
RTÜK
RADYO VE TELEVİZYON ÜST KURULU

T.C.

RADYO VE TELEVİZYON ÜST KURULU

KAMU SEKTÖRÜNDE VERİ GÜVENLİĞİNİN SAĞLANMASINDA BLOK ZİNCİRİ (BLOCKCHAIN) TEKNOLOJİSİ KULLANIMI VE RTÜK İNCELEMESİ

UZMANLIK TEZİ

ENES ÇELİKER

DANIŞMAN: ÜST KURUL UZMANI ŞAHİN COŞKUN

ANKARA

TEMMUZ, 2023

Radyo ve Televizyon Üst Kurulu Başkanlığına,

Enes Çeliker adlı Üst Kurul Uzman Yardımcısının hazırladığı "Kamu Sektöründe Veri Güvenliğinin Sağlanmasında Blok Zinciri (Blockchain) Teknolojisi Kullanımı ve RTÜK İncelemesi" başlıklı bu çalışma, Tez Değerlendirme Komisyonu tarafından oy birliği/ oy çokluğu ile **Uzmanlık Tezi** olarak kabul edilmiştir.

Komisyon Üyeleri	İmza
Başkan :	
Üye :	
Üye :	
Üye :	
Üye :	

ONAY

Bu tez Radyo ve Televizyon Üst Kurulu Uzmanlığı Yönetmeliği'nin ilgili maddeleri uyarıca …./…./20…. tarihinde kabul edilmiştir.

Ebubekir ŞAHİN

Üst Kurul Başkanı

ETİK İLKELERE UYGUNLUK BEYANI

Bu tez çalışmasında;

Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,

Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,

Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,

Kullanılan verilerde ve ortaya çıkan sonuçlarda herhangi bir değişiklik yapmadığımı,

Sunduğum çalışmanın özgün olduğunu bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim. …./…./.20….

Enes ÇELİKER

Üst Kurul Uzman Yardımcısı

İTHAF

Bu tez, hayatımın her anında desteklerini üzerimde hissettiğim sevgili anneme ve eşime ithaf edilmiştir.

TEŞEKKÜR

"Kamu Sektöründe Veri Güvenliğinin Sağlanmasında Blok Zinciri (Blockchain) Teknolojisi Kullanımı ve RTÜK İncelemesi" isimli bu tezin konusunun belirlenmesinden kaynakların toplanmasına kadar her aşamada bilgi ve tecrübelerini paylaşan Üst Kurul Uzmanı Şahin COŞKUN'a, tez hazırlığı sürecinde üzerimdeki iş yükünü hafifleten Üst Kurul Uzmanı Sayın Orhan GÜMÜŞSOY'a, idarecilerim Daire Başkan Yardımcısı İbrahim ESER ve Daire Başkanı Olcay ÇİÇEKLİTAŞ'a teşekkürlerimi sunarım.

ÖZET

KAMU SEKTÖRÜNDE VERİ GÜVENLİĞİNİN SAĞLANMASINDA BLOK ZİNCİRİ (BLOCKCHAIN) TEKNOLOJİSİ KULLANIMI VE RTÜK İNCELEMESİ

ÇELİKER, Enes

Uzmanlık Tezi

Tez Danışmanı: Üst Kurul Uzmanı Şahin COŞKUN

Temmuz, 2023

Bütün sosyal ve ekonomik hayatı yakın gelecekte ciddi boyutta etkilemesi düşünülen blok zinciri teknolojisi, çeşitli uygulama alanlarıyla hem kamu ve hem özel sektörde kullanılabilmektedir. Blok zinciri teknolojisi, günümüzde internet üzerinden sağlanan birçok kamusal hizmeti daha güvenli hale getirme potansiyeline sahip olduğundan, blok zincirin sağlayacağı avantajların ve dezavantajların yakından incelenmesi önem arz etmektedir. Bu çalışmada blok zincir teknolojisi, kamu sektöründeki verilerin güvenliğini sağlanmak yönüyle incelenmektedir. Bu kapsamda blok zincirinin kamu sektöründe kullanımı, dünyadaki ve Türkiye'deki örnekler üzerinden incelenmiştir. Bu çalışma sonucunda Türkiye'nin blok zinciri teknolojisi ile dijital dönüşümü için olumlu bir yaklaşım sergilediği ve bu doğrultuda çalışmalar yaptığı görülmüştür.

Anahtar Sözcükler: Blok Zinciri, P2P Ağ, Dağıtık Defter Teknolojisi, Kriptografi

ABSTRACT

USE OF BLOCKCHAIN TECHNOLOGY IN ENSURING DATA SECURITY IN THE PUBLIC SECTOR AND RTÜK REVIEW

ÇELİKER, Enes

Specialization Thesis

Thesis Advisor: Supreme Council Specialist Şahin COŞKUN

July, 2023

Blockchain technology, which is thought to affect social and economic life in the near future, can be used in both the public and private sectors with its various application areas. Since block chain technology has the potential to make many public services more secure today, it is important to closely examine the advantages and disadvantages of the blockchain. Blockchain technology is examined in terms of ensuring the safety of data in the public sector. In this context, the use of the blockchain in the public sector is examined through examples in the world and in Turkey. As a result of this study, it has been seen that Turkey has a positive approach for the digital transformation with the blockchain technology and that it has been working in this direction.

Keywords: Blockchain, P2P Network, Distributed Ledger Technology, Cryptography

İÇİNDEKİLER

ETİK İLKELERE UYGUNLUK BEYANI i
İTHAF ii
TEŞEKKÜR iii
ÖZET iv
ABSTRACT v
İÇİNDEKİLER vi
TABLOLAR DİZİNİ ix
ŞEKİLLER DİZİNİ x
KISALTMALAR/SİMGELER xi
BÖLÜM 1 1
1. GİRİŞ 1
1.1 Problemler 3
1.2. Amaç 3
1.3. Önem 4
1.4. Sayıltılar 5
1.5. Sınırlılıklar 5
1.6. Tanımlar 5
BÖLÜM 2 7
2. YÖNTEM 7
2.1. Araştırma Modeli 7
2.2. Evren ve Örneklem 7
2.3. Verilerin Toplanması 7
2.4. Verilerin Çözümlenmesi 8
BÖLÜM 3 9
3. BLOK ZİNCİR NEDİR? 9
3.1. Blok Zinciri'nin Tarihçesi 10

3.2. Bitcoin'in Tarihçesi 11
3.3. Blok Zincir'in Teknik Özellikleri 14
3.3.1. Dağıtık Veri Tabanı (Distributed Ledger) Yapısı 14
3.3.2. Blok Zincirinde Güven İlişkisi 16
3.3.3. Değiştirilememe ve Silinememe Özelliği 17
3.3.4. Anonimlik Özelliği 18
3.3.5. İşlemlerin Diğer Katılımcılar Tarafından Doğrulanması 19
3.3.6. Blok Özelliği 20
3.4. Blok Zinciri Türleri 21
3.4.1. Açık Blok Zinciri Ağları 21
3.4.2. Özel Blok Zinciri Ağları 23
3.5. Bitcoin'in Güvenilirliğini Sağlayan Unsurlar 27
BÖLÜM 4 29
4. BLOK ZİNCİRİ NASIL ÇALIŞIR ? 29
4.1. Blok Zincirde Merkeziyetsizlik 31
4.2. Blok Zincirin Güvenliğini Sağlayan Unsurlar 32
4.2.1. Kimlik Denetimi (Authentication) 33
4.2.2. Veri Bütünlüğü (İntegrity) 34
4.2.3. Erişim (Availability) 37
4.2.4. Gizlilik (Confidentiality) 37
4.2.5. İşlem Sıralaması (Transaction Ordering) 37
4.3. Blok Zincirin Kriptografik Yapısı 38
4.3.1. Kriptografik Özet Fonksiyonu 41
4.4. Blok Zincirin Ağ Yapısı 43
4.4.1. Bitcoin Ağında Blokların Zincire Eklenmesi 43
4.4.2. İki Farklı Zincir Oluşturma Durumu (Tie Breaking) 44
4.4.3. İşlemleri Geri Döndürmenin Zor Olması 44

4.4.4. İşlem Onayı Alma 45
4.4.5. Mahremiyet Sorunları 46
4.5. Blok Zincirin Eksikleri 46
4.6. Uzlaşı Algoritmaları 48
4.6.1. Proof of Stake 49
4.6.2. Byzantine Fault Tolerance (BFT) 50
BÖLÜM 5 52
5. BLOK ZİNCİRİ UYGULAMALARI 52
5.1. Blok Zinciri Teknolojisinin Uygun Kullanım Alanları 53
5.2. Blok Zincirin IOT Cihazlar Üzerinde Kullanımı 57
5.3. Dünya Üzerinde Blok Zinciri Uygulamaları 59
5.3.1. D5 Ülkeleri 59
5.3.2. Diğer Ülkelerde Blok Zinciri Uygulamaları 62
5.4. Türkiye Örnekleri 63
5.4.1. TOGG 63
5.4.2. e-Devlet: Dijital Kimlik 64
5.4.3. TÜBİTAK: ‘Blokzincir Araştırma Laboratuvarı 65
5.4.4. Blockchain Türkiye Platformu (BCTP) 65
5.4.5. Sanayi ve Teknoloji Bakanlığı: Sanayi ve Teknoloji Stratejisi (2023) 65
5.4.6. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı: On Birinci Kalkınma Planı 67
5.5. RTÜK İncelemesi 67
6. SONUÇ VE ÖNERİLER 69
6.1. Sonuç 69
6.2. Öneriler 72
KAYNAKÇA 73
ÖZGEÇMİŞ 77

TABLOLAR DİZİNİ

Tablo 1 12
Tablo 2 55

ŞEKİLLER DİZİNİ

Şekil 1 16
Şekil 2 17
Şekil 3 19
Şekil 4 21
Şekil 5 29
Şekil 6 34
Şekil 7 36
Şekil 8 39
Şekil 9 40
Şekil 10 42

KISALTMALAR/SİMGELER

Kısaltma	Açıklama
BDDK	Bankacılık Düzenleme ve Denetleme Kurumu
BFT	Byzantine Fault Tolerance
BTC	Bitcoin
DLT	Distributed Ledger Technology
DPoS	Delegated Proof of Stake
EBYS	Elektronik Belge Yönetim Sistemi
IoT	Nesnelerin İnterneti (Internet of Things)
Max	Maximum
NATO	North Atlantic Treaty Organization
Nonce	Number Used Once
NFT	Non Fungible Token
PoW	Proof of Work
PoS	Proof of Stake
P2P	Peer to Peer
PoA	Proof of Assignment
P2P	Peer to Peer
SPK	Sermaye Piyasası Kurumu
Tx	İşlem (Transaction)
TPS	Saniyedeki İşlem Sayısı (Transaction Per Second)
UK	Birleşik Krallık

BÖLÜM 1

1. GİRİŞ

Blok zinciri teknolojisi duyulmaya başlandığı ilk zamanlarda, bu teknolojiyi insanlar kripto paralar üzerinden alım satım yaparak finansal değer sağlayacakları ortam olarak bilmekteydi. Nitekim kripto paraların ilk duyulduğu, henüz çoğu kişinin bilmediği zamanlarda, kripto para borsasına giren kişilerin ciddi miktarda finansal kazanç sağladıkları gözlemlenmiştir. Bu sebeple blok zinciri teknolojisinin finansal alanda kullanımı büyüktür. Özellikle ülkemizde blok zincirin finansal bir değer olarak kullanımı oldukça büyüktür. 2020 Dünya Bankası verilerine göre Türkiye, kripto para kullanımında Nijerya, Vietnam ve Filipinler den sonra 4. sırada sırada yer almaktadır (Tecim, Yılmaz ve Karakoyunlu, 2023). Ancak, blok zincirin yaygın kullanımı olan kripto paralar haricinde çok fazla kullanım alanı mevcuttur.

Literatürde yıkıcı teknolojilerden biri olarak geçen blok zinciri, dünyayı en çok değiştiren teknolojiler arasında beşinci sırada gelmektedir. Blok zincirin önünde gelen diğer dört teknoloji ise mainframe, kişisel bilgisayarlar, internet ve sosyal medyadır. Örneğin, bilgisayarın ve internetin icadı ele alındığında, bu icatlardan önceki insan hayatı ile sonraki hayat kıyaslandığında birçok alanda ciddi bir değişiminin olduğu göze çarpmaktadır. Bu icatların arasında yer edinmiş olan blok zincir teknolojisinin ise günümüzle gelecek arasında benzer bir değişime sebep olacağı düşünülmektedir. Günümüz internet ağı, ilk olarak Amerika Birleşik Devletleri'nin Kaliforniya eyaletindeki iki bilgisayarın birbirine bağlanıp birbiri ile haberleşmesinden ibaretti. Daha sonraları başka bilgisayarlar eklenerek bağlantılar artmış ve günümüz internet ağını oluşturmuştur. Dolayısıyla kimi akademisyenlere göre internet, büyümesi düşünülüp güvenlik gereksinimleri karşılanarak oluşturulmuş güvenli bir ağ değildir. Nitekim siber güvenlik kavramı, internetin icadından çok uzun zaman sonra hayatımıza girmiştir.

Günümüz internetinin zafiyetlerini kapatmak üzere antivirüs uygulamaları, işletim sistemi yamaları vb. birçok teknik geliştirilmektedir. Ancak büyük çoğunluğu, bu tezin konusu olan blok zincir konsepti kadar siber güvenlik alanında derin bir çözüm sunmamaktadır. Blok zincirin yıkıcı teknolojilerden biri olarak adlandırılmasının sebebi de

budur. Bu yönüyle blok zinciri teknolojisi, günümüz internet ağını değiştirebilme potansiyeli olan bir teknolojidir. Blok zinciri teknolojisinin bütün yönleriyle uygulanmasıyla birlikte daha güvenli, daha şeffaf bir veri paylaşım ortamı sağlanacağı öne sürülmektedir. Finans sektörüne yeni bir yön vererek bütün borsa sektörünü büyük çapta etkileyen blok zincirinin siber güvenlik sektörünü de büyük oranda etkileyeceği beklenmektedir.

Blok zincirin evrimsel gelişiminde ilk olarak kripto paralarda kullanılan haliyle blok zinciri 1.0 olarak adlandırılmaktadır. Daha sonra akıllı sözleşmelerin geliştirilmesiyle otomatize uygulamalar yapılabilir hale gelmiş ve blok zinciri 2.0 kavramı literatüre girmiştir. En son olarak, günümüzde, blok zinciri teknolojileri şirketler ve kamu kurumları tarafından kullanılmaya başlandıkça blok zinciri 3.0 halini almıştır.

Bu tezde blok zinciri 1.0 ile ortaya çıkan ve kripto paralarla temelleri atılan blok zincirin temel işleyişi kripto paralar üzerinden anlatılacaktır. Ardından kripto paralardaki güvenliği ve mahremiyeti sağlayan mekanizmaların veri güvenliğinde nasıl kullanılacağı anlatılacaktır. Nihai hedef olarak kamu kurumlarının blok zincirin sağladığı veri güvenliğine sahip olabilmesi adına araştırmalara yer verilecektir.

Blok zincirinin sağladığı faydaların yanı sıra; blok zincir kavramının oluştuğu ilk yıllarda şirketler ve araştırmacılar blok zinciri teknolojisini bütün sistemlerin siber güvenliğini sağlayacak bir çözüm olarak ele almış ve bu çözüme uygun sorunları bulmaya çalışmışlardır. Ancak blok zinciri bütün sorunlara çözüm olabilecek bir teknoloji değildir. Bazı projelerde blok zincirini kullanmak faydalıyken, bazı projelerde günümüz teknolojileri daha verimli sonuçlar ortaya koymaktadır.

Günümüzde bir veriye ulaşmak istenildiğinde bu veriye ait istek bilgisayara girilir. Örneğin, tarayıcıya bir web sitesinin ismi yazılır ve web sitesinin görüntülenmesi istenir. Bu web sitesinin bulunduğu sunucu, bilgisayara olumlu yanıt verirse web sitesi bilgisayarda görüntülenebilir. Bu sisteme sunucu-istemci mimarisi denilmektedir. Blok zincirinde ise durum daha farklıdır. Burada herkes bir istemci olabilir; aynı zamanda herkes bir sunucu gibi de davranabilir. Çünkü ağa bağlı makineler aynı zamanda veri tutma görevi üstlenen bir sunucu görevi de üstlenir. Bu ağ yapısına dağıtık yapılar denilmektedir. Blok zinciri teknolojisinde ağ alt yapısı olarak dağıtık ağlar kullanmaktadır. Bu sayede veriler tek bir makinede silinse dahi diğer makineler üzerlerinde ilgili veri tutulduğu için verinin kaybolma riski bulunmamaktadır. Aynı mantıkla verilerin değiştirilebilme riski de yoktur. Ayrıca makinelerden birçoğu kapalı durumda dahi olsa tek bir makinenin çalışıyor olması o veriye

erişimi mümkün kılar. Bütün bu sayılanlar siber güvenliğin gizlilik, bütünlük, erişilebilirlik kavramlarını ifade etmektedir. Blok zincirin doğal yapısı gereği, verileri bu açılardan güvende tutacağı savunulmaktadır.

1.1 Problemler

Araştırmanın çıkış noktası olarak; siber tehditlerin oldukça yoğun olduğu günümüzde, kamu sektöründe veri güvenliğinin daha yüksek seviyede nasıl sağlanabileceği problemi seçilmiştir. Bu probleme çözüm olarak önerilen yöntemin faydalı olabilmesi adına, alt problemler aşağıdaki gibi belirlenmiş ve bu alt problemlerin çözümü araştırılmıştır.

- Veri güvenliğini sağlayan unsurlar nedir?
- Blok zinciri teknolojisi veri güvenliğini nasıl sağlamaktadır?
- Blok zinciri teknolojisinin günümüz güvenlik çözümlerine kıyasla avantajları ve dezavantajları nedir, nasıl değerlendirilmelidir?
- Hangi alanlarda blok zinciri bir çözüm olarak uygulanabilir?
- Dünya üzerinde veri güvenliğini sağlama konusunda blok zinciri teknolojisi ne yöne doğru gitmektedir?
- Diğer ülkelerde kamu kurumları blok zinciri teknolojisini hangi alanlarda kullanmaktadır?
- Türkiye, blok zinciri teknolojisini geliştirme konusunda hangi aşamadadır ve neler gerçekleştirilmektedir?

Üst Kurul'un sunmakta olduğu internet hizmetleri ve aldığı siber güvenlik tedbirleri günümüz yaygın teknolojileriyle sağlanmakta iken henüz gelişim aşamasında olan blok zinciri teknolojisi kullanılmamaktadır. Bu tezde, blok zinciri teknolojisinin Üst Kurul'a sağlayacağı faydaların neler olduğunun açıklanmasının yanı sıra; blok zinciri teknolojisinin ülkemizde gelişim sağlayabilmesi için Üst Kurul'un sağlayacağı katkılar üzerinde durulmuştur.

1.2. Amaç

Tezin amacı, veri güvenliğini sağlamada güncel teknolojileri araştırmak ve bunların çözüm olarak nasıl kullanılması gerektiğini irdeleyip, kamu sektöründeki verilerin

güvenliğinin sağlanması için gerekli teknik detayları gün yüzüne çıkarmaktır. İnternetin güvenliği için yeni bir çözüm olarak öngörülen blok zinciri teknolojisinin veri güvenliği alanında nasıl çalıştığı, finans sektörünün haricinde nerelerde kullanılabildiği ve kullanıldığı durumda getireceği avantaj ve dezavantajlar değerlendirilerek bir çözüm önerisinde bulunmak amaçlanmıştır.

Önümüzdeki zamanlarda hemen her alanda olduğu gibi medya sektöründe de blok zinciri teknolojisinin yoğun olarak kullanılacağı hipotezinden yola çıkarak Üst Kurul'un bu teknolojiye katkı ve uyum sağlaması için yapılması gerekenler araştırılmıştır. Veri güvenliği açısından ise; Üst Kurul veri merkezinde barındırılan verilerin güvenliği için, siber saldırılara karşı daha dayanıklı olan blok zinciri teknolojisinin kullanım imkânları değerlendirilmiştir. Ayrıca, ülkemizde blok zinciri teknolojisinin daha hızlı gelişim gösterebilmesi için Üst Kurul'un sağlayacağı katkıların neler olabileceği değerlendirilmiştir.

1.3. Önem

Blok zinciri teknolojisinin internet üzerinde yeni bir çağ açacağı değerlendirilerek, kamu kurumlarının bu yeni çağda veri güvenliklerini nasıl daha iyi sağlayabilecekleri konusuna blok zinciri teknolojisi tam olarak yaygınlaşmadan hazır olunması gereklidir. Aksi halde teknoloji üreten değil teknolojiyi takip eden bir konumda olunması kaçınılmazdır. Günümüz internet hizmetlerinin en temelinde problem olduğu akademisyenler tarafından ifade edilmektedir. Güvenliği önceleyen yeni bir ağ yapısı ile ortaya çıkan blok zinciri teknolojisi günümüz internetinin yapısını yıkıcı olarak değiştirebilecek potansiyeldedir. Blok zinciri teknolojisinin bu etkisi düşünüldüğünde konunun daha ileri çalışmalarla geliştirilmesi gereklidir. Toplumda teknoloji dönüşümünün sağlanmasındaki en önemli adımlardan biri, teknoloji kullanıcılarını bilinçlendirme ve yetişmiş teknik insan kaynağı oluşturmaktır. Bu çalışmanın, teknoloji kullanıcısı bireyler için bir farkındalık oluşturacağı, bilgi teknolojileri personelleri için ise blok zinciri teknolojisinin iç yüzünü anlatması sebebiyle faydalı bir kaynak olabileceği düşünülmektedir.

1.4. Sayıltılar

Blok zinciri teknolojisinin veri güvenliğine sağladığı katkılar incelendiğinde gelecekte blok zincirinin bu alanda daha fazla yer bulacağı varsayılmıştır. Olası çalışma alanları işaret edilerek günümüzde kullanılan teknolojilerin bir dönüşüm geçireceği ve blok zinciri tabanlı uygulamalara geçiş yapılacağı düşünülmüştür.

1.5. Sınırlılıklar

Tez konusu olan blok zincirinin uzlaşı protokollerinden en yaygın olan protokolleri üzerinde durulmuş, nispeten daha az kullanılan ve akademisyenlerin yeni geliştirmekte olduğu algoritmalar incelenmemiştir. Ağ seviyesinde blok zinciri teknolojisinin nasıl çalıştığı ve nerelerde kullanıldığına değinilmiştir, ancak blok zinciri yazılımı üzerinde durulmamıştır.

1.6.Tanımlar

Ağ (Network): Bilgisayar ağları içerisinde geçen bu kavram, birden çok bilgisayarın veya iletişim cihazının kablolu veya kablosuz iletişim hatlarıyla birbirine bağlayan, dolayısıyla iki cihaz arasındaki veri aktarımını sağlayan iletişim sistemidir.

Bitcoin: Satoshi Nakamoto takma isimli anonim bir kişi veya topluluk tarafından 2008 yılında icat edilmiş olan kripto paradır.

Blok: Blok zinciri teknolojisinde ancak belli bir sayıda işlem topluluğunun birleşmesi ve bu işlemlerin doğrulanması sonucu oluşan veri tabanıdır.

Blok Zincir Ağı: Dağıtık ağ mimarisini kullanan işlemler topluluğundan oluşan blokların birbirine bağlanmasıyla oluşan gelişmiş bir veri tabanı teknolojisidir.

Broadcast: Bir mesajın ağdaki bütün cihazlara gönderilmesini sağlayan haberleşme protokolüdür.

Hacker: Bilgisayar sistemlerinin hata ve açıklarından faydalanarak sisteme yetkisiz erişen kötü niyetli kişidir.

İş Kanıtı (Proof of Work): Bitcoin'in uzlaşı algoritması olarak çalışan, oldukça güvenli olan ancak fazla enerji tüketimi isteyen, en bilinen uzlaşı protokolüdür.

Kripto para: Genellikle internet üzerinden kullanılmak üzere tasarlanmış, merkezî olmayan dijital para birimleridir.

Metaverse: Sanal ve artırılmış gerçeklik cihazlarıyla erişilebilen, 3 boyutlu dijital ortamları destekleyen, internetin varsayımsal bir halidir.

Non Fungible Token (NFT): Nitelikli fikri tapu, dijital bir varlığın benzersiz olduğunu yani orijinal olduğunu onaylayan, blok zinciri teknolojisinde tutulan veridir.

Peer-to-Peer (P2P): Bir diğer ifadeyle eşler arası ağ, merkezi bir sunucu gibi üçüncü taraf sistemlere ihtiyaç olmadan kullanıcıların doğrudan birbirleri arasında gerçekleştirdiği veri paylaşımı ağını ifade eder.

Web 3.0: Merkeziyetsiz bir şekilde kullanılan blok zinciri destekli interneti ifade etmektedir.

BÖLÜM 2

2. YÖNTEM

Bu araştırmada, nitel araştırma yöntemi kullanılmıştır. Konu ile ilgili veriler ulusal/uluslararası kabul görmüş makalelerden, tezlerden, dergilerden, konferans notlarından toplanarak analiz edilmiş, yorumlanmış ve problemin çözümüne ilişkin teknik detaylar incelenmiştir. Blok zinciri kavramı incelenirken ne, nasıl, hangi saikle gibi sorular sorularak teknolojinin hizmet ettiği şey sorgulanmıştır. Blok zinciri teknolojisini araştırırken, teknik detayları haricinde konu ile ilgili kamu kurum ve kuruluşlarının yayınladığı mevzuatlar ve bildiriler, güvenilirliği yüksek olan haber organlarının dijital haberleri kaynak olarak kullanılmıştır.

2.1. Araştırma Modeli

Bu çalışmada araştırma yöntemi olarak betimsel araştırma yöntemi kullanılmıştır. Çalışma süresince mevcut durumlardan örnekler aktarılmış, hangi amaca varılmak istenildiği, ne yapılmak istenildiği, hangi problemin çözülmek istenildiği gibi sorular doğrultusunda yorumlanan ve analiz edilen veriler açıklanmıştır.

2.2. Evren ve Örneklem

Bu çalışmanın evreni blok zinciri teknolojisi, örneklemi ise veri güvenliğinin blok zinciri ile sağlanması ve kamu sektöründeki blok zinciri uygulamalarıdır.

2.3. Verilerin Toplanması

Veriler toplanırken doküman analizi ve kaynak tarama metodu kullanılmıştır. Kaynak tarama sürecinde ekseriyetle dijital kaynaklar kullanılmıştır. Bu kaynaklar, internet ortamına yüklenen erişime açık teknik kitaplar, kamu haber organlarının haberleri, kamu

kamu kurum ve kuruluşlarınca yayımlanan bildiriler ve mevzuatlar, internet haberleri, konferans kayıtları, üniversite ders kayıtları, makaleler ve tezlerden oluşmaktadır.

2.4. Verilerin Çözümlenmesi

Teze konu olan kaynaklar en genel konudan başlanarak sıralanmış, öncelikle konuya ilişkin genel bilgiler derlenmiştir. Konuya esas oluşturacak önemli başlıklar not edilerek genelden özele doğru sıralanmıştır. Bu süre zarfında oluşturulan başlıklar belirli bir temanın ve fikrin uyumu gözetilerek bağlamın devamlılığını sağlayacak şekilde sıralanmıştır. Toplanan verilerin problem için ne gibi çıkarımları, sonuçları ortaya koyduğunu gösteren betimleme yöntemi kullanılmıştır. Betimlenen veriler ışığında çıkarımlarda ve yargılarda bulunulmuştur. Sonuç bölümünde bu çıkarımlar ifade edilmiş ve hem Türkiye'deki kamu kurumları hem de Radyo ve Televizyon Üst Kurulu özelinde önerilerde bulunulmuştur.

