarıyla veri alışverişinde bulunur. Bu veriler, sırayla her bir tarafın veri silolarında tipik olarak dönüştürülür ve depolanır, yalnızca aşağı doğru iletilmesi gerektiğinde yeniden ortaya çıkar. Merkezi olmayan bir veri depolama sistemiyle, tüm kişiler gerçek zamanlı olarak paylaşılan her veriye istediği zaman erişim sağlayabilir [68].

- **Zayıf olan noktaları azaltır**

Ademi merkeziyetçilik, belirli aktörlere çok fazla güvenilebileceği sistemlerdeki zayıf noktaları azaltabilir. Bu zayıf noktalar; kaynakların tükenmesi, periyodik kesintiler, darboğazlar, iyi hizmet için yeterli teşvik eksikliği, yolsuzluk nedeniyle vaat edilen hizmetlerin sağlanamaması ve sistemik arızalardır [68].

[8] DAO, işletmenin sahip olduğu ve üyeleri tarafından demokratik bir şekilde yönetildiği, dünya çapında benzer düşünen insanlarla çalışmanın bir yoludur.

- **Kaynak dağıtımını iyileştirme**

Merkezi olmayan yapı ile hizmetlerin daha iyi performans, doğruluk, süreklilik ve tutarlılığın yanı sıra üçüncü tarafın iletişimine ihtiyaç duymadan daha düşük hata olasılığı sağlanması için kaynakların dağıtımını iyileştirmeye yardımcı olur [67].

2.4.2 Şeffaflık ve Gizlilik

Blokzincirin teknolojisinde her blok bir önceki blok ile ilgili bilgi içerir. Yapılan işlemler ile kişilerin kimlik bilgilerini doğrular. Ayrıca, herhangi bir üçüncü tarafın iletişimi yoktur. Halka açık dağıtılmış bir defter kullanılır, yapılan tüm işlemler otomatik olarak bu deftere kaydedilir. Bu, blokzincir ağındaki tüm kullanıcıların tüm işlemleri denetlediği anlamına gelir. Kullanıcılar dünyanın herhangi bir yerinden işlem yapabilir, tek yapmaları gereken kendilerini bu defterlere kaydettirmek. Blokzincir teknolojisi, ağdaki herkesin defterin bir kopyasına sahip olması nedeniyle işlemlerin şeffaflığını artırır. Bu durum, blokzincir defterlerini kurcalamaya karşı korumalı hale getirir [27]. Kullanıcılar şüpheli bir işlem tespit ettiğinde ilgili işlemi reddedebilir. Blokzincirin açıklığı, bir platformu daha şeffaf hale getirir, böylece kullanıcılar bir dolandırıcılık endişesi olmadan bir sözleşme yapabilir.

Blokzincir teknolojisindeki gizlilik, blokzinciri özel kılan bir başka özeliktir. Gerekli verileri yayınlandığında blokzincir ağındaki gizlilik korunabilir ve bilgilerin kötüye kullanılmayacağından emin olunabilir. Kişilerin işlemlerini ve kimliklerini gizli tutmaları için erişimin sınırlı olduğu özel ağlar oluşturulabilir ve kişiler blokzincir ağına eklenecek varlıklar listesinden seçim yapabilir [25].

2.4.3. Kurcalamaya Karşı Dirençlilik

Blokzincir ağını kurcalamaya karşı dayanıklı tutmak için madenci adı verilen bir kullanıcı vardır. Madenci, madencilik adı altında işlemleri doğrular. Madencilik yapan kişiler, blokların karma yapısını kullanarak blokların hepsini birbirine bağlar bu da uygulamada yapılan işlemleri daha tutarlı ve kalıcı hale getirir [25]. Bu süreç PoW olarak adlandırılır (Bölüm 2.5.3 açıklandı), büyük bir hesaplama gücü gerektirir. PoW sayesinde blokzincir izlenebilir.

2.4.4. Blokzincir Değişmezliği

Blokzincir uygulamasındaki değişmezlik, kavramsal olarak blokzincirin değişmez ve silinmez kalması için bir blokzincir defterinin değişmeden kalma yeteneği olarak tanımlanan temel blokzincir özelliklerinden biridir. Blokzincir uygulamasındaki işlemin detaylarında her bilgi bloğu, bir şifreleme (simetrik ve asimetrik algoritmalar) ilkesi, bir karma değer ve zaman damgası kullanarak optimize eder. Kullanılan karma değer, uygulamadaki her blok tarafından ayrı olarak oluşturulan sayısal verilerden oluşur. Ağdaki blokların her biri karma değeri veya dijital imzayı sadece kendisi için değil, kendinden önceki blok için de içerir [70].

Bloğun tüm işlemlerinde Merkle ağaç yapısı kullanılır. Bir Merkle ağacı, Merkle kökü adı verilen tek bir karma olana kadar işlem çiftlerinin özyinelemeli olarak karmalanmasıyla oluşturulan bir veri yapısıdır. Merkle ağaç yapısı Bölüm 2.3.2 açıklandı. Bitcoin'deki Merkle ağacı, kriptografik karma algoritması, Güvenli Karma Algoritması (Secure Hash Algorithm-SHA256)[9] olarak da bilinen SHA256[10]'nın iki kez uygulanmasıdır. Bu, blokların geriye dönük olarak birbirine bağlanmasını ve değişmez olmasını sağlar. Blokzincir uygulamasının bu özelliği ile sisteme kimsenin izinsiz bir şekilde girmemesini, bloğa kaydedilen verileri değiştirmemesini ve bozulmamasını sağlar. Blokzincir uygulamasında verilerin kopyasını bulunduran düğümlerin fikir birliğine varması âdem-i merkeziyetçiliği ve dağıtılmış olması açısından önemlidir. Bu uzlaşma diğer bir deyişle fikir birliği, blokzincir uygulamasındaki verilerin orijinal halinin korunmasını sağlar. Değişmezlik ve silinememe blokzincir uygulamasının kesin özelliklerindendir. Böylece, veri denetleme, yönetme ve yetkilendirme açısından veriler daha çok verimli ve güvenli olur.

Bir blokzincirin sahip olduğu blok ne kadar uzun olursa, veri kurcalama saldırılarına karşı o kadar dirençli olur, çünkü bir rakip blokzincirin herhangi bir yerindeki verileri değiştirirse sonraki bloktaki karma işaretçinin yanlış olmasına neden olur. Bu nedenle

[9] SHA olarak da bilinen Güvenli Karma Algoritmalar, verileri güvende tutmak için tasarlanmış bir şifreleme işlevleri ailesidir. Bir karma işlevi kullanarak verileri dönüştürerek çalışır: bit düzeyinde işlemler, modüler eklemeler ve sıkıştırma işlevlerinden oluşan bir algoritma.

[10] SHA256, dijital bilgileri korumanın en güvenli yollarından biri olarak tanımlanır. SHA256, herhangi bir girdiden 256 bit (64 karakter uzunluğunda) rastgele harf ve sayı dizisi üreten bir matematiksel işlemdir.

blokzincir ağında düzgün bir şekilde konuşlandırılan veriler asla değiştirilemez, kaldırılamaz ve silinemez. Blokzincir ağında şimdilik depolanmış olan verilerle oynanması mümkün olmasa da ağa veriler eklenebilir. Bu nedenle, blokzincir uygulamaları yalnızca ekleme, kurcalamaya dayanıklı ve değişmez veri yapıları olarak bilinir. Bir işlem blokzincir ağına dâhil edildikten sonra işlemleri silmek, güncellemek veya geri almak neredeyse imkânsızdır. Ancak, düğüm sayısının sınırlı olan izin tabanlı blokzincir uygulamalarında, konsorsiyumun düğümlerin çoğunluğunun kendi gerçek versiyonlarına oy verme ve her zaman bir olasılık olduğundan, blokzincir verileri kurcalamak imkânsız değildir. Bu nedenle, halka açık blokzincir uygulamalarında uzun bir blokzincirin varlığı, blokların karma tabanlı bütünlüğünü değiştirmenin son derece yüksek maliyeti nedeniyle blokzincirin derin geçmişini değişmez kılıyor olsa da özel blokzincir uygulamalarında değişmezliği sağlamak çoğunluk olduğu sürece çok daha ucuz ve daha güçlüdür.

2.4.4.1. Blokzincir Değişmezliğinin Zorlukları

- **%51 saldırı,** bu mekanizma için çok sayıda zorluk vardır. Yüzde 51 saldırı, bir saldırganın ağın diğer tüm üyeleri üzerinde büyük bir bilgi işlem gücü elde edebileceğini gösterir. Tek bir varlığın sorumlu olmadığı merkezi olmayan bir ağın şeklidir. Günümüzde madencilik pazarlarındaki artış ve madencilik kapasitesinin kiralanabilir olması nedeniyle insanların böyle bir saldırıyı kolayca gerçekleştirebilir. Saldırıyı yapacak kişiler ilk olarak "değişmez" verileri değiştirmeyi amaçlar.
- **Kuantum hesaplama,** bu alandaki bir diğer büyük zorluk, blokzincir değişmezlik özelliğini tehdit eden kuantum hesaplamadır. Uzmanlar tarafından kuantum hesaplamanın sistemin güvenliğini kırmak için kişinin özel anahtarına erişebilen blokzincir ağının genel anahtarı tersine mühendislikle alma yeteneğine sahip olabileceğini iddia ediliyor. Bu durum, blokzincir uygulamasındaki işlemlerin neredeyse % 50'sini etkileyebilen güvenlik için bir tehdit olduğunu söyleyebiliriz.

Çözüm; uzmanlar, "yüzde 51 saldırısının" daha güçlü bir protokol oluşturarak ve devredilen hisse ispatı veya sadece hisse ispatı algoritması gibi bir konsensüs algoritması kullanılarak üstesinden gelinebileceği öne sürülüyor. Böyle bir tehditte bu

gibi çözüm önerilerin güvenilir olduğunu söylemek oldukça zordur. Gelecekte kuantum ile oluşturulan blokzincir sistemi, geçmiş verileri daha güvenli bir şekilde kayıt altına alabilecektir.

2.4.5. Ölçeklenebilirlik

Blokzincir teknolojisinin ölçeklenebilirlik sorunları üç kategoride sınıflandırılabilir: Bunlar, verim, maliyet ve kapasite. Birçok blokzincir uygulamasında blok boyutu sınırı aşması nedeniyle yapılan işlemlerin bloğa eklemede bekleme sorunu yaşanıyor. Ayrıca blok oluşturma süresi kısaysa birçok çatal üretilir (Bölüm 2.5.1.1'de açıklandı), bu nedenle blok oluşturma süresi yapay olarak azaltılamaz. Bu nedenlerden dolayı verim sınırlıdır. Bir işlem oluşturulduktan sonra kullanıcının işlem ücretini ödemesi gerekir, bu da mikro ödemeler gibi hafif işlemler olarak ücretlendirilir. Yapılan işlemlerin hepsi sadece zincirde depolanırsa kapasite zincirini sürdürmek için büyük olur, bu da ölçeklendirme sorununa neden olur [28].

Ölçeklenebilirlik sorununu çözmek için yöntemleri beş kategoriye ayırmış: Bunlar, zincir içi ve dışı, yan ve alt zincir ve zincirler arası çözümlerdir [28].

- **Zincir dışı** yaklaşımındaki amaç; işlemler blokzincir ağının dışında yapılarak ölçeklenebilirliği iyileştirmektir. Bu çözüm, ana zincir durumunu korur. Avantajı ise işlem maliyetini ve ana zincir üzerindeki yükü azaltarak bekleme süresini minimuma indirir. Ancak işlem ücreti ortadan kalktıkça reşit olmayanların karları düşebiliyor, dolayısıyla ekosistemleri değişebiliyor.
- **Yan zincir**, farklı olan blokzincir uygulamaların varlıklarını aralarında değiştirmektir. Ve amaçları, başka bir blokzincirin işlevini mevcut blokzincir uygulamasına getirmektir. Bu da, blokzincir uygulamaların birlikte çalışabilirliğini sağlar. Böylece, bir blokzincir uygulamasındaki bir işlem başka bir blokzincir uygulamasında kullanılabilir.
- **Çocuk zincir,** alt zincirde yapılan tüm işlemleri yapar ve üst zincire kaydeder. Alt zincir, normal bir blokzincir gibi davranır ve burada yapılan tüm işlemler, ana zincirde Merkle kök karması (hash) gibi kaydedilir. Ana zincirdeki blok doğrulaması ile akıllı sözleşmedeki saldırganlık kanıtı yapılır, yapılan doğrulamaya isteğe bağlı olarak herkes katılabilir. Alt zincirin Merkle kök

karması üst zincire taşınır ve alt zincir özelliklerine göre bölünerek üst zincirde işlenebilir.

- **Zincirler arası**, bazı blokzincir platformların arasında senkronizasyon sağlamanın bir diğer yoludur. Yan zincir önerisine benzer, yan zincir uygulanmasının altyapı teknolojisi olduğunu söyleyebiliriz. Avantajı ise diğer blokzincir uygulamalarını bir araya getirebilmesi ve aralarında veri alışverişi yapabilmesidir. Dezavantajı ise her iki blokzincirin de PoW tabanlı aynı algoritmayı kullanması gerektiği ve taraflar arasında bir kişinin tembel olması durumunda son kullanma tarihine neredeyse ulaşıldığında değişimin tamamlanabilmesidir.
- **Zincir içi,** çözümün en temel örneklerinden biri büyük bloktur. Bu yöntemin avantajı, iletim sınırının daha yüksek olması ve iletim maliyetinin geleneksel yola göre daha düşük olmasıdır. Dezavantajı ise blok büyüdükçe yayılma hızının azalması ve çatallaşmanın belli aralıklarla daha fazla meydana gelmesidir. Bundan dolayı, blok boyutu ile ilgili işlemler ölçeklenebilirlik için uygun bir yaklaşım değildir.

2.4.6. Anonimlik

Bir blokzincirde, üyelerin kimliğinin ve aralarındaki işlemlerin anonim kalması zorunludur. Ancak, anonimlik mekanizması, blokzincir güncellemesi için gerekli olan işlemin doğrulanmasını engellememeli, gerçek dünyadaki bir kullanıcının kimliğini gizlenmesi anonimlik gereksinimini karşılamamaktadır. Blokzincirde güçlü bir anonimlik kavramı tanımlamaya ihtiyaç vardır. Blokzincir tabanlı bir sistem, blokzincir güncellemesi için gerekli olan herhangi bir potansiyel madenci tarafından doğrulamaya izin verirken kimlik gizliliğini ve işlemsel gizliliği elde ederse anonimliği korur [69].

2.4.7. Denetlenebilirlik

Bitcoin blokzincir uygulaması, Harcanmayan İşlem Çıktısı (Unspent Transaction Output-UTXO)[11] modeline dayalı olarak kullanıcı bakiyeleri hakkındaki verileri depolar [24]. Herhangi bir işlem, önceden harcanmamış bazı işlemlere atıfta bulunmak zorundadır. Mevcut işlem blokzincir ağına kaydedildiğinde yönlendirilen bu harcanmamış işlemlerin durumu harcanmamıştan harcanmışa geçer. İşlemler kolayca doğrulanabilir ve izlenebilir [69].

2.5. Konsensüs Protokolleri

Kriptografik şifreleme ve P2P teknolojisine ek olarak uzlaşma protokolleri de blokzincir siteminin önemli bir özelliğidir. Başarılı bir fikir birliği protokolü, blokzincir ağının hata durumunu ve güvenlik garantisini verebilir. Blokzincir merkezi olmayan bir yapıda olduğundan veri tabanına hangi verilerin eklenip eklenmeyeceğine karar veren bir aktör veya yönetici yoktur. Bunun yerine, düğümler, kayıtlarına bir işlem eklemeye veya reddetmeye karar vermek için kullanabilecekleri bir dizi anlaşmaya ihtiyaç duyar. Bu anlaşmalar dizisi, bir fikir birliği mekanizması olarak da bilinir. Blokzincir yalnızca düğümlerin çoğu (%51) tarafından kabul edildiğinde güncellenir, bu durumda fikir birliğine varmış olurlar. Bu, kişisel verinin korunmasıyla ile ilgili önemli bir süreçtir. Dağıtılmış sistemlerde mükemmel bir konsensüs protokolü yoktur. Mutabakat protokolünün tutarlılık, kullanılabilirlik ve hata toleransı arasında bir dengenin kurulması gerekir [29]. Ayrıca, konsensüs protokolünün, konsensüs sürecini kasıtlı olarak baltalayan bazı kötü niyetli düğümler olacağı için bizans generalleri probleminin (Bölüm 2.5.2 açıklandı) de ele alınması gerekir [30].

2.5.1. Blokzincirin Fikir Birliğine Varmasının Önemi

Farklı amaçlarda kullanılan binlerce blokzincir uygulaması vardır. Bununla birlikte, hepsinin tek ortak bir noktası vardır, doğru kayıtlar tutup verileri korumak. Bir bankanın aksine, blokzincir uygulamaların kayıtları güncel tutmakla görevli herhangi bir merkezi otorite yoktur. Başvurulacak hiçbir yönetici, operatör, kurum veya kuruluş yoktur. Ağın

[11] Harcanmamış bir işlem çıktısı (UTXO), yeni bir işlemde girdi olarak kullanılabilecek bir işlem çıktısını ifade eder. Özünde, UTXO'lar her blokzincir işleminin nerede başladığını ve bittiğini tanımlar. Bu model, Bitcoin ve diğer birçok kripto para biriminin temel bir unsurudur.

mevcut durumu hakkında bir anlaşmaya varma sürecini ağdaki düğümler yönetiyor. Bunlar blokzincirin tam bir kaydını tutan düğüm olarak adlandırılan bilgisayarlardır. Pratik olarak herkes bir düğüm başlatabilir, istenirse çok kısa bir sürede herhangi bir kullanıcı da bir düğüm başlatabilir. Bu durumda, ağın güvenliği için her işlemi manuel olarak gözden geçirmek gerekmez. Bu süreç, doğrudan yazılım tarafından tanımlanmış bir dizi kural tanımlanarak gerçekleştirilir.

Önemli veriler ve kullanıcı bakiyeleri söz konusu olduğunda, blokzincir platformun hatasız kalması ve yalnızca gerçek işlemleri kaydetmesi oldukça önemlidir. Bu nedenle, düğümlerin çelişkili bilgileri kaydetmesini önlemek için blokzincir uygulamasını güncellenmeden önce mevcut durum hakkında bir anlaşmaya varılır. Bu, bir oylama süreci olarak da düşünülebilir. Düğümlerin yarısından fazlası (en az %51) bir işlemi dâhil etmek için oy kullanırsa işlem blokzincir ağına eklenecektir, yoksa çöp olur. Fikir birliğini korumaya dâhil olan kullanıcılar, kötü niyetli davranmalarını önlemek için bir şeyleri tehlikeye atmalıdır, çünkü yakalandıklarında hisselerini kaybederler. Diğer taraftan, dürüst davranmak için genellikle bazı teşvikler vardır. Sadece birkaç kişi tarafından güvence altına alınan bir sistem, gizli anlaşma yoluyla kolayca bozulabilir, ancak potansiyel olarak on binlerce insan söz konusu olduğunda bu pek mümkün değildir. Bugün birçok fikir birliği mekanizması mevcuttur. Bununla birlikte, bilinen birkaç yaygın blokzincir konsensüs mekanizması vardır. Bilinen bazı konsensüs algoritmalar;

- Hisse Kanıtı (Proof of Stake-PoS),
- İş Kanıtı (Proof of Work-PoW),
- Kullanılabilir İş İspatı (Reusable Proofs of Work-RPoW),
- Yetkilendirilmiş Hisse İspatı (Delegated Proof of Stake-DPoS),
- Ripple[12]
- Tendermint[13] [31].

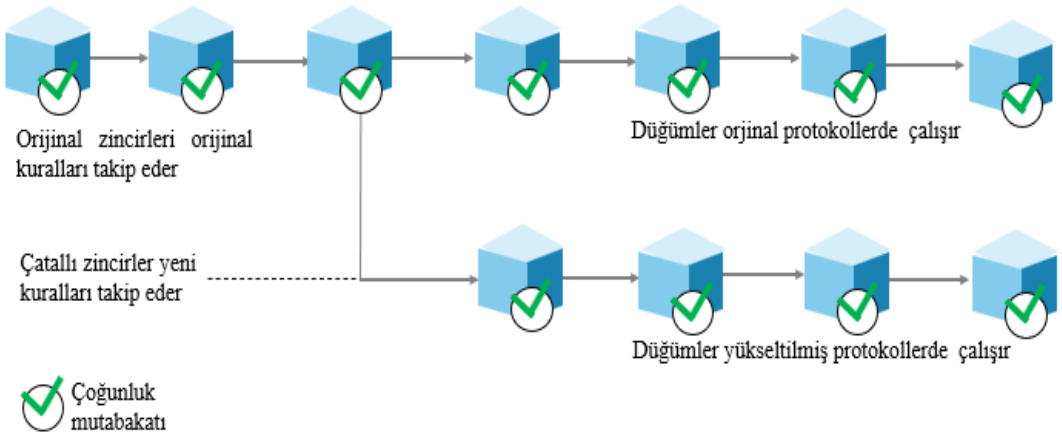
[12] Ripple, bankaların hızlı küresel finansal anlaşmalar yapmasına yardımcı olmak için blokzinciri teknolojisini kullanan bir ödeme protokolü, kripto para yaratıcısı ve yüksek teknoloji ödeme firmasıdır. Ripple, blokzincir teknolojisini kullanarak güvenlik, güvenilirlik ve doğrulanabilirlik sunar.

Sayısız mutabakat mekanizması arasındaki temel fark, birden fazla işlemin kimlik doğrulamasını nasıl hesapladıkları ve ödedikleri belirlenebilir.

2.5.1.1. Çatal (Fork)

Bu yöntemle sıfırdan başlamak yerine mevcut blokzincir uygulamasında değişiklikler yapılır. Ağ çatallaşırken blokzincirin iki modeli oluşturulur. Fikir birliği ağındaki zincirin aynı yerinde iki bloğu da onaylanabilir. Blokzincir ağının bir parçası çatallardan herhangi birini işleyerek blok ekleme işlemine devam edebilir, çatallaşan diğer parçası için de başka çatal kullanılır. Ağdaki her bir bloğun karma yapıları farklılık göstereceğinden zincirler arasında uyumsuzluk oluşur, bundan dolayı ağın hangi çatalla işlem yapacağı konusunda fikir birliğine varılması gerekir.

