BLOKZİNCİR ALTYAPISI KULLANARAK DİJİTAL KİMLİK DOĞRULAMA

Mustafa Aydın
151402212

YÜKSEK LİSANS TEZİ
Bilgisayar Mühendisliği Anabilim Dalı
Bilgisayar Mühendisliği Tezli Yüksek Lisans
Danışman: Prof. Dr. Oruç Raif Önvural

İstanbul
T.C. Maltepe Üniversitesi
Fen Bilimleri Enstitüsü
Eylül 2019

BLOKZİNCİR ALTYAPISI KULLANARAK DİJİTAL KİMLİK DOĞRULAMA

Mustafa Aydın
151402212
Orcid: 0000-0001-7640-7470

YÜKSEK LİSANS TEZİ
Bilgisayar Mühendisliği Anabilim Dalı
Bilgisayar Mühendisliği Tezli Yüsek Lisans
Danışman: Prof. Dr. Oruç Raif Önvural

İstanbul
T.C. Maltepe Üniversitesi
Fen Bilimleri Enstitüsü
Eylül, 2019



TEŞEKKÜR

Bu araştırmadaki önerileri, yardımları, desteği ve ilgisi için değerli hocam Prof. Dr. Oruç Raif Önvural ve Prof. Dr. Emin Murat Esin'e, yüksek lisans eğitimim boyunca benden bilgisini ve desteğini esirgemeyen tüm hocalarıma sonsuz teşekkürlerimi sunuyorum.

Her zaman beni destekleyen aileme, eşime, oğullarım Fatih ve Akif'e en içten dileklerimle teşekkür ediyorum.

Mustafa Aydın

Eylül 2019

ÖZ

BLOKZİNCİR ALTYAPISI KULLANILARAK DİJİTAL KİMLİK DOĞRULAMA

Mustafa Aydın
Yüksek Lisans Tezi
Bilgisayar Mühendisliği Anabilim Dalı
Bilgisayar Mühendisliği Yüksek Lisans Programı
Danışman: Prof. Dr. Oruç Raif Önvural
Maltepe Üniversitesi Fen Bilimleri Enstitüsü, 2019

İnternet ilk oluşturulduğunda, birbirine bağlanan tüm bilgisayarlar güvenilirdi. Sistem sayısı azdı ve bu sistemleri çalıştıran insanlar birbirlerini tanıyorlardı, bu nedenle sistemler arasında kimin veri gönderdiğini bilmek için mekanizmalara ihtiyaçları yoktu. İnternetteki sistem sayısı arttıkça güven hızla azaldı ve kiminle kimin iletişim kurduğunu tanımlamak için sistemlere birçok mekanizma eklendi. Kullanılan en yaygın mekanizma olan kullanıcı kimlikleri ve şifreleri ile ilgili birçok problem bulunmaktadır.

Kimlik doğrulama, bir kişinin veya bir uygulamanın gerçekte iddia ettiği kişi veya uygulama olduğunun tespit edilmesi amacıyla yapılan işlemler bütünüdür. Kimlik doğrulama yöntemleri, genel olarak donanım tabanlı, biyometrik ve bilgi tabanlı kimlik doğrulama olmak üzere üç bölüme ayrılır. Günümüzde kimlik doğrulama ile ilgili en büyük sorun güvendir. Bugün itibariyle, kişisel veya dijital kimliklerimizin çevrimiçi kimlik doğrulamasını tamamen güvence altına almak için yeterli bir sistem yoktur.

Blokzincir teknolojisi, güvenilir ve merkezi bir otoriteye ihtiyaç duymadan bu soruna bir çözüm getirebilir. Daha spesifik olarak, bireyler ve işletmeler kimliklerini blokzincirde saklayabilir ve doğrulayabilir, bu da kişilerin, kişisel bilgilerine kimin sahip olduğu ve ona nasıl eriştikleri konusunda daha fazla kontrol sahibi olmalarını sağlayabilir. Bu çalışma kapsamında blokzincir teknolojisi incelenerek, digital kimlik doğrulama sisteminin nasıl olması gerektiği incelenmiştir.

Anahtar Sözcükler: Blokzincir; Hyperledger; Dağıtık Kayıt Defteri; İş İspatı; Merkle Ağacı; Şifreleme; Kimlik Doğrulama; Dijital Kimlik.

ABSTRACT

DIGITAL IDENTITY VERIFICATION USING BLOCKCHAIN FRAMEWORK

Mustafa AYDIN
Master Thesis
Department of Computer Engineering
Computer Engineering Programme
Advisor: Prof. Dr. Oruç Raif ÖNVURAL
Maltepe University Graduate School of Science and Engineering, 2019

When the Internet was first created, all of the computers were securely connected. Because there were only a few systems run by operators knowing each other, they didn't need any mechanisms to determine the sender of any data between these systems. However, as the number of systems within the Internet increased, this level of trust had a sharp fall and many mechanisms were incorporated into the systems to define the communicating parties. The most common mechanisms are user IDs and passwords, which are associated with many problems.

Authentication is the process of verification of the claims related to the real identity of a person or an application. The methods of authentication are categorized into three main groups: hardware-based, biometric and knowledge-based authentication. Security is the most important problem in modern authentication. Today, we still don't have an adequate system to secure online authentication of our personal or digital IDs.

Blockchain technology can offer a solution for this problem without the need for a reliable central authority. More specifically, individuals and organizations can store and verify their identities in a blockchain, enabling individuals to have more control over their personal information being shared and accessed by other parties. This study analyzes blockchain technology to determine how a digital authentication system should work.

Keywords: Blockchain; Hyperledger; Distributed Ledger; Proof of Work; Merkle Tree; Encryption; Authentication; Digital Identity.

İÇİNDEKİLER

JÜRİ VE ENSTİTÜ ONAYI ..... İ
ETİK İLKE VE KURALLARA UYUM BEYANI ..... İV
TEŞEKKÜR ..... İV
ÖZ V
ABSTRACT ..... Vİ
İÇİNDEKİLER ..... Vİİ
TABLOLAR LİSTESİ ..... İX
ŞEKİLLER LİSTESİ X
KISALTMALAR ..... Xİİ
ÖZGEÇMİŞ ..... Xİ V
BÖLÜM 1. GİRİŞ 1
BÖLÜM 2. BLOK ZİNCİR 3

2.1.Kriptoloji 6
2.1.1.Simetrik Şifreleme 7
2.1.2.Asimetrik Şifreleme 8
2.1.3.Özetleme(Hash) Fonksiyonları 10
2.1.4.Sayısal İmza 11
2.1.5.Gizlilik ve Kimlik Denetimi 12
2.2.Blok 13
2.2.1.Genesis Blok 14
2.2.2.Blok Yapısı 14
2.2.3.Blok Başlığı 15
2.3.İşlemler 18
2.4.Dağıtılmış Hesap Defteri 21
2.5.Uzlaşma Yöntemleri 23
2.6.Madencilik 27
2.7.Çatallanma 28
2.8.Yetim Blok 29
2.9.Blokzincir Platformları 30
2.9.1.Etherum 32
2.9.2.Hyperledger 32
2.9.3.R3 Corda 35
2.9.4.Ripple 35
2.9.5.Quorum 36
2.9.6.EOS 36
2.9.7.OpenChain 36
2.9.8.Stellar 37
2.10.Blokzincir Uygulama Alanları 37
BÖLÜM 3. KİMLİK DOĞRULAMA METOTLARI 39

3.1.Donanım Tabanlı Kimlik Doğrulama 40
3.2.Biyometrik Kimlik Doğrulama 41
3.3.Bilgi Tabanlı Kimlik Doğrulama 41
BÖLÜM 4. BLOKZİNCİR TABANLI GELİŞRİRİLEN KİMLİK DOĞRULAMA UYGULAMALARI 43