BÖLÜM 3

3. BLOK ZİNCİR NEDİR?

Bu bölümde blok zincir teknolojisi alanında akıllı kontratlardan (smart contract) önce neler yapıldığı tarif edilmektedir. Blok zincir konseptlerini açıklamak için en uygun örneğin Bitcoin örneği olması sebebiyle, Bitcoin'in nasıl çalıştığı ve Bitcoin'deki değişik konseptlerin blok zincire nasıl uygulandığı bu bölümün içeriğinde yer almaktadır.

Kripto paralar, blok zincir teknolojisinin en anlamlı uygulama alanlarından birisi olmakla beraber blok zincir teknolojisinin başka hangi alanlarda kullanılabileceği sorusu akademik camianın ve özel sektörden birçok şirketin peşinde olduğu en güncel ve en çok uğraşılan araştırma konularından bir tanesidir. Bununla birlikte, blok zincirin ne zaman kullanılıp ne zaman kullanılmaması gerektiği önemli bir konudur. 2008 yılında Bitcoin'in ortaya çıkmasıyla beraber, blok zincir teknolojisinin hızlıca yayılmaya başladığı ilk yıllarda; blok zincir teknolojisi çözüm olarak görülüp, bu çözüme karşılık gelen problemler üretilmeye çalışılmaktaydı. Bu problemlerin çoğuna bakıldığında ise blok zincir çözümü gerektirmeyen hatta blok zincir kullanılması durumunda çok anlamlı olmayan, neticede üstün performans alınamayacak problemler olduğu anlaşılmaktaydı. Bu yolla başlatılmış olan projelerin büyük çoğunluğu öngörüleceği üzere hayata geçirilmemiştir. Bunun sebebi, blok zincir kullanıldığında çok iyi bir çözüm olacak problemler/projeler varken, blok zincir kullanmanın verimsiz olduğu problemler bulunmaktadır.

"Blok zincir nedir?" sorusunun en net cevabı için "her bitcoin blok zincirdir ancak her blok zincir bitcoin değildir" önermesi kullanılabilir. Özellikle blok zincir 1.0 diye de isimlendirilen Bitcoin'den sonra blok zincir teknolojisinde gelişen ve eklenen yeni özellikler hesaba katıldığında "blok zincir eşit değildir Bitcoin" önermesini kullanmak doğrudur. Blok zincir çok geniş bir kavram olmakla beraber; esasen Bitcoin'in altında yatan teknolojiyi, daha açık ifade ile ağ topolojisini ve veri yapısını kullanmaktadır. Bitcoin'de kullanılan peer-to-peer (P2P) ağ yapısı uzlaşı algoritmalarıyla ile birlikte ağa bağlanan katılımcıların birbirleri ile olan ilişkisini belirli kurallar içerisinde belirleyebilecek bir yapıda çalışmaktadır (Nakamoto, 2008).

Blok zinciri aynı zamanda bilgi teknolojileri dünyasında "yıkıcı teknolojiler" olarak isimlendirilen yani dünyayı çok değiştiren teknolojiler arasında beşinci sırada gelmektedir

(Farhan, 2017). Blok zincirin önünde gelen diğer dört teknoloji ise mainframe, kişisel bilgisayarlar, internet ve sosyal medyadır. En genel örnek olarak bilgisayarın ve internetin icadı ele alındığında, bu icatlardan önceki insan hayatı ile sonraki hayat kıyaslandığında birçok boyutta ciddi bir değişimin olduğu göze çarpmaktadır. Bu icatların arasında yer edinmiş olan blok zincir teknolojisi ile ilgili olarak da günümüzle gelecek arasında benzer bir değişime sebep olacağı görüşü benimsenmekle beraber bu görüşe katılmayanlar da mevcuttur.

3.1. Blok Zinciri'nin Tarihçesi

Blok zincirin tarihsel gelişimi için bazı kavramsal dönemler oluşturulmuştur. Bunlardan blok zinciri 1.0 kripto paraları, blok zinciri 2.0 merkeziyetsiz çalışan uygulamaları destekleyen akıllı sözleşmeleri (smart contracts), blok zinciri 3.0 dağıtık sistemlerin gelişip yaygınlaşarak kamu ve özel söktör uygulamalarında yer bulduğu dönemi ifade etmektedir.

Blok zincirinin keşfedilmesinden önce, blok zinciri 1.0 olarak da adlandırılabilen Bitcoin ile günümüze gelen kripto paraların yapılması araştırmacılar ve matematikçiler tarafından düşünülmekte ve denenmekteydi. Araştırmacı ve matematikçilerin haricinde kriptografiyle uğraşan kişiler, yazılımcılar ve daha birçok uzmanlık isteyen alanın birlikte çalışması elzem bir konuydu. Çünkü günümüzde belki de insanların en çok önem verdiği şey yani para söz konusu olmaktadır. Fiziksel olarak gözle görülüp elle tutulamayan bu kripto paraların güvenilirliği ve el değiştirmesi çok sağlam kurgulanmak zorundadır.

Blok zinciri öncesi oluşturulmuş olan bu kripto paraların örnekleri arasında Beenz, Flooz, E-Gold, DigiCash gibi örnekler verilebilir. Bu örneklerin çoğunun karşılaştığı sorun ise terminolojisi çifte harcama (double-spending) olan yani aynı paranın birden fazla kez harcanabilmesi problemidir. Sanal olan bir para kopyalanıp başka bir yerde harcanabilmekteydi. Elbette bir paranın kopyalanıp birden fazla yerde harcanmaması gerekmektedir. Ancak sanal olan bu paralar kötü niyetli kişilerce sistemin açığı bulunarak kopyalanabilmekteydi.

Bitcoin'in çözdüğü en büyük sorunlardan biri de çifte harcama problemini aşmış olmasıdır. Bitcoin'de bu paraların birçok yerde harcanamamasının sebebi, yapılan harcamaların ve transferlerin tarihçesinin ve bilgilerinin kayıt defterinde tutulmasıdır. Bu

kayıt defteri ise ağdaki bütün katılımcılara aktarılarak her düğümde bu bilginin bulunması sağlanmaktadır. Ayrıca, değişik düğümlerin katılımıyla oluşturulan uzlaşı algoritmalarıyla doğrulama işlemi gerçekleştirilmekte, dolayısıyla belirli bir paranın daha önce kullanılıp kullanılmadığı bilgisi ağdaki düğümler tarafından doğrulanmaktadır. Yani, blok zinciri ağındaki düğümlerde tutulan bilgiler paranın kendisi değil, paranın değişim (transection) bilgisidir. Bitcoin'de düğümlerde tutulmakta olan bir bilgi kabaca; A kişisinden B kişine, T tarihinde x miktar para gönderildiği bilgisidir. Burada manipüle edilen sistem yine bu bilgilerin değiştirilmesi yoluyla yapılabilmektedir. Ağdaki düğümlerin çoğunu ele geçiren bir kişi A kişisinin parayı, başka bir kişi olan, C kişisine gönderdiği yönünde bilgiyi ağa yazarsa geri kalan diğer azınlık düğümler çoğunluğa uyarak yeni bilgi olarak bu manipüle edilmiş bilgiyi kendi bloklarına yazarlar. Ancak, Bitcoin gibi çok büyük ağlarda bu %51 çoğunluğu manipüle etmek imkânsıza yakındır. Manipüle edilse dahi bunu gerçekleştirmek için harcayacağı bilgisayar donanımı ve enerji maliyeti ciddi boyutlara ulaşacaktır. Esasında kötü niyetli bu kişi manipülasyonu yapmak yerine Bitcoin madenciliği yapsa daha çok kazanç sağlayabilecektir. Bitcoin bu şekilde hem kötü niyetli kişileri hem de bütün katılımcıları ağa katılma ve doğru işlemi gerçekleştirme yönünde teşvik etmektedir.

3.2. Bitcoin'in Tarihçesi

2009 yılında çıkan Bitcoin günümüzde halen büyüklük olarak en tepede olan kripto paradır. Kripto paraların değerleri piyasanın ve siyasetin durumuna göre değişse de coinmarketcap.com sitesinde yer alan verilere göre Bitcoin'in liderliği halen devam etmektedir. Bu şekilde liderliğini sürdüren Bitcoin'in ilk çıkışı "Bitcoin: A Peer-to-Peer Electronic Cash System" başlıklı bir makale aracılığıyla olmuştur. Satoshi Nakamoto ismiyle yayımlanan bu makalenin gerçek yayıncısının bu isime mi sahip olduğu, bir kişinin ya da grubun takma ismi mi olduğu halen bilinmemektedir. Makalenin kısaca özeti "güvene dayanmayan elektronik ödemeler" şeklinde tanımlanmıştır (Nakamoto, 2008). İlk blok zinciri uygulaması olarak tasvir edilebilen Bitcoin'nin gelişiminde neler yaşandığı kronolojik olarak Tablo 1'de gösterilmektedir.

Tablo 1

Bitcoin Tarihinde Gerçekleşen Önemli Olaylar

Zaman	İşlemler
Ocak 2009	İlk açık kaynak Bitcoin kullanıcısı çıkarılmıştır.
2010 yılı ortaları	Satoshi Nakamoto, 1milyon Bitcoin (BTC) toplayarak ortadan kaybolmuştur.
Nisan 2010	3. parti yazılım ve işletmeler işin içine girmiş ve Bitcoin alım satımına olanak sağlayan BitcoinMarket.com piyasaya çıkmıştır.
Mayıs 2010	10.000 BTC ödenip iki pizza satın alınarak Bitcoin ile yapılan ilk gerçek dünya işlemi gerçekleşmiştir.
Ağustos 2010	İlk ve en büyük güvenlik açığı ortaya çıktıktan sonra protokol tamamen güncellenerek ağdaki bütün bilgisayarlara yeni versiyona geçilmesi için güncellenmiştir.
Mayıs 2011	BitPay ismiyle global ve online ticari ölçekte Bitcoin ödeme servisi ortaya çıktı.
Temmuz 2011	Bitcoin keskin bir yükseliş yaparak 31$'a çıkmış ve bu ilk balon olarak kabul edilmiştir.
Kasım 2011	Bitcoin'in başarısından etkilenerek alternatif bir coin olan Litecoin ortaya çıkmıştır (Bitcoin'den farklı madencilik algoritmasına sahip ve daha hızlı işlem gerçekleştirilmekteydi).
Haziran 2012	Bir başka coin olan Ripple ortaya çıkmıştır (günümüz bankacılık sistemine çok benzeyen düşük işlem ücretli para göndermeyi hedefleyen protokoldür).
Eylül 2012	Bitcoin vakfı kuruldu.
Ekim 2012	1.000'den fazla ticari işletme Bitcoin'i bir ödeme aracı olarak kullanmaya başladı (Bu gelişme Bitcoin'in artık dünyaca kabul edilebilir hale geldiğini ortaya koymuş ve sonraki gelişmeler daha hızlı gerçekleşmeye başlamıştır).
Ağustos 2013	Bir Teksas federal yargıcı Bitcoin'in bir para birimi olduğunu dile getirerek bu doğrultuda yargısal kararını vermiştir.
Ekim 2013	FBI tarafından, "Silk Road" isimli web sitesinde 26.000 BTC değerinde uyuşturucu ticareti yapıldığı tespit edildi. (Bitcoin'deki yarı anonimlikten dolayı bir sürü illegal insan Bitcoin'i kullanmaya

başlamıştır. Ransomware isimli kötü niyetli fidye yazılımları yine Bitcoin yöntemiyle ödeme almaktadır).

Bitcoin'de Ağustos 2010 yılında çıkan güvenlik açığının haricinde şu ana kadar çok büyük güvenlik açıkları ortaya çıkmamıştır. Ancak Bitcoin alım satımı yapan siteleri bu durumdan hariç tutmak gereklidir. Kripto borsası olarak geçen bu tarz aracı site ve uygulamalar Bitcoin ağ alt yapısını kullanmamakta ve güven ilişkisi sadece uygulamayı kullananla uygulama arasında olmaktadır. Bitcoin alım satım işlemleri, Bitcoin'in açık kaynak kodunu bilgisayara indirerek bir aracıya ihtiyaç duymadan yapılabilir. Aracısız yapılan bu işlemlerde direkt olarak Bitcoin ağ alt yapısına sahip sistemler üzerinde işlem yapılabilmektedir. Bu işlem için, bazen elektronik USB bellek kullanılmakta, bazen ise kare koddan oluşan bir kâğıt üzerine baskı yaparak bu kare kod vasıtası ile işlemler yapılabilir. Yanma, yıpranma gibi ihtimallere karşı USB bellek elbette daha güvenli olabilmekle beraber bu cihazın kaybolması durumunda tüm varlık kaybedilmiş olmaktadır. Bu işlemin yapılmasıyla Bitcoin kriptografik yapısında kullanılan açık anahtar ve gizli anahtar eşlenikleri fiziksel olarak kullanıcısının elinde bulunmakta ve bu durumda anahtarlar aracı kurumlarla paylaşılmamış olmaktadır. Aracı kurumların kullanıldığı durumlarda anahtar eşlenikleri aracı kurumlar tarafından oluşturulmakta ve saklanmaktadır. Bu durumda aracı kurumların anahtarları nerde ve nasıl sakladıklarının iyi araştırılması gerekmektedir. Çünkü, gizli anahtarın ele geçirilmesi durumunda kişinin parası da çalınmış demektir. Bu tarz çalınma vakalarında Bitcoin'in merkezi bir yapısı olmadığı için şikâyet mercii bulunmamaktadır ve para, geri dönüşü olmayacak şekilde kaybolmuş olarak değerlendirilebilmektedir. Günümüzde kullandığımız banka gibi merkezi yapılarda bu durum değişiklik göstermektedir. Çaldırılan bir paranın iz takibi yapılarak veya bankanın hukuki sorumluluğu göz önüne alınarak direkt olarak bankadan temin etme yoluyla da paranın dönüşü sağlanabilmektedir. Ancak Bitcoin özelinde bahsi geçen güvensiz aracı kuruluşların kişilerin paralarını çalarak ülke dışına kaçma girişimlerindeki sorun, Bitcoin'deki kripto paraların güvensizliği ile ilgili değil insanların paylaştıkları anahtarların çalınması yoluyla gerçekleşmiştir. Bu sebeple, anahtarların tutulduğu aracı kurumların güvenilir olması gerekmektedir.

Bitcoin'in yarı anonimlik özelliğinden, yani gerçek kimliğin paylaşılmasının gerekli olmamasından dolayı illegal insanlar tarafından da ödeme aracı olarak kullanılmasına da kapı açmıştır. Örneğin, günümüzde çok yaygın olarak görülen ve ransomware olarak bilinen

fidye yazılımları bilgisayara bulaştığında içindeki verileri çözülemeyecek şekilde şifreler. Virüsü bulaştıran kötü niyetli kişiler ardından şifrenin çözülebilmesi için yine Bitcoin ile ödeme yapılmasını ister. Mağdur, eğer verilerine erişmek istiyorsa ve verilerinin bir yedeği yoksa bu ödemeyi yapmak durumunda kalmaktadır. Ayrıca, bu tarz ransomware saldırılarından korunmak için kurum ve kişilerin gerekli siber güvenlik tedbirlerini alması elzem bir konudur. Ransomeware için ilgili ödeme eğer banka ile yapılmış olsa, parayı talep eden banka hesabının bulunması çok kolay olmaktaydı. Ancak Bitcoin'de kimlik takibinin olmaması illegal kişiler tarafından kullanılmasının önünü açmaktadır.

Blok zinciri teknolojisinin getirdiği avantajların yanında bahsi geçen dezavantajları değerlendirildiğinde, özellikle, kripto paraların ödeme sistemi olarak kullanılması konusunda adli, hukuki ve finansal zemininin hazırlanması gerekliliği bulunmaktadır. Ancak tezimizde blok zincirin kripto para olarak kullanılmasından ziyade, kamu sektöründe ve Üst Kurul özelinde, blok zincir teknolojisinin kripto paraların güvenliğini sağladığı gibi verilerin güvenliğini nasıl sağlayabileceği üzerinde durulmuştur. Çünkü, bilinmektedir ki blok zincirin kriptografik yapısı, günümüzde kırılması çok zor bir teknoloji yapısındadır.

3.3. Blok Zincir'in Teknik Özellikleri

Blok zincirinde kullanılmakta olan bazı temel teknik özelliklere bu başlık altında değinilmektedir. Blok zincire ait bu özellikler hem kripto paralarda kullanılırken hem de başka projelerde blok zincirin uygulanabilirliğini değerlendirirken göz önünde bulundurulması gerekli olan özelliklerin başlıcalarıdır.

3.3.1. Dağıtık Veri Tabanı (Distributed Ledger) Yapısı

Blok zincir, daha önceden bazı özel uygulamalarda kullanılmakta olan P2P ağ topolojisini kendi veri tabanı yapısında kullanmaktadır. Hali hazırda yaygın olarak kullanılmakta olan sunucu-istemci ağ topolojisinden ayrılan temel nokta buradadır.

Sunucu-istemci ağ topolojisinde merkezi bir sunucuya bağlı birden çok bilgisayardan söz edilmektedir. İstemci olarak kabul ettiğimiz kişisel bilgisayarlar, tablet, telefon ve internet of things (IoT) gibi internete bağlı her türlü cihaz, verileri merkezi olarak belli bir yerde hizmet vermekte olan sunuculardan almakta veya bu sunuculara veri göndermektedir.

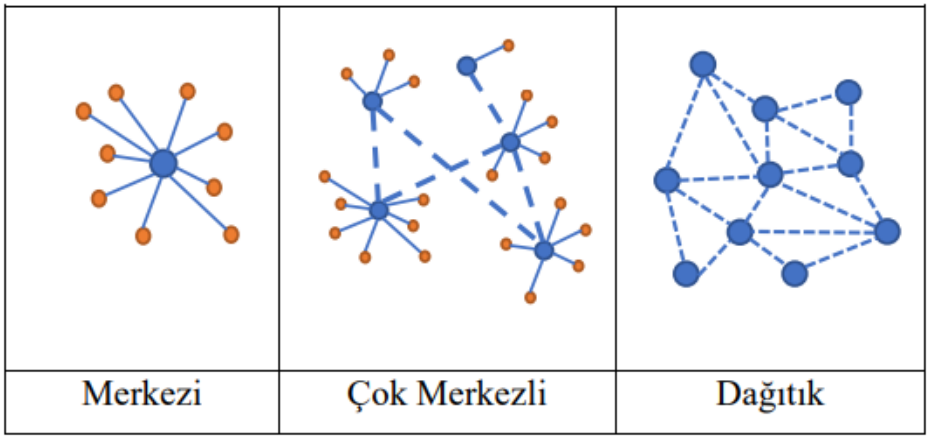
Örneğin; Google şirketinin hizmet vermekte olduğu Gmail e-posta uygulaması, e-posta verilerinin tamamını kendi bünyesinde barındırdığı merkezi sunucularda tutmaktadır. Gmail posta adresine sahip bir kişi, sunucu-istemci ağ yapısına sahip Google sunucularına erişerek e-postalarını görüntüleyebilmektedir. Bu merkezi sunucunun enerji ihtiyacı, donanım maliyeti, siber güvenlik ve sistem bakımı gereksinimleri gibi ihtiyaçları Google tarafından karşılanmaktadır. Bu merkezi sunucu tarafından işlenebilecek suçlarda veya bilgi belge taleplerinde muhatap direkt olarak Google'ın kendisidir.

P2P ağ yapısına göre veriler, güçlü merkezi bir sunucuya değil, ağa bağlı olan masaüstü bilgisayarlar gibi son kullanıcı cihazları üzerinde tutulmaktadır. Bu ağ yapısına göre bir veriye erişmek isteyen ağ katılımcısı, esasında bu veriye sahip olan başka bir kişinin bilgisayarına erişmektedir. P2P ağ yapısına bir örnek olarak ise; 2000 yılında piyasaya çıkmış olan müzik uygulaması LimeWire verilebilir. LimeWire'de merkezi bir sunucu bulunmamaktadır. LimeWire kullanmak isteyen kişiler, uygulamanın P2P ağının bir katılımcısı olarak kendi bilgisayarlarında tuttukları müzik verilerini hem diğer katılımcılara sunmakta hem de diğer bilgisayarların üzerinde tuttukları müzikleri kendi bilgisayarlarına indirebilmektedirler. Bu ağ yapısında, her kullanıcı bilgisayarı elbette kendi enerji ihtiyacını kendi karşılamakta, bilgisayarlarının güvenlik ve sistem ihtiyaçlarından yine kendileri sorumlu tutulmaktadır.

Block zincirin kullanmış olduğu P2P ağ topolojisi, Blok zinciri terminolojisinde dağıtık kayıt defteri veya distributed ledger olarak tanımlanmıştır. Blok zincir, P2P ağ topolojisi gereği verilerini merkezi bir sunucu üzerinde değil, dağıtık olma özelliği sebebiyle birbirlerine bir ağ aracılığıyla bağlı olan ve birbirinden bağımsız çalışan bir grup üzerinde tutmaktadır.

Şekil 1

Merkezi, Çok Merkezli ve Merkezi Olmayan Ağ Yapıları (Gürfidan & Arısoy, 2021, s.52)



Şekil 1'de günümüzde yaygın olarak kullanılmakta olan merkezi ve çok merkezli olan sunucu-istemci ağ yapısı ve blok zincirin ağ yapısı olan dağıtık ağ yapısı gösterilmiştir. Hali hazırda kullanılmakta olan ağ yapısına sahip merkezi ve çok merkezli yapılarda gösterilen turuncu noktalar bilgisayar, tablet, telefon ve IoT gibi istemcileri, mavi noktalar ise sunucuları ifade etmektedir. Blok zincirin dağıtık yapısını oluşturan P2P ağ yapısının gösterildiği son resimde ise bilgisayar, tablet, telefon gibi cihazların tamamı aynı zamanda bir sunucu görevi üstlenmiş gibi mavi noktalarla gösterilmiş ve bir örümcek ağı gibi her nokta birbirine bir ağ ile merkezi bir yapı olmaksızın bağlanmıştır. Dağıtık yapılarda birbirine bağlanan her bir mavi nokta blok zincir terminolojisinde düğüm (node) olarak isimlendirilmekte ve her düğüm aynı zamanda hem sunucu hem de istemci görevi görmektedir (Zeki, 2020, para.1).

3.3.2. Blok Zincirinde Güven İlişkisi

Blok zincirin çok önemli özelliklerinden birisi de birbirine bağlı olan düğümlerin birbirleri ile güven ilişkisinin olmaması ve sıfır güven ilkesi ile çalışmalarıdır. Bu güvensizlik ise merkeziyetsizliği getiren ve merkezi olmayan yapıların güvenli olmasını sağlayan bir ilkedir. Örneğin bir kişiye para göndermek istenildiğinde merkezi bir yapı olan banka aracılığı ile bu işlem yapılır ve bu işlemin ispatını yine dekont temini ile bankanın yapması beklenir. Ancak merkezi olmayan bir sistemde yani bankanın olmadığı ve grup

içindeki katılımcıların birbirine güvenmediği yapılarda, yani bir blok zinciri yapısında, bir kişiye para gönderildiğinde bu işlem bilgisi gruptaki diğer bütün katılımcılarla paylaşılır. Katılımcılar ise bu işlem bilgisini hiçbir şekilde silinmemek üzere kaydederler. Bu örnek üzerinden; merkezi yapılarda banka, Bankacılık Düzenleme ve Denetleme Kurumu (BDDK), Sermaye Piyasası Kurumu (SPK), mahkemeler gibi güçlü kurum ve kuruluşlara güvenilmektedir. Blok zinciri sistemlerdeki güveni ise matematiksel işlemlerle şifrelenmiş kriptografik yapılar sağlamaktadır.

Şekil 2

Bitcoin ve Amerikan Doları Karşılaştırması



Şekil 2'de görüleceği üzere Amerikan dolarında nasıl ki "*In God We Trust*" yani "Tanrıya güveniyoruz" ifadesi yer almakta ise Bitcoin amblemi içerisinde de "*In Cryptography We Trust*" yani "Kriptografiye güveniyoruz" ifadesi bu yapılardaki güvenin dayanağı temsil edilmiştir.

Blok zincirin kriptografik yapısının sağladığı bir özellik olarak, blok zinciri üzerinde bir işlem yapıldığında bu işlem inkâr edilememektedir. Çünkü her bir işlemin üzerinde dijital imza bulunmakta ve bu dijital imzalar başka bir kişi tarafından ele geçirilmediği sürece taklit edilmesi imkânsıza yakın boyuttadır.

3.3.3. Değiştirilememe ve Silinememe Özelliği

Blok zinciri ağını konvansiyonel ağ yapılarına göre daha güvenli yapan bir diğer özelliği ise verilerin silinememe ve değiştirilememe özelliğidir. Blok zinciri sadece veri

ekleme özelliği bulunan ancak silme ve değiştirme kabiliyeti olmayan bir veri tabanı olarak düşünülebilir. Blok zincirin ilk kurulumundan itibaren yapılan bütün işlem kayıtları blok zincir yapısında tutulmaya devam etmektedir. Blok zincirinde bir veri artık kullanılmayacak duruma geldiyse dahi bu veri silinmez, bunun yerine eski verinin artık kullanılmadığına dair yeni bir veri yazılır. Bu durumda dahi geriye yönelik işlem kayıtları blok zincirinde tutulmaya ve gösterilmeye devam eder. Bu özellik, kurum ve kuruluşların blok zinciri teknolojisini kullanarak sunabilecekleri şeffaflık açısından oldukça önemlidir. Blok zincirinde verilerin silinememesi ve değiştirilememesi özelliği, birçok verinin veri tabanlarında birikmesine ve gereksiz disk kapasitesi kullanımına sebep olmakla birlikte güvenli veri tutulması istenilen uygulamalarda büyük avantaj sağlamakta, ayrıca geçmişe yönelik adli analiz işlemlerine kesin bilgi sağlamak açısından çeşitli avantajları bulunmaktadır.

Bu durumun, blok zinciri teknolojisinin her yazılım uygulaması için uygun olmadığı, kısıtlı veri tabanına sahip ve veri güvenliği endişesi taşımayan yazılım uygulamalarında kullanılmasının uygun olmadığını gösterir. Bu teknoloji ancak güvenlik endişesi taşıyan uygulamalarda efektif bir şekilde çalışmaktadır. Örneğin; bankacılık uygulamalarında belirli bir miktar paranın birçok kişinin sahipliğinde el değiştirmesi ve daha sonra bu sahipliğin değiştirilemeyecek ve silinemeyecek olması denetim mekanizmaları açısından ciddi boyutta kolaylık sağlamakta ve denetim mekanizmalarındaki bürokrasi ve iş gücünü azaltarak işlemleri hızlandırmaktadır.

