T.C.
İSTANBUL AREL ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
İŞLETME ANABİLİM DALI

HAVACILIK ENDÜSTRİSİNDE BLOCKCHAİN TEKNOLOJİİSİNİN POTANSİYALİNİ KEŞFETMEK

YÜKSEK LİSANS TEZİ

ABDURRAHIM TAÇILIK

İSTANBUL, 2021

T.C.
İSTANBUL AREL ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
İŞLETME ANABİLİM DALI

HAVACILIK ENDÜSTRİSİNDE BLOCKCHAİN TEKNOLOJİİSİNİN POTANSİYALİNİ KEŞFETMEK

YÜKSEK LİSANS TEZİ

ABDURRAHİM TAÇILIK

İSTANBUL, 2021

KABUL VE ONAY

ABDURRAHİM TAÇILIK tarafından hazırlanan "**Havacılık Endüstrisinde Blockchain Teknolojiisinin Potansiyalini Keşfetmek"** adlı tez çalışmasının savunma tarihi 14.06.2021 tarihinde yapılmış olup aşağıda verilen jüri tarafından oy birliği /oy çokluğu ile İstanbul Arel Üniversitesi Lisansüstü Eğitim Enstitüsü İşletme Anabilim Dalı olarak kabul edilmiştir.

Jüri Üyeleri İmza

Danışman
DR. SEÇİL GÜRÜN KARATEPE

Eş Danışman

DOÇ.DR. ZEYNEP HATİPOĞLU

Üye

DR. ELVİN DİNLER KISAÇTUTAN

İstanbul Arel Üniversitesi Lisansüstü Eğitim Enstitüsü Yönetim Kurulu'nun

……. tarih ve..... sayılı kararıyla onaylanmıştır.

…….

Prof. Dr. Ali AKDEMİR

Lisansüstü Eğitim Enstitüsü Müdürü

YEMİN METNİ

Yüksek Lisans Tezi olarak sunduğum "**Havacılık Endüstrisinde Blockchain Teknolojiisinin Potansiyalini Keşfetmek**" başlıklı bu çalışmanın, bilimsel ahlak ve geleneklere uygun şekilde tarafımdan yazıldığını, yararlandığım eserlerin tamamının kaynaklarda gösterildiğini ve çalışmanın içinde kullanıldıkları her yerde bunlara atıf yapıldığını belirtir ve bunu onurumla doğrularım.

14.06.2021

ABDURRAHİM TAÇILIK

ÖZET

HAVACILIK ENDÜSTRİSİNDE BLOCKCHAİN TEKNOLOJİSİNİN POTANSİYELİNİ KEŞFETMEK
YÜKSEK LİSANS TEZİ
ABDURRAHİM TAÇILIK
İSTANBUL AREL ÜNİVERSİTESİ LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ İŞLETME ANABİLİM DALI
(DANIŞMAN: DR.ÖĞR.ÜYESİ SEÇİL GÜRÜN KARATEPE)

İSTANBUL, 2021

Blockchain teknolojisi, kurumsal yapıların işleyişlerinde bulunan sorunlar ve global kriz ile beraber bir kere daha sarsılmakta olan güvene paralel olarak meydana gelmektedir. Yeni bir sistem sunmasından dolayı blockchain teknolojisi önemli ve dikkat çeken bir alandır. Blockchaine benzemekte olan pek çok teknolojinin geliştirilmesi için çabalanmıştır. Merkezi sistemlere karşı gücün dağınık bulunduğu daha güvenilir ve özgür bir veri ağı modelinin oluşturulmaya çabalanması, bu teknolojilerin ortak özeliği olarak karşımıza çıkmaktadır. Buradan hareketle merkezi kurumlara karşı bulunan güvensizlik ve işleyişte olan sorunların daha önceden fark edildiği ve değiştirilmesi için uğraşıldığı anlaşılmaktadır. Bu teknoloji, bir merkeze bağlı olmadan kriptografi kullanılarak ve veri blokları şeklinde zincirlenmesi modeli ile meydana getirilmektedir. Güvenilir olmaları ise söz konusu teknolojilerin en mühim noktalarıdır. Var olan sistemlere kıyasla blockchain teknolojisinin değer, veri ya da öteki bilgilerin muhafaza edilmesi ve transferinin sağlanmasında daha kullanışlı olması söz konusudur. Blockchain teknolojisi, bilhassa havacılık sektöründe önemli değişimleri sağlamıştır. Havacılık sektöründe blockchain teknolojilerinin ele alınması bu çalışmanın amacını oluşturmaktadır.

Bu araştırmada yalnızca literatür taraması kapsamında elde edilen verilerden faydalanılmıştır.

Anahtar Kelimeler: Teknoloji, Blockchain, Havacılık Endüstrisi

ABSTRACT

DISCOVERING THE POTENTIAL OF BLOCKCHAIN TECHNOLOGY IN THE AVIATION INDUSTRY

MSC THESIS

ABDURRAHİM TAÇILIK

GRADUATE SCHOOL, ISTANBUL AREL UNIVERSITY

BUSINESS ADMINISTRATION

(SUPERVISOR: DR.ÖĞR.ÜYESİ SEÇİL GÜRÜN KARATEPE)

İSTANBUL, 2021

Blockchain technology occurs in parallel with the problems in the functioning of corporate structures and the trust that is being shaken once again with the global crisis. Blockchain technology is an important and attention-grabbing field because it offers a new system. Efforts have been made to develop many technologies similar to blockchain. The common feature of these technologies is the effort to create a more reliable and free data network model where the power is dispersed against central systems. From this point of view, it is understood that the distrust towards the central institutions and the problems in operation were noticed before and efforts were made to change them. This technology is created by using cryptography without being connected to a center and by chaining it in the form of data blocks. Being reliable is the most important point of these technologies. Compared to existing systems, blockchain technology is more useful in maintaining and transferring value, data or other information. Blockchain technology has brought significant changes, especially in the aviation industry. The aim of this study is to consider blockchain technologies in the aviation industry.

In this study, only the data obtained within the scope of literature review was used.

Key Words: Technology, Blockchain, Aviation Industry

İÇİNDEKİLER

Sayfa

ŞEKİL LİSTESİ

Sayfa

TABLO LİSTESİ

Sayfa

KISALTMA VE SEMBOL LİSTESİ

SHA	:	Amerika Birleşik Devletleri Federal Bilgi İşleme Standardı
NSA	:	Amerika Birleşik Devletleri Ulusal Güvenlik Ajansı
NIST	:	Ulusal Standartlar ve Teknoloji Enstitüsü Kısaltma
PBFT		Bizans Hata Toleransı
ABD		Amerika Birleşik Devletleri
IIF		Uluslararası Finans Enstitüsü
PoW		Emek/İş Kanıtı

ÖNSÖZ

14.06.2021

ABDURRAHİM TAÇILIK

1 GİRİŞ

Kişiler arasında bulunan etkileşimin daha kolay hale gelmesini sağlamak ve güven duyulan bir üçüncü taraf olmak, modern toplumlarda kurumsal yapıların temel vazifesidir. Bu etkileşimde çözüm şeklinde değerlendirilen kurumların bugün kendilerinin birer problem olması söz konusudur. Bu durumun ortaya çıkmasında ise, pek çok merkezi yapının oluşma amacından şaşması ve gün geçtikçe daha karışık ve iç içe gelen iletişim biçimlerinin bulunması etkili olmaktadır. Teknolojinin ilerlemesi bu iletişimi hem kolaylaştırmakta hem de kurumsal yapılarda olan işleyişlerden olan beklentileri arttırmaktadır. Burada dönüşüme ve gelişmeye adapte olmada yetersiz kalan kurumsal yapıların eski fonksiyonlarını kaybetmesi söz konusudur.

Güvenirlik sorunu, modern toplumsal yaşamın işleyişinde bulunan ana yapılar olan kurumlar hakkındaki en problemlerden biri olarak karşımıza çıkmaktadır. Köklü yapılar üzerinde kurulduğu düşünülen finans ve bankacılık sektörü kadar 2008 küresek finans krizinde bu yapıları düzenlemekte olan merkezi kurumlara karşı da güven sorunu oluşmuştur. Hem finans sektörü hem de merkezi şekilde işlemekte olan neredeyse bütün kurumlar için bu güvensizlik ortaya çıkmıştır. Yetersiz teknolojik alt yapının bulunması ve işlevsel hale getirilmesinin mümkün olmaması neticesinde meydana gelen sorunlar, bu güvensizliğin ana nedenlerinden biridir. Kurumlardan çok insanlar alıcı, kullanıcı ya da alıcı şeklinde teknoloji vasıtası ile direkt birbirleri ile oluşturdukları iletişime karşı güven duymaktadır. Gelecek dönemde bu sorunun iki muhtemel neticesi bulunmaktadır. Bunlar kurumların dönüşmesi ya da ortadan kalkmasıdır. Kurumların yapıları çerçevesinde bu neticelerin değişebilmesi mümkündür.

Blockchain teknolojisinin sağladığı özellikler burada gündeme gelmektedir. Verilerin bloklar şeklinde bir merkeze bağlı olmadan kriptografi kullanılarak zincirlenmesi modeli ile meydana getirilen bu teknoloji güven sağlamaktadır. Blockchain teknolojisi çalışmanın literatür araştırmasında olan ilk bölümde ele alınmıştır. Bu şekilde bu yeni teknolojinin daha iyi şekilde anlaşılabilmesi hedeflenmiştir. Uzun bir süredir bu şekilde bir sistemin varlığı, geçmişe bakıldığında karşımıza çıkmaktadır. İnsanlar tarafından merkezi otoritelerin işleyiş biçimleri güvensiz ve yetersiz bulunmaktadır. Bu

çerçevede blockchain teknolojisini meydana getirene dek pek çok benzer çalışma gerçekleştirmişlerdir. Blockchain teknolojisine son zamanlarda ilgi gösterilmektedir. Aslında bu durumun nedeni de yine aynı sebeptir. İnsanlar bilhassa mali manada meydana gelen krizler, kurumsal yapıda bulunan güven ve uyum sorunları, merkezi otorite tarafından sergilenen katı tutumlar sonucunda yeni bir sistemi yaratmak istemektedir.

Blockchain teknolojisinin, ortaya çıkan sorunların çözülmesinde yeterli gelip gelmeyeceği halen bir tartışma konusudur. Ancak geliştirilmiş olan proje ve uygulamalar ile önemli derecede başarı elde edilmesi söz konusudur. Bu araştırmanın amacı havacılık sektöründe blockchain teknolojilerinin incelenmesidir. Blockchain teknolojileriyle beraber havacılık sektöründe yeni deneyimler yaşanmaktadır. Hem yolcu tarafından hem de üretim-tedarik aşamasında, blockchain teknolojileri ile benzersiz bir dönüşüm gerçekleşmektedir. Bununla beraber literatürde havacılık sektöründe blockchain teknolojilerinin incelendiği çalışma sayısı oldukça sınırlıdır. Bu araştırma havacılık sektöründe blockchain teknolojilerinin incelenmesi açısından literatüre katkı sağlayacaktır.

2 BLOCKCHAIN TEKNOLOJİSİ

2.1 Blok Zincir Teknolojisi

Savunmasız bir SPOT merkezi ağlarda yer almaktadır. Blok zincir teknolojisi bu problemi gidermek amacı ile bizlere dağıtılmış bir ağ yapısı arz etmektedir. Verim sistemi içinde bulunan tüm katılımcılar blok zincirde kayıt tutmaktadır. Birbirlerini tanımayan bireylerin paylaşılmış olan işlem kayıtlarına güven duymalarını sağlayan teknoloji, blok zincir olarak karşımıza çıkmaktadır. Kısacası blok zinciri, birbirlerine karşı güveni bulunmayan katılımcıların yer aldığı ağda işlemleri güvence altına alarak güveni sağlayan teknolojilerdir. Burada güven, bütün katılımcılara sistemin en başında tanımlanmış olan kurallar ve bu kurallar doğrultusunda meydana getirilen kayıt zincirinin dağıtılması ile gerçekleştirilmektedir (Usta & Doğantekin, 2018). Bilgisayarlardan yararlanarak işlerini doğrulayabilmek amacı ile paylaşılmış olan işlem kayıtlarının ağda yer alan bütün katılımcılara dağıtılması söz konusudur. Böylece üçüncü tarafa olan gereksinimi doğrulama yöntemi sona erdirmektedir. Blok zinciri ilk bakışta karışık görünmektedir. Ancak esasında katılımcı bir ağda bulunan bütün bilgisayarlara kopyalanan işlemleri kayıt altında tutmak amacı ile yararlanılan veri tabanı çeşididir (Deloitte LLP, 2016).

Belli bir merkezi bulunmayan güvenli kayıt vazifesi ve doğrulama sistemi görevini üstlenmesi, gayrimenkullerin, varlıkların kayıtlarının tutulması, diploma, evlilik, ölüm gibi süreçlerin belgelerin kayıt altına alınması, mali belgeleri işlenmesi, düzenlenmesi gibi pek çok alanda kullanılabilecek bir teknoloji olarak karşımıza çıkmaktadır. Bu teknoloji yapısal olarak dijital kimlikler bağlamında günümüze kadar görülmeyen bir denetim ve kontrol olanağı sağlamaktadır (Dilek, 2018). Block zincir sistemine dahil olan tüm bloklar bağlamında geçmişe yönelik bir geri dönme olanağının olması şeffaflığın sağlanmasına imkan vermektedir. Var olan kayıtların farklılaştırılmasına mani olan sistemi sayesinde yönetim ihtiyacını ortadan kaldırmaktadır. Evrak, aracı ve yönetim süreçlerinin ortadan kaldırması nedeniyle maliyetlerin oldukça düşmesini sağlamaktadır (Beck ve diğ., 2016). Block zincir uygulamalarının maliyetleri düşüren ve işlemleri kolaylaştıran etkileri bu teknolojilerin bazı ülkelerin kamu sektöründe kullanılmaya başlamasına neden olmuştur. Block zinciri

uygulamalarının kamu sektöründe kullanıldığı bağlı işlemler şu şekilde sıralanabilir (Sayar, 2019):

- Pasaport ve dijital kimlik
- Enerji dağıtımı
- Doküman yönetim süreçleri
- Seçimlerin yerine getirilmesi (Oylama)
- Vergi sistemleri
- Akıllı kontratlar
- Sosyal Güvenlik Sistemleri

2.1.1 Blok

Blok ismi verilen sabit yapılarda bir blok zincirinde yer alan veriler muhafaza edilmektedir. Ayrıca bir blok 2 bölümden meydana gelmektedir:

1. Blok başlığı (Header); bloğun meydana getirildiği zaman (Timestamp), benzersiz bir blok referans numarası bir önceki bloğun başlığının özeti ve bu bloğun merkleroot'unun özetinden (Hash of Block Data) meydana gelmektedir.
2. Blok gövdesi; çoğunlukla gerçekleştirilen işlemler benzeri sayısal varlık ve talimatların onay verilmiş bir listesi, miktarı ve söz konusu bu işleme taraf olanların adreslerinden meydana gelmektedir.

Zincirde birbirlerine bağlı önceki bütün bloklara ulaşmak en son bloktan başlayarak mümkün olmaktadır. Dolayısıyla birinciden başlayarak blok zincirinde bulunan bütün varlıkların ve yapılan işlemlerin bütün tarihçesini blok zincirinin koruduğu söylenebilmektedir. Bu şekilde blok zincirindeki veriler doğrulanabilmektedir. Aynı zamanda bu verilerin denetlenmesi de mümkün olmaktadır.

Blok zincirdeki ilk bloğa Başlangıç Bloğu (Genesis Block) adı verilmektedir. Bu bağlamda herhangi bir bloktan geriye yönelik bakmaya başlandığında son olarak bu bloğa erişilmektedir.

2.1.2 Düğüm

Düğüm blok zinciri meydana getiren veri bloklarının muhafaza edildiği bütün cihazlar olarak karşımıza çıkmaktadır. Bir blok zincirinin alt yapısını bu düğümler meydana getirmektedir. Aynı zamanda verileri depolama, koruma ve yayama vazifesi de bulunmaktadır. Her bir düğümde teorik olarak blok zincirinin bir kopyasının bulunması söz konusudur.

Blok zincirine yeni bir işlem bloğunu ilave etmek isteyen madencinin bloğu ağda yer alan bütün düğümlerde yararlanılır. Düğümlerin bloğu ret ya da kabul etmesi, blokta bulunan işlem ve imzaların geçerliliği doğrultusunda gerçekleşmektedir. Yeni bir işlem bloğunu bir düğümün kabullenmesi ile birlikte bahsi geçen bu bloğu daha önceden kayıt altına alınan blokların sonuna ilave edilmektedir. Aşağıda düğümlerin görevlerine yer verilmiştir:

- Blok zinciriyle işlem geçmişinin senkronize edilebilmesi amacı ile öteki düğümlere yaymak ve yayınlamak
- İşlem bloğunun geçerliliğine bakmak, bu bloğu ret ya da kabul etmek
- Blokları kayıt altına almak ve muhafaza etmek

Düğümlerin yetki ve görevlerinin farklı blok zincir yapılarında sınırlandırmak ve çeşitlemek mümkündür. Düğüm türlerine aşağıda yer verilmiştir (Pinto, 2018):

Düğüm: İşlemleri hem alabilen hem de gönderebilen blok zincir ağında çalışmakta olan bir istemci olarak karşımıza çıkmaktadır.

Tam düğüm: Blok zincirinin tam bir kopyasını tutmakta olan ve ağda çalışan istemci olarak ifade edilmektedir. Gerçekleştirdikleri işlemler arasında işlemleri alma, gönderme ve blok zinciri blok girişleri ve madencilerin onaylarıyla güncelleme yer almaktadır.

Ana düğümler: Merkezi olamayan idare ve bütçeleme ana düğümler tarafından sağlanmaktadır. Hem düğümün bir kopyasını hem de onaylanmamış işlemlerin bellek havuzu ya da arzu edilmeyen işlem çıkışları önbelleği benzeri ek verileri yapılarında

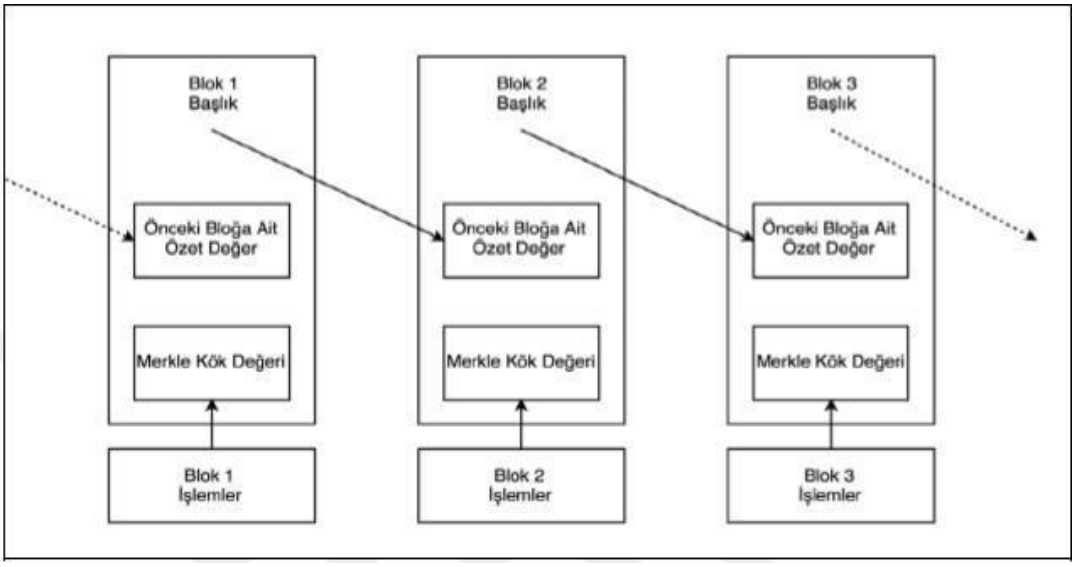
barındırması söz konusudur. Bu şekilde yeni alınmış olan işlemlerin ve çıkarılmış blokları hızlı biçimde doğrulaması mümkün hale gelmektedir. Ana düğüm, alınan işlem ya da blokların geçerli olması durumunda güncellemektedir. Ayrıca bağlı düğümlere de aktarımını sağlamaktadır. Bunun yanı sıra öteki düğümlere ana düğümün güvenmesi gerekli olmamaktadır. Bu durumun nedeni ise ana düğümün onlardan almış olduğu bütün bilgileri bağımsız şekilde doğruluyor olmasıdır.

2.1.3 Özet Fonksiyonları

Blok zincir teknolojisinde geçmiş kayıtların muhafaza edilmesi, değişemez olması ve göndericinin kimliğinin güvene alınması için kriptografiden yararlanılmaktadır. Bu şekilde güvenli olarak işlemler gerçekleştirilmektedir. Aynı zamanda bütün bilgiler güvence altında tutulabilmektedir.

Düz bir metinden meydana gelen verilerin sabit boyutlu rastgele verilere dönüştürülmesinde kriptografik özet fonksiyonlarından yararlanılması söz konusudur. Tek yönlü çalışan bu özet fonksiyonları ile baştaki düz metnin sonuç değerlerden geri dönüştürülmesi mümkün hale getirilmektedir. Çoğunlukla tek yönlü olan özel fonksiyonlarda zayıf çakışmaya dayanıklılık isimli 2 güvenlik ihtiyaç söz konusudur. Temel özet fonksiyonunun çevrilmesini bunlardan birincisi sağlamaktadır. Diğeri ise aynı özet değeri bulunan 2 giriş metnini bulmanın basit olmadığını belirtmektedir (Wang ve diğ., 2019).

Değişmezlik, blok zincirinin en mühim özelliklerinden biri olarak karşımıza çıkmaktadır. Bu durumda özet fonksiyonların rolü oldukça büyüktür. Her bloğun kendisinden önceki bloğun özetini barındırması söz konusudur. Böylece genesis ismi verilen ilk bloktan son bloğa doğru uzanan bir bloklar zinciri meydana getirilmektedir. Zincirin içerisinde yer alan herhangi bir blokta bulunan verinin değiştirilmesini ise bu metot daha güç hale getirmektedir. Bir bloğun değişmesi halinde bütün blokların yenilenmesinin gerekli olması, bu durumun gerekçesi olarak gösterilmektedir. Özetleme faaliyeti ise aşağıdaki gösterildiği gibi yürütülmektedir.



Şekil 2.1 Özetleme Fonksiyonu

Kaynak: Usta & Doğantekin, 2017 akt. Kınacı, M. (2019).Yüksek Lisans Tezi, Blockchaın Teknolojisi Ve Akıllı Sözleşmelerin Yaygınlaşmasının Önündeki Engeller, Yüksek Lisans Tezi, Bahçeşehir Üniversitesi, Fen Bilimleri Enstitüsü.

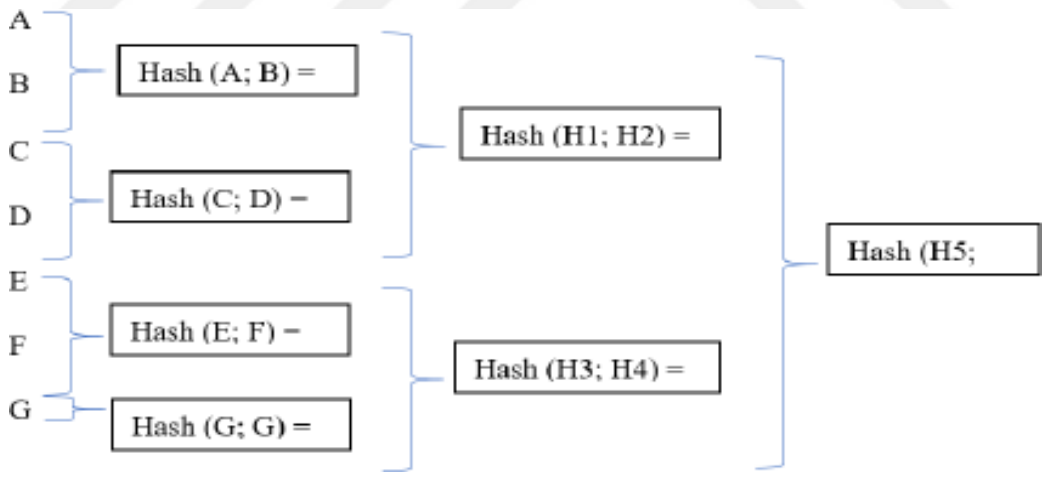
Yukarıdaki özetleme fonksiyonu ile büyük verilerden dijital parmak izi ve küçük bir özet bilgi temin edilmektedir. Özetleme fonksiyonları yapısal olarak tek yönlü çalışmaktadır. Bu açıdan özet bilgilerden kaynağa erişilmesi mümkün olmamaktadır. Minik bir veri değişikliği bile söz konusu olursa açığa oldukça farklı bir özet bilgi yığını meydana gelmektedir. Ortaya çıkan bu tabloya ise "çığ etkisi" denilmektedir (Kınacı, 2019).