4.1.The CivicApp 43
4.2.SecureKey and IBM Blockchain 44

4.3.MONI 44
4.4.E-Stonia 45
4.5.Kimlic 45
4.6.Persona 46
4.7.Object Tech 46
4.8.SelfKey 47
4.9.OVCODE 47
4.10.Authenteq 48
BÖLÜM 5. HYPERLEDGER INDY İLE DİJİTAL KİMLİK DOĞRULAMA UYGULAMASI 49
5.1.Temel Kavramlar 49
5.2.Kimlik Doğrulama Uygulaması 54
BÖLÜM 6. SONUÇ 64
KAYNAKÇA 66

TABLOLAR LİSTESİ

Tablo 1. Blok yapısı 14

Tablo 2. Blok başlığı 15

Tablo 3. İşlem veri yapısı 19

Tablo 4. Blokzincir platformları 32

ŞEKİLLER LİSTESİ

Şekil 1. Blokzincir çalışma mantığı 5

Şekil 2. Blokzincir teknolojisinin geleceği 6

Şekil 3. Şifreleme teknikleri 7

Şekil 4. Simetrik şifreleme..... 8

Şekil 5. Asimetrik şifreleme 9

Şekil 6. Eliptik eğri şifrelemesi..... 9

Şekil 7. SHA-256 özet fonksiyonu örneği 10

Şekil 8. Mesajın imzanlanması ve doğrulanması 12

Şekil 9. Blokların birbirlerine eklenerek zincir oluşturması 14

Şekil 10. Blok başlığı..... 15

Şekil 11. Merkle ağacındaki düğümlerin hesaplanması 16

Şekil 12.Zorluk seviyesi 18

Şekil 13. Blokzincir işlem yapısı 19

Şekil 14. Merkezi, çok merkezli ve dağıtık ağ yapıları 21

Şekil 15. Dağıtık işlem kayıtları sınıflandırılması 23

Şekil 16. Bitcoin ağının özetleme kapasitesi 28

Şekil 17. Yetim blok..... 29

Şekil 18. Hyperledger ekosistemi 33

Şekil 19. Kimlik doğrulama metotların sınıflandırılması 40

Şekil 20. Dağıtılmış tanımlayıcı 50

Şekil 21.Şema ve kimlik tanımı arasındaki ilişki 55

Şekil 22.Elif'in transkript alması 56

Şekil 23.Elif, Doruk A.Ş için ispat oluşturması 57

Şekil 24.Elif'in Maltepe Üniversitesine bağlantı isteği göndermesi 58

Şekil 25. Elif için Maltepe Üniversitesi ile ilişki onayı 58

Şekil 26. Maltepe Üniversitesi için Elif ile ilişki onayı 59

Şekil 27. Maltepe Üniversitesinin kimlik teklifi göndermesi 59

Şekil 28. Elif'in kimliği kabul etmesi 60

Şekil 29. Elif'in Doruk A.Ş'ye bağlantı isteği göndermesi 60

Şekil 30. Elif için Doruk A.Ş ile ilişki onayı 61

Şekil 31. Doruk A.Ş için Elif ile ilişki onayı 61

Şekil 32. Doruk A.Ş'nin kimlik bilgilerini istemesi 62

Şekil 33. Elif'in Doruk A.Ş ile kimlik bilgilerini paylaşması 62

Şekil 34. Doruk A.Ş, Elif'e ait kimlik bilgilerini doğrulması 63

KISALTMALAR

DES : Veri Şifreleme Standardı

DEA : Veri Kodlama Algoritması

NBS : Ulusal Standartlar Bürosu

DHKE : Diffie-Hellmann Anahtar Değişim Algoritması

ECC : Eliptik Eğri Algoritması

SHA : Güvenli Özet Algoritması

ECM : Eliptik Eğri Çarpımı

UTXO : Gönderilmeyen İşlem Çıktısı

DLT : Dağıtık Defter Teknolojisi

BFT : Bizans Hata Toleransı

PoW : İş İspatı

PoS : Pay İspatı

ICO : Dijital Para Arzı

EVM : Etherum Sanal Makinesi

IoT : Nesnelerin İnterneti

SDK : Yazılım Geliştirme Kiti

PoET : Geçen Zamanın Kanıtı

XRP : Ripple

ETH : Etherum

SCP : Stellar Konsensüs Protokolü

KYC : Müşteri Tanıma İşlemleri

TKŞ : Tek Kullanımlık Şifre

ATM : Otamatik Para Makinesi

PIN : Kişisel Kimlik Numarası

AB : Avrupa Birliği

API : Uygulama Programlama Arayüzü

ID : Kimlik

DID : Dağıtılmış Tanımlayıcı

W3C : Dünya Web Konsorsiyumu

ZKP : Sıfır Bilgi Kanıtı

RBFT : Yedekli Bizans Hata Toleransı

ÖZGEÇMİŞ

Mustafa AYDIN

Bilgisayar Mühendsiliği Anabilim Dalı

Eğitim

Derece	*Yıl*	*Üniversite, Enstitü, Anabilim/Anasanat Dalı*
Y.Ls.	2019	Maltepe Üniversitesi, Fen Bilimler Enstitüsü Bilgisayar Mühensliği Anabilim Dalı
Ls.	2007	Sakarya Üniversitesi, Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü
Lise	1997	Adıyaman Lisesi

İş/İstihdam

Yıl	*Görev*
2012 -	Kıdemli Yazılım Uzmanı. Vakıfbank
2009- 2012	Yazılım Uzmanı. Albarakatürk

Kişisel Bilgiler

Doğum yeri ve yılı	: Besni, 1981Cinsiyet:E
Yabancı diller	: İngilizce
GSM / e-posta	: 05321648727 / mustafa.aydin02@gmail.com

BÖLÜM 1. GİRİŞ

Çevrimiçi işlemlerin çoğu, bireylerin hizmetlere erişebilmek için bazı kişisel bilgilerini açıklamasını gerektirir. Örneğin, Amazon Pay, PayPal ve Google Cüzdan gibi platformlarda finansal işlemler gerçekleştirilmeden önce, kullanıcıların her zaman kayıt ve giriş bilgilerini girmeleri gerekir ve zaman için bu bilgi birçok veri veritabanında saklanır ve farklı platformlarda var olmaya başlarlar, bu da birçok güvenlik sorununun başlangıcını oluşturur. Kimlik bilgileri gizlilik içeren bilgilerdir. Çevrimiçi veritabanlarında yer alan bilgiler, kişinin izni olmaksızın üçüncü taraflarla paylaşılabilir veya çalınabilir.

2018'de 4,5 milyar kişisel veri kayıdı sızdırıldı. (www.cbronline.com, 2018) Facebook, Google ve Amazon, 2018'de büyük miktarda müşteri verisini güvende tutamayan üç büyük şirkettir. Şirketler verilerimizi güvende tutmayı başarsalar bile, kimliğimize olan sahipliğimizi kaybediyoruz.

Kimlikle ilgili problemleri aşağıdaki gibi tanımlayabiliriz.