3.3.4. Anonimlik Özelliği

Block zincirinde tam anonimlikten söz edilememektedir. Yani yapılan bir işlemin kimin tarafından yapıldığının kimse tarafından bilinememesi tam olarak söz konusu olmamakta. Blok zinciri konseptlerinde kişiler esasen kendi kimliklerini kullanmamakta, public key olarak isimlendirilen açık anahtarlarını kullanmaktadırlar. Bu işlem tam anlamıyla anonimlik sağladığı şeklinde görünse de, her işlemde kişiler aynı açık anahtarları kullandıkları durumda bir defa dahi belirli bir işlemin hangi kişi tarafından gerçekleştirildiğinin bilinmesi durumunda kişinin bu açık adresinden dolayı bütün yaptığı işlemler tespit edilebilir. Bu sebeple blok zincirinde tam anonimlik değil pseudonymity denilen yarı anonimlik vardır. Yani belirli bir işlemi kimin yaptığı bilinmediği sürece gizli

kalınabilmekte, ancak açık anahtarın kime ait olduğunun tespit edildiği durumda kişinin işlemlerinin tamamı bilinebilir hale gelmektedir.

Blok zinciri teknolojisi ile suçluların ödeme aldığı ve bu yöntem ile saklanabildikleri yönündeki genel kanaat pseudonymity sayesinde bir miktar kırılabilmektedir. Hali hazırda siber suçlarla mücadele birimleri blok zinciri üzerinden işlenen suçlarla mücadele etmektedir. Yakalanan siber suçlulardan elde edilen malzemeler ise blok zincir teknoloji ile değişim göstermektedir. Önceden, tabanca gibi silahların sergilendiği emniyet panolarında, Şekil 3'teki gibi madencilik yapmakta kullanılan CPU, ekran kartı gibi cihazlar görünmektedir.

Şekil 3

Kripto Para Üretmek İçin Kullanılan Cihazların Sergilendiği Pano (Gazete Birlik, 2017)



3.3.5. İşlemlerin Diğer Katılımcılar Tarafından Doğrulanması

Blok zincirde oluşan her işlem, bloğa yazılmadan önce ağ üzerindeki diğer düğümlere gönderilerek işlemin diğer düğümler tarafından da doğrulanması sağlanır.

Örneğin, birisine gönderilmek istenilen bir paranın gerçekten göndermek isteyen kişide olup olmadığı ağdaki diğer düğümlerde kontrol edilmektedir.

Bazı blok zincir tiplerinde doğrulamayı bütün düğümler yaparken, bazı blok zincirler bütün düğümler tarafından yapılan doğrulamayı gereksiz görerek, sadece belirli düğümlerin bu doğrulamayı yapması şeklinde farklılaşmıştır. Bu farklılaşma, blok zinciri ağındaki trafiği azaltmak, işlem sürelerini kısaltmak, elektrik sarfiyatını azaltmak gibi motivasyonlarla gerçekleştirilmektedir. Bu açılardan fayda sağlarken ağdaki diğer düğümlerin doğulama işlemlerine katılımı engellendiği için ağdaki diğer katılımcıların tam güveni sağlanamamaktadır. Kullanılacak blok zinciri uygulamasına göre hangi tip blok zinciri ağının kullanılacağına karar verilmektedir. İlk geliştirilen blok zinciri ağı olma özelliğine sahip Bitcoin Proof of Work (PoW) algoritmasını kullanarak ağdaki bütün katılımcıların doğrulama işlemini yapmasını sağlamaktadır. Bitcoin bu doğrulama işlemlerine bütün düğümlerin katılımını sağlamak için gönderilen kripto paradan işlem ücreti alarak bu doğrulamayı sağlayan düğümlere ödül vermektedir. Ödülü kazanmak için çalışan düğümlere madenci (miner), yapılan işlemlere ise madencilik (mining) ismi verilmektedir. Bütün düğümler veya bazı düğümler tarafından yapılan doğrulama işlemine ise uluslararası isimlendirmeyle distributed consensus yani "dağıtık uzlaşı" ismi verilmektedir.

3.3.6. Blok Özelliği

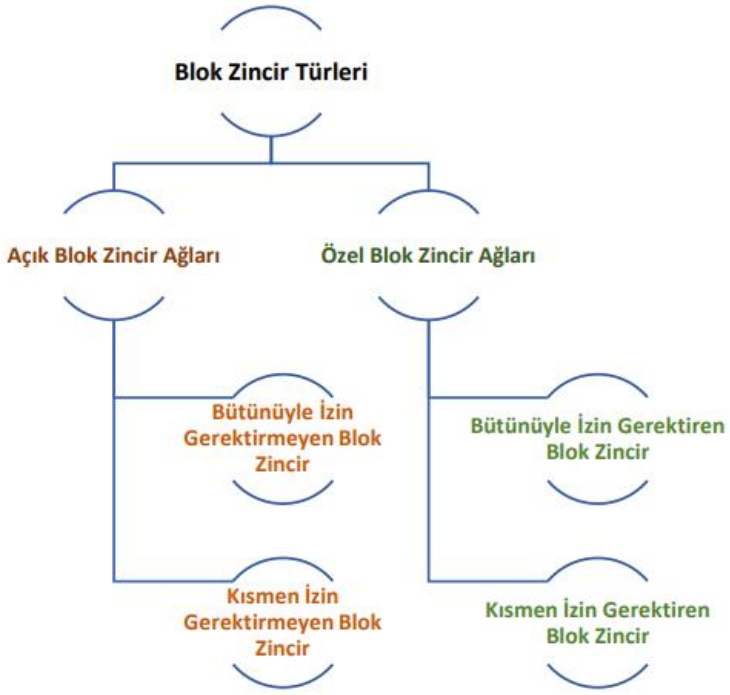
Blok zinciri adını aldığı şekilde blokların zincir şeklinde birbirine bağlanması ile gelişmekte olan bir teknolojidir. Zincir ne kadar büyürse yani blok sayısı ne kadar çoksa zincirin kırılması, daha somut ifadeyle bilgisayar korsanlarınca zafiyete uğratılması o kadar zor olmaktadır. Bunun sebebi, blok zincirin kriptografik özelliği olan kriptografi fonksiyonlarının tek yönlü olarak (sadece şifrelemek amaçlı kullanılıp, çözülmesi çok zordur) çalışmasından kaynaklanmaktadır. Blokların içerisinde ise blok zincir içerisinde yapılan işlemler ve veriler tutulmaktadır. Blok zincirinde tutulan verilerden kasıt, Bitcoin örneğinde, iki kişinin adresi arasında yapılan para transferi bilgisidir. Bloklar belli bir miktar işlem sayısını tutabilecek kapasitede olmakla beraber bu miktar, hangi blok zincirin kullanıldığına göre değişmektedir. Blok kapasitesi dolduğunda blok oluşmuş olur, yeni blok için yeni işlemler yapılması beklenir. Uzlaşı (consensus) algoritmalarına katılan düğümler, bloğa hangi işlemlerin kaydedileceğine, işlemlerin zinciri aldatmaya yönelik zararlı bir işlem olup olmadığına karar vermektedir.

3.4. Blok Zinciri Türleri

Kullanılacak blok zinciri uygulamasının teknik özelliklerine göre blok zinciri ağ yapısı da özelleşmektedir. Ağa dâhil olacak düğümlerin yetkileri bu ağ yapısında en başından belirlenmektedir. Düğümler, blok zincir üzerindeki verileri okuyabilme, yazabilme, uzlaşı algoritmalarına katılabilme gibi izinlere sahip olabilir veya sınırlandırılabilir. Blok zinciri ağı sınıflandırması için Şekil 4'teki yaklaşım kullanılabilir.

Şekil 4

Blok Zinciri Türleri (Gürfidan & Arısoy, 2021, s.58)



3.4.1. Açık Blok Zinciri Ağları

Katılımı herhangi bir kontrole tabi olmayan, isteyen herkesin direkt katılımına olanak sağlayan, kaynak kodları dahi açık kaynak kodlardan oluşan büyük bir dağıtık ağ yapısına sahiptir. Katılımcıların tümü zincir içesindeki verileri okuyabilir ve doğrulukları kullanılan uzlaşı protokolü tarafından onaylandığı takdirde veri yazabilirler. Ancak, yine de bu blok zincir yapılarında farklı uzlaşı protokolleri ile katılımcıların yetkileri açık veya izin gerektiren şeklinde oluşturulabilir (Aktaş, 2018).

Açık blok zinciri ağlarında kontrolsüz katılım esasında katılımcıların ihtiyatlı davranması gereksinimini de beraberinde getirmektedir. Çünkü katılımcıların kötü niyetli kişiler olma olasılığı da bulunmaktadır. Bu durumda açık blok zinciri ağlarında, bloğa yazılacak bilginin doğruluğunu kontrol etmek için uzlaşı protokollerinden en zorlayıcı olanlarının seçilmesi önem arz etmektedir. Bitcoin örneği açık blok zinciri türlerine verilebilecek en iyi örnektir ve uzlaşı protokolü olarak düğümlerin tamamının onayını alarak bloğa veri eklenmesini sağlayan PoW protokolü kullanmaktadır. PoW protokolünde, kötü amaçlı bir kişinin ağın %51'den fazlasını ele geçirerek kendi amaçları doğrultusunda ağa bilgiler yazması oldukça zorlayıcıdır. Hatta ağı manipüle etme amacı uğrunda harcayacağı para işin sonunda başarılı olsa dahi kazanabileceği paradan, Bitcoin ağ zincirinin çok büyümüş olmasından dolayı, çok daha fazla olacaktır. Bitcoin burada güvenliği ön plana koyarak PoW uzlaşı protokolündeki ağ yavaşlığı ve toplamdaki enerji sarfiyatının fazla olması dezavantajını da göze almaktadır.

3.4.1.1. Bütünüyle İzin Gerektirmeyen Blok Zinciri Ağları

Bütünüyle izin gerektirmeyen blok zinciri ağ yapısında, katılımcıların ağ üzerindeki verileri okuyabilmesinde herhangi bir kısıtlama yoktur. Katılımcılar, ağa dâhil olabilir, blok zinciri oluşturabilir ve verileri bir sınırlama olmaksızın okuyabilirler. İlgili ağ yapısında daha önceden belirlenmiş olan uzlaşı algoritmasına, bir diğer deyişiyle uzlaşı protokolüne, uyarak mutabakat süreçlerine katılabilirler.

Bu tip ağ yapılarında amaç, ağa katılan düğüm sayısını artırarak zincir sayısını artırmak, dolayısıyla ağın güvenliğini sağlamaktır. Düğüm sayısının artmasıyla, ağı manipüle etme amacı taşıyan kötü niyetli kişilerin daha fazla çaba sarf etmesi sağlanmış ve bu çabaya karşılık elde edilebilecek kâr miktarı düşürülmüştür. Ağa yeni katılan her bir düğüm hem ağın bir parçası, hem de ağın güvenliğini artıran bir bileşen olmaktadır. Bu uygulamanın en bilenen örneği, kripto para birimlerinden Bitcoin'dir.

3.4.1.2. Kısmen İzin Gerektirmeyen Blok Zinciri Ağları

Kısmen izin gerektirmeyen blok zinciri ağ yapılarında zincir üzerindeki verileri okumak için herhangi bir izin gerekmezken, zincire blok eklemek için izin ihtiyacı

duyulmaktadır. Bu ağ yapısındaki temel amaç zincire eklenen bilgilerin doğruluğu yani bilginin güvenilirliğini sağlamak olduğu söylenebilir.

Bu tarz ağ yapılarında, herkesin erişimine açık olan zincir üzerindeki verilerin olabildiğince çok kişi tarafından görüntülenebilmesi, ancak; uzlaşı protokolüne uygun olarak ağa blok eklenmesi için izin gerekliliği mevcuttur. Bu yapıya en uygun senaryo olarak haber siteleri örnek verilebilir. Haberlerin herkes tarafından okunabilmesi, ancak; yeni bir haber ekleneceği zaman bu haberin sadece izin verilen birkaç farklı haber kaynağı merkezi tarafından ve daha önce belirlenmiş olan uzlaşı protokolüne uygun olarak haberin doğruluğunun onaylanmasıyla mümkündür. Böylelikle, yanlış haberlerin yayılması önlenmiş olmaktadır (Usta ve ark., 2018). Bu örneğe benzer yapıda, çevrim içi müzik siteleri, çevrim içi sanat galerileri örnek verilebilir.

Kamu kuruluşlarının ve dahi Radyo ve Televizyon Üst Kurulu'nun topluma açık olarak yayınlayacağı haber, bildiri ve içeriklerinin paylaşılmasında bu ağ yapısının kullanılması uygun olacaktır. Bu sayede, haberin veya bildirinin manipülatif kişi ve kurumlarca dışarıdan değil, resmi olarak kurum açıklaması olduğu yönündeki kanaatin oluşabilmesi için toplum veya haberin ilgilisi kişilerce güçlü bir dayanak noktası oluşturacak bir teknoloji kullanılmış olacaktır. Günümüzde TÜBİTAK, kamuda kullanılan açık kaynak kodlu yazılımların blok zincir tabanlı dağıtık olarak çalıştıracak bir proje üzerine çalışmaktadır. Üst Kurul, blok zincir ağı üzerine çalışacak insan kaynağını TÜBİTAK ile birleştirerek daha etkin bir sonuç alacaktır. Blok zinciri ağları, doğası gereği katılımcısı arttıkça güvenliği artmaktadır. Bu açıdan da düşünüldüğünde, TÜBİTAK gibi kamu kurumları ile ortak çalışmalar yapmanın, blok zinciri teknolojisinin ülkemizdeki gelişimini destekleme konusunda faydası büyük olacaktır. Teknik açıdan değerlendirildiğinde; günümüz teknolojiyle merkezi ve tek bir kaynaktan yapılan haber ve bildiriler, blok zincirdeki birçok doğrulayıcı kamu kurumu tarafından doğrularak paylaşılan haber ve bildirilere göre zafiyete daha fazla maruz kalma ihtimali vardır.

3.4.2. Özel Blok Zinciri Ağları

Özel blok zinciri ağları açık blok zincirine göre daha küçük ve kapalı ağlardır. Genellikle şirket veya kurumlar tarafından oluşturulmuş, toplumun kullanımına kapalı ve kendi ihtiyaçları doğrultusunda özel olarak ağı oluşturuluş blok zinciri tipidir. Bu blok zinciri

tiplerinde katılımcılar birbirine güvenen kişilerden oluşmaktadırlar ve paylaşılan veriler yüksek gizlilikteki verilerdir. Örneğin; günümüzde North Atlantic Treaty Organization (NATO)'nun belge paylaşımında blok zinciri teknolojisinin kullanımı tartışılmaktadır (Konrad Wrona, Michal Jarosz, 2018). NATO'nun paylaşacağı yüksek güvenlik gerektiren belgeler yine kapalı blok zinciri ağlarında yapılabilecektir.

3.4.2.1. Kısmen İzin Gerektiren Blok Zinciri Ağları

Kısmen izin gerektiren blok zinciri yapılarında, zincir üzerinde blok oluşturabilmek için herhangi bir izine ihtiyaç duyulmamaktadır. Ancak, zincir üzerindeki veriler ancak izinli kişiler tarafından okunabilmektedir. Buradaki amaç, verilerin yalnızca yetkili kişilerce okunabilmesi ve verilerin güvenliğinin ağa katılan düğümlerin artırılmasıyla sağlanmasıdır.

Bu ağ yapısı, bir kayıtçı sistemi ile örnek verilecek olursa, ilgili sistem herkese açık vaziyette bulunmaktadır. İsteyen herkes bu sisteme girerek istediği işlemi yapabilir. Ancak bu yapılan işlemler sistem tarafından kayıt edilmektedir. Eklenen bu kayıtların bilgisi (bilginin ham hali değil, yalnızca meta datası paylaşılmakta) ise yine ağın katılımcısı olan bütün düğümler ile paylaşılarak zincir oluşturulması sağlanır. Böylelikle zincirin uzunluğu artarak güvenliği artmış olur. Ancak, ilgili kayıtlara ağın sadece yetkili katılımcıları erişebilmektedir. Daha gündelik bir örnekle açıklamak gerekirse, herkese açık olarak yapılan anket sistemi örnek olarak verilebilir. İsteyen herkes anketin bir katılımcısı yani sistemin bir düğümü olabilir, oy kullanarak kendi bilgisini üretebilir yani kendi bloğunu oluşturabilir ve bu blok, blok zinciri yapısı itibariyle diğer düğümlerle paylaşılır. Ancak, sistemin hiçbir kullanıcısı kimin hangi oyu kullandığını göremez, sadece anketör kişiler, yani; sistemin yetki verdiği kişiler bu bilgileri görebilir.

Blok zincirinde temel prensip olan, zincir uzunluğunun atmasıyla ağın manipülasyonun önlenmesi ve ağın güvenliğinin artması prensibi burada kullanılmaktadır. İsteyen herkes tarafından ağın katılımcısı olmanın önü açılmış, ancak; verilerin gizliliği sebebiyle verilerin yalnızca yetkili kişilerce görüntülenebilmesi sağlanmıştır. Burada en önemli sorun, verileri görmeye yetkili olmayan ancak ağın katılımcısı pozisyonunda olan düğümlerin ağa katılımını teşvik etmektir. Bu teşvik, uzlaşı protokolüyle çeşitli ödüllendirmelerle sağlanmaktadır. Bir müzik indirme uygulaması için bu ödül daha çok müzik indirmeye izin vermek olabilirken, kripto paralar gibi finansal uygulamalarda her

yapılan transferin doğruluğunu onaylayan düğümlere bu transferden komisyon vermek şeklinde ödüller verilerek teşvik sağlanabilmektedir. Bu gibi somut kazançların yanı sıra; örneğin anket ve oylama uygulamalarında ödül, kişinin kendi düşüncesini yansıtan bir takım veya gruba oy kullanmasıyla, fikirlerini daha ses getirir hale getirme dürtüsü olabilmektedir.

Üst Kurul ve diğer kamu kuruluşlarındaki anket ve oylama işlemleri bu ağ yapısı kullanılarak bilgi güvenliği günümüz teknolojilerine göre daha fazla korunmuş olabilir. Bu uygulama blok zincire en uygun uygulamalar arasında yer almakla birlikte oylama ve anketlerdeki güvenlik sorununu daha iyi bir şekilde çözebilen bir teknoloji olmuştu. Yani blok zincir ne zaman kullanılır, ne zaman kullanılmaz sorusundaki ne zaman kullanılmalı sorusuna verilecek uygulamalar arasında yer almaktadır. Günümüzde yaygın olarak kullanılan ve internet üzerinden yapılan oylama ve anketler, merkezi bir veya birkaç tane sunucu üzerinde çalışmaktadır. Bunun dezavantajı bu sunucuların zafiyetini tespit ederek sunucuya erişen yetkisiz bir kişinin oylama sonuçlarını etkileyebilmesi veya sonuçlara erişilemez hale getirebilmesi ihtimalidir. Ancak dağıtık sistemlerde tek bir düğümün (sunucu veya bilgisayar) zafiyete uğraması diğer düğümleri etkilemeyeceğinden sistem halen güvenlidir. Öyle ki, sistemdeki birçok düğüm zafiyete uğrasa dahi blok zincir ağının yani bilginin doğruluğu ve erişim halen mümkündür. Örneğin, PoW uzlaşı algoritmasında ağdaki bütün düğümlerin en az %51'i, Avalanghe uzlaşı algoritmasında ise ağdaki bütün düğümlerin en az %80'i ele geçirilmediği durumda sistem halen güvenlidir. Ayrıca günümüz sistemleri DDoS ataklarını önemli ölçüde durdurabilmesine rağmen %100 bir çözüm mümkün değilken, Bitcoin'in altyapısında kullanılan PoW uzlaşı algoritması DDoS ataklarına karşı %100 koruma sağlamaktadır. Buradan görüleceği üzere; merkezi sistemlerde bir sunucunun ele geçirilmesiyle veri güvenliği zafiyete uğrarken, 100 katılımcısı olan blok zincir ağında 80 sunucunun birden ele geçirilmesi gereklidir. Zincire katılan düğüm sayısı arttıkça ve uzlaşı algoritmaları geliştikçe ağı manipüle etmek ciddi boyutta zorlaşmaktadır.

3.4.2.2. Bütünüyle İzin Gerektiren Blok Zinciri Ağları

Bütünüyle izin gerektiren blok zinciri yapılarında zincire blok eklemek, verileri okumak ve uzlaşı protokollerine katılmak için izin gerekmektedir. Dışarıya tamamen kapalı olan bu blok zinciri yapılarının katmanlı bir güvenlik sağlamak amaçlı üst düzey güvenlik

isteyen uygulamalarda kullanılması yerinde olmaktadır. Askeri teknolojiler, sağlık ve finans uygulamaları bu tarz blok zinciri yapısını kullanmanın en uygun olacağı yapılardır.

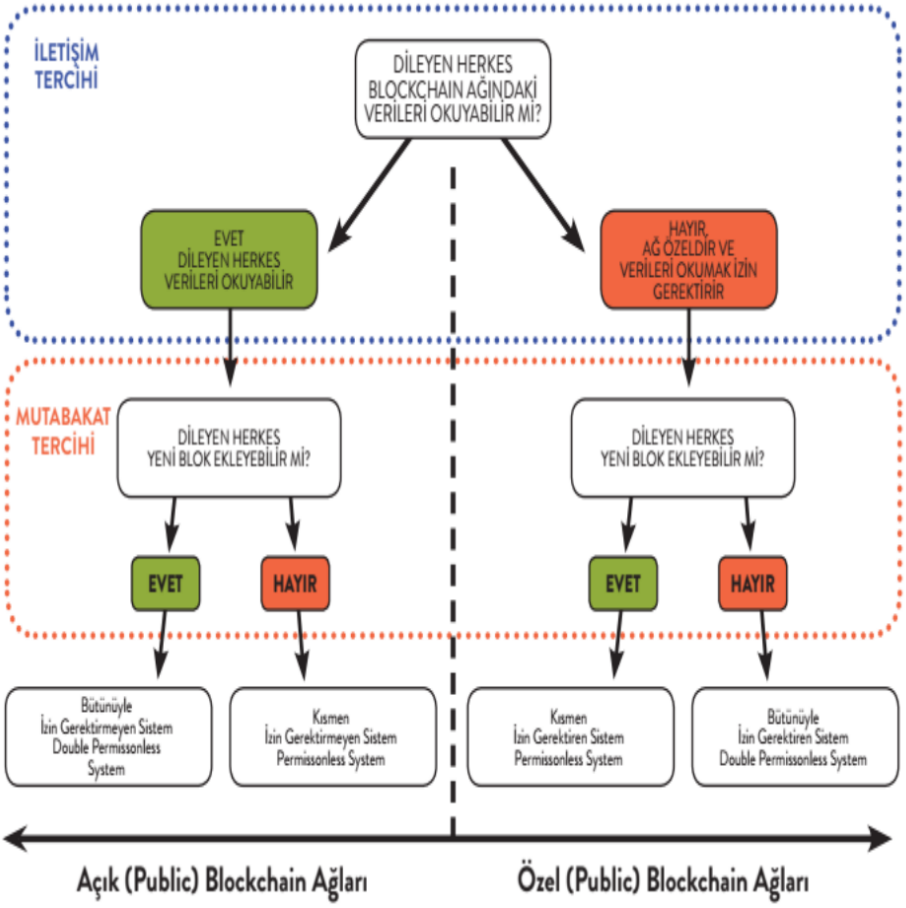
Kamu sektöründe bu tip blok zinciri yapıları için, kullanımının en uygun olduğu sistem, hali hazırda kullanmakta olduğumuz e-nabız uygulamasıdır. E-nabız uygulamasına sadece doktorlar ve hastaneler veri ekleyebilmekte ve eklenen bu verileri yine yalnızca doktorlar görebilmekte. Hastalar kendi verilerini kısmen görebilse de başka hastaların verilerini hastalar görüntüleyememektedir ve sisteme veri ekleyememektedir (kısmi olarak kendileriyle alakalı boy kilo gibi kritik olmayan verileri ekleyebilmektedirler) (e-Nabız). E-nabız sisteminde her bir doktorun kullandığı bilgisayar düğüm vazifesi görmekte, doktorlar verileri hem ekleyerek zincire blok oluşturabilmekte hem de diğer doktorların oluşturduğu verileri okuma yetkisine sahip olmaktadır. Uzlaşı protokollerine bütün doktorların bilgisayarları veya ağda oluşabilecek yükü azaltmak adına bazı doktor veya sistem yöneticilerinin bilgisayarları katılarak güvenlik üst seviyede sağlanabilmektedir. Kamuda veri güvenliğinin sağlanmasında e-devlet uygulamaları öncelik göstermektedir. En önemli e-devlet uygulamalarından sayılabilecek e-nabız uygulaması ise tezimizde savunduğumuz kamu sektöründeki veri güvenliğinin sağlanmasında blok zinciri teknolojisinin en önemli kullanım alanı olduğu düşünülmekte ve bu alanda araştırma ve geliştirmelere ihtiyaç olduğu öngörülmektedir.

RTÜK özelinde ise yine kamu sektöründe kullanılmakta olan elektronik belge yönetim sistemi (EBYS) uygulamalarında blok zinciri teknolojisinin büyük fayda sağlayacağı düşünülmektedir. Her kurumda kullanılmakta olan EBYS sunucuları birer düğüm olarak kurgulanıp, bütünüyle izin gerektiren blok zinciri yapısıyla sadece kamu kurumlarının katılım sağlayacağı bir ağ yapısı hali hazırda kullanılmakta olan EBYS hizmetinin güvenliğini sağlamada yardımcı olacağı değerlendirilmektedir. Önerilen sistemde, her bir sunucu veri üretebilir, uzlaşı protokollerine katılabilir, ancak; yalnızca görmekte yetkili oldukları bilgileri görebilmektedirler. EBYS'de blok zincirinin kullanımı üzerine araştırma ve geliştirmelerin bu alanda da büyük fayda sağlayacağı öngörülmektedir.

Blok zinciri türleri görsel olarak özetlenecek olursa, aşağıda verilen genel özellik şeması (Şekil 5) faydalı olacaktır.

Şekil 5

Blok Zincirlerinin Genel Özelliklerinin Gösterimi



3.5. Bitcoin'in Güvenilirliğini Sağlayan Unsurlar

Ortaya çıkışıyla beraber blok zinciri konseptinin yaygınlaşmasını sağlaması sebebiyle Bitcoin, blok zinciri 1.0 olarak nitelendirilmektedir. Bitcoin'in güvenilirliğini sağlayan birkaç unsur şu şekilde sıralanabilmektedir.

3.5.1. Kimlik Denetimi Özelliği

Kimlik denetimi özelliği, bir paranın veya verinin doğru kişiye gidip gitmediğinden emin olunması prensibini ifade eder.

3.5.2. Veri Bütünlüğü:

Siber güvenliğin sağlanması için, genel kabul görmüş üç unsurdan bahsedilmektedir. Bu üç unsur; gizlilik, erişilebilirlik ve bütünlük unsurlarıdır. Verinin yetkisiz kişiler tarafından görüntülenmemesini sağlamak gizliliği ifade ederken, istenilen zamanda bu veriye ulaşılabilmesi ve erişimin engellenemez olması erişilebilirlik unsurunu ifade etmektedir. Bütünlük unsuru; verinin belirli bir parçasının değil, bir bütün olarak tamamının korunmasını ifade eder.

Blok zinciri konseptinde bahsedilen bütünlük unsuru daha gündelik bir örnekle, kripto paranın çifte harcanma hatasının olmaması ve kötü niyetli kişilerin yapılan işlemleri değiştirerek kendilerine çıkar sağlayamaması gibi verinin bütün olarak doğruluğunu garanti eder.