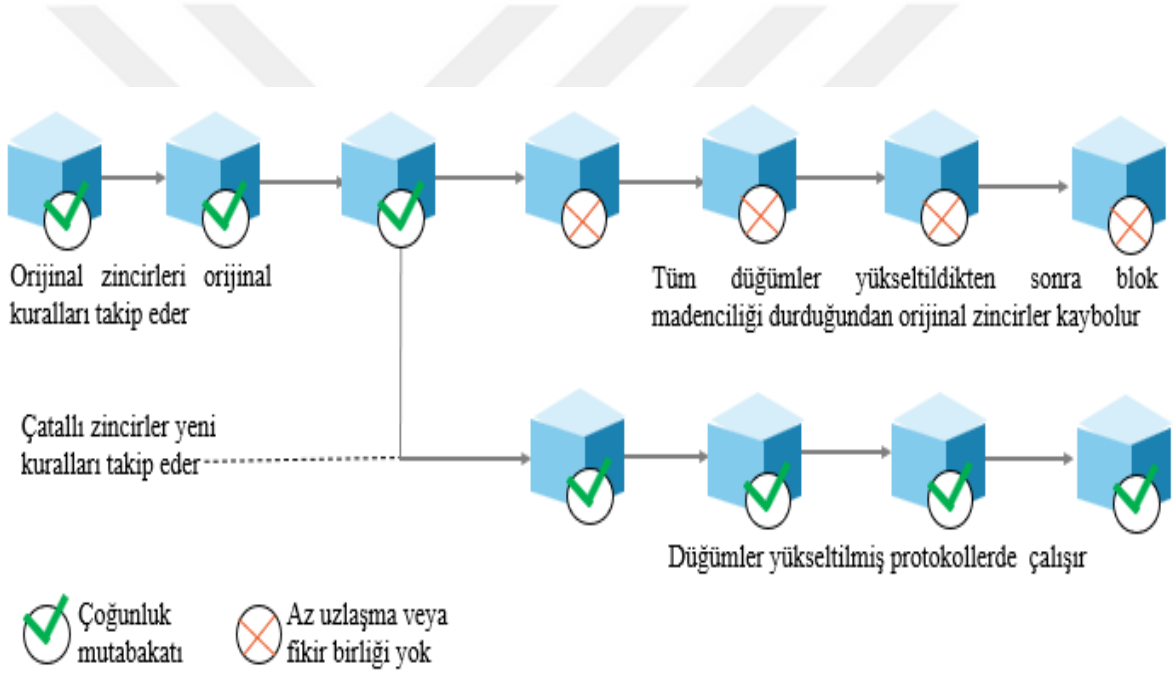
- **Sert çatal**, ağda bulunan her bir kullanıcının mevcut yazılım ve donanımın son sürümüne yüklemesini ve güncellemesini gerektirir. Bu durumda yazılımda köklü ve nitelikli bir iyileştirme yapılır. Ayrıca, önceki sürümün düğümlerinde çalışan uygulama ya da yazılım artık sürüm güncellendiği için kabul edilmeyecektir. Diğer bir deyişle güncel sürüm oybirliği ile kabul edilmemişse aynı yazılımın başka bir versiyonunu kullanarak Şekil 2.8'de gösterildiği gibi iki blokzincir şeklinde çatallaşabilir.



Şekil 2. 8 Sert Çatalın (Fork) Çalışma Mekanizması. [32]

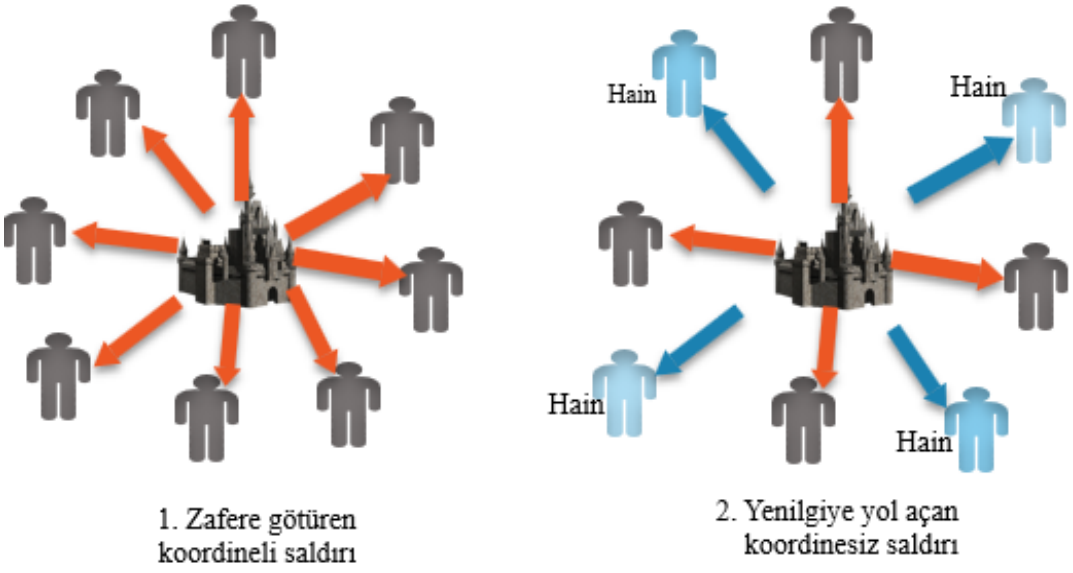
[13] Tendermint Core adı verilen konsensüs protokolüdür, aynı işlemlerin tüm makinede aynı sırayla kaydedilmesini sağlar. Blokzincir uygulama arayüzü kullanarak işlemlerin herhangi bir programlama dilinde işlenmesini sağlar.

- **Yumuşak çatal**, Yumuşak çatal geriye dönük doğrulanabilir. Yükseltilmiş blokzincir uygulaması, işlemlerin doğrulanmasından sorumludur (bkz: Şekil 2.9). Ancak güncellenmeyen düğümlerin yeni blokları geçerli olmaya devam edecektir. Bu sadece tek yönlü çalışır, yükseltilmiş blokzincir uygulaması, güncellenmemiş düğümleri tanımayacaktır. Yumuşak çatalın doğru bir şekilde çalışması için kullanıcıların çoğu uzlaşarak yükseltme yapmalıdır. Ağdaki güncel kural ve işlemler ne kadar çok madenci tarafından kabul edilirse ağın güvenirliliği ve doğrululuğu çatallaşmadan sonra o kadar yüksek olur. Yumuşak çatal modeli, Bitcoin ve Ethereum gibi blokzincir uygulamalarda yaygın olarak kullanılmaktadır.



Şekil 2. 9 Yumuşak Çatalın (Fork) Çalışma Mekanizması. [32]

2.5.2. Bizans Generalleri Problemi



Şekil 2. 10 Bizans Generallerinin Sorunu. [33]

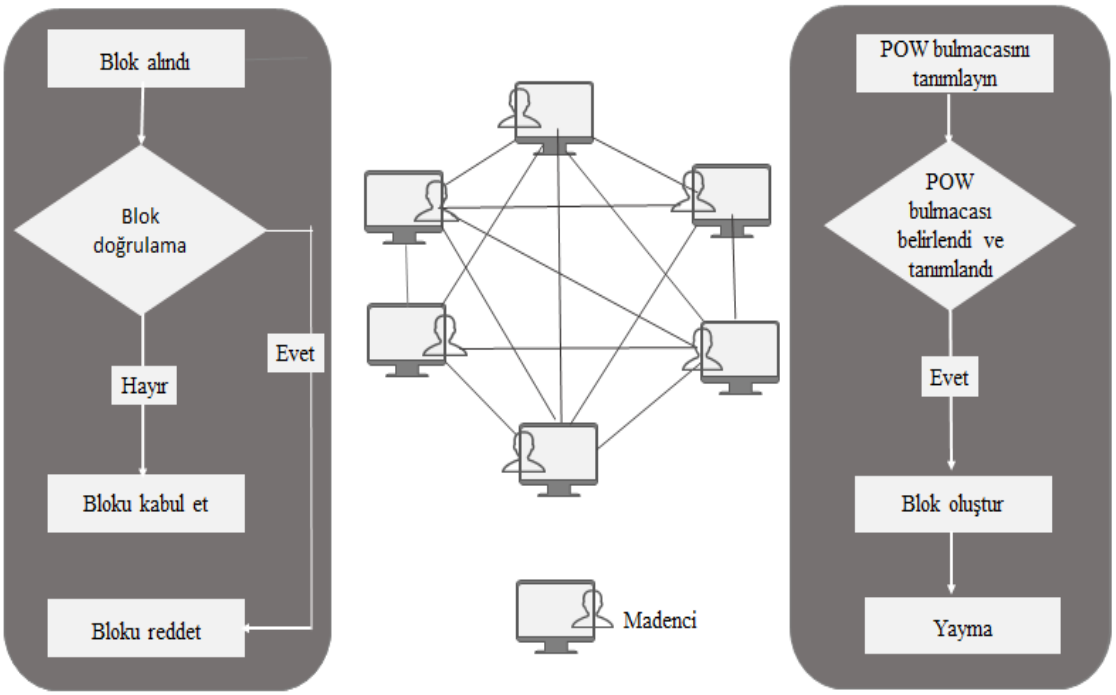
Bizans generallerinin sorunu şu şekilde açıklanabilir: Generaller, istedikleri kuşatılmış bir şehrin dışında konumlandırıp saldırı zamanını seçerler. Şekil 2.10'de gösterildiği gibi en az yarısı aynı anda saldırıda bulunurlarsa galip gelebileceklerini biliyorlar. Ancak saldırı zamanını iyi koordine etmezlerse savaşı kaybederler. Ayrıca bazı generallerin sadakatsiz olduğundan şüphelenildiği için saldırının zamanıyla ilgili sahte mesajlar gönderilir. Generaller birbirleriyle yalnızca at sırtındaki haberciler aracılığıyla iletişim kurabildiklerinden bir mesajın gerçekliğini doğrulamanın hiçbir yolu yoktur. Bu koşullarda saldırının zamanlaması konusunda iyi bir fikir birliğine varmaları gerekir.

Bitcoin'den önce bu sorunun çözülmesinin imkânsız olduğu düşünülüyordu. Bilgisayar bilimcileri 1982'de generallerin sorununun bir "komutan ve teğmen" sorununa indirgenebileceğini ve tüm teğmenlerin sadık oldukları sürece komutanın emirlerine göre hareket etmek zorunda olduklarını açıkladılar. Sorunun ancak generallerin üçte ikisinden fazlasının sadık olması durumunda çözüme kavuşabileceğini gösterdiler [33]. Bu durumda anlaşmazlık geçici olarak kabul edilir ve çelişen görüşlerin çözümü oy çokluğu ile belirlenir. Bu, merkezi bir kontrolör olmadan daha önce mümkün olmayan uygulamaları merkezi olmayan bir şekilde oluşturmayı mümkün kılar. Bitcoin uygulamasının sunduğu çözüm ise şu şekildedir: Herhangi bir zamanda herhangi bir general bir saldırı zamanını belirleyebilir. İlk duyulan saldırı süresi resmi plan olarak

kabul edilir. Ancak, bir mesajın iletilmesi hemen gerçekleşmez, bu nedenle farklı generaller önce farklı planları duyabilir. Bu nedenle, bir general bir plan yaptığında bu plana dayalı olarak zor bir matematik problemini çözmelidir. İçlerinden biri, bir çözüm bulur bulmaz onu plana ekler ve yeni bir plan oluşturur. Yeni planı diğer generallere gönderir. Bundan sonra, bunu duyan herkes, yine birkaç dakika sürmesi gereken bu yeni resmi planı genişletmeye başlar. Her general, o zamana kadar duyduğu en uzun ömürlü çözümü uzatmak için bildiği en sık genişletilmiş plan üzerinde çalışır. Bir çözüm birden çok kez genişletildikten sonra, en uzun hesaplama zincirinde bulunan saldırı süresi gerçek saldırı süresi olarak kabul edilir. Bu en uzun blokzincirin salt varlığı generallerin çoğunluğunun en az %51 yaratılmasına dâhil olduğunun kanıtıdır. Bilgi işlem gücünün yarısından daha azına sahip hiçbir saldırgan aynı süre içinde benzer uzunlukta başka bir zincir üretemez.

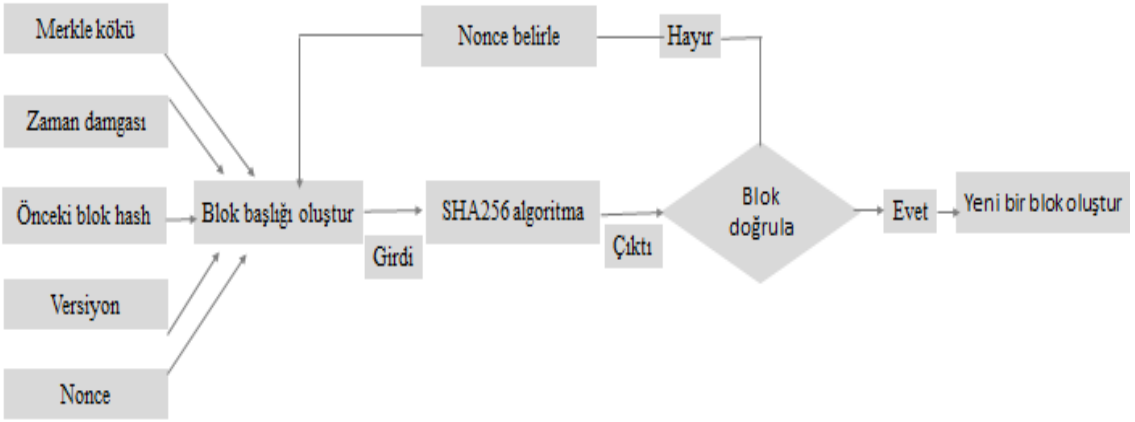
Bizans Generalleri Problemi genellikle dağıtık yapıdaki mimarilerde görülen bir problemdir. Ağdaki veri kümeleri, aralarındaki anlaşma ile farklı düğümler arasında kullanılabilir. Bu ortak kullanım, ağdaki düğümlere saldırı yapılabilir ve bu da yapılan anlaşma içeriğinin değişmesine diğer bir deyişle bozulmasına sebep olabilir. Normal düğümlerin kurcalanmış bilgileri ayırt etmesi ve diğer normal düğümlerle tutarlı sonuçlar elde etmesi gerekir. Konsensüs algoritması, dağıtık sistemde uzun yıllardır çalışmaktadır. Blokzincir teknolojisinde PoW, PoS ve DPoS gibi önemli konsensüs algoritmaları kullanılmaktadır.

2.5.3. İş Kanıtı (PoW)



Şekil 2. 11 Blokzincirde PoW Çalışma Mekanizması. [34]

PoW ilk olarak kullanılan popüler fikir birliği protokolüdür, birçok blokzincir tabanlı sistemde yaygın olarak kullanılmaktadır. Kullanıcıların, blokzincir ağına katılmaları, kayıt defterine yeni bir blok eklemeye hak kazanmaları ve yeterlilik kazanmaları için yapılan iş kanıtlanmalıdır. PoW, bir hizmet talebinde bulunan kişinin bir ağa katılmak için bir kriptografik bulmacayı çözmesi olarak da tanımlanabilir. Başlangıçta hizmet reddi önlemine karşı hashcash önerilmiştir [35]. Blokzincirde ve özellikle Bitcoin'de yeni veri blokları için uygun başlığı bulmak ve bunları blozincir ağına eklemek için doğrulama teknikleri olarak da kullanılır. Bir blok eklemek için, bir düğümün bir maliyet fonksiyonunu çözmesi gerekir, bu da belirli kısıtlamalarla önceden tanımlanmış bir karma formatla sonuçlanır.



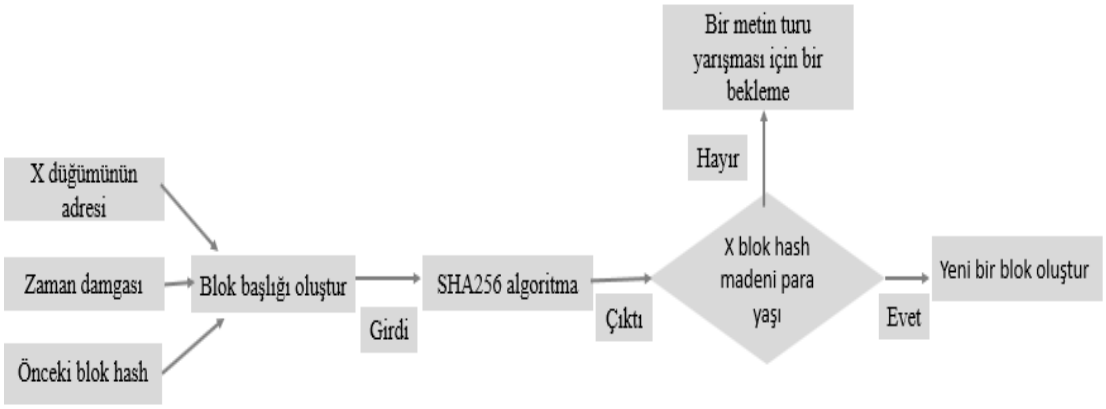
Şekil 2. 12 Blokzincirde PoW Akış Diyagramı. [29]

Blokzincir ağında, düğümlerin fikir birliğine varması ve madenci tarafından sağlanan blok karmasının geçerli bir PoW olduğunu kabul etmesi beklenir. (bkz: Şekil 2.11 ve Şekil 2.12). Bu mekanizmada, her madencinin öncelikle blokzincirde bir PoW bulmacası tanımlaması gerekir. Oluşturulan bulmaca, sistemde yer alan diğer tüm düğümler tarafından görülebilir ve erişilebilir olacaktır. Sadece PoW bulmacasını çözebilen düğüm, blokzincir ağındaki verileri tutma, erişme ve değiştirebilme yetkisine sahip olur. PoW kullanımında her konsensüs protokol evresinde yeni bir blok yaratmak için yeni bir düğüm seçer. İşleme katılan düğümlerin sisteme dâhil olması için bir kriptografik bulmacayı doğru bir şekilde çözmeleri gerekiyor. İlgili bulmacaya önce başlayan düğüm, yeni bir blok oluşturma yetkisine sahip olur. PoW'da blok oluşturma ve yapılan işlemlerin akışı Şekil 2.12'de gösterilmiştir.

Bir PoW'un kriptografik bulmacasını çözmek kolay değil. Ağdaki düğümlerden doğru dönüşü alabilmek için "nonce[14]" değerinin ayarlanması gerekir, bu da yapılan işlemler için fazlaca hesaplama gücünü gerektirir. Kötü niyetli bir kişinin zincirdeki bir bloğu bozması mümkündür, ancak ağdaki geçerli blok sayısı arttıkça iş yükü de artar, bu da ağdaki uzun bir zinciri yok etmek ya da bozmak için daha çok hesaplama gücünü gerektirir.

[14] Nonce, "yalnızca bir kez kullanılan sayı"nın kısaltmasıdır ve kripto para madenciliği bağlamında, yeniden düzenlendiğinde zorluk seviyesi kısıtlamalarını karşılayan bir blokzincir ağındaki karma bir bloğa eklenen bir sayıdır.

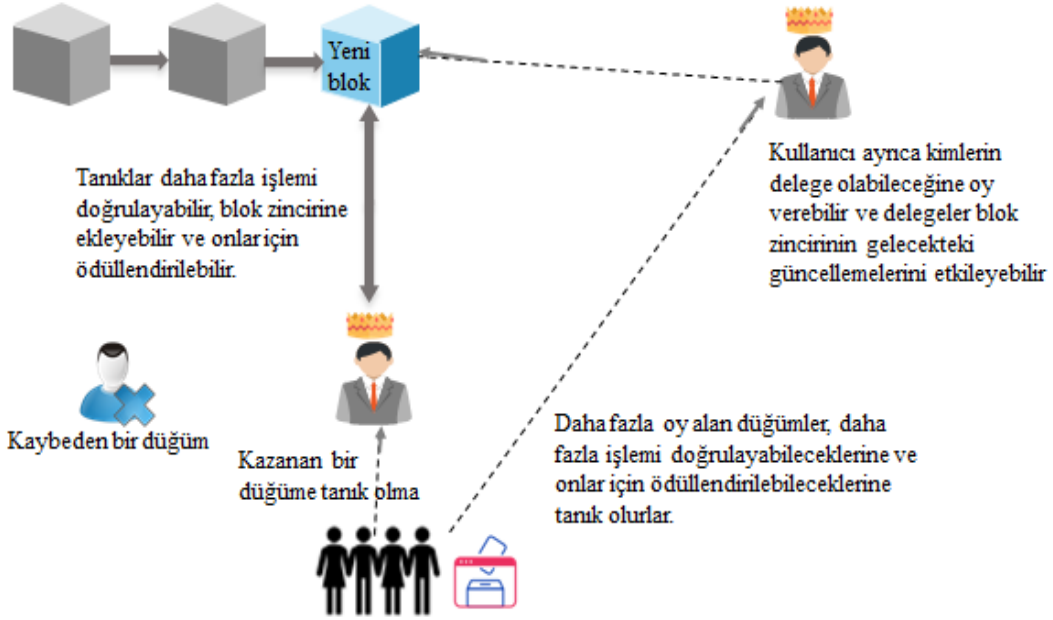
2.5.4. Hisse Kanıtı (PoS)



Şekil 2. 13 Blokzincirde PoS Akış Diyagramı. [29]

PoS, bir sonraki bloğu oluşturan düğümün seçildiği blokzincir ağına blokları doğrulamak ve eklemek için son zamanlarda kullanılan yaygın bir yöntemdir [36]. Ağda bulunan bir düğüm, sistemde ne kadar çok paya sahipse o kadar çok blokları ekleme ve doğrulama yetkisine sahip olur. Bu durum, sistemdeki aktörlerin daha dürüst olmalarını sağlar, aksi durumda yanlış davranışlarda bulunurlarsa sahip oldukları hisseleri de kaybederler. PoS yönteminde, yeni blok oluşturma işlemi hesaplama gücünden çok sahip olunan hisseye bağlıdır. Sistemdeki tüm düğümlerin kriptografik bulmacayı çözmesi gerekir. PoW'den farkı, ağdaki düğümlerin çok kez “nonce” ayarlamasına ihtiyaç duymamasıdır, bu bulmacayı çözmenin yolu sahip olunan hissedir. Bu nedenle PoS, fikir birliğine varmak için çok fazla hesaplama gücü tüketmek yerine dâhili para teşvikinin bir yolunu kullanan, enerji tasarrufu sağlayan bir fikir birliği protokolüdür. PoS'un akışı Şekil 2.13’te gösterilmektedir. PoS da PoW gibi olasılıksal kesinlik konsensüs protokolüdür.