- Kullanıcı kimlikleri / parolalar normdur, ancak çok fazla parolaya sahip olduğumuzda bunlar yönetmek zordur.
- Kimliğimizi kanıtlamak için başka türlü kullanabileceğimiz diğer kişisel bilgiler ve tanımlayıcılar güvenilir değildir, çünkü verilerin gerçekten kişiye ait olup olmadığını söylemek mümkün değildir.
- Kullanabileceğimiz kimlik özellikleri güvenilir olmadığından kendimiz hakkında bir şeyler ispatlamak için sık sık kağıt belgelere başvurmak zorunda kalırız.
- Kullandığımız tanımlayıcılar, siteler arasında ilişkilendirilir ve hakkımızda çıkarımlar yapılmasına izin verir.
- Tanımlayıcıların merkezileştirilmiş veritabanları ve bu tanımlayıcılarla ilişkili insanlar hakkındaki veriler bilgisayar korsanları tarafından hedeflenmektedir ve sık sık çalındığı hakkında haberler çıkmaktadır.
- Merkezi tanımlayıcılar, bu tanımlayıcıları kontrol edenler tarafından kötüye kullanılabilir.

Yukarıda vurgulanan sorunlar tek bir gerçeğe işaret etmektedir; mevcut çevrimiçi kimlik yönetim sistemleri sürdürülebilir olmaktan uzaktır.

Blokzincir altyapısı kullanılarak kişilerin kimliklerini hırsızlığa karşı koruyan ve hileli faaliyetleri büyük ölçüde azaltan bir platform oluşturulabilir. Blokzincir tabanlı kimlik doğrulama sistemi, bireylere güvenli olarak birden fazla kullanıcı adı ve şifreyi değiştirecek şifreli dijital kimlikler oluşturma özgürlüğü sunar. Bu teknoloji aynı zamanda kullanıcıların farklı işlem ortamlarında paylaşmak istediği verileri belirlemesine, aynı zamanda kimlik hırsızlığı ve dolandırıcılık gibi işlemlerden korunmalarına yardım edebilir.

Bu çalışmada merkezi olmayan, açık kaynaklı blokzincir platformu kullanılarak, bir kimlik yönetim sistemi geliştirilecektir. Bu sistemde dijital kimlik oluşturulduktan sonra herhangi bir hizmet için, oluştulan kimliği doğrulamak için güvenilmez şifre / e-posta kombinasyonlarına ihtiyaç olmayacaktır.

Bu çalışmanın birinci bölümünde kimlik ile ilgili problemler tanımlanmış, ikinci bölümde blokzincir teknolojisinin mimarisi, yapısı, sahip olduğu özellikleri, kriptoloji ve en çok kullanılan blokzincir platformları incelenmişitir. Üçüncü bölümde kimlik doğrulama ve kimlik doğrulama metotları incelenmiştir. Dördüncü bölümde blokzincir teknolojisi kullanılarak geliştirilmiş örnekler incelenmiştir. Beşinci bölümde digital kimlik geliştirmek için tasarlanan hyperlenger iny incelenmiş ve önyüz uygulaması geliştirilmiştir.

Bu tez kapsamında, blokzincir ile ilgili bilgiler verilirken ilk olması ve en çok bilinmesinden dolayı “Bitcoin” teknolojisi ve çalışma presipleri ile incelenmiştir.

BÖLÜM 2. BLOK ZİNCİR

Blokzincir, ilk olarak 31 Ekim 2008 tarihinde Satoshi Nakamoto tarafından yayınlanan "Bitcoin:Eşler Arası Elektronik Nakit Sistemi" (Bitcoin: A Peer-to-Peer Electronic Cash System) adlı makalesiyle ortaya çıkmıştır. (Nakamoto, 2008) Satoshi Nakamoto, 2009 yılında Bitcoin yazılımını geliştirerek sistemin kurulmasını sağlamıştır. Nakamoto, 2010 yılı ortalarına kadar Bitcoin sistemini geliştirmeye devam etmiş ve ardından projeden desteğini çekerek ortadan kaybolmuştur.

Birinci internet devrimi müzik, video, doküman, haberleşme gibi veri transferi sağlarken blokzincir teknolojisi, bu verilerin haricinde değer atfedilen para, kimlik gibi varlıkların da transfer edilmesini sağlayan güvenilir dağıtık veritabanıdır. (www.tubitak.gov.tr, 2019)

Blokzincir kriptografi sistemi ile üretilen veri bloklarından oluşur. Blokzincir sistemi güvenilir bir merkez olmadan eşler arasında işlem yapılabilecek bir yapı sunmaktadır. Buna ek olarak teknolojisi sayesinde geriye dönük işlemlerin izlenebilirliğini sağlar ve yapılan işlemlerin değiştirilmesini engeller. Bu sistemde güvenilir üçüncü bir tarafa ihtiyaç duyulmaz ve maliyetler düşürülür. (Beck & diğerleri., 2016)

Kullanıcılar, başka bir kuruluşa kaydolmayı gerektiren merkezi bir hesaba ihtiyaç duymamaktadır. Bir adrese ait özel anahtar mevcut ise internet'e bağlı herhangi bir bilgisayar ve akıllı telefondan özel anahtar kullanarak bu adres ile ilişkilendirilmiş olan hesap yönetilebilinir.

Bitcoin blokzincir teknolojisi, dijital paranın yeni bir biçimini elde etmek için BitTorrent gibi eşler arası dosya paylaşım teknolojisine benzer bir biçimde açık anahtar şifreleme yöntemini birleştirerek çifte harcama sorununu çözmektedir. Paranın mülkiyeti kamuya açık muhasebe defterine kaydedilirken, bitcoin kriptografik protokoller ve madencilik topluluğu tarafından teyit edilmektedir

Açık kaynak kod kullanan blokzincir protokollerinde tüm kullanıcılar, blokzincir kodunun herhangi bir güvenlik kusuru veya bir arka kapı içerip içermediğini kontrol edebilmektedir. Blokzincirdeki tüm işlemlere ilişkin bilgiler tüm kullanıcılar tarafından erişilebilir durumdadır. Bu şeffaflık, tüm kullanıcıların diğer kullanıcıların kopyalarıyla

tutarlı olması için defterin/kayıtların kopyasını kontrol etmelerini sağlamaktadır. Ayrıca düzgün olarak bağlı herhangi bir düğüm, veri kümesinde bir işlemin mevcut olup olmadığını belirli bir kesinlik ile doğrulayabilmektedir. Bir işlemi oluşturan herhangi bir düğüm doğrulama sonrası işlemin geçerli olup olmadığını, gerçekleşip gerçekleşemeyeceğini makul bir düzeyde belirleyebilmektedir. Diğer bir ifadeyle, yeni işlem girişini geçersiz kılacak herhangi bir çelişkili işlem veya kripto parabiriminin başka bir yerde harcanması (iki defa harcanması) gibi işlemler onaylanmamaktadır. (Gronbaek, 2016)

Blokzincir farklı kullanım alanlarına göre değişik özelliklere sahibtir. Genel olarak servisleri üç temel unsurdan oluşur. (www.hyperledger.org, 2016)