3.5.3. Kullanılabilirlik Özelliği:

Bitcoin'in bir diğer önemli özelliği ise barındırdığı kripto paraların istenilen zamanda kullanılabilir, harcanabilir ve erişilebilir olması özelliğidir. Yani kripto para sisteminin belli bir zamanda kapalı olma durumu yoktur. Sistem içerisinde bulunan düğümlerden biri kapalı olsa dahi ağ üzerindeki diğer düğümler açık olduğu için sistem daima çalışır durumdadır. Kapalı düğüm/bilgisayar tekrar açıldığında diğer düğümlerden geçmiş bilgileri toplayarak üzerindeki bloğa daha sonra yazabilmektedir.

3.5.4. Gizlilik:

Günümüz dünyasında gizlilik ve mahremiyet oldukça ön plandadır. Mahremiyet sayesinde insanlarda güven duygusu oluşabilmekte ve rahat hareket edebilmektedir. Blok zincir teknolojisindeki mahremiyet özelliği, günümüzde bankacılıkta ve diğer alanlarda da kullanılmakta olan teknolojiden daha fazlasını sağlamaktadır. Bir diğer deyişle anonimlik özelliği blok zincirin en güçlü olduğu konulardan bir tanesidir. Örneğin, bir kişiye gönderilecek yüklü miktarda bir paranın kim tarafından ve ya kime gönderildiğinin gizli kalması blok zincirin bir diğer önemli ve blok zincirin güvenliğini sağlayan unsurudur (Houmansadr A., 2015).

BÖLÜM 4

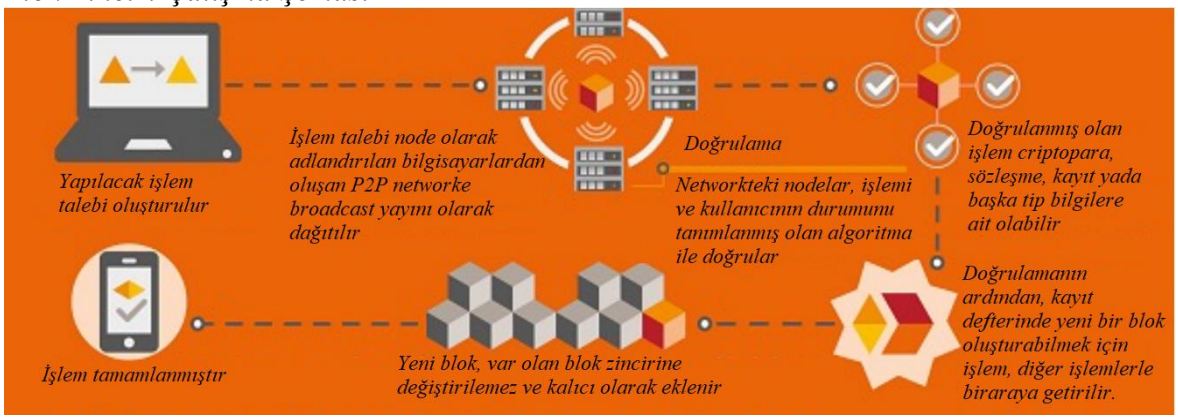
4. BLOK ZİNCİRİ NASIL ÇALIŞIR?

Blok zinciri tarihi gelişimi ve neden blok zincire ihtiyaç duyulduğu konularından sonra, blok zinciri teknolojisinin teknik detayları bu bölümde anlatılarak konunun netlik kazanması amaçlanmaktadır.

Blok zinciri basitçe bir kayıt defteridir. Kayıt defteri üzerine, blok zincirinin oluştuğu günden itibaren üretilen bütün verilerin birer kopyası yazılmaktadır. Bu üretilen veriler belli bir miktara ulaştığında blokları oluştururlar. Örneğin; bazı blok zincirlerinde yüz veri üretilip bir araya geldiğinde blok oluşurken, bazılarında bin verinin birleşimi bir blok oluşmasına müsaade edebilir. Oluşan bloklar ise bir araya gelerek kırılması zor zincirler üretirler.

Şekil 5

Blok Zinciri Çalışma Şeması



Şekil 5'te blok zincirinde bir işlem yapılmak istendiğinde arka planda gerçekleşen işlemler gösterilmiştir. Örneğin, A kişisinden B kişisine para göndermek istenildiğinde, sırasıyla blok zincir ağında aşağıdaki işlemler gerçekleşir.

1. Yapılacak para gönderme işlemi mesaj olarak hazırlanır.

2. Oluşturulan işlemin mesajı ağdaki herkese, yani bütün düğümlere (node) dağıtılır.

Bu dağıtma yani ağdaki düğümlere mesajı duyurma işlemi, bilgisayar ağlarında yayın olarak adlandırılır. Yayının herkese yapılması ise broadcast yayını olarak adlandırılır. Mesajı yayınlamak isteyen düğüm kendine bir ağ aracılığıyla bağlı olan düğümlere bu mesajı broadcast yöntemiyle duyurur. Bu mesajı alan düğümler ise yine kendilerine bağlı olan düğümlere ilgili mesajı broadcast yapar. Broadcast mesajı bu yöntemle ağdaki bütün düğümlere (node) mesajı ulaştıracak şekilde yayını yapılmaya devam eder. Blok zinciri ağının ilk oluşturulduğu günden itibaren yapılan işlemlerin bütün düğümlere (node) yayın yapılmasıyla, kayıt defterindeki işlemlerin birer kopyası bütün düğümlere de kaydedilmiş olmaktadır. Aynı zamanda bu kopyaların tamamı bir biriyle aynıdır. Yani bir düğümdeki kayıt defteri başka bir düğümdekiyle aynıdır.

3. Yayını yapılmış olan işlem bütün düğümler tarafından, düğümlerdeki kayıt defterine bakılarak kontrol işlemin güvenilirliği kontrol edilir. Örneğin, gönderilmek istenilen bu paranın daha önce gönderilip gönderilmediği kontrol edilir. Bu işlem sayesinde Bölüm 1'de bahsi geçen, blok zincirin güvenirliğini sağlayan özellik olan veri bütünlüğü özelliği sayesinde çifte harcamanın gerçekleşmesi önlenmektedir. Ya da parayı göndermek isteyen A kişisinde bu paranın bulunup bulunmadığı yine düğümler tarafından kayıt defterlerine bakılarak kontrol edilir. Eğer bütün kontroller sonucunda işlemin gerçekleşmesinde bir sorun görülmezse düğümler tarafından onay mesajı gönderir (bu onaylama ve kontrol işlemini yapacak olan düğümler farklı blok zinciri ağlarında farklılık gösterebilir. Bitcoin gibi PoW uzlaşı algoritması çalıştıran ağlarda bütün düğümler tarafından bu doğrulama işlemi gerçekleştirilirken, izin gerektiren blok zinciri ağlarında belli birkaç düğüme bu görev verilebilir. Bu, blok zinciri ağını oluşturan kişinin problemi çözmek için belirleyeceği yola en uygun olan algoritmayı seçmesiyle ağı oluştururken en başta belirlenir). Onay mesajını gönderecek olan düğümler, onay mesajını gönderirken kendi aralarında yarışa girmektedirler. Bu yarış, sistem tarafından verilen kriptografik bir puzzle çözme yarışıdır. Bitcoin platformunda yarışın ödülü, onaylama işlemi gerçekleşirken sistem tarafından üretilen Bitcoin'i kazanma olurken, farklı konsept blok zinciri ağlarında farklı ödüller verilmektedir. Örneğin; blok zincir ağında müzik indirme uygulaması yapılacak olursa, yarışın kazananına daha fazla müzik indirmek için kredi sağlanması şeklinde olabilir. Ancak, belirlenen ödül ne olursa olsun açık blok zinciri ağlarında teşvik vermek gereklidir. Aksi halde, yarışı kazanmak için harcanacak elektrik ve

donanım maliyetinden dolayı düğümlerin bu yarışa girmek veya doğrulama işlemi yapmak için gönüllü olması beklenemez. Katılımcılarının birbirine güvendiği özel blok zinciri ağlarında bu tarz teşviklere gerek olmaksızın düğümlerin her halükarda işlem yapacağı varsayılarak güvene dayalı bir uzlaşı algoritması belirlenmesi mümkündür. Blok zinciri ağında tek bir düğümün değil, çoğunluğu oluşturan sayıda düğümlerin veya sistem tarafından belirlenmiş olan belli başlı düğümlerin onaylama işlemine karar vermesi uzlaşı protokolleri ile belirlenir. Uzlaşı protokolü ile belirlenen en az sayıdaki düğümün işleme onay vermesi durumunda işlem gerçekleşebilir.

4. İşlemin gerçekleştiğine dair bilgi kayıt defterlerine kaydedilir. Düğüm üzerinde bulunan kayıt defterinde birden çok verinin birikmesi ile bir blok oluşur. Her bir blokta tutulacak veri sayısı sistem tarafından belirlenmektedir.

5. Oluşan blok, hali hazırda bulunan blok zincir ağına bir zincir olarak eklenir. Bloğun zincire eklenmesi, blok zinciri uygulamalarında işlemin tamamlandığı anlamını taşımaktadır.

Blok zinciri ağlarında zincir ne kadar çoksa, bir diğer deyişle zincir ne kadar uzunsa, blok zinciri ağı o kadar güvenlidir anlamına gelmektedir.

4.1. Blok Zincirde Merkeziyetsizlik

Blok zincirinde yeni yapılan bir işlemin bitmesinin akabinde, yani bloğun oluşup zincire eklenmesinin akabinde, bütün düğümlerdeki bilgilerin güncellenmesi gerekmektedir. Bu bilginin güncellenmesi, peer-to-peer denilen eşlenikler arası yapı vasıtasıyla gerçekleşmektedir. Birbirine eşit hiyerarşide bulunan, yani merkeziyetsiz bir yapıdaki, bilgisayarların bilgiyi kendi aralarında dağıtması sonucu bilginin ağ üzerinde dolaşması işlemidir.

Eğer ki, blok zinciri ağına sonradan katılan bir düğüm varsa, bu düğüm kişi veya kurum bilgisayarı olabilir, ağ üzerinde geçmişten günümüze kadar yapılmış bütün işlemlerin bir kopyasını kendi üzerinde de tutma zorunluluğu bulunur. Örneğin Bitcoin blok zinciri ağında geçmişten günümüze 726,086 blok oluşturulmuştur. Bitcoin madenciliğine yeni

başlayan kişi bu blokların tümünü kendi üzerinde tutmaya başlayarak sisteme dâhil olur. Gerçek şu ki, bahsi geçen 726,086 blok sayısı gün geçtikçe artmakta ve bunun bir sonu bulunmamaktadır. Dolayısıyla, bu kadar fazla bloğu okuma/yazma işlemi yapması için sisteme dâhil olan bilgisayarın güçlü bilgisayarlar olması gerekmektedir (Özsoy Adnan, 2020). Gündelik kullanım için üretilen orta halli bir bigisayarlar ve işlemciler bu büyüklükteki matematiksel işlemleri yapamayacaktır. Kripto para madenciliği için matematiksel hesaplamalar gibi birbirini takip eden işlemlerin hızlı bir şekilde işlenmesini sağlayan GPU denilen donanım parçaları kullanılmaktadır. Ayrıca bu donanımı çalıştıran yazılım, yine gündelik kullanım için üretilen seri hesaplama yazılımları değil, paralel hesaplama programları kullanılmaktadır.

4.2. Blok Zincirin Güvenliğini Sağlayan Unsurlar

Günümüz ağ teknolojileri ve yazılımlarını daha güvenli yapmak konusunda akademik ve profesyonel çalışmalar sürmektedir. Bu süre içerisinde sistemler ne kadar güvenli hale getirilmiş olunursa olunsun, çeşitli sebeplerle %100 bir güvenlikten hiçbir zaman söz edilememektedir. Ancak blok zincir teknolojisi, güvenliği daha önce hiç olmadığı adar artırmaktadır. Bu bölümde blok zincirin günümüz sistemlerine kıyasla güvenliğinin fazla olması birkaç hususta tarif edilmektedir.

Zincir yapısı, blok zincirin güvenliği sağlayan başlıca unsurlardan biridir. Zincir yapısında; örneğin Bitcoin'i ele alacak olursak bir bloğun geçerli sayılabilmesi için %50+1 oy gereklidir veya diğer yönden ağın manipüle edilebilmesi için yine ağın %50+1'inin ele geçirilmesi gereklidir. Örneğin blok zinciri ağında on adet düğüm varsa, bunlardan altı tanesi zararlı bir koalisyonla birleştilerse var olmamış bir işlemi olmuş gibi gösterebilir, diğer dört katılımcı buna karşı çıksa bile ağın çoğunluğu işlemi doğru kabul ettiği için işlem geçerli kabul edilmektedir. Bu sebeple, ağdaki katılımcı sayısı yani düğüm sayısı ne kadar artarsa kötü niyetli kişilerin ağın çoğunluğunu ele geçirme kabiliyeti bu oranda azalır. Bitcoin, Etherium gibi kripto para ağının güçlü güvenlik özelliği bu katılımcı sayılarının çokluğuna bağlıdır.

Güvenliği sağlayan bir diğer özellik, düğümlerin onay mesajı gönderirken kriptografik puzzle'ı çözmesi gerektiğinden dolayı, bir düğümün birden fazla oy gönderememesidir. Bu kriptografik puzzle oldukça zor bir matematiksel problemdir. Problemin çözülmesi için

gerekli bilgisayar/elektrik gücü, ağın diğer katılımlarının oylarını geçebilecek seviyede fazladan oy kullanma durumunu güçleştirmektedir.

Bloklara yazılmış olan işlemleri değiştirememe özelliği, blok zincirin bir diğer güvenlik özelliğidir. Bloklar üzerindeki işlem tarihçesini değiştirmek isteyen kötü niyetli kişi, bloğun sonrasında gelen bütün blokların iş kanıtını çözmesi gerektiğinden dolayı bu yeni iş kanıtlarını çözmek için fazladan bilgisayar gücü ve elektrik gibi kaynaklar tüketmektedir. Öyle ki, büyük blok zinciri uygulamalarında, işlemlerin tarihçesini değiştirirken harcanan enerji ve iş gücü, blok üzerindeki işlemleri değiştirebilmiş olsa dahi kazanacağı kazançtan çok daha büyük olmaktadır. Diğer taraftan bakıldığında, işlemleri manipüle etmek için harcanan enerji legal işlerde kullanılsa sistemin ödülü daha fazla kazanç getirecektir. Bu vesileyle, sistem, katılımcılarını legal işlemler yapmaya teşvik etmektedir.

Kötü niyetli işlemlerden biri olarak aynı paranın iki defa harcanma problemi blok zinciri ağı tarafından kolaylıkla engellenmektedir. İşlem tarihçesini ağın bütün doğrulayıcıları kontrol etmektedir. Yani aynı kripto paranın birden çok yerde kullanılmadığını bu doğrulayıcılar garanti etmektedir. Ağdaki her bir madenci harcanacak paranın ilk defa harcandığına dair onay göndermekte, bu onayın ardından işlem geçerli sayılmakta ve işlem kanıtı oluşturularak bloğa yazılmakta, ardından zincire eklenerek değiştirilmesi zor hale getirilmektedir (Houmansadr Amir, 2015)

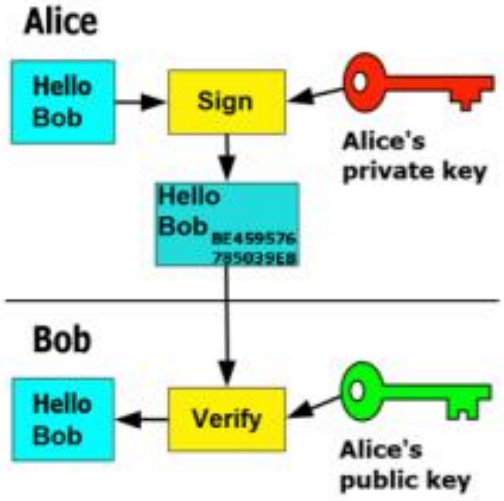
En yaygın ve en fazla blok sayısına sahip blok zinciri uygulamalarından biri olan Bitcoin'in güvenliği genel başlıklar altında tarif edilecek olursa bu başlıklar kimlik denetimi özelliği, işlem bütünlüğü, erişim ve güvenlik olarak sıralanabilir. Bahsi geçen bu dört konu başlığı esasında siber güvenliğin sağlanmasında aranan dört temel unsurdur. Siber güvenliğin dört saç ayağını oluşturan bu unsurların Bitcoin özelinde nasıl sağlandığını göstermek için konu başlıkları incelenecektir.

4.2.1. Kimlik Denetimi (Authentication)

Bitcoin'deki açık anahtar kriptografisi ile oluşturulan dijital imzalar sayesinde bir işlem içerisinde bulunan gönderici ve alıcı tarafın doğru kişiler olduğu, taklit olmadığı garanti edilir. Açık anahtar şifrelemesi Bitcoin'in kriptografik yapısını oluşturan unsurlardandır. Açık anahtar şifrelemesi, basitçe, "Hello Bob" mesajı gönderen ve alan iki kişi üzerinden anlatılacak olursa;

Şekil 6

Açık anahtarlı şifreleme (IQT News , 2019)



Şekil 6 üzerinde gösterilmekte olan "Hello Bob" mesajı her türlü gizli mesajı, gizli kimliği veya her hangi bir gizli bilgiyi ifade eder. Bu mesajın ancak gönderici Alice ve mesajı alan Bob tarafından görüntülenmesi gerekmektedir. Bu sebeple, Alice, başlangıçta sadece kendisinin görebildiği mesajı, Bob'un herkes tarafından açıkça bulunabilen açık anahtarıyla matematiksel işleme sokarak şifreler. Bob'a gönderilecek her türlü mesaj için yine Bob'un açık anahtarı kullanılır. Daha sonra bu şifreli veri ağ üzerinde gönderilerek Bob'a ulaşması beklenir. Bu şifreli veri ancak Bob'un gizli anahtarıyla çözülebilecektir. Çünkü kriptografik özet fonksiyonu ile kişinin açık anahtarı, aynı kişinin gizli anahtarından üretilmektedir. Dolayısıyla gizli anahtara sahip olmayan kötü niyetli kişiler şifreli mesajı ele geçirseler dahi gizli anahtarı bilmedikleri için onlar için anlamsız bir veri elde etmiş olurlar. Burada dikkat edilmesi gereken ve kişinin saklamakla yükümlü olduğu ise gizli anahtarıdır. Gizli anahtar ele geçirildiği takdirde, kişiye gönderilen bütün gizli veriler çözülebilecektir.

Bitcoin özelinde, gönderici ve alıcı arasında gerçekleşen bu dijital imza işlemi kişilerin kimlik doğrulama işlemini sağlamaktadır.

4.2.2. Veri Bütünlüğü (İntegrity)

Veri bütünlüğünden kasıt, bir verinin bir parçasına değil tamamına eksiksiz olarak erişilmesi, verinin kötü niyetli kişilerce değiştirilememiş olmasını ifade eder. Bir başka

deyişle verinin doğruluğu ve tutarlılığının güvencesi anlamına gelir (Süngü Murat, 20 Temmuz 2020). Örneğin, ağ üzerinde bulunan bir kişinin başka bir kişi gibi davranıp onun paraları üzerinde işlem sağlayamaması Bitcoin'in veya blok zinciri ağlarının veri bütünlüğü özelliğindendir.

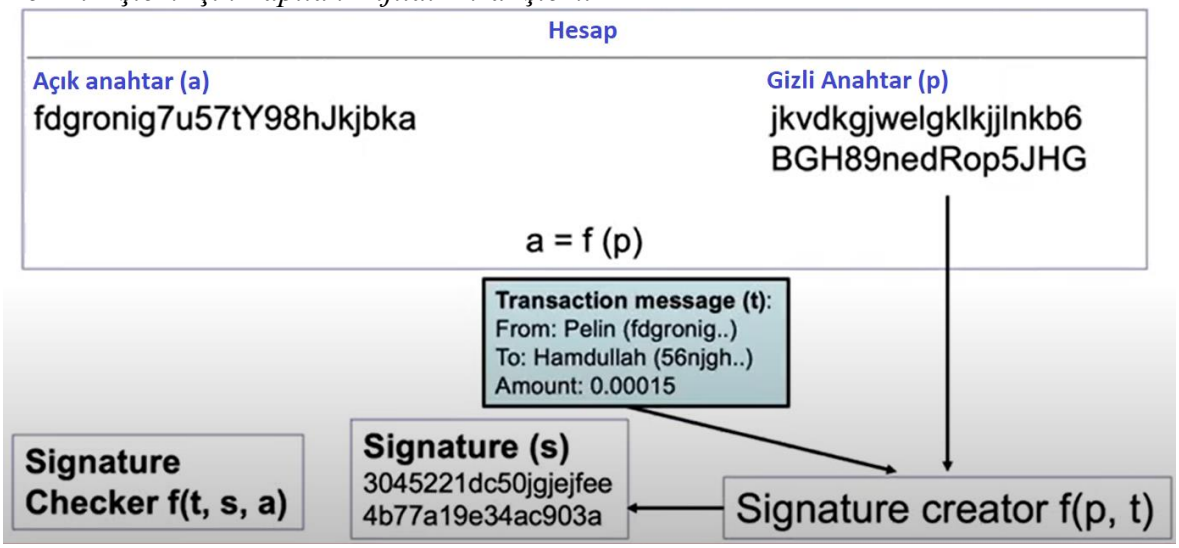
Bitcoin tarihi boyunca yapılan bütün işlemlerin blok zinciri ağı üzerinde tutulduğunu ve bu zincirin oldukça uzun olmasından dolayı manipüle edilerek içeriğinin değiştirilmesinin neredeyse imkânsız olduğu daha önce bahsedilmişti. Bunun teknik veya kriptografik detayı ise yine dijital imzalar ve kriptografik özet fonksiyonlarıdır. Kötü niyetli kişilerin Bitcoin ağındaki kişinin sahip olduğu parayı çalamamasının sebebi yapılan işlemlerin dijital imza ile imzalanmasıdır.

Blok zinciri ağı üzerinde kişinin/kurumun öncelikle bir hesabı bulunmaktadır. Sonrasında bu hesaba ait ve ağdaki herkese yayımlanan açık anahtarı bulunmaktadır. Bir de bu açık anahtara karşılık gelen ve sadece hesabın sahibi tarafından bilinmesi gereken gizli anahtarı bulunmaktadır. Esasen, bu gizli anahtarın ele geçirilmesi, hesabın çalınması (hack) anlamına gelmektedir. Elde edilen gizli anahtar ile anahtarın sahibi kişi adına her işlem gerçekleştirilebilir. O sebeple, gizli anahtarın iyi şekilde muhafaza edilmesi önemlidir. Günümüzün elektronik imza sim kartları aynı şekilde çalışmaktadır. Geçmişteki Bitcoin hikâyelerinde anlatılan, bilgisayarda depolanan Bitcoin'in bilgisayarların çalınmasıyla kaybedilmesi hikâyesi yine gizli anahtarların bilgisayarın içinde bulunması ve bilgisayarla beraber çalınmasından kaynaklanmaktadır.

Bitcoin'de olduğu kadar günümüz dijital imzalarında kullanılan açık anahtar ve gizli anahtar birbiri ile ilişkilidir. Bir diğer ifadeyle birbirinden üretilmektedir. Ancak, başka bir açık anahtara sahip kişi, başka birine ait gizli anahtarı üretemez. Şekil 7'de dijital imza fonksiyonunun nasıl çalıştığı gösterilmektedir.

Şekil 7

Her Bir İşlem İçin Yapılan Dijital İmza İşlemi



Blok zinciri ağında yapılmak istenilen işlem (para göndermek, mesaj göndermek, bilgi güncellemek olabilir) gizli anahtar yardımıyla dijital imza fonksiyonuna sokulur yani mesaj imzalanır. Bu fonksiyon sonucunda çıkan imza (Signature (s)) bir dizi anlamsız rakamdan ve sayıdan oluşmaktadır. Şu anlık bu mesajı anlamlı halde sadece mesajı ilk üreten kişi bilmektedir. Ağdaki diğer katılımcılar daha doğru ifade ile onaylayıcılar, yayımlanan ve ilk etapta anlamsız görünen bu mesaj, dijital imza kontrol fonksiyonu (Signature Checker f(t,s,a)) ile bu mesajın imzasını kontrol ederler. Mesajın veya işlemin imzasının geçerliliği kontrol edilen ilk unsurdur. Bu imzanın geçerliliğinin kontrolü mesajın doğruluğundan da önce yapılır. Örneğin kripto para gönderimi esnasında kişinin cüzdanında, göndermek istediği miktardan daha fazla miktarda para olması gerekmektedir. Dijital imza kontrol işlemi bu balans kontrol işleminden de önce yapılmaktadır. Dijital imza kontrol fonksiyonuna giren unsurlar, imzalanmış mesaj ve mesajı imzalayan kişinin açık anahtardır. Bu şekilde kontrol edilen imzalanmış mesaj, işlem sonucunda anlamlı hale gelir ve kontol edici kişi tarafından görüntülenebilir. Yani mesaj, ilk üretildiği andaki gibi açıkça görülebilir.

Dijital imzada özetle, mesajı üreten kişi, mesajını sadece kendisinin bildiği gizli anahtarla şifreler. Bu şifreli mesaj ise ağın bütün katılımcıları/onaylayıcıları tarafından görünebilen, mesajı üreten kişinin açık anahtarı ile deşifre edebilir. Kötü niyetli bir kişi başka bir gizli anahtar (mesajı üreten kişinin gizli anahtarını elde edemediğini düşünürsek) ile mesajı imzalarsa, mesajı üreten kişinin açık anahtarını kullanan imza kontrol fonksiyonu,

hiç anlamlı olmayan yine bir dizi rakam ve sayı mesajı ortaya çıkarır. Dolayısıyla bu işlem geçersiz kabul edilir.

4.2.3. Erişim (Availability)

Blok zinciri ağlarının ve Bitcoin ağının bir diğer özelliği ağa her an katılım sağlayabilme özelliğidir. Bir bilgisayarın ağa katıldığı zaman geçmişten günümüze ağ üzerinde tutulan verilen tamamını yine kendi üzerinde tutması gerektiği belirtilmişti. İlk defa ağa katılacak olan veya hali hazırda ağa katılmış ancak elektrik kesintisi vb. sebeplerle ağdan kopmuş olan bilgisayarların tekrar eski bilgilere erişmesi, bütün broadcast mesajlarının peer-to-peer ağ üzerinde yayılması sayesinde sağlanabilmektedir.

4.2.4. Gizlilik (Confidentiality)

Bitcoin'de tam anonimlik olmamakla birlikte tam anonimliği sağlayan başka blok zinciri ağları bulunmaktadır. Bitcoin yarı anonimlik özelliği kullanmaktadır. (Houmansadr Amir, 2015)

4.2.5. İşlem Sıralaması (Transaction Ordering)

Blok zincirin günümüz finans sistemlerinin ikamesi olarak kullanılmasına ve blok zincirin güvenlik unsurundan bahsedilmesine en büyük etmenlerden biri, aynı paranın iki defa kullanılmasının önüne geçilmesidir.