2.5.5. Yetkilendirilmiş Hisse İspatı (DPoS)



Şekil 2. 14 Blokzincirde DPoS Akış Diyagramı. [37]

DPoS, pay sahibi olan düğümlerin blok doğrulayıcıları seçmesine izin vermektedir [38]. Kullanıcılarının bir sonraki bloğu onaylamak için oy kullandığı ve delegeler seçtiği PoS konseptinin popüler bir evrimidir (bkz: Şekil 2.14). Delegeler, oylama gücü doğrudan sahip oldukları jeton sayısına bağlı olan jeton sahipleri tarafından oylanır. Bu oylama şekli, paydaşların kendileri blok oluşturmak yerine destekledikleri delegelere blok oluşturma hakkını vererek hesaplama güç tüketimini 0'a düşürmelerini sağlar. Delegeler sırayla blok oluşturamazlarsa görevden alınacaklar ve paydaşlar onları değiştirmek için yeni düğümler seçecektir. DPoS, fikir birliğine varmak için yeterli hisseye sahip olan kişilerin oylarından faydalanmanın demokratik bir yoludur. DPoS'u PoW ve PoS ile kıyaslarsak; daha maliyet olarak daha düşük ve verimi yüksek bir konsensüs protokolüdür. BitShares, EOS, vb. gibi DPoS'u benimseyen bazı kripto para birimleri de vardır [38].

3. BLOKZİNCİR GÜVENLİĞİ VE GÜVENLİK SORUNLARI

3.1. Blokzincir Katmanlarının Güvenlik Analizi

Tablo 3. 1 Blokzincir Katmanlarının Temel Yapısı. [39]

Programlanabilir Para Birimi	Programlanabilir Finansal	Programlanabilir Toplum
	Uygulama katmanı	
Script Kod	Algoritma& Mekanizması	Akıllı Sözleşme
	Sözleşme katmanı	
Para Birimi Sorunu Mekanizması	Para Birimi Dağıtım Mekanizması	
	Teşvik katmanı	
Pow (Proof-of Work)	PoS (Proof-of-Stake)	DPoS(Delegated Proof-of-Stake)
	Fikir birliği katmanı	
P2P Ağı	İletim Protokolü	Doğrulama Mekanizması
	Ağ katmanı	
Veri Blokları	Zincir Yapısı	Zaman Damgası
Hash Fonksiyonu	Merkle Ağacı	Asimetrik Şifreleme
	Veri katmanı	

Blokzincir sistemi Tablo 3.1'de gösterildiği gibi veri katmanı, ağ, fikir birliği, teşvik, sözleşme ve uygulama katmanlarından oluşur [40]. Veri katmanı, alt katmanın veri bloklarını ve ilgili asimetrik şifreleme ve zaman damgası teknolojilerini içerir. Ağdaki her bir katmanın güvenlik ve yapısı ile ilgili detaylı açıklamalar aşağıda verilmiştir.

3.1.1. Veri Katmanı

Veri katmanında, her düğümün karma işlevi, SHA, RSA[15], Merkle ağaç veri yapısı vb. kullanılır. İşlemler, belirli bir zamanda alınan zaman damgası ile yeni bir bloğa kapsüllenir.

[15] RSA şifreleme algoritması, birçok ürün ve hizmette yaygın olarak kullanılan asimetrik bir şifreleme algoritmasıdır. Asimetrik şifreleme, verileri şifrelemek ve şifresini çözmek için matematiksel olarak bağlantılı bir anahtar çifti kullanır.

3.1.2. Ağ Katmanı

Bu katman, dağıtılmış ağ, veri iletim işlemleri ve ağdaki verileri doğrulama işlemlerini yapar. Ağ katmanı, her bir düğümün veri doğrulamasını, iletimini ve yapılan işlemin kayıt sürecine dâhil olmasını sağlar. Bir blok eğer ağda bulunan düğümlerin çoğu tarafından doğrulanmazsa, doğruluğu kanıtlanamaz. Blokzincir uygulamasının bilgi aktarımı esas olarak P2P ağına bağlıdır. P2P ağı, birbirlerinin IP'sini açığa çıkarması gereken bilgi iletimi için yakındaki düğümlere dayanır. Blokzincir ağında kötü niyetli bir saldırgan olursa ağda bulunan diğer düğümlerde güvenlik açığının olması çok daha kolay olur. Halka açık blokzincir ağının düğümü herhangi bir bilgisayar ya da bulut sistemindeki sunucu olabilir.

3.1.3. Konsensüs Katmanı

Tablo 3. 2 Konsensüs Mekanizması Saldırı Yöntemleri ve Uygulama Kapsamı. [36]

Saldırı yöntemleri	PoW	PoS	DPoS
Rüşvet saldırısı	-	+	-
Uzun menzilli saldırısı	-	+	+
Madeni para yaşı biriktirme Saldırısı	-	+	+
Ön hesaplama saldırısı	-	+	-
Sibil saldırısı	+	+	+

Konsensüs katmanı esas olarak fikir birliğini kapsar. Konsensüs katmanı, blokzincir teknolojisini dağıtılmış ağı bile mantıklı ve güvenilir kılar. Konsensüs katmanı, blokzincir uygulamasının diğer (P2P) teknolojilerinden ayırt etme gücünü verir. Yaygın olarak kullanılan fikir birliği mekanizmaları; PoW, PoS ve DPoS. Ağda oluşan saldırılar arasında Rüşvet, Uzun Menzilli, Birikim, Ön Hesaplama ve Sybil saldırıları yer alır. Tablo 3.2'de konsensüs katmanı için saldırıların PoW, PoS ve DPoS açısından uygulama kapsamı gösterilmektedir.

3.1.4. Teşvik Katmanı

Teşvik katmanının amacı düğümleri blokzincir ağına katmak için çeşitli yönlendirmeler yapmaktır. Düğüm sayısının çok olması blokzincir uygulamasının güvenliğini artırır. Örneğin, Bitcoin teknolojinin güvenliği, ağdaki düğümlerin iş kanıtına ve karma (hash)

algoritmasının hesaplama gücüne dayanmaktadır. Blokzincir ağındaki bir düğümün herhangi bir işlemi doğrulama süreci, bilgi işlem kaynakları ve elektrik gücüne bağlıdır. Ağdaki düğümlere daha fazla katılım sağlamak için blokzincir teknolojisi çoğu zaman ağdaki kullanıcıları sanal para olarak ödüllendirir. Örneğin, Bitcoin, Litecoin ve Ethereum gibi birçok teknoloji bu mekanizmanın ürünleridir. Blokzincir teknolojisindeki projelerin bulmacalardan aldıkları ödülleri azaltmak yerine herhangi bir işlem yapmadan otomatik olarak ayarlamak için piyasa şartlarına uyumlu olması gerekiyor. Bir sonraki bloğu oluşturan Bitcoin madencilerini teşvik etmek için para birimi çıkarma ve para birimi dağıtım mekanizması dâhil ederek ekonomik faktörleri blokzincir çerçevesinde birleştirir. Esasen teşvik katmanı, farklı dağıtılmış düğümler arasında kitle kaynak kullanımı sorununu ele alır. Bu nedenle, tüm blokzincir sisteminin güvenliğinin gerçekleştirilebilmesi için bireylerin maksimum kârını garanti edecek verimli bir kitle kaynaklı mekanizma olmalıdır.

3.1.5. Sözleşme Katmanı

Bu kapmanda kullanılan kodlama dili ve algoritmalardan kaynaklanan önemli dosyaları, akıllı sözleşmeleri ve kullanılan algoritmaları bulundurur. Sözleşme katmanı, blokzincir uygulamasında esnek bilgisayar programı ve veri işlemlerin ön şartıdır. Akıllı sözleşme blokzincir sistemin bir parçasıdır, ayrıca kişinin müdahalesi olmadan çalıştırılabilen herhangi bir bilgisayar programından çok daha fazlasıdır.

3.1.6. Uygulama Katmanı

Bu katman, dijital para birimi mekanizmalarını içeren ve çok sayıda parasal fonları idare eden borsalar gibi merkezde bulunan ana düğümlerin güvenlik ile ilgili problemleri içerir. Düğümler, tüm blokzincir uygulamasının bozuk noktasındadır ve saldırı oranı yüksek maliyeti ise daha düşüktür, bu da kötü niyetli saldırganların öncelikli amacıdır. Borsa sunucusunun yetkisi alınıp anahtar bilgileri değiştirilirse saldırgan tarafından fon anahtarı çalınabilir, işlem miktarını değiştirebilir veya hassas bilgileri sızdırarak borsaya ekonomik ve itibar açısından yıkıcı darbeler verebilir.

3.2. Blokzincir Sınıflandırması

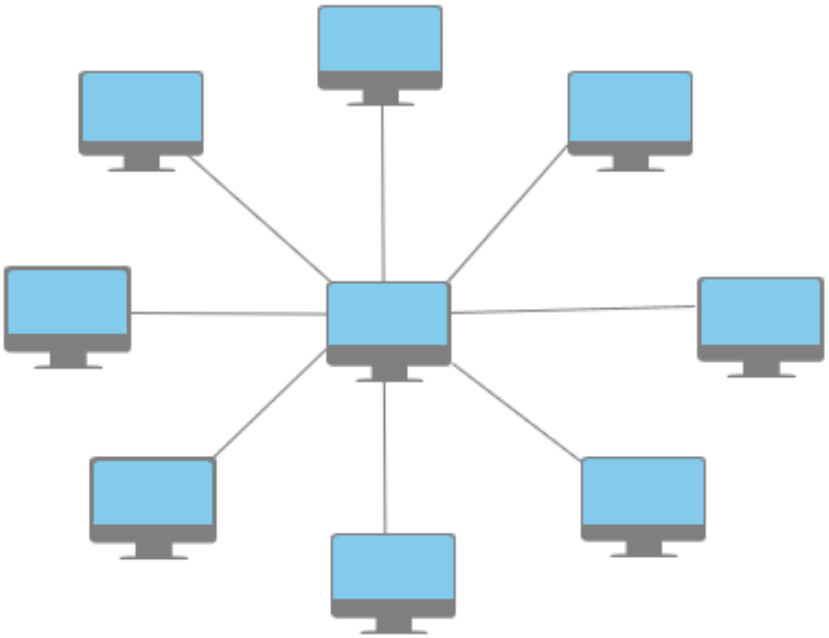
Tablo 3. 3 İzin Modeline Göre Segmentlere Ayrılmış Ana Blokzincir Türleri. [41]

	Tipi		Yazma	Okuma	İşlem	Örnek
Blokzincir Tipleri	• **Açık**	• İzinsiz genel	• Herkes	• Herkes	• Herkes	• Bitcoin, Ethereum
	• **Açık**	• İzinli genel	• Tüm yetkili katılımcılar	• Herkes	• Tüm yetkili katılımcılar	• Halk tarafından görüntülenebilen tedarik zinciri defteri
	• **Kapalı**	• İzinsiz özel	• Herkes	• Tüm yetkili katılımcılar	• Tüm yetkili katılımcılar	• Paylaşılan bir defteri çalıştıran birden çok banka
	• **Kapalı**	• İzinli özel	• Sadece ağ operatörü	• Tüm yetkili katılımcılar	• Sadece ağ operatörü	• Ana şirket yan kuruluşu arasında paylaşılan harici banka defteri

Blokzincir mimarisi, kullanıcılara, dağıtılmış deftere okuma/yazma gibi haklar verir. Okuma izni, genel veya özel erişim sunup sunmadığına ve yazma ise fikir birliği anlaşmaları için izinli/izinsiz erişimi desteklenip desteklenmediğine bağlıdır (bkz: Tablo 3.3). İzinli blokzincir teknolojisi, kişilerin düğüm yaratıldığında dağıtılmış deftere kimin yazma ve okuma yetkisinin olduğunu belirler. İzin verilen blokzincir uygulamalara farklı erişim özellikleri tahsis edilir. İzinsiz bir blokzincir uygulaması, herhangi bir kişinin kısıtlama olmaksızın zincire yazmasına izin verir.

Özel ve genel özellikler, blokzincir ağındaki kişilerin verileri okuma ve yazma yetkisini tanımlar. Mevcut mali hizmet uygulamalarında genel olarak özel veya genel izinli uygulamalar kullanılır. Teknolojinin benimsenmesi ve teknolojiye olan güvenin artmasıyla mali hizmetlerde izinsiz özniteliklerin kabul edilebilir olmasıyla iş durumlarının gelişmesi mümkündür [41]. Üç önemli farklı blokzincir mimarisi tanımlanabilir.

3.2.1. Genel Blokzincir



Şekil 3. 1 Genel Blokzincir Yapısı. [42]

Herkesin erişebileceği bir konsensüs blokzinciridir. Blokzincir topolojisinde herkes işlem gönderebilir ve onaylayabilir. Blokzincir uygulamaları "tamamen merkezi olmayan", verilerin açığa çıktığı Bitcoin blokzincir uygulaması gibi karakteristik olarak kabul edilip kullanılır. **Şekil 3.1**'de genel blokzincir modeli gösterilmektedir.

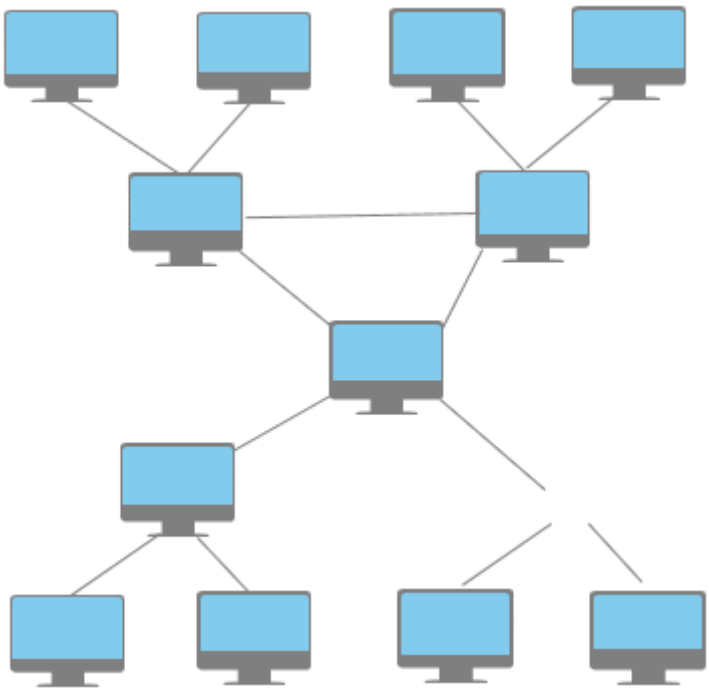
3.2.1.1. Genel İzinsiz Blokzincir

Adından da anlaşılacağı gibi, izinsiz bir blokzincir, herkesin ağın bir parçası olmasına ve bakımına katkıda bulunmasına izin veren bir tür blokzincir ağıdır. Başka bir deyişle, izinsiz blokzincir sistemi, halka açık, merkezi olmayan bir defterdir. Yapılan işlemler genellikle halka açık olduğu için şeffaftır ve kullanıcıların özel anahtarlar dışındaki tüm bilgilere erişmesine izin verir. Kullanıcılar ağdaki tüm işlemleri görüntüleyebilir. Blokzincir ağlarının kullanıcıları ağa güvenmeye teşvik etmesi gerektiğinden şeffaflık gereklidir. Ağda bulunan bazı kullanıcılar isimsiz veya sahte isimli olabilir. Bu da çoğu izinsiz blokzincir teknolojisinin bir adres oluştururken kullanıcılardan herhangi bir kişisel bilgi vermelerini istemez. İzinsiz bir blokzincir ile herhangi bir kullanıcı ağa düğüm ekleyebilir. Bitcoin de dahil olmak üzere kripto para gibi birimlerde faydalı olsa da gizlilik ile ilgili problemler sıkça yaşanmaktadır.

3.2.1.2. Genel İzinli Blokzincir

Sovrin Vakfı [43] tarafından tanıtılan bir kavramdır. Herkesin kullanımına açık olan, herkes tarafından okunabilen veya değiştirilebilen blokzincir örneklerini tanımlar. Bu tür bir blokzincir yalnızca seçilmiş bir grup katılımcılar deftere yazabilirler.

3.2.2. Özel Blokzincir



Şekil 3. 2 Özel Blokzincir Yapısı. [42]

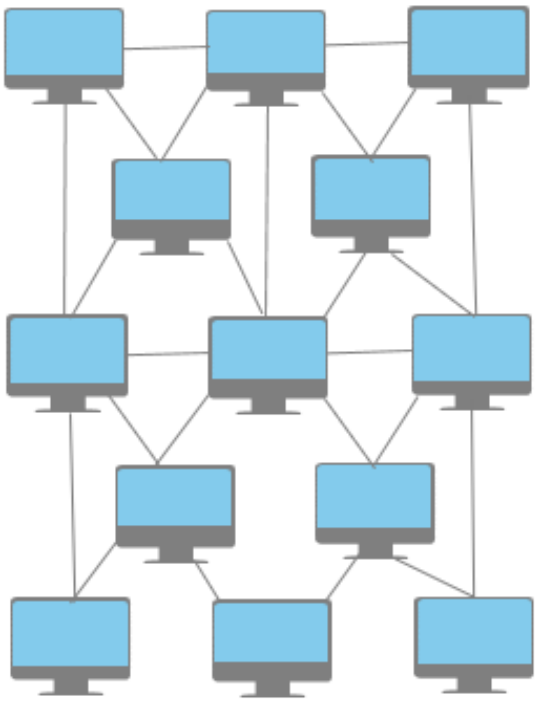
Yazma izninin tek bir kuruluşta olduğu bir blokzincirdir. Katılımcıların okuma izni genellikle halka açık veya belli bir aşamaya kadar kısıtlıdır. Bir şirket içinde, veri tabanı yönetimi, denetim vb. gibi ek seçenekler de vardır. Çoğu durumda, genel erişim gerekli değildir. Ağda bulunan katılımcıların bulunma biçimine göre blokzincirler halka açık (genel) blokzincir, konsorsiyum blokzincir ve özel blokzincir şeklinde gruplandırılır [44]. Özel blokzincir modeli **Şekil 3.2**'de gösterilmektedir.

3.2.2.1. Özel İzinli Blokzincir

Özel blokzincir uygulamaları olarak da bilinen özel izinli blokzincir uygulamaları farklı şekilde çalışır. İzin verilen blokzincir ağında, ağın bir parçası olmak için izne ihtiyaç vardır. Ağ sahibi, ilgili ağa kimlerin katılıp katılamayacağını belirler. Ağda bulunan kişiler, ağ ve dağıtılmış defter yapısında yapılacak işlemler için erişim izni almaları

gerekir. İzinli blokzincir uygulamaları, değişen derecelerde ademi merkeziyetçiliğe sahip olabilir. Ayrıca kısmen merkezi veya tamamen merkezi olabilir. Blokzincirin üyeleri, genellikle ağın sahip olması gereken ademi merkeziyetçilik düzeyine ve dağıtması gereken fikir birliği algoritmalarına karar verir. İzinsiz muadillerinin aksine, izinli blokzincir uygulamaların şeffaflık sağlaması gerekmez. Erişim kontrol mekanizması değişebilir ve mevcut katılımcılar gelecekteki katılımcılara karar verebilir; bir düzenleyici otorite katılım için lisans verebilir veya bunun yerine kararları bir konsorsiyum verebilir. Konsensüs, katılımcı paydaşlar arasındaki özel anlaşmalar sayesinde gerçekleştirilir

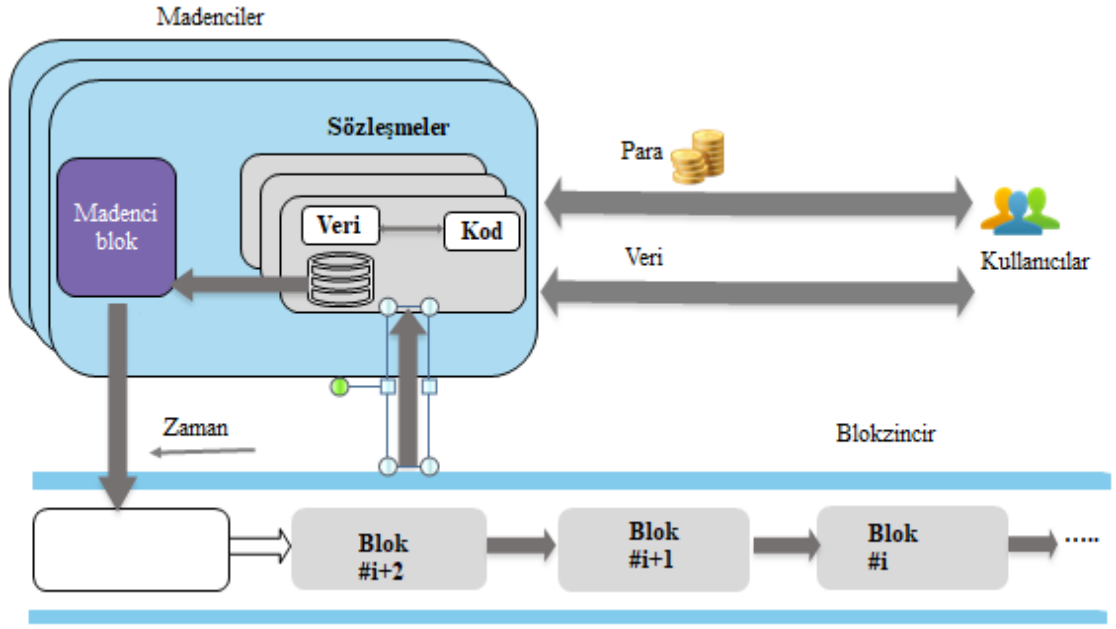
3.2.3. Konsorsiyum Blokzincir



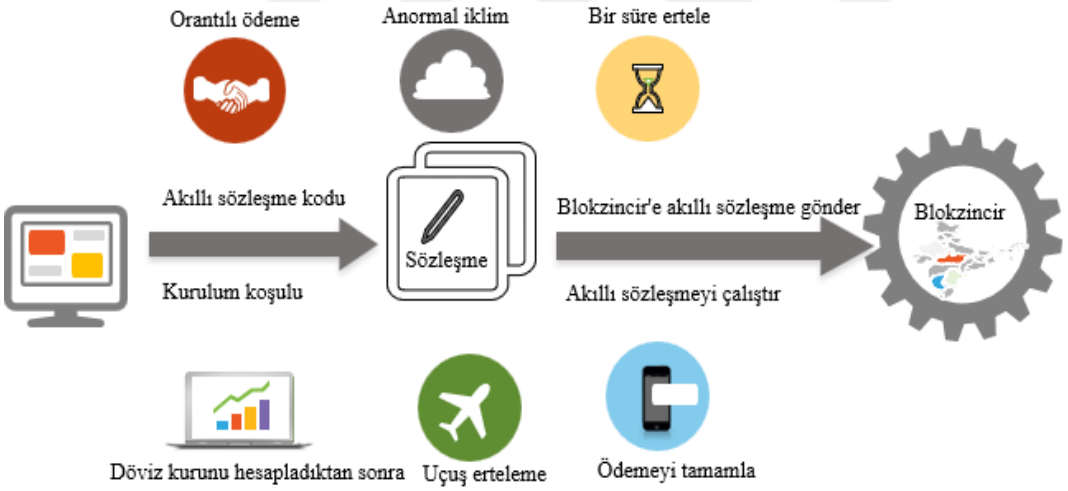
Şekil 3. 3 Konsorsiyum Blokzincir Yapısı. [42]

Genel ve özel zincir arasında olan bu yapı, konsensüs süreci için önceden seçilmiş düğümler tarafından kontrol edilen blokzincir platformunu ifade eder. Blokzincir okuma hakkı halka açık olabilir veya katılımcılar tarafından sınırlandırılabilir veya "hibrit" olabilir [42]. Bu tür zincirler "kısmen merkezi olmayan" olarak adlandırılabilir. **Şekil 3.3**'te konsorsiyum blokzincir modeli gösterilmektedir.