- Eşler Arası Protokol
- Dağıtık Kayıt Teknolojisi
- Fikir Birliği Protokolü

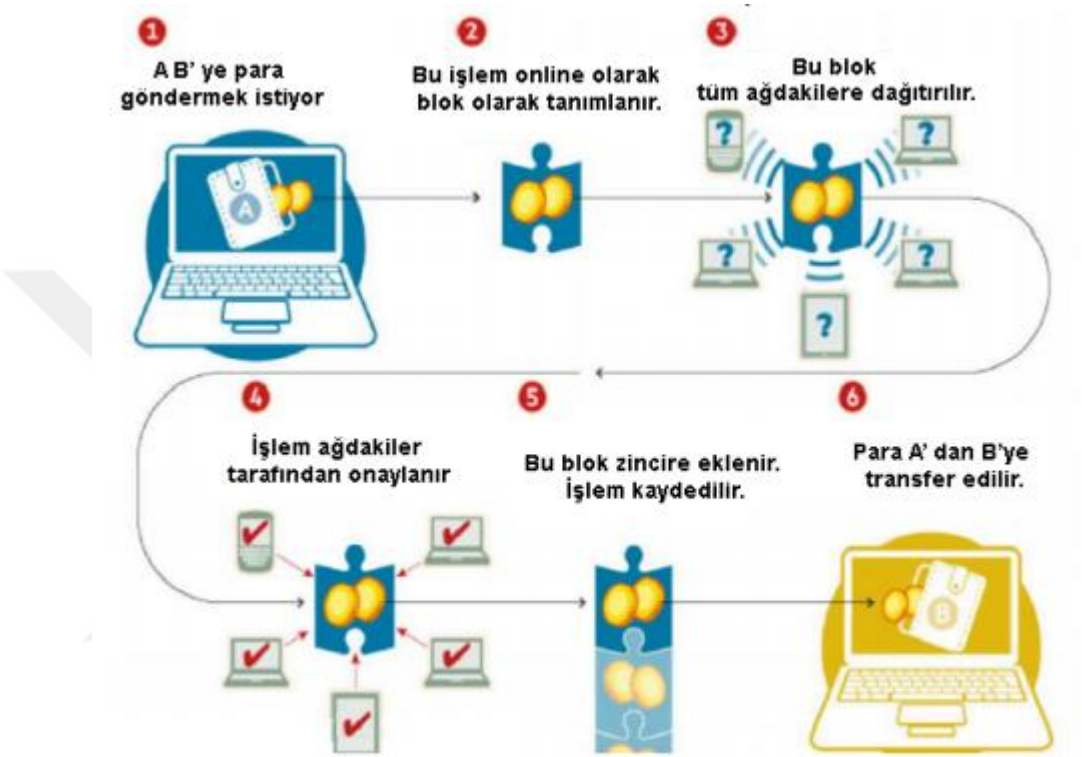
Düğümler daima en uzun zinciri doğru olarak kabul eder ve bu zincire blok eklemeye çalışır. Eğer birden fazla farklı düğüm, yeni üretilen bloğun iki ayrı versiyonunu yayınlarsa, diğer düğümler bunlardan herhangi birini alabilir. Bu durumda düğümler ilk aldıkları bloğu doğru kabul edip zinciri uzatmaya devam ederler, diğer bloğu da daha fazla genişleme olasılığına karşı saklarlar. Eşitlik bir sonraki iş kanıtı bulunduğunda ve zincirlerden birisi daha uzun olduğunda bozulmuş olacaktır. Kısa kalan zincirde çalışan düğümler de uzun zinciri alıp genişletmeye çalışıcaktır.

Eklenen yeni blokların bütün düğümlere ulaşması gerekli değildir. Belirli bir sayıda düğüme eriştiklerinde çok beklemeden bloğa dahil olacaklardır. Blok yayınları mesaj kayıplarına karşı toleranslıdır. Bir düğüm yeni üretilen bloğu alamazsa bir sonraki bloğu aldığında kaçırdığı bloğu fark eder ve talep eder.

Ağı çalıştırmak için gereken adımlar şunlardır; (Nakamoto, 2008)

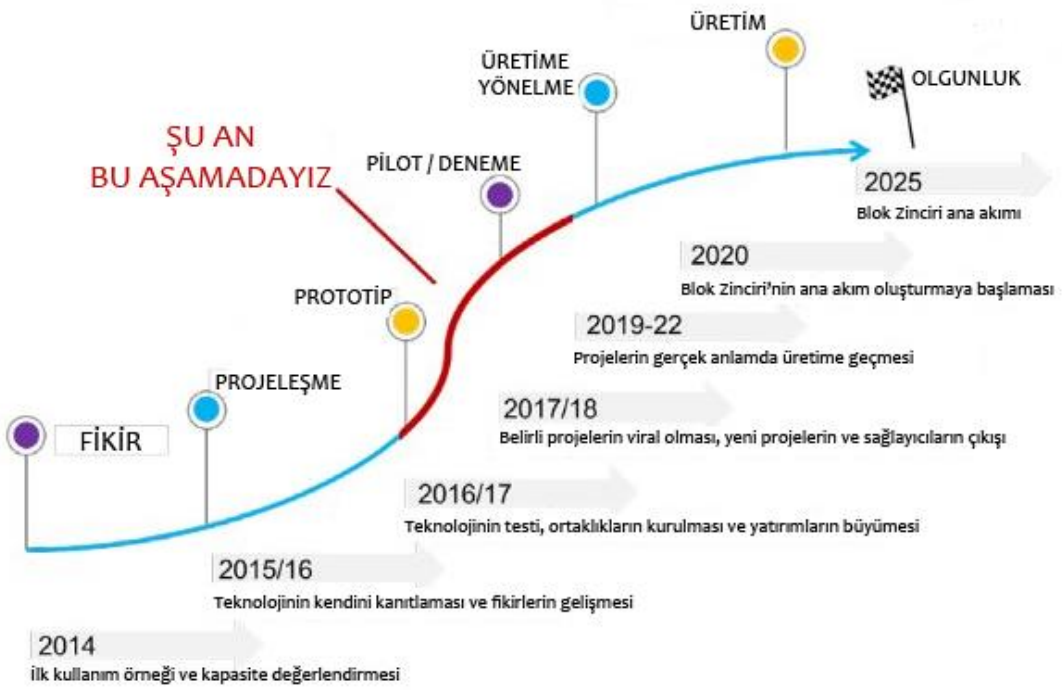
- Her yeni işlem bütün düğümlere yayınlanır.
- Bütün düğümler yeni işlemleri blok içine alır.
- Bütün düğümler kendi üreteceği blok için iş kanıtı bulmaya çalışır.
- İş kanıtını bulan ilk düğüm, diğer bütün düğümlere bu kanıtı gönderir.

- Düğümler blok işindeki bütün işlemler doğrulanmışsa ve daha önce harcanmamışsa bloğu kabul eder.
- Düğümler, kabul edilen bloğun özet değerini kullanarak zincirdeki yeni bloğu oluşturmaya çalışır.



Şekil 1. Blokzincir çalışma mantığı (Crosby & diğerleri., 2016)

Kripto paraların finans piyaslarını etkilenmesiyle birlikte öncelikle merkez bankaları, devlet kurumları, büyük bankalar ve teknoloji şirketleri blokzincir teknolojisini araştırmakta ve bu teknoloji ile ilgili yatırım yapmaktadırlar. Ayrıca birçok teknoloji şirketi blokzincir teknolojisinin geliştirilmesi ile ilgili işbirliği oluşturdukları bilinmektedir.