Günümüz ağ teknolojilerini manipüle etmek, blok zincir ağını manipüle etmekten çok daha kolaydır. Söz gelimi, sistemi kandırmaya çalışan kötü niyetli bir kişi, iki farklı kişiye, aynı parayı, aynı anda göndermeye çalıştığı farz edilirse; örneğin, 50 lira kripto parası olan bir kişi, bu 50 lirayı hem A kişisine hem B kişisine aynı anda gönderme talimatı verirse blok zincir bu işlemi kendi peer-to-peer ağına dağıtır. Ağ üzerinde hangi işlemin daha hızlı yayıldığına göre hangi işlemin geçerli olacağı değişir. Daha önce ağa gönderilmiş bir işlemin dahi, ağdaki yavaşlıktan dolayı, daha geç yayılması ve netice itibarıyla geçersiz olması durumunda mümkündür. Dijital imza, işlemin doğru kişi tarafından yapıldığını garanti eder,

ancak ne zaman yapıldığını, hangi işlemin öncelikli olduğunu garanti etmez. Yani hangi işlemin geçerli olacağı ağın durumuna, işlemin hangi düğüme ne zaman ulaşacağına bağlıdır. Bunun yanında, iki defa harcama problemi olarak isimlendirilen aynı anda, aynı parayı, iki farklı kişiye gönderme problemini blok zincir ağının tüm onay verici düğümleri/madencileri kendi aralarında iletişim kurarak bir diğer deyişle aralarındaki uzlaşı protokolüyle engeller.

Bir bloğun oluşabilmesi için belli sayıda işlemler topluluğunun bulunması gerekmektedir. Tek başına bir işlem blok oluşturmak ve madencilerin bu bloğu zincirlerine eklemesi durumu yoktur. Yapılan bir işlem söz gelimi, bir işlemler havuzunda bekletilir. Belirli sayıda işlem havuzda biriktiği zaman, ağdaki madenci diye adlandırılan düğümler bu işlemleri onaylamak amacıyla alırlar ve bu işlemler havuzundan blok yapmaya uğraşırlar. Bu uğraşı matematiksel bir puzzle çözmektir. Çözülen puzzle sonucu bir rakam üretilir. Üretilen rakam doğru üretildiyse yani puzzle doğru çözüldüyse, bu rakam ağa gönderilir ve madenci kripto para ile ödüllendirilir. Başarılı madencinin ürettiği blok ağ üzerinde dağıtılarak blok zincire yeni blok olarak eklenir.

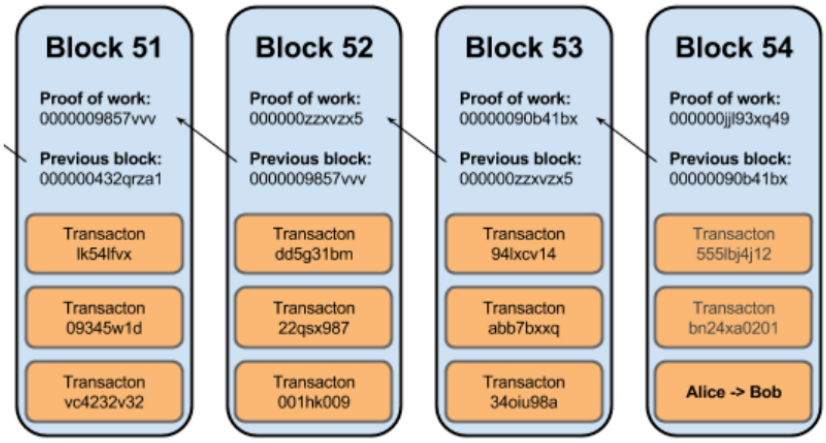
4.3. Blok Zincirin Kriptografik Yapısı

Blokların birbirine eklenmesiyle oluşturulan blok zincir yapısı ve blokların yapısı bu bölümde tarif edilecektir.

Şekil 8'de gösterildiği üzere, blokların her birinin bir numarası bulunmaktadır ve bloklar aynı zamanda kendinden önce gelen bloğun numarasını (şekilde "Previous block" olarak gösterilen satır) kendi bloğunda tutmaktadır. Blokların zincir oluşturmasından kastedilen de aslında budur. Bloklar içerisinde en baş satırda yer alan ve "işlemin kanıtı" olarak Türkçeye çevrilebilen "Proof of work" madenci (miner) tarafından o bloğun oluşması için çözülmüş olan puzzle'ın sonucudur. Blokların içerisinde "Transaction" olarak ifade edilip, turuncu kutularla gösterilenler bloğun oluşması için gerekli işlemlerdir. Dolayısıyla, şekle göre bir bloğun oluşması için seçilen işlem havuzunda en az 3 farklı işlem bulunması gereklidir.

Şekil 8

Blok Zincir Yapısı (Brikman Yevgeniy, 24 Nisan 2014)



Bir bloğun içerisinde, bir önceki bloktan gelen özet çıktısı, yapılan işlemlerin kendi özelliklerinden gelen bir çıktı ve son olarak bu ikisine bağlı olarak hesaplanan "nonce" (number used once) denilen tek sefer kullanılan sayı bulunmaktadır. Nonce değeri Şekil 8'de Proof of work ile gösterilen değerdir. Esasen madencilerin çözmeye çalıştıkları matematiksel puzzle nonce diye adlandırılan sayıyı bulmaktır.

$$f(txn + 521\ tahmini\ sayı\ (random\ guess) + A\ kişisi > B\ kişisi\ 5TL)$$

Örneğin, yukarıdaki formül A kişisinden B kişisine gönderilmeye çalışılan 5 TL'lik para işleminin blok haline gelebilmesi gerekli girdileri göstermektedir. "tnx" bir önceki bloktan gelen kriptografik özet sayısını ifade eder. Fonksiyonun içerisinde ayrıca, bir tane rastgele sayı tahmini yapılmaya çalışılır ve bu sayı nonce diye ifade edilen sayıdır. Sistem, madenciden, A kişisinden B kişisine 5TL gönderme işlemini, nonce değerini ve daha önceki bloktan gelen kriptografik özet sayısını fonksiyona sokarak belirli bir koşulu sağlamasını ister. Bu şart, söz gelimi Bitcoin'de Şekil 8'de gösterildiği üzere Proof of work: 0000009857vvv değerindeki gibi proof of work ifadesinin altı adet sıfırla başlaması gerekliliği olabilir. Eğer proof of work ifadesinin başında daha fazla sıfır olması isteniliyorsa daha zor bir ifade çözülmesi isteniyor demektir. Bitcoin bu zorluk derecesini ağın yoğunluğuna göre kendisi ayarlamaktadır. Ağ çok yoğunsa yani madenci sayısı çok fazlaysa işlemi zorlaştırmakta, diğer zamanlarda daha kolay işlemlerle sisteme blok eklenmesine müsaade etmektedir. Problemi zorlaştırıp kolaylaştırma işlemini diğer blok zinciri uygulamalarında da kullanmak mümkündür. Zorluk derecesi ile belirlenen sayıya ilk ulaşan madenci işlemini kanıtlatmak üzere ağa gönderir. Ardından ağdaki diğer katılımcılar, rasgele sayıyı bulma işlemin doğrularlar. Kriptografik özet fonksiyonlarının doğrulama özelliği,

özeti üretme özelliğinden çok daha kolaydır. Bunun sebebi kriptografik özet fonksiyonlarının tek yönlü çalışmasıdır. Madenci için nonce değerini bulmak zaman, enerji ve güç isterken, madencinin bulduğu nonce değerinin doğruluğunu kontrol etmek oldukça kolaydır. Nonce değerini bulurken madencinin hangi değerleri kullandığını bulmak yine çok zor bir işlemdir. Bu matematiksel zorluk blok zincirin güvenliğini sağlayan bir diğer hususdur.

Şekil 9

Bitcoin'de 778.862'inci Bloğun Örnek Yapısı

Bitcoin Block 778,862

Mined on March 01, 2023 10:58:41 • All Blocks

Details

Hash	00000-2b02d	Depth	6
Capacity	237.45%	Size	2,489,814
Distance	45m 35s	Version	0×20400000
BTC	4,305.5831	Merkle Root	ad-3f
Value	$100,529,252	Difficulty	43,053,844,193,928.45
Value Today	$100,870,900	Nonce	755,587,648
Average Value	1.9998063777 BTC	Bits	386,304,419
Median Value	0.00753371 BTC	Weight	3,993,399 WU
Input Value	4,305.69 BTC	Minted	6.25 BTC
Output Value	4,311.94 BTC	Reward	6.35903987 BTC
Transactions	2,153	Mined on	01 Mar 2023 22:58:41
Witness Tx's	1,929	Height	778,862
Inputs	4,984	Confirmations	6
Outputs	5,794	Fee Range	0-181 sat/vByte
Fees	0.10903987 BTC	Average Fee	0.00005065
Fees Kb	0.0000438 BTC	Median Fee	0.00002820
Fees kWU	0.0000273 BTC	Miner	ViaBTC

Zincirin oluşması için, blok oluşurken üretilmiş olan iş kanıtı (proof of work) bir sonraki blokta önceki bloğun iş kanıtı (previous block) şeklinde tutulmaktadır. Örneğin Şekil 8'de Blok 51'deki bir işlem değiştiği zaman, Blok 51'in iş kanıtı da değişmek zorundadır. Çünkü iş kanıtı bulunurken blok içerisindeki işlemler de fonksiyona dâhil olmaktadır. İş kanıtı değişen Blok 51, geçerliliği sağlattırmak için kendi iş kanıtını "önceki bloğun iş kanıtı" olarak tutan Blok 52'den de değiştirmek zorundadır. "previous blok" değeri değişen Blok 52'nin iş kanıtı da yine değişmek durumundadır. Çünkü Blok 52'nin iş kanıtı fonksiyonuna "önceki bloğun iş kanıtı" girmektedir. Bu şekilde, Blok 51'deki işlemlerden birini değiştirmek isteyen bir kişi, kendinden sonra gelen bütün blokların değerini değiştirmek durumundadır. Zincirdeki blok sayısının uzamasıyla zincirin güvenliğinin artması bu sebeptendir. Şekil 9 gerçek bir bloğun yapısıdır. Bu şekilde gösterilen nonce değeri, bloğun iş kanıtı olan hash değerini üretmesi gereken sayıdır. Gerçek bir Bitcoindeki

bu özet değeri çok daha uzundur (000000000000000000016e49400520adb0fcc760098bbe418a41bb8afc72b02d)

4.3.1. Kriptografik Özet Fonksiyonu

Blok zincirin güvenliğini sağlayan en büyük unsurların başında gelen kriptografik özet fonksiyonu aslında yeni bir teknoloji olmayan ama blok zincirin temelinde kullandığı bir şifreleme yöntemidir. Kriptografik özet fonksiyonunun bazı özellikleri şunlardır; tutarlı, tek yönlü, çatışmaya dayanıklı.

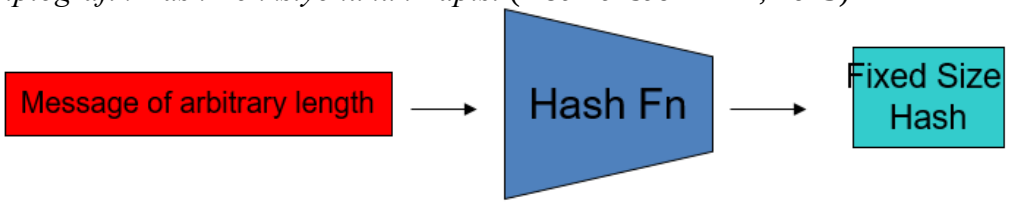
Kriptografik özet fonksiyonuna hash(X) aynı X değeri verildiğinde her zaman aynı sonucu verir. Bu, özet fonksiyonunun kullandığı matematiksel fonksiyonunun değişken olmamasının sonucudur.

Tek yönlü olarak çalışan kriptografik hash fonksiyonunun bu özelliği güvenliği sağlayan en önemli unsurdur. Uzun yıllardır birçok alanda kullanılmakta olan özet fonksiyonu, sisteme izinsiz erişim işlemleri ve tersine mühendislik uygulamalarına karşı dayanıklıdır. Tek yönlü olmasından kasıt, özet(X)=Y şeklinde bir özet fonksiyonu olduğu varsayılırsa verilen X değeri için Y'yi bulmak kolaydır. Ağdaki doğrulayıcı düğümlerin yaptığı işlem aslında budur. Ancak verilen Y değeri için X değerini bulmak oldukça zordur.

Çatışmaya dayanıklı olma özelliği ise, fonksiyonun farklı değerler alması durumunda aynı sonucu üretmesinin düşük ihtimalli olması özelliğidir. Yani, hash(W)=Z fonksiyonunda W girdisi verildiğinde Z sonucu üretilmektedir. Farklı bir değer verildiğinde, örneğin X, sonucun Z çıkma olasılığı çok düşüktür. Bunun blok zincirdeki önemi, eğer farklı girdilere aynı sonuçlar üretebilen bir fonksiyon ile işlem yapılmış olsaydı, ağa saldıran kötü niyetli kişilerin ağ üzerinde değişiklik yapması çok daha kolay olurdu. Söz gelimi, farklı bütün girdi değerleri için aynı sonucu üreten bir fonksiyona hangi değer girilirse girilsin aynı sonucu üreteceği için bloklar içerisindeki işlemleri değiştirmek oldukça kolay olacaktı. Çünkü değişen işlemlerle beraber iş kanıtı değişmeyecek, dolayısıyla zincir üzerinde diğer bloklara müdahale etmeye gerek kalmadan değiştirilmeye çalışılan blok değiştirilebilecekti. Bloklara zincir olma özelliğini kazandıran bu özellik kriptografik özet fonksiyonunun bir özelliğidir.

Şekil 10

Kriptografik Hash Fonksiyonunun Yapısı (Houmansadr Amir, 2015)



Kriptografik özet fonksiyonları Şekil 10'da da görüleceği üzere, hangi uzunlukta mesaj gelirse gelsin çıktı uzunluğu her zaman aynıdır. Örneğin, hash(X)=Z fonksiyonunda X değeri ister tek rakamlı bir sayı olsun, ister 100 bit'lik sayı ve harf dizisi olsun, fonksiyon her zaman sabit bit değerli (örneğin 64 bit'lik) bir sonuç üretir.

Madenciler çözdüğü;

$$f(txn + 521\ tahmini\ sayı\ (random\ guess) + A\ kişisi > B\ kişisi\ 5TL)$$

problemine işlem havuzundaki işlemleri, bir önceki bloğun iş kanıtını ve random guess denilen (nonce) tahmini sayıyı koyarak, istenilen özellikleri sağlayan bir sayı (iş kanıtı/proof of work) bulmaya çalışırlar. Örneğin, istenilen sonuç değerinin ilk on dokuz hanesi sıfır ile başlaması ve başka diğer şartları da beraberinde sağlaması gibi. İstenilen sonuç değerini bulabilmek için madenci, sıfırdan başlayarak bütün nonce değerlerini dener. Yani nonce değeri tamamen rastgele seçilerek bulunur. Zaten güvenli bir kriptografik özet fonksiyonu kullanan bir sistemde, nonce değeri ipucu verecek şekilde, tahmin edilmesi kolay bir değer olmamalıdır. Bu yüzden işlem oldukça zordur ve çokça zaman ve enerji ister.

Günümüzde kripto para madencileri, nonce değerini bulma işlemini birbirlerine kolaylaştırmak için madenci havuzu oluşturmuşlardır. Bir havuza dâhil olan madencilerin her birine farklı sayı aralıklarında sayılar denemeleri istenilmektedir. Yani denenmesi gereken nonce değerleri dağıtılmıştır. Aralarından biri nonce değerini bulduğunda havuzdaki diğer paydaşlara aldığı ödülden dağıtmak durumundadır. Bu şekilde havuz içerisindeki madenciler arasında çıkar birliği bulunmaktadır. Söz gelimi, bir madencinin bir adet bilgisayarı olsa nonce değerini bulmak için 0'dan 1000000'a kadar tek bir bilgisayar üzerinde deneme yapsa, 1000 paydaşlı bir havuzda, 1000 bilgisayara bölüştürülerek yapılan denemeden daha uzun sürede sonuca ulaşma olasılığı yüksektir. Blok zincir ağları ise genel itibarıyla ilk nonce değerini bulan madenciye ödül vermektedir. Bu sebeple madenciler tarafından madenci havuzu çok üyeden oluşan veya bilgisayarları güçlü üyelerden oluşan

madenci havuzlarına üye olmak cazip haldedir. Buradaki sorun, blok zincir merkeziyetsiz yapısıyla ün salmıştı ve güvenliğini sağlayan özelliğini yine bu merkeziyetsiz yapısından almaktaydı. Ancak, madenci havuzlarının oluşmasıyla gelinen nokta, havuzu güçlü olanın ağı ele geçirebileceği sorunudur. Bu durum henüz Bitcoin, Etherium gibi kullanıcı sayısı fazla olan ağlar üzerinde sorun teşkil etmemektedir. Ancak, yine de merkeziyetsizlik vurgusu yapılarak, güçlü olanın sistemi ele geçirebileceği senaryosu ortadadır. Bu sebeple, bu tezin konusu, kripto paralar özelinde blok zincir ağ sistemini tarif ederek, kripto para sektöründe bulunan problemlerden ayrıştırılmış, paydaşlarının (madenci, doğrulayıcı ve işlem gerçekleştiren taraf) tamamı kamu kurumlarından oluşan, kapalı bir kamu blok zinciri ağı tasarlamaktır.

4.4. Blok Zincirin Ağ Yapısı

Bitcoin ilk gündeme gelen ve en çok kullanıcısı bulunan, dolayısıyla en güvenli blok zincir ağlarından biridir. Hemen her blok zincir ağı peer-to-peer ağını kullanmakta ve temel özelliklerde birbirleriyle benzerlik göstermekle birlikte kullandıkları uzlaşı protokollerinde farklılık göstermektedirler. Bu uzlaşı algoritmalarındaki farklılık zincirin yapısında değişiklik göstermekle birlikte, ifade edildiği üzere ağ yapıları üzerinde yine benzer özellik göstermektedir. Bu bölümde başta bitcoin ağ yapısı olmak üzere diğer blok zinciri uygulamalarının kullandıkları uzlaşı algoritmalarından kaynaklanan farklı zincir yapıları ve blokların ağ tarafından onaylanma işlemleri açıklanacaktır.

4.4.1. Bitcoin Ağında Blokların Zincire Eklenmesi

Bitcoin ağı diğer bütün blok zincir ağları gibi peer-to-peer yani noktadan noktaya bağlantı kurarak katılımcılarını kendi arasında haberleştirmektedir. Ayrıca her düğüm, blok zincir ağının kullandığı aynı algoritmayı kullanır. Bitcoin ağında her peer-to-peer düğüm aşağıdaki işlemleri takip edecek şekilde çalışmaktadır.

- Yapılmak istenilen her yeni işlem broadcast yayını ile ağdaki bütün düğümlere (node) yayınlanır.
- Her madenci (miner) yeni gerçekleşecek işlemleri kendi bloğunda iş kanıtlarını bulmak üzere (proof of work) toplar.

- Her düğüm topladığı işlere ait iş kanıtlarını bulmak üzere çalışır. İş kanıtını elde etmek matematiksel olarak zor bir süreçtir, tahminidir ve aynı işlemlere ait iş kanıtını en erken bulan düğüm matematiksel puzzle çözme yarışını kazanır.
- Puzzle'ı çözen düğüm, sonucunu bütün blok zincir ağındaki bütün düğümlere broadcast yöntemiyle dağıtır.
- Ağdaki düğümler bloğu aşağıdaki iki şartın sağlanmasıyla kabul eder.
    - Dijital imzanın kontrol edilmesiyle bloktaki işlemler geçerliliği doğrulanır,
    - Bloktaki bütün işlemlerin kontrol edilesiyle "aynı paranın iki defa harcanması problemi" nin olmadığı teyit edilir.
- Düğümler, bloğu kabul ettiğini duyurur. Düğüm bir bloğu kabul etme işlemini, düğümlerin yeni bir blok oluştuğunda blok içerisindeki önceki özet (previous hash) değerine kabul ettikleri düğümün iş kanıtı özet değerini yazarak yapar.

4.4.2. İki Farklı Zincir Oluşturma Durumu (Tie Breaking)

Blok zincir uygulamalarında yapılmış olan bir işlemin blok oluşturabilmesi için kriptografik puzzle çözmesi gerektiği ifade edilmişti. Ancak iki farklı madenci farklı işlemleri ele alarak iş kanıtı oluşturmaya çalıştıklarında ve aynı anda iş kanıtlarını çözüp ağa onaylatmak üzere gönderdiklerinde zincirin çatallaşması durumu oluşur. Ağ üzerinde milyonlarca düğüm olmasından dolayı bu senaryo çokça gerçekleşmektedir. Her iki blokta onaylanır ve zincire dâhil olur. Ancak aynı anda gerçekleştirilen bu işlem birbirleri arasında öncelik sıralaması olmadığından dolayı, belirli zamanlarda iki tane farklı zincir oluşur. Daha sonra ağdaki düğümler, ağa yeni ekleyecekleri bir blok oluştuğunda, her iki zincirde de bloğun bir kopyasını tutup, en uzun olan taraftaki zincire eklemektedirler. Dağıtık sistemlerde bu duruma nihai tutarlılık (eventual consistency) denilmektedir. Nihai tutarlılık, herhangi bir anda tutarlılık sağlamayan ancak işin sonunda mutlaka tutarlılık sağlayacak olan sistemlere denilmektedir.

4.4.3. İşlemleri Geri Döndürmenin Zor Olması

Bitcoin'in de kullanmış olduğu proof of work uzlaşı algoritması işlemlerin onaylanması için ciddi boyutta enerji harcanmasına sebep olan bir algoritma olmasının en

önemli avantajı bu nispette güvenliği artırmasıdır. Proof of work kullanan algoritmaların özellikle, dayanıklılık (tempering) ve işlemleri tersine çevirme (reverting) gibi kötü niyetli amaçların önüne geçmektedir. Yapılması gereken hesaplamaların büyüklüğü katılımcı sayısının artmasıyla geometrik olarak artmaktadır. Yani zincir büyüdükçe zararlı işlemlere karşı direnç çok daha büyük oranda artmaktadır.

4.4.4. İşlem Onayı Alma

Günümüz finansal sitemlerinde para transferleri saniyeler içerisinde gerçekleşmektedir. Blok zincir ağında ise işlemlerin güvenliği açısından işlemler bu kadar hızlı olmamakta hatta saatler alabilmektedir.

Örneğin Bitcoin bir işlemin yeterince olgun olduğuna karar vermesi için en az 6 blok onayı gerekmektedir (her bir bloğun tahmini 10 dakikada onay verdiği varsayılırsa en az bir saatlik bir süre gerekmektedir). 6 onaydan sonra işlemin doğru olduğu kabul edilerek, bloğun zincire kabul edilmesi ve sisteme yazma işlemi gerçekleşebilmektedir. Eğer iş kanıtı oluşturan bir madenci ödül olarak coin kazanacaksa, bu coin 120 kadar onaydan sonra kullanılabilir hale gelmektedir. İşlerin bu denli uzun sürmesi güvenliği artırma amacı taşımaktadır. Bununda altında yatan kök neden, kötü niyetli kişilerin blok zincir ağının %50'den fazlasını ele geçirip zararlı işlemler yapmasını önlemektir. Yani, özellikle proof of work kullanan bitcoin gibi blok zinciri ağları güvenden kazanırken zamandan kaybetmektedir. Özellikler merkeziyetsizlik vurgusu yapılan bu sistemlerde güveliğin tam sağlandığından emin olmak gereklidir.

Bazı blok zincir uygulamaları başka uzlaşı protokolleri kullanarak para transferi gibi gündelik işleri daha hızlı yapabilmektedir. Ya da özel olarak oluşturulmuş bir blok zincir ağında blok içerisine giren işlem sayısı artırılarak onay süreci hızlandırılabilir. Bunlar oluşturulacak sistemdeki sistem parametreleridir ve verilecek ödün ve kazanılacak kazanç birlikte değerlendirilerek daha farklı sistemler oluşturulabilmektedir.

Özellikle çok daha büyük miktardaki parasal işlemleri gerçekleştirmek için daha uzun süreler beklenilerek güvenliğin artırılmış olması avantajlı bir durum sağlayacaktır.

4.4.5. Mahremiyet Sorunları

Bitcoin özelinde tam mahremiyet bulunmamakta, yarı anonimlik kullanılmaktadır ve blok zincir ağı üzerinde yapılan bütün işlemler uygulama var olduğu sürece orada kalmaktadır. İşlemler silinemediği için daha sonradan açık anahtarların ele geçirilmesi durumunda, kişinin daha önce yaptığı işlemleri bir birine bağlayarak kişinin kimliği dâhil blok zinciri ağı boyunca yapılan bütün işlemleri görme olanağına sahip olmaktadır. Bitcoin tam anonimlik sağlamadığı için mahremiyet konusu bitcoin için bir sorun olarak göz önüne alınabilir. Bitcoin'den sonra tam anonimlik sağlayan blok zincir uygulamaları geliştirilmiştir. Burada oluşan sorun ise tam anonimliği kötü niyetle kullanmak isteyip, iş konusu yasa dışı olan ticaret yapmak isteyen kişilerin bu platformlara yönlendirilmiş olmasıdır.

Bütün bu açık blok zincir ağlarındaki avantaj ve dezavantajlarının yanında, blok zincir uygulamaları sadece parasal konularda değil birçok farklı alanda kullanılabilir. Örneğin sağlık kayıtları tutulan bir sistemde, kayda giren bir veri blok zincir çalışma mantığı gereği yine silinemeyecektir, ancak veri güncellenerek silinmiş gibi gösterilebilir veya kimsenin erişememesini sağlanabilecektir. Bu sebeple mahremiyetin tam olarak sağlanamaması açısından değişik uygulamalarda değişik kararlar almak gereklidir.

4.5. Blok Zincirin Eksikleri

Blok zincirin sağlayacağı faydalar yadsınamaz, ancak, henüz olgunlaşma sürecini tamamlamamış bu sistemin bazı eksiklikleri bu başlıkta açıklanacaktır. Hâlihazırda kullanılmakta olan blok zincir uygulamalarının, sahip olduğu eksiklikler üzerine akademik çalışmalar devam etmektedir. Bu eksikliklerden bazılarına bu bölümde yer verilmektedir.

Blok zincirin dağıtık yapısı üzerine sıkça durulmaktadır. Ancak sistem dağıtık bir mimariye sahipken, işlemler aslında dağıtık olarak yapılmamakta, birçok farklı yerde birbirinin aynısı işlemler farklı düğümlerce yapılmaktadır. Yani, işlemlerin yapılması için iş bölümü yapılmamakta, her düğüm her işi birbirinin kopyası şekilde yapmaktadır. Örneğin bir donanım üzerinde işlemcinin parçalanması/dağıtılması, birden çok işin aynı anda, farklı işlemciler üzerinde iş bölümü yapılarak kaynakların tam kapasite kullanmasını amaçlar. Bu şekilde dağıtılmış işlemcilerle gerçekleştirilen dağıtık uygulamalar işlem süresini oldukça

kısaltarak donanım kaynaklarını tam kapasite kullanmayı mümkün kılar. Öte yandan blok zincir üzerindeki donanım kaynakları, aynı işi yapmak için yarış içine girerler, aynı problemi daha önce çözmeye çalışır, bunun neticesinde çok az bir farkla işlemi önce gerçekleştiren kişi ödüllendirilir diğer tüm kaynakların uğraşı ise israf edilmiş olur.

Yine kaynak kullanımı konusunda depolama ünitelerinin fazlaca kullanılması söz konusudur. Sürekli büyüyen blok zinciri ağı ile veri tabanları sürekli olarak ve ciddi boyutta büyümektedir. Blok zincirin çalışma istemi gereği sistemin katılımcısı her düğüm tüm sistemdeki veri tabanını tutmak durumundadır. Büyüyen sistemlerle birlikte fazlaca depolama kaynağı sorunu blok zincirin önemli problemlerinden biridir.