SHA256 blok zincirinde yararlanılan en popüler özet fonksiyonudur. Bu fonksiyon SHA (SecureHashAlgorithms) adlı bir özet fonksiyonu ailesinin algoritmalarından biri olarak karşımıza çıkmaktadır. Aynı zamanda Amerika Birleşik Devletleri Federal Bilgi İşleme Standardı SHA olarak karşımıza çıkmaktadır. Amerika Birleşik Devletleri Ulusal Güvenlik Ajansı (NSA) bu ailede bulunan algoritmaların pek çoğunu SHA0 (1993), SHA1 (1995), SHA2 (2001) dahil olmak üzere tasarlamıştır. Keccak tarafından SHA3 (2014) üretilmiştir. Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) ise sadece dolgu yönteminde değişiklik yapmıştır. Kripto para biriminde ve blok zincirinde var olan güvenlik gereksinimini gidermek amacı ile SHA2 ve SHA3'den yararlanılması tavsiye edilmektedir (Wang ve diğ, 2019).

2.1.4 Merkle Ağaç Yapısı

İşlemin orijinal bilgisini barındıran özet şeklinde bilinen bir tanımla kodu bütün işlemlerde bulunmaktadır. Merkle Ağacı şeklinde isimlendirilen bir sistemde bir blokta toplanan işlemlerin özet değerlerinin bir araya getirilmesi söz konusudur. Önceki bloğun zaman damgası ve özeti benzeri öteki bilgiler ile beraber bahsi geçen bu özet değeri bir bloğun başlığına ilave edilmektedir. Bunun yanı sıra blokların değiştirilmesine ve hile yapılmasında yeni blokta bulunan önceki özet değeri engel olmaktadır. Verilerin o anda bulunduğunu ise zaman damgası kanıtlamaktadır. Temel olarak blokta yer alan bütün işlemlerin organizasyonunda Merkle ağacından yararlanıldığı söylenebilmektedir.

Ralph Merkle tarafından Merkle ağacı tavsiye edilmiştir. Bu öneriyi veri entegrasyonunun verimli biçimde doğrulması açısından sunmuştur. Veriler, bütünlüklerin kontrol edilmesi amacı ile düğümler halinde değerlendirilmektedir. 2 alt düğümün bir araya gelmesinden üst düğümler meydana gelmektedir. Kök düğümüne doğru bu hesaplama sürmektedir. Ayrıca kökün özeti, tüm ağacın son özeti olarak karşımıza çıkmaktadır. Merkle Ağaç Yapısı Örneği Şekil 2.2'de görüldüğü gibidir.



Şekil 2.2 Merkle Ağaç Yapısı Örneği

Kaynak: Yılmaz, O. (2019). Block-Chain Teknolojisi ve B2B Finans İşlemlerinde Kullanılabilirliği, İstanbul Aydın Üniversitesi, Fen Bilimleri Enstitüsü.

2.1.5 Dijital İmzalar

İşlemin dijital imzayla doğrulanması, blok zincirinde bir işlemin meydana getirilmesinde gerekli olmaktadır. İmzalama ve doğrulama olmak üzere tipik bir dijital imza işlemi 2 aşamadan oluşmaktadır. Gönderen tarafın bir işlemi imzalamayı talep etmesi halinde ilk olarak işlemden türetilmiş olan bir özet değerinin üretilmesi söz konusudur. Bu özet daha sonra özel anahtar yardımı ile şifrelenmektedir. Şifreli özet alıcı tarafa orijinal veriler ile beraber gönderilmektedir. Alıcı taraf ise doğrulama işlemi yapmaktadır. Bunu alınan işlemi, şifrelenmiş özet ve alınan verilerden sağlanan değeri, gönderenin yararlandığı özet fonksiyonu ile kıyaslayarak gerçekleştirmektedir.

2.1.6 Mutabakat

Her düğümün gelen blokları onaylaması ve kendi blok zincir kopyasını ilave etmesi blok zincirinde gereklidir. Bir başka ifade ile ağda bulunan bütün kullanıcılar kabul ve doğrulma yapmalıdır. Mutabakat ise bu doğrulama ve kabul işlemine verilen isimdir. Fakat bütün ağ durumunun her düğüm için farklı bir görünümünün bulunması söz konusudur. Dolayısıyla bu problem ile baş edebilmek amacı ile dağıtılmış bir mekanizma gereksinimi ortaya çıkmaktadır. Ayrıca blok zincirinde dağıtılmış mekanizmada uzlaşmaya varılması mühim bir parça olarak karşımıza çıkmaktadır. Genellikle yararlanılan 3 mutabakat algoritması bulunmaktadır. Bunlara aşağıda kısaca yer verilmiştir.

2.1.6.1 İş Kanıtı (PoW)

Blok zincirde en fazla yararlanılan algoritma İş kanıtı (PoW) mutabakat algoritması olarak karşımıza çıkmaktadır. Uygun blokları meydana getirerek ve PoW örneklerini çözerek bütün katılımcıların işlem gücüyle oy kullandığı kabul görmektedir. Bitcoinhash tabanlı bir PoW kullanılması bu duruma örnek olarak gösterilmektedir.

Önceki blok özeti ve merkle kök özeti benzeri ek blok parametreleriyle beraber özeti alınması durumunda bu metotta, bir hedef değerinden daha az olan bir değerin bulunması gerekli olmaktadır. Bahsi geçen bu değer nonce değeri olarak adlandırılmaktadır. Madeni tarafından bu şekilde bir değerin bulunması sonucunda bu

değer ile blok meydana getirilmektedir. Aynı zamanda öteki düğümlere iletilmesi de söz konusudur. Bu işlem madencilik şeklinde ifade edilmektedir. Bloğun özet değerini ağda yer alan öteki düğümlerin hesaplaması ile hedef değerinden daha küçük olma şartını yerine getirip getirmediği kontrol edilerek iş kanıtı yapılmaktadır. Bunun yanı sıra PoW hem çok yavaş hem de oldukça önemli derece enerjiyi gerekli kılmaktadır.

Temel haliyle iş kanıtı (PoW) süreci şu aşamalar dahilinde meydana getirilmektedir (Durbilmez, 2018):

- Yeni blok dahilinde bulunması arzu edilen bilgiler seçilmektedir.
- Söz konusu verilerden yararlanılarak Merkle ağacı yapısı ile Merkle kök değerleri meydana getirilmektedir.
- Merkle kök değeri, bir evvelki bloğun zaman bilgisi, özet değerleri ve ard arda yükselen bir sayaç biçiminde tanımlanabilen bir nonce değerinden yararlanılarak blok başlıkları meydana getirilir.
- Block başlıkları özetlenip makul bir değer meydana getirilip getirilmediği denetlenir.
- Makul bir blok özet değeri meydana gelmişse yeni blok düzgün bir biçimde meydana getirilmiş demektir. Bu blok ağ üzerindeki tüm makinelerle paylaşılır.
- Makul bir blok özet değeri yaratılamamışsa nonce değeri yükseltilerek makul bir değer meydana getirilmeye çalışmaktadır.

2.1.6.2 Hisse Kanıtı (PoS)

Bir blok meydana getiren düğümün ağ da kabul görmeden önce belli oranda bir miktar kripto paraya ulaşabildiğinin kanıtını sağlaması PoS'a göre gerekmektedir. Aynı zamanda daha çok para birimi bulunan bireyin ağa saldırma olasılığının az olduğu varsayımı doğrultusunda belli miktarda katılımcıların değerinin bulunduğunu kanıtlanması bu metotta gereli olmaktadır (Zheng ve diğ., 2018). Dolayısıyla blok zincirini koruma sürecinde yalnızca PoS'yi kullanabilenlerin katılması mümkündür. PoS, enerji tasarrufu bakımından PoW ile kıyaslanması durumunda ise enerji tüketiminde daha verimli olan bir hizmet arz ettiği görülmektedir.

2.1.6.3 Bizans Hata Toleransı

Dağıtılmış olan bir bilgisayar ağının arzu edilen bir biçimde fonksiyonunu yerine getirmesi ve öteki düğümlere sistemin kötü niyetli düğümlerinin yanlış bilgi vermesine ya da yaymasına karşı yeterli olacak biçimde sistemde uzlaşmanın sağlanması, Bizans Hata Toleransı (PBFT) olarak ifade edilmektedir. Ağın doğru işlevi ve sistemde bulunan dürüst düğümlerin eriştiği doğru mutabakatta bahsi geçen bu kötü niyetli düğümlerin etkilerinin düşürülerek arızalara karşı sistemin korunması buradaki gaye olarak karşımıza çıkmaktadır.

Bizans hatalarıyla baş edebilmek amacı ile bu algoritmanın bir durum makinesi çoğaltma tekniği sunması söz konusudur. PBFT modelinde yer alan bütün düğümler aslında bir düğümün birincil düğüm ve ötekilerinin ise yedek düğümler şeklinde isimlendirildiği bir sıra ile sıralanır. Sistemde bulunan bütün düğümler birbirleri ile iletişim içerisindedir. Bütün dürüst düğümlerin sistemin çoğunluğunun sistem durumu hakkında bir anlaşmaya ulaşması hedeflenmektedir. Ayrıca mesajların belli bir eş düğümden gelmekte olduğunu düğümler kanıtlamaktadır. Mesajın aktarımı esnasında değiştirilmediğini de düğümlerin doğrulması söz konusudur.

2.2 Blockchain Teknolojisinin Gelişim Süreci

SatoshiNakamoto tarafından 2008 senesinde yazılan makaleyle beraber blockchain teknolojisi meydana gelmiştir. Ancak öncesinde de benzer teknolojilerin uygulandığı ya da uygulanmaya çalışıldığı görülmektedir. Dolayısıyla ilk olarak blockchain teknolojisine gelesiye kadar süren süreç ve araştırmalar ele alınmalıdır. Birtakım birey ve gruplar tarafından 1990'lı senelerde mahremiyet özgürlüğü elektronik ortamda sağlama ve bunu eyleme geçirme manasında ciddi derecede yoğunlaşmalar söz konusudur (Kardeş, 2019). Blockchain teknolojisinin kavramsal temellerinin ise bu dönemlerde kaleme alınan 3 farklı makale ile atıldığı söylenebilmektedir (Usta &Doğantekin, 2017):

- 1991 senesinde Stuart Haber ve W. ScottStornetta tarafından bir makale yazılmıştır. Bu makalede zaman damgasıyla kripto paralarla belgelerin ne şekilde kullanılacağı ele alınmıştır.

- 1996 senesinde RossAnderson tarafından kaleme alınan makalede kayıtları tutulan güncellemelerin silinmesinin mümkün olmadığı merkezi olmayan bir veri depolama sistemi ifade edilmiştir.
- 1998 senesinde Bruce Schneier ve John Kelsey'in hazırladığı makalede ise, şifrelemeden güvenilmemekte olan makinlerde tutulan günlük dosyalarının (logfiles) barındırdığı hassas bilgilerin korunmasında ne şekilde yararlanılacağı belirtilmektedir.

1992 senesinde sistem Stuart Haber ve W. ScottStornetta tarafından geliştirilmiştir. Bu şekilde bir blokta veriler muhafaza edilebilir olmuştur. Ancak daha verimli duruma getirilen sistem kullanılmıştır. 2004 senesine gelindiğinde ise patent bitmiştir. 2004 senesinde bilgisayar bilimcisi olan Harold Thomas Finney tarafından RPoW isimli bir sistem tanınmıştır. Bu sistemde yeniden kullanılabilir iş ispatı bulunmaktadır. Bireyler arasında token aktarımı bu sistem ile sağlanmıştır. Bunun yanı sıra bahsi geçen bu sistem kripto paraların başlangıcı olması bakımından da oldukça önemlidir. 12 Ocak 2009 tarihinde Hal Finney (Harold Thomas Finney),dünyanın ilk Bitcoin işleminde SatoshiNakamoto'dan 10 Bitcoin alması ile ilk Bitcoin alıcısı sıfatına sahiptir.

1999 senesinde nobel ödüllü ekonomist MiltonFriedmantarafından bir açıklama yapılmıştır. Bu açıklamada; "Güvenilir bir e-nakit eksik olan tek şeydir. Bu şekilde internette, B'yi, B de A'yı bilmeden A'dan B'ye transfer yapılması mümkün hale gelmektedir. Hükümetlerin rollerinin düşürülmesinde bu durum önemli bir güçtür" şeklinde ifadelere yer verilmiştir. Blockchain teknolojisinde olduğu benzeri Friedman'ın bahsi geçen bu ifadesi merkezi otoriteden bağımsız olan bir veri transfer sisteminden söz ettiği karşımıza çıkmaktadır.

2.2.1 Şifre Punk (Cypherpunk) Hareketi

İnternetin gelişimi ve kriptoloji üzerine tartışmaların gerçekleştirildiği bir elektronik posta grubu 1992 senesinde meydana getirilmiştir. Bu grup kriptolog ve bilgisayar mühendislerinden oluşmaktadır. Aynı zamanda Hal Finney,EricHughes, JulianAssange, David Chaum,NickSzabo ve Timothy May bu grubun kurucuları arasında bulunmaktadır. ŞifrepunkManifestosu"nu 1993 senesinde bu grubun yayınlaması

sonucunda pek çok destekçi kazanmıştır. Ayrıca grup kişiler arasında var olan etkileşimin yine kişilerce idare edilmesinin gerekli olduğunu iddia etmektedir. 1992 senesinde Şifrepunk hareketinin kurucularından olan Timothy C. May, tarafından Kripto Anarşist Manifestosunda yayımlanmıştır. Burada "Dünyada bir hayalet dolaşıyor, kripto anarşi hayaleti" ifadesi ile makalesine başladığı görülmektedir.

May de şifrepunk grubunun öteki üyeleri benzeri dünyanın önde gelen alanlarında çalışmalar gerçekleştirmiştir. Aynı zamanda gelecek dönemde teknolojinin beraberinde neleri doğuracağı konusunda tahminler yürüterek araştırmalar yapmıştır. May 2 bireyin anonim biçimde veri alışverişi gerçekleştirilebileceğinin üzerinde yoğunlaşmıştır. Ayrıca hükümetlerin düzenlemelerinin yapısının, iktisadi işlemleri idare etme ve bilgiyi gizleme biçiminin meydana gelecek gelişmeler sonucunda bütünü ile değişeceği yönünde tahminlerde bulunmuştur. Bunun yanı sıra itibarın doğasında değişmeler yaşanacağı hakkındaki söylemlerde Kripto Anarşist Manifestoda üzerinde durulan en önemli durumlardan biri olarak karşımıza çıkmaktadır. İtibar May tarafından, bugünün kredi puanlarından ziyade müzakerelerde en mühim unsurlardan biri olacağı öne sürülmektedir. Bu çerçevede olacağını belirttiği devrimin ise, ekonomik ve sosyal bir devrim olacağı üzerinde durmuştur.

Devletlerin, May tarafından kripto anarşi şeklinde isimlendirilen teknolojilere engel olacağı ileri sürülmektedir. Hem uyuşturucu satıcıları ve vergi kaçakçılarının teknolojiden yararlanması hem de toplumsal parçalanma benzeri ulusal güvenlik endişeleri ne teknolojinin yol açacağı devletler tarafından belirtilmektedir. Dolayısıyla devletler, teknolojinin gelişimini bu gerekçeler doğrultusunda yavaşlatmaya hatta durdurmaya uğraşmaktadır. May tarafından bu endişenin doğru olduğu ifade edilmektedir. Aynı zamanda ulusal sırların, çalıntı ve yasadışı ürünlerin ticaretini kripto anarşinin mümkün hale getireceği belirtilmektedir. Fakat kripto anarşinin yayılmasında bu hususların hiçbirinin engelleyemeyeceği üzerinde durulmaktadır.

May tarafından Kripto Anarşist Manifestonun Orta Çağ'ın toplumsal ve iktidar yapısını matbaanın etkilemesi benzeri kurumların ve ekonomik bulunan devlet müdahalesi yapısında gelecek teknolojilerin radikal değişikliklere neden olacağı ifade edilmektedir. May, son olarak bilginin özgürleşmesi üzerinde durmuştur. Bu çerçevede

adeta dikenli tel benzeri önemsiz olarak algılanan bir icadın ABD batı sınırında yer alan büyük çiftliklerde bulunan çitlerin kalmasına imkân tanıması, bu sebeple de buradaki mülkiyet ve mera hakkı olgularının tamamen değiştirmesini örnek göstermektedir. Bu durum benzeri matematiğin sır dolu bir dalının geliştirmiş olduğu bu önemsiz olarak algılanan keşif de fikri mülkiyetin etrafında yer alan dikenli telleri söken bir tel makası görevi göreceğini ileri sürmektedir (May, 1992). Manifestoyu ise "Kalk, dikenli telli çitlerinden başka kaybedecek bir şeyin yok!" sözleriyle Marx'ın Komünist Manifesto'sunda bulunan ifadelerine benzer şekilde "Kalk, dikenli telli çitlerinden başka kaybedecek bir şeyin yok!" sözleri ile manifestoyu bitirdiği görülmektedir.

Kitlesel gözetleme vasıtası ile global firmalar ve istihbarat kuruluşlarının (muktedirlerin) temel özgürlüklere karşı gerçekleştirdikleri saldırılara güçlü şifreleme metotlarıyla karşılık veren, siyasi ve toplumsal değişim aracı olarak şifreyazımına (kriptografi) dikkat çeken barışçı eylemciler şeklinde Şifrepunklartarafından kendilerini ifade ettikleri söylenebilmektedir (Güven & Şahinöz, 2018).

Şifrepunklar tarafından kendilerinin anonim sistemin inşa edilmesine adanmış oldukları ifade edilmektedir. Ayrıca anonim posta sistemleri, elektronik para, şifreleme ve dijital imzalarla mahremiyetlerini savunduklarını belirtmektedirler (Hughes, 1993).

1993 senesinde EricHughes, Şifrepunk Manifestosunu yayınlamıştır. Burada mahremiyet olgusuna yoğunlaşmıştır. Bu çerçevede kişisel bilgilerde var olan mahremiyetin sağlanması ile açık bir toplumun sağlanmasının mümkün olacağını belirtmiştir. Anonim kalmak ise mahremiyetin sağlanmasında gerekli olmaktadır. Taraflar arasında yapılan işlemde sadece o işlemin yapılacağı kadar bilginin paylaşılması, burada bahsi geçen anonimlik ile anlatılmak istenen durumdur. Dijital ortamda gerçekleştirilen alışverişlerde, fiziksel ortamda nakit ile gerçekleştirilen bir alışverişte kimlik bilgilerinin verilmesinin gerekli olmadığı benzeri bireyin kimlik bilgilerinin hepsine ulaşılmasının gerekli olmadığını belirtmektedir. Burada gizlilikle anonim kalmak arasında bulunan fark karşımıza çıkmaktadır. Gizlilikten ziyade anonim kalma mahremiyeti belirtmektedir. Şifrepunk grubun savunduğu üzere kriptografiden yararlanılarak anonim kalarak ve güvenli biçimde veri transferinin gerçekleştirilebilmesi mümkün olmaktadır.

2.2.2 DigiCash

1990 senesinde Amerikalı kriptograf ve bilgisayar bilimcisi David Chaum, Digicash'ı kurmuştur. Digicash kullanıcıların kimlik bilgilerinin gizli bulunduğu bir elektronik ödeme sistemi firması olarak karşımıza çıkmaktadır. Bu mananda Bitcoin ve blockchainden önce ilk ciddi girişim olmasından dolayı önem arz etmektedir.

Ecashadlı kripto para digicash firması tarafından çıkartılmıştır. Web üzerinde gerçekleştirilmiş olan alışverişlerde bu kripto para, kullanıcıların ödemeleri daha basit ve güvenilir kılan alternatif bir sistem olmaktadır. Kredi kartı ile gerçekleştirilen masrafların yüksekliğine karşı çıkmış olduğu dönemde Ecash'de masraflar oldukça azdır. Aynı zamanda nakit alışverişi yapma benzeri kullanıcına gizlilik sağlaması da söz konusudur (Konukseven& Özen, 2018). Bunun yanı sıra Bitcoin ve blockchain teknolojisinden farklı şekilde Ecash, merkezi bir yapıya bağlı olmaktadır.

Digicash, Deutsche Bank ve CreditSuissebenzeri bankalarla anlaşmaya sahiptir. Ancak 1998 senesinde iflas başvurusu yapmıştır. Alternatif ve yenilikçi bir ödeme sistemi olmasına karşın firmanın batmasının nedenlerinden biri olarak David Chaum'un kişiliği ileri sürülmüştür.

Chaum tarafından anonimlik ve dijital kimlik hakkında önemli çalışmalar yürütülmüştür. "İyi geliştirilmiş olan bir dijital para sistemiyle kötü bir elektronik para sistemi arasında bulunan fark, gerçek bir demokrasiye mi yoksa diktatörlüğe mi sahip olacağımızı belirleyecektir" ifadeleri 1996 senesinde vermiş olduğu bir röportajda aktarmıştır. NickSzabo bir yıl kadar Digicash'te faaliyet göstermiştir. Bu doğrultuda gelecek dönemde Bitgold görüşünü ortaya atacağı düşünüldüğünde Bitcoin görüşünün peşinde koşanların bir avuç kişi olduğunu belirten örneklerden biri olarak karşımıza çıkmaktadır (Konukseven& Özen, 2018).

2.2.3 Bitgold

Bitgold isimli elektronik para sistemini 1998 senesinde bilgisayar bilimcisi olan NickSzabo tarafından geliştirilmiştir. Bu sistem yılında Bitcoin'e en yakın sistem olarak değerlendirilmektedir. Ayrıca bu sistemde blockchain teknolojisi benzeri merkezi

olmayan bir sistem sunulması söz konusudur. Fakat Bitgold öteki sistemlerin aksine hiçbir zaman kullanılmamıştır. Tüm bu durumlar NickSzabo'nun esasında Satoshi Nakamoto olabileceği hakkında söylentilerin meydana gelmesine yol açmıştır.

2005 NickSzabo tarafından bir makale yayınlanmıştır. Var olan para hakkındaki problemin, değerinin üçüncü bir tarafa karşı bulunan güvene bağlı bulunmasından dolayı ortaya çıktığı bu makalede ifade edilmiştir (Szabo, 2005). Değer transferi için değerli metallerden yararlanılması durumunda ise bu sorunun bağımsız olması söz konusudur. Fakat bahsi geçen bu metallerin işlenmesi ve kullanımı ciddi bir maliyeti doğurmaktadır. Söz konusu bu değerli metaller standart bir miktarda belirlenerek karşılığında madeni para şeklinde kullanılması amacı ile sürece güvenilir bir üçüncü taraf katılmaktadır. Dijital ortamda bu üretilen paralardan yararlanılması mümkün değildir. Burada Szabo tarafından Bitgold tavsiye edilmektedir. Maliyetleri yüksek olan bitlerin güvenilir üçüncü taraflara minimum bağımlılık ile çevrim içi şekilde oluşturabileceği ardından benzer biçimde minimum güvenle güvenci biçimde muhafaza edilip, test edilen ve aktarılan bir protokol olarak Bitgold ifade edilmektedir (Szabo, 2005).

Aşağıda Bitgold'un çalışma sistemine yer verilmiştir (Szabo, Bit Gold, 2019):

1. Genel bir bit dizesi, "meydan okuma dizisi" meydana getirilmektedir (bkz. 5. adım).
2. Alice, güvenli karşılaştırma işlevinden bilgisayarında yararlanarak çalışma dizgisinin zorlu bitlerinden iş kanıtını meydana getirmektedir.
3. İşin kanıtının güvenli biçimde zaman damgalı olması söz konusudur. Bazı farklı zaman damgası hizmeti ile çalışması, belli bir zaman damgasının hizmetine ciddi derece güvenilmesinde gerekli olmaktadır.
4. Çalışma dizesi ve meydana okuma dizesinin Alice zaman damgası kanıtını dağıtık mülk kayıt defterine eklemektedir. Bunu Bitgold için yapmaktadır. Bu noktada düzgün biçimde kayıt defterinin çalıştırılmasında tek bir sunucuya güven duyulmamaktadır.
5. Son meydana getirilen bitgold dizisinin bir sonra meydana getirilmiş olan dizgi ile alakalı bitleri sağlaması söz konusudur.