3.2.4. Akılı Sözleşmeler



Şekil 3. 4 Akıllı Sözleşmenin Çalışma Mekanizması. [34]



Şekil 3. 5 Akıllı Sözleşmelerin Kullanım Alanları

İlk olarak 1990'ların başında Nick Szabo tarafından akıllı sözleşmeler önerildi [7]. Blokzincir uygulamaların gelişmesiyle akıllı sözleşmelere olan ilgi arttı. 2015 yılında kurulan akıllı sözleşme, Ethereum'un temel niteliklerindendir. Akıllı sözleşme, kaynak kodunda yazılan ve bilgisayarlar tarafından yürütülen blokzincirin kurcalamaya karşı korumalı mekanizmasını entegre eden dijital bir sözleşmedir [45]. Daha genel ifadeyle akıllı sözleşmeler kendi kendini uygulayan sözleşmelerdir. İyi geliştirilmiş bir akıllı sözleşme, ağın yönetiminde görevli herhangi bir üçüncü tarafa ihtiyaç duymaz.

[46]. Blokzincir uygulamasında akıllı sözleşmeler kaydedildiğinde sistemdeki kişiler tarafında değiştirilemez ve silinemez. Sistemin diğer katılımcıları tarafından geçersiz kılınacağından hiç kimse fonların serbest bırakılması için sözleşmenin yürütülmesini zorlayamaz. Geliştiriciler, ihtiyaçlarına göre akıllı sözleşmelerde herhangi bir talimat belirleyebilir; diğer sözleşmelerle etkileşime girenler çeşitli uygulama türlerini geliştirebilir ve veri depolayabilir (bkz: Şekil 3.4).

Akıllı sözleşmeler, genellikle oylama mekanizmasında ve kripto para sisteminde kullanılmaktadır. (bkz: Şekil 3.5). Akıllı sözleşme uygulamalarını yazmak için kullanılan başlıca programlama dilleri; Solidity, Serpent ve Düşük Düzeyli Dil (Low-Level Language-LLL) [47]. Günümüzdeki çoğu geliştiriciler, akıllı sözleşmeler uygulamalarını yazmak ve bayt kodunda çalıştırmak için Solidity programlama dilini kullanıyor.

3.2.4.1. İzin Verilen İşlemler

Bir zincirde sonuçları büyük olan işlevleri yürütmek için akıllı sözleşmeler yazılabilir. Bir blokzincir uygulamasında hangi akıllı sözleşmelerin yazılmasına izin verildiğini kontrol eden standartlar, zincirin bütünlüğünü veya güvenliğini olumsuz yönde etkileyebilecek işlev riskini azaltmak için gerekli endüstri rehberliği sağlanabilir [41]. Bir zincirin veri bütünlüğünü, güvenliğini ve platform kararlılığını olumsuz yönde etkileyebilecek sınırsız akıllı sözleşme işlevlerinin sonuçlarından kaçınmak için endüstri gereksinimleri ve rehberlik için standart geliştirilmelidir.

3.2.4.2. Harici Uygulamalarla Etkileşim

Akıllı sözleşmelerin blokzincir dışındaki uygulamalarla etkileşimi yüksektir. Bu ister dünyadaki kodun yürütülmesini etkileyen bazı olaylarla ilgili verileri güvenli hale getirmek için bir kâhine (oracles) atıfta bulunmak olsun, isterse harici bir uygulama tarafından üzerinde işlem yapılacak çıktılar oluşturmak olsun, bu kodun blokzincirin alıcı uygulamalarında bir yuva bulması gerekir. Günümüzde, başka mimarilerle bağ oluştururken güvenlik ile ilgili olası riskleri minimuma indirecek talimatlar bulunmamaktadır. Blokzincir uygulamaları, ağdaki tüm düğümlerle eş zamanlı olma ihtiyacı ile düzenlenmiştir. Ancak, ağdaki başka bir zincirle etkileşimde bulunan başka düğümlerdeki uygulamalar eşzamanlı olarak tasarlanmamıştır. Verilerin doğruluğu,

bütünlüğü, güvenliği ve dengesi için rehberlik yapma üzere harici uygulamalarla akıllı sözleşme etkileşimleri için belli başlı standartlar geliştirilmelidir [41]. Bu teknoloji açısından çok önemli olsa da standartları geliştirmeden önce ilgili sistemin olgunlaşması için biraz süreye ihtiyacı vardır.

3.2.4.3. Kod Kurulumunun Güvenliği

Blokzincir mimarisinde, akıllı sözleşme yazılan kodun anlaşılır, doğru olması ve ağda bulunan düğümlerde aynı olması oldukça önemlidir. Ağda iyi niyetli olmayan veya doğru olmayan akıllı sözleşme ile ilgili özellikleri kullanma becerisi bulunursa, akıllı sözleşmelerde var olan tutumun hepsini değiştirebilir. Akıllı sözleşme sistemindeki kod bloğu ilgili sisteme indirildiğinde, kod bloğu doğrulabilir ve kod blok ile ilgili değişiklik olmayacağına dair kanıtlanabilir bir sigorta olmalıdır. Sistemde yetkiye sahip olan kullanıcılar tarafından kurulup ve yönetilmesi için kontrol mekanizmaları olmalıdır [41].

3.3. Kriptografik Algoritmalar

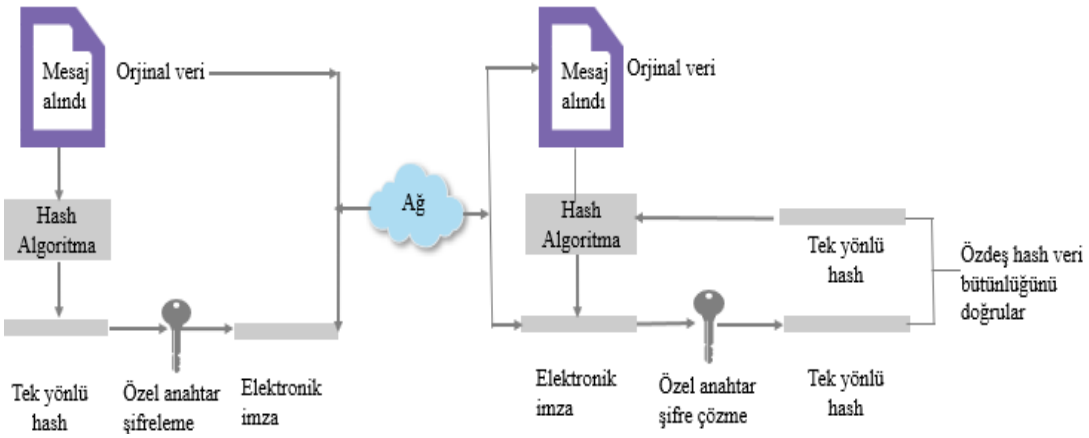
Blokzincir sisteminde bulunan verilerin güvenlik ihtiyaçlarını karşılamak için çok kademeli şifreleme algoritmaları kullanılmaktadır. Şifreleme algoritmalarına (ECDSA, Simetrik, Asimetrik gibi algoritmalar) destek veren blokzincir sistemi, kişisel verilerin güvenliği sağlamak için çeşitli şifreleme algoritmalarını kullanır. Başlıca kullanılan şifreleme algoritmaları:

- ECDSA: secp256k1 ve secp256r1 [16]eğrileri
- Simetrik, asimetrik şifreleme algoritması: Üçlü Veri Şifreleme Standardı (Triple Data Encryption Standart-3DES) ve Gelişmiş Şifreleme Standardı (Advanced Encryption Standard-AES) algoritmaları
- Anahtar değişimi: Eliptik-Eğri Diffie–Hellman (Elliptic-Curve Diffie–Hellman-ECDH)
- Karma (hash): SHA256, Keccak256 karmaları

[16] secp256r1 bir NIST eğrisidir. NIST eğrileri yaygın olarak kullanılmaktadır ve diğer eğrilerinden daha fazla incelemeye tabi tutulmuştur.

3.3.1. Eliptik Eğri Dijital İmza (Elliptic Curve Digital Signature Algorithm-ECDSA)

ECDSA, Dijital İmza Algoritmasının (DSA) benzeridir. ECDSA, yıllara göre farklı standartları oluşmuştur. 1999 tarihinde Amerikan Ulusal Standartlar Enstitüsü (American National Standards Institute-ANSI), 2000 tarihinde ise Elektrik Elektronik Mühendisleri Enstitüsü (Institute of Electrical and Electronics Engineers- IEEE) ve Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology-NIST) adıyla varyantları olmuştur. 1998 tarihinde Uluslararası Standartlar Teşkilatı (International Organization for Standardization-ISO) tarafından onaylanmıştır. Eliptik eğri kriptografisinin doğrulama gücü diğer şifrele algoritmalarından daha yüksektir.

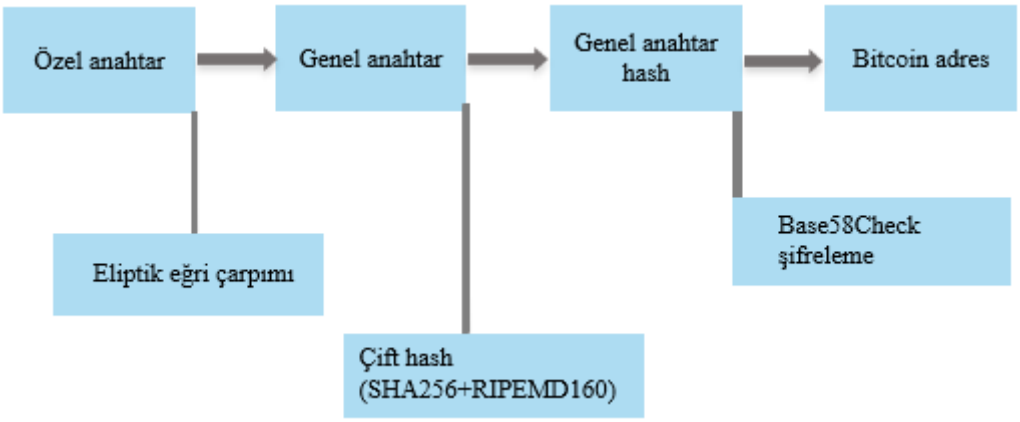


Şekil 3. 6 Asimetrik Kriptografi ve Dijital İmzalar

Kriptografik teknolojileri olarak simetrik ve asimetrik şifreleme algoritmaları kullanılır. Asimetrik şifreleme algoritmasında, mesajı şifreleme ve şifre çözme anahtarı birbirinden farklıdır ve sırasıyla genel anahtar ve özel anahtar olarak adlandırılır (bkz: Şekil 3.6). Kişiye özel anahtarın gelişigüzel olarak karmaşık sayı algoritmasından oluşturulması gerekir ve halka açık olan bu anahtar, tek yönlü bir algoritma ile hesaplanır. Güvensiz kanallarda iletilebilen asimetrik şifreleme algoritması, halka açık ve kişiye özel anahtarların çok sayıda önemli özelliklerine sahiptir.

Eliptik Eğri algoritması, herkesçe bilinen ortak anahtar çifti olan bir şifreleme algoritmasıdır. Yapılan işlemin güvenliği ve zorluğu ise eliptik eğri ayrık logaritma hesaplama gücüne bağlıdır [48]. Blokzincir teknolojisi, işlemlerdeki imzalama ve doğrulama için ECDSA eğrisi olarak bilinen secp256k1'i kullanır. Benzer şekilde

ağdaki düğümler arasında mesaj iletim sırasında bütünlüğü ve doğruluğu ispatlamak için ECDSA eğrisi olarak bilinen secp256r1 kullanır. Bitcoin uygulamasında özel ve genel anahtar çifti ortak anahtar şifreleme algoritmasıyla oluşturulur.



Şekil 3. 7 Bitcoin Adres. [49]

Bitcoin ağındaki ödeme işlemleri, alıcının adresi Şekil 3.7'de gösterildiği gibi Bitcoin adresi olarak tanımlanan ortak anahtar aracılığıyla oluşturulur [49]. Kişiye özel olan anahtar gelişigüzel olarak seçilen bir karmaşık sayıdır ve genel anahtar, özel anahtarın hesaplaması zor olan eliptik eğri çarpımının şifrelenmesiyle oluşturulur. Ortak anahtar çifti ile Bitcoin adresini üretmek için tek yönlü şifreli karma işlemi uygulanır. Bir Bitcoin özel anahtarı oluşturmak için 1 ile 2 üzeri 256 arasında bir sayı seçilir. Seçilen sayı ile hesaplanan işlem sonucunun tahmin edilemez veya tekrarlanamaz olması gerekir.

Bitcoin uygulaması Şekil 3.7'de gösterildiği gibi Bitcoin adresini üretmek için çift karma, SHA256 ve RIPEMD160 [17]yapılarını kullanır; Ethereum uygulaması ise Ethereum adresini oluşturmak için Keccak256 karma algoritmasını kullanır. Bitcoin ağında ortak anahtar çifti olarak bilinen özel ve genel anahtar kullanılır. Ortak anahtar karma değeri olarak 160 bitlik bir sayı elde etmek için RIPEMD160 karma değerini yeniden hesaplar. Genel anahtar karması, Bitcoin adresi oluşturmak için şifrelenmiş Base58'dir. Base58 sadece Bitcoin sisteminde değil, benzer şekilde sıkıştırma, kolay

[17] RIPEMD-160, Merkle–Damgård yapısına dayalı bir kriptografik karma işlevidir. Bitcoin standardında kullanılır. RIPEMD-160 algoritması 160-bit çıktı üretirken 128 bitlik bir karma özet üreten RIPEMD algoritmasının güçlendirilmiş bir versiyonudur.

okuma ve hata bulma gibi diğer kripto para birimleri kullanımı açısından geniş bir kullanım kitlesine sahiptir. Bitcoin teknolojisi Base58 kodlamasında Base58Check'i kullanır. Sistemdeki hataları giderilmesi için işlenmiş verilere 4 baytlık hata kodu kullanılır.

3.3.2. Simetrik Şifreleme Algoritması

Blokzincir teknolojisi, ağdaki düğümler arasında şifreli metin aktarımı sağlamak için simetrik şifreleme algoritmalarından AES ve 3DES algoritmaları kullanılır. 3DES ağdaki verileri şifrelemek için 56-bit anahtar kullanan Veri Şifreleme Standardı (Data Encryption Standard-DES) simetrik şifreleme algoritmasının ayrı bir versiyonudur. DES, ABD' de simetrik şifrelemesi kullanan bir şifreleme modelidir. DES simetrik şifreleme algoritması, 56-bitlik anahtar ve kriptografik blok metodu kullanırken, kriptografik blok metodunda mesaj 64-bit büyüklüğünde mesajı ayrı bloklara parçalar ve daha sonra ilgili mesajı kriptografik yöntemlerle şifreler. 3DES simetrik şifreleme algoritması, DES'ten çok daha güvenlidir.

Simetrik şifrele algoritmalarından olan AES, ABD tarafından kullanılan gelişmiş bir blok şifreleme türüdür. AES şifreleme algoritması, permütasyon gibi hesaplaması zor matematiksel işlemlere dayanır. Ayrıca AES, permütasyon işlemlerin gelişimi için çeşitli yöntemleri kullanır. AES şifreleme algoritması, 128, 192 ve 256 bit uzunluğunda anahtarları kullanan ve sistemdeki verileri 128-bit uzunluğundaki anahtarla şifreleyen aynı şekilde şifresini çözen simetrik bir anahtar algoritmasıdır. Genel ve özel anahtar parolası kullanan anahtarın aksine, simetrik anahtar şifreleri ağdaki verileri şifrelemek ve şifresini çözmek için tek anahtar kullanır. Blok şifresi aracılığıyla şifrelenmiş verilerin giriş verileriyle eşit bit değerine sahip olması gerekiyor.

3.3.3. Hash Algoritması

SHA, NIST tarafından yayınlanan ve kriptografik işlevinin genel özelliklerine sahip bir kriptografik karma işlevidir. SHA256 karma algoritması, 256-bitlik mesaj ya da metnin özeti olarak oluşan SHA-2 algoritma kümesinin elemanlarından biridir. Temelde, her metin bloğuna sıkıştırma işlemi uygulanır. Veri sıkıştırma, karma değeri oluşturmada önemli faydalar sağlar. Karma, sıkıştırma olmasa da daha büyük bir veri seti alması ve daha yönetilebilir bir forma küçültmesi bakımından dosya sıkıştırmaya çok benzer

şekilde çalışabilir. Karma hesaplaması için Keccak256 algoritmasını da kullanan blokzincir mimarisi, aynı zamanda adres hesaplaması için de kullanılabilir. Karma fonksiyonların temel amacı sistemdeki verilerin bütünlüğünü sağlamaktır. Ayrıca karma fonksiyonu, veri setini alan ve boyutu değiştirmeden karma özetine çeviren, girdiden bağımsız bir ortalama doğrusal zaman algoritmasıdır. Başarılı bir karma işlemin özellikleri şunlardır:

- **Tek yönlü fonksiyon**, ağda herhangi bir çarpışma olmadığı sürece aynı girdi her zaman aynı çıktıyı üretir.
- **Verimli**, çıktı zamanında hesaplanır, dağıtılır, çıktı aralığına eşit olarak yayılır, yani benzer veriler benzer verilerle ilişkilendirilmemelidir. Bu durum, verimliliği pozitif yönde etkiler.
- **Ön görüntü direnci**, karma değerine ve çarpışma direncine bağlı olarak a girişini bulmak mümkün olmamalıdır. Blokzincirlerde verileri düzenlemek ve birbirine bağlamak için karma fonksiyonlar kullanılır. Blokzincir sisteminde karma fonksiyonlarının diğer önemli özelliği ağdaki verileri birbirine bağlamasıdır. Bu, önceki bloğun karma değeri, işlemlerin Merkle kökü, zamanı ve nonce değerini içeren blok başlığındaki çeşitli öğelerin hash değerinin alınmasıyla yapılır. Merkle ağacı [18] kavramı, her işlemin karma değerin alınması, Merkle kökü olarak bilinen üst düğüm elde edilene kadar bir ağaç yapısı oluşturmak için hash edilmesidir.

4. BLOKZİNCİR UYGULAMASINDA KİŞİSEL VERİLERİN TUTULMASI

4.1. Kişisel Veri Tanımı

Kişisel veri tanım olarak kimliği belli olan gerçek kişiye bağlı olan her çeşit bilgi olarak tanımlanır [50]. Blokzincir teknolojisinde, bir bireyin açık anahtarı, kişisel verileri olarak kabul edilir ve bu nedenle GDPR ve KVKK uyum yükümlülüklerine ihtiyaç duyulmaktadır [51]. Bu kişisel veriler, tanımlayıcı bir isim, kimlik numarası, konum verileri, çevrimiçi tanımlayıcı veya bu gerçek kişinin fiziksel, fizyolojik, genetik, zihinsel, ekonomik, kültürel veya sosyal kimliğine ilişkin faktörler olabilir. Sunucuların aldığı farklı tanımlayıcılar ve farklı verilerle bir araya geldiğinde veri kişilerin profillerini oluşturarak bazı izler bırakabilir. Bazı durumlarda, bilgi tek başına bir kişiyi ayırt etmeyebilir, ancak bu bilgi diğer bilgi parçalarıyla birleştiğinde kişiyi tanımlayabilir.

4.2. Avrupa Birliği ve Türkiye'nin Genel Veri Koruma Yönetmeliği

GDPR ve KVKK, yakın tarihte veri gizliliği düzenlemesinde yapılan en büyük değişikliklerdendir. GDPR, 1995 tarihli Veri Koruma Yönergesi yerine Mayıs 2018'de yürürlüğe girmiştir. KVKK ise Türkiye'de kişisel olarak tanımlanan verilerin korunmasına yönelik en önemli gelişme olup 7 Nisan 2016'da kabul edilip 6698 sayılı kanunla yürürlüğe girdi. Verileri işlenen gerçek kişiler ile bu kişisel verileri kullanan gerçek ve tüzel kişiler arasında kanuna uygunluğun yürütülmesi amacıyla 7 Nisan 2018 tarihinde yürürlüğe girdi. GDPR kapsamında temel amaç; Avrupa genelinde veri gizliliği yasalarını uyumlu hale getirmek ve özellikle AB vatandaşlarının mahremiyetini korumak ve güçlendirmektir [11]. KVKK'da da benzer şekilde temel amaç kişisel verileri korumaktır. Sistemlerdeki hizmet sağlayıcılar, bireylerin rızasının ne için olduğunu belirtilmesi gerektiğini ve kullanıcı rızasını geri çekmenin zor olmadığını belirtir. Kişi verdiği onaydan vazgeçerse veya kişiye ait verileri kullanım olarak rızası dışında olursa hizmet sağlayıcısının bu kişilerle ilgili verileri silmesi gerekir. Hizmet sağlayıcı kullanıcının isteği üzerine verilerin işlenip işlenmediğine dair bir rapor sunmalıdır. Hizmet sağlayıcı tüm bu kişisel verileri kullanıcıya makine tarafından okunabilir ve anlaşılır bir biçimde sunmalıdır. Erişim hakkına benzer şekilde veri taşınabilirliği hakkı da vardır; kullanıcı, kişisel verilerinin makine tarafından okunabilir

bir biçimde denetleyiciden bir özetini alabilmeli ve verilerini başka bir denetleyiciye aktarma hakkına sahip olmalıdır.

GDPR kapsamında yapılan kişisel veri ihlalleri büyükse şirket, kurum ve kuruluşlar tarafından 20 milyon Euro'ya veya küresel cironun %4'üne kadar büyük para cezaların ödenmesi gerekebilir. KVKK kapsamında ise 18. madde uyarınca cezalar 2020 yılı için en düşük 9.000 TL ve en yüksek 1.800.000 TL olarak belirtilmiştir. KVKK'daki alt ve üst sınır olarak belirtilen para cezaları için kurulun takdir hakkı bulunmaktadır

4.3. Blokzincir ile GDPR ve KVKK Arasındaki Uyumsuzluklar

Tablo 4. 1 GDPR ve Blokzincir Hedefleri Arasındaki Farklar

GDPR	Blokzincir
Veri kontrolü	Merkezi olmayan
Silme hakkı Düzeltme hakkı	Değişmez
İşlemeyi kısıtlama hakkı	Tüm paydaşlara dağıtıldı

Tablo 4.1'de gösterildiği gibi GDPR ve KVKK'nın blokzincirin uyum sağlama kabiliyetini sorgulayan çeşitli alanları vardır.