Blok zincirin bir güvenlik gereksinimi olarak ortaya çıkan doğrulama işlerinin gerçekleşmesi için belli bir süre işlemin beklemesi gerekmektedir. Bu bekleme işlemi günümüz teknolojilerine kıyasla oldukça fazladır. Örneğin, günümüz bankacılık sistemlerinde para transferleri anında gerçekleşebilirken blok zinciri uygulaması olan Bitcoin'de gönderilmeye çalışılan bir coin için ortalama en az bir saat bekleme gerçekleşmektedir. (Bitcon ağı saniyede en fazla 7 işlem gerçekleştirebileceği ve her bir işlemin 10 dakikada bir doğrulama sürecine alındığından hareketle bir saat ortalama bekleme süresi hesap edilmektedir)

Bitcoin ağının kullandığı ve oldukça güvenilir bir uzlaşı algoritması olan PoW oldukça fazla enerji tüketmektedir (100.000 kişilik bir şehrin tükettiği enerji miktarına eş değer).

Blok zincirin bir diğer güvenlik özelliği olarak, kötü niyetli bir kişinin zararlı bir işlem yapabilmesi için ağın %50' den fazlasını ele geçirmesi gerekmektedir. Bu işlem için oldukça fazla enerji harcaması gerekmektedir. Ancak, buna rağmen, ağın %51'inin ele geçirilmesi durumunda alternatif bir tarih yazılması mümkündür.

Blok zincir ağı üzerinde yapılan işlemlerde tam anonimlik bulunmamakta, yarı anonimlik bulunmaktadır. Bunun neticesi olarak ağ üzerinde yapılan bütün işlemleri bütün katılımcılar görebilecektir. Bu durum mahremiyet sorunlarını beraberinde getirmektedir.

Blok zincirin teknolojik boyutlarının yanında, regülasyonu, ilgili mevzuatının hazırlanması, hukuki boyutu gibi alanlarda eksiklikler bulunmakta, üzerine yapılacak çalışmaları beklemektedir.

Bütün bu bahsedilen sorunların üzerinde araştırmacılar oldukça çaba harcamaktadırlar. Literatür incelendiğinde, blok zincirinin bu eksiklikleri üzerine birçok farklı meslek grubundan insanların tez ve makalelerine rastlanmaktadır.

4.6. Uzlaşı Algoritmaları

Blok zincirin en basit haliyle çalışma mantığı buraya kadar tarif edilmiş olup ilk yıllarda kullanılmakta olan blok zinciri uygulamaları iş kanıtı denilen "proof of work" oldukça güvenlik sağlamıştı. Zaman içerisinde ihtiyaçlar doğrultusunda blok zinciri ağında da gelişmeler yaşanmış ve yaşanmaya devam etmektedir. Bu süreç içerisinde çeşitli konsensüs algoritmaları gelişmiştir.

Proof of Authority (PoA), ağdaki doğrulayıcıların anonim veya yarı anonim olarak değil, doğrulayıcı rolündeki belirli kişilerin kimliklerinin bilindiği ve bu kişilerin belirli koşullarla ağa katıldığı bir uzlaşı algoritmasıdır. Bir diğer uzlaşı algoritmalarına örnek olarak Delegated Proof of Stake (DPoS), Proof of Assignment (PoA) ve daha bir sürü çeşitli uzlaşı algoritması verilebilir. Bu algoritmalardan hangisinin kullanılması gerektiği, hangisinin çalıştırılmak istenilen uygulamada daha faydalı çalışacağına analizi sonucu karar verilir. Örneğin; dünyadaki herkese açık bir sistem olan bitcoin'in güvenliğini sağlamak için çok enerji harcayan PoW mantıklı olabilir.

Ancak tezimize konu kamu blok zinciri uygulamaları kapsamında enerji sarfiyatından tasarruf sağlanabilir ve güvenlik kaygısı kapalı ağ olduğundan dolayı göz ardı edilebilir. Çünkü ağ katılımcıları kamu kurumlarından oluşmakta ve katılımcılar birbirini zaten bürokratik anlamda tanımakta ve güvenmektedir. Kamu blok zinciri ağına katılmak isteyen kurumlardan ek güvenlik tedbirleri alması istenilebilir, bu vasıtayla istem dışı zafiyetlerden kaynaklı üçüncül kişilerin ağ üzerinde işlem yapması engellenebilir.

Hali hazırda; kamu kurumları arasında ihtiyaç duyulan veri iletişimi KamuNet ağı üzerinden sağlanmaktadır. Kapalı ağ olan bu ağ yapısı, dışarıya açık ağdan daha güvenli olduğu için kullanılmaktadır. KamuNet ağına dâhil olarak olmak isteyen kurumların bazı güvenlik gereksinimlerini yerine getirmeleri gerekmektedir. Örneğin, 21 Haziran 2017 tarih ve 30103 sayılı "Kamunet Ağına Bağlanma Ve Kamunet Ağının Denetimine İlişkin Usul Ve Esaslar Hakkındaki Tebliğ"in 4. maddesinin 1. fıkra (b) bendinde "Kurmuş olduğu BGYS için, TS ISO/IEC 27001 veya ISO/IEC 27001 standardına göre belgesini alır..." ifadesi

geçmektedir (Resmi Gazete, 2017). Bu hüküm gereği, KamuNet ağına bağlı kamu kurumları, bir siber güvenlik standardı belgesi olan TS ISO/IEC 27001 belgesine sahiptirler. TS ISO/IEC 27001 belgesi gibi bir belge blok zincir ağına yetkisiz erişimleri engellemek için ve paydaşalar arasındaki güven duygusunu pekiştirmek için şart koşulabilir.

4.6.1. Proof of Stake

Bir diğer uzlaşı algoritması olarak proof of stake (PoS), proof of work (PoW)'e göre daha hafif ve az enerji harcayan bir algoritmadır. Proof of Work algoritmasında madenciler sistemden direkt olaran coin kazanırken, Proof of Stake'de madencilerin yerini onaylayıcılar almaktadır. Onaylayıcılar ellerindeki coinlerin belli bir kısmını kasaya koyarak kriptografik puzzle'ı çözdüklerinde kasaya koyulan coin oranında daha fazlasını almak üzere işlem yapmaktadırlar. Ardından onaylama işlemi devam eder. Burada işlem aslında bir bahis mantığına dönüşmektedir. İşlem havuzundan zincire eklenebileceği düşünülen bir blok seçilerek bu bloğa bahis yatırılır, eğer bahis yatırılan bloğu zincire ekleyebilirse yani bloğu onaylayabilirse yatırılan bahis oranında coin kazanılmaktadır.

4.6.1.1. Casper

Casper, PoS mekanizmasını kullanan ve en yaygın bilinen blok zincirlerinden biri olan Etherium'un kullandığı uzlaşı algoritmasıdır. Etherium'un Proof of Stake uzlaşı algoritmasını kullanmasının sebebi Bitcoin'de kullanılmakta olan proof of work'ün çok fazla enerji harcıyor olması, bu sebeple sürdürülebilir olmamasıdır. Öyle ki, bir sene içerisinde bitcoin üretmek için harcanan toplam enerji Danimarka'nın bir yıllık toplam tükettiği enerji miktarına hale geldiğini gösteren araştırmalar bulunmaktadır (Jezard Adam, 2017). PoW ekolojik çevre açısından ve sistemin sürdürülebilirliği açısından güzel bir yöntem değildi. Ancak PoW'ün bu kadar enerji harcamasının sebebi de güvenliği artırmaktır. Dolayısıyla PoS ile ilerlendiği durumda PoW'ün sağladığı kadar güvenlik sağlanamayabilir. Bu durumda PoS algoritmasının mümkün olduğunca güvenli tasarlanması gerekmektedir. Çünkü PoW'te bir sisteme saldırıldığı zaman çalınmak istenen miktardan çok daha fazla miktarda enerji maliyetin altına girilmiş olmaktaydı. PoS'e saldırmak ise çok daha ucuz maliyet gerektirmektedir.

Bu problemi çözmek için, Bitcoin'in tasarlanmış şeklinden memnun olmayarak Bitcoin'den ayrılıp Etherium'u kuran Vitaly Buterin "Casper" isimli algoritma ile bir ödül-ceza mekanizması geliştirmiştir. Ağı manipüle etmeye çalışan kişilerden ether alacak şekilde tasarlanan bu algoritma ile insanların ağı yanıltmasının önüne geçilmek amaçlanmaktadır. Buterin bu algoritmayı, bloğunda, kendi cümleleriyle şöyle tarif etmiştir:

Casper'da ekonomik kesinlik, doğrulayıcıların katılım için depozito yatırmalarını zorunlu kılarak ve herhangi bir şekilde protokolün bazı kuralları ihlal eden hareket tespit edilmesi halinde depozitolarının yanmasıyla gerçekleştirilir (slashing conditions).

Kesinti koşulu (slashing conditions) şöyle görünebilir:

Doğrulayıcı, formun imzalı bir mesajını göndermesi durumunda

["PREPARE", epoch, HASH1, epoch_source1]

ve formun imzalı bir mesajı

["PREPARE", epoch, HASH2, epoch_source2]

HASH1 != HASH2 iken, veya epoch_source1 != epoch_source2, ancak epoch değeri her iki mesajda da aynıysa, bu durumda doğrulayıcının depozitosu kesilir (yani silinir)

(Buterin Vitalik, 2017, p. 5-11).

4.6.2. Byzantine Fault Tolerance (BFT)

Byzantine Fault Tolerance, izinli blok zinciri platformlarında çokça kullanılan ve en bilinen algoritmadır. Günümüzde izinli blok zincir uygulamalarında yaygınca kullanılan Hyperledger Fabric bu algoritmayı kullanmaktadır ve dağıtık sistemlerdeki Bizans generalleri problemi bu algoritmanın çıkış noktasıdır.

Bizans generalleri problemi, bir grup general ve askerin bir kaleye saldırması için hazırlık yapılması üzerine üretilmiş bir problemdir. Farklı yerlerde bulunan generallerin bu yere saldırabilmesi için bütün generallerin aynı anda saldırmaları gerekmektedir. Ancak aralarından en az bir generalin hain olduğu durum söz konusudur. Problem, bu generallerin birbiri ile nasıl haberleşip saldırı kararını alabilecekleri üzerinedir. Problemi çözmek için oluşturulan uzlaşı (consensus), bütün generallerin kararları toplanarak, generallerin

çoğunluğu, yani 2/3'ünden fazlası aynı karara varıyorsa, bu karar ile doğru sonuca ulaşılabileceği yönündedir.

BÖLÜM 5

5. BLOK ZİNCİRİ UYGULAMALARI

Dünya üzerinde blok zincir kullanan ciddi sayıda platform ve uygulamalar mevcuttur. Etherium, Hyperledger Fabric, Corda, Ripple, Quorum, IBM, Stellar bu uygulamalardan sadece en yaygın bilinenlerden bazılarıdır. Birçok hizmet kolunda farklı amaçlar doğrultusunda üretilen uygulamalar mevcuttur. Örneğin, özel ve kamu işletmeleri alanında, değerlerin (finansal ya da sanal bütün varlıkların olabilir) alışverişi alanında, tarım alanında blok zincir uygulamalarının başarılı örnekleri bulunabilir.

Blok zincirin en mantıklı kullanım alanlarından bir tanesi, örneğin tarım alanında, tedarik zinciri uygulamalarıdır. Wallmart gibi dünya tedarik zinciri liderlerinden olan firma hali hazırda tedarik süreçlerini yönetmek için blok zinciri teknolojisini kullanmaktadır (Mukherjee Srishti, 2022). Tedarik zinciri uygulamalarında blok zincirin bu denli öne çıkmasının sebebi, tarlada üretilen bir malın, tarladan çıkarak markete ulaşana kadar hangi aşamalardan geçtiğinin kayıt altında tutulması ve bu işlerin hiçbir otorite tarafından değiştirilememesi ve silinememesidir. Bu süreçlerin tüketici tarafından görünebilir olması ve gerçekleştirilen işlemlere şeffaflık getirmesi benzeri görülmemiş bir uygulamadır (case study, t.y.). Günümüzde oldukça yaygınlaşan nesnelerin interneti cihazlarını (IoT) blok zinciri uygulamalarıyla birleştirecek birçok uygulama alanı bulunmaktadır. Gıda tedarik süreçlerinde blok zincirin kullanılmasıyla, örneğin, kamyonun sıcaklık algılama sensörlerinden alınan verilerin blok zincire eklenmesiyle kamyona yüklenen bir gıdanın hangi ortam koşullarında taşındığını tüketici görebilir ve gıdanın bozulmuş olabilme ihtimalini daha ürünü satın almadan anlayabilir. Benzer şekilde ürünlerin tarlada hangi koşullarda üretildiği bilgileri, IoT cihazlardan alınan bilgilerle bloklara yazabilir ve tüketici ilgili gıdanın geçmişini bu şekilde gözlemleyebilme olanağına sahip olabilmektedir.

Bir diğer blok zincirin uygulama alanı olarak bireysel elektrik üretim süreci örnek gösterilebilir. Gerek yurt dışı gerek yurt içi örnekleriyle, insanlar kendi evlerinin çatılarında elektrik üreterek kendi evlerinde kullanabilmekte, fazlasını komşularına satabilmektelerdir. Blok zincirin bu elektrik dağıtım işlerinde kullanılması, gerek elektrik dağıtım gerekse ödeme süreçlerini hızlandırabilmektedir. Örneğin, elektriğin komşu eve verilmesiyle otomatik olarak paranın üretici kişiye gönderilmesi işlemi gerçekleşebilir. Bu iş büyük

ölçekteki elektrik sağlayıcısı şirketler bazında düşünüldüğü zaman kayıp/kaçak bedelleri ortadan kalkabilecektir. Tabi bu işlemler, otomatik olması blok zincir 1.0 olarak adlandırılan basit blok zinciri ağlarında değil, işin içine akıllı kontratların girmesiyle otomatize olabilen blok zincir ağlarıyla mümkündür. Blok zincirin enerji alanında bu şekilde çok fazla uygulaması vardır. Avrupada TenneT projesiyle, ilk merkeziyetsiz dağıtık sistem, güvenli ve akıllı enerji dağıtım sistemi olarak çeşitli bölgelere enerji dağıtımı sağlanmıştır (Insights Ledger, 2020).

Diploma gibi belgelerin onaylanması bir başka faydalı blok zinciri uygulamalarındandır. Blok zincirin dağıtık veri tabanı sayesinde merkezi sistemde oluşabilecek kaza veya doğal afetler sonucu verilerinin kaybolması kaygısı taşımadan kıymetli belgelerin bu sistemle onaylanması büyük fayda sağlamaktadır.

Özellikle biyografik kimlik denetimlerinde blok zinciri uygulamaları oldukça önemlidir. Örneğin açık anahtar kriptolamada, kimlik sertifikaları belirli organizasyonlar tarafından tutulmaktadır. Bir belge imzalanacağı zaman bu organizasyonlardan yardım alarak imzalama işlemi gerçekleşmektedir. Bu organizasyonların saldırıya uğraması durumunda, bu duruma "single contra failure" denilmektedir, kimlik doğrulama işlemleri yapılamayacak ve bütün iş ve işlemler duracak seviyeye gelecektir. Bu noktada dağıtık sistemler kullanılması avantaj sağlamaktadır. Açık anahtar kriptografiyi blok zinciri kullanarak dağıtıklaştırma çalışmaları ayrıca yapılmaktadır.

5.1. Blok Zinciri Teknolojisinin Uygun Kullanım Alanları

Birçok alanda çığır açabilecek bir teknoloji olan blok zincirini elbette her şeyin çözümü olarak görmek mümkün değildir. Bazı alanlarda blok zincir uygulamaları fayda sağlarken bazı alanlarda kullanılması faydasızdır. Öyle ki, blok zinciri kullanmadan geliştirilen çözümler bu durumlarda daha fazla fayda sağlamaktadır. Bu sebeple, blok zinciri bir çözüm olarak ele alıp buna uygun problemler üretmek emek israfıdır. Buna bağlı olarak, problemi analiz edip, çözümü üzerine düşünülmeli, blok zincirin bu problemde ne gibi fayda ve maliyetler getireceği iyi değerlendirilmelidir. Bu konu kapsamında, blok zincire en uygun gözüken bazı uygulama alanları bu bölümde açıklanmaktadır.

Tez kapsamında elde edilen sonuçlara göre, kamu hizmetleri açısından bakıldığında blok zincir teknolojisinin, kamu kurumlarının sistemlerine yüklenen verileri değiştirilemez ve

silinemez halde muhafaza edebildiği, kamu işlerini çok daha şeffaf hale getirdiğinden dolayı vatandaşların devlete olan güvenin artıracağı, blok zinciri sistemi ile siber güvenliğin yüksek oranda artacağı sonucuna varılmıştır. Ayrıca, blok zinciri teknolojisiyle sosyal yardımların dağıtılmasında, tapu sicil işlemlerinde, kimlik doğrulaması gerektiren işlerde dijital kimlik kullanımı yoluyla günümüzde kullanılan mevcut sistemlere kıyasla güvenlik seviyesinin yükseltilebileceği sonucuna varılmıştır. Özellikle Birleşik Krallığın blok zinciri çalışmalarına bakıldığında kamu yönetimi alanına dijital dönüşüm, yönetişim veya reform bağlamında ileri çalışmalara vesile olacağı öngörülmektedir. Dijital dönüşümünü en yüksek oranda gerçekleştiren ülkelerin başında gelen Estonya örneğinden görüleceği üzere blok zinciri sadece dar alanda değil toplumun birçok noktasına yayılan gündelik alanlarda da gelişim göstermiştir. Ayrıca Estonya'nın geliştirmiş olduğu blok zinciri teknolojisini Finlandiya'nın da kullanıyor olması blok zinciri teknolojisinin küresel çapta yayılma gerçekleştirebileceğini göstermektedir. Blok zincir ağının yaygınlaşarak teknoloji dönüşümünü beraberinde getirmesi durumunda, kendini güncelleyemeyen kamu kurumlarının, teknoloji transferini sağlayan tedarikçilere bağımlı kalma riski mevcuttur. Devletler ve vatandaşların kritik verilerini depolayan kamu kurumları veri bütünlüğü ve gizliliğinin korunması konusunda gerekli tedbirleri almalıdır. Bu tedbirler arasında en güvenli altyapıyı blok zinciri ağının sunduğu aşikârdır.

Ekonomik Kalkınma ve İşbirliği Örgütü (OECD)'nün analizine göre, dünya üzerinde blok zincirinin en yaygın kullanıldığı ilk on proje tipi ve bu teknolojiyi en çok kullanan ilk on sektör sırasıyla Tablo 2'de gösterilmektedir. Tablonun en dikkat çekici yeri, blok zincirinin en yaygın kullanıldığı sektörün devlet hizmetleri olduğudur. Bir başka ifadeyle, Dünyada kamu otoriteleri blok zincire en çok yatırım yapan kuruluşlardır. Özellikle gelişmiş ülkeler, blok zincir teknolojisinin gelişimi üzerine ciddi yatırım yapmaktadırlar. Bu sebeple, ülkemizin, bu teknoloji gelişimi ve dönüşümünde geride kalmaması için bu tezde blok zincirinin dijital verilerin güvenliğine olan katkısı üzerinde durularak, dünyadaki blok zinciri uygulamaları anlatılmış ve ülkemize yönelik olası kullanım alanları işaret edilmiştir.

Tablo 2

(Berryhill, Bourgery & Hanson, 2018)

	Proje Tipi	Sektörler
1	Strateji/Araştırma	Devlet Hizmetleri
2	Kimlik (Yetki Belgeleri/Lisanslar/Onaylar)	Mali Hizmetler
3	Kişisel Kayıtlar (Sağlık, Finans vb.)	Teknoloji ve Nesnelerin İnterneti
4	Ekonomik Kalkınma	Sağlık Sektörü
5	Finansal Hizmetler/Piyasa Altyapısı	Emlak Sektörü
6	Tapu Sicili	Tedarik Zinciri
7	Dijital Para (Merkez Bankası İhracı)	Enerji Sektörü
8	Avantajlar/Yetkiler	Ulaşım
9	Uyumluluk/Raporlama	Eğitim
10	Araştırma/Standartlar	Telekom

Devletin tuttuğu tapu kayıt sistemleri, diplomalar, lisanslar gibi değerli kâğıtlar üzerindeki işlemler blok zinciri ile güvenli, değiştirilemez ve yok edilemez şekilde saklanabilmektedir.

Biyografik kimlik denetimlerinde özellikle adından söz ettiren blok zinciri, blok zincir destekli pasaportlar gibi uluslararası seyahat güvenliğini sağlama uygulamalarında kullanımı önemli fayda sağlayacaktır.

Birleşik Krallık, Singapur, Birleşik Arap Emirlikleri gibi ülkeler blok zinciri maliyetleri düşürmenin bir yolu, yeni bir finansal araç ve temiz kayıt tutmanın bir yolu olarak görmekte ve bu yönde çalışmalarına yön vermektedir.

Sınır dışı para göndermenin en maliyetsiz yolu yine kripto paralar üzerinden sağlanabilmektedir. Ülkeden ülkeye değişen para transfer ücretleri, limitleri gibi kısıtlamalara takılmadan kripto paraya dönüştürülen değerler, blok zinciri ağı üzerinden çok düşük maliyetlerle gönderilebilmektedir, hatta bazı blok zinciri uygulamaları maliyet dahi çıkarmamaktadır.

Blok zincirin şeffaflığı sayesinde, mortgage destekli menkul alım satımı işleri ile emlakçılık sektöründe kolaylıklar sağlayacaktır.

IoT destekli akıllı şehirler, akıllı evler, giyilebilir teknolojik cihazlar ve daha birçok alanda IoT cihazlarının çokça kullanılması, güvenliği tam olarak sağlanamamış, ucuz olması sebebiyle tercih edilen IoT cihazlarının kullanımını da beraberinde getirmektedir. Robot süpürgeler, bebek monitörleri, kamera sistemleri gibi cihazların bir bileşeni olarak çalışan IoT cihazlar aslında güvenlik, gizlilik ve mahremiyet açısından çok büyük risk teşkil etmektedir. Birçok kişinin siber güvenlik konusundaki farkındalıklarının çok düşük olduğu düşünüldüğünde, birçok IoT cihaz kötü niyetli kişilerin saldırılarına açık durumdadır. Blok zincirinin IoT cihazlarında kullanılmasıyla, cihazlardan alınan verilerin güvenli bir şekilde tutulması ve işlenmesi sayesinde, IoT sistemlerinin güvenliğine katkı sağlamaktadır.

Dijital hakların yönetimi konusu günümüz teknolojilerinde bir problem iken blok zinciri bu konulara getirilebilecek uygun çözümlerden biridir. Dijital müzik, resim gibi varlıkların kopyalanma yoluyla dağıtılması ve bu varlıkların esas üreticisinin bundan kâr sağlayamaması günümüz internetinin sorunlarındandır. Blok zinciri ağıyla, bu varlıkların blok zinciri üzerinde sergilenmesi ve dağıtılması hakkaniyetli bir durum oluşturacaktır. Blok zincir tarihi boyunca yapılmış her işlem ağ üzerinde tutulmakta olduğu için dijital bir varlığın ilk sahibinin kim olduğu, daha sonra kimler üzerinde el değiştirdiği rahatlıkla ve şüpheye yer vermeyecek şekilde bulunabilmektedir. Ayrıca blok zincirin bu özelliği vasıtasıyla, niteliği suç olan unsurların dağılmasının önüne geçilebilmekte veya sorumluların kimler olduğunun tespiti kolayca yapılabilmektedir.

Paydaşları çok olan, iş birliği ile yapılan yazılım geliştirme projelerinde blok zincirin katkısı önemli olacaktır.

Merkeziyetsiz finans uygulamaları, Non Fungible Token (NFT), Web 3.0, Metaverse blok zincirin diğer uygulama alanlarıdır.

Bütün bu sayılan alanlarda ve daha fazlasında kullanılma potansiyeli olan ve bu alanlara sağlayacağı muhtemel katkısıyla, blok zincir, dünyayı değiştirme potansiyeli olan bir teknoloji olarak görülmektedir.

5.2. Blok Zincirin IOT Cihazlar Üzerinde Kullanımı

IoT cihazlar, başka sistem ve cihazlarla haberleşmek için internet kullanan, üzerinde bulundurduğu sensör, yazılım ve diğer teknolojik donanımlar ile etrafından veri toplayan veya topladığı verileri ilgili işini yapmak amacıyla anlamlandıran cihazlardır. Bu cihazlar gündelik ev aletlerinden endüstriyel araçlara kadar çok fazla çeşitte değişiklik göstermektedir. Dijitalleşmenin artmasıyla son 10 yıllık dönemde oldukça adından söz ettiren IoT cihazlar, farkında olmadığımız yerlerde dahi hayatımıza girmiştir. Akıllı evlerde kullanılan sensörler, buzdolabındaki kameralar, bebek monitörleri, robot süpürgeler, yeni nesil arabalar ve dahi birçok teknolojik aletler IoT özellikleri ile donatılmıştır.

Nesnelerin interneti (IoT) alanındaki bu gelişmeler, zamanla IoT cihazların güvenliğine yeni sorunlar getirmiştir. Bu cihazların güvenliği ve uygulanabilir çözümleri üzerine birçok araştırma yapılmış, ancak ne yazık ki, IoT cihazlarına yapılan saldırıların artması, bu sistemlerin güvenliğini sağlamayı zorlaştırmıştır ve bu alandaki araştırmaların artmasına halen oldukça ihtiyaç vardır (Emina Džaferović, Ajla Sokol, Ali Abd Almisreb, Syamimi Mohd Norzeli, 2019). Buna karşılık, ne yazık ki, bazı IoT cihaz üreticileri maliyeti düşürmek için güvenlik çözümleri geliştirmemektedir. IoT cihazlara ait bazı güvenlik sorunları şu şekilde sıralanabilir:

Gizlilik: Kullanmakta olduğumuz IoT cihazlar ihtiyaç odaklı üretilmiş ve güvenlik gereksinimleri göz ardı edilmiş veya üretildiği dönemin güvenlik gereksinimlerini karşılar halde üretilerek günümüzün güvenlik ihtiyaçlarına cevap veremez halde gelmişlerdir. Güvenliği yeterince sağlayamayan bu cihazlar, örneğin bebek monitörlerinin ele geçirilmesiyle kötü niyetli kişilerin çocuklarla iletişim kurduğuna şahit olunmaktadır (TRT Haber, 2019).

Cihaz kimlik doğrulaması: IoT cihazının veri gönderir veya alırken orijinal bir cihaz olduğundan emin olunması gereklidir. Aksi takdirde, taklit edilen veya ele geçirilen cihazların veri paylaşması veya işlem yapması sonucu ciddi zararlar doğabilmektedir.

Geniş saldırı yüzeyi: IoT cihaz sayısının çok hızlı bir şekilde artması ve gerek üreticilerin gerekse kullanıcıların güvenlik bilinç düzeylerinin yetersiz olması sebebiyle bu cihazlar kötü niyetli kişiler tarafından hedef alınmakta ve kolaylıkla ele geçirilmektedir. İnternete bağlı gerçek kişilere ait bilgisayar sayısı, IoT cihazlarının sayısının yanında oldukça düşük kalmaktadır. Bu sebeple ele geçirilen IoT cihazları ile yoğunluğu yüksek

DoS/DDoS saldırıları yapılabilmekte veya IoT cihazlarından daha fazla veri ele geçirilebilmektedir.