6. Bob, bit gold başlık kaydında bulunan başlık zinciri kontrol edilmektedir. Buradaki amaç Alice'in belirli bir bit gold dizisinin bulunduğunun kanıtlanmasıdır.
7. Bob bir bit gold dizisinin değerinin test etmek amacı ile zaman damgasını, zorluk bitlerini ve çalışma ispatının dizesini kontrol etmektedir. Ayrıca bunları doğrulmaktadır.

Szabo tarafından bugüne dek yararlanılan para şekilleri güvensiz olarak nitelendirilmiştir. Gerekçe olarak ise hırsızlıktan sahteciliğe dek uzanan etkenlerinin yanı sıra en kötüsünü enflasyon olarak belirtmiştir. Enflasyon ve öteki güven zedeleyici tehlikelerin giderilmesi için bu manada Bitgold'ların etkili olacağı ileri sürülmektedir.

2.2.4 Satoshi Nakamoto ve Bitcoin: Eşler Arası Elektronik Nakit Sistemi

2008 senesinde global bir kriz meydana gelmiştir. Mortgage Krizi olarak da adlandırılan bu kriz ile pek çok finans kuruluşu, çok uluslu firmalar ve büyük bankalar iflas ettiklerini açıklamışlardır. Kişiler tarafından, merkezi kurumlarda meydana gelen bu durumdan dolayı oluşan güvensizlik ortamında başta bankalar olmak üzere pek çok kuruma karşı tepki ile yaklaşıldığı görülmektedir.

LehmanBrothers tarafından 2008 yılı ekim ayında iflası açıklanmıştır. Bu iflastan sonra Şifrepunk grubunun üyelerinden biri olan SatoshiNakamoto tarafından öteki üyelerin yer aldığı e-posta grubuna 1 Kasım 2008 tarihinde, "Bitcoin: Eşler Arası Elektronik Nakit Sistemi" (Bitcoin: A Peer-to-Peer Electronic Cash System) adlı makalesi atılmıştır. Blockchain altyapısıyla Bitcoin adlı kripto paranın ne şekilde çalıştığı hakkındaki teknik detaylara bu makalede yer verilmiştir. O zamana dek gerçekleştirilen çalışmalar sonucunda meydana getirilen blockchain sisteminde de aynı bu mesaj bulunmaktaydı. Bu mesaj ise, güvenilir üçüncü taraf yani aracı gereksiniminin bulunmadığı bir sistemle merkezi yapı olmadan değer transferinin gerçekleştirilebilmesidir.

SatoshiNakamotoJapon asıllı ve 5 Nisan 1975 tarihinde doğan bir erkek olarak bilinmektedir. Ancak gerçek bir kimlik olup olmadığı konusunda kesin bir bilgi bulunmamaktadır. Bu hesap üzerinden 2009 senesinden sonra bir işlem

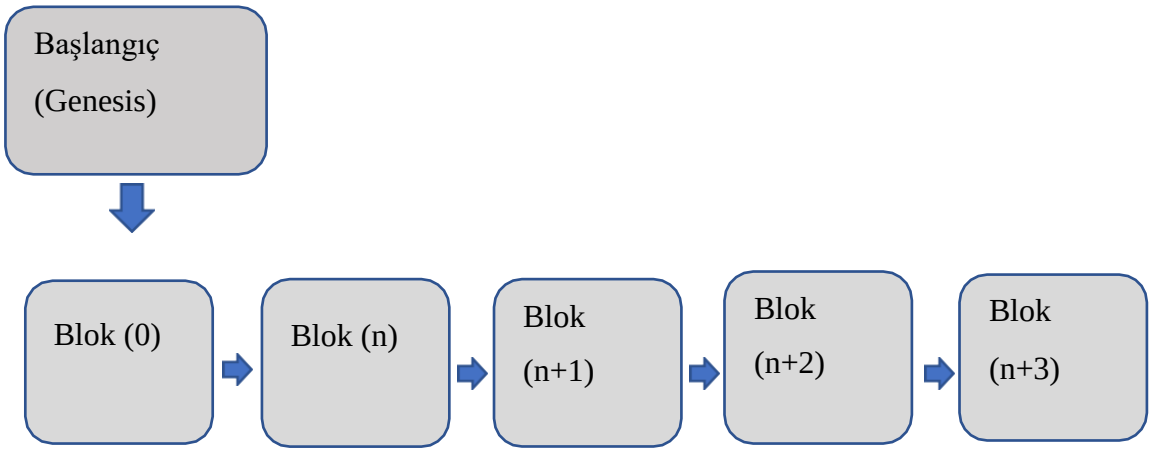
gerçekleştirilmemiştir. Ayrıca bu kimlikte kimsenin de ortaya çıkmaması durumunda bu adın takma bir ad olduğu konusunda düşünceler doğmuştur. Ayrıca SatoshiNakamoto adının tek bir kişiden ziyade bir grubu temsil ettiği hakkında da iddialar bulunmaktadır. NickSzabo'nun esasında SatoshiNakamoto olduğu ileri sürülmektedir. Nedeni olarak ise daha öncesinde gerçekleştirdiği çalışmalar ve yine aynı elektronik posta grubunda yer alması gösterilmektedir. Fakat bu durum kendisi tarafından pek çok kez inkâr edilmiştir.

Dijital ortamda gerçekleştirilen alışverişlerde taraflar arasında bir güvenin sağlanması amacı ile üçüncü bir taraf olarak aracı kurum gereksiniminin bulunduğu dokuz sayfadan meydana gelen makalenin giriş kısmındaifade edilmiştir. Sundukları hizmet karşılığında bu güvenirliği sağlayan üçüncü tarafların aracılık maliyeti alması söz konusudur. Fakat bu durum zamanla aracılıktan dolayı maliyetleri yükseltmektedir. Ayrıca alınan kullanıcı bilgilerin doğru kullanılmamasına ya da gereğinden çok bilgi alınmasına yol açmaktadır.

Blockchain tabanlı sistemde Nakamoto tarafından Bitcoin ismi verilen ödeme şekli ile, güvenden ziyade şifreleme kanıtı üzerine kurulu olan, 2 tarafından birbirleriyle direkt bağlantıda bulunduğu elektronik ödeme sistemi tavsiye edilmektedir (Nakamoto, 2008). Bu sistem merkezi bir yapısı bulunmayan eşler arası (Peer to Peer) internet ağından yararlanmaktadır. Aynı zamana banka benzeri finansal bir kuruluşun aracılık yapmasına gerek kalmadan para transferini yapması ve pek çok alanda yeni bir modellerini meydana getirmesinden dolayı devrim niteliğinde bir gelişme olarak nitelendirilmektedir (Yıldırım, 2019).

2.3 Blockchain Çalışma Prensibi

Blok zincir yaklaşımında isminden de anlaşılacağı üzere verilerin muhafaza edildiği yapılar blok olarak tanımlanmaktadır. Bahsi geçen bu blok yapıların bir zincir biçimde (zaman bakımından doğrusal bir dizi yapısında) düzenlenmesi söz konusudur. Genesis (başlangıç) blok, bu zincir dahilinde bulunan ilk blok yapısına verilen isimdir.



Şekil 2.3 Blok Zincirleri (https://bctr.org/blockchain-nedir/ esinlenerek çizilmiştir, 01.03.2021)

Blok başlığı içerisinde yer alan bilgilerin bir güvenli özetleme algoritmasından toplu bir biçimde geçirilmesiyle ise o bloğa ait özetleme bilgisine (blockhash) erişilmektedir.

1 MB uzunluğuna sahip olan bloklarda her birinde minimum 1 işlem tutulması söz konusudur. Ayrıca blok hakkında veriyi tutan üst bilgi 80 Byteboyuta sahiptir. 350- 500 arasında bir blokta işlem verisi tutulmaktadır. Bunun yanı sıra minimum 250 Byte boyutunda bir transfer işlemi yapılmaktadır (Çarkacıoğlu, 2016:43).

Madencilik ise, blockchainine yeni blokların ilave edilmesidir. Madenci, madencilik işlemi için bir uğraş veren her bir üyenin adıdır. Blockchainin kaydedilmesi ve transfer işlemlerinin yapılmasında madenciler zorunlu uygulayıcılar olarak karşımıza çıkmaktadır. Başlangıçtaki blok meydana getirme ödülü Bitcoin'de 50 bitcoindir. Ödülün her 210.000 blokta yarılanması söz konusudur. Ortalama dört senelik bir zamanı belirten bu yarılanmanın hesaplanması durumunda 2140 senedine dek süreceği tahmin edilmektedir (Antonopoulos, 2014:2).

Ağda bulunan bütün taraflar vasıtası ile transfer işlemlerinin hepsi takip edilebilmektedir. Madencilerin onaylamış olduğu işlemlerin toplanması ile bloklar meydana gelmektedir.

Bütün bloklar kendisinden önce gelen blok hakkında özet bilgiyi barındırmaktadır. Var olan blok tarafından kendi özet verisinin meydana getirilmesiyle, bu hazırlanan özet bilgiden daha sonra gelecek olan blok için yararlanılmaktadır.

Bu yapıya şayet bir saldırganın müdahalede bulunmak istemesi durumunda ise, blockchain ağı içerisinde hedeflediği bloğun içeriğinde değişiklikler yapabilmesi için bazı durumlar gereklidir. Bunlar; hedef bloğu ve bu bloğu izleyen öteki bütün blokların değiştirilmesidir (Wang, 2018: 96). Bu senaryo devamlılık gösteren bir blok üretimi ya da kötü niyetleri birisinin değişim esnasında blockchaine yeni bloklar eklemesi ve blok üretim algoritmasının mantığı doğrultusunda mümkündür. Ancak pratik bakımından normal şartlarda saldırı gerçekleştirilememektedir.

Tarafların kim olduğunun bilinmesi bir transfer işleminin yapılmasında gereklidir. Fakat tarafların kişisel bilgilerinin verilmesi zorunlu değildir. Çünkü gizlilik korunmaya çalışılmaktadır. Tarafları adresleyebilmek amacı ile elektronik hesap cüzdanlarından yararlanılmaktadır. Esasında gizli ve açık anahtarı bulunan adres verisinden cüzdan meydana gelmektedir. SHA-256 özetleme algoritması ve açık anahtardan yararlanılması ile cüzdan adresi hazırlanmaktadır. Base58 kodlama sistemini adresler kullanmaktadır. Örneğin bir cüzdan adresi "1ELiFNCg6v1wnc6cxTrY4m1MNDC5e5Vb1B" biçimdedir. Bu adresin gizli anahtarına ise "5JNbVn7tXtkAp5rYagA9ZPaGDBCRueqycsyxTugpW" biçimde örnek verilebilmektedir. Bu cüzdan hakkında gizli anahtarı sadece cüzdanın sahibi bilmektedir. Ayrıca bu noktada bir hak sahipliği ve yasal ilişkilendirme bulunmamaktadır. Dolayısıyla en mühim durumlardan biri anahtarın gizliliğinin koruma altına alınmasıdır. İşlemlerin gizli anahtardan yararlanılarak imzalanması, bir elektronik cüzdan üzerinden harcama gerçekleştirilmesinde gerekli olmaktadır. Dolayısıyla bu verinin gizliliği sağlanmalıdır. Yalnızca adres hakkında bilgi sahibi olunması bir cüzdana gönderim işlemin gerçekleştirilmesinde yeterlidir (Kırbaş, 2018: 79).

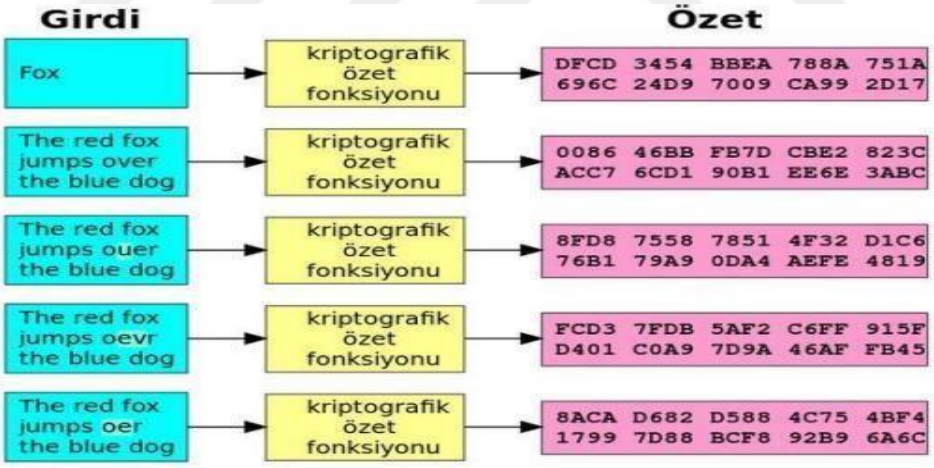
2.3.1 HASH Fonksiyonları

Bir girdi şeklinde rastgele uzunlukta olan verileri almış olan ve karma değeri ismi verilen sabit uzunluğa sahip bir bit dizgisi oluşturan algoritma, bir karma işlevi olarak karşımıza çıkmaktadır.

Hash fonksiyonu, verilerin bütünlüğü kontrol etmek maksadıyla yararlanılan ve ait olduğu verinin birinci sektöründen en son sektörüne olan tüm bitlerin özel bir algoritmik işleme maruz kalması neticesinde eşi benzeri olmayan sabit bir değer meydana getiren matematiksel fonksiyonlardır. Bu yönüyle benzer eşi benzeri olmaması nedeniyle özgün olmakta ve benzerleri üretilememektedir. Hash fonksiyonlarının sahip olduğu özellikler şu şekilde sıralanabilecektir (Okuyucu, 2020):

- Hash fonksiyonların yalnızca tek yönlü olmaktadır. Özetlenmiş verilerden asıl verilerin elde edilmesi mümkün değildir.
- Hash fonksiyonlarında anahtar kullanımı söz konusu değildir.
- Hash fonksiyonları dahilinde asimetrik veya simetrik gibi birkategorizasyon yapmak mümkün değildir.
- Blok uzunlukları ne ölçüde fazla olursa, bütünlüğün o düzeyde güvenli olması söz konusu olacaktır.

Genel itibariyle hash değerlerinin hesaplanması şu şekilde gösterilebilecektir.



Şekil 2.4 Genel İtibariyle Hash Değerinin Hesaplanma Biçimi

Kaynak: Okuyucu, H.H. (2020). Hash Fonksiyonlarının Adli Bilişimde Uygulamaları ve C++ İle Şifreleme Algoritması Tasarımı, Yüksek Lisans Tezi, Karabük Üniversitesi, Elektrik ve Elektronik Mühendisliği Bölümü.

Görüldüğü gibi Hash fonksiyonları ana verideki ufak bir değişikliği bile tamamen eşsiz bir biçimde özetlemektedir. Bu durum hash fonksiyonlarının eşsiz veriler ortaya

koymasına neden olmaktadır. Bu doğrultuda bu fonksiyonların farklı alanlarda kullanıldığı görülmektedir. Bu alanlar şu şekilde ifade edilebilir (Cihat, 2012):

- Dosya bütünlüğü,
- Dijital imza,
- Kimlik Doğrulama Protokolleri,
- Şifre Koruması,
- Rootkit Tespiti

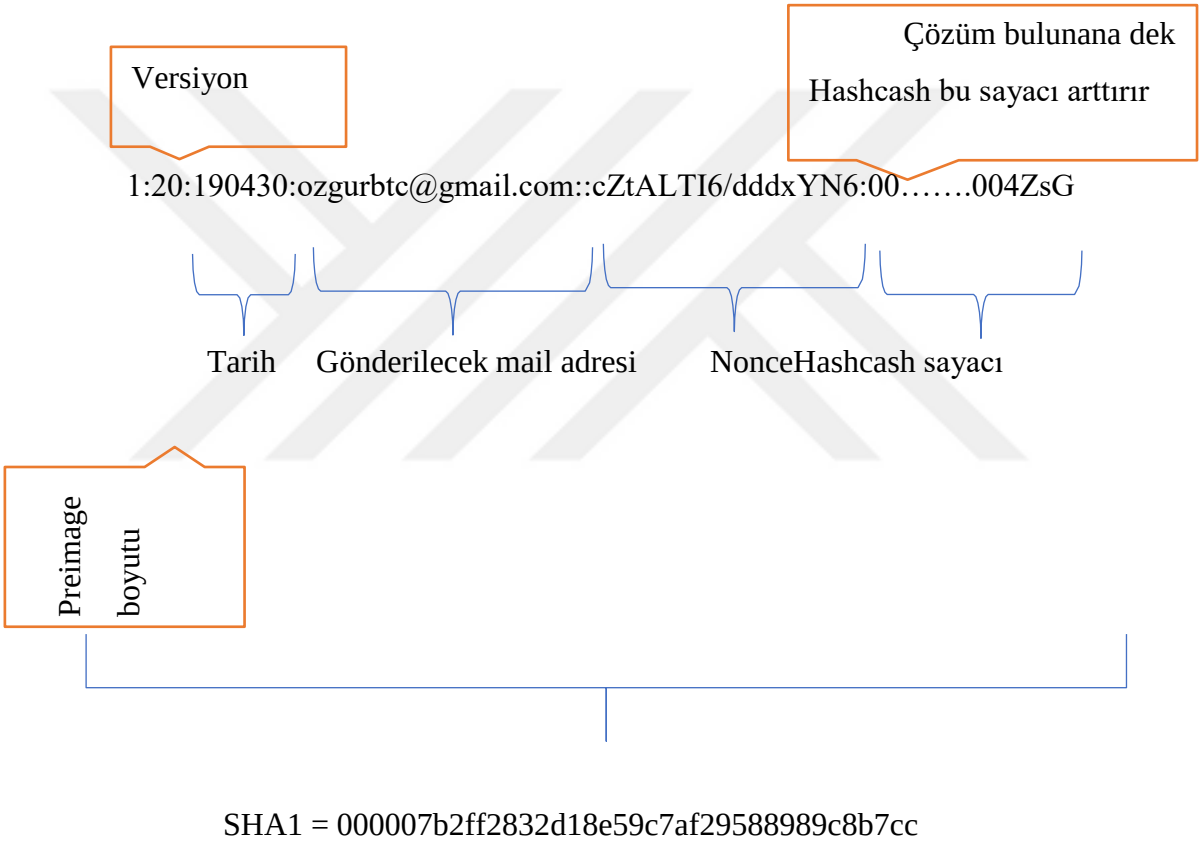
Aynı giriş verileri için karma değerin daima aynı olması söz konusudur. Hesaplamalarda karma fonksiyonlar kullanılmaktadır. Karma tablolardan yararlanarak hızlı biçimde veril kayıtlarında bu fonksiyonların kullanılması bu duruma örnek olarak gösterilebilmektedir. Çoğunlukla olası giriş verilerinin boyutlarına kıyasla karma değerlerin boyutları daha azdır. Dolayısıyla pek çok girdi veri noktasının tek bir hash değerini paylaşması söz konusudur. İyi bir karma fonksiyonunda karma değerlere, giriş değerlerinin orantısal olarak dağıtılması gerekmektedir. Bu şekilde aynı sayıda olası giriş değerine bütün karma değerler bağlanması gereklidir. Mümkün olduğu derecede karma değerinin rastgele davranmasının sağlanması ile bu orantılılık sağlanabilmektedir. Ancak rastgele olduğu gibi karma değerin davranmasına karşın halen bir belirleyici olduğu göz önünde bulundurulmalıdır. Aynı zamanda bir girdinin verilmesi durumundan daima onun karma değerinin aynı olması söz konusudur. Çalışma kanıtı (Proof of Work) gerçekleştirmek amacı ile Bitcoin şifreleme karma işlevlerinden yararlanmaktadır. Hash işlevleri doğrultusunda güvenli karma işlevleri şeklinde de isimlendirilen kriptografik karma işlevleri ek ihtiyaçlar yaratmaktadır (Franco, 2015: 96):

Tek yönlü (Önleme) direnci: Giriş verilerini saptamak karma değer dikkate alındığında hesaplama bakımından uygun değildir. İş kanıtının uygulanmaya konulması bakımından bu önem arz eden bir özellik olarak karşımıza çıkmaktadır.

Zayıf çarpışma direnci: Aynı karma değeri bulunan bir başka girdinin bulunması bir girdi verilmesi durumunda hesaplama bakımından olanaksızdır.

Güçlü çarpışma direnci: Sayısal açıdan aynı karma değeri ile neticelenen 2 girdi veri noktasını saptamak imkânsızdır.

SHA256 ^ 2'den Bitcoin, işim ispat fonksiyonu şeklinde yararlanmaktadır. SHA256 hashing fonksiyonunun 2 defa uygulanması SHA256 ^ 2 olarak karşımıza çıkmaktadır. NSA (Ulusal Güvenlik Dairesi, National Security Agency) tarafından tasarlanmış olan ve 2001 senesinde NIST (Ulusal Standartlar ve Teknoloji Enstitüsü, NationalInstitute of StandardsandTechnology) tarafından yayınlanmış olan karma fonksiyon kümesinin (SHA-2) bir parçası olarak SHA2561 değerlendirilmektedir. 256 bit uzunluğunda bulunan bu ailenin karma fonksiyonu olarak SHA256 karşımıza çıkmaktadır (Franco, 2015: 96).



Şekil 2.5 Hashcash Başlığının Bir Örneği (Franco, 2015: 104 esinlenerek çizilmiştir)

Resmi kurumdan gelmiş olan lastik damga ya da bir mektupta olan posta damgası benzerifiziksel bir zaman dalgası ile benzerlik gösteren dijital zaman damgası; dijital bir belgenin belli bir zamanda bulunduğunu kanıtlamaktadır. Aynı zamanda bir dijital para birimde bulunan işlemlerin yapıldığını, 2 taraf arasında bir sözleşme yapıldığını ya da bir internet sitesinde işlem yapıldığını belgelemek benzeri uygulamaları bulunmaktadır. Çoğunlukla güvenliğin sağlanması bakımından gerekli olan verileri dijital zaman

dalgasında yer alan bilgiler vermektedir. Bir karmadan yararlanma farklı avantajları sunmaktadır. Zaman damgasını korumak amacı ile zaman damgası bulunacak bilgilerin kullanılan ortamdan ayrı ve özel tutulması bu avantajlarından birincisidir. Çoğunlukla karma onu meydana getiren bilgilere kıyasla ciddi derecede saha küçüktür. Bu durumun da depolama maliyetini azaltması ikinci avantajı olarak karşımıza çıkmaktadır. Son sağladığı avantaj ise, çoğunlukla dijital imzaların daha önceden saptanan bir boyutta bulunan veriler üzerinde en iyi biçimde çalışmasıdır (Franco, 2015: 99).

Hashcash bir çalışma kanıtı (PoW) sistemi olarak karşımıza çıkmaktadır. Aynı zamanda bitcoinde madencilik algoritmasının bir parçası olarak yararlanılmaktadır. Aşağıda hashcash'ın içerdiklerine yer verilmiştir (Franco, 2015: 104):

- Hashcash protokolünün sürümü,
- 1. Preimage boyutu, 20 bit ya da 5 ilk sıfır karakteri içermektedir. Başlangıç kısmi karma inversiyon için sıfır bitlerin sayısını belirtmektedir.
- 190430 ya da 30 Nisan 2019 şeklinde elektronik postanın gönderim tarihi belirtilmektedir. Sadece belli zamanda hash jetonunun geçerli olması söz konusudur.
- Örnekte ozgurbtc@gmail.com şeklinde alıcı e-posta adresinden yararlanılmıştır.
- Sadece bir e-posta için kullanılan bir nonce2
- Örnekte cZtALTI6/dddxYN6 şeklinde yalnızca bir elektronik posta için kullanılan bir nonce2'dir. Buradaki gaye ise, pek çok elektronik postanın gönderilmesinde yararlanılan hashcash başlığına engel olmaktır. Bir önbellekte alıcı e-posta sunucusunun verileri muhafaza etmesi mümkündür. Bu aynı hashcash başlığını birden çok elektronik postada bir botnet3 ustasının tekrardan kullanmasının önüne geçmektedir.
- Örnekte sayaç 00… 004ZsG şeklindedir. Bu sayacı hashcash'in bütün başlığın karmasının ön şart ihtiyacı ile eşleşebileceği bir değere kadar yükseltmesi söz konusudur.

2.3.2 Eşler Arası Değer Değişim Sistemi

Yeni iletişim şeklinde uyum gösteren bir ödeme sistemine olan sınırsız, hızlı ve güvenilir paraya olan gereksinimi bitcoin gidermiştir (Antonopoulos 2014:1). Aynı zamanda tam anlamıyla uygulanabilir olan bir dijital paranın (ya da tahvil, hisse senedi ya da lisanlar benzeri bir dijital varlığın) meydana gelmesinde çifte harcama ve orijinallik onayı olmak üzere 2 ana teknik problem çıkmaktadır.