Şekil 2. Blokzincir teknolojisinin geleceği (www.businessinsider.com, 2018)

2.1.Kriptoloji

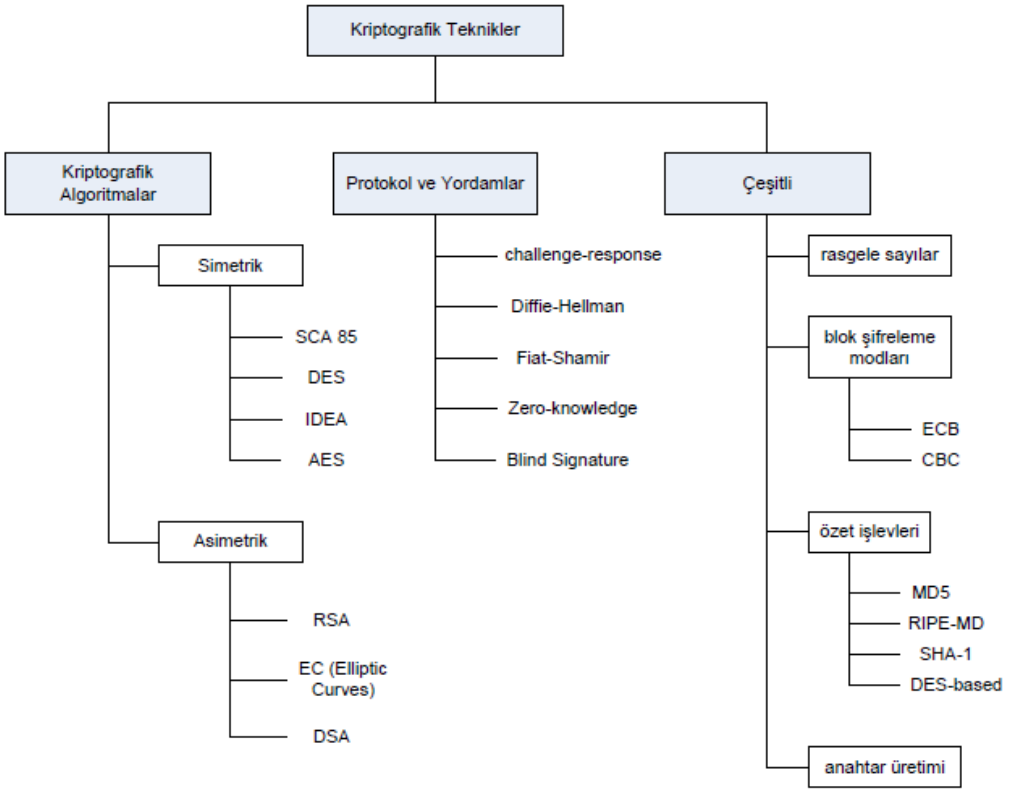
Kriptoloji, köken olarak eski Yunanca'da yer alan "kryptos logos" kelimelerinin birleşmesinden oluşmaktadır. Kryptos kelimesi gizli anlamına, logos ise bilim anlamına gelmektedir. Kriptoloji kavramı temel olarak kriptografi ve kriptoanaliz olmak üzere iki alana ayrılır. Kriptografi verilerin şifrelenmesi ve deşifrelenmesi ile ilgili yöntemler, Kriptoanaliz ise varolan kriptografik sistemlerin kırılması ile ilgili çalışmalar yapan bilim dalıdır.

Kriptografi ile dört temel amaç sağlanmaya çalışılır. *Gizlilik;* gönderilen bilginin bir başkası tarafından okunamaması, *Bütünlük;* gönderilen bilginin karşı tarafa değişmemiş olarak ulaşması, *Asıllama;* göndericinin gönderdiği kişiyi doğrulaması, *Paketleme(kaplama);* ise kaba kuvvet saldırılarına karşı durma olarak özetlenebilir. (Stallings, 2000)

Kriptografik algoritmalar kullanılan anahtara bağlı olarak Simetrik ve Asimetrik olmak üzere iki ayrı gruba ayrılırlar. Simetrik algoritmalarda şifreleme ve deşifreleme

için kullanılan anahtar aynı anahtardır. Asimetrik algoritmalarda ise şifreleme için kullanılan anahtar ile deşifreleme için kullanılan anahtar farklıdır.

Şekil 3.'de bilinen en temel kriptografik yordamlar ve tekniklerle ilgili bir sınıflandırma gösterilmektedir.

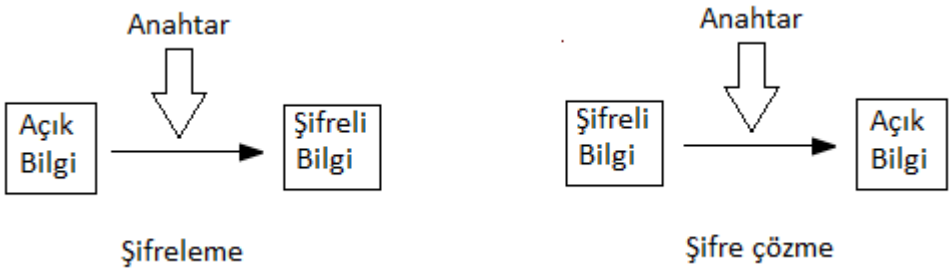


Şekil 3. Şifreleme teknikleri (Başak, 2014)

2.1.1.Simetrik Şifreleme

1940'lı yılların sonlarında Caulde Shannon'un yayınladığı teorik makale simetrik veya gizli anahtarlı şifrelemenin temellerini oluşturmuştur. Bu çalışmada önerilen simetrik anahtarlama yöntemi birçok modern kriptografi sistemin temeli olmuştur. (Shannon, 1946)

Simetrik kriptografik algoritmalar aynı gizli anahtar kullanılarak bir verinin hem şifrelenmesi hem de deşifrelenmesi temeline dayanarak gerçekleştirilen algoritmalardır.



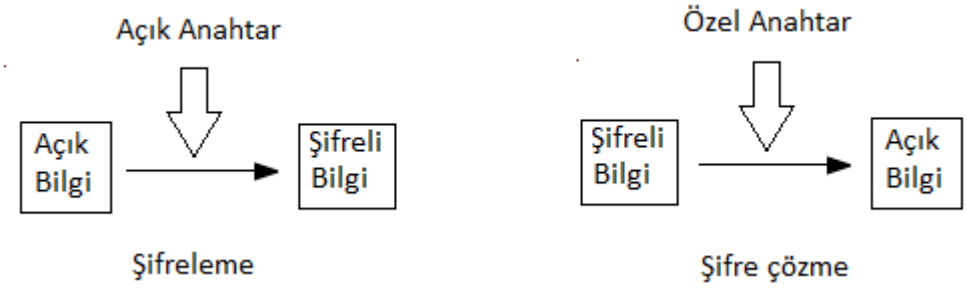
Şekil 4. Simetrik şifreleme

DES Algoritması: IBM tarafından 1977 yılında geliştirilen ve DEA (Data Encription Algorithm) olarak tanımlanan algoritma daha sonra NBS (US National Bureau of Standarts) tarafından standartlaştırılarak DES adını almıştır. DES, en iyi bilinen ve en yaygın kullanılan simetrik şifreleme algoritmasıdır.

2.1.2.Asimetrik Şifreleme

1976 yılında Whitfield Diffie ve Martin E. Hellman biri açık diğeri özel olan iki farklı anahtar kullanarak şifreleme algoritması geliştirilebileceğini gösterdiler. (Diffie-Hellmann Key Exchange Algorithm – DHKE). Asimetrik algoritmalar, kişilerin açık (public) anahtar ile şifreledikleri bir bilgiyi sadece özel (private) anahtara sahip kişi tarafından deşifre edilebildiği bir algoritmadır.