4.3.1. Bilgilendirilme Hakkı

GDPR ve KVKK, verileri koruma yasası gereğince kendi haklarını savunmak için müracaat ettikleri minimum bir gerçek veya tüzel kişi ve kişisel veri denetleyicisi olduğu hipotezine dayanmaktadır. GDPR kapsamındaki 13 ve 14. maddeler gereğince, kişisel verilerin bazı amaçlar için toplanması ve kullanılması ile ilgili kişilere bilgilendirilme hakkı verilir. Bu durum, GDPR ve KVKK kapsamında çok önemli şeffaflık gereksinimidir. Bireyler, kişisel verilerinin işlenme amaçlarını, bu kişisel verilerin saklanma sürelerini ve kimlerle paylaşılacağına dair bilgi edinme hakkına sahiptir. Bu bilgiler, kişilere, verilerinin toplandığı sırada verilmelidir.

Tablo 4. 2 Blokzincir Uygulamalarında Bireyin Hakları Problemi

	Amaç	Uyumsuzluk
• **Bilgilendirilme Hakkı**	• Bireyler, verilerinin işlenme amaçlarını, saklama sürelerini ve kimlerle nasıl paylaşılacağına dair bilgi alma hakkına sahiptir	• Blokzincir teknolojisi, âdem-i merkeziyetçiliği sağlamaya çalışır. Bu durumda veri denetleyicisinin kim tarafından seçileceği belirsizdir
• **Silme ve İşlemeyi Kısıtlama Hakkı**	• Veri sahipleri, verilere erişim için sözlü veya yazılı olarak istekte bulunduktan sonra verilerin gecikmeksizin düzeltilmesi gerekir	• Blokzincir uygulamasındaki veriler ve işlemler, verileri bilgisayar ağlarında tutan taraflara dağıtıldığından, ağdaki tüm tarafların erişim hakkına uymasını gerektirecektir
• **Silme ve İşlemeyi Kısıtlama Hakkı**	• Veri sahipleri, istemeleri durumunda kişisel bilgilerinin kurum ve kuruluşlarca işlenmesini kısıtlama veya engelleme hakkına sahiptir.	• Blokzincir sadece ekleme işlemi yapılan veri tabanlarıdır, silme işlemleri için fikir birliğine varılması gerekir.

GDPR ve KVKK'nın blokzincir teknolojisi ile uygulamasında ilk sorun şudur (bkz: Tablo 4.2): Bir blokzincirin veri denetleyicisi ve işlemcisi kimdir? Blokzincir, âdem-i merkeziyetçiliği sağlamaya çalışır, durum böyle olunca, işlemenin amaçlarını ve araçlarını hangi tarafın belirlediği genellikle belirsizdir. Bu durum, özellikle düzenleme kapsamındaki kontrolörlük kavramının belirsiz sınırları ışığında sorumluluk ve hesap verebilirlik dağılımını zor hale getirir. Bu açıdan daha karmaşık bir faktör son içtihat hukuku gelişmeleri ışığında hangi kuruluşların kontrolör olarak nitelendirildiğini yasal kesinlik eksikliği ile doludur.

Özel blokzincir uygulamaları, bir şirket tarafından organize edilen blokzincir üzerinde kontrole sahip olduklarını ve amacı belirleme yeteneğine sahip olduklarını varsayarak genellikle kontrolör olarak nitelendirilebilecek bir merkezi operatör veya grup olduğundan kontrolörleri ve işlemcileri tanımlamayı kolaylaştırır. Kamu blokzincir uygulamaları ise genellikle merkezi bir yapı veya konsorsiyumdan yoksundur. Ayrıca birden fazla taraf sıklıkla bir blokzincir uygulamasındaki verileri veya işlemleri işler. Bu durumda, tüm tarafların işlemci olmasının pratikliği sorgulanmalıdır. Açık bir kontrolör veya işleyici belirleme yeteneği olmadan bireyin bilgilendirilme hakkını kullanmak için kime yaklaşacağı veya ulaşabileceği belirsizdir.

4.3.2. Erişim ve Düzeltme Hakkı

KVKK ve GDPR'ın 15. maddesi gereğince kişisel verilere erişim olarak isimlendirilen erişim hakkı, veriye sahip olan bireylere kişisel verilerinin bir nüshasını ve gerekli diğer

bilgileri alma hakkı verir. Verilerinin nasıl ve neden kullanıldığını ve kullanımın yasal olup olmadığını anlamalarına yardımcı olur. Kişiler, verilerine erişmek için yazılı veya sözlü talepte bulunabilir ve denetleyicinin talebe yanıt vermesi için 30 güne kadar süresi vardır [52] (bkz: Tablo 4.2). Yine belirli bir denetleyiciyi belirleme yeteneği olmadan, erişim haklarını kullanmak için bireysel bir yaklaşım kim olur? Ek olarak, blokzincir uygulamasındaki işlemler veya veriler, verileri bilgisayarlarında tutan taraflara dağıtıldığından blokzincir ağında kişisel verilerin tutulduğu birçok yer olabilir. Bu durum, tüm tarafların erişim hakkına uymasını gerektirecektir. Bireylerin yalnızca kişisel verilerine erişme hakkı yoktur, verilerin doğru olması gerekir ve yanlışsa bireyin verilerin düzeltilmesini isteme hakkı vardır. Ayrıca GDPR ve KVKK kapsamında, kişisel verilerin eksik olması durumunda, veri sahibine eksik bilgileri tamamlama hakkını sunar. Erişim hakkına benzer şekilde, talep sözlü veya yazılı olarak yapılabilir ve kontrolörün talebe yanıt vermesi için 30 güne kadar süresi vardır. Blokzincir uygulamaları, erişim ve düzeltme hakların kullanımını zorlaştırır.

4.3.3. Silme ve İşlemeyi Kısıtlama Hakkı

Silme ve işlemeyi kısıtlama hakkı, GDPR'ın 16. ve 17. ve KVKK'nın 7. maddeleri gereğince kişilerin isteği doğrultusunda kişisel verilerin düzenleyebileceği veya silinebileceği hipotezine dayanmaktadır [53]. Buna benzer şekilde "unutulma hakkı" olarak da bilinir. Bu kişilerin sahip olduğu hak mutlak değildir ve genellikle belirli koşularda geçerlidir. Hakkın uygulanamadığı durumlar çoğunlukla yasal gereklilikler, kamu politikası, bilimsel araştırma, halk sağlığının korunması ve talebin "açıkça temelsiz" olduğu durumlardır. Bununla birlikte, bu istisnalar blokzincir ağındaki veriler veya işlemler için geçerli değilse denetleyicinin GDPR ve KVKK kapsamında kişisel verileri silmesi gerekir. Silme hakkına başka bir alternatif ise bir bireyin verilerinin işlenme kısıtlama veya bastırma hakkıdır ve bu, belirli durumlarda silme hakkının kullanım ihtiyacını engeller.

Bireyler bazı nedenlerden dolayı kişisel verilerini kısıtlamayı istemeleri durumunda kişisel bilgilerinin kurum ve kuruluşlarca işlenmesini kısıtlama veya engelleme hakkına sahiptir (bkz: Tablo 4.2). Sebebi ise bu verilerin kullanıcının bilgisi olmadan nasıl ve nerede kullanılmasıyla ilgili problemlerin olmasıdır. Çoğu durumda, bir bireyin kişisel verileri süresiz olarak kısıtlanamaz, ancak kısıtlamanın belirli bir süre boyunca

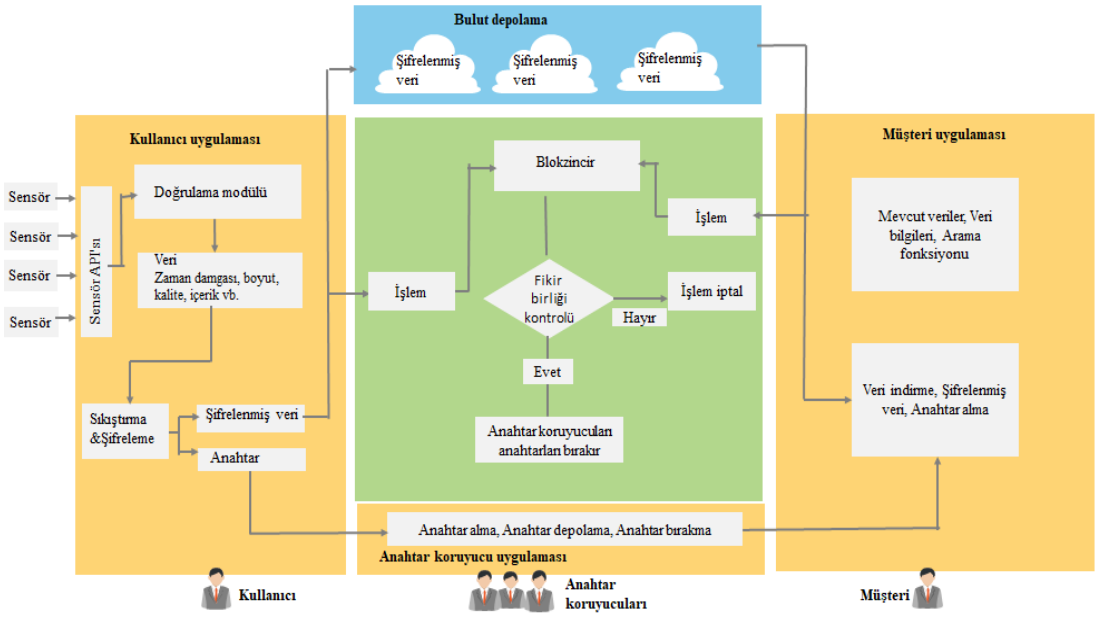
yürürlükte olması gerekir. Ancak blokzincir, veri bütünlüğünü sağlamak ve ağdaki güveni artırmak için bu tür veri değişikliklerini kasıtlı olarak zahmetli hale getirir ve veriler bir blokzincir ağındaki bir işlemin parçasıysa zincir değişmez ve geri döndürülemez, bu nedenle veriler silinemez. Bu durumda, GDPR ve KVKK ile uyumlu olmaz. Bu hakka uymayı zorlaştıran durum ise kişisel verilerin başkalarına ifşa edilmesinin imkânsız olmadığı veya orantısız bir çaba gerektirmediği sürece her bir alıcıyla temasa geçilmesi ve silme talebi hakkında bilgilendirilmesi gerektiğidir. Kontrolörler, veri sahiplerini bu alıcılar hakkında bilgilendirmelidir.

Kişisel veri koruma kanununun mevzuatı alanındaki belirsizlikler, kişisel veri muhafaza etme kapsamındaki belirsizlikler gittikçe artmaktadır. Halka açık anahtarlar ve işlem bilgilerin dağıtılmış defterde kaydedilen kişisel verilerin KVKK ve GDPR'nin kanun kapsamında kişisel veri olarak onaylanacağına dair tartışma devam etmektedir [54]. Tartışmalardan biri, şifrelenmiş veya karma değeri alınmış verilerin hala kişisel veri olarak nitelendirilip nitelendirilmediğidir. Bu tür veriler muhtemelen KVKK ve GDPR amaçları için kişisel veri olarak nitelendirilir, yani bu tür verilerin işlendiği yerde veri koruma yasası geçerlidir. Yapılan bu analiz daha önce kişisel bilgi olan verilerin GDPR kapsamında anonimleştirilip anonimleştirilemeyeceği konusundaki belirsizliklerin güçlüklerini de belirtmektedir. GDPR ve KVKK, işlenen kişisel verilerin minimumda tutulmasını ve yalnızca önceden belirlenmiş amaçlar için işlenmesini gerektirirken bu ilkelerin blokzincir teknolojilerine uygulanması zor olabilir. Blokzincir uygulamasındaki defter biçimi, kişisel veriler eklendikçe büyüyen sadece ekleme işlemi yapılan veri tabanıdır, silme ve değiştirme işlemleri için de fikir birliğine varılması gerekir. Ayrıca, bu kişisel veriler çok sayıda aynı olmayan düğümlerde çoğaltılabilir.

Blokzincir bağlamında kişisel veri işlemenin "amacının" nasıl uygulanması gerektiği, özellikle bunun yalnızca ilk işlemi mi kapsadığı yoksa aynı zamanda kişisel verilerin sürekli işlenmesini mi kapsadığı belirsizdir. Son yıllarda muhtemelen en çok tartışılan konu, silme hakkı (“unutulma hakkı”) ile blokzincir arasındaki uyumsuzluktur. Aslında blokzincir genellikle verilerin tek taraflı değiştirilmesini imkânsız hale getirmek için tasarlanmıştır. Bu, elbette GDPR'nin, belirli durumlarda kişisel verilerin değiştirilmesi (GDPR Madde 16 kapsamında) ve silinmesi (GDPR Madde 17 kapsamında) gerekliliklerileyle uzlaştırılması zordur [55].

4.4. Blokzincirde Kişisel Verilerin Tutulması ile İlgili Yapılan Çalışmalar

Blokzincir teknolojisine dayalı bir teknik çerçeve sunulmuştur. GDPR'ın çeşitli yasal gerekliliklerıyle başa çıkmanın ve bunları uygulamanın yollarını ve yasa koyuculardan teknolojik değişikliklere ayak uyduran yeni yasal doktrin biçimleri ele alınmıştır [56]. Tasarıma göre gizlilik doktrinini (Madde 25 sn. 3 GDPR) belirleyen sertifikasyon mekanizmaları, yasal gereklilikler ve teknik tasarım kararları arasında ortak bir yol bulmak için bir araç olarak hizmet edebilir. GDPR uyumlu bilgi teknoloji çözümleri için minimum gereksinimleri veya yüksek standartları işaretleyebilirler.



Şekil 4. 1 Bulut Depolamada Blokzincir Tabanlı Veri Paylaşım Sistemi**.** [57]

Kullanıcıların kişisel sağlık verilerini kolay ve güvenli bir şekilde paylaşabilmelerini sağlamak ve araştırmacıların ticari veri tüketicilerinin gerekli verileri verimli ve şeffaf bir şekilde elde etmelerine yardımcı olmak için blokzincir ve bulut depolama teknolojilerine dayalı GDPR gibi veri düzenlemelerine uygun olarak kişisel veri paylaşım sistemi önerilmektir [57]. Çalışmadaki kişisel verileri depolama ve paylaşım sisteminin mimarisi Şekil 4.1'de açıklanmıştır. Bu sistemde 6 rol tanımlanmıştır:

- **Kullanıcılar (Users):** Kişisel verileri üretmek, yüklemek ve paylaşmak.
- **Anahtar Tutucular (Key Keepers):** Kullanıcı verileri sisteme yüklendikten sonra verilerin şifresinin çözülmesi için özel anahtarları tutmak ve bir işlem onaylandığında anahtarları müşterilere vermek.

- **Müşteri (Customer):** Kullanıcı verilerini satın almak ve parasal açıdan kullanıcılara (anahtar sahiplerine) hizmet ödülleri sağlamak.
- **Kullanıcı Uygulaması (Customer):** Bir mobil bilgi işlem cihazında çalıştırmak için toplanan kişisel veriler, iyi puan için güvenli doğrulama modülünden geçecektir. İşlem doğrulandıktan sonra bazı tanımlamalarla birleştirilecektir. Birleşen veriler, karma ve simetrik şifreleme yöntemleriyle sıkıştırılıp ve oluşturulan anahtarla şifrelenecektir. Şifrelenmiş ve sıkıştırılmış veriler daha sonra bir bulut sisteminde depolanacaktır. Depolanan verilerin şifresini çözen anahtar, bazı paylaşımlara ayrılarak ve anahtar sahiplerine verilecektir. Son olarak oluşturulan işlemler blokzincirin düğümlerine yayınlanacaktır. İşlem, kullanıcının genel anahtarını ve şifrelenmiş veriye olan bağlantıyı içerir.
- **Anahtar Koruyucu Uygulaması (Key Keeper Application):** İnternete bağlantısı olan bulut sunucusunda ya da yerel bir yapıda tutulur. Verilerin paylaşımı doğrulandığında ilgili işlemin alıcısına denk olan anahtar paylaşımı için bilgilendirilecektir.
- **Müşteri Uygulaması (Customer Application):** İnternete bağlı yerel bir cihazda veya bir bulut sunucusunda çalışır. Müşteriye mevcut tüm veri kümelerini gösterebilir ve belirli bir veri kümesi türünü aramasına izin verebilir. İşlem daha sonra blokzincir düğümlerine yayınlanacaktır. İşlem onaylandıktan sonra, uygulama, anahtar sahiplerinden şifrelenmiş verilere ve şifre çözme anahtarlarına bir bağlantı alacaktır. Daha sonra müşteri verileri yereline indirebilir ve özel anahtarlarla şifresini çözebilir.

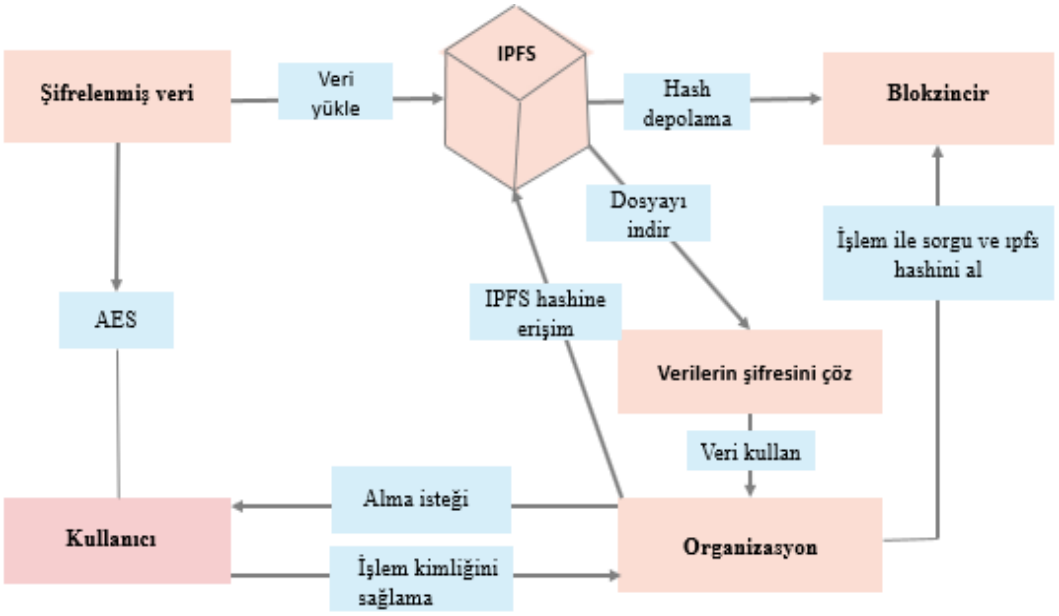
Kişisel verilerin silinmesi konusunda üç ana yaklaşım ortaya koymuştur [58]. Bunlardan ilki, kişisel verilerin tanımlanabilir bir veri denetleyicisinin kontrolü altında bir veri tabanında zincir dışı depolanmasıdır. Blokzincir, kişisel verilerin depolandığı veri tabanına bağlantı olarak kullanılabilecek bir kama değeri tutar. GDPR ve KVKK, silinme hakkı kapsamında silinmesi gereken yalnızca zincir içi karma değer ile bağlantılı herhangi bir konuyu tanımlamak için kullanılan zincir dışı verilerdir. Önerilen bu çözüm, verilerin belirli bir dereceye kadar kontrolü tek bir merkezi partinin elinde kaldığından, blokzincir uygulamaların ademi merkeziyetçilik ilkesine ters olarak kabul

edilebilir [59].

İkinci yaklaşım, "anahtar imha" ile ilgilidir. Blokzincir uygulamalarında depolanan veriler için yeterince güçlü bir şifreleme algoritmasının kullanılması, verilerin şifreleme anahtarı yok edilerek "silinebileceğini" göstermektedir. Bu durumda, verilerin şifresini çözmek imkânsız olduğu için ağdaki bilgilere artık erişilemez. Verilerin zincirden gerçekten silinmemesi, yalnızca veri sahibi tarafından erişilebilir olması veya hiç erişilememesi şeklinde yorumlanabilir. Buna uygun olarak, verilerin veya anahtarların imha edilmesi, kişilerin yeniden tanımlanması olasılığını ortadan kaldırmaz. Ayrıca, AB yetkililerinin görüşünde kaba kuvvet saldırılarının hipotezleri ve teknolojinin evrimi de dikkate alınmalıdır.

Üçüncü yaklaşım, bukalemun karma değeri ile ilgilidir. Verilerin karmasını almak veya anahtarların imhasıyla bu tür verileri erişilemez hale getirmek yerine, bir trapdoor fonksiyonunu (tuzak kapı işlev fonksiyonu)[18] içeren karma değer işlevlerinin kullanımı yoluyla "düzeltilebilir blokzincir" tasarlamaktır. Ancak, bukalemun karma değeri, blokzincirin yeniden düzenlenmiş bilgileri içerecek olan eski başlıklarını ortadan kaldıramaz ve madenciler de değişiklikleri kabul edip etmeme konusunda takdir yetkisine sahiptir [59]. Burada, yasal bir çatışmanın nedenleri, siyasi âdem-i merkeziyetçilik ilkeleri ve veri koruma kurallarının bir karışımı olarak ortaya çıkıyor. Mimarilerine, kullanımlarına, hizmetlerine veya işlevlerine göre birden fazla blokzincir türünü daha fazla göz önünde bulundurarak gelecekte silme sorununa hangi çözümün hâkim olabileceğini söylemek oldukça zor.

[18] Bir tuzak kapısı işlevi, bir yönde hesaplanması kolay, ancak ters yönde hesaplamanın zor olduğuna inanılan ve özel bilgi olmadan "kapalı kapı" olarak adlandırılan bir fonksiyondur. Çıktı dizisine genellikle karma değer denilir. Karma değerleri genellikle giriş dizilerini işaretlemek için kullanılır.