Dijital para ya da öteki dijital varlıkların fiziksel varlıklardan tek farkı, bir bilgisayar (bit dizisi) biçiminde olmasıdır. Öteki bütün dijital dosyalarda olduğu gibi bunlarında kopyalanması mümkündür. Nakit ya da menkul kıymetler hesap bakiyesi benzeri hesap sahibinin bakiyesinin defteri tutacak bir aracının bulunmaması durumunda biri koyasını saklarken biri kartı gönderebilmektedir. Bu durum çift harcama sorunu şeklinde nitelendirilmektedir. Harcamalarda merkezi bir deftere karşı çevrimiçi şekilde kontrolünün sağlanması ile bu duruma engel olunabilmektedir (Chaum, 1992: 98). Dolayısıyla dijital varlığın bütün işlemlerinin yetkili bir kaydına gereksinim ortaya çıkmaktadır.

Katılımcılar tarafından depolama kapasitesi ya da işlem gücü benzeri kendi donanım kaynaklarının bir bölümünün paylaşılmakta olduğu, eşler arasında dağıtılmış bir ağ mimarisi olarak Schollmeier (2001)'in bir ağ tanımladığı görülmektedir. Ağın arz ettiği içerik ve hizmetin sağlanmasında bahsi geçen bu paylaşılan kaynaklar gerekli olmaktadır. İş birliği bakımından yararlanılan alanları paylaşmak ve depolamak bu duruma örnek olarak gösterilebilmektedir. Aynı zamanda öteki meslektaşların aracı kuruluşlar bulunmadan direkt şekilde ulaşabilmeleri mümkündür.

Çifte harcama ve orijinallik onayı problemlerini ortadan kaldırabilmek için Nakamoto bir çözüm önerisi sunmuştur. Bu çözüm ise; özel ya da açık anahtar şifreleme metotları ile belli fikir birliği mekanizmalarıyla beraber devamlı biçimde güncellenmekte olan ve kamuya açık olan bir muhasebe sisteminin bulunması doğrultusundadır.

Dijital paranın Hofmann (2018) tarafından da ifade edildiği gibi genel bir kabul görmeden önce hem korunması hem de halkın güvenini elde etmesi gerekmektedir. Dolayısıyla her şekilde sahteciliğin önüne geçilmelidir. Dijital paralar sadece değeri

belirtmektedir. Bu sebeple depolamada ya da makbuzda dijital para birimi işlemlerinin transit geçiş esnasında kurcalama yapılmasına engel olacak biçimde gerçekleştirilmesi gerekli olmaktadır. Bitcoin işlemlerinde var olan bankacılık sisteminin aksine ağın pek çok katılımcısının kaydını tutması, muhafaza etmesi ve yayınlaması bu duruma örnek olarak gösterilebilmektedir. Bir merkezi sunucudan ziyade mutabakat ya da herhangi bir manuel müdahale bulunmamaktadır. Dolayısıyla dakikalar içerisinde işlemlerin arka planda değerlenmesi mümkün hale gelmektedir (Hofmann, 2018: 36).

Zincir şeklinde adlandırılmasına karşın blok zincir aslında yalnızca bir zincir olmamaktadır. Ağda bütün blok zincirlerin kendi veri blokları bulunmaktadır. Düğüm bu veri bloklarına verilen isimdir. Birtakım ara bağlantı metotları vasıtası ile bütün düğümler direkt veya dolaylı biçimde bağlanır. Düğümlerini kenarlarından birbirlerine bağlayan ana yapılara olarak blockchainler de çeşitli türde ağlar vardır. Üç tipik topolojiden blockchainde yararlanılmaktadır. Bunlar dağıtık topoloji, merkezi topoloji ve merkezi olmayan topoloji olarak karşımıza çıkmaktadır. Düğümlerin organizasyonun sağlanması için temel olarak topolojilerin blockchainlere destekte bulunması söz konusudur (He, 2018: 142).

Bloklar halinde bütün işlemlerin mimarı şeklinde dağıtılan eşler arası bir ağın kayıt ettiği, paylaşılan bir veri tabanı bulunan blockchain olarak meydana getirilen bu yetkili kayıt karşımıza çıkmaktadır. Belli bir dönemde verinin bulunmasının gerekli olduğu zaman damgası sunucusuyla ispatlanmaktadır. Ayrıca kronolojik bir düzenin işlem bloklarına verilmesi amacı ile bütün işlemlerin zamanda damgalı olduğu manasını taşımaktadır. Yeni bir blok bütün işlemleri pekiştirmektedir. Bu şekilde öncekine kriptografik şekilde zincirlenir. Aynı zamanda bütün işlemlerin geçmişi paralarının sahiplerini tanımlaması söz konusudur. Kopyalanması mümkün olmayan fiili benzersiz varlıkları da (dijital belirteçler) meydana getirmektedir (Hofmann, 2018: 37). Bitcoin benzeri kripto paralarda ise aynı paranın ikinci defa yeniden harcanması ya da işlemin iptal edilmesinin istenmesi halinde, teorik olarak işlemin kayıt altına alındığı dijital blok zincirinin kötü niyetli bir katılımcı tarafından yeniden yapılması mümkün değildir (Nakamoto, 2008: 2).

W. Difé ve M. Hellman 1976 senesinde işleyişte bu müdahalenin engellenmesi için tavsiye edilen ve blockchain tasarımınaNakamoto'nun entegre etmiş olduğu bir konsept olan dijital imzalara erişilmiştir. İşlemi yani mesajı dijital imza, şifreli şekilde imzalanmış olan bir belge halinde getirmektedir. Bu şekilde okuyan herkes göndericinin kim olduğu hakkında kesin bilgi sağlamaktadır. İmzalar, mesajları imzalamak amacı ile gizli bir anahtardan yararlanmaktadır. Ortak bir anahtar kullanarak da bunları doğrulamaya çalışmaktadır. Bu şekilde halka açık olan aracılığı ile sadece özel anahtarlar ile imzalanmış olan mesajların doğrulanabilmesi mümkün olmaktadır. Bahsi geçen bu işlem şifreleme kanıtı olarak adlandırılmaktadır. Aynı zamanda dijital imzalar zinciri şeklinde elektronik paralar ifade edilmektedir (Chaum, 1992: 96). Dolayısıyla nakit bulundurma ile madeni paraların kilidini açmak amacı ile anahtarın bulunması eşdeğer olmaktadır. Özel anahtarın kaybedilmesi durumunda ise, karşılık gelen dijital cüzdanda bulunan bütün madeni paralarında kaybolması söz konusudur (Antonopoulos, 2014: 231).

Aynı esnada, en iyi biçimde verimliliği, güvenliği ve hızı doğrulama sürecinin sağlayabileceği hakkında olan tartışmalar çözüme kavuşturulmamış olarak görülmektedir. Fakat en çok kullanılan işlem PoW5 olarak karşımıza çıkmaktadır (Antonopolous, 2014: 205). Teorik olarak en fazla saniyede yedi işlem gerçekleştirmesinde karşın gerçek blok büyüklüğünün 1 MB ile sınırlı olması söz konusudur. Bu durum maalesef temel ekonomiye hizmet arz etmekte yetersiz gelmektedir (Hofmann, 2018: 42). Visa'nın ağı bu duruma karşın saniyede 50.000'den çok işlemi gerçekleştirebilmesi mümkündür (VisaNet, 2019).

Bunun yanı sıra yasal sistemleri zayıf olan ülkelerde yer alan veya firmalara ideolojik açıdan karşı olan önemli derecede bilinmeyen taraflardan (büyük madenciler) madencilik endüstrisinin meydana geldiği söylenebilmektedir (Greenspan, 2015: 11). Yeni meydana getirilecek olan blokta yer alan bilgileri tekrardan yazabilecek 1Thash ya da F2Pool (bitcoin.info) ve karma hesaplama gücününpotansiyel olarak yüzde 51'ini kontrol edebilecek büyük madencilerin yer aldığı bir havuzda bitcoinnin bulunması bu duruma örnek olarak gösterilebilmektedir.

Bahsi geçen bu sebeplerden ötürü farklı finansal kurumlar tarafından kendi özel ağlarının ya da ortak sistemlerinin bulunması görüşü ortaya çıkmıştır. Aynı zamanda

izinli defterler şeklinde isimlendirilen güvenilir olan ve daha önceden seçilen onaylama düğümleriyle çalışmaya başladıkları görülmektedir. Bu olgunun Uluslararası Finans Enstitüsü (IIF) (2015)'nün yayımlanmış olduğu makalede de bahsedildiği üzere bitcoin ve öteki pek çok kripto para birimi ya da alternatif hizmet arz edenlerin tümüyle merkezi olmayan tasarımı ile örtüşmesi söz konusudur.

Ethereum projesi, blokzimcir alanında en mühim yeniliklerden biri olarak karşımıza çıkmaktadır. 2013 senesinde mucitleri arasında yer alan V. Buterin'ın kaleme aldığı bir makalede ilkelerin çekirdeği tavsiye edilmiştir. Turing-complete programlama diliyle geliştirilen açıl kaynaklı olan bir dijital para birimi olarak Ethereum karşımıza çıkmaktadır (Buterin, 2013).

PoW benzeri zorlu hesaplama metotları ile güven altında tutulan, halka tümü ile açık ve kontrolsüz olan bir ağı bulunmamaktadır. Bu çözümler ulaşıl izinlerinin oldukça sıkı biçimde kontrol altında tutulduğu ve Blockchaini durumunu okuma veya seçme haklarının tercih edilen kullanıcılarla sınırlı olduğu bir sistem meydana getirmesi söz konusudur. Buterin 2015 senesinde blog yazısında 2 tane izin verilmiş olan blockchaini uygulamasını sınıflandırmıştır. Bu kategoriler şu şekildedir (Buterin, 2015):

1. Konsorsiyum blokajı
2. Tamamen özel blokaj

1. Konsorsiyum blokajları: Burada önceden seçilen düğüm setinin konsensüs sürecini kontrol etmiş olduğu muhasebe sistemleri belirtilmektedir. Her biri bloğu geçerli hale getirmek amacı ile her bloğu imzalaması gerekli olan ve her biri bir düğüm işletmekte olan on beş mali kurumdan meydana gelen bir konsorsiyum bu duruma örnek olarak gösterilebilmektedir. Ayrıca katılımcılara blockchaini okuma hakkının sınırlı ya da açık olması söz konusudur.

2. Tamamen özel blokajlar: Bir kuruluşta izinler merkezi olarak kalmaktadır. Ayrıca herkese okuma izinleri açık ya da kapalı sayıda katılımcıyla sınırlıdır. Tek bir firma için olası uygulamalar veri tabanı idaresi, denetim ya da öteki iç kullanımları barındırmaktadır. Dolayısıyla pek çok durumda kamuya açık olan bir okunabilirlik gerekmemektedir. Düğümler izin verilen Blockchainlerde bilinmektedir. Bu nedenle

zorunlu olmayan hesaplamalı blok meydana getirme avantajı bulunmaktadır (Greenspan, 2015). Aynı zamanda bu durum artan ölçeklenebilirliğe ve daha hızlı doğrulma işlemlerine izin tanımaktadır. Böylece ekonominin işlem hacimlerine ana akım daha çok uyum sağlayabilmektedir. Ayrıca yasa koyucular ve düzenleyiciler içinde daha elverişli olması söz konusudur.

2.4 İşleyişteki Mekanizmalar

Saldırılara engel olmak amacı ile blockchain şifreleme, verilerin bütünlüğünü koruma ve kimlik doğrulama yetilerinden yararlanmaktadır. Dolayısıyla blockchainler güvenli veri alışverişini sağlaması açısında gereken alt yapıyı sağlamaktadır. Bu altyapıda bulutla bağlantılı olan platformlar ve yüksek ölçeklendirilebilir olay odaklı mimariler gerekli kılan işlemler de bulunmaktadır (Mylrea, 2017: 21).

2.4.1 Emek Kanıtı (Proof of Work)

Hesaplama kimliğini gidermek amacı ile gereken hesaplama maliyetinden Emek/İş Kanıtı (PoW), yeni eklenen bloğun güvencesi şeklinde yararlanmaktadır. Aynı zamanda ödül olarak da gelir sağlamaktadır. Dağıtılmış düğümlerin hesaplamalı güç rekabetiyle fikir birliğinin ve verilerin tutarlılığının güvenliğini sağlamak amacı ile yararlanılan bitcoin ile alakalı SatoshiNakamoto tarafından kaleme alınan makalede PoW fikir birliği mekanizması tavsiye edilmiştir (Nakamoto, 2008:.3). Bütün düğümlerin bitcoin sisteminde bir SHA256 matematik sorununu kendi bilgisayar güçleriyle gidermek amacı ile rekabet etmesi söz konusudur. Ayrıca bir sorunun hesaplanması için karışık olmasına karşın doğrulanması oldukça basittir. Blok hesapları hakkı elde eden bu problemi giderenlere otomatik şekilde bitcoinin ödül olarak üretmesi söz konusudur (Zheng, 2018: 560).

Çoğunlukla birden çok başta olan sıfırdan ihtiyaçları giderene blok başlığının karma değeri meydana gelmektedir. Blok başlığın karma değeri, hedef karma değerinin küçüklüğüne göre yüksek olmaktadır. Ayrıca yeni bloğu kazanmak ve uygun rastgele sayıyı belirlemek daha güç olmaktadır. Böylece bitcoinBlockchain sisteminin tahribatsız değişimi ve güvenliği garantiye alınmaktadır (Wang, 2018: 96).

PoW konsensüs mekanizmasında yüksek bir işlem gücü bulunmaktadır. Blok yapıların kurcalanması ya da bir saldırı düzenlenmesi halinde ise sorunu bütün blokların tekrardan hesaplaması gerekli hale gelmektedir. Aynı zamanda ana zincire sahte zincirin uzunluğunun geçmesini hesaplama hızının sağlaması söz konusudur. Bunun yanı sıra bahsi geçen bu saldırının maliyeti, var olan maliyetin oldukça üzerine çıkmaktadır (Franco, 2015: 102).

2.4.2 Hisse Kanıtı (Proof of Stake)

Madenciler tarafından işlerini yapabilmek için PoW metotları oldukça zor bir matematik denklemi çözülmedir. Madeni paraya sahip olanlar PoS sisteminde, bankacı/madenci görevini almaktadır. Ayrıca yeni basılan madeni paralar ile bu paralara ödül verilmektedir.

Örneğin bir malı satarak satıcı tarafından 10.000 ETH alındığı düşünüldüğünde, bu parayı alması gerekmektedir. Aynı zamanda ağda mülkünü de yayınlamalıdır. Blockchaininde mülkiyet yayını muhafaza edilmektedir. Ayrıca bu veriden satıcının ETH'leri harcamayı seçmesi durumunda da geçerli işlemi doğrulamak amacı ile tekrar yararlanılmaktadır. Satıcının cüzdanında paraları uygulamada 7 gün tutması mümkündür. Bu şekilde paranın satıcıya ait olduğu herkes tarafından bilinir hale gelmektedir. Bunun yanı sıra ağ içim satıcının coin'lerdeki hissesi hakkındaki bilgiler önem arz etmektedir. Daha çok coinle bu değer ödüllendirilmektedir. Satıcının hesabında bu durumda 7 günün ardından net 11.000 ETH yer almaktadır. Bu da fazladan 1.000 ETH hissesi ile bağlantılı olduğunu belirtmektedir. 7 gün içerisinde verilen bu örnekte satıcının%10'luk bir faiz ödemesi almakta ve bilgisayar kodu olan "merkez bankası" bunu garantilemektedir.

Ağda bulunan bazı katılımcılara gönderilecek bir sonraki bloğu bir hisse kanıtı protokolünün ödüllendirmesi söz konusudur. Çoğunlukla bu süreç, fon paylarıyla orantılı şekilde katılımcıların bir sonraki bloğu meydana getirmek amacı ile seçildiği manasında adil ve rastgele biçimde gerçekleştirilmektedir (Franco, 2015: 235).

2.4.3 PoW ve PoS Karşılaştırması

Proof-of-Work ve Proof-of-Stake olmak üzere iki çeşit veri madenciliğinden Blockchain teknolojisi tabanlı kripto paralarda yararlanılmaktadır. Bunlar PoW ve PoS şeklinde kısaca belirtilmektedir.

PoWrürü madencilik ele alındığında coinin kazılmış olan bloklar kadar olduğu karşımıza çıkmaktadır. Gereken algoritmaları bazı durumlarda bir grup bazı durumlarda ise bir birey çözmektedir. Bu şekilde Blockchaindeki bir sonra olan blok zincire dahil edilmektedir. Yatırımcılar tarafından bu madencilik tipinde veri blokları doğrulama evresinde esas uğraş gösterilmektedir. İşlemlerin doğrulanması ise yapılan çözümlerle gerçekleştirilmektedir. Ayrıca yeni coin'lerin üretimi de söz konusudur. Blok doğrulaması PoW tipi madencilikte gerçekleştirilirken aktif bir görevi bulunmamaktadır. Bu sebeple ödül kazanımı bulunmamaktadır.

Ödül, yeni bloğu çözmüş olan 2 bireye PoW tipi madencilikte verilir. Blok algoritmasının bu durumda çözülebilmesi noktasında yüksek işlemci gücü ihtiyacı ortaya çıkmaktadır. Bu durum aynı zamanda madencilik çiftliklerin meydana gelme sebebidir. Bahsi geçen bu çiftliklerde sayısı milyonlar ile ifade edilebilecek derecede fazla kapasitede işlemciler faaliyet göstermektedir. Zaman içerisinde madencilik işleminin kurumsallaşmaya başladığı görülmektedir. Bugün bitcoin madenciliğinin normal bir kişinin evinde yer alan masaüstü bilgisayarı kullanarak gerçekleştirebilmesi mümkün olmamaktadır. Dolayısıyla ilk olarak merkeze bağlı olmama görüşü ile ortaya çıkan bitcoinin bu düşüncesinin zarar gördüğü söylenebilmektedir (Antonopoulos, 2014: 27).

PoW madenciliği için bireysel kullanıcılar tarafından bugün ASIC adlı çipler satın alınmaktadır. Böylece madencilik yapmayı sürdürmektedirler (Franco, 2015, 47).

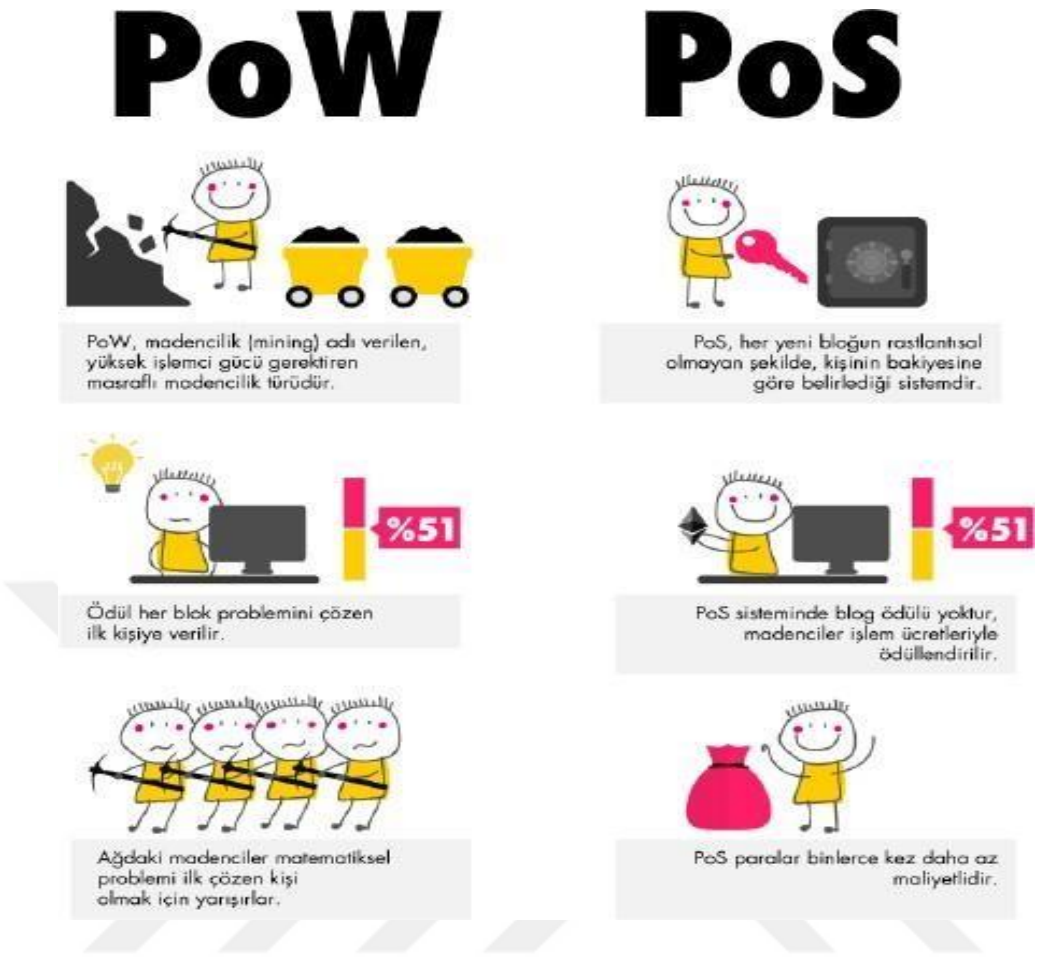
ASICsözcüğü Application SpecificIntegrated Circuit2in kısaltılmış hali olarak karşımıza çıkmaktadır. Vazifeler arasında ASIC hızlı geçişlerde bulunmaktadır. Bu şekilde algoritmada bulunan hesaplamalar için bir görev ara belleğinden yararlanmaktadır. Dijital para birimine yönelik, belli bir karma algoritmasına dayalı madencilik donanım parçası ASIC çipi olarak ifade edilmektedir (Koin Bülteni, 2019-b).

PoS ağda yer alan işlemleri doğrulmanın bir başka çeşidi olarak karşımıza çıkmaktadır. Esasında bu metot madencilik tanımına uygunluk göstermemektedir. Yeni bir paranın kullanıcılar tarafından üretilmesinde bir işlemin gerçekleştirilmesine gerek bulunmaması, bu durumun gerekçesi olarak gösterilmektedir. Dolayısıyla mining'den ziyade asıl ifadesi minting olarak belirtilmektedir. Bu durumun aslında madencilik değil de bir para basma olduğu söylenebilmektedir (Franco, 2015: 234).

PoS metodun da ödül kazanılması durumunda, kripto paranın tutulması amacı ile açılmış olan elektronik cüzdan hesabından yararlanılması söz konusudur. Elektronik cüzdanda yer alan coin miktarıyla, elde edilecek ödül arasında doğru yönlü bir ilişki bulunmaktadır. Ödül, cüzdanda bulunan para miktarına göre artış göstermektedir. Yani burada yeni bir paranın üretildiği söylenebilmektedir. Bunun yanı sıra coinlerin kıdemi, elektronik cüzdana yer alan coinlerin kalış süreleri uzaması ile belirlenmektedir. Bu sebeple o düzeyde işlem doğrulamasının yapılması halinde sağlanan ödülün miktarının artması söz konusudur (Franco, 2015: 234).

Coinlerin her birinin PoS yönteminde başlangıçta belirlenen bir senelik getirileri bulunmaktadır. Burada sabit getiri sağlamayı güvence altına alan yatırımların yer aldığı ifade edilmektedir. Bahsi geçen bu sabit getiri PoW sisteminde bulunmamaktadır. Ayrıca madencilik çiftliklerinin sayılarında, ağda yer alan düğüm ve operasyon sayılarının yükselmesine bağlı olarak bir artış meydana gelmektedir. Bireysel kullanıcıların getiri sağlama ihtimali, bu durumun bir getirisi olarak azalmaktadır.

PoS'un, PoW'a kıyasla maliyette tasarruf sağladığı görülmektedir. Aynı zamanda elektik tüketim maliyeti yok denecek kadar azdır. Bunun yanı sıra ödül, cüzdanda yer alan bakiyeye bağlıdır. Bu nedenle yatırımcılar tarafından daha çok yatırımda bulunulması özendirilmektedir. Şekil 2.6'dA PoW ve PoS karşılaştırması yer almaktadır.



Şekil 2.6 PoW ve PoS'un Karşılaştırılması

Kaynak: www.blockgeeks.com, 2019, akt. Gerdan, M. (2019). Blockchain Teknolojisiyle Gıda Güvenliği ve Yumurta Sektörü İçin Örnek Bir Uygulama, Yüksek Lisans Tezi, Marmara Üniversitesi, Sosyal Bilimler Enstitüsü.