Asimetrik diğer bir ismiyle açık anahtarlı kriptografik sistemlerde şifreleme ve şifre çözme için kullanılan anahtarlar birbirinden farklıdır. Bu tür sistemlerde her kullanıcının açık ve özel olmak üzere bir çift anahtarı vardır. Bu anahtarların en önemli özelliği anahtarlardan hiçbiri hem şifreleme hem de şifre çözme işleminde kullanılamaz. Anahtarlardan birinin şifrelediğini ancak ve ancak diğer anahtar açmaktadır. Bu anahtarlardan açık olanı herkes tarafından bilinmektedir. Özel anahtar ise yalnızca anahtar sahibi tarafından bilinmektedir. Ayrıca bir kişiye ait açık anahtardan yola çıkarak özel anahtarının hesaplanması teorik olarak çok zordur. Bu zorluğu anahtarlar arasındaki çarpanlara ayırma veya ayrık logaritma problemlerinin çözüm güçlüğü gibi matematiksel yöntemler sağlamaktadır. (Dulaney, 2011)



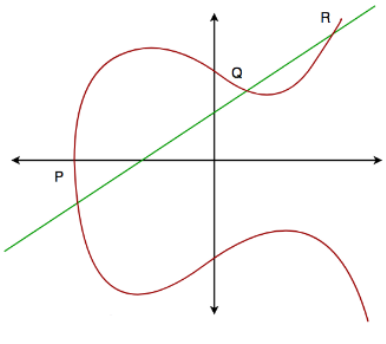
Şekil 5. Asimetrik şifreleme

RSA Algoritması: 1978 yılında, Ronald L. Rivest, Adi Shamir ve Leonardo Adleman yukarıdaki kriterleri sağlayan RSA(soyisimlerinin başharfleri) adında bir algoritma sundular. Bu algoritma büyük sayı aritmetiğine dayanan oldukça basit çalışma prensibi olan bir algoritmadır. Her iki anahtarda büyük asal sayılardan üretilir.

Açık anahtar ve özel anahtar arasındaki matematiksel ilişki tek yönlü kabul edilir. Açık anahtarın kilitlediği belgeyi özel anahtar ile açmak çok kolaydır. Ancak açık anahtar kullanarak özel anahtarı elde etmek neredeyse imkansızdır. Bu nedenle açık anahtar herkesle paylaşılabilir.

Eliptik Eğri Algoritması(ECC): 1985 yılında birbirlerinden habersiz Victor Miller ve Neal Koblitz tarafından asimetrik kriptografik algoritmalar oluşturmak için eliptik eğrileri kullanarak geliştirilen bir algoritmadır.

Eliptik eğriler sonlu üç boyutlu uzayda $y2 = x3 + ax + b$ denklemini sağlayan eğrilerin bir kümesidir. ECC'nin güvenirliği eliptik eğri ayrık logaritmik problemin zorluğuna dayanır.



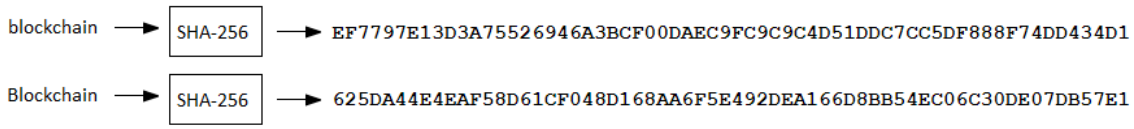
Şekil 6. Eliptik eğri şifrelemesi

Bu fonksiyonun en belirgin özelliği; y eksenine göre simetrik olması ve herhangi bir noktadan çizilen bir doğrunun toplamda 3 noktadan geçmesidir.

ECC ile yapılan şifreleme kolayca uygulanabilmekte ancak çıktıdan girdiyi elde etmek oldukça zordur. ECC diğer kriptografik tekniklere kıyasla daha küçük boyuta ve daha hızlı anahtar üretimi sağlar. 3072 bitlik RSA'nın sağladığı güvenliği ECC256 sağlayabilmektedir. Kripto para güvenliğinde genellikle ECC şifreleme yöntemi tercih edilmektedir.

2.1.3.Özetleme(Hash) Fonksiyonları

Özetleme fonksiyonları, herhangi uzunluktaki bir veriyi sabit uzunlukta bir veriye dönüştüren ve aynı girdinin her zaman aynı çıktıyı verdiği tek yönlü fonksiyonlardır. Girdi işleminde yapılan en küçük bir değişiklik, çıktı değerini tamamen değiştirir.



Şekil 7. SHA-256 özet fonksiyonu örneği

Özetleme fonksiyonları modern kriptografide veri bütünlüğünü kontrol etmek için kullanılmaktadır. Haberleşmede gönderici taraf iletmek istediği veriyi bu fonksiyonlar ile işleme sokar ve özet değeri elde eder. Veri ve özet değer alıcıya gönderilir, alıcı verinin tekrar özetini alır ve karşı tarafın gönderdiği özet ile kıyaslar. Eğer özetler eşlenirse veri iletim kanalından değişmeden geldiği ispatlanmış olur. (Yıldırım, 2014)

Özetleme fonksiyonlarının güvenli ve verimli bir sekilde kullanılabilmeleri için birtakım gereksinimleri yerine getirmeleri gerekmektedir. Bu gereksinimler asağıdaki gibi maddelendirilebilir. (Stallings, 2000)

- H fonksiyonu uzunluğuna bağımlı olmaksızın bütün mesajlara uygulanabilmelidir.
- H fonksiyonu her türlü girdi için sabit bir çıktı üretmelidir.

- Herhangi bir (x) girdisi için H(x) kolayca hesaplanabilir olmalı, yazılımsal ve donanımsal olarak uygulanabilir olmalıdır.
- H(x)=h olacak şekilde h'nin bilinen değerleri için x değerinin hesaplanabilmesi zor olmalıdır. Bu, fonksiyonun tek yönlü özelliği olarak da bilinmektedir. Bu özellik olmazsa gizli değer kullanılarak gerçekleştirilen bir iletişim ortamında, hattı dinleyerek mesaj ve şifrelenmiş mesajdan elde edilen hash değeri bilgisine sahip olan saldırgan, fonksiyonu tersi yönüne işleterek gizli değeri elde edebilir.
- x'in bilinen değerleri için x'e eşit olmayan ancak H(y)=H(X) eşitliğini sağlayan bir y değerinin hesaplanması güç olmalıdır. Bu durum zayıf çarpışma direnci olarak adlandırılmaktadır. Bir mesajın, alternatifi olan bir mesaj için birbirine eşit hash değerlerinin hesaplanması çok zordur.
- H(x)=H(y) olacak şekilde (x,y) ikilisinin hesaplanması güç olmalıdır. Bu durum güçlü çarpışma direnci olarak da bilinmektedir.

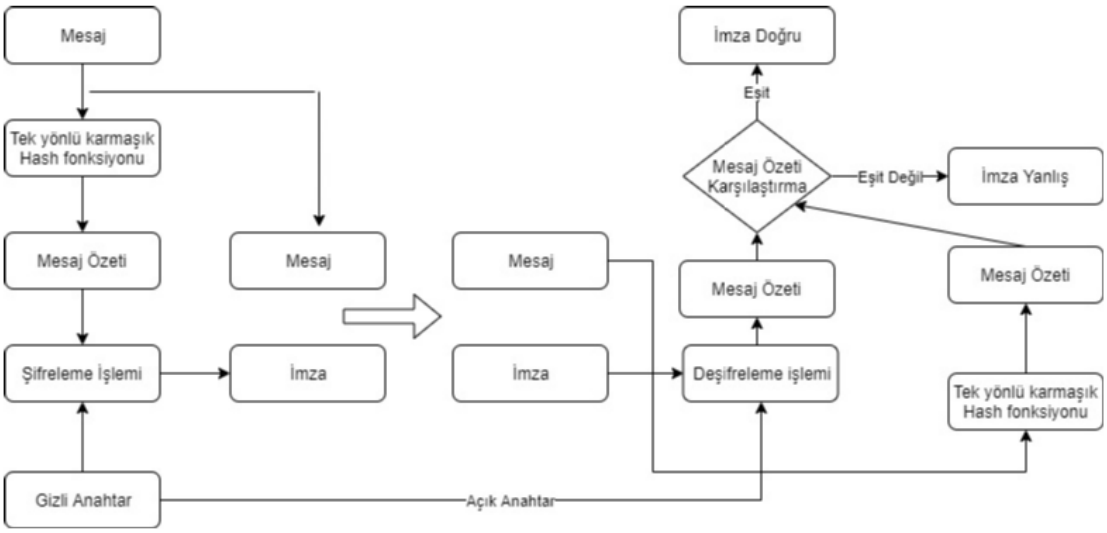
Blokzincir teknolojisinde özet oluşturma işlemlerinde SHA-256 algoritması kullanılır. Bu algoritma SHA-2 algoritma ailesisinin alt dalıdır. (Murat, 2014)