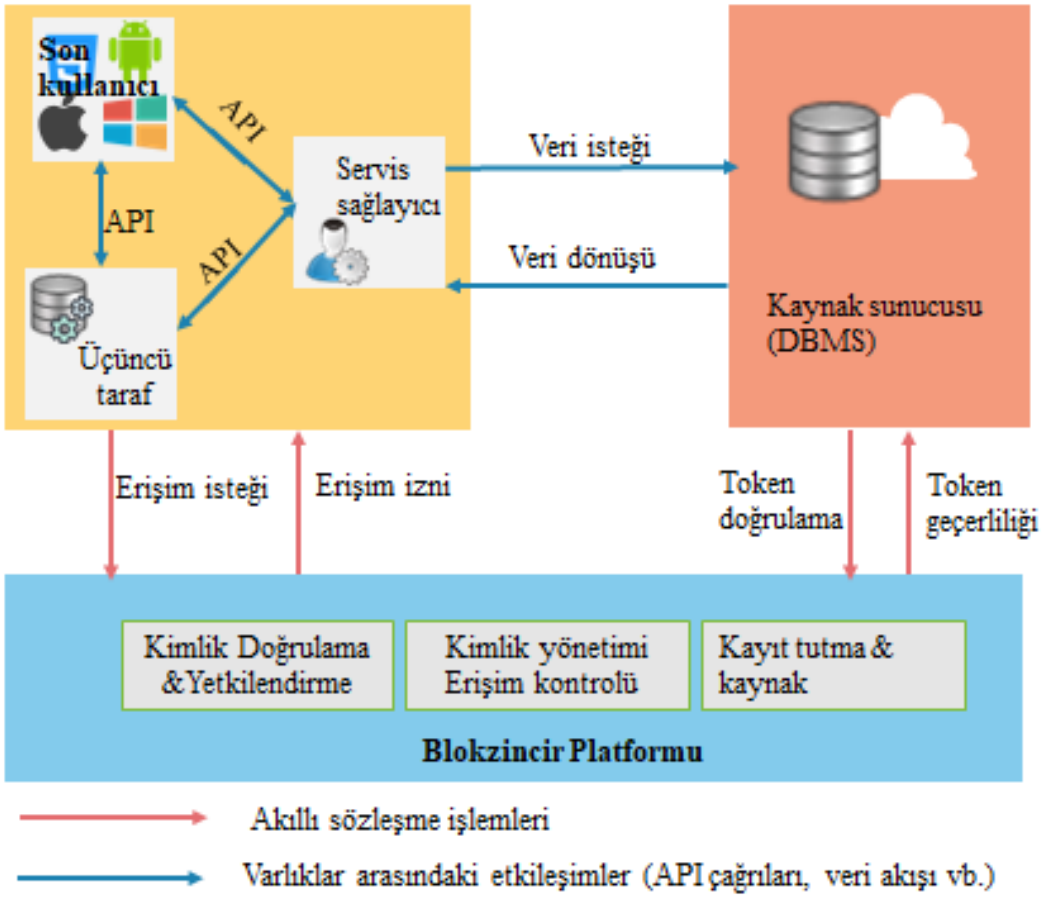


Şekil 4. 2 IPFS Bulut Depolama Mimarisi. [61]

Blokzincir uygulamasını kullanan güvenli Gezegenler Arası Dosya Sistemi (InterPlanetary File System-IPFS[19] bulut depolama sistemini kullanmaktadır [61]. Bununla, güvenilmeyen ortamlarda depolanan veriler korunur. Şekil 4.2'de gösterildiği gibi veriler bulutta saklanacak, burada dosyayı tanımlayan bilgiler sadece blokzincir ağında mevcut olacak. Önerilen modelde, AES256 şifreleme algoritması kullanılır. Blokzincir ağında depolanan veriler herkese açıktır, bu nedenle depoya ve erişim kontrolüne gönderilmeden önce şifrelenir. Veri sahibi tarafından sağlanan şifreleme anahtarı, bir belgenin şifresini çözmek ve dosyayı indirmek için kullanılır. Önerilen sistemin kullanıcıları; vatandaşlar, devlet ve özel kuruluşlardır. Sistemden yararlanmak isteyen vatandaşlar sisteme kaydolduktan sonra şifrelenmiş ve IPFS dağıtılmış bulutta saklanan belgeleri yükleyebilir. Ek güvenlik hizmeti sağlamak için belgeler şifrelenir ve ardından sisteme yüklenir. IPFS bulut sistemi üzerinden depolanan belgelere erişim için önce kimliğin doğrulanması gerekir. Doğrulamadan sonra, kimlik kullanılarak istenen belge aranabilir. Kullanıcı, her belge için açık anahtarı yalnızca yönetici tarafından doğrulanan kuruluşlarla paylaşır. Kuruluş, istenen belgeyi bulursa kullanıcıdan

[19] IPFS, Gezegenler Arası Dosya Sistemi olarak tanımlanır. Özünde, dosyaları depolayabilen ve zaman içindeki sürümleri izleyebilen sürümlü bir dosya sistemidir. Ayrıca dosyaların bir ağ üzerinde nasıl hareket ettiğini tanımlayarak dağıtılmış bir dosya sistemi haline getirir. Bu iki özelliği birleştirerek IPFS, HTTP gibi mevcut internet protokollerini kullanma şeklimizi geliştirir.

blokzincir ağında depolanan belgeye erişmesini ister. Bir kullanıcı bir talep aldığında, belgeye erişmek isteyen kuruluşa işlem kimliği (karma değeri alınmış) gönderir. Kuruluş, işlem kimliği ile blokzincir ağında sorgulama yapar. Sorgulama doğrulanırsa, karması alınmış belge alınır. Bu durumda, IPFS sisteminde depolanan şifreli belgenin şifresini çözebilir ve istenen dosyayı indirebilir. Önerilen sistemde, güvenli belge yüklenmesini sağlamak için Firebase veri tabanı ve blokzincir tabanlı akıllı sözleşme kullanılır.



Şekil 4. 3 Kişisel Veri Yönetimi ve Paylaşım Şeması. [62]

Veri erişiminin muhasebeleştirilmesi ve denetlenmesi için verileri somut olarak depolayan bir depolama katmanından ayrıştırılmasına ile ilgili bir sistem benimsenmiştir (bkz: Şekil 4.3) [62]. Blokzincir kullanılarak GDPR uyumlu bir kişisel veri yönetimi platformu için teknik mekanizmalara sahip bir tasarım konseptinin yanı sıra izin verilen bir blokzincir çerçevesi üzerine inşa edilmiş profil yönetim sistemi kullanım senaryosunun ayrıntılı bir uygulaması yapılmıştır. Yapılan tasarımın temel amacı, GDPR'ın yasal gerekliliklerini yerine getirmek için dağıtılmış defter yapısı ve

asimetrik (genel ve özel anahtar çifti) şifreleme özeliklerinden faydalanarak kişisel veri bakımından blokzincir ve akıllı sözleşmenin gelişmekte olan özelliklerini korumaktır [63]. Bu amaçla, bir blokzincir ağı, yeni bir merkezi olmayan erişim belirteci konsepti ile konsolide edilen yetkilendirilmiş bir kimlik doğrulama ve yetkilendirme sunucusu, otomatikleştirilmiş bir erişim kontrol yöneticisi ve bir rol olarak tasarlanmıştır. Zincir dışı bir kaynak sunucusunda saklanan kişisel verilere erişmek isteyen taraflar için değişmez günlük kaydı sistemi önerilmiştir. Ayrıca önerilen tasarım modelini izleyerek, bir kişisel veri yönetimi platformu yalnızca belirlenmiş veri sahiplerin ve kontrolörlerinin izinleri oluşturmasına, güncellemesine ve geri çekmesine izin verilmiştir ve yalnızca yetkili veri işlemcileri ve sahipleri arasında kararlaştırılan ilgili veri kullanım politikasında tanımlanan kurallara uyarak kişisel verileri işleyebilir. Platform yalnızca veri sahibi hakları için mekanizmalar sağlamakla kalmaz, aynı zamanda kişisel veri işlemek ve veri hesap verebilirliğini göstermek için bir veri kontrolör olarak görev yapar. Bir servis sağlayıcı, blokzincir tabanlı kişisel veri yönetimi platformuna dürüstçe katılarak blokzincir ağı tarafından GDPR ile uyumlu olup olmadığını kontrol edebilir. Aksi takdirde, herhangi bir ihlal daha sonra denetim makamları tarafından GDPR uyum soruşturması için kullanılabilecek olan ihlallerin bir kaydı olarak değişmez bir dağıtılmış deftere kaydedilir.

Hyperledger Fabric (HLF)[20] izinli blokzincir çerçevesi üzerine inşa edilen ve veri depolama için dürüst bir kaynak hizmeti ile iş birliği yapan sistemdir. Sosyal ağ servis sağlayıcının, GDPR gerekliliklerıyle tamamen uyumlu olduğu onaylanmıştır. Yapılan öneri sadece GDPR kaynaklı kişisel verilerin değil, aynı zamanda dijital varlıkların yönetiminde de temel bir çözüm ortaya koyulmaktadır.

GDPR'ın 17. Maddesi ile dağıtılmış defterler arasındaki zorlu uzlaşmaya ilişkin farkındalık arttıkça, çeşitli aktörler tarafından verilerin tamamen yok edilmesine yönelik bir dizi teknik alternatif değerlendirildi [55]. Önerilen çözüm, kişinin sahip olduğu özel

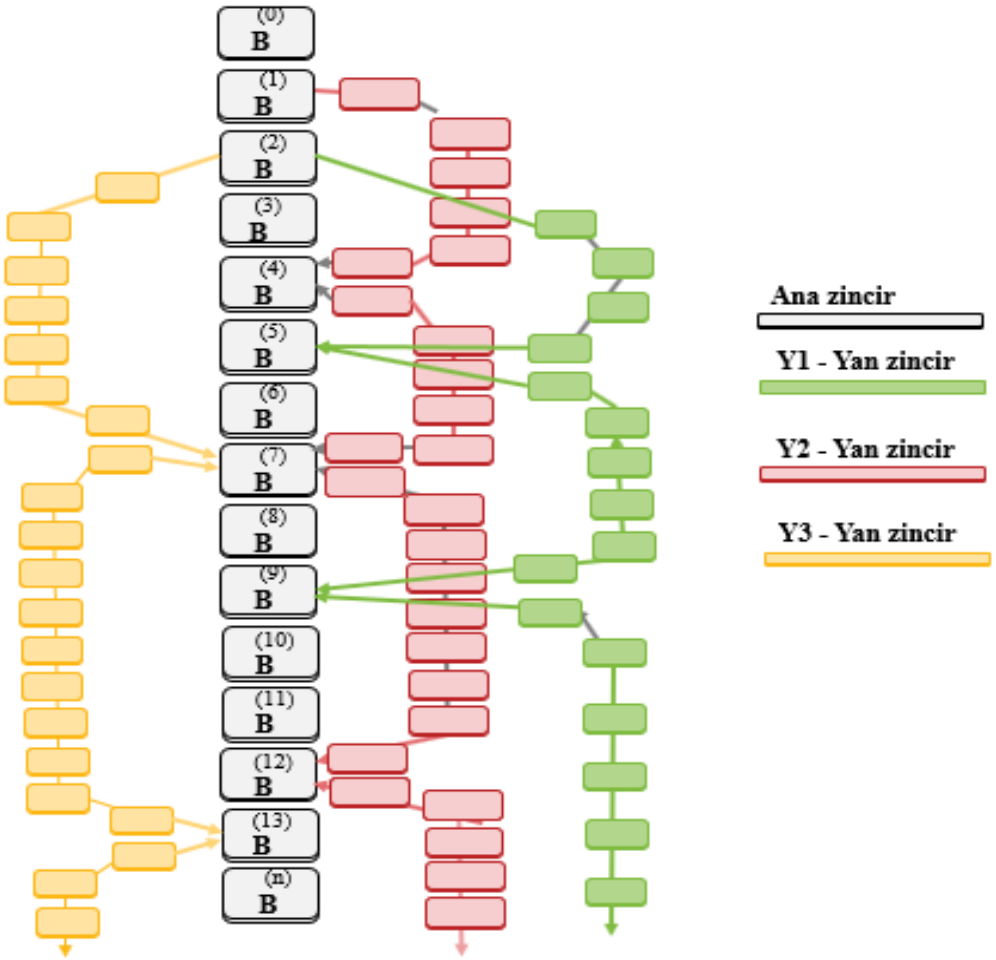
[20] Hyperledger Fabric, modüler bir mimariye sahip uygulamalar veya çözümler geliştirmek için bir temel olarak tasarlanmıştır. Hesap verebilirlik, gizliliği ve şeffaflık korurken geniş ölçekte performans sağlayan benzersiz bir fikir birliği yaklaşımı sunar. Hyperledger blokzincirleri, genellikle izin verilen blokzincirlerdir; bu, her bir tarafın açıkça tanımlandığı ve her işlemin doğrulandığı, yetkilendirildiği, doğrulandığı ve izlendiği anlamına gelir. Hyperledger'ın ana hedefi, iş kullanım durumlarını desteklemek için kurumsal düzeyde, açık kaynak, dağıtılmış defter çerçeveleri ve kod tabanları oluşturmaktır.

anahtarın ortadan kaldırılmasıdır; bu da, genel anahtarla şifrelenmiş bu verilere erişimi zorlaştırır. Bu, Fransız veri koruma otoritesi Commission Nationale de l'Informatique et des Libertés (CNIL) tarafından bu konudaki rehberliğinde öne sürülen çözümdür. CNIL, anahtarlanmış karma fonksiyonunun gizli anahtarının işlenmek üzere saklandığı diğer sistemlerden gelen bilgilerle birlikte silinmesi durumunda silmenin elde edilebileceğini öne sürmüştür. Buna, aynı zamanda budama ve bukalemun karmaları ve sıfır bilgi kanıtı olan redakte edilebilir blokzincir uygulamaları da dâhildir.

Şifreleme anahtarlarının silinmesi önerilmiştir [64]. Kişisel bilgilerin blokzincir ağında tutulması ve veri sahibinin verilerini silinmesi talep etmesi durumunda erişimi imkânsız hale getirmektir. Bu da kişisel verilerin blokzincir ağında tutulan bir kişinin sahip olduğu bilgilerin erişimine onay veren ve kişinin isteğiyle ya da belli bir süre geçtikten sonra silinip ve iptal edilebilen anahtar veya karma ile şifrelenip zaman damgası kullanılarak gerçekleştirilebilir. Bir veri sahibinin blokzincir verilerinin silinmesini talep etmesi durumunda anahtar silinecektir. Bu durum, bilgileri erişilemez hale getirecek ve aslında veriler blokzincir ağında kaybolacaktır. GDPR yetkililerinin bunu bir çözüm olarak kabul edip etmeyecekleri henüz belli değil.

Veri hesabı kabiliyetini ve kaynak takibini desteklemek için blokzincir tabanlı bir yaklaşımın kullanılması önerilmiştir [65]. Veri erişimi ve kullanımı ile ilgili şeffaflığı artıran bir blokzincir ağında dağıtılan kamu tarafından denetlenebilir sözleşmelerin kullanımına dayanmaktadır. GDPR tarafından getirilen gereksinimler ışığındaki odak nokta, konu açısından, öznenin verilerine denetleyiciler tarafından erişildiğinde ve muhtemelen veri işleyicilere iletildiğinde veri hesap verebilirliğini ve kaynak takibini destekleyen çözümlerin eksikliğidir. Denetleyiciler, kişilerin haklarını ihlal etmeden verilere erişilip erişilmediğini, kullanılıp kullanılmadığını ve aktarılıp aktarılmadığını doğrulamak için güvenilir ve şeffaf bir çözüm kullanılarak yetkilendirilmelidir. Platformun tasarım konularını, analizini, iki modelin tasarımını ve uygulamasını gösteriyor. Bunun yerine ikinci modelde, her bir kontrolör, kullanıcıların sözleşmeye katılmasına veya sözleşmeden ayrılmasına izin veren bir ara yüz ile bir blokzincir sözleşmesinde kullanım kontrol politikalarını ifade eder; bir politika şablonları kitaplığından talep üzerine seçilebilen bu politikalar, veri erişimi, kullanım yaşı ve veri işleyicilere aktarım koşullarını ifade eder. Kullanıcı gizliliği, veri sorumluluğu ve veri izleme ayrıntı düzeyi ile ilgili olarak her model, makale boyunca tartışılan farklı

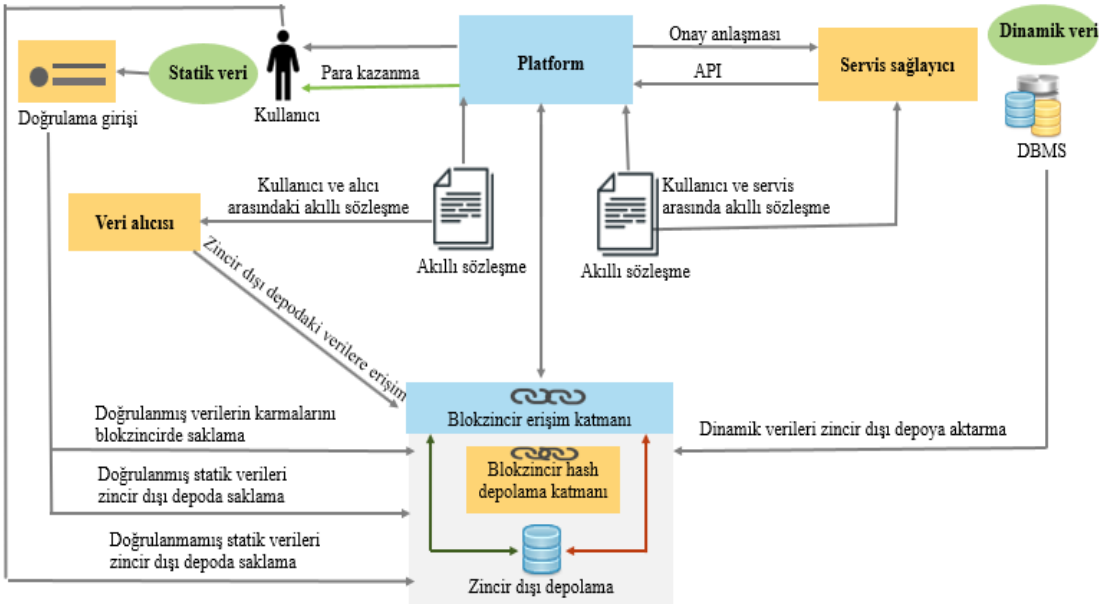
özellikler sağlar. Elde edilen sonuç ise blokzincir tabanlı veri sorumluluğu ve kaynak izleme çözümlerinin tasarım seçimlerinin, uygulanmasının ve performans/ölçeklenebilirlik analizi yapar.



Şekil 4. 4 Ana Zincir Yan Zincir Mimarisi. [19]

Merkezi olmayan eşler arası ağ düğümlerinin toplu katkısıyla işlemlerin onaylanabileceği ve değiştirilebileceği bir blokzincir oluşturma yöntemi öneriliyor [19]. Birkaç yan zincir kullanarak işlem değiştirme sürecini verimli bir şekilde yönetir. Blokzincir ağındaki işlemleri kaydetmek ve yan zincirlerin başlatılması ve sonlandırılmasını kontrol etmek için bir ana zincir kullanılır. Şekil 4.4'te gösterildiği gibi her bir yan zincirin blok madencilik süreci sadece ana zincirden değil, aynı zamanda diğer yan zincirlerden de neredeyse bağımsız olarak ilerler. Blok uzunluğuna ve eş özelliklerine bağlı olarak verimliliği değişebilir. İzin tabanlı yöntemlere göre herhangi bir merkezi otoriteye ve güvene dayalı olmayan bir ortamdaki işlemleri onaylamadaki fikir birliği kolaydır.

Veri sahipleri, işlemlerin zorluk seviyesini seçerek işlem seviyesinde değişiklik yaparak veri sahiplerin işlemlerinin zorluk seviyesini seçmelerine olanak tanır. İşlemin değiştirilmesinin kötü amaçlarla yapılmasını önlemek için çeşitli şifreleme teknikleri kullanılır. Çeşitli şifreleme algoritmaları kullanılarak, işlem değişikliğin kötü amaçlarla yapılması önlenir. Geleneksel blokzincir sistemine benzer bir yapıya sahiptir ve bu yüzden mevcut blokzincir sistemine kolayca uyarlanabilir. 'Düzeltme hakkı' ve 'unutulma hakkı' gibi veri koruma düzenlemelerinin temel taleplerine uygundur.

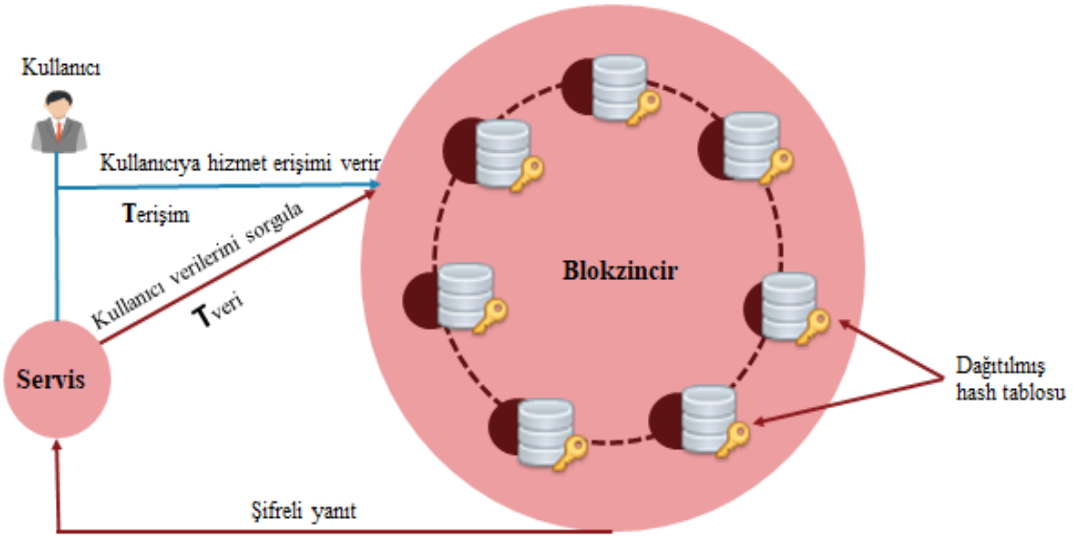


Şekil 4. 5 Blokzincir Tabanlı Kişisel Veri ve Kimlik Yönetim Sistem Mimarisi. [11]

Kullanıcıların kişisel verilerdeki denetlemenin yanında şeffaflığı öne çıkaran bir fikri savunmaktadır [11]. Sistem birkaç bileşen içerir. Bu bileşenler, Şekil 4.5'te gösterildiği gibi akıllı sözleşme, erişim, kimlik, blokzincir platformu, zincir dışı veri deposu ve kullanıcı grafik ara yüzüdür. Statik veri tipi olarak, kullanıcının adı, yaşı ve adresi gibi kişisel bilgilerdir. Kullanıcı, tanımlama işlevini kullanmak veya verilerinin değerini artırmak için verilerini bir kurum tarafından doğrulayabilir. Öte yandan, bir hizmet kullanılırken oluşturulan ve hizmet sağlayıcının kontrolünde olan dinamik veri tipi kullanılabilir. Buradaki ana odak noktası, verilere sahip olmak değil, kullanıcıdan ilgili hizmete ilişkin izinleri kontrol ederek servis sağlayıcıdaki veri akışını kontrol etmektir. Blokzincir, tüm taraflar arasında dağıtılan bir güven ile kişisel veri ekosistemindeki kontrolü kullanıcının eline verme potansiyeline sahiptir. Akıllı sözleşmeler, koşullar değişmez kodunda saklanıp ve yürütüldüğünden, her iki taraftan da düşük maliyetlerle

güven düzeyini artırır. Bununla birlikte, birçok düğümde çoğaltıldığı için blokzincirin üzerinde kişisel verileri depolamak için uygun bir araç olmadığını belirtmek önemlidir.

GDPR kapsamında, blokzincir ağında saklanan veriler silinemediğinden unutulma hakkı zorluğun üstesinden gelmek ve kullanıcıların kişisel verilerini depolamak için zincir dışı depo kullanmayı ve zincir dışı depodaki kişisel verilerin depolama konumuna bir karma veri işaretçisi depolaması önerildi. Bu şekilde, kişiler, GDPR'nin unutulma hakkını kullanmak isterse GDPR'ye uymak için zincir dışı depodaki kişisel veriler silinir ve blokzincir ağında depolanan değişmez karma veri işaretçisi geçersiz olur ve GDPR uyumlu hale gelir. Sistem tasarım yönergelerin genel amacı, kullanıcıya bütünsel kişisel veri yönetim aracı sağlamaktır; bu, sistem kullanıcısının veriler üzerinde tam şeffaflık ve kontrol sağlayacağı anlamına gelir.

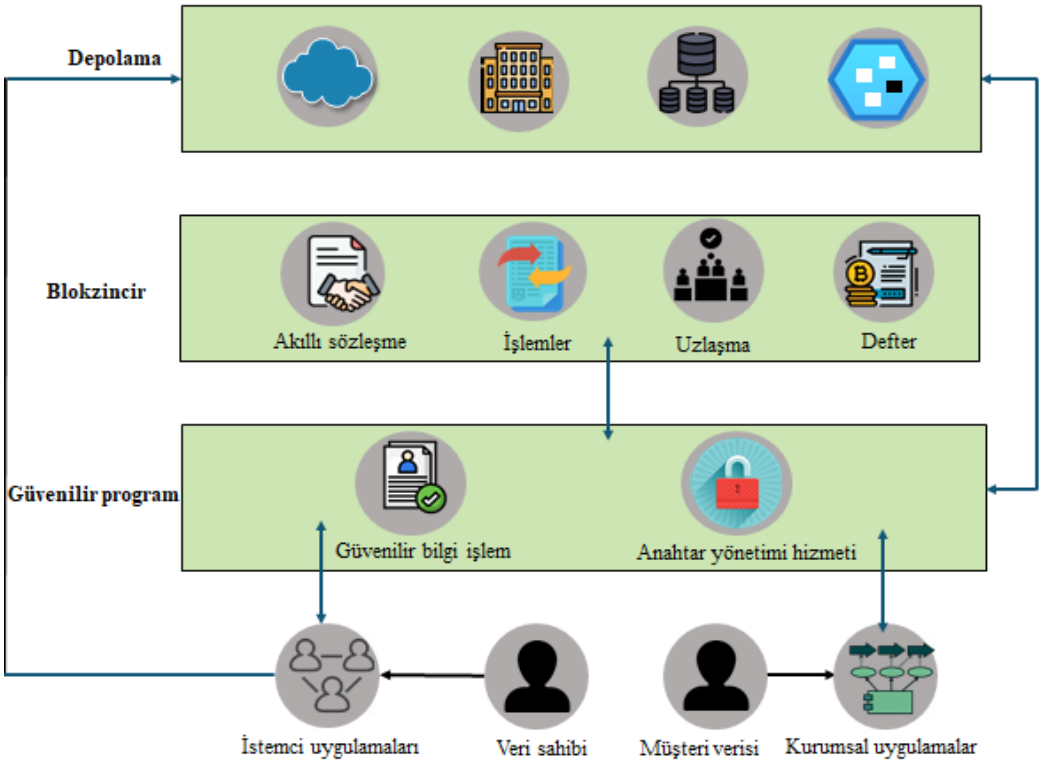


Şekil 4. 6 Merkezi Olmayan Platforma Genel Bakış. [39]

Şekil 4.6.'de gösterildiği gibi mimariyi belirten üç nitelik bulunmaktadır, bunların ilki sitemi kullanan kullanıcılar, diğeri servisler ve son olarak düğümlerdir [39]. Sistemde bulunan kullanıcılar genel olarak anonimdir. Sistem şöyle tasarlanmış: Blokzincir uygulaması iki çeşit operasyonu onaylar: Erişim kontrolü yönetimi için Terişim ve veri ile ilgili işlemler için Tveri kullanılır. Bu tür işlemler mobil uygulamalarında yapılan geliştirmeye kolay bir şekilde entegre edilebilir. Kullanıcı, kendisine ait verilerin gizliliğini sağlamak için bu sistemi kullanan uygulamayı indirir. Kullanıcı sisteme ilk kez kaydolduğunda, kullanıcı için hizmet kimliği oluşturulur ve verilen izinlerle bir Terişim işleminde blokzincir ağına gönderilir. Uygulamadaki kişiye ait veriler (güvenlik

numaraları, IP adresi, ev konumu, ehliyet, kimlik, pasaport vb.) bir anahtar kullanılarak şifrelenir ve bir Tveri aracılığıyla blokzincir sistemine gönderilir, bu blokzincir ağı dışında bir anahtar ve ilgili değere yönlendirilirken anahtar korunur. Hizmet ve kullanıcı, kendisine ait anahtar ile Tveri ile sorgulama yapabilir. Sorgulamadan sonra, dijital imzanın hizmet veya kullanıcıya ait olup olmadığı doğrular. Sağlanan hizmet ile erişim izinleri bakılabilir. Kullanıcı, istediği zaman daha önce kaydedilmiş verilere erişimi iptal etmek için yeni izinle bir Terişim kullanarak izinleri değiştirebilir.

Dağıtılmış karma tablosu, blokzincir uygulamasında okuma/yazma işlemlerin onayı sağlanan bir düğümle korunur. Uygulamada depolanan veriler, düğümlerde gelişigüzel dağıtılır ve kopyası alınır. Bu modelle, verilerin kontrollü kullanıcıdadır. Dijital imzalarla imzalanmış ve birleştirilmiş işlemler, blokzincir uygulamasının âdem-i merkeziyetçilik yapısı ile kötü niyetli düşmanların ağı bozmamasını sağlar. Ağda yalnızca karması alınmış veriler depolandığından, kötü niyetli bir kullanıcı genel defterden herhangi bir şey öğrenemez. Kötü niyetli kullanıcı anahtarlardan birini alırsa (özel veya gizli), ağdaki veriler hala güvendedir. Yalnızca takma isimlendirme ve şifrelemeye dayanan bu yöntem, blokzincirin unutulma (silme) hakkıyla uyumsuzluk sorununu ele alır. Bu çözüm genel olarak işe yarayabilir, ancak GDPR ve KVKK genel yasal gerekliliklere uygunluğu açısından tam olarak yeterli olmayabilir.



Şekil 4. 7 Kullanıcı Kontrollü ve Gizliliği Koruyan Veri Paylaşım Sistemi. [66]

Kişisel verilerin depolanması ve yönetimi için merkezi bir hizmet sağlayıcı güvenli bulunduğundan, verilerin kötü amaçla kullanılması, saldırıya uğraması veya kullanıcının izni olmadan başka bir kurum veya kuruluşa satılması gibi riskleri azaltmak zordur [66]. Ethereum, Blokzincir teknolojisi, zincir dışı veri tutma, şifreleme ve karma değeri alma gibi çözümler bulunmaktadır. Veri denetimine çözüm olarak MultiChain[21] özel izinli blokzincir sistemi önerilmektedir. Kullanıcı verilerin depolanması ve paylaşılması özel MultiChain'de yapılacaktır ve sadece erişim kontrol işlemleri Ethereum'da saklanacaktır. Önerilen bu sistemle kullanıcıya ait kişisel veriler blokzincir ağında depolanmamaktadır. Kullanıcıya ait bu kişisel veriler, zincir dışına depolanmadan önce karması alınır ve çeşitli şifreleme algoritmalarla şifrelenir.

İstemci uygulamalarındaki bu veri sahipleri, verilerini direk zincir dışında depolayabilir (bkz Şekil 4.7). Kullanıcıya ait verilere erişimle şartları ise verilerin karma ve meta

[21] 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, açıklık ve gizlilik sorununu çözer.

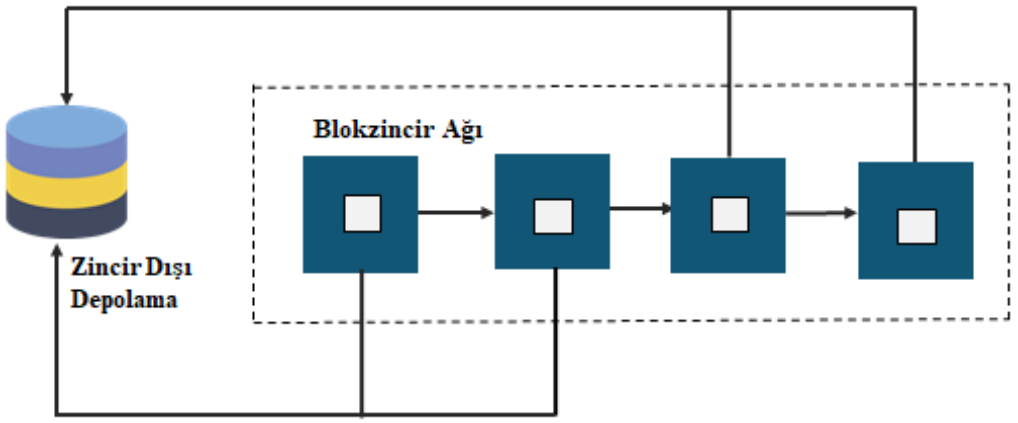
verileri akıllı sözleşmelerde kodlanır ve bir blokzincir sisteminde yayınlanır. Müşteri, kullanıcı ait verilere ulaşmak için akıllı sözleşmeleri kullandığından, sözleşmelerin başarılı olarak başlatılması, şifrelenmiş verilerinin şifresini çözmek için ilgili anahtarın serbest bırakılmasıyla sonuçlanır. Blokzincir uygulamasından karması alınmış verilerin karma değeri çıkarılır ve bu karma değeri zincir dışında depolanan kişisel verileri almak için kullanılır.

Blokzincir uygulaması ve akıllı sözleşmeler, kişilere kimin, ne zaman ve ne gibi amaçlarla verilerine ulaştığı ile ilgili şeffaflık sağlayarak kişilerin veri paylaşımı amacıyla paylaşılabilecek veri türü ve uygulama grupları belirleyerek sistemdeki kullanıcıları destekler. Kullanıcıların isteğiyle yayınlanmış verileri depolamadan ve bant genişliğinden tasarruf sağlayan zincir dışı olarak depolayabilir. Zincir dışında depolanan verilere MultiChain aracılığıyla erişim sağlanır.

5. BLOKZİNCİRDE KİŞİSEL VERİLERİN TUTULMASI TANIMLANAN KAVRAMLAR

Bu bölümde, blokzincir ağında kişisel verileri depolamak için literatürlerde yaygın olarak tanımlanan kavramlar detaylandırıldı. Bunlar, en çok tartışılan kavram olan zincir dışı depolama, değişebilir blokzincir, şifreleme, anahtar silme ve son olarak hukuki tartışmadır.

5.1. Zincir Dışı Depolama



Şekil 5. 1 Zincir Dışı Depolama Mimarisi. [67]

Zincir Dışı Depolama, kişisel verilerin blokzincir ağı üzerinde GDPR uyumlu işlenmesi için gözden geçirilen literatürlerde en çok tartışılan kavramdır. Verilerin "zincir dışı" saklanması, kişisel veya genel olarak faydalı verilerin blokzincir ağı içinde tutulmadığı, ancak dışarıda, örneğin geleneksel bir veri tabanında depolanması anlamına gelir [59]. Gerçek verilerin depolandığı dış depolama konumuna yalnızca bir referans “karma değer” blokzincir ağına kaydedilir [1]. Genel olarak, bir blokzincir ağının dışında daha büyük veri kümelerinin depolanması tavsiye edilir, çünkü bir blokzincir üzerindeki depolama kapasitesi maliyetlidir ve şu anda performans açısından çok iyi değildir.

Ethereum blokzincir uygulamasında bir Gigabyte veri depolamanın maliyetini Gigabyte başına yaklaşık 17.500 Ethereum olarak belirledi. Şekil 5.1’de gösterildiği gibi zincir dışı veriler blokzincir ağının dışında depolanıyor. Bu, genellikle verilerin gizliliğini ve bütünlüğünü garanti eden güvenilir bir üçüncü tarafın yeniden devreye alınması anlamına gelir. Bu durum, blokzincir ilkelerini ihlal ediyor gibi görünse de merkezi bir tarafa belirli bir derecede kontrol sağlamaktadır. Bu nedenle, zincir dışı konum için

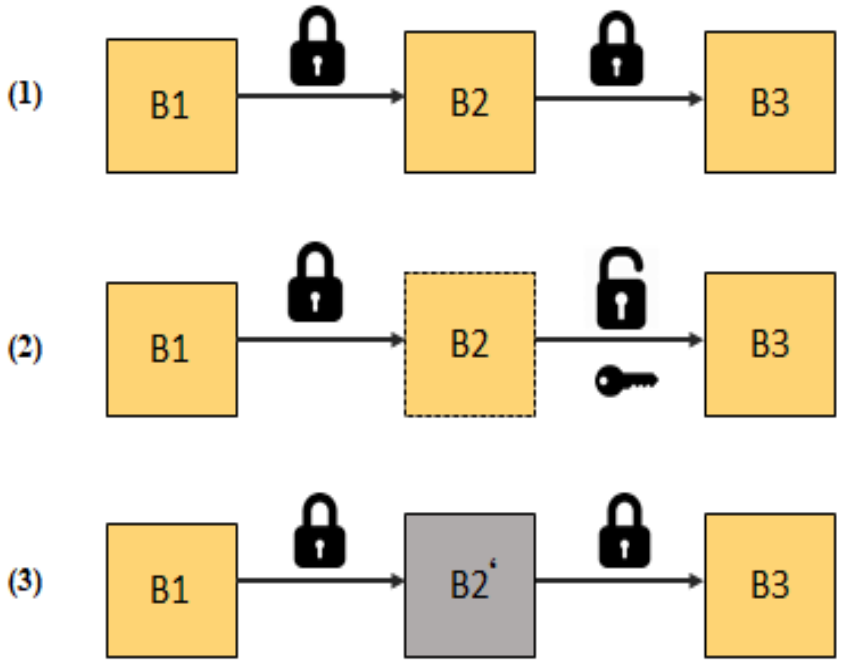
dosyaları adlarına göre değil karma değerlerine göre depolayan, içerik adreslenebilir bir depolama kullanılmasını önermektedir [61]. Bu durumda, veriler artık güvenilir bir şekilde dışarıda tutulabilir, çünkü verilerdeki bir değişiklik karma değerini ve dolayısıyla depolama konumunu değiştirir.

GDPR bağlamında, kişisel verilerin zincir dışında tutulması, ilk bakışta birçok fayda sağlar. Bazı çalışmalarda, bu prosedürle kişisel verinin blokzincir ağında tutulmaması GDPR gerekliliklerinin karşılanabileceğini iddia ediyor [59]. Kişisel verilerin karma değerinin hala zincirde tutulması, referans veya doğruluk kanıtı olarak çalışması mümkündür. Şu anda, kişisel verilerin özet değerlerinin anonim veriler olarak kabul edilebileceği veya daha büyük olasılıkla takma adlı veriler olarak ele alınması gerektiği kesin olarak söylenemez.

5.2. Değiştirilebilir Blokzincir

Düzeltilebilir blokzincir uygulaması üzerinde önceden yazılmış bir veya daha fazla bloğu yeniden yazmak herhangi bir sayıda zaten var olan bloğu daha küçük bir sayıya sıkıştırmak ve mevcut zincire bir veya daha fazla blok eklemek anlamına gelir. İlk başta, temel kavramlarından biri olan blokzincir sistemin değişmezliği ile çelişiyor gibi görünüyor. Ancak, değişmezliğin blokzincir teknolojisine dayalı tüm yeni uygulamalar için uygun olmayacağını savunuyor. Veriler hatalıysa veya kanunen gerekliyse silinebilmelidir [60]. Bir blokzincir uygulamasının değişmezliği, her bloğu öncekine bağlayan kama değerlerinin çarpışma direncinden gelir. Blokzincir uygulamasını değişebilir kılmak için konsept, "bukalemun karma fonksiyonu" [22]olarak adlandırılan özel bir formdan yararlanır [60]. Bir bukalemun karma fonksiyonu, çarpışma oluşturmak için kullanılabilecek bir trapdoor gibi bir şeye sahip olması farkıyla diğer herhangi bir karma fonksiyonu gibi çalışır.

[22] Bir bukalemun karma değeri, bir genel anahtarın mevcudiyetiyle belirli bir karma fonksiyon tipidir. Bukalemun karma işlevleri, ortak anahtarın bilgisinin bir tarafın karma işlevini hesaplamasına izin verecek şekilde yapılandırılır. Buna karşılık, trapdoor bilgisi, verilen her girdi için bir çarpışma bulma sürecini çok daha basit hale getirir.



Şekil 5. 2 Düzeltilebilir Blokzincir İlkeleri. [67]

Şekil 5.2'de gösterildiği gibi değişebilir blokzincir üç farklı aşamayı sunar. (1)'de, değişebilir blokzincir diğer herhangi bir blokzincir gibi davranır ve tüm kilitler güvenli olduğundan hiçbir değişiklik yapılamaz. (2)'de B2 ve B3 arasındaki bağlantı gizli anahtarla açılır ve değişiklik yapılabilir. (3)'te B2'deki değişiklikler tamamlanır ve B2' bloğu şeklinde sonuçlanır. B2' ve B3 arasındaki bağlantı tekrar kilitlenir ve artık değişiklik yapılması mümkün değildir.

Hash fonksiyonunun kilidinin anahtarı kaybolduğunda veya yok edildiğinde blokları değiştirmenin mümkün olmadığını ve blokzincirin tekrar değişmez olduğunu fark etmek önemlidir.

Analiz edilen literatürde, değişebilir blokzincir konseptinin blokzincir ve GDPR çatışması bağlamında potansiyel kullanımını belirlendi. Kişisel verileri içeren blokları doğrudan kaldırma fikri birçok sorunu çözecektir. Bununla birlikte, kavram aynı zamanda bazı sorunlarla da karşı karşıyadır. İlk olarak, mevcut bir blokzincir uygulamasına yeniden düzenlenebilirlik eklemek mümkün değildir. Bu, konsept için kararın ağ kurulmadan önce verilmesi gerekir [59]. İkincisi, blokzincirin eski kopyaları yine de düzeltilmiş verileri içerecektir [60]. Son olarak, bir tarafın blokzincir sistemini kendi lehine düzenlemesi riski her zaman vardır. GDPR bağlamında, bu kavram, kişisel

verilerin blokzincir ağında saklanması ile veri gizliliği düzenlemesi arasındaki çatışma sorunlarını çözüyor gibi görünüyor. Zincir üzerinde depolandıktan sonra verileri silme veya değiştirme yeteneği büyük bir avantajdır. Blokzincir ağındaki tüm katılımcıların GDPR'ye uygun olarak çalıştığından emin olunmalıdır, bu da blokzincir uygulamasına yönelik düzeltmelerin derhal gerçekleştirildiği ve eski kopyaların güvenilir bir şekilde silindiği anlamına gelir. Bu özellik, harici bir tarafça denetlenebilir.

5.3. Hukuki Tartışma

Hukuki tartışma, bu yönetmeliğin bazı bölümlerinin kesin olmayan tanımıyla ilgilenir. Blokzincir teknolojisinin değişmezliği nedeniyle blokzincir ağında depolanan kişisel verileri silmek gerçek bir zorluktur. Blokzincirin düzgün çalışması için kalıcı bir zincire ihtiyaç duyması nedeniyle, zincir üzerinde depolanan kişisel verilerin işlenmesi için gerekli olduğunu iddia etmek mümkün olabilir. Dolayısıyla veri sahibinin unutulma hakkı burada uygulanamaz. Tüm bu yasal tartışmalar şu anda ihtiyatlı bir şekilde ele alınmalıdır. Bu alandaki yargıların eksikliği nedeniyle bu kavram gri bir alanda işliyor. Bu özelliklerin gelecekte bir mahkeme tarafından yasadışı olarak kabul edilmesi çok muhtemeldir. Bu durumda, kanunen gerekli olsa bile mevcut bir blokzincir uygulamasından kişisel verilerin tutulması mümkün değildir.

5.4. Şifreleme ve Anahtar Silme

Şifreleme ve Anahtar Silme literatür taraması sırasında tanımlanan son kavram. GDPR uyumluluğuna ulaşmak için bir blokzincir üzerindeki verilerin şifrelenmesi ile ilgilidir. Bazı araştırmalarda, bir blokzincir uygulaması üzerinde depolanan verilerin şifrelenmesini ve silinmesi gerektiğinde şifreleme anahtarını basitçe imha edilmesi önerilmektedir [58], [59]. Bu konseptle, şifreleme anahtarı artık mevcut olmadığından verilere erişilemez hale geliyor. Bu durumda, verilerin ağda silindiği varsayılıyor. GDPR açısından, bu kavram eleştirel olarak görülmelidir. İlk olarak, bugünün şifreleme algoritmalarının gelecekte artık güvenli kabul edilmemesi mümkündür, bu nedenle orijinal şifreleme anahtarı bilgisi olmadan verilerin şifresini çözmek mümkün olabilir. Şifrelemenin yalnızca belirli bir süre boyunca gizliliği garanti ettiğini, ancak anonimleştirmenin süresiz olarak sürmesi gerektiğini belirtmek önemlidir.

Tablo 5.1’de gösterildiği gibi çalışmada tartışılan kavramlara genel bir bakış sağlar ve

her bir kavramın avantaj ve dezavantajları özetlenmektedir.