2012 senesinde ilk kez PoS yöntemini birtakım alternatif kripto paralar kullanmıştır. PoW'danPoS'a geçenler arasında oldukça popüler olan kripto para birimi Ethereum yer almaktadır. Bu şekilde doğrulama süreçlerinin ve blok üretiminin hız kazanması amaçlanmaktadır. Ayrıca enerji gereksiniminin düşmesi hedeflenmektedir (Ethereum, 2017). PoS yönteminden yararlanan coinler arasında MorningStar,Peercoin,OkCash ve Ohmcoin benzeri görece yeni coinlerin pek çoğu yer almaktadır.

2.5 Blockchain Uygulama Güvenliği

Bir blokta geçmişin değiştirilmesi için Nakamoto tarafından gerçekleştirilen çalışmada (Nakamoto, 2008), blok zincire bütün blokların yeniden eklenmesinin gerekli olduğu belirtilmektedir. İşlem geçmişinin değiştirilmesi amacı ile bir girişimde bulunulması durumunda ise, değiştirilmiş olan bloğun özet değeri de farklılaşacaktır. Bu şekilde önceki bloklarla artış eşleşmesi mümkün değildir. Blok zincirde hile yapılması bu durum sonucunda güç hale gelmektedir. Bunun yanı sıra devamlı şekilde madenciler tarafından işlemler gözlenmektedir. Bu gözlemlemelerin neticesinde tutarlı bulunmayan işlemlerin kabul edilmemesi söz konusudur.

Kriptografiyle blok zincirinin, güvenli bir altyapı meydana getirmesine karşı halen hile yapılabilmesi mümkündür. Aşağıda hilenin hangi yollar ile gerçekleştirildiğinin bazılarına yer verilmiştir:

Geliştiricilerin test edilmesine ve onay almış kriptografi araçlarından yararlanılmasına karşı arzu etmeden güvenli olmayan yöntemler ile bunların toplanabilme olasılığının bulunması bahsi geçen yollardan biri olarak karşımıza çıkmaktadır. Bilhassa dikkat edilmesi gereken nokta, yararlanılan algoritmaların geliştirilmesi için değiştirilmesi esnasıdır. Zira meydana getirilen algoritmalarda güvenlik açıklarının kalma ihtimali vardır.

Bunun yanı sıra blok zincir teknolojisinden kötü yönlü olarak da yararlanılabildiği görülmektedir. Yüzde 51 şeklinde isimlendirilen saldırı, bu şekilde sistemi kötüye kullanmanın yollarından birini oluşturmaktadır. Bu saldırı da ağın yüzde 51'inin biri tarafından kontrol edildiği manasını taşımaktadır. Bu şekilde bilgiler olması gereken gibi doğrulanamamaktadır. Neticede ise blok zincire yanlış bilgi ilave edilmektedir.

Var olan blok zincir sisteminde, araştırmacıların birçok açık bulduğu görülmektedir. Blok zinciri bozmanın metotlarından biri de madencilik gücünün yarısından azını bulundurmalarına karşın öteki madencilerdir (Eyal& Sirer, 2018). Hali hazırda çözülmüş kripto-bulmacalar üzerindebencil bir madenci tarafından öteki düğümleri zaman harcamaya sevk etmesi ile haksız bir üstünlük sağlayabilmesi mümkün olmaktadır.

Tutulma atağı" (eclipseattack)' da bir diğer ihtimal olarak karşımıza çıkmaktadır. Blok zincirinde yer alan düğümlerin verilerin kıyaslanması amacı ile devamlı iletişim içerisinde bulunması gerekli olmaktadır. Bir saldırgan tarafından bir düğümüm iletişiminin eline alınması ve ağın geri kalanından gelmiş görünümü çizen hatalı verilerin kabul edilmesi sonucunda bundan sahte işlemlerin onaylanmasında veya kaynak israfından yararlanabilmesi söz konusudur.

Gerçek dünya ile blok zincir sisteminin bağlantı kurmuş olduğu noktalarda mühim problemler meydana gelebilmektedir. Sorunların ortaya çıktığı alanlara örnek olarak üçüncü taraf uygulamaları ve yazılım istemcileri gösterilebilmektedir. Kripto parası bulunan bütün kişiler tarafından özel anahtarların muhafaza edilmesi amacı ile yararlanılan web bağlantılı cüzdan uygulamalarına saldırganların sızabilme olasılıkları bulunmaktadır. Bilhassa saldırganların hedefinde çevrimiçi cüzdanlar yer almaktadır. Kullanıcılar tarafından paranın nerdeyse hepsinin çevrimdışı donanım cüzdanlarında tuttukları pek çok kripto para borsasında öne sürülmektedir. Fakat bu durumun daima doğru olmadığını Japonya merkezli bir kripto para borsası olarak karşımıza çıkan Coincheck'in 500 milyon doların üzerindeki kripto para değerinin çalınması durumu gözler önüne sermektedir (Cheng, 2018).

Gerçek dünyayla blok zincirleri arasında en karışık olan temas noktası, akıllı sözleşmeler olarak karşımıza çıkmaktadır. Akıllı sözleşmeler işlemlerin otomatikleştirilebileceği birtakım blok zincirlerde muhafaza edilen bilgisayar programlarıdır. Ethereum'un blok zincirine yazılan akıllı bir sözleşmede tahmin edilememiş olan bir açığı bilgisayar korsanları 2016 senesinde kullanmıştır. Bu şekilde o zamandaortalama 70 milyon dolar değerinde olan 3,6 milyon ETH'nin yeni bir blok zincir tabanlı yatırım fonu olan DAO'dan çalınması söz konusudur (Siegel, 2016). Blok zincirinde DAO kodu yaşamaktadır. Bu nedenle hard fork şeklinde isimlendirilen tartışmalı bir yazılım güncellemesi, parayı geri almak amacı ile Ethereum topluluğu tarafından gerçekleştirilmiştir. Bu şekilde paranın çalınmadan önce olan blok zincir kayıtlarına dek geri dönüşmüştür. Bu doğrultuda yeni bir blok zincir versiyonu meydana getirilmiştir.

2.6 Blockchain Uygulamalarının Dezavantajları

Blok zincir ekosisteminin gelişmesi ve çeşitli kullanımların oluşması ile birlikte bütün sektörlerde yeni bağımlılıklar ortaya çıkmaktadır. Aynı zamanda tartışmalı ve karmaşık problemler ile de karşılaşılacaktır (DeloitteLLP, 2016).

1. Kültür ve Organizasyon: Kurumsal bir çözümün parçası olarak blok zincirden yararlanılmasının sakıncalı olacağına dair düşünceler bulunmaktadır. Çünkü hem yeni bir teknoloji hem de gelişiminin daha ilk evrelerinde olması söz konusudur. Blok zincir tabanlı bir sisteme günümüzdeki sistemlerde yapılan işlemlerin geçirilmesi belli bir süreyi gerektirmektedir. Ortalama olarak minimum 10 yılda bahsi geçen bu sistemin yaygınlaşabileceği tahmin edilmektedir (The Economist, 2016).

2. Maliyet ve Performans: Çevrede, blok zincirde yeni blokların oluşturulması negatif yönlü bir etki yaratmaktadır. Her yeni bloğun meydana gelmesi ya da yeni bir işlemin doğrulanması durumunda madencilik sürecinin oldukça fazla miktarda enerji kaynağı tüketmesi söz konusudur. Bunun yanı sıra bu yeni teknolojinin işlemleri merkezi tabanlarına göre çok karışıktır. Bunun nedeni ise mutabakat mekanizmaları, imza doğrulama ve aynı işlemi her düğümün gerçekleştirmesi benzeri özelliklerinin bulunmasıdır. Bu durumlar sonucunda da geleneksel bir merkezi veri tabanına kıyasla işlem süresi daha çok olmaktadır.

3. Düzenleme: Düzenleme konusunda da blok zincir teknolojisinin uygulanmasında bazı yasal engeller de bulunmaktadır. Geleneksel ödeme ağında bulunan verimsizlikler ile baş edebilmek amacı ile bitcoin blok zincir benzeri birtakım teknolojilerin bilhassa düzenlemelere uygunsuz olarak tasarlanması söz konusudur. Bunun yanı sıra gözetimin azaltılması da blok zincirin orijinal hedeflerinden biri olarak karşımıza çıkmaktadır (DeloitteLLP, 2016). Ayrıca blok zincir teknolojisinin gelişimine sıkı düzenlemelerin engel olacağı hakkında da varsayımlar bulunmaktadır.

4. Güvenlik ve Gizlilik: İşlemlerin kişilerden ziyade cüzdanlara bağlanmasıyla takma ad kullanımını yani südonimliğiBitcoin benzeri kripto paraların sunması söz konusudur. Blok zincirin pek çok potansiyel uygulamasıakıllı sözleşmelerin ve işlemlerin belli kimlikler ile tartışmasız biçimde ilişkilendirilmesini gerekli kılmaktadır. Bu

durumun neticesinde ise paylaşılmış olan defterde muhafaza edilen ve ulaşılması mümkün olan verilerin güvenlik ve gizlilikleri hakkında problemleri ortaya çıkartmaktadır (DeloitteLLP, 2016).

3 HAVAYOLU SEKTÖRÜNDE BLOCKCHAİN KULLANIM DURUMLARI, FIRSATLAR VE GİRİŞİMLER

3.1 Havayolu Sektöründe Blockchain Kullanım Durumları

3.1.1 Gelecek Vaat Eden Kullanım Durumları

Blockchain uygulamalarının farklı konulara hitap eden özelliklerinin var olması ilerleyen dönemde farklı uygulamalar kapsamında kendini gösterebilme olasılığını ortaya çıkarmaktadır. Bu bağlamda blockchain uygulamalarının kendilerini günümüzde farklı Startup projeleri dahilinde göstermekte ve blockchain uygulamalarının geleceğiyle ilgili bazı izlenimler yakalanmasını sağlamaktadır. Tablo 3.1 dahilinde havayolu işletmeleri kapsamında gelecek vadeden bazı startup projelerine yer verilmektedir.

Tablo 3.1 Havayolu İşletmelerinde Geleceğe Hitap Eden Startup Projeleri (Zeren & Demirel, 2020: 177-178'den esinlenerek çizilmiştir.)

Dapps (Merkezsiz Uygulamalar) Proje Adı	Uygulamayla İlgili Bilgiler	Uygulama Alanı	Menşei
Blockchain Taksi	Havayolundan yararlanan yolcuların uçuş bilgilerini bir araya getiren akıllı sözleşmeler meydana getirmektedir	Havayolu İşletmeleri	İsviçre
Aeron	Çevrimiçi uçak biletinin rezervasyonu ile satın alınmasında blockchain teknolojisinden yararlanmışlardır	Havayolu İşletmeleri	Belize
SKYBIT	Çevrimiçi uçak biletinin rezervasyonu ile satın alınmasında blockchain teknolojisinden yararlanmışlar ve kripto paralar üzerinden ödeme yapılmasını temin etmişlerdir.	Havayolu İşletmeleri	Mynmar
FLYLA GmbH	Çevrimiçi uçak biletinin rezervasyonu ile satın alınmasında blockchain teknolojisinden yararlanmışlardır	Havayolu İşletmeleri	Almanya
Commute 21 LTD	Yolcu taşımacılığında kullanılan uçakların pilotsuz	Havayolu İşletmeleri	Çin

	uçmasını sağlayacak sistemleri geliştirilmesi üzerinde çalışmaktadır.		
Coavni	Yolcular ile pilotlar arasında uçuş platformu meydana getirilmesini temin etmişlerdir	Havayolu İşletmeleri	Fransa

Tablo 3.1'de de görüldüğü gibi havayolu işletmeleri dahilinde taksicilik uygulamaları, biletlerin rezervasyonları ve satın alınmaları ile biletlerin kripto paralar kullanılarak alınmaları, pilotsuz yolcu taşımacılığı ile yolcu ve pilotlar arasında yolcu platformları oluşturulması gibi farklı uygulamaların gelecekte yaygınlaşması beklenmektedir. Genel anlamda blockchain uygulamalarının gelecekte havayolları kapsamında kullanımları şu alanlarda kendini gösterebilecektir (thinktech, 2021);

1. Biletleme: Havayolu hizmetlerinde biletmeyle ilgili karmaşık şartlar bulunmakta. Bu bağlamda blockchain uygulamaları ile biletlerin ne biçimde satılacakları ve ne biçimde kullanılacakları belli bir düzene oturtulabilecektir. Böylelikle dünyanın herhangi bir noktasından bilet alınması mümkün olabilecektir.
2. Kimlik Yönetimi: Sahte kimlik ve diğer kimlikle ilgili sorunlar blockchain uygulamaları ile kolayca yönetilebilecektir.
3. Sadakat Programları: Seyahatler kapsamında kazanılan miller ya da miller bunların ortaklarınca belirtilen bir biçimde değerli şekilde harcanabilir hale getirilebilir.
4. Karışmış Bagajların Takip Edilmesi: Havaalanlarında bagajlar devamlı olarak yer değiştirmek durumundadır. Bagajlarla ilgi kuvvetli RFID çözümler olmasa bile birinin bagajıyla ilgili sorunlar ortaya çıktığında, bagajdan kimin sorumlu olduğunun belirlenmesi kapsamında gözetim değişiklikleri kayıtların var olması önem arz etmektedir. Burada yarı-özel blockchain uygulamaları takip açısından objektif bir göz temin etmektedir.
5. Bakım: Blockchain uygulamaları ile uçak parçalarının dijital kopyaları meydana getirilerek, uçak parçalarının üretimden çıktıkları andan itibaren izlenebilecekleri kayıtlar meydana getirilebilir.

3.1.2 Sadakat Programları

Blockchain uygulamalarının günümüzde daha etkin ve basitleştirilmiş bir biçimde yolcu kimliklerinin belirlenmesi, havayolları ile seyahat acenteleri arasındaki ödemelerin kolaylaştırılması, bagaj takibinin geliştirilmesi, güvenli yolcu kimliği belirleme sistemlerini sağlaması gibi uygulamalarda kullanılması ile birlikte kullanıcı dostu müşteri sadakati programlarını kullanılması daha kolay hale getirdiği ifade edilmektedir (Amadeus, 2017). Sadakat programların öncelikli olarak turizm sektöründe ön planda olmaktadır. Burada sadakat puanları yemek, ulaşım (havayolu ve diğerleri) ve diğer platformlardan edinilen kazanılan sadakat puanlarının birbirlerine dönüştürülmesi zor olmakla beraber blockchain sistemi kapsamında puanlar tekbir defter altında kayıt altına alınabilmekte, sınıflanabilmekte ve elde edilen puanlar güncel bir forma dönüştürülebilmektedir (Kowalewski, McLaughlin ve Hill, 2017).

Blockchain uygulamalarının özellikle turizm kapsamında kullanılması ile birlikte havacılık alanında kullanımında yaygınlaşmasını sağlamıştır. Özellikle blockchain uygulamaları ile birlikte güvensizlik, sahtekârlık ve çifte rezervasyon azalmakla birlikte kimlik kontrolü, yerleşiklik, kimlik kontrolü, saydamlık ve bu doğrultuda sadakat uygulamaları artış gösterecektir. Bununla birlikte blockchain teknolojisi bağlamında merkezsiz bir rezervasyon sistemiyle beraber problemsiz bagaj takibi, güvenli ödeme, uçaklarda gecikmenin olmaması doğrultusunda sadakat programlarının kullanımı daha kolay hale gelecektir (Kowalewski, McLaughlin ve Hill, 2017; Anushva, 2019).

3.1.3 Uçak Parçalarının Temeli

Uçaklar havayolu hizmetlerinin temelini oluşturmaktadır. Bilindiği üzere uçaklar binlerce parçadan meydana gelmekte ve olası arızaların engellenmesi veya tamir süreçlerinin gerçekleştirilmesi açısından bu parçaların belli sürelerde bakımı ve değişimi gerekmektedir. Uçaklar kapsamında pek çok parçanın bulunması bu parçaların değişim ve tamir zamanlarının takip edilmesini zorlaştırmaktadır. Blockchain üzerinden bu parçaların kullanım sürelerinin yıl ve saat bazından kaydedilmesi, farklı parçaların nitelikleri ile üretici bilgilerinin tek bir dijital defterde bir araya getirilmesi mümkün olacaktır. Bu durum hep kolay takibi sağlamakla birlikte giderlerin de azalmasını sağlayacaktır (Sadıç, 2018).

Uçak parçalarının dijital kopyalarının oluşturularak yine blockchain üzerinden karşı karşıya kaldıkları süreçlerin takip edilebilmesi mümkün olacaktır. Bu açıdan uçak parçaları fabrika üretiminden çıktıkları andan itibaren takip edilebilir bir niteliğe sahip olacaktır. Kullanım ömürleri kapsamında takipleri sağlanan parçaların değişim zamanlarının geldiğinin belirlenmesi de daha kolay hale gelmektedir (thinktech, 2021). Dünyanın önemli uçak motoru tedarikçilerinden biri olan GE Avination şirketi uçak parçalarını fabrikadan uçuş sürecine geçişte Azure Blockchain uygulamalarından yararlanarak takip ettiği ifade edilmektedir (Microsoft, 2021).

Uçak bakım ve tamir sektörü (MRO)'nün genel olarak karşı karşıya sorunlarla ilgili olarak blockchain teknolojisinden yararlanmaya başlamış olduğu söylenmektedir. Yeni faaliyete geçen MRO Blockchain Birliği üyeleri içerisinde SITA, FLYdocs, Cathay Pacific, Bolloré, HAECO Grubu gibi sektördeki önemli firmalar yer almaktadır. Bu bağlamda PwC tarafından yapılan bir çalışma doğrultusunda blockchain uygulamalarının MRO sektöründeki firmalara %5 maliyet tasarrufu sağlayabilme imkanına sahip olmakla birlikte havacılık sektöründe ise %4 gelir artışı sağlama potansiyeline sahiptir (Huillet, 2020).

3.2 Havayolu Sektöründe Blockchain Fırsatlar Ve Girişimler

3.2.1 Havacılıkta Fırsatlar

3.2.1.1 Sık Uçuş Noktaları

Blockchain, bu varlıkları dijital ve yaygın hale getirmek için tokenize ederek sık uçan yolcu noktalarının kazanılmasını, harcanmasını, muhasebesini ve mutabakatını önemli ölçüde düzene sokma yeteneğine sahiptir. Yolcu yükü faktörlerinin sürekli artması iyi haber olsa da, havayollarının bilet için puanların kullanılmasını kolaylaştırmasını zorlaştırmaktadır. Bilanço yükümlülüğü sorununa ek olarak, puan kazanma, kullanma ve değiştirme süreci, özellikle ittifaklar arasında yenilik için olgunlaşmış durumdadır (thinktech, 2021).

3.2.1.2 Bagaj, Kargo ve Yedek Parçalar

Blockchain, yolcu çantaları, kargo ve uçak yedek parçaları gibi değerli varlıkların durumunun ve konumunun takibini çok güvenilir ve değişmez bir şekilde, bu varlıkların konumları değiştirdikçe daha kolay hale getirmektedir. Bu durum söz konusu öğelerin değer zinciri boyunca hareket ederken görünürlüğü ve şeffaflığı artırmak için bir fırsat sağlamaktadır. Bu yeni yetenekler potansiyel olarak yeni ürün geliştirme alanlarının kilidini açabilir, sürecin düzene sokulmasını destekleyebilir ve sağlayıcıların aksaklıklarla başa çıkmaları için onlara bazı imkanlar sağlayabilir (thinktech, 2021).

3.2.1.3 Dağıtım ve Ödeme

Blockchain, hava yollarının, seyahat acentelerinin ve dağıtım alanındaki diğer kişilerin seyahat ürünlerini ve hizmetlerini beraber sunarken daha iyi işbirliği yapmasına olanak tanımaktadır. Beklenen değişiklikler, ilgili tüm tarafların dağıtım erişimini genişletebilir ve seyahat ürünlerinin ve hizmetlerinin bir araya getirilme şeklinin verimliliğini artırabilmektedir. Ayrıca, ödemeyi daha şeffaf, gerçek zamanlı ve düşük maliyetli hale getirme yeteneğine de sahiptir (Sheikh vd., 2019).

3.2.1.4 Yolcu ve Mürettebat Kimlik Yönetimi

Blockchain, yolcuların kimlik yönetimini kolaylaştırabilir, deneyimi artırabilir, gizliliği koruyabilir ve ayrıca havayollarının ve daha geniş değer zincirinin dijital ortamlarda iş yapmasını sağlayabilir (Buterin, 2014).

3.2.1.5 Seyahat Değer Zincirindeki Akıllı Sözleşmeler

Blockchain uygulamalarının ön plana çıkması ile birlikte akıllı sözleşmeler en fazla talep edilen uygulamalardan biri haline gelmiştir. Bunun nedeni ise bir blok zinciri kapsamında sahtekarlık,sansür ve kesinti riski söz konusu olmadan, kendi içerisinde depolanma imkanına sahip olmalarıdır (Mendling vd., 2018). Akıllı sözleşmeler temelde yasal sözleşmelerle direkt olarak bağlantı içerisinde olmasalar bile bu programlar, sözleşmedeki hesaplar kapsamında evvelden kararlaştırılmış işlemleri yerine getirecek program komutlarından meydana gelmektedir. Blockchain'deki hesaplardaki gibi akıllı sözleşmelerin bir adresi bulunmaktadır. Bu sözleşmeler bir kere blok sistemin dâhil

olmaları sonrasında değişikliğe uğramaları mümkün olmamaktadır. Sözleşmelerin şartları sağlanması halinde blockchain sistemine bağlı makinelerce otomatik bir biçimde işleme başlatılan süreçler komutlar içermesi nedeniyle otomasyon kapsamında önemli etkilere sahip olmaktadır (Buterin, 2014).

Akıllı sözleşmeler blockchain uygulamalarından yararlanılarak kullanıldığı için blockchainin niteliklerini de içinde barındırmaktadır. Bu bakımdan akıllı sözleşmeler blockchain uygulamalarının gelişim kaydetmesinde önemli görevler üstlenmektedir. Geleneksel sözleşmelere kıyasla akıllı sözleşmeleri farklılaştıran yararlar şu şekilde ifade edilebilir (Sheikh vd., 2019):

- Müşterilerle direkt olarak iletişim kurma.
- Güvenilir olma: Akıllı sözleşmeler kapsamında iş sözleşmeleri otomatik yürütülmeleri nedeniyle yok edilemez ve değiştirilemezler.
- Veri kaybının olmaması: İşlemler kapsamında bir aracı olmaması nedeniyle ağ kapsamında verileri koruyan ve yetkililer tarafından erişilen blockchain uygulamaları, merkezi olmayan bir hizmet sağlamaktadır.
- Maliyet Etkinliği: Müşteriler ve iş adamları her işlem açısından direkt etkileşime girebilmesinden dolayı ek ücretler ortaya çıkmamaktadır.
- Sahtekârlığa İzin Vermemesi: Akıllı sözleşmelerinin dağıtılmış blockchain zincirine kaydedilmesi sebebiyle ağda doğrulanması söz konusu olmaktadır. Bu sebeple, diğer katılımcıların akıllı sözleşme verilerini değiştirebilmesi mümkün değildir.
- Kayıt Koruması: Akıllı sözleşmeler blockchain kapsamında sıralı olarak saklanmaktadır.

Akıllı sözleşmeler blockchain uygulamaları yaygınlaştıkça giderek yaygın hale gelmektedir. Söz konusu yaygınlaşmanın kanıtları da şu şekilde sıralandırılabilir (Deloitte, 2016):

- Ethereum tabanlı bir firma yapmış olduğu çalışmalara 150 milyon doların üzerinde para ayırarak, temelde akıllı sözleşme tabanlı uygulamalar üretmektedir.

- 2016 yılının ilk üç aylık döneminde akıllı sözleşme toplamı 116 milyon dolar olmuştur. Bu değer evvelki üç, üç aylık dönemin 2 katından fazladır. Bununla beraber blockchain fonlarının %86'sının muhasebeleştirildiği görülmüştür.
- Blockchain kapsamındaki uygulamaları değerlendirmek maksadıyla kurulan yapıya (Post-Trade Distributed Ledger Group) 37 finansal kuruluşun üye olduğu görülmüştür.
- Avustralya Menkul Kıymetler Borsası kullanmakta olduğu sistem yerine, blockchain tabanlı bir sistem geliştirmek üzere çeşitli çalışmalar yapmaktadır.
- Global bankalardan bazılarının akıllı sözleşmelerden yararlanarak tedarik zinciri platformu ve ticaret finansmanı ile beraber kavram kanıtlama sistemleri üretme sürecine başladığı ifade edilmektedir.