Veri bütünlüğü: Bir verinin erişildiği her tarihte doğruluğunun ve tutarlılığının korunmasıdır. Ancak IoT cihazların kablosuz ağ aracılığıyla veri aktarımı esnasında, ağda zayıflama, bozulma veya gürültü eklenmesi gibi çeşitli sebeplerle verilerinde bozulmalar meydana gelmektedir.

Dağıtılmış hizmet reddi (Distributed Denial of Service - DDoS) saldırıları: IoT cihazların ilk üretildiği yıllar yaklaşık 40 yıl öncesine tekabül etmektedir. Üretildiği yıllarda siber güvenliğin ve siber saldırıların günümüzdeki kadar fazla olmadığı düşünüldüğünde güvenlik zafiyetleri oldukça fazladır. Uzun yıllar önce üretilip günümüze kadar gelerek kullanımı devam eden bu cihazlar, aslında önemli ölçüde kendi sistemlerinin yanı sıra diğer sistemlere de zarar vermektedir. Varsayılan şifreler (default password), hali hazırda her sistem için üçüncü kişiler tarafından tahmin edilebileceği için zarar teşkil ederken, IoT cihazlarının büyük çoğunluğunda bu şifreler kullanılmaktadır, bazı cihazlara erişim esnasında şifre dahi sorulmamaktadır. Uzun yıllar önce üretilen bu tip cihazların güncelleme desteği de olmadığı için günümüz güvenlik gereksinimlerinin çok gerisinde kalmıştır. Cihazlar bu şekilde ele geçirilmesi kolay olunca kötü niyetli kişiler bu cihazları zombi bilgisayar (botnet) ağına dâhil edip bu cihazlar üzerinden DDoS saldırıları gerçekleştirmektedir.

Cihaz kapasitesi kısıtlamaları: IoT cihazlar genellikle bir bilgisayar gibi güçlü donanım özelliklerine sahip değildir. Hafızaları, ön bellekleri gibi donanımları çok küçük boyutta olduklarından üzerinde tuttukları veriler de bu nispette küçük olmaktadır.

Blok zincirin IoT cihazlar üzerindeki en önemli kullanım amacı, IoT cihazlardan alınan verilerin geri döndürülemez şekilde ağa yazılması ve geri dönüp yapılan işlemlerin incelenmesine imkân vermesidir. Savunma sistemleri alanında, askeri çalışmalar esnasında birbirine güvenmeyen gruplar arasındaki işbirliği için kullanılması, yapılan bir işlemi öncelikle bütün guruplar onaylayacağı için, IoT cihazlardan alınan verilerin silinemez ve değiştirilemez şekilde ağa yazılması blok zincirin uygun kullanım alanlarından bir tanesidir.

Sensörlerden gelen verilerin inkâr edilemez şekilde ağa yazılmasıyla, daha sonradan yapılacak araştırmalarda sorumlu personelin bulunması konusundaki problemleri gidermektedir. Örneğin otonom araçlarda sensörlerden gelen verilerin blok zincir ağına yazılmasıyla, bir kaza durumunda kazaya sebebiyet veren etkenlerin ve ya sorumluların

bulunması imkânını artırmaktadır. Farklı noktalarda bulunan araçlardan bulundukları konumdaki trafik verilerini alması ve blok zincir ağına paylaşım yapmasıyla, trafik problemlerinin öngörülmesi veya giderilmesi mümkün kılınmaktadır.

5.3. Dünya Üzerinde Blok Zinciri Uygulamaları

Dünya üzerindeki çeşitli ülkeler, blok zincirinin kripto paralar dışındaki kullanım alanlarına ait projelerine sürat kazandırmış durumda, hem araştırma geliştirme faaliyetlerine devam etmekte hem hukuki alt yapısı üzerine çalışmalar yapmaktadırlar. Bu bölümde çeşitli ülkelerdeki blok zincir uygulaması örneklerine yer verilmektedir.

5.3.1. D5 Ülkeleri

Dijital 5 (D5) olarak Türkçeye çevrilen Digital Nations 5; Birleşik Krallık, Estonya, Güney Kore, Yeni Zelanda, İsrail arasında kurulan bir iş birliği ağıdır. D5 ağının amacı kamudaki dijitalleşme süreçlerinde oluşan sorunlara ortak çözümler üretmektir. D5 ülkelerine daha sonraki yıllarda Kanada, Uruguay, Meksika ve Portekiz eklenerek D9 adını almıştır.

Birleşik Krallık (UK), Bilim ofisi aracılığıyla yayımladığı rapora göre, dağıtık defter teknolojisinin (DLT) kamu sektöründeki dönüşüm potansiyeli gösterilmektedir (Hancock, M., & Vaizey, E., 2015). Blok zincirin teknoloji, yönetişim, gizlilik, güvenlik gibi özelliklerine vurgu yapılmakta, ayrıca büyümekte olan kamu hizmetlerindeki zorlukların aşılmasında blok zincir teknolojisinin faydalarına yer vermektedir. Birleşik krallık, kamu sektöründe blok zinciri aktif olarak kullanmasa da şimdilik gerekli alt yapılarını hazırlamaktadırlar. İngiltere Bankası günümüzde kullandıkları ödeme sistemlerini gelecekte oluşacak taleplere karşılık verebilmesi için değiştirmeye çalışmaktadır. Özellikle, gelecekte oluşabilecek finans sistemlerine ve özel sektördeki yeniliklere uyum sağlama, tehditlere karşı dayanıklı olma ve para politikalarının gelişimine destek olma gibi hedefleri doğrultusunda blok zincir teknolojisinin bu alanlardan bazılarına çözüm olabileceği ve güvenliği artıracağından bahsedilmiştir (Ojo & Adebayo, 2017). Aynı zamanda Birleşik Krallık Hükümeti, blok zincir tabanlı teknoloji ile çalışan bir sosyal yardım ödemesini test etmiştir. İhtiyaç sahipleri bu uygulamayı telefonlarına yükleyerek sosyal yardım alabilmekte

ve harcamalarını yine bu uygulama üzerinden yapmaktadırlar. Bu test ile Hükümet blok zincir teknolojisinin halk tarafından kullanılabilme durumunu gözlemlemiş ve yapılan yardım ödemelerinin daha güvenli teknolojilerle sağlanıp sağlanamayacağını gözlemlemişlerdir. Birleşik Krallık'taki bir başka uygulama Kraliçenin ev satışı sırasında kullanılarak deneme çalışması yapılan tapu sicil işlemidir. Bütün bu projelerdeki ortak amaç hükümetin yolsuzluk ve sahtekârlığı önleyerek bürokratik işlemlere hız kazandırmakta ve devlet ile vatandaş arasındaki ilişkiler şeffaf hale gelerek devlete olan güveni artırmaktadır.

Dijitalleşmede en önde gelen ülkelerden biri olan Estonya blok zincir yapısını kamu sektöründe ilk kullanan ülke olmuştur. Estonya'daki kamu kurumları, veri bütünlüğü ve sistem birliği için blok zinciri teknolojisini kullanmaktadır (Priit Martinson, 2018). Estonya Hükümeti blok zinciri teknolojisini, veri tabanlarına yönelik yapılabilecek olası ihlalleri en aza indirerek devlete ait verilere %100 güven sağlamak için kullanmaktadır. Bu sebeple Estonya'daki kamu kurumları kendi geliştirmiş oldukları blok zinciri ağını kullanarak verilerin merkezi tek bir yerde değil, gerçek zamanlı olarak birçok farklı kurum tarafından doğrulamasını gerçekleştirmektedir. Sağlık verilerini yine DLT uygulamalarında tutan Estonya Hükümeti, bu sayede vatandaşlar üzerindeki idari yükün azaldığını belirtmiştir. Kamu sektöründeki dijitalleşmesini neredeyse tamamlamış Estonya, e-Vergi, e-Ticaret, e-Polis, e-Hukuk, e-Adalet gibi hizmetler geliştirmiştir. Özellikle hukuk hizmetlerinin blok zinciri üzerinden gerçekleştirilmesi mahkemedeki dava sürelerini kısaltmıştır. E-Polis uygulamasını Finlandiya ile beraber kullanarak her iki ülke tarafındaki suçluların takibine imkân sağlanmıştır. Ayrıca, hükümet tarafından imzalanmış olan elektronik kimliklerle vatandaşlar doğum belgelerini, evlilik düzenlemelerini, vasiyetnamelerini, iş sözleşmelerini ve tapu kayıtları gibi belgelerini merkezi bir kuruma gitmeden dünyanın her yerinden noter onayına sunarak kullanabilmektedirler (Mattila, 2016).

Güney Kore Hükümeti blok zinciri üzerine çalışacak küçük ve orta büyüklükteki işletmelere (KOBİ) sermaye sağlayarak blok zincirin finansal alanlardaki kullanımını desteklemiştir. Güney Kore'nin kalabalık bir eyaleti olan Gyeonggi Hükümeti bir yardım kampanyası oylamasını blok zinciri ağı üzerinden yapmıştır. Akıllı sözleşmeler kullanılarak yapılan bu oylama sisteminde 9 binden fazla kişi oy kullanmıştır (Garrett Keirns, 2017). Güney Kore Hükümeti özellikle bankacılık ve sağlık alanlarında blok zinciri uygulamalarını aktif olarak kullanmaktadır. Sağlık alanında hasta ile sigorta şirketi arasında kurulmuş olan DLT vasıtasıyla iki tarafta sağlık verilerinde ortak yetkiye sahiptir. Bankacılık alanında dijital kimlik uygulaması geliştirilerek, banka kullanıcıları kimlik kartı taşımak yerine mobil

telefonlarındaki bir uygulama ile kimlik tanıtım işlemleri gerçekleştirebilmektedir. Güney Kore başta bankacılık, sigortacılık olmak üzere sanat eserlerinin korunması ve akıllı şehirler gibi projeleri desteklemektedir. Ayrıca ülkede, gümrükleme, hayvancılık sektöründe tedarik zinciri uygulamaları, e-oylama, e-belge yönetimi, gayrimenkul ticareti ve deniz lojistiği gibi alanlarda pilot blok zinciri uygulamaları geliştirilmiştir (T.C. Sanayi ve Teknoloji Bakanlığı, 2019).

Yeni Zelanda Hükümeti, kamu sektöründeki ve özel sektördeki blok zinciri projelerini desteklemek için "İnovasyon Fonu" adında teşvik paketi kurmuştur. Fon kapsamında dijital kimlik ve ödeme sistemlerindeki işlerin optimizasyonuna maddi destek sağlamaktadır. Ayrıca, Yeni Zelanda nesli tükenmekte olan hayvanları korumak için blok zinciri teknolojisi kullanmaktadır. Bunu, tedarik zinciri uygulamasıyla, orkinos balıklarının tekneden başlayarak süper markete gelene kadarki süreçlerini takip ederek yapmaktadır. Bu sayede yasadışı avlamanın önüne geçilmektedir. Yeni Zelanda hükümetinin desteğiyle dağıtık sistemlerin incelenmesi ve uygulanması için Yeni Zelanda Blok Zinciri Birliği (BlockchainNZ) kurulmuştur. Derneğin ilk işi, "Dasset" isimli ulusal para birimi ile satın alınabilen kripto para üretmek olmuştur. Bu sayede Yeni Zelanda dolarının ulusal piyasalarda daha iyi bir konuma gelmesi hedeflenmiş, ayrıca, üretilen kripto paranın hukuki dayanağını oluşturacak yasalar çıkarmıştır (Blockchainnz, 2019). Para Aklama ve Terörle Mücadele 2013 (AML / CFT Yasası), 2013 Finansal Piyasalar Davranışı (MYK Yasası) ve Finansal Hizmet Sağlayıcılar (Kayıt ve Anlaşmazlık Çözümü) yasaları kripto para üretimine göre düzenlenen bazı yasalardır (Anand ve ark., 2011). Çoğunlukla finansal piyasalar ve tarım alanında blok zinciri teknolojisini geliştiren Yeni Zelanda, kripto para üretimi konusunda özel şirketleri desteklemektedir. Ayrıca, tarım alanında üretilen gıdaların güvenirliğini artırmak, ürünlerin tazeliği, kalitesi, nerede üretildiği gibi bilgilere ulaşmak için blok zincirini kullanmaktadır.

İsrail'de bulunan IBM Araştırma Merkezi, blok zincir geliştirme alanında hayli ilerlemiş ve küresel pazara hâkim bir konum elde etmiştir. Birçok uluslararası firma IBM'in geliştirdiği blok zincir çözümlerini kullanmaktadır (IBM, 2020). İsrail'de bulunan girişimler, siber güvenlik, tedarik zinciri, dijital kimlik, oylama, sağlık, çevre, uluslararası ticaret gibi birçok alanda blok zinciri test uygulamalarını hayata geçirmektedir. İsrail hükümeti özellikle start-up'lar ve askeri amaçlı geliştirilen blok zinciri projelerine kaynak ayırmaktadır. İsrail Hükümeti, Avustralya'daki Commonwealth Bank ile blok zinciri teknolojisinin para transferinde kullanılması üzerine ortak çalışma yapmaktadır. Online

ticaret işlerinin güvenliğini sağlamak, üretilen şarkıların ve müziklerin dijital hakkını korumak, kredi kartlarından Bitcoin satın almak gibi uygulamalar geliştirilen İsrail'deki ATM'lerden Bitcoin çekilebilmektedir (Karch, 2014). Ancak bütün bu üretilen projelerin tüketiciler, hükümet ve şirketler tarafından çok da kullanılmadığı söylenmektedir. İsrail Hükümeti blok zinciri teknolojisini desteklese de birçok iş hayatı eleştirmenleri olumsuz yönde kanaatlerini dile getirmektedir (Katsiri, 2019). Diğer 4 ülkeyle kıyaslandığında İsrail'in çalışmaları daha az olmasına rağmen, yine de İsrail'in D5 üyesi olması dikkat çekicidir (Özaltın ve Ersoy, 2020).

5.3.2. Diğer Ülkelerde Blok Zinciri Uygulamaları

Dünya üzerinde birçok ülkede binlerce blok zinciri uygulamaları geliştirilmekte ve aktif olarak kullanılmaktadır. Burada verilen blok zinciri örnekleri sadece bir fikir vermesi açısından anlatılmakta ve verilen örneklerden çok daha fazlası internet ortamından elde edilebilmektedir.

Singapur'daki "Smart Nation Project" adlı blok zinciri uygulaması kapsamında akıllı şehirlerdeki bilgilerin güvenli bir şekilde paylaşılması, trafik sıkışıklığının azaltılması ve planlı ulaşımı sağlamak amaçlanmıştır. Ayrıca, aynı proje düşük enerjili konut sağlama amacıyla geliştirilen Hindistan'daki uydu şehirlerde ve akıllı şebekelerde kullanılmıştır.

Birleşik Arap Emirlikleri'nde internet üzerindeki her bilgiyi blok zinciri üzerinde tutmak üzere çalışmalarına yön vermektedir. Dubai Hükümeti, kamu kurumlarını blok zinciri teknolojisine teşvik etmek için özel kamu blok zinciri iş birliği ağı olan Küresel Blok Zinciri Konseyi'ni (Global Blockchain Conuncil) kurmuştur. Ülkede, Emirates Entegre Telekominikasyon Şirketi, hizmet sağlayıcılarından oluşan blok zinciri ağında sağlık kayıtlarını tutan pilot uygulama geliştirmiştir.

Amerika Birleşik Devletleri ve Birleşik Krallık, sınırlarını güvenli hale getirmek için blok zinciri uygulamaları geliştirmektedir. Brexit sınır kapıları sorununu blok zinciri ile çözme konusunda tartışmalar mevcuttur (Chalmers John, 2019).

Çin, büyük veri (big data) problemleri üzerine blok zinciri üzerinde çalışmalar yapmaktadır. Blok zincirin büyük veri konusunda çözmesi beklenen sorunlar, büyük verilerin güvenliğinden emin olma, taraflar arasındaki veri transferindeki güven sorununu

çözme, bir değerin sahipliği, kökeni ve güvenilirliği gibi konulardan emin olmak gibi sorunlardır.

Blok zinciri teknolojinin en uygun kullanım alanlarından biri olan e-oylama sistemi, 2014 yılında Danimarka'da Danish Liberal Alliance partisi tarafından parti içi bir oylama yapmak için kullanılmış, daha sonra bu oylama teknolojisi Amerika'da liberal partilerin oy sayımında da kullanılmıştır. E-oylama sistemlerinde kullanılan blok zinciri teknolojisi, oluşturduğu şeffaflık güven sayesinde demokrasinin gelişimi için önemli bir unsur olduğu düşünülmektedir.

İspanya'da Madrid Carlos III Üniversitesi blok zinciri sistemine kayıtlı, sertifikalandırılmış ilk diplomaları öğrencilerine dağıtmıştır. Bu sayede mezun olan öğrenciler iş başvurularında diplomalarını şirketler ile paylaşabilmekte ve bu diplomaları güvenli bir şekilde telefon uygulamalarından yönetebilme imkânına sahip olmuşlardır (Universitad Carlos III de Madrid, 2018).

Gürcistan tapu tescil işlerindeki prosedürlerin basitleştirilmesi, düzenlenmesi ve modernizasyonu konusunda çeşitli avantajlar sağlayan blok zinciri teknolojisini mülk kayıtlarının tutulması işlerinde kullanmaktadırlar (Collosa, 2021).

5.4. Türkiye Örnekleri

5.4.1. TOGG

7 Ocak 2022 tarihinde, TOGG marka yerli otomobil firması, Avalange algoritmasını kullanan Ava Labs ile stratejik iş birliğini, resmi internet sitesinde yayımlayarak duyurmuştur (Togg, 2022). 2022 yılında yapılan Avalange Zirvesinde konuşan Togg CEO'su Gürcan Karakaş blok zinciri teknolojisinin Togg otomobilinde nasıl kullanılacağını şu ifadelere anlatmıştır:

> …dekarbonizasyon, akıllı yaşam, e-cüzdan, akıllı lokasyon, uzaktan güncelleme, akıllı bağlantı hizmetleri sayesinde kullanıcılara kesintisiz bir mobilite deneyimi sunacağız. Blok zinciri; hızlı, güvenli ve çevre dostu mobilite hizmetleri ve akıllı cihaz güvenliğinde kullanılacak bir teknoloji olarak öne çıkıyor. Dijitalize edilmiş veri ve diğer varlıklar blok

> zinciri aracılığıyla güvenli biçimde saklanıp transfer edilebilecek. Bu nedenle blok zinciri ve yapay zeka, ekosistemlerin merkezinde yer alacak….Yasal düzenlemeler çerçevesinde blok zinciri, techfin ve fintech gibi yeni nesil teknolojilerle kullanıcılarımıza güvenli, hızlı ve çevre dostu hizmetler sunmanın yöntemlerini geliştiriyoruz… (Aslanhan, 2022, p. 6)

Bunun yanında bir diğer önemli özellik olarak Togg, büyük bir tüketici elektroniği fuarı olan Consumer Electronics Show'da (CES) blok zinciri ağı üzerinde çalışan tedarik zinciri uygulamasını tanıttı. Bu uygulama, kullanıcıların araçlarının servis geçmişine, ulaşım geçmişine ve değişen parçalarının neler olduğu gibi bilgilere erişimi kolay ve şeffaf bir hale getirecektir (Garip, 2023). Bu sayede kullanıcılar araçlarının bakım ve onarım süreçlerinden daha fazla haberdar olacaklardır.

5.4.2. e-Devlet: Dijital Kimlik

Blok zinciri uygulamaları alanında bir diğer önemli atılım ise e-devlet projesinde gerçekleşmiştir. Kamudaki dijital dönüşümü büyük oranda sağlamakta olan e-devlet kapısı projesi, blok zinciri transferini de gerçekleştirmek üzere incelemeler yapmaktadır. Blok zinciri teknolojisi ile geliştirilen dijital kimlik uygulaması ilk kez Cumhurbaşkanı Yardımcısı Fuat Oktay Tarafından Dijital Türkiye 2023 birinci toplantısında şu sözlerle tanıtmıştır:

> e-Devlet'te yeni bir devrim olacak blokzincir tabanlı bir giriş sistemini, "dijital kimliği" getiriyoruz. e-cüzdan uygulaması kapsamında çalışacak giriş sistemi ile vatandaşlarımız, blokzincir ağında oluşturulmuş dijital kimliklerle e-Devlet'e girebilecek. On-line e-Devlet'ten off-line e-Devlet'e geçişin yani kullanıcılar açısından dijital bilgilerinin cep telefonlarında güvenli bir şekilde tutulabildiği bir sisteme doğru evrilerek ilk adımlarını bugün attığımız bu çalışmamız, gelişerek yeni kolaylıkların kapısını aralayacak (Kutbe, 2023).

5.4.3. TÜBİTAK: 'Blokzincir Araştırma Laboratuvarı

Blok zincirinin Türkiye'deki ar-ge faaliyetlerini yürütmek amacıyla TÜBİTAK Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi'nde Blokzincir Araştırma Laboratuvarı (BCLabs) kurulmuştur. Kamu ve özel sektörün ihtiyaçlarına istinaden blok zinciri altyapısının kurulması, blok zincirinin mahremiyet ve güvenlik analizinin yapılması, iş modelinin geliştirilmesi, kitle fonlama yaklaşımları vs. çeşitli teknik detayları gerçekleştirmek üzerine faaliyetini sürdüren Blokzincir Araştırma Laboratuvarı, blok zincirinin anlaşılmasını, blok zinciri becerilerinin geliştirilmesini amaçlamaktadır.

Bu kapsamda Bilgem, kamu kurumları, özel sektörler ve akademisyenlerle iş birliği yapmakta, daha şeffaf ve verimli bir ağ yapısının kurulması için finans, tedarik zincirleri, IoT, sağlık, risk yönetimi gibi birçok alanda blok zinciri tabanlı çözümler geliştirmektedir.

5.4.4. Blockchain Türkiye Platformu (BCTP)

Türkiye Bilişim Vakfı (TBV) tarafından kurulmuş olan Blockchain Türkiye Platformu, merkeziyetsiz sistem kurmayı ve Türkiye'yi bu konuda bölgesinde lider yapmayı vizyon edinmiş, kâr amacı gütmeyen bir kuruluştur. Blok zincirinin Türkiye'de kullanımının artması, faydalarının araştırılması gibi amaçlarla eğitimler vermekte, etkinlikler düzenlemekte, yayınlar yapmakta ve kamu kurumları, üniversiteler ve diğer ülkelerin kuruluşlarıyla iş birlikleri yapmak gibi işlerle blok zinciri üzerine etkin çalışmalar yapmaktadır.

5.4.5. Sanayi ve Teknoloji Bakanlığı: Sanayi ve Teknoloji Stratejisi (2023)

2019 yılında Sanayi ve Teknoloji Bakanlığı'nın yayımladığı Sanayi ve Teknoloji Stratejisi (2023) raporunun "Alt Yapı-Ulusal Blokzincir Altyapısı" başlığı altında ifade edildiği üzere, ulusal bir blok zinciri ağı alt yapısının oluşturulması hedeflenmiştir. İlgili raporda blok zinciri ile ilgili şu ifadeler yer almıştır:

-Kamu, özel sektör ve bireylere ait verilerin etik kurallar dikkate alınarak, anonim hale getirilmesi ve mümkün olan en geniş seviyede açık olarak paylaşılması konularında merkezi, tekil ve güvenilir veri altyapısının oluşturulması için çalışmalar başlatılmıştır.

-Cumhurbaşkanlığı Dijital Dönüşüm Ofisi ile birlikte kamunun topladığı verilerden "Kamu Veri Havuzu" oluşturulacak ve kamuoyunun kullanımına açılacaktır.

-Blokzincir teknolojisi üzerinde uygulama geliştirme yetkinliğinin oluşması için öncelikle kamu merkezli uygulamalardan (örneğin, tapu kayıt, diploma, gümrük uygulamaları vb.) blokzincir altyapısına taşınabilir olanların tespit edilerek "Açık Kaynak Platformu" inisiyatifi bünyesinde projelendirilmesi sağlanacaktır.

- Yeni, güvenli iş modeli ve süreçlerin (tedarik zinciri, bankacılık, hukuki takip uygulamaları vb.) testi için geliştirilen blok zincir altyapısında kurgu ve uygulama modelleri üzerinden pilot uygulamaların yapılması için test ortamı ve katılımcı kümesi oluşturulacaktır.

-Geliştirilen blokzincir uygulamalarının mevzuata uyumluluk testlerinin yapılması için düzenleyici kurul ile "sanal mevzuat test alanı" (regulatory sandbox) oluşturulması, testleri başarı ile tamamlayan girişimlerin sertifikasyonunun yapılarak yatırım almalarının desteklenmesi hedeflenmektedir (T.C. Sanayi ve Teknoloji Bakanlığı 2023 Sanayi ve Teknoloji Stratejisi, 2019, s. 76-80).

Pek çok ülke blok zinciri teknolojisine mesafeli yaklaşırken, bakanlık nezdinde Türkiye'nin böyle köklü değişim gerektiren bir teknoloji ile ilgili girişimde bulunması oldukça önemli bir vizyondur.

5.4.6. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı: On Birinci Kalkınma Planı

Kamu sektöründe, blok zinciri özelinde bir diğer önemli atılım ise Cumhurbaşkanlığı'nın yayımladığı 2019-2023 dönemlerini kapsayan on birinci kalkınma planı ile gerçekleşmiştir. Bu plana göre blok zinciri çözümlerinin geliştirilebilmesi için gerekli alt yapı, yazılım ve donanım gibi alanlara yatırım yapılacağı ve ulaşım ve gümrük işlerinde kullanılmak üzere blok zinciri alt yapı çalışmalarının tamamlanacağı ifade edilmiştir.

Ayrıca, blok zinciri üzerinde çalışan dijital Merkez Bankası parasının geliştirileceği ifade edilmiştir (T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, On Birinci Kalkınma Planı 2019-2023).

5.5. RTÜK İncelemesi

Radyo ve Televizyon Üst Kurulu bilgi hizmetlerini merkezi bir ağ yapısında istemci-sunucu mimarisiyle vermektedir. P2P gibi dağıtık sistemler olarak adlandırılan, verinin birden çok noktada işlenip temin edildiği bir ağ sistemi mevcut değildir.

Bu teze konu olan ve aynı zamanda dağıtık sistemlerden biri olan blok zinciri ağ teknolojisi henüz gelişmekte olan bir teknolojidir. Bazı alanlarda aktif olarak kullanılsa da, birçok alanda henüz gelişimini tamamlamış bir teknoloji olmamakla birlikte olgunlaşma sürecini tamamlamasının ardından gelecek yıllarda internetin bütün alt yapısında değişime yol açacağı öngörülmektedir. Blok zincirin olgunlaşmamasından kasıt, henüz hukuki temelleri ve regülasyonları üzerinde hukukçuların ve kamu yönetimi biliminin çalışmalarına devam etmesi, teknik boyuttaki eksilerinin belirlenmesi ile akademinin bu eksikler üzerinde çalışması anlamını taşımaktadır.

İnternetin değişime uğrayacağı dönem geldiğinde, kurumların bu teknoloji dönüşümüne hazır olmasında büyük fayda vardır. Teknoloji dönüşümünün unsurlarından biri de teknolojiyi kullanan insanları eğitmektir. Bu sebeple Üst Kurul personellerinin bilgi teknolojilerinde en azından temel seviyede bilgi sahibi olması Üst Kurulun sağlayacağı bilgi hizmetlerinin kalitesini de artıracaktır.