SHA-256 algoritması ile girdi işleminden bağımsız olarak her zaman 256-bit(32 byte) bir özet oluşur. Özet değeri 256 adet 0 veya 1 den oluşmuş dizedir. SHA-256 algoritması en güvenilir özetleme fonksiyonlarından biridir. Özet değerinden girdi işleminin ne olduğu anlaşılamaz. 256 adet 0 veya 1 den oluşmuş bir dizeden $2^{256} \approx 1.15 \times 10^{77}$farklı çıktı üretilebilir. Bu değer oldukça büyüktür. Bu değerlerin oluşturduğu kümede çakışmanın olabilmesi için en az 2^{128} deneme yapılmalıdır. Mevcut işlemci kapasitesi ile böyle bir deneme yapılması çok zordur.

2.1.4.Sayısal İmza

Güvenirliği matematiksel olarak ispatlanmış, gizli ve açık anahtar çifti ile çalışan şifreleme işlemidir. Sayısal imzayı kullananmak isteyen bir kişinin güvenilir bir otoriteden gizli ve açık anahtar çiftini alması gerekir. Gizli anahtar ile şifrelenen girdi, yalnızca gizli anahtar çiftine ait açık anahtar ile çözülür. Gizli anahtar kişiye özeldir ve sadece sahibi tarafından bilinir. Açık anahtar mesaja ek olarak gönderilebileceği gibi paylaşılmasında da herhangi bir sakınca yoktur. (Çarkacıoğlu, 2014)

Gizli anahtar kullanılarak açık anahtar elde edilir. Bu işlem için eliptik eğri çarpım (elliptic curve multiplication, ECM) yöntemi kullanılır. Bu yöntemde gizli anahtar, açık anahtardan elde edilemediği tek yönlü bir işlemdir. (Antonopoulos, 2014)



Şekil 8. Mesajın imzanlanması ve doğrulanması (Yüksel, 2006)

2.1.5. Gizlilik ve Kimlik Denetimi

Veri güvenliği için gizlilik yöntemi aşağıdaki şekilde sağlanmaktadır:

- Şifreleme ve şifre çözme için kullanılacak anahtarlar önceden oluşturulur.
- Şifreleme anahtarı(açık anahtar – public key) herkesçe erişilebilecek bir şekilde paylaşılır. Özel anahtar gizli tutulur.
- A kişisi tarafından, sadece B kişisinin görüntüleyebileceği bir mesaj göndermek isterse mesajı B kişisinin açık anahtarı ile şifreler.
- B kişisi, gelen mesajı özel anahtarı ile şifresini çözer. Bu mesajı elde eden başka hiç kimse çözemez, mesajı çözecek özel anahtarı yalnızca B kişisi tarafından bilinmektedir.

Yukarda yapılan işlemlerle B kişisi kendisinden başka hiç kimsenin okuyamadığı bir mesaj alır. Bu durumda gizlilik sağlanır ama mesajın kimden geldiği bilinmez. (Yerlikaya, 2006)

Yukarıda yapılan işlemlerin son iki adımı aşağıdaki gibi gerçekleştiğinde kimlik denetimi de gerçekleştirilmektedir:

- A kişisi, B kişisine mesajın A kişisinin tarafından gönderildiğine emin olmasını istiyorsa mesajı kendi gizli anahtarı ile şifreler.
- B kişisi gelen mesajı A kişisinin açık anahtarıyla çözer. A kişisinin açık anahtarı herkes tarafından bilindiği için A ve B dışındaki diğer alıcılarda bunu yapabilir. B kişisi bu senaryo ile mesajı A kişisinin gönderdiğini ve bir değişikliğe uğramadığını bilir. Çünkü A kişisine ait özel anahtar ile şifrelenen mesaj yalnızca A kişisinin açık anahtarıyla çözülebilir.

Bu durumda gizlilik yerine kimlik denetimi sağlanır. Hem gizlilik hem de kimlik denetiminin sağlanması için işlemler aşağıdaki gibi gerçekleştirilmelidir.

- A kişisi, B kişisine mesajın A kişisi tarafından gönderildiğine ve başka hiç kimseninin bu mesajı görüntülemediğinden emin olmasını isterse, kendi gizli anahtarı ile şifrelediği mesajı B kişisinin açık anahtarı ile şifreler.

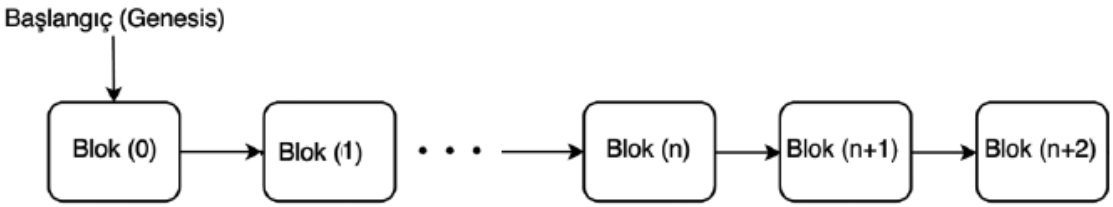
Bu durumda hem gizlilik hem de iki taraflı kimlik denetimi sağlanır. (Eren, 2005)

2.2.Blok

Blok, Bitcoin ağına ait verilerin kalıcı olarak kaydedildiği dosyalardır. Bir blok daha önce herhangi bir bloğa girmemiş işlem kayıtlarından oluşur. Bloklar kayıt defterinin sayfası gibidir. Yeni bir bloğun oluşturulabilmesi için önceki bloğun özet değerine ihtiyaç vardır. Yeni blok oluşturulurken önceki bloğun özet değerinin kullanılması ile genessis bloğundan geçerli bir blokzinciri oluşturma etkisi oluşturur. Zincirdeki bir önceki bloğa ebeveyn blok (parent blok) denir.

Bir bloğun üzerine yeni bir blok oluşturduktan sonra bir daha değiştirilemezler. Tüm sistem bir döngü içinde çalışır ve veriler kalıcı olarak depolanır. Bu da kullanıcının önceden kaydedilmiş işlem verilerinin tahrif edilmesini neredeyse imkansız kılar.

Kullanıcıların yaptığı işlemler, kim tarafından kime ödendiği gibi bilgiler blok içinde saklanır. Hesap bilgileri kullanıcı ile ilişkilendirilmediği için gizlilik sağlanır.



Şekil 9. Blokların birbirlerine eklenerek zincir oluşturması

Bitcoin ağında blok üretiminin ortalama on dakikada oluşturulması planlanmıştır. Ağa katılan işlem gücü artarsa, sistem zorluk derecesini arttırarak blok üretiminin zorluğu artırılır. Böylelikle işlem gücünden bağımsız olarak blok üretim periyotu aynı kalır.

2.2.1.Genesis Blok

Bir blokzincirde üretilen ilk bloğa "Genesis" blok denir. Genesis blok herhangi bir bloğa bağlı değildir. Bir önceki bloğa atıfta bulunulmaması özel bir durumdur. Bitcoin blokzincirinde genesis bloğu "**The Times 03/Jan/2009 Chancellor on brink of second bailout for banks**" notu ile üretilmiştir. Bu bloğun üretilmesinden kaynaklanan 50 BTC'lik ödül genesis bloğunu ifade ettiği için harcanamaz.