3.2.1.6 IATA Blockchain Endüstrisi Girişimleri

Uluslararası Hava Taşımacılığı Birliği (International Air Transport Association (IATA) 1945 yılında Küba-Havana'da kurulmuştur. Bu birlik uçak yolcularının güvenilir, emniyetli, faydalı ve ekonomik hava hizmetlerini sağlamaları teşvik etmek maksadıyla havayollarının işbirliği içerisine girmeleri ile birlikte kurulmuştur. IATA'nın koyduğu standartlar ve prosedürler kapsamında günümüzün havacılık taşımacılık hizmetleri 1945 yılına kıyasla 100 kat büyük bir sektör haline gelmiştir (IATA, 2021). Günümüzde IATA gelişmelere açık bir biçimde çalışmalarını sürdürmektedir. Bu bağlamda blockchain uygulamaların gelişimler kapsamında IATA; IATA Coin, IATA Dijital Sertifika Yetkilisi, Dijital Finans ve Seyahat Tablosu girişimler içerisindedir.

3.2.1.7 IATA Coin

IATA Coin, havacılık endüstrinin sahip olduğu uluslar üstü dijital para birimi kavramını ifade etmektedir. Bu proje özellikle IATA Yerleşim Sistemi'ne bağlı olan IATA Takas Odası dahilinde blockchain teknolojisinden yararlanmayı amaçlamaktadır. Bu süreç 2014 yılında kripto paraların geliştirilmesi ve araştırılması ile ilgili sürecin devamını oluşturmaktadır. Özellikle 2018 yılında IATA Coin daha çok akıllı sözleşme, daha fazla farklı para birimi ve daha fazla havayolunun kullanımı ile birlikte gelişim kaydetmiştir (IATA, 2018).

3.2.1.8 IATA Dijital Sertifika Yetkilisi

IATA'nın temelde pek çok öğe ile ilgili olarak sertifika yetkilisi olduğu görülmektedir. Günümüzde IATA dijital alanda da kendini göstermeye başlamıştır. Dijital Sertifika Otoritesi (DCA) kavramı, Blockchain, Yapay Zeka ve Biyometri gibi gelişmekte olan teknolojilerden yararlanarak ticari havacılık dağıtım alanında (örneğin acenteler, havayolları, toplayıcılar, yolcular) dijital kimlik yönetimini kolaylaştıran bir platform olarak karşımıza çıkmaktadır. DCA' nın günümüzdeki ve ilerleyen dönemdeki şartlarda çalışması ve uyumlu olması beklenmektedir (IATA, 2018).

IATA, kendine üye olan havayollarının finansal sağlığını sürdürebilmesini sağlayabilmek, değer zincirindeki ortakların güvenli ve emniyetli bir şekilde iş yapmalarını temin edebilmek ve güvenilir yüksek kaliteli verilere gerçek zamanlı erişim sağlayacak bir çözüm oluşturmak için çeşitli çalışmalar yapmaktadır. Bu bağlamda DCA başta şu unsurları içerisinde bulundurmaktadır (IATA, 2018):

- Kurumların kimlik yönetimi süreci (Örneğin seyahat acentesi kimliği),
- İçeriğin bütünlüğünü daha kolay hale getirmek (Örneğin havayolu teklifi bütünlüğü)
- Sertifika doğrulama platformunun kullanılabilirliği.

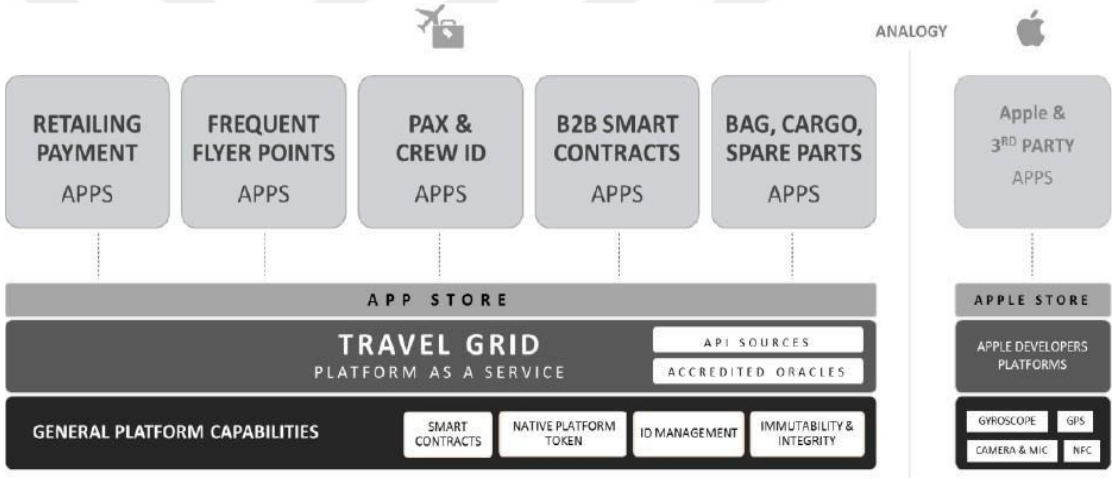
3.2.1.9 Dijital Finans

Dijital Finans girişimi, havayolu doğrudan operasyonel arka ofis maliyetini düşürmek ve arka ofis verimliliğini artırmak için Blockchain teknolojisi tarafından desteklenen Akıllı Sözleşme gibi mevcut yeni teknolojilerin en iyi nasıl kullanılacağına dair bir araştırmadır. Bu girişim, IATA Finansal Gelişim Çalışma Grubu tarafından desteklenmektedir. Bunun esas olarak havayolları ile havalimanı, yer hizmetleri ve diğer havalimanı hizmet sağlayıcıları gibi tedarikçiler arasındaki tedarikten ödemeye kadar süreci kesintiye uğratan Akıllı Sözleşmelerin kullanılması yoluyla gerçekleşmesi öngörülüyor. Muhasebe sürecini düzene koymanın yanı sıra sözleşmenin basitleştirilmesi, sözleşmenin uygulanması, gerçeğin tek bir kaynağına sahip olarak anlaşmazlıkların önlenmesi, hizmet sunumunun yerine getirilmesi aşamasında izlenmesi

ve gerçek zamanlı hizmet kabulünün başlatılması, mutabakat, faturalama ve ödeme süreçlerini düzenlemesi beklenmektedir (IATA, 2018).

3.2.1.10 Seyahat Tablosu

IATA'nın araştırma ve geliştirme girişimleri ve çeşitli çalışmaları kapsamında seyahat tablosu konsepti ticari havacılıkta ortaklarla işbirliği kurulabilmesi dahilinde geliştirilmiştir. Bu kavram, endüstri tarafından kullanılabilecek Blockchain yetenekleri sağlayan demokratik, ancak hızlı, verimli ve esnek bir ortamın çoğalmasına izin verecek ortak bir şebekenin oluşturulmasıyla ilgilidir. Bu bağlamda teknoloji devi olan Apple ortak çözümler oluşturulabilmesi adına bir platform ve ekosistem yaratmıştır (IATA, 2018). Bu seyahat tablosu Şekil 3.1'de görüldüğü gibidir.



Şekil 3.1 Apple Tarafından Oluşturulan Seyahat Tablosu (IATA, 2018: 19 esinlenerek oluşturulmuştur)

- Seyahat Tablosu vizyonu, gerçek zamanlı dijital etkileşimleri kolaylaştırır ve finansal işlemlerin maliyetini en aza indirerek havayollarını, seyahat acentelerini, otelleri ve diğerlerini yüksek maliyetlerden azaltır.
- Seyahat Tablosu, NDC ve One Order gibi endüstri dönüşümlerini destekleyen dijital kimlik yönetiminin altyapısı olacağı düşünülmektedir.
- Seyahat Tablosu, sözleşmelerin yönetilmesi, teslimatı izleme ve uygulama, mutabakat, düzeltmeler, faturalama ve ödeme gibi tedarikten ödemeye uçtan uca süreçleri önemli ölçüde basitleştirebilir.

- Seyahat Tablosu, dijital varlıkların değer zinciri boyunca sorunsuz bir şekilde süzülmesini sağlayarak yeni perakende fırsatları, daha verimli operasyonlar ve sorunsuz bir yolcu deneyimi sağlamaktadır.

3.3 Havacılık Sektöründe Blok Zinciri Girişimleri

3.3.1 Aeron

Aeron, Havacılık sektörünün güvenliği için blockchain uygulamalarının uygun olduğunu iddia ediyor. Bu bağlamda iş modellerinin, lisanslı özel pilotları işe alırken veya uçak sahipleriyle iş yaparken güvenliği artırmak için pilotların uçuş günlüklerinden kullanarak oluşturabileceklerini ifade etmektedirler (IATA, 2018).

3.3.2 Loyyal

Loyyal, müşteri teşviklerinin yaratılmasını, müşterilerin ödüllendirilmesini ve müşteri yönetimi sürecini yeniden icat ettiğini iddia ediyor. Burada blok zincir uygulamalarıyla birlikte uzlaştırma ve mutabakat sistemlerindeki maliyeti düşürmeyi mümkün kılarken aynı zamanda ortak ağın geliştirilmesinin mümkün olacağını ifade etmektedir (IATA, 2018).

3.3.3 Ozone

Ozone hava taşımacılığında alternatif bir dağıtım sistemi ortaya koymuştur. Ozone tarafından ortaya konulan bu sistem, özellikle geçmişteki sistemlerin sınırlamalarını aşma ve yeni bir ürün katalogu meydana getirmeyi amaçlamaktadır. Bu bağlamda Ozone pek çok müşteri ve dağıtımcıyla birlikte ikincil bir pazar etkinleştirmeye odaklanmaktadır (IATA, 2018).

3.3.4 SITA FlightChain

SITA yetkili bazı kurumların katılımı ile birlikte bazı havalimanları ve havayollarıyla ile beraber uçuş bilgilerinin tutulduğu ortak bir defter oluşturulmasını amaçlamıştır. Bu bağlamda SITA Britisih Havayolları, Heathrow, Cenevre Havaalanı ve

Miami Uluslar arası Havalanı ile birlikte SITA'nın Ar-Ge araştırmalarını akıllı sözleşmelerine çeviren FlightChain sistemini yayınlamıştır (IATA, 2018).

3.3.5 TravelBlock

TravelBlock, blok zincir teknolojisinden yararlanarak geleneksel Küresel Dağıtım Sistemine bir alternatif meydana getirmeyi amaçlamaktadır. TravelBlock meydana getirdiği bu sistem dahilinde tüketiciler açısından daha fazla şeffaflık ve görünürlük elde etmekle beraber maliyet güvenliği ve tasarrufu sağladığını iddia etmektedir (IATA, 2018).

3.3.6 TravelChain

TravelChain, seyahat endüstrisi dahilindeki tüm kurumların yönetime dahil olmasını sağlayan açık kaynaklı bir blok zincir uygulamasını olduğunu ileri sürüyor. Bu sistem dahilinde hizmetle ilgili bilgiler dışında denetim ve derecelendirmeye yönelik bilgilerin paylaşımını sağlayacak öğelere yer verilmesi de öngörülmektedir (IATA, 2018).

3.3.7 TripBit

TripBit, blok zincir uygulamaları ile kripto para sisteminden yararlanarak seyahat endüstrisi kapsamında ödemeyi daha hale getirecek bir sistem önermektedir. Burada ödemelerin uçuşlar, oteller ve etkinlikler kapsamında alınması öngörülmektedir (IATA, 2018).

3.3.8 Trustabit

Trustabit, blok zincir uygulamaları kapsamında geciken ya da iptal edilen uçuşlar dahilinde müşterilerin tazminat alabilmelerine yardımcı olmayı öngören bir yapı oluşturmayı amaçlamaktadır. Bu süreç, uçuş kesintileri olduğunda yolculara otomatik olarak kupon vermeyi blok zincir uygulamaları kapsamında akıllı sözleşmelerinin kullanılması ile gerçekleştirilmektedir (IATA, 2018).

3.3.9 Winding Tree

Winding Tree, oteller ve seyahat endüstrisi için envanter yönetimi ve dağıtım envanteri süreçlerini ortadan kaldıracak bir yapı ortaya çıkarmayı hedeflemektedir.

Konsept kapsamında seyahat rezervasyonlarıyla ilgili işlemlerin kayıt altına alınacağı bir pazar meydana getirerek, merkezi olmayan ve dağıtılmış bir defter oluşturulması öngörülmektedir (IATA, 2018).

3.4 Diğer Girişimler

Havacılık sektöründeki diğer blok zincir uygulamalarının bazıları şunlardır:

- Singapur Havayolları KrisFlyer Sık Uçuş Programı, diğer avantajların yanı sıra puanların kullanılmasını kolaylaştırmak için Blockchain'den yararlanıyor.
- Brüksel Havalimanı BRUcloud programı isimli Blok zincir uygulamalarından yararlanan açık bir veri paylaşım platformunu kullanmaktadır.
- Air France KLM, uçak bakımı açısından blok zincir teknolojisi kullanımını test etmektedir.
- Boeing, blok zincirli anti-spoofing GPS sisteminden yararlanmak için patent başvurusunda bulunmuştur.

4 HAVAYOLU SEKTÖRÜNDE BLOCKCHAİN UYGULAMA ÖRNEKLERİ

4.1 Araştırmanın Yöntemi, Kapsamı ve Sınırlılıkları

Araştırmada yöntem olarak literatür taraması yöntemi kullanılmıştır. Araştırma kapsamında nicel ve nitel veri analizi tekniklerinden faydalanılamamıştır. Türkiye'de havayolu sektörü açısından blockchain teknolojilerinin yeni olması ve bu alanda sektörel uygulamaların yetersiz olması nedeniyle, saha araştırması yapılamamıştır.

Araştırmada nicel ve nitel veri analizi kapsamında saha araştırması veya bir uygulama yapılamamıştır. Saha araştırması kapsamında havayolu şirketi ile görüşme yapılamamıştır. Görüşme taleplerinin reddedilmesi ve blockchain teknolojilerine yönelik gerekli bilgi ve deneyimine sahip personelin olmaması gibi nedenlerden dolayı, saha araştırması yapılamamıştır. Türkiye'de havayolu sektöründe blockchain teknolojilerinin yaygın olarak kullanılmaması ve yöneticilerin bu konuda yeterli tecrübeye sahip olmaması nedeniyle, görüşme veya anket formu uygulanamamıştır.

Saha araştırmasının yapılamaması nedeniyle literatür taraması kapsamında daha önce yapılan çalışmalar ve bu alanda yapılmış sektör raporları değerlendirmeye alınmıştır. havayolu sektörü açısından blockchain teknolojilerine yönelik güncel çalışmalar ve uygulamalar değerlendirilmiştir. Biyometrik havaalanı yolculuğu ve uçak parça tedarik sistemi uygulamaları gibi havayolu sektöründe blockchain teknolojilerine ilişkin detaylandırmalar yapılmıştır. Araştırma havayolu sektöründe blockchain teknolojilerine ilişkin biyometrik havaalanı yolculuğu ve uçak parça tedarik sistemi uygulamalarının daha önce yapılan çalışmalar kapsamında incelenmesi ile sınırlıdır.

Araştırmanın bu bölümünde havayolu sektörü açısından blockchain teknolojilerine yönelik uluslararası alanda yapılan örnek uygulamalara yer verilmiştir. Çalışma kapsamında özellikle biyometrik havaalanı yolculuğu ve uçak parça tedarik sistemi uygulamaları üzerinden blockchain teknolojileri üzerinde durulmuştur.

4.2 Biyometrik Havaalanı Yolculuğu

Yolcuların havalimanı boyunca seyahat etmek hiç de kolay değildir. Bir yolcu, uçağa güvenli bir şekilde binmeden önce çok sayıda çember ve engelden geçer. Günümüzde birçok havalimanı, yolcu işleme için izole çözümler uygulamaktadır. Bu teknolojilerden bazıları, otomatik self servis kiosklar ve çanta etiketi, self servis çanta bırakma, biniş ve sınır kontrolü için otomatik self servis kapıları içerir. Bu çözümler, yolcu kullanımını geliştirmek için biyometrik sistemlerle entegre edilebilir.

Yolcu işleme teknolojileri, yolcuların bir havalimanından geçerken yaşadıkları deneyim üzerinde büyük bir etkiye sahiptir. Yolcular, çoğu kez genel memnuniyet seviyesini azaltan, zahmetli bir planlama ve programlama, check-in adımları, bagaj yönetimi ve güvenlik kontrolü sürecinden geçerler. Self servis kiosk check-in'leri, kiosk çantası etiketleme, havalimanı mobil uygulamaları, kendi kendine biniş kapıları ve bagaj takibi gibi güncel teknolojilerin hepsi günümüz hava yolculuğunun ayrılmaz bir parçasıdır. Ülke çapındaki havalimanları, yeni teknolojilerin tanıtımına farklı şekilde öncelik vermekte ve her uygulamada çeşitli sonuçlar elde edilmektedir. Uygulanacak çeşitli kontrol noktaları ve güvenlik önlemleri ile, verimli yolcu işlemeyi başarmanın çoğu zaman zor olduğu kanıtlanmıştır. Biyometri, artan sayıda gezgini verimli ve hızlı bir şekilde işlerken güvenliği sürdürmenin zorluklarının üstesinden gelmeye yardımcı olmak için bu mevcut self servis teknolojilerle birleştirilebilir (Patel, 2018).

Biyometriye bağlı tek bir jeton kimliği kullanılarak, havalimanlarında yolcu işlemleri hızlandırılabilir. Tek jeton kimliği bu şekilde çalışır. Bir müşteri uçuş rezervasyonu yaptığında, kendisine biyometrik tek bir jeton kimliği verilir. Token ID, yolcuların her kontrol noktasında pasaport ve biniş kartlarını göstermek zorunda kalmadan check-in, bagaj bırakma, güvenlik, giden yolcu ve biniş işlemlerini yüz tanıma teknolojisini kullanarak tamamlamalarına olanak tanır. Biyometrik kimlik daha sonra pasaport görevi görür (Patel, 2018).

4.2.1 Teknik Durum

Bugünlerde, bir yolcunun seyahat yolculuğu, daha self-servis odaklı süreçler kullansa bile, basit olmaktan başka her şeydir. Yolculuğun tamamı genellikle dört aşamada kategorize edilir: seyahat öncesi, check-in, bagaj yönetimi ve güvenlik

kontrolü. Aşağıda, bir müşterinin nihai hedefine ulaşmak için gerçekleştirmesi gereken işlemlerin listesi bulunmaktadır (Patel, 2018).

- Seyahat öncesi aşama: En uygun uçuşu arayın, bileti onaylayın, bagajınızı hazırlayın, isteğe bağlı çevrimiçi check-in (kalkıştan önceki 24 saat içinde) ve havalimanına seyahat edin.
- Havaalanında check-in: İç hatlar için uçuştan iki saat önce veya dış hatlar için uçuştan üç saat önce, havalimanında yol bulma, selfservis yolcu check-in kiosku ve belge tarama ve doğrulama.
- Bagaj yönetimi aşaması: Self servis bagaj etiketleme kiosku ve check-in bagajı bırakma.
- Güvenlik kontrolü aşaması: Yolcu çıkış kontrolü, güvenlik erişimi, güvenlik taraması, biniş kapısını bulma, biniş kartını tarama ve uçağa binme.

Yukarıda açıklanan işlem ortalama 1,5 ila 3 saat arasında sürebilir. Sonuçta, hantal vize süreçleri nedeniyle, uzun kuyruklar ve kağıt belgelere aşırı güven, seyahatleri dostça olmayan bir hale getirir (Sorenson, 2018). Dünyanın dört bir yanındaki havalimanlarının, yolcuların yolculuklarını iyileştirmek için yenilikçi bir teknoloji tasarlaması gerekiyor. Sorenson, havalimanlarında biyometri kullanılarak bir yolcunun seyahatlerinin nasıl mümkün olacağına dair bir paradigma değişikliğine inanıyor. Ayrıca, havalimanlarındaki verimlilik, yeniden tasarlanmış bir hava yolculuğunu mümkün kılacak ve tüm dünyada inanılmaz sorunsuz bir deneyim sunacaktır (Sorenson, 2018).

4.2.2 Tek Token Yolcu İşleme Teknolojileri

Yeni teknolojinin önemli bir avantajı, endüstri standardı Ortak Kullanım Self Servis (CUSS) ekipmanı ve Ortak Kullanım Terminal Ekipmanı (CUTE) dahil olmak üzere mevcut havaalanı altyapısını kullanma ve entegre etme yeteneğidir (SITA, 2018). Yolcu işleme yolculuğunun temel adımlarını, mevcut yolcu işleme teknolojileri

bölümünde açıklandığı gibi biyometrik teknolojiyle birleştirerek, her yolcu temas noktası hızlandırılacak ve güvenli hale getirilecektir (SITA, 2018).

Şirketler her zaman endüstriyi değiştirecek etkiye sahip yeni teknolojileri incelerler. Blockchain teknolojileri, dijital güvenliği ve veri gizliliğini geliştirme yeteneklerinden dolayı günümüzde sıcak bir konudur (Back, 2017). Blockchain altyapısı, en iyi bilinen sanal para birimi olan Bitcoin ile referanslanır. Blok zinciri ilk olarak Bitcoin ile başladı, ancak o zamandan beri çeşitli kullanım durumlarına sahip birden fazla şirkete genişledi. Birden fazla blok zinciri türü vardır, ancak işletmeler defter tabanlı bir sistem arayışındadır. Bu kurumsal blok zincirlerinde depolanan veri türü, müşteri adlarından tam işlem kayıtlarına kadar her şeyi içerebilir. Blok zincirleri, verileri SHA-256 gibi karma algoritmalarla güvenli hale getiren bir Merkle Karma Ağacına dayanır. Veriler kayıtta saklanıyorsa, bilgilerin bütünlüğünü artırmak için daha fazla şifreleme ve karma oluşturma ile korunabilir. Blok zinciri, tüm dünyada defterin binlerce kopyasına sahip, yüksek düzeyde dağıtılmış bir veritabanı defteridir. Veri bloklarını birbirine bağlamak, zinciri oluşturmak için kullanılan karma algoritmanın kırılması neredeyse imkansızdır (Bauerle, 2017).

Gelişmekte olan teknolojilerin çoğu, dijital kimlik ve veri gizliliği sorumluluklarını geliştirmek için blockchain kullanmaktadır (Back, 2018). Bir havaalanında blockchain teknolojisini uygulayarak, biyometriye dayalı tek bir token kimliği oluşturarak yolcuların kimliğini doğrulayabilir. Bir havalimanı, Şekil 4.1'de gösterildiği gibi akıcı bir müşteri deneyimi için altı farklı biyometrik teknolojiyi entegre edebilir. Bir müşteri uçuş rezervasyonu yaptığında, kendisine bir biyometrik belirteç kimliği verilir. Yolcu, biyometrik kendi kendine check-in kiosk veya çevrimiçi check-in kullanarak havalimanına vardığında, yolcu uygun Tek Token Kimliği ile kimliğini doğrular (SITA, 2018). Bunu kioskta yapmak, bekleme süresini kısaltacak ve yolculara birden fazla check-in seçeneği sunacaktır.

Şekil 4.1 Biyometrik Havalimanı Yolculuğu

Kaynak: SITA, 2018.

Jeton kimliği, yolcu biyometrik ayrıntılarının yüz taraması ve parmak izi ile yakalanmasıyla verilir. Yolcuların fotoğrafı çekilir, yüzleri e-pasaportlarının biyometrik çipinde tutulan görüntüye göre veya bir havayolunun yolcu beyannamesine göre kontrol edilir ve manuel kimlik kontrolüne gerek kalmadan havalimanından geçerler. Ayrıca, biyometrik jeton yolculuk için pasaport, biniş kartı ve kimlik görevi görür (Thornhill, 2016).

Tek jeton seyahatinin anahtarı, sağlam bir jeton oluşturmak için verileri sürecin mümkün olduğunca erken bir aşamasında toplamak ve doğrulamaktır. Bu hem biyometrik hem de biyografik bilgileri içerir. Ve sonra gerekirse, yolculuğun çeşitli adımlarında daha ayrıntılı bilgilerle güncellenmektedir (SITA, 2018). Token Kimliği, yolcuların her kontrol noktasında pasaportlarını ve biniş kartlarını göstermek zorunda kalmadan yüz tanıma teknolojisini kullanarak check-in, bagaj bırakma, güvenlik, giden göçmenlik ve biniş işlemlerini tamamlamalarına olanak tanıyacaktır (SITA, 2018).

Yolcu biyometrik kimlikle check-in yaptığında, aynı kioskta yolcu çantalarını tartabilir ve kendi bagajını etiketleyebilir. Etiketleme tamamlandıktan sonra, yolcular pasaport veya biniş kartını göstermek zorunda kalmadan otomatik bir çanta bırakma alanına kolayca çantalarını bırakabilirler.