Tablo 5. 1 Tanımlanan Kavramların Avantajları ve Dezavantajları. [67]

Konsept	Avantajları	Dezavantajları
• **Zincir Dışı Depolama**	• Kişisel veriler zincir dışında saklanır • Yalnızca zincir dışı depolama konumuna bir referans ve verilerin karması zincir üzerinde tutulur • Büyük verilerin işlenmesini sağlar	• Bir TTP'nin e-girişini gerektirebilir • Kişisel verilerin zincir dışında saklanma şekline bağlı olarak, zincirdeki karma, kişisel veriler olarak ele alınmalıdır. • Verilerin tutulduğu yere bağlı olarak büyük teknik değişiklikler gerektirebilir
• **Düzeltilebilir Blokincir**	• Kişisel verileri doğrudan blokzincir üzerinde değiştirmenin ve silmenin bir yolunu sunar • Blokzincirin kullanım şeklinde bir değişiklik gerektirmez	• Teknik uyarlamalar gerektirir • Düzeltilebilirlik mevcut bir blokzincire eklenemez • Gizli anahtar kaybolursa blokzincir değişmez kalır • Düzeltilmiş blokların eski kopyalarını silmek için düğümler gerekir • Düğümler bu özelliği kendi lehlerine kötüye kullanabilir • Büyük veriler için zincir dışı depolama gerektirebilir
• **Hukuki Argümanlar**	• Blokzincir teknolojisinde herhangi bir değişiklik gerekli değil • Artık kullanılmayan veriler yeni bir işlemle geçersiz kılınabilir	• Yasal gri alanda çalıştığı için konsept çok dikkatli ele alınmalıdır. • Yargı, bu kavramın GDPR ile uyumlu olmadığını beyan edebilir • Büyük veriler için zincir dışı depolama gerektirebilir
• **Şifreleme ve Anahtar Silme**	• Blokzincir teknolojisinde herhangi bir değişiklik gerekli değil • Zincirdeki veriler şifreli olarak saklanır • Verilerin blokzincirden kaldırılması gerektiğinde, şifreleme anahtarı basitçe yok edilir	• GDPR uyumluluğu için ana kavram olarak kullanılmamalıdır • Şifrelenmiş kişisel veriler, takma adlı veriler olarak ele alınmalıdır • Güncel teknolojinin kullanımı ile gelecekte verilerin şifresini çözebilir • Yargı, bu kavramın GDPR ile uyumlu olmadığını beyan edebilir • Büyük veriler için zincir dışı depolama gerektirebilir

6. SONUÇ

Araştırmada, yapılandırılmış bir literatür taraması yapıldı ve akademik literatürde ve uygulayıcı kaynaklarında blokzincir kullanarak kişisel verilerin GDPR ve KVKK uygunluğu ile ilgili mevcut potansiyel kavramlar açıklandı. İncelenen literatürlerde en çok tartışılan kavram zincir dışı depolamadır. Bu konseptle, kişisel veriler blokzincir ağının dışında tutulur ve blokzincir ağında ise zincir dışındaki konuma atıfta bulunur. Sorun şu ki, çoğu durumda verilerin özeti şeklinde bir "doğruluk kanıtı" zincirde tutulur ve karma veriler kişisel veriler de olabilir. Bu kavram pratikte zaten uygulanmaktadır.

Tanımlanan ikinci kavram olan değişebilir blokzincir, bir bloğun ilgili karmasını değiştirmeden verinin değiştirilmesine izin veren özel bir karma algoritmadan yararlanır. Bu, blokzincir üzerindeki verilerin değiştirilmesini ve silinmesini sağlar ve KVKK ve GDPR'nin gereklilikleri açısından çok ilginç bir çözümdür. Olumsuz tarafı, bu kavram genellikle temel özelliklerinden biri olan blokzincir sistemin değişmezliğinin ihlali olarak eleştirilir.

Bir sonraki kavram olan hukuki tartışmalardır. Bir yandan unutulma hakkının mutlak bir hak olmadığı ve blokzincire eskisini geçersiz kılan yeni bir işlem eklenerek blokzincir uygulaması üzerindeki verilerin değiştirilebileceği veya silinebileceği iddia edilirken, öte yandan blokzincirin düzgün çalışması için tutarlı veri işlemenin gerekli olduğunu iddia edilmektedir.

Son konsept olan Şifreleme ve Anahtar Silme, kişisel verilerin blokzincir ağında depolanmadan önce şifrelenmesi ve anahtarın ayrı olarak saklanması tekniğidir. Depolanan bu veriler artık gerekli değilse şifreleme anahtarı basitçe silinir ve bu nedenle verilere artık erişilemez. Bu yöntemin ana eleştirisi, yakın gelecekte şifre çözme anahtarına ihtiyaç duymadan verilerin şifresinin çözülmesinin mümkün olabileceği ve verilere tekrar erişilebilir olmasıdır. Genel olarak, şu anda kişisel verilerin bir genel blokzincir ağında saklanmaması şiddetle tavsiye edilmektedir. Kişisel veriler bir genel blokzincir ağında saklandıysa verilerin KVKK ve GDPR'nin bölgesel kapsamında kalması garanti edilemez ve kişisel verilerin üçüncü ülkelere aktarılması ilkeleri ihlal edilebilir. Hukuki tartışma kavramı gri alanda hareket eder ve bu nedenle bu yöntemin yasadışı ilan edilmesi her zaman mümkündür. Kişisel veriler blokzincir var olduğu sürece blokzincir üzerinde şifrelenmiş halde kalır. Şifre çözme anahtarı yok

edilse bile, veriler şu anda kişisel veri olarak sayılır.

Görünüşe göre yalnızca zincir dışı depolama ve değişebilir blokzincir kavramları veri koruma düzenlemeleri kapsamında uyumlu işlemeyi garanti edebilir. Zincir dışı depolama modeli kullanılırken genellikle "doğruluk kanıtı" olarak zincirde kalan karma değerinin yeniden hesaplanmasının mümkün olmadığına dikkat edilmelidir. Değişebilir blokzincir modelin uygulanması gerekiyorsa gizli anahtarın çok güvenli bir şekilde yönetilmesi önemlidir. Anahtar kaybolursa blokzincir ağında depolanan verileri yeniden düzenlemek mümkün değildir.

Avrupa Birliği (AB) özelinde GDPR ve Türkiye özelinde KVKK, kişilerin başta sosyal medya olmak üzere kamu hizmetlerinde (sağlık, bankacılık, vb.) ve diğer çeşitli işlemler boyunca dijital ortamda bıraktıkları her türlü veri ve bilginin; kişilik haklarını 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 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, yaş, e-posta, cep telefonu numarası ve konum gibi çeşitli kişisel bilgilerin ele geçirildiği bilinmektedir. Yetkili otoriteler tarafından yapılan teknik ve idari incelemelerde 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 hassasiyet ve güvenliği 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.

7. KAYNAKLAR/REFERENCES

[1] Zyskind, G., Nathan, O., Pentland, A.S. (2015) Decentralizing Privacy: Using Blockchain to Protect Personal Data, *IEEE Security and Privacy Workshops*, ss.180-184. DOI: 10.1109/SPW.2015.27.

[2] Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025, 7 Hazian 2021, https://www.statista.com/statistics/871513/worldwide-data-created/ Erişim Tarihi: 07.01.2021

[3] Sim, W.L., Chua, H.N., Tahir, M. (2019) BlockChain: Blockchain for Identity Management: The Implications to Personal Data Protection, *IEEE Conference on Application, Information and Network Security (AINS)*. DOI: 10.1109/AINS47559.2019.8968708.

[4] Halpin, H., Piekarska, M. (2019) Introduction to Security and Privacy on the Blockchain, *ACM Computing Surveys*, Article No: 51. https://hal.inria.fr/hal-01673293/document Erişim Tarihi: 28.04.2021.

[5] Cadwalladr, C., Graham-Harrison, E. (2018) 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, The Guardian. https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=5833&context=libphilprac Erişim Tarihi: 05.06.2021.

[6] Zou, Y., Mhaidli, A. H., McCall, A., Schaub, F. (2018) "*I have got nothing to lose": Consumers' risk perceptions and protective actions after the equifax data breach, In: Fourteenth Symposium on Usable Privacy and Security*, ss.197–216. https://www.usenix.org/system/files/conference/soups2018/soups2018-zou.pdf Erişim Tarihi: 01.06.2021.

[7] Stephen, S., Alex, A. (2018) A Review on BlockChain Security, *IOP Conf. Ser.: Mater. Sci. Eng*. 396 012030. DOI:10.1088/1757-899X/396/1/012030.

[8] Eugdpr (2019). Information Portal, https://eugdpr.org/ Erişim Tarihi: 03.03.2021.

[9] Barati, M., Rana, O., Petri, I., Theodorakopouls, G. (2020) GDPR Compliance Verification in Internet of Things. DOI: 10.1109/ACCESS.2020.3005509.

[10] Iredale, G. (2020) History Of Blockchain Technology: A Detailed Guide, 3 Kasım 2020, http://101blockchains.com/history-of-blockchain-timeline/ Erişim Tarihi: 03.11.2020.

[11] Faber, B., Michelet, G., Weidmann, N., Mukkamala, R.R., Vatrapu, R. (2019) BPDIMS: A Blockchain-based Personal Data and Identity Management System, *In proceedings of the 52nd Hawaii International Conference on System Sciences*. DOI:10.24251/HICSS.2019.821.

[12] Vurgun, Ş., Akpınar, M.G. (2020) Blokzincir Teknolojisi ve Unutulma Hakkı Blockchain Technology and Right To Be Forgotten, 13, 74. https://www.sosyalarastirmalar.com/articles/blokchain-technology-and-right-to-be-

forgotten.pdf Erişim Tarihi: 28.04.2021.

[13] What is Blockchain?, 17 Ekim 2019, https://blockchainhub.net/blockchain-intro/ Erişim Tarihi: 01.04.2021.

[14] Türkiye Bilişim Vakfı (2019) Kişisel Verilerin Korunması Hukuku ve Blokzinciri Teknoloisi Raporu, Kasım 2019. https://bctr.org/dokumanlar/KVKK_ve_Blokzincir_Teknolojisi.pdf Erişim Tarihi: 12.05.2021.

[15] Investopedia (2020) What is Blockchain? https://www.investopedia.com/terms/b/blockchain.asp, Erişim Tarihi: 04.10.2021.

[16] Appinventiv (2020) Blockchain vs. Traditional Database: What Should Be a Startup's Choice, 22 Eylül 2020, https://appinventiv.com/blog/traditional-database-vs-blockchain/ Erişim Tarihi: 14.07.2021.

[17] Ali, S., Wang, G., White, B., Cottrell, R.L. (2018) A Blockchain-based Decentralized Data Storage and Access Framework for PingER. *17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering.* DOI: 10.1109/TrustCom/BigDataSE.2018.00179

[18] Merkle, R. C. (1980) *"Protocols for public key cryptosystems",* in Security and Privacy, 1980 IEEE Symposium on, pp. 122–122, IEEE. DOI: 10.1109/SP.1980.10006.

[19] Lee, D., Park, N. (2020) Blockchain based privacy preserving multimedia intelligent video surveillance using secure Merkle tree," *Multimedia Tools and Applications*, pp. 1–18. DOI: https://doi.org/10.1007/s11042-020-08776-y.

[20] Johnson, D., Menezes, A., Vanstone, S. (2001) The elliptic curve digital signature algorithm (ECDSA). *International Journal of Information Security*, volume 1, ss.36–63 (2001). DOI: https://doi.org/10.1007/s102070100002.

[21] Shaban, M. (2019) Blockchain-based platforms for genomic data sharing: a de-centralized approach in response to the governance problems? *Journal of the American Medical Informatics Association*, Volume 26, Issue 1, January 2019, Pages 76–80 DOI: https://doi.org/10.1093/jamia/ocy149.

[22] Tradeix (2018) https://tradeix.com/distributed-ledger-technology/ Erişim Tarihi: 38.07.2021.

[23] Koteska, B., Karafiloski, E., Mishev, A. (2017) Blockchain Implementation Quality Challenges: A Literature Review. http://ceur-ws.org/Vol-1938/paper-kot.pdf Erişim Tarihi: 27.05.2021.

[24] Nakamoto, S. (2018) Bitcoin: *A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf Erişim Tarihi: 11.05.2021.

[25] Taskinsoy, J. (2019) Blockchain: A Misunderstood Digital Revolution. Things You Need to Know about Blockchain.

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3466480 (Erişim Tarihi: 15.04.2021.

[26] Lin, I.C. ve Liao, Z.C. (2017) A Survey of Blockchain Security Issues and Challenges, *International Journal of Network Security*, 19 (5), ss.653-659.

[27] Akleylek, S., Seyhan, K. (2018) Blok Zinciri Bileşenleri ve Uygulamaları Üzerine Bir Derleme. DOI: 10.25045/NCInfoSec.2018.05.

[28] Soohyeong, K., Kwon, Y., Cho, S. (2018) A Survey of Scalability Solutions on Blockchain.

[29] Zhang, S., Lee, j.H. (2020) Analysis of the main consensus protocols of blockchain, *ICT Express*, 6(2), ss.93-97. DOI: https://doi.org/10.1016/j.icte.2019.08.001

[30] Lamport, L., Shostak, R., Pease, M. (October 2019) The Byzantine generals problem, *SRI International*, ss.203–226. https://lamport.azurewebsites.net/pubs/byz.pdf Erişim Tarihi: 18.09.2021.

[31] Ahmad, F., Ahmad, Z., Kerrache, C. A., Kurugollu, F., Adnane, A., Barka, E. (2019) Blockchain in internet-of-things: architecture, applications and research directions, International Conference on Computer and Information Sciences (ICCIS), 2019: IEEE, ss. 1- 6. DOI: 10.1109/ICCISCI.2019.8716450.

[32] How do Hard and Soft Forks work?, https://www.bitpanda.com/academy/en/lessons/how-do-hard-and-soft-forks-work/ Erişim Tarihi: 10.04.2021.

[33] Bitcoin's Proof of Work: The problem of the Byzantine Generals, 18 Şubat 2020,

https://medium.com/swlh/bitcoins-proof-of-work-the-problem-of-the-byzantine generals- 33dc4540442, Erişim Tarihi: 09.08.2021

[34] Singh, S.K., Kumar, S. (2021) Blockchain Technology: Introduction, Integration and Security Issues with IoT. https://www.researchgate.net/publication/348802886_Blockchain_Technology_Introduction_Integration_and_Security_Issues_with_IoT Erişim Tarihi: 10.05.2021.

[35] Back A. (2002) *Hashcash denial of service counter measure*, 1 Ağustos 2002, http://www.hashcash.org/ papers/hashcash.pdf Erişim Tarihi: 25.08.2021

[36] BitFury Group, (2015) Proof of stake versus proof of work, 13 Eylül 2015. https://bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf Erişim Tarihi: 21.04.2021.

[37] The DPOS consent system – Delegated proof of stake, 21.Temuz 2019. https://www.cripto51.com/en/2019/07/21/the-dpos-consent-system-delegate-proof-of-stake/ Erişim Tarihi: 10.07.2021.

[38] Larimer, D. (2014) Delegated proof-of-stake (dpos), Bitshare whitepaper, https://how.bitshares.works/en/master/technology/dpos.html Erişim Tarihi: 07.05.2021.

[39] Fu, D., Fang, L. (2016) Blockchain-based Trusted Computing in Social Network.

DOI: 10.1109/CompComm.2016.7924656.

[40] Yuan, Y., Wang, F. (April 2016) Blockchain: The State of the Art and Future Trends, Acta Automatica Sinica, vol. 42, no.4, ss.481-494.

[41] ASC X9 (2018) Study Group Report Distributed Ledger and Blockchain Technology Study Group, April 6, 2018. https://x9.org/wp-content/uploads/2018/04/Distributed-Ledger-and-Blockchain-Technology-Study-Group-Report-FINAL.pdf Erişim Tarihi: 07.06.2021.

[42] Velliangiri, Dr.S., Karthikeyan, Dr.P. (2020) Blockchain Technology: Challenges and Security issues in Consensus algorithm. DOI: 10.1109/ICCCI48352.2020.9104132.

[43] Bernade, J.B., Canovas, J.L., Jose, L. Hermandez-Ramos, J.L., Moreno, R.T., Skarmeta, A. (2019) Privacy-Preserving Solutions for Blockchain: Review and Challenges. *IEEE Access*, 7, 164908-164940, DOI: 10.1109/ACCESS.2019.2950872.

[44] Yun, X., Wen, W., Lang, B., Yan, H., Ding, L., Li, J., Zhou, Y. (2018) Communications in Computer and Information Science.

[45] Lin, X. (2017) *"Semi-centralized Blockchain Smart Contracts: Centralized Verification and Smart Computing under Chains in the Ethereum Blockchain"*, Taiwan, R.O.C.:Department of Information Engineering, National Taiwan University.

[46] Destefanis, G., Marchesi, M., Ortu, M., Tonelli, R., Bracciali, A., Hierons, R. (2018) Smart Contracts Vulnerabilities: A Call for Blockchain Software Engineering? DOI:10.1109/IWBOSE.2018.8327567.

[47] He, B. (2017) *"An Empirical Study of Online Shopping Using Blockchain Technology"*, Taiwan, R.O.C. :Department of Distribution Management, Takming University of Science and Technology.

[48] Miyaji, A. (1994) Elliptic Curves Suitable for Cryptosystems. *Ieice Transactions on Fundamentals of Electronics Communications & Computer Sciences*, 77, ss.98-105. https://www.researchgate.net/publication/29681815_On_Secure_and_Fast_Elliptic_Curve_Cryptosystems_over_F_p Eişim Tarihi: 26.09.2021.

[49] He, P., Yu, G., Zhang, Y.F. (2017) Prospective Review of Blockchain Technology and Application. *Computer Science*, 44, ss:1-7.

[50] Article 29 (2007) Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 20 June, 01248/07/EN, WP 136. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp131_en.pdf Erişim: Tarihi: 17.06.2021.

[51] Blockchain and GDPR, 16 Kasım 2020. https://block.co/blockchain-and-gdpr/ Erişim Tarihi: 14.06.2021.

[52] Information Commissioner's Office (2020) *"Individual rights: Right to be*

informed", Guide to the General Data Protection Regulation (GDPR), accessed June 1.

[53] Blockchain and the GDPR: Can the conflicts be resolved?, Ağustos 2020 https://compliancecosmos.org/blockchain-and-gdpr-can-conflicts-be-resolved Erişim Tarihi: 12.05.2021.

[54] Team, I. P. (2017) EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide, Cambridge, U.K.:IT Governance. https://www.itgovernanceusa.com/download/EU-GDPR-Implementation-and-Compliance-Guide.pdf Erişim Tarihi: 18.07.2021.

[55] EPRS (2019) Blockchain and the General Data Protection Regulation, Can distributed ledgers be squared with European data protection law? https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf Erişim Tarihi: 13.12.2020.

[56] Wirth, C., Kolain, M. (2018) Privacy by BlockChain Design: A Blockchain-enabled GDPR-compliant Approach for Handling Personal Data. DOI: http://dx.doi.org/10.18420/blockchain2018_03.

[57] Zheng, X., Mukkamala, R., Vatrapu, R., Ordieres-Mere, J. (2018) Blockchain-based Personal Health Data Sharing System Using Cloud Storage. DOI: 10.1109/HealthCom.2018.8531125.

[58] Pagallo, U., Bassi, E., Crepaldi, M., Durante, M. (2018) *"Chronicle of a Clash Foretold: Blockchains and the GDPR's Right to Erasure,"* in Legal Knowledge and Information Systems: JURIX 2018: *The Thirty-first Annual Conference*, 2018, vol. 313, p. 81: IOS Press. DOI: 10.3233/978-1-61499-935-5-81.

[59] Ibáñez, L.D., O'Hara, K., Simperi, E. (2018) On Blockchains and the General Data Protection Regulation, *University of Southampton*. https://eprints.soton.ac.uk/422879/1/BLockchains_GDPR_4.pdf Erişim Tarihi: 28.07.2021.

[60] Ateniese, G., Magri, B., Venturi, D., Andrade, E. (2017) Redactable Blockchain–or–rewriting History in Bitcoin and Friends. Security and Privacy (EuroS&P), *IEEE European Symposium*. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7961975 Erişim Tarihi: 26.05.2021.

[61] Desai, S., Shelke, R., Deshmukh, O., Choudhary, H., Sambare, S.S. (2020) Blockchain based secure data storage and access control system using IPFS, *Journal of Critical Reviews*, 7(19), 1254-1260, DOI: 10.1109/ICCUBEA47591.2019.9129015.

[62] Truong, N.B., Sun, K., Lee, G.M., Yike Guo, Y. (2019) GDPR-Compliant Personal Data Management: A Blockchain-based Solution. DOI: 10.1109/TIFS.2019.2948287.

[63] Walport, M. (2016) *"Distributed ledger technology: Beyond blockchain*," UK Government Office for Science, vol. 1.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf Erişim Tarihi: 08.06.2021.

[64] Blockchain versus GDPR and who should adjust most, 9 Ekim 2018, https://www.finextra.com/blogposting/16102/blockchain-versus-gdpr-and-who-should-adjust-most Erişim Tarihi: 02.04.2021.

[65] 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, DOI: 10.1145/3098954.3098958.

[66] Shrestha, A.K., Vassileva, J., Deters, R. (2020) A Blockchain Platform for User Data. DOI: https://doi.org/10.3389/fbloc.2020.497985.

[67] Zemler, F. (2019) Concepts for GDPR-Compliant Processing of Personal Data on Blockchain. https://www.researchgate.net/publication/338117615_Concepts_for_GDPR-Compliant_Processing_of_Personal_Data_on_Blockchain_A_Literature_Review Erişim Tarihi: 10.05.2021.

[68] What is Decentralization in Blockchain? https://aws.amazon.com/tr/blockchain/decentralization-in-blockchain/ Erişim Tarihi: 10.09.2021.

[69] Atlam, H. F., Alenezi, A., Alassafi, M.O. (2018) Wills, G.B., Blockchain with Internet of Things: Benefits, Challenges, and Future Directions DOI: 10.5815/ijisa.2018.06.05.

[70] Massias, H., Avila, X. S. & Quisquater, J-J. (1999) Design of a Secure Timestamping Service with Minimal Trust Requirements. *In 20th Symposium on Information Theory in the Benelux*.

8. ÖZGEÇMİŞ

2008 yılında Yunus Emre Lisesinde Fen Bilimleri alanında okudum ve 85 not ortalamasıyla 2011 yılında mezun oldum. Son olarak 2012 yılında lisans eğitimine başladığım Yıldırım Beyazıt Üniversitesi Fen Bilimleri Fakültesi Bilgisayar Mühendisliği (İngilizce) bölümünden 2017 yılında 3,08 not ortalamasıyla mezun oldum.

2017 yılında Document Intelligence Traffic Information Systems (Netbeans Java, NoSQL Apache Cassandra, MySQL) başlıklı lisans bitirme tezini hazırladım. 2015 yılında Krizma Bilgisayar Yazılım Sistemleri San. Tic. Ltd. Şti. 7 aylık staj yaptım. Staj süresince T.C. Ministry of Health Turkey Organs Tissues Information System ve Student Information System (Student Automation) (asp.net Visual Studio) projelerinde geliştirme yaptım. 2016 yılında Minova Technology GmbH staj yaptım. Staj süresince Featured mitrack-V Advanced Telemetry Tracking Device pojesinde geliştirme yaptım (PhP, Node.js, WAMP Server, MySQL). 2018 yılında TÜBİTAK BİLGEM UEKAE bünyesinde yazılım geliştirme mühendisi olarak işe başladım. Projelerde Java ile Netbeans Platform swing ui uygulamaları ve sunucular için api kodları geliştirdim. Java dili kullanarak Netbeans platform altyapısı ile İstemci ve Yönetici uygulamalarını geliştirdim. 2020 yılında Marmara Üniversitesi Fen Bilimleri Enstitüsü Bilgi Güvenliği Mühendisliği Tezli yüksek lisans eğitimini aldım. Yüksek lisans tezimi Blokzincir Uygulamasında Kişisel Verilerin Tutulması üzerine yaptım.