2.2.2.Blok Yapısı

Blok, temel olarak blok başlığı ve blok gövdesinden oluşur. Blok gövdesinde bloğu oluşturan işlemler vardır. Ortalama işlem boyutu 250 byte civarındadır. Bir blok 5 bölümden oluşur. Bunlar Tablo 1'deki gibidir.

Alan Adı	Boyut	Açıklama
Sihirli Sayı	4 Byte	Blok başlangıcını gösteririr. (0xD9B4BEF9)
Blok Boyutu	4 Byte	Toplam blok büyüklüğü
Blok Başlığı	80 Byte	Blok başlığının büyüklüğü
İşlem Sayısı	1-9 Byte	Kaç adet işlem olduğunu gösterir
İşlemler	Değişken	Blok içindeki işlemler

Tablo 1. Blok yapısı

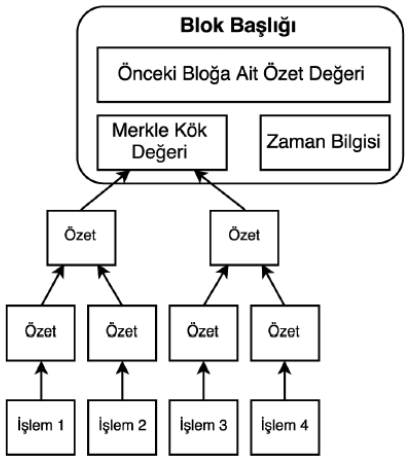
2.2.3.Blok Başlığı

Blok başlığı 6 alandan oluşmaktadır. Bunlar Tablo 2'deki gibidir.

Alan Adı	Boyut	Açıklama
Versiyon	4 Byte	Yazılım versiyonu
Önceki Bloğun Özeti	32 Byte	Bir önceki bloğun hash değeri
Merkle Kökü	32 Byte	Merkle kökü hash değeri
Zaman Damgası	4 Byte	Bloğun oluşturulma zamanı
Zorluk Derecesi	4 Byte	Güncel iş ispatı zorluk derecesi
Nonce	4 Byte	Sayaç

Tablo 2. Blok başlığı

Blok içerisindeki veri bütünlüğünü kontrol etmek için blok başlığı temel olarak; önceki bloğun özeti, merkle kökü, zaman bilgilerini içermektedir.



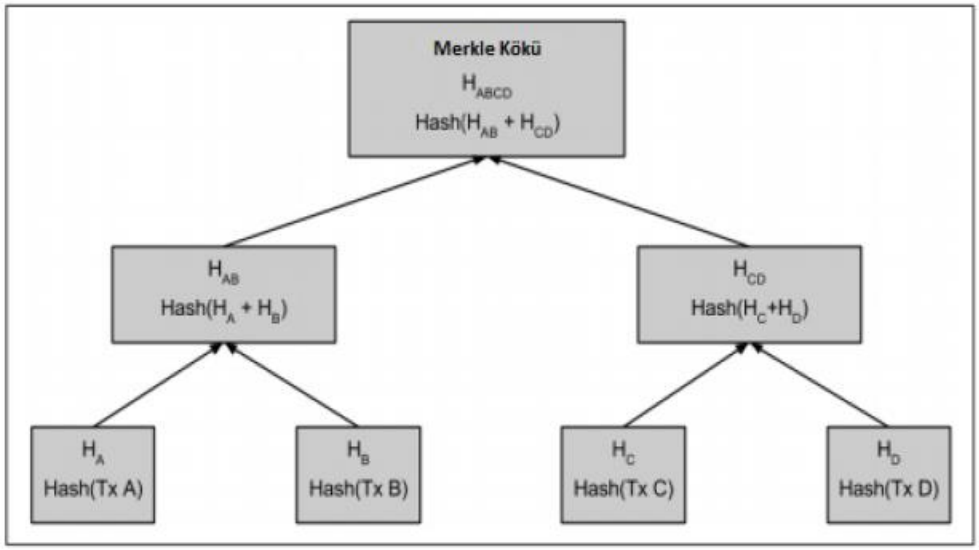
Şekil 10. Blok başlığı

Versiyon: Bir blok oluşturulurken yapısı, uzunluğu, kayıtların şekli gibi uyulması gereken kurallar vardır. Bu kurallar zaman içerisinde değişebilir. Bloğun hangi kurallara göre oluşturulduğu versiyon numarasına göre belirlenir.

Önceki Bloğun Özeti: Blokları birbirine bağlayan unsur bloğun özet değeridir. Bir blok oluşturulurken girdilerinden bir taneside önceki bloğun özet değeridir. Bu özellik zincirin değiştilemez olmasını sağlar.

Merkle Kökü: Merkle ağacı adını matematikçi Ralph Merkle'den alır. Çok fazla bilgi tek bir özet değerle temsil edilir. Bunun için her bir işlemin özet değeri hesaplanır.

Sonra özetler birleştirilir ve birleştirilen özetlerin tekrar özeti alınır. Bu işlem tek bir özet elde edilinceye kadar devam eder. Elde edilen son özet değere Merkle kökü dedir.



Şekil 11. Merkle ağacındaki düğümlerin hesaplanması

Merkele ağacı blockzincir sisteminde işlemlerin özet değerinin hesaplanması için kullanılır. Bitcoin sisteminde özet alma işlemi için SHA-256 algoritması kullanılmaktadır. Özet alma işlemi iki defa uygulandığı için çift SHA-256 olarak isimlendirilmektedir. N adet veri kullanılarak oluşturan merkle ağacında, bir işlemin olup olmadığının kontrolü en fazla 2*log2(N) işlemde kontrol edilebilir.

Kök özetinin oluşturulması, tüm dallar ve yapraklar bilindiği sürece hızlı ve kolaydır. Kök özeti biliniyorsa, ancak işlemler bilinmiyorsa, işlemleri tahmin etmek imkansızdır. Madenciler herhangi bir zamanda blokta yer alan işlemleri kullanarak kök özet değerini doğrulayabilirler. Özet işlemi aynı olduğu sürece, madenciler belirli bir işlem için her zaman aynı özet değerini elde eder. Bu da işlemlerin doğrulanması için çok kullanışlı bir yoldur. (Balcısoy, 2017)

Zaman Damgası: Bloğun üretildiği zamanı gösterir. Unix'in Epoch zaman formatında gösterilir. 1 Ocak 1970 GMT 00:00'dan itibaren kaç saniye geçtiğini gösterir. Alabileceği maksimum değer 19 Ocak 2038 GMT 03:14:08 dir. Bu tarihe Y2038 problemi denir.

Zorluk Derecesi: Belirli bir hedefin altında bir özet bulmanın ne kadar zor olabildiğinin bir ölçüsüdür. Bitcoin ağında blokların ortalama 10 dakikada bir oluşturulması hedeflenmiştir. Bu sebeble bilgisayarlara iş yaptırarak bloğun özetinin bulunması sağlanır. Bu iş yapmaya literatürde problem çözmek denir. Problem hesaplanacak özet değerinin belli bir sayıdan küçük olmasıdır. Hedef değer her 2016 bloktan sonra tekrar hesaplanmaktadır. Bu da yaklaşık olarak iki haftalık bir süreye denk gelmektedir. Önceki 2016 bloğu bulmak iki haftadan az sürdüyse zorluk artar. Eğer iki haftadan fazla sürerse, zorluk azalır. Zorluktaki değişim, önceki 2016 bloğun bulması gereken iki hafta içinde veya iki haftanın altında kalan süre ile orantılıdır.