Yolcu daha sonra ek aramalar yapmadan TSA Pre✓® gibi program için parmak izlerini tarayabilecekleri güvenlikten geçebilir (TSA, 2018). Yolcu daha sonra

Otomatik Sınır Kontrolü (ABC) Kapılarından geçer ve sonunda müşteri, biyometriklerini kullanarak Havaalanı Self Servis Kapıları ile uçağa biner. Tek jetonla yolcular, havalimanı boyunca sorunsuz bir işlem sürecine sahip olacaklar (Patel, 2018).

4.2.3 Yüz Tanıma

Yüz tanıma sistemi, önceden kaydedilmiş bir kaynaktan alınan dijital bir görüntüyle ilgili olarak bir kişiyi tanımlama ve doğrulama yeteneğine sahip teknolojik bir uygulama anlamına gelir. Yüz tanıma sistemleri, insan yüzlerini algılamak ve tanımlamak için programlanan bilgisayar tabanlı güvenlik sistemleridir. Yüz Tanıma Teknolojisi (FRT), yüz özelliklerini analiz etmeyi, özellikleri bir veri tabanında depolamayı ve yüzleri tanımlamak için kullanmayı içerir. Yüz tanıma sistemini kullanırken, birincil görevi bir insan yüzünü kalıplar gibi tanımak ve çıkarmaktır. Yüz çıkarıldıktan sonra sistem, gözler arasındaki mesafe, elmacık kemiklerinin şekli ve diğer ayırt edilebilir özellikler gibi yüzün algılanması için özel sinir mekanizmalarını ölçer. Bu ölçümler, doğru eşleşmeyi bulmak için tüm resim veri tabanı aracılığıyla karşılaştırılır. FRT üç göreve ayrılmıştır: yüz doğrulama, yüz tanıma ve izleme listesi (Intona, 2017).

Yüz doğrulama, kimlik doğrulama ile ilgilidir. Bir bireyin gerçekliğini doğrulamak, kullanıcının iddia ettiği kişi olup olmadığı sorusuna cevap vererek yapılabilir. Yüz doğrulamasını değerlendirmek için, doğrulama performansı ya yanlış bir ret ya da yanlış kabuldür. Yanlış ret, meşru kullanıcıların tanınma ve erişim izni alma hızıdır. Yanlış kabul, sistem sahtekarlara erişim izni verilen bir hata yaptığında sistem çıktısıdır (Intona, 2017).

Yüz tanıma, soruyu kullanıcının kim olduğuna veya kimliğinin ne olduğuna yanıt verir. Yüz tanıma, yüzün kimliğini belirlemek için onu araştırır ve bir veri tabanıyla eşleştirir. Tanımlama, kapalı küme tanımlama sorunları ile açık küme tanımlama sorunları arasında ayrım yapılarak test edilir. Kapalı küme tanımlama probleminde, sensör önceden referans veri tabanında bilinen yüz gözlemini alırken, açık küme tanımlama, sistemin referans veri tabanında bulunmayanları ifade eder (Intona, 2017).

İzleme listesi, sistemin aradığı şüpheliyi açıklar. İzleme listeleri, açık küme bir tanımlama görevinden türetilmiştir. Bir sistem, izleme listesinde bir kişiyi aramak için tüm veri tabanını karşılaştırır ve eşleştiğini tanımlar. Doğru bir eşleşme üzerine, sistem bir alarmı tetikleyecektir (Intona, 2017). 2015 yılında, ABD Gümrük ve Sınır Koruması (CBP), Washington Dulles Uluslararası Havaalanında yüz karşılaştırma teknolojisini test etti. "Bu testin sonuçları, sistemin gerçek pasaportlar ve canlı yakalanan görüntülerle başarılı bir şekilde eşleştiğini belirledi" (CBP, 2018). Yüz tanıma teknolojilerini halihazırda benimsemiş kilit ülkeler, Avustralya sınır kuvveti ve Yeni Zelanda gümrük hizmetleridir. Otomatik yüz tanıma, Smart Gate adlı bir biniş sistemidir. Smart Gate, yolcuların yüzünü pasaportun mikroçipindeki verilerle karşılaştırır (Patel, 2018).

4.2.4 Parmak İzi Tanıma Parmak

Parmak İzi yolcu işlemlerini büyük ölçüde iyileştirebildiğinden, yüz tanıma yazılımını diğer biyometrilerle birleştirmek gibi çok faktörlü bir kimlik doğrulama sisteminde kullanılan biyometrik sistem entegrasyonu sağlar. Parmak izi herkese özgüdür ve kimsenin tahmin edemeyeceği için güvenlik sağlar. Ayrıca biyometrik varlığı nedeniyle parmak izleri unutulmazdır (Poza, 2016). Tüm parmak izi veri işlemleri, bir sistem ana işlemcisine yüklenen kodun ve verilerin gizliliğini ve bütünlüğünü garanti eden bir Güvenilir Yürütme Ortamı (TEE) içindegerçekleştirilir.

Daha önce tartışıldığı gibi, her parmak izi kullanıcısına özeldir ve bir parmak izi tarayıcısının yardımıyla dijital bir parmak izi formunun bir görüntüsü toplanır. Her benzersiz parmak izi, cihazın güvenli olmasını sağlayan benzersiz bir koda dönüştürülür. Bir havaalanında, güvenlik kontrol noktalarına genellikle otomatik bir parmak izi tarayıcısı yerleştirilir (Patel, 2018).

Üç tür tarayıcı vardır: Optik, kapasitif ve ultrasonik. Optik bir sensör, kişinin parmak görüntüsünün bir görüntüsünü yakalar. En açık ve en karanlık alanları analiz ederek sırtlar, şekiller veya işaretler gibi benzersiz desenleri ayırt etmeye yardımcı olan algoritmalar kullanır (Triggs, 2018). Birinin, hassas ayrıntıları atlamak için 2B bir resim veya bir protez kullanabileceğinden, optik tarayıcı son derece güvensizdir (Triggs, 2018).

Optik sensörlerle karşılaştırıldığında, kapasitif sensörler, bir parmak izinin verilerini toplamak için bir dizi küçük kapasitör devresi kullanır ve bir parmak izinin ayrıntılarını izlemek için küçük elektrik ve iletken yükler kullanır. İletken plakaları ve çıkıntıları kullanmanın sonucu, "çıkıntıların parmak izine kadar oldukça ayrıntılı bir görüntüsünü" sağlayan daha güvenli bir parmak izi tarayıcısıdır (Triggs, 2018).

Ayrıca, ultrasonik tarayıcı donanımı hem bir ultrasonik verici hem de bir alıcıdan oluşur. Tarayıcı, ultrasonik bir darbeyi sıçratarak bir kullanıcının parmak izinin çıkıntılarının ve ayırt edici özelliklerinin 3B modelini oluşturur. Bunlar birlikte, cildin altını görmesini ve parmağın canlı olduğunu doğrulamasını sağlarken, biyometrik bir ölçü olarak daha fazla bilgi sağlar (Triggs, 2018).

Günümüzde, TSA, TSA Pre✓(TSA, 2018) adı verilen operasyonel ve güvenlik etkisi için biyometrik kimlik doğrulama teknolojisini değerlendirmek için bir kavram kanıtı sürecinden geçiyor. Bu programa kaydolarak, yolculara her yolcuya özel bir "Bilinen Yolcu Numarası" verilir. TSA, yolcu parmak izlerini “kanun yaptırımı, göçmenlik ve istihbarat veri tabanlarının yanı sıra hükümet izleme listesi ve Hastalık Kontrol ve Önleme Merkezlerinin sağlık endişeleri nedeniyle seyahat etmesine izin verilmeyen kişilerin listesi” ile eşleştirir (Future Travel Experience, 2015). Yolcuların kimliklerini doğrulamak için parmak izlerinin kullanılması hem biniş kartı hem de kimlik belgesi görevi görür. TSA Pre✓, gezginleri güvenlik kontrol noktasından hızlandırabilecek tarama sürecini hızlandırır (Patel, 2018).

4.2.5 İris Tanıma

İris, gözün görünür renkli kısmıdır. Parmak izlerine benzer şekilde, tek yumurta ikizleri de dahil hiçbir iki iris birbirine benzemez. Üstelik sağ ve sol göz desenleri bile birbirinden benzersizdir. İris paterni, iki yaşından sonra değişmeden kalır. İris tanımlama sistemi, tarayıcının irisi çıkarırken bir kişinin gözünün konumunu hesaplamasını sağlayan matematiksel algoritmalar kullanır. Tarayıcı, iris üzerinde belirgin işaretler ve desenler çizer ve gözden beş ila 24 inç uzaklıkta siyah beyaz bir resim alır. Bu teknoloji, havalimanlarında ve sınır noktalarında kullanım için etkilidir.

Birleşik Arap Emirlikleri (BAE), sınır kontrol noktaları için bir iris biyometrik sistemi geliştirdi. 2016 yılında Dubai havaalanı 83,6 milyon yolcuyu izledi ve 2035

yılına kadar 7,2 milyar yolcuya ulaşacağı tahmin ediliyor. Yine de, tüm sınır kontrol noktaları iris tanıma gibi bir biyometrik tanımlama sistemi benimseyinceye kadar, çok sayıda yolcu trafiğini yönetmek zor görünmektedir. BAE, sınır kontrol noktalarında, sınır dışı edilen kişilerin ülkeye tekrar girmemesini sağlamak için iris tanımayı zorunlu kıldı. Sınır dışı edilen kişinin sahte kimlik ve tahrif edilmiş belgelerle BAE'ye girmesini önlemek için, gelen tüm yolcuların iris kodları, kayıtlı bir merkezi veri tabanıyla gerçek zamanlı olarak kapsamlı bir şekilde karşılaştırılır (Patel, 2018).

4.2.6 Gelişen Biyometrik Teknolojiler

Kullanıcı kimlik doğrulama sistemi için kullanılan başka bir benzersiz biyometri, perioküler, retina ve yürüyüş modellerini içerir. Göz çevresi gözlemcisi, irise benzer şekilde, en yoğun biyomedikal özelliklere sahip gözleri çevreleyen bölgeyi gözlemler. Göz çevresi özellikleri, şekil, boyut ve renk bakımından farklılık gösteren göz kapakları, kaşlar ve göz küresini içerir. Perioküler bölge, yüz ve iris tanıma arasında bir denge bulur. Örneğin, bir yüz görüntüsü belli bir mesafeden çekildiğinde, iris desenleri düşük çözünürlüklü olabilir (Patel, 2018).

Sadece iris kapalı bir mesafeden yakalanırsa, yüz özellikleri kullanılamaz. Bu nedenle, perioküler sistemin hem yüz hem de göz bölgelerini geniş mesafelerden yakalaması bir avantaja sahiptir. Perioküler, birey yaş ilerledikçe bile şekil ve konumda çok az değişiklik yaşar (Jain, 2009).

Hem iris hem de perioküler gözün karakteristik özelliğiyken, diğer bir göz biyometrik yöntemi retinadır. Retina, gözün arka kısmında bulunur. Biyometrik sistemler, bireyleri retina kan damarlarına göre tanımlar çünkü bunlar benzersizdir ve bu nedenle tanımlama için uygundur. Bir retina biyometresi, dijital bir görüntü elde etmek için yakınlarda ve düşük yoğunluklu bir ışının doğrudan bireylere yansıtılmasıyla yakalanır (Jain, 2009).

Yürüyüşün uygulanması gibi bazı biyometrik yöntemler, bireylerin yürüyüş şeklini değerlendirir. Yürüyüş, düşük çözünürlüklü güvenlik kameralarının bireyleri tanımlamak için insan siluetini algılamasına izin verir. Yürüme, bir kişinin veya nesnenin ne kadar hızlı, ne kadar uzağa ve ne kadar kuvvetle hareket ettiğini ölçebilir. Yürüme, bir kişinin fiziksel olarak herhangi bir şeye dokunması veya bir cihazın

yanına yaklaşması gerekmediğinden, invaziv değildir. Yürüme paternleri, bütünsel ve özellik temelli olarak sınıflandırılır. Bütünsel olanlar hareket tarafından üretilen vücut hareket istatistiklerini hesaplarken, özellik temelli olanlar daha iyi tanımlamak için bireylerin adımlarını ve kinematiğini hesaplar (Jain, 2009).

Biyometri geliştikçe, tüm bu uygulamalar havalimanları gibi daha gelişmiş güvenlik sistemlerine entegre edilebilir. Havaalanlarında biyometri kullanımının başarılı bir şekilde benimsenmesi, zaman ve para açısından kaynak tasarrufu sağlayacaktır.

4.3 Uçak Parça Tedarik Sistemi Uygulamaları

Tedarik zinciri yönetimi, herhangi bir endüstriyel sektörün bel kemiğidir. Küresel olarak dağıtılan ve belirli ürün türlerinin üretiminde uzmanlaşmış farklı sanayi kuruluşları, başka bir üreticinin başka bir ürünü veya nihai ürünün bir kısmını üretmesini gerektirecek belirli segmentler için üretim evleri olarak işletilmektedir. Nihai ürüne ulaşmadan önce, ürünün ayrı parçaları, çok katmanlı tedarik zinciri adı verilen bir dizi tedarik zincirinden geçer. Havacılık endüstrisi, bu sürecin ne kadar karmaşık olabileceğinin ve tüm bu sürecin nasıl işlediğinin mükemmel bir örneğini temsil ediyor. Bireysel parçalar veya uçak gövde bölümleri ithal edilir, uygun bir envanter tutulur ve ardından yurt içinde monte edilir. Uçak, gerekli hizmet türüne bağlı olarak başka bir bölgeye revizyon yapabilir.

Bu tedarik zincirleri iyi düzenlenir ve ayrı ayrı şirketler tarafından kendi seviyelerinde uygun şekilde izlenir. Kara borsalarda satılan parçaların veya segmentlerin değiştirilmesi, kötü kalitede çoğaltılması ve hizmet dışı bırakılmış veya önceki ürünlerin olası bir riski vardır. Ürün üretiminin tek bir tedarik zinciri yoktur, ancak segment üretimi için büyük ölçüde birbirine bağlı olan, birbirine bağımlı üreticilere yönelik bir ağ vardır. Bu zincirde ilerlemeden önce, ürünü gelecekteki kullanım için değerli ve verimli kılacak belirli gereksinimleri karşılaması gereken belirli ön koşullar vardır. Çoğu durumda, belirli gereksinimler karşılanmadığında, bunlar ya iade edilir ya da yeniden üretilir, bu da nihai ürünlerin elde edilmesindeki gecikmeyi daha da artırır (Madhwal ve Panfilov, 2017).

Herhangi bir tedarik zincirindeki amaç, doğru ürünün doğru zamanda üretilmesini ve zincirde doğru akışta olmasını sağlamaktır. İhtiyaç duyulan talepleri üretmek ve karşılamak için nakliye şekli gibi dış faktörlere ve stokların mevcudiyeti gibi iç faktörlere büyük ölçüde bağımlıdır. Bu zincirler aşırı miktarda akış bilgisi, ürün ve paradan oluşur. Tedarik zinciri yönetiminin bileşenleri karmaşıktır ancak aşağıdakilere dayanır:

- Envanterin Planlanması, yani üretim merkezinin hangi bölümünden gerekli ürünü temin etmek kolay olacaktır, vb.
- Hammadde tedarikçisi ile ilişki kurmada gelişmek.
- Ürünün kalitesini ölçmek.
- Nihai ürünü gerekli tarafa ulaştırmak
- Çalıştırın, yani nihayet ürünü gerektiği gibi test etmek ve çalıştırmak

Bir hava aracının servis, parça değişimi veya bir bütün olarak performans testi için kullanılabileceği bazı durumlarda revizyon gerektiği durumlar vardır. Uçaklar, hizmet almak için bir yerden diğerine hareket eder, çünkü bu belirli hizmet belirli bir yer merkezinde mevcut olabilir. Bu, kalite ve performans işaretlemesini sağlar ve herhangi bir hata hatası varsa, o zaman onarılır veya değiştirilir.

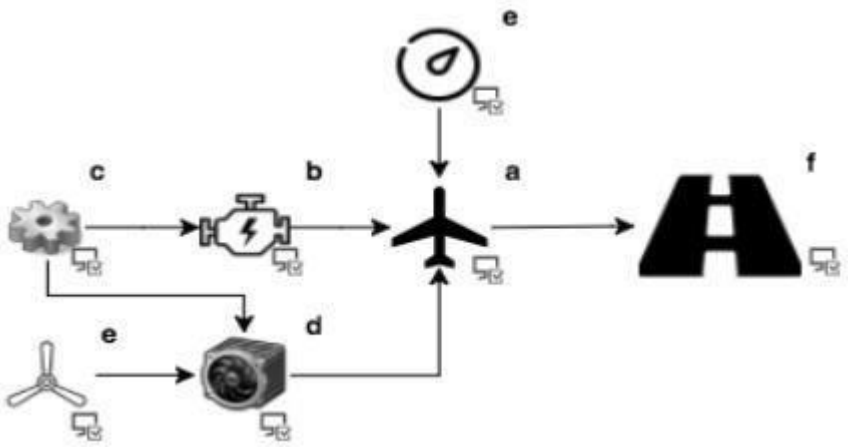
Blockchain teknolojisi [9], günümüzün BT çağında hayati bir rol oynamaktadır. Başlangıçta, kullanıcılar arasında tüm işlemleri anonim olarak güncelleyecek ve tek bir tarafın müdahale etmesi zor olacak bireysel defterleri etkinleştirerek farklı kullanıcılar arasındaki işlemleri kaydetmek için kullanılan ortak veri tabanını dağıtmaya odaklanan Bitcoin tarafından tanıtılmıştır. Blockchain, izlenebilirlik gerektirir; açık defter ile, iki tarafın anonim kalmasına rağmen, hangi ürünün zincirin hangi üyesine işlem gördüğünü tespit edebilir.

Havacılık tedarik zinciri ağında, kullanıcı işleme dahil olan tarafların erişimine sahip olacaktır. Nihai üründe bir hata veya arıza varsa, onu tedarik yoluna kadar kolayca izleyebilir. İlerlemeyi izleyebilir ve bununla gelecekteki üretimi planlayabilir. Endüstri 4.0'daki tasarım ilkelerini desteklemek için aşağıdakiler önerilmektedir (Madhwal ve Panfilov, 2017):

- Birlikte çalışabilirlik: Her bir segmentin sensör veya özel kimlik ile etkinleştirilmesi, farklı katman gövdelerinin birbirine bağlanmasına ve birbiriyle iletişim kurmasına yardımcı olur.
- Bilgi Şeffaflığı: Her seviyede bireysel süreçleri gösterme yeteneği, örneğin bu zincirde herhangi bir seviyede herhangi bir değişiklik yapılırsa tüm kullanıcılar değişiklik ile yeni detaylarla güncellenecektir.
- Teknik Yardım: Bu, sistemlerin bilgiye dayalı kararlar almak, gelecekteki planlama ve sorunları hızlı bir şekilde çözmek için bilgileri kapsamlı bir şekilde toplayarak ve görselleştirerek zincirdeki bireyi desteklemesine yardımcı olur.
- Merkezi Olmayan Kararlar: Bireysel şirketlerin kendi kararlarını vermelerini ve görevlerini yerine getirmelerini sağlamak.

Akıllı Sözleşmelerin tanıtımı, istenen ve markalı ürüne kadar arzuların gerçekleştirilmesine yardımcı olabilir. Bu süreç, ürünlerin seri numarası, geçerliliği gibi tüm ayrıntılara, yani kimlik doğrulamasını ve benzersizliğini garanti edecek tüm bilgilere sahip olacaktır.. Artık birçok çokuluslu şirket, kullanıcıya varış yeri veya zamanıyla ilgili durum güncellemelerini sağlıyor. Bu, dolandırıcılığı azaltmaya, gecikmeleri azaltmaya, kağıt işlerini, diğer israfları vb. azaltmaya yardımcı olacak küresel zincir tedarikinde güvenli şeffaflık elde etmeye yardımcı olmaktadır.

Örnek bir model olarak havacılık endüstrisinin tedarik zincirine Blockchain'i ima edilme süreci ve bu ağdaki bireysel kullanıcıların platformlarında paylaşılan detayların, havacılık sektörlerine kâr ve güvenlik açısından nasıl fayda sağlayabileceğini izleyebilmek adına şu model dikkat çekmektedir.



Şekil 4.2 Örnek Tedarik Zinciri

Kaynak: Madhwal ve Panfilov, 2017

Bir montaj merkezinde 'a' başlayalım, bu montaj göbekleri farklı yerlerden farklı parçalar tedarik eder ve tek bir uçakta birleştirilir. Bu hub, tedarik zincirinin motor ve türbin gibi parçaları sırasıyla farklı "b" ve "d" parçalarından tedarik eden bağımsız gövdelerinden biridir. Örneğin, türbin için bir parça 'a' merkezindeki bir uçağa tedarik edilirken ve monte edilirken, ağın tüm üyeleri arasında bir işlem ve montaj defteri güncellenerek, benzersiz kimliğe sahip türbinin diğer bölümlerle birlikte bir araya getirildiğini ve bu da kendisi benzersiz kimliğin yeni bir ürünü gibi davranacaktır. Tedarik defteri, bireysel üyeler arasında işlem ayrıntılarını gösterecek işlem defteri ile entegre edilecek olan her seviyede üretilen tüm yeni ürünlerin kaydını tutacaktır. Bu ağın tamamı, üretim ayrıntılarını gösterecek ürünlerin ayrıntılarıyla birlikte tek tek şirketler için envanter kaydı olarak da çalışabilir (Madhwal ve Panfilov, 2017).

Şimdi ayrı montaj merkezlerinde kendi tedarik zinciri yollarını koruyacaklar. Bu zincirdeki bazı ürün seviyesinde, eğer bir ürün değiştirilirse veya kurcalanırsa ve bu ürünü alacak olanın veri tabanı, merkezi olmayan defter nedeniyle manipüle edilirse, bu işlem uyumsuzluk olacağından doğrulanmayacaktır. Örneğin, seri numarasında olabilir ve bu nedenle bu, gelecekte meydana gelebilecek arızaları önleyebilir ve bir çeşit arızayı önleyebilir.

Parça bir uçağa monte edildikten ve bir amaca hizmet ettiğinde (ticari, özel, vb.), herhangi bir bakım merkezindeki revizyon sırasında, mühendisler gerekli tüm bakımı, kalan ömrü kontrol etmek için uygun ve kolay bir erişime sahip olacaktır. Ürün beklentisi, dolayısıyla zamanı azaltır ve işin verimliliğini arttırır. Herhangi bir parçanın kullanım süresi dolmak üzereyse, önceden gösterilecek ve performans çalışma sırasında ve paralel izleme ile de izlenebilecektir.

Blockchain, finans / bankacılık sistemlerinde katma değer süreçleri için kanıtlandığı şekilde, tedarik zinciri sistemlerine zamanında, verimli ve şeffaf işlemlerin önemli avantajlarını doğal olarak sağlayabilmektedir.

Kullanılan yaklaşım, havacılık endüstrisini açıklayıcı bir örnek alarak Blockchain ile tedarik zinciri arasındaki bağlantıyı kurmaya yönelik en son çalışmaları incelemekti. Bu çalışma, Blockchain'in tedarik zinciri araştırmalarında iyi bir bağlantıya sahip olduğunu ve tedarik zinciri yönetiminde (SCM) Blockchain kullanımının arttığını göstermektedir. Lojistikte, Blockchain, bir gönderi ile ilgili tüm belgelerin barındırılabileceği tek bir dijital yer oluşturmak için çoğunlukla dijital dağıtılmış bir defter olarak kullanılmıştır.

Blockchain'in en önemli avantajlarından biri, geleneksel BT çözümlerinden daha güvenli olmasıdır. Blockchain'in, uçak parçalarının izlenebilirliğini artırmada ve yedek parçaların orijinalliğini sağlamada etkili olabileceğini önermektedir. Gelecekte, Rusya'da üretilen ve Hintli havayollarına ve devlet müşterilerine teslim edilen parçaların kimliğini doğrulamak için teknolojiyi geliştirmeyi ve test etmeyi planlamaktadır. Çözüm, sensörlerden veya RFID etiketlerinden bilgi alır ve parçaları fabrikadan uçağa kadar takip etmek için bunları Blockchain'e kaydeder. Tedarik zincirindeki işlemlerle ilgili tüm bilgilerin mevcudiyetiyle, sahte ürünlerde azalma beklentisi elde edilebilir. Dahası, akıllı sözleşmenin bu ağa eklenmesi, üçüncü tarafın katılımını ortadan kaldırabileceği için yolsuzluk olasılığını en aza indirecek ve veri bilgilerinin yayılmasıyla savunma, özel parçalar gibi farklı sektörlerden alıcılar kendi kendilerine satın alma kabiliyetine sahip olacaklardır (Madhwal ve Panfilov, 2017).