Blok zinciri teknolojisi Üst Kurul bünyesinde, blok zinciri tabanlı dijital kimlik uygulamaları, satın alım-ihale işlerinde, anket uygulamalarında, video kamera kayıt sisteminde, log alma cihazlarında, telif haklarının korunmasında, dezenformasyonla mücadelede, isteğe bağlı yayıncılıkta tüketicilere yönelik içerik dağıtımında ve ödeme sistemleri geliştirilmesinde, medya hizmet sağlayıcılarının şeffaflığının sağlanmasında, müzik kayıtlarında ve seçim dönemlerindeki yayınların yönetilmesi gibi alanlarda uygun çözümler sunabileceği düşünülmektedir.

Ayrıca, Radyo ve Televizyon Üst Kurulu olarak blok zinciri teknolojisinin kamu sektöründe kullanımına ilişkin olası katkımız yalnızca, kurum ihtiyacına yönelik münferit blok zincir uygulamaları değildir. TÜBİTAK, HAVELSAN, Turkcell, üniversiteler, THY gibi kurumların paydaşı olduğu BAĞ ismi verilen kamu blok zinciri test ağı gibi test ağlarına katılarak kamu blok zincirini geliştirme çalışmalarına katkı sağlayabilecektir. Bu çalışma hem güçleri birleştirmek açısından fayda sağlayacak, hem de test ağı olarak kullanılan blok zincir ağı ne kadar çok katılımcıya sahipse o derece güvenliği de artmaktadır.

6. SONUÇ VE ÖNERİLER

6.1. Sonuç

Bir kavramı incelenirken ne, nasıl, hangi saikle gibi sorular sorularak kavramın hizmet ettiği şey sorgulanmaktadır. Bu teze konu olan blok zinciri kavramı bu yönüyle incelendiğinde, "blok zinciri nedir, nasıl çalışır, hangi saikle kullanılmaktadır veya kullanılmalıdır" gibi sorulara yanıt vermek amaçlanmaktadır.

Blok zincirin ne olduğu, nasıl çalıştığı sorusuna bakıldığında, esasında hali hazırda kullanımda olan dağıtık sistemlerin geliştirilmiş bir halidir. Veri güvenliğine farklı bir boyut getirmiş olan dağıtık sistemler, yaklaşık 45 yıllık yeni olarak kabul edilen bir alandır. Bu alan ilk kez, Türk bir bilgisayar mühendisi ve akademisyen olan Prof. Dr. Eralp Akkoyunlu isimli akademiyen ve arkadaşlarının bir grup gangster problemini ortaya atmasıyla başlamış (Akkoyunlu, E. A.; Ekanadham, K.; Huber, R. V. ,1975, s.73) ve Leslie Lamport tarafından Bizanslı Generaller problemiyle (Lamport, L.; Shostak, R.; Pease, M., 1982) gelişmiştir. Bu alanda, 47 yıl boyunca sadece iki protokol ailesi gelişmiştir. Birincisi klasik algoritma veya klasik çözümler olarak tanımlanan, Leslie Lamport tarafından 45 yıl önce temeli oluşturulup, Barbara Liskov tarafından geliştirilmiş olan ve günümüzde bilinen bütün sistemlerin alt yapısında kullanılan protokol ailesidir. Örneğin, maillerine bakmak isteyen bir kişi hangi bilgisayardan mail uygulamasına giriş yaparsa yapsın aynı mailleri görmektedir. Bunun sebebi klasik bir mekanizma olan eş zamanlı karar alma mekanizmasıdır. 45 yıl boyunca hemen hemen bütün akademisyenler, içerisinde yüzlerce protokol bulunan ve çoğunluğu birbirinin aynısı olan, bu tip klasik algoritmalar üzerine çalışmalarını yürütmekteydi. İkinci protokol ailesi ise, 2008 yılında, Satoshi Nakamoto takma ismini kullanan anonim bir kişi veya grup tarafından klasik algoritmaların ölçeklenebilir olmaması ve açık sistemler için uygulanabilir olmaması sebebiyle ortaya çıkardığı Nakamoto Konsensüs Protokolüdür. Günümüzde Bitcoin ile adından söz ettirmekte olan Satoshi Nakamoto'nun buluşu, bu uzlaşı protokolüdür. Bu büyük atılım, internet üzerindeki verilerde oluşabilecek her türlü zararlı harekete karşı çok dayanıklı bir sistemdir. Ancak, yine Nakamoto Konsensüs Protokolü ile gelen madencilik sistemi çok fazla elektrik harcayan, dolayısıyla ekoloji için oldukça kötü ve donanım temini açısından ve madenci havuzlarının oluşmasıyla birlikte ortaya çıkan Bitcoin sistemi oldukça merkezi hale gelmiştir (Eyal, Sirer, 2013). Son bir yılda yapılan

bitcoin madenciliğinin yaklaşık %75'i 20'ye yakın madenci havuzları tarafından yapmaktadır (Hashrate Distribution, t.y.). Dolayısıyla sistem, bu 20 madenci havuzu etrafında büyük ölçüde merkezileşmiştir. Bitcoin ağındaki bu merkezileşmenin sebebi, havuzun içerisindeki kişilerin finansal kazançlarını artırma yönelimidir. Esasında bu 20 adet sistemin paydaşını koordine etmek için blok zinciri gibi dağıtık bir yapıya da ihtiyaç duyulmamaktadır. Bu sebeple günümüzde Bitcoin, 20-25 kişi üzerinde çalışacak klasik protokol ailelerinden biriyle yönetilebilir bir yapı halini almıştır. Satoshi Nakamoto Bitcoin'in sistemini ortaya çıkarırken yazdığı makalede hedeflediği şey, binlerce kişi üzerine dağılmış merkeziyetsiz bir yapı kurmaktı. Satoshi'nin bu vizyonu, bugünlerde aldığı şekliyle gerçekleşememiştir. Bir diğer yönden, enerji sarfiyatı açısından bakıldığında, 2020 verilerine göre dünya üzerinde sadece Bitcoin madenciliği için harcanan enerji, yedi nükleer enerji santralinin ürettiği enerjiye eşdeğerdir. (Redman Jamie, 2020, para1) Bu sebeple kripto paralara harcanan enerjinin daha faydalı ve dünyaya katkı sağlayacak bir alana yönlendirilmesi daha doğru olmaktadır. Bu tez ile amaçlanan kripto paraların altında yatan teknolojiyi bilgi güvenliğinde daha az madencilik gerektiren uzlaşı algoritmalarıyla, dolayısıyla daha az enerji tüketerek daha yüksek bir güvenlik sağlamak ve kamu sektörüne dağıtılmış merkeziyetsiz bir sistem kurmaktır.

Blok zincir teknolojisinin hangi saikle kamu sektöründe kullanılması gerektiği sorusuna gelindiğinde, gelecek dönemlerde kamu yönetim süreçlerinin insanlık tarihi boyunca hiç olmadığı kadar bilgi teknolojilerine bağlı olacağı düşünülmektedir. Blok zinciri teknolojisi dağıtık ağ yapısına sahip olması sebebiyle kamu hizmetlerinden faydalanan kişilerin, aynı zamanda, blok zincir ağının katılımcısı olarak, yönetime katılma olanaklarını artırmaktadır. Bunun yanı sıra, son dönemlerde şirket ve kurumların yaşadığı siber saldırılar ile veri tabanlarındaki bilgiler çalınmakta veya ayrıcalıklı yetkiye sahip kötü niyetli kurum çalışanlarınca kurum verileri üzerinde değişiklik yapılabilmektedir. Personel ve kurum bilgilerinin kötü niyetli kişilerin eline geçmesiyle bu bilgiler dolandırıcılık hadiselerinde kullanılmakta ve kurum itibarları zedelenmektedir. Blok zinciri teknolojisiyle devlet içerisindeki yolsuzluk ve sahtekârlık önlenebilmekte, yetki sahibi ayrıcalıklı kullanıcıların verileri değiştirmesi engellenmekte, bürokratik işlemlere hız kazandırılmakta ve devlet ile vatandaş arasındaki ilişkiler şeffaf hale gelerek devlete olan güven artmaktadır. Ayrıca, merkezi olan veri merkezlerinde yaşanan elektrik kesintisi gibi basit bir problem sebebiyle dahi kurumun sağladığı internet hizmetleri aksayabilmektedir. Bu tür problemlerin kök nedeni veri yönetiminin merkezi bir sistem üzerinden yapılmasıdır. Blok zinciri ağ yapısının,

bahsi geçen sorunları günümüzde büyük oranda çözecek yegâne teknoloji olduğu düşünülmektedir.

Blok zinciri teknolojisinin vergilendirme sistemlerinde kullanılması, vergi tahsilatının kolaylaşmasını, KDV gibi vergilerden kaçırma oranının azalmasını, işlem maliyetlerinin düşmesini, nakit akış problemlerinin çözülmesini, ödemelerin zamanında toplanmasını ve denetim mekanizmalarındaki bürokrasiyi azaltarak denetim elemanı eksikliği problemini ortadan kaldırmayı mümkün kılmaktadır. Blok zincirinin bu alanda kullanılmasını inceleyen Norveç Hükümeti Vergi Dairelerinde pilot bir uygulama geliştirmiştir. Bu uygulama beklenildiği gibi ifade edilen sorunları çözmüş, ancak, blok zincirine eklenen verilerin hiçbir zaman değiştirilememesi ve silinememesi, özel hayatın gizliliği ve unutulma hakkını ihlal ettiği değerlendirilmiştir. Daha ileri araştırmalar için diğer kamu kurumlarıyla bu pilot sistem geliştirilmeye devam etmekte olup halen net bir sonuca varılmamıştır (Ølnes ve Jansen 2018).

Finansal teknolojiler alanında, blok zincirin ödeme sistemlerinde kullanımının 2007 yılından günümüze kadar arttığına şahit olmaktayız. Benzer sistemler; ekonomistler, akademisyenler ve teknoloji geliştiriciler tarafından daha önce de tartışılmış örnek sistemler oluşturuluş, ancak hayat bulmamıştı. Çünkü bu sistemler, içerisinde çifte harcama problemi gibi problemler barındırmaktaydı. Bitcoin'in uzlaşı algoritması olan PoW'ün yayımlanmasıyla geçmişteki problemlere çözüm bulunmuş ve kripto paraların gündelik hatta kullanılmasının önü açılmıştır. Nitekim 5 Ekim 2009 tarihinde New Liberty Standart isimli borsa ilk Bitcoin kurunu yayınlamış; 22 Mayıs 2010 tarihinde bir kişi, 2 pizza için 10.000 Bitcoin ödemesi yaparak ilk gerçek Bitcoin alışverişini gerçekleştirmiştir. Günümüzde Microsoft Bitcoin'i ödeme aracı olarak kabul etmiş; AXA sigorta İsviçre'deki müşterilerine Bitcoin'le ödeme yapma imkânı tanımaya başlamış; Tesla Amerika Birleşik Devletleri'nde araç satışlarında Bitcoin'le ödeme yapılmasını kabul edeceğini açıklamıştır (euronews, 2021).

Bütün bu gelişmelerin yanı sıra, Norveç örneğinden görüleceği üzere blok zinciri teknolojisinin birçok avantajı bulunurken, bazı uygulamalarda bazı problemleri de beraberinde getirmektedir. Blok zinciri her probleme çözüm oluşturacak bir sistem değil, bazı problemlere çok iyi çözüm oluşturacak bir teknolojidir. Blok zincirin hangi problemlere iyi bir çözüm olacağı değerlendirilmeli ve bu uygulamalar hayata geçirilmelidir.

6.2. Öneriler

Radyo ve Televizyon Üst Kurulu başta olmak üzere tüm kamu kurum ve kuruluşlarının, hem kurumları bünyesinde çalışan personellere verdiği hizmetler hem de dışarıdaki vatandaşlara verdiği hizmetler değerlendirildiğinde, blok zincir teknolojisinin ülkemiz sınırlarında gelişimi için tavsiye edilen öneriler aşağıdaki gibidir:

- Blok zincir ağının yaygınlaşarak teknoloji dönüşümünü beraberinde getirmesi ihtimali göz önünde bulundurulduğunda, kamu kurumlarının bu dönüşümü gerçekleştiremeyip teknoloji transferini sağlayan tedarikçilere bağımlı kalma riskine karşı her kamu kurumu günümüzde blok zinciri üzerinde çalışmalar yapmalıdır.
- Katılımcıları sadece birbirine güvenen kamu kurumları olan ve yine kamu kurumları tarafında geliştirilen blok zincir ağı kurulmalı veya var olan blok zincir ağına kamu kurumlarının yüksek oranda katılımı sağlanarak test ortamları geliştirilmelidir.
- Tasarlanan blok zinciri ağı staking gibi ekolojik ve enerji tüketimine çok ihtiyaç duymayan uzlaşı algoritmaları ile çalışmalıdır.
- Tercih edilen uzlaşı protokolü, blok zinciri ağının katılımcılarına devlet kurumlarının koyduğu kurallara uyma zorunluluğu getirmelidir. Bu sayede hukuki alt yapısı uygun bir ağ üzerinde gerekli çalışmalar gerçekleştirilmelidir.
- Kamu sektörünün dijitalleşmesini hızlandırmak amacıyla gerekli altyapının oluşabilmesi için Radyo Televizyon Üst Kurulu bu alanda yapılan çalışmalara ortak olmalı ve katkı sağlamalıdır.
- Radyo ve Televizyon Üst Kurulunun, oluşturulan blok zincir çalışmalarına katkı sağlayabilmesi için belli sayıda personelin kamu blok zincir projesinin gelişimi için tahsis edilmesi sağlanmalıdır. Ayrıca, dijital dönüşümün en önemli adımı olan yetişmiş insan kaynağı arzı için yüksek nitelikli ve uzun soluklu eğitimler verilmesi, kamu blok zinciri projesinin olgunlaşabilmesi için en önemli husus olarak değerlendirilmektedir.

KAYNAKÇA

Akkoyunlu, E. A.; Ekanadham, K.; Huber, R. V. (1975). Some constraints and trade-offs in the design of network communications (s.73)

Aktaş G. (2018). Akıllı Sınır Yaklaşımı Çerçevesinde Blok Zinciri Teknolojisinin Gümrük İşlemlerinde Potansiyel Kullanım alanları (s.18-31)

Anand, Y., Pauleen, D. J., ve Dexter, S. (2011). Reserve Bank of New Zealand: Journey Toward Knowledge Management, Case Studies in Knowledge Management, United States of America: Idea Group Pub.

Aslanhan U. (2022, 24 Mart) Togg, Avrupa'nın önde gelen blok zinciri etkinliği Avalanche Zirvesi'ne davet edildi https://www.aa.com.tr/tr/bilim-teknoloji/togg-avrupanin-onde-gelen-blok-zinciri-etkinligi-avalanche-zirvesine-davet-edildi/2544863 Erişim Tarihi: 09 Mart 2023

Berryhill, J., Bourgery, T. & Hanson, A. (2018). Blokchains Unchained: Blokchain Technology and Its Use In The Public Sector (s.22)

Blockchainnz. (2019). BlockchainNZ Member Profile: Dasset. Blockchain Association of New Zealand https://blockchain.org.nz/2019/06/11/blockchainnz-member-profiledasset/ Erişim Tarihi: 11 Şubat 2023

Brikman Yevgeniy (2014, 24 Nisan) Bitcoin by analogy https://www.ybrikman.com/writing/2014/04/24/bitcoin-by-analogy/ Erişim Tarihi: 1 Mart 2023

Britannica (2019, t.y.). Encyclopedia Britannica Web Sitesi, https://www.britannica.com/technology/history-of-technology Erişim Tarihi: 08 Ocak 2023

Buterin Vitalik (2017, 2 Mart) Minimal Slashing Conditions (s. 5-11) https://medium.com/@VitalikButerin/minimal-slashing-conditions-20f0b500fc6c Erişim Tarihi: 4 Mart 2023

Case Study (t.y.): How Walmart brought unprecedented transparency to the food supply chain with Hyperledger Fabric https://www.hyperledger.org/learn/publications/walmart-case-study Erişim Tarihi: 4 Mart 2023

Chalmers John (2019, 7 Ekim) Can Blockchain solve Brexit's border puzzle? Experts are sceptical https://www.reuters.com/article/uk-britain-eu-border-idUSKBN1WM1XP Erişim Tarihi: 5 Mart 2023

Coinmaketcap https://coinmarketcap.com/ Erişim Tarihi: 1 Ekim 2022

Collaso, A. (2021). Blochchain in public sector, https://www.ciat.org/ciatblog-blockchain-en-el-sectorpublico/?lang=en Erişim Tarihi: 12 Ekim 2022

Emina Džaferović, Ajla Sokol, Ali Abd Almisreb, Syamimi Mohd Norzeli (2019, Haziran) DoS and DDoS vulnerability of IoT: A review https://doi.org/10.37868/sei.v1i1.36 Erişim Tarihi: 5 Mart 2023

Euronews https://tr.euronews.com/2021/12/05/bitcoin-ile-al-sveris-kripto-para-ile-odeme-kabul-eden-sirketler-hangileri Erişim Tarihi: 15 Ekim 2022

Eyal Ittay, Emin Gür Sirer (2013, 1 Kasım) Majority is not Enough: Bitcoin Mining is Vulnerable

E-nabız https://enabiz.gov.tr/Yardim/Index?page=a1&detail=b1) Erişim Tarihi: 1 Ekim 2022

Farhan M. (2017, 18 Aralık) Blockchain 2.0 | The 5th disruptive computing paradigm after mainframes https://www.linkedin.com/pulse/blockchain-20-5th-disruptive-computing-paradigm-after-mohammed-farhan Erişim Tarihi: 12 Eylül 2022

Garip E. (2023, 9 Ocak) Togg, dünyada bir ilk olan akıllı cihaza entegre dijital varlık cüzdanını CES'te tanıttı https://www.aa.com.tr/tr/ekonomi/togg-dunyada-bir-ilk-olan-akilli-cihaza-entegre-dijital-varlik-cuzdanini-ces-te-tanitti/2782976 Erişim Tarihi: 09 Ocak 2023

Garrett K.. (2017, 7 Mart). Local Government in South Korea Taps Blockchain for Community Vote https://www.coindesk.com/markets/2017/03/07/local-government-in-south-korea-taps-blockchain-for-community-vote/ Erişim Tarihi: 11 Mart 2023

Gazete Birlik (2017, 16 Kasım). Polisten Türkiye'de ilk 'Bitcoin' Operasyonu https://www.gazetebirlik.com/haber/polisten-turkiyede-ilk-bitcoin-operasyonu-121102/) (Para. 1) Erişim Tarihi: 10 Eylül 2022

Gürfidan & Arısoy (2021). Veri güvenliği için Blockchain Teknolojisi (s.52, s.58)

Hancock, M., ve Vaizey, E. (2015). Distributed ledger technology: Beyond block chain. UK: Government Chief Scientific Adviser

Hashrate (t.y.) Distribution https://www.blockchain.com/explorer/charts/pools Erişim Tarihi: 15 Kasım 2022

Houmansadr Amir (2015). https://people.cs.umass.edu/~amir/courses/CMPSCI660-SP15/slides/15-Bitcoin.pptx Erişim Tarihi. 27 Şubat 2022

Houmansadr Amir (2015) Secure Digital Currency: Bitcoin https://people.cs.umass.edu/~amir/courses/CMPSCI660-SP15/slides/15-Bitcoin.pptx Erişim Tarihi: 2 Mart 2023

Houmansadr A. (2015). https://people.cs.umass.edu/~amir/courses/CMPSCI660-SP15/slides/15-Bitcoin.pptx Erişim Tarihi: 09 Ekim 2022

IBM. (2020). IBM Research, Haifa http://www.research.ibm.com/labs/haifa/ Erişim Tarihi: 11 Ocak 2023

Insights Ledger (2020, 29 Nisan) Blockchain energy platform launched by Swiss, Dutch, Italian national electricity grids https://www.ledgerinsights.com/blockchain-energy-platform-electricity-grid-tennet-swissgrid-terna/ Erişim Tarihi: 5 Mart 2023

IQT News (2021, 18 Temmuz). Post-Quantum Digital Signatures https://www.insidequantumtechnology.com/news-archive/post-quantum-digital-signatures/ Erişim Tarihi: 27 Şubat 2022

Jezard Adam (2017, 15 Aralık) In 2020 Bitcoin will consume more power than the world does today https://www.weforum.org/agenda/2017/12/bitcoin-consume-more-power-than-world-2020/ Erişim Tarihi: 3 Mart 2023

Karch, G. M. (2014). Bitcoin, the law and emerging public policy: Towards 21st century regulatory scheme. Florida & University Law Review, s. 193-244.

Katsiri, R. (2019). Israel missing out on blockchain, study finds https://en.globes.co.il/en/article-israel-missing-out-on-blockchain-study-finds-1001308975 Erişim Tarihi: 11 Ocak 2023

Kohli et. Al. (2023) "An analysis of energy consumption and carbon footprints of cryptocurrencies and possible solutions," Digital Communications and Networks Volume 9, Yayın Tarihi 1 Şubat 2023, s. 79-89, https://doi.org/10.1016/j.dcan.2022.06.017

Konrad Wrona, Michal Jarosz (2018). Does NATO need a blockchain?

Kutbe H. (223, 2 Ocak) Cumhurbaşkanı Yardımcısı Oktay: e-Devlet'te yeni bir devrim olacak 'dijital kimliği' getiriyoruz https://www.aa.com.tr/tr/bilim-teknoloji/cumhurbaskani-yardimcisi-oktay-e-devlette-yeni-bir-devrim-olacak-dijital-kimligi-getiriyoruz/2777905 Erişim Tarihi: 12 Ekim 2022

Lamport, L.; Shostak, R.; Pease, M. (1982). The Byzantine Generals Problem

Mattila J. (2016). "The Blockchain Phenomenon – The Disruptive Potential of Distributed Consensus Architectures," ETLA Working Papers (s.13)

Mukherjee Srishti (2022, 2 Şubat) How Walmart uses blockchain to manage its supply chain https://analyticsindiamag.com/how-walmart-uses-blockchain-to-manage-its-supply-chain/ Erişim Tarihi: 4 Mart 2023

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

Ojo, A. ve Adebayo, S. (2017). Government 3.0 – Next Generation Government Technology Infrastructure and Services. Springer International Publishing, 32, 283–298.

Ølnes, S., & Jansen, A. (2018, Mayıs). Blockchain technology as infrastructure in public sector: an analytical framework. In Proceedings of the 19th annual international conference on digital government research: governance in the data age (s. 1-10)

Özaltın, O. ve Ersoy, M. (2020). Kamu Yönetiminde Blokzincir Kullanımı: D5 Örneği. Erişim Tarihi: 11 Aralık 2022

Özsoy Adnan (2020, Temmuz 29). Dağıtık sistemler, Koşut (Paralel) Hesaplama ve Blokzinciri Üzerine (para. 2). https://medium.com/@hubmbtanitim_38784/da%C4%9F%C4%B1t%C4%B1k-sistemler-ko%C5%9Fut-paralel-hesaplama-ve-blokzinciri-%C3%BCzerine-7712daae7124 Erişim Tarihi: 27 Şubat 2022

Priit M. (2018). Estonia – the Digital Republic Secured by Blockchain. Estonia: PWC.

PWC https://www.pwc.com/us/en/financial-services/research-institute/blockchain.html Erişim Tarihi: 09 Ekim 2022

Qanplatform “Proof-of-Randomness (PoR) consensus algorithm” https://learn.qanplatform.com/technology/technology-features/proof-of-randomness-por-consensus-algorithm Erişim Tarihi : 25 May 2022

Redman Jamie (2020, 20 Ağustos). The Bitcoin Network Now Consumes 7 Nuclear Plants Worth of Power https://news.bitcoin.com/the-bitcoin-network-now-consumes-7-nuclear-plants-worth-of-power/ Erişim Tarihi: 29 Aralık 2022

Resmi Gazete (2017, 21 Haziran) 21 Haziran 2017 tarih ve 30103 sayılı "Kamunet Ağına Bağlanma Ve Kamunet Ağının Denetimine İlişkin Usul Ve Esaslar Hakkındaki Tebliğ”

Süngü Murat (2020, 20 Temmuz) Veri Bütünlüğü(Data Integrity) https://medium.com/@muratsng/veri-b%C3%BCt%C3%BCnl%C3%BC%C4%9F%C3%BC-data-integrity-34034c0878d9 Erişim Tarihi: 27 Şubat 2022

T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı (2019), On Birinci Kalkınma Planı (2019-2023), https://www.sbb.gov.tr/ Erişim Tarihi: 15 Ekim 2022

T.C. Sanayi ve Teknoloji Bakanlığı (2019). 2023 Sanayi ve Teknoloji Stratejisi, https://www.sanayi.gov.tr (s.80)

Team Rocket (2018, 16 Mayıs) Snowflake to Avalanche: A Novel Metastable Consensus Protocol Family for Cryptocurrencies

Tecim, E., Yılmaz, F. ve Karakoyunlu, M. (2023). Metafor ve olgusal gerçeklik olarak kripto para algısı. Manas Sosyal Araştırmalar Dergisi, 12(1), 270-289. doi:10.33206/mjss.1177017

Togg (2020, 7 ocak) Togg and Ava Labs Announce Strategic Partnership at CES 2022 to Build First Mobility Blockchain Solutions on Avalanche https://www.togg.com.tr/en/togg-and-ava-labs-announce-strategic-partnership.html Erişim Tarihi: 21 Kasım 2022

TRT Haber (2019, 13 Aralık) Bilgisayar korsanı, çocukların odasındaki kamerayı hackledi https://www.trthaber.com/haber/dunya/bilgisayar-korsani-cocuklarin-odasindaki-kamerayi-hackledi-446398.html Erişim Tarihi: 5 Mart 2023

Universidad Carlos III de Madrid (2018), Universidad Carlos III de Madrid is issuing degree certificates with blockchain, https://www.uc3m.es Erişim Tarihi: 5 Ekim 2022

Usta A., Doğantekin S. (2018). Blockchain 101 v.2. Bankalararası Kart merkezi (s.18)

Zeki (2020, 28 Haziran). P2P Network Yapısı ve Kullanım Alanları (para.1). https://sabahlatan.com/blog/p2p-network-ve-kullanim-alanlari/ Erişim Tarihi: 13 Eylül 2022

ÖZGEÇMİŞ

Kişisel Bilgiler

Adı ve Soyadı: Enes ÇELİKER

E-Posta Adresi: enesceliker@rtuk.gov.tr

İş Deneyimi:

Unvan	**Görev Yeri**	**Yıl**
Üst Kurul Uzman Yardımcısı	Radyo ve Televizyon Üst Kurulu	2019- Devam Ediyor

Akademik Bilgiler

Öğrenim Durumu:

Derece	**Bölüm/Program**	**Üniversite**	**Yıl**
Hazırlık Sınıfı	İngilizce Hazırlık Sınıfı	Pamukkale Üniversitesi	2011-2012
Lisans	Bilgisayar Mühendisliği (İng.)	Pamukkale Üniversitesi	2012-2016
Yüksek Lisans	Bilgisayar Mühendisliği (İng.)	Hacettepe Üniversitesi	2022- Devam ediyor

Yayınlar:

H. Özkul, E. Çeliker, M. Aydos, A. Özsoy, " Comparison of Top 10 Well-Known Blockchain Consensus Algorithms," 16th International Conference On Information Security And Cryptology, 2023

RTÜK