SCM uygulamasına Blockchain girişinin gelecekteki araştırması için başka ilginç alanlar vardır. Özellikle, büyük bir şirketin küçük üreticilerden yedek parça satın almasının yaygın olduğu küresel uçak parçası tedarik zincirlerinde iş yapmanın

maliyetini düşürmek için Blockchain kullanma hedeflenmektedir. Bu genellikle uçtan uca tedarik zinciri boyunca maliyetleri artırır. Potansiyel olarak, Blockchain teknolojisi, stratejik tedarik ile ilgili finansal maliyetleri büyük ölçüde azaltabilir.

5 SONUÇ VE ÖNERİLER

5.1 Sonuçlar

Var oluşlarını devam ettirebilmek amacı ile toplumsal yapılar hayatta kalma mücadelesi içerisindedir. Yer aldıkları çerçeve adapte olarak meşruiyet elde etmeleri, bu aşamadaki en mühim faktördür. Yaşamın bütün alanlarındaki gibi kurumlarda bulunan çevreye adapte olma uğraşında yaşanan değişim kaçınılmazdır. Bir yapıyı meydana getiren parçalar arasında var olan ilişkilerin nitelik ve nicelik açısından farklılaşması, değişim olarak tanımlanabilmektedir. Kurumsal değişim ise, süreç, davranış ve yapıların değişmesiyle meydana gelmektedir. Bu değişim, kurumların sürdürülebilirliği adında gerekli bir durumdur. Ayrıca kurumsal çevrenin gerekli kıldıkları bağlamında değişimin meydana gelmesi söz konusudur. Globalleşme ve teknolojik ilerlemenin artması ile beraber bugün bu gelişmeler oldukça hızlı şekilde yayılıp uygulanabilmektedir. Dolayısıyla çok hızlı biçimde kurumsal çevredeki değişimler yaşanmaktadır. Sağlıklı biçimde kurumlarda ortaya çıkan değişimlerin işleyebilmesinde yaşanan değişimlerin kurumsal yapılar tarafından algılanabilmesi gerekmektedir. Aynı zamanda bunları yorumlanması ve kendi süreçlerine katılarak idare edilmesi de odlukça önemlidir.

Kurumsal çevre benzeri dışsal aktörlerde hızlı şekilde meydana gelen değişim neticesinde bugün yer aldığı çevreye adapte olmaya çalışan kurumların bu hıza uyum sağlayamadığı görülmektedir. Ayrıca gün geçtikçe temel fonksiyonu olan güvenilir üçüncü taraf olma özelliklerinde de aksaklıklar yaşanmaktadır. Teknolojik ilerlemeler paralel şekilde dijital dönüşümler yaşanmaktadır. Özel sektörden kamuya, iş yapma biçiminden sosyal yaşama dek pek çok alanda dijital dönüşümün etkilerini görebilmek mümkündür. Bütün teknolojik ilerlemeler paralelinde değişimi de doğurmaktadır. Kurumsal çevrede yaşanan değişime göre, kişiler arasında var olan iletişimin güvenilir üçüncü tarafı şeklinde olan kurumsal yapıların bu hızda meydana gelen bir değişimi kabul edip kendi bünyelerinde uygulayabilmesi daha yavaş olmaktadır. Kurum yapısında teknolojik gelişmenin değişim sürecinde ise, kurumunun kurumsal yapıyı, idare süreçlerini, insan boyutunu yani kurumda faaliyet gösteren kişileri ve kurumun gayesi üzerinde bir etki yaratması söz konusudur. İlerleyen teknolojiye bu çerçevede adapte olarak benimsemeye çabalayan kurumların yeni ödül yapılarını, yeni

örgütlenme şekillerini, yeni gözetim kanallarını ve pek çok başka değişimleri de yapması gerekli olmaktadır.

Kurumsal yapıların değişimin hızına uyum sağlayamaması sonucunda sistemlerinde pek çok bakımdan sorunlar ortaya çıkabilmektedir. Organizasyon yapısında bulunan dijital dönüşümün tam manası ile yapılmaması, sistemler arasında var olan uyumsuzluklar ve doğru şekilde dijitalleşmeden yararlanılmaması benzeri faktörler ele alındığında, güvenirlik problemleri ile baş edebilmek amacı ile meydana getiren kurumların bir güven problemi oluşturan yapı halini aldığı karşımıza çıkmaktadır. Teknik sebeplere ek olarak kurumlara karşı kişilerin güvenlerinin düşmesinde ortaya çıkan krizlerinde etkisiz söz konusudur. Geçmişte sarsılmaz, büyük ve güvenilir olarak değerlendirilen pek çok kurum, bilhassa 2008 global krizinin ardından tartışılmaya başlanmıştır. Finans sektörü başta olmak üzere Lehman Brothers benzeri uluslararası köklü şirketlerin iflasa gitmesinden dolayı pek çok alanda kurumlara olan bakış açılarında değişimler meydana gelmiştir.

Güvenilir olmaları, kriptpgrafi kullanılarak, bir merkezi tabi olmadan, bloklar hakinde verilerin zincirlenmesi modeli ile oluşan bu teknolojilerin en mühim noktaları olmaktadır. Var olan sistemlere kıyasla blockchain teknolojilerinin bazı avantajları bulunmaktadır. Bunlar; ağda bloklara kayıt edilen değer, veri ya da öteki bilgilerin saklanması ve transfer edilmesinin daha kullanışlı olmasıdır. Bunun yanı sıra bütün alanlarda çeşitli işlemlerin yapılabilmesi için meydana getirilen bu ağlardan yararlanılabilmektedir. Kripto paralar ve Bitcoin üzerinden Blockchain uygulamaları yaygınlık göstermektedir. Buna karşın dünyada ulaşılan noktada finans sektörü dışında da teknolojinin potansiyeli anlaşılmıştır. Dolayısıyla uygulama alanlarının genişlemesi söz konusudur.

Blockchain devrim niteliğindedir ve şüphesiz dünyayı değiştirme potansiyeli vardır. Blockchain ile ilgili en güzel şey, kriptografi ve fikir birliği mekanizmasının birbirine güvenmeyen tarafları bir araya getirme araçları sunmasıdır. Paydaşlar, bir blockchain yolculuğuna çıkmanın hem heyecan verici hem de talepkar olacağına hazırlıklı olmalıdır. Gelişmelerden önce yapılması gereken birçok husus söz konusudur. Yasal düzenlemelerden, süreçlerine ve ilgili verileri anlamaya ve teknik uzmanlığa kadar birçok farklı yetenek gerektirecektir. Blockchain'i benimsemek ve bir

temel oluşturabilmek için birlikte çalışabilirlik oluşturmak, gerekli standartları araştırmak için projeler başlatılması önerilmektedir.

Teknoloji ve dijitalleşme sürekli gelişmekte, iş yerlerini ve süreçlerini etkilemektedir. Bu aynı zamanda, Uluslararası Havalimanları Konseyi'nin (ACI) havalimanlarının artık sadece yolcuların varış noktalarına ulaşmasını kolaylaştıran yer olmadığını ilan ettiği havacılık endüstrisinde de geçerlidir. Artık havalimanı, kişilerin yolculuğunu dijital çözümlere dayalı bir sonraki seviyeye taşımak amacıyla dijital ve veriye dayalı havalimanları yaratmayı amaçlayan önemli bir ağ geçidi ve ekonomik makineye dönüşmüştür (Jenkins & Nolan, 2020; Jones, 2019). Yeni teknoloji uygulamaları, havalimanında rahat, kişisel ve ilgili bir geçişe dayalı sorunsuz bir seyahat sağlayarak, yolcu deneyimini iyileştirmek için yeni fırsatlar ve olanaklar sağlayacaktır (Mullan, 2020). Benzer şekilde teknoloji, yeni iş modelleri aracılığıyla geliri artırma olanakları sağlamaktadır (Beck ve diğerleri, 2017).

Ancak teknolojinin gelişmesi ve kullanımı, tek başına geleceğin yolcularına sorunsuz seyahat sunan havalimanına doğru ilerlemeyi sağlamakta yeterli değildir. Kilit bir unsur, yeni teknolojinin uygulamalarından yararlanmak için gerekli olan ekosistemdeki aktörler arasında birlikte çalışabilirliktir (Hartshorn, 2020). Ayrıca, bir paydaşın operasyonlarının diğerinin çalışmasına izin vermesi nedeniyle çeşitli paydaşlar birbirine bağımlı olarak değerlendirilebilir. Bu nedenle, işbirliğinin ortak bir odak noktası olması beklenebilir. Ancak, şu anda işbirliği ve birlikte çalışabilirlik, yolculuğun daha da geliştirilmesi ve operasyonların iyileştirilmesi için bir engel olarak kabul edilmektedir. Paydaşlar arasındaki sınırlı veri paylaşımı, havalimanları daha dijital ve veri odaklı olmayı amaçladığından paradoksaldır (Copenhagen Airports A/S, 2020). Birlikte çalışabilirliğe sahip olmak, operasyonları ve nihayetinde yolcu deneyimini iyileştirebilir (Hartshorn, 2020), bu sayede verilerin potansiyelini daha da açığa çıkarmak için birincil odak noktası olması gerekir (Copenhagen Airports A/S, 2020).

Blockchain teknolojileri, tedarik zinciri aktörleri arasında güveni ve veri paylaşımını iyileştirebilir. Blok zinciri teknolojilerinin tanıtımı, genellikle bağlı sistemlerin ve cihazların (yani IoT) İnternetinin yayılmasıyla ilgilidir. Blockchain veri tabanlarının fiziksel dünya ile bağlantılı olması gerekir ve birçok çalışmada bu bağlantının IoT cihazları tarafından sürdürüleceği öngörülmektedir. “Otonom” ve

"bağlı" araçlar arasında mümkün olacak işbirlikçi veri paylaşımı, işlemler ve diğer herhangi bir veri (veya para birimi) alışverişi, geleneksel veri tabanları tarafından garanti edilemeyen belirli özellikleri garanti edebilen blok zincir teknolojilerinin kullanımıyla kolaylaştırılabilir. Havacılık sektörüne uygulanan blockchain teknolojileri, geliştirmenin erken bir aşamasındadır ve geliştirilmesi gerekmektedir.

5.2 Öneriler

- Havacılık sektöründe blockchain teknolojilerinin gelişmesi ve uygulanabilirliğinin sağlanması adına daha fazla çalışma yapılmalıdır.
- Havacılık sektörü ve devletler tarafından ortak çalışmalar kapsamında blockchain teknolojilerine yönelik uygulanabilirlik ve güvenlik çalışmaları yütürülmelidir.
- Blochain dışında kimlik bilgilerinin ilişkisel veri tabanında muhafaza edilmesi performansı yükseltmektedir. Bu şekilde zaman içerisinde meydana gelebilecek depolama yükünden blok zincirin kurtulması mümkün olmaktadır. Fakat güvenli erişim kontrolünü ve veri gizliliğini sağlayacak biçimde bu şekilde bir veri depolama sisteminin oluşturulması gerekmektedir.
- İleride yapılacak olan çalışmalarda farklı sektörlerde blockchain teknolojisi incelenerek sektörler bazında uygulanabilirliği ve sorunları üzerinden tartışılabilir.

6 KAYNAKLAR

Amadeus. (2017). Blockchain: Harnessing Its Potential in Travel. https://amadeus.com/en/insights/research-report/blockchain-harnessing-its-potential-in-travel

Antonopoulos, M. A. (2014). Mastering Bitcoin - Unlocking Digital Currencies. O'Reilly Media.

Anushya. (2019). How Blockchain Technology can Transform Travel and Tourism Industry?. https://Www.Bitdeal.Net/Blockhain-In-Travel-And-Tourism.

Back, A. (2017). Using Blockchain for Digital Identity & Crypto Assets. Retrieved from medium.com/blockchain-review/self-sovereign-identity-and-the-digitization-of-realworld-assets-738e87dc530c

Bauerle, N. (2017). What is Blockchain Technology? Retrieved from https://www.coindesk.com/information/what-is-blockchain-technology/

Beck, R., Avital, M., Rossi, M., & Thatcher, J. B. (2017). Blockchain technology in business and information systems research.

Beck, R., Stenum Czepluch, J., Lollike, N., & Malone, S. (2016). Blockchain – The Gateway to Trust-Free Cryptographic Transactions. Twenty-Fourth European Conference on Information

Buterin V. (2014). A Next-Generation Smart Contract and Decentralized Application Platform. White Paper.

Buterin, V. (2013). A Next Generation Smart Contract And Decentralized Application Platform. https://ethereumbuilders.gitbooks.io/guide/content/en/whitepaper.html

Buterin, V. (2015). On Public and Private Blockchains. 21 Mart 2019 tarihinde https://blog.ethereum.org/2015/08/07/on-public-and-private-Blockchains

CBP (2018). Customs and Border Protection. Retrieved from https://www.cbp.gov

Chaum, D. (1992). Achieving Electronic Privacy. Scientific American, 267 (2): 96–101

Cheng, E. (2018). Japanese cryptocurrency exchange loses more than $500 million to hackers. https://www.cnbc.com/2018/01/26/japanese-cryptocurrency-exchange-loses-morethan-500-million-to-hackers.html

Cihat, E. "Kriptografik hash fonksiyonlarının incelenmesi", Yüksek Lisans Tezi Trakya Üniversitesi Fen Bilimleri Enstitüsü, Edirne (2012).

Copenhagen Airports A/S (2020). Travelling towards the airport of the future – Consolidated Financial Report of 2019.

Çarkacıoğlu, A. (2016). Kripto-Para Bitcoin. Sermaye Piyasası Kurulu Araştırma Raporu, Ankara.

Deloitte LLP. (2016). Blockchain Enigma Paradox Opportunity. https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitteuk-blockchain-full-report.pdf

Deloitte, 2016. Deloitte , CFO Insights getting smart about smart contract

Dilek, Ş. (2018). Blockchain Teknolojisi ve Bitcoin. İstanbul: Seta.

Durbilmez Erözel, S. (2018). Blockchaın Teknolojisinin Finans Sektöründeki Yeri ve Uygulamaları, Yüksek Lisans Tezi, Marmara Üniversitesi, Sosyal Bilimler Enstitüsü.

Ethereum (2017). White Paper, https://whitepaper.io/coin/ethereum

Eyal, I., & Sirer, E. G. (2018). Majority is not Enough: Bitcoin Mining is Vulnerable. https://www.cs.cornell.edu/~ie53/publications/btcProcFC.pdf, [Ziyaret Tarihi: 15.01.2021].

Franco, P. (2015). Understanding Bitcoin: Cryptography, Engineering and Economics, John Wiley & Sons, Incorporated.

Future Travel Experience (2015). Biometric Technology Enabling Seamless Airport Vision. Retrieved from http://www.futuretravelexperience.com/2015/07/biometrictechnology-driving-seamless-airport-vision/

Gerdan, M. (2019). Blockchain Teknolojisiyle Gıda Güvenliği ve Yumurta Sektörü İçin Örnek Bir Uygulama, Yüksek Lisans Tezi, Marmara Üniversitesi, Sosyal Bilimler Enstitüsü.

Greenspan, G. (2015). Ending The Bitcoin Versus Blockchain Debate. http://www.multichain.com/ blog/2015/07/bitcoin-vs- Blockchain-debate/

Güven, V., & Şahinöz, E. (2018). Blockchain - Kripto Paralar - Bitcoin. İstanbul: Kronik Kitap.

Hartshorn, R. (2020). Technology Will Only Get Us So Far. International Airport Review, Issue 1, February 2020.

He, Y. (2018). A Novel Cross-Chain Mechanism for Blockchains. Qiu, M. (Ed.). Smart Blockchain. Springer, 139-148.

Hofmann, E., Strewe, U. M., Bosia, N. (2018). Supply Chain Fnance and Blockchain Technology. Springer.

Hughes, E. (1993). A Cypherpunk's Manifesto. Activism: https://www.activism.net/cypherpunk/manifesto.html adresinden alındı.

Huillet, Marie, (2020). Uçak Bakım ve Tamir Sektörü Blockchain Birliği Oluşturdu, https://tr.cointelegraph.com/news/aircraft-maintenance-repair-industry-is-latest-to-form-blockchain-alliance, 05.02.2020.

IATA. (2018). Blockchain in Aviation: Exploring The Fundamentels, Use Cases, And Industry Inıtıatıves, White Paper.

IATA. (2021). The Founding of IATA, https://www.iata.org/en/about/history/

Intona, L., & Nissenbaum, H. (2017). Facial Recognition Technology. Retrieved from https://www.nyu.edu/projects/nissenbaum/papers/facial_recognition_report.pdf

Jain, A. K., Ross, A., & Park, U. (2009). Periocular Biometrics in the Visible. Retrieved from http://www.cse.msu.edu/~rossarun/pubs/ParkRossJain_Periocular_BTAS09.pdf

Jenkins. M., & Nolan. T. (2020). Investing in airport technology services is central to Miami's vision. International Airport Review. from:https://www.internationalairportreview.com/article/115215/airport-it-technology-miamiairport-maurice/

Jones, D. (2019). How will airports of the future embrace digitalisation? International Airport Review. from:https://www.internationalairportreview.com/article/94522/airports-future-digitalisation/

Kardeş, B. (2019). Kripto Paralar ve Temel Analiz. İstanbul: Sokak Kitapları Yayınları.

Kınacı, M. (2019).Yüksek Lisans Tezi, Blockchaın Teknolojisi Ve Akıllı Sözleşmelerin Yaygınlaşmasının Önündeki Engeller, Yüksek Lisans Tezi, Bahçeşehir Üniversitesi, Fen Bilimleri Enstitüsü.

Kırbaş, İ. (2018). Blockchaini Teknolojisi ve Yakın Gelecekteki Uygulama Alanları. Mehmet Akif Ersoy Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 9 (1), 75-82

Koin Bülteni (2019-b). ASIC Nedir? https://koinbulteni.com/asicnedir adresinden alınmıştır.

Konukseven, S., & Özen, T. (2018). 50 Yıllık Hayal Bitcoin. İstanbul: MediaCat.

Kowalewski, Dan , Jessica McLaughlin, ve Alex J. Hill. Blockchain Will Transform Customer Loyalty Programs . https://hbr.org/2017/03/blockchain-will-transform-customer-loyalty-programs

May, T. C. (1992). The Crypto Anarchist Manifesto. 2020 tarihinde Activism: https://www.activism.net/cypherpunk/crypto-anarchy.html adresinden alındı.

Mendling, Jan, Ingo Weber, Wil Van Der Aalst, … ve Liming Zhu (2018) "Blockchains For Business Process Management – Challenges and Opportunities", ACM Transactions on Management Information Systems, C:9 (1), ss.0:1-0:16.

Microsoft. (2021). Customer Stories- GE Aviation's Digital Group streamlines tracking of aircraft parts, reduces inefficiencies with Azure Blockchain Technologies, https://customers.microsoft.com/en-us/story/755328-ge-aviation-manufacturing-azure

Mullan, R. (2017). No longer passenger experience; It's now seamless travel. International Airport Review. https://www.internationalairportreview.com/article/33223/seamless-travel-pte/

Mylrea, M., Gourisetti, S. (2017) Blockchain For Smart Grid Resilience: Exchanging Distributed Energy at Speed, Scale and Security. 2017 Resilience Week (RWS), Wilmington, USA, 18-23.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. 7 Mart 2019 tarihinde http://www.bitcoin.org/bitcoin.pdf adresinden alınmıştır.

Okuyucu, H.H. (2020). Hash Fonksiyonlarının Adli Bilişimde Uygulamaları ve C++ İle Şifreleme Algoritması Tasarımı, Yüksek Lisans Tezi, Karabük Üniversitesi, Elektrik ve Elektronik Mühendisliği Bölümü

Patel, V. (2018). Airport Passenger Processing Technology: A Biometric Airport Journey. Master of Science in Cybersecurity Engineering at Embry-Riddle Aeronautical University.

Pinto, R. (2018). How Blockchain Can Solve Identity Management Problems. https://www.forbes.com/sites/forbestechcouncil/2018/07/27/how-blockchain-cansolve-identity-management-problems/#795ece8e13f5, [Ziyaret Tarihi: 10.02.2021].

Poza, D. (2016). Fingerprint Authentication Gives You High Security and Low Friction Auth0. Retrieved from https://auth0.com/blog/how-fingerprint-auth-gives-yousecurity/

Sadıç, B. (2018). Blockchain ve Havacılık için Vaadettikleri https://www.linkedin.com/pulse/blockchain-ve-havac%C4%B1l%C4%B1k-i%C3%A7in-vaadettikleri-berat-sad%C4%B1%C3%A7, 19.03.2021.

Sayar, S. (2019). DİJİTALLEŞME İLE YENİ OLUŞAN KAVRAMLAR: ENDÜSTRİ 4.0, IOT VE BLOCKCHAİN UYGULAMALARI, Yüksek Lisans Tezi, Maltepe Üniversitesi, Sosyal Bilimler Enstitüsü..

Sheikh, Husneara, Rahima Meer Azmathullah ve Faiza Rizwan (2019) "Smart Contract Development, Adoption and Challenges: The Powered Blockchain",

International Research Journal of Advanced Engineering and Science, C:4 (2), ss.321-324.

SITA (2018). SITA. Retrieved from https://www.sita.aero

Siegel, D. (2016). Understanding The DAO Attack. https://www.coindesk.com/understandingdao-hack-journalists, [Ziyaret Tarihi: 15.02.2021].

Sorenson, A. (2018). A Paradigm Shift in How We Travel. Retrieved from https://www.linkedin.com/pulse/paradigm-shift-how-we-travel-arne-sorenson-1/?trackingId=a4BJrFrz9F1wMNEGQ6Yyxg%3D%3D&lipi=urn%3Ali%3Apage%3Ad_flagship3_search_srp_content%3BnWePi4GxTuq7E3Fm%2FwAfdQ%3D%3D&licu=urn%3Ali%3Acontrol%3Ad_flagship3_search_srp_co

Szabo, N. (2005). Bit Gold. 2021 tarihinde Satoshi Nakamoto Institute: https://nakamotoinstitute.org/bit-gold/ adresinden alındı.

Szabo, N. (2019). Bit Gold. (M. Gülecen, Editör) 2020 tarihinde Medium: https://medium.com/@mesutgulecen/bit-gold-nick-szabo-türkçe-9787c2d90ade adresinden alındı.

The Economist. (2015). The great chain of being sure about things. https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-aboutthings, [Ziyaret Tarihi: 01.12.2018].

Thinktech STM Teknolojik Düşünme Merkezi, Havacılık Sektörü ve Blockchain- II, https://thinktech.stm.com.tr/uploads/raporlar/pdf/63201815185113_stm_blog_blockchain2.pdf

Thornhill. T. (2016). Inside the Airport Of 2040 Where There Are NO Security Queues Thanks to Super-Fast 'Molecular Scanners'. Retrieved from http://www.dailymail.co.uk/travel/article-3957806/Inside-airport-2040-NO-securityqueues-thanks-super-fast-molecular-scanners.html

Triggs, R. (2018). How Fingerprint Scanners Work: Optical, Capacitive, And Ultrasonic Variants Explained. Retrieved from Web. https://www.androidauthority.com/howfingerprint-scanners-work-670934

TSA (2018). Transportation Security Administration. Retrieved from https://www.tsa.gov

Usta, A., & Doğantekin, S. (2017). Blockchain 101. İstanbul: MediaCat.

Usta, A., & Doğantekin, S. (2018). Blockchain 101 v2. İstanbul: Bankalararası Kart Merkezi.

VisaNet (2019). 20 Nisan 2019 tarihinde https://www.visa.com.tr/visa/visanet.html adresinden alınmıştır.

Wang, L., Shen, X., Li, J., Shao, J., & Yang, Y. (2019). Cryptographic primitives in blockchains. Journal of Network and Computer Applications.

Wang, W. (2018). A Vision for Trust, Security and Privacy of Blockchain. Qiu, M. (Ed.). Smart Blockchain. Springer, 93-98.

Yıldırım, M. (2019). Blok Zincir Teknolojisi, Kripto Paralar ve Ülkelerin Kripto Paralara Yaklaşımları. Bartın Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 10(20), 265-277.

Yılmaz, O. (2019). Block-Chain Teknolojisi ve B2B Finans İşlemlerinde Kullanılabilirliği, İstanbul Aydın Üniversitesi, Fen Bilimleri Enstitüsü.

Zeren, S. K., & Demirel, E. (2020). Turizm Endüstrisinde Yeni Trend: Blockchaın Startup Projeleri. Journal of Tourism Intelligence and Smartness, 3(2), 169-188.

Zheng, B., Zhu, L., Shen, M. (2018). Scalable And Privacy-Preserving Data Sharing Based On Blockchain. J. Comput. Sci. Technol. 33 (3), 557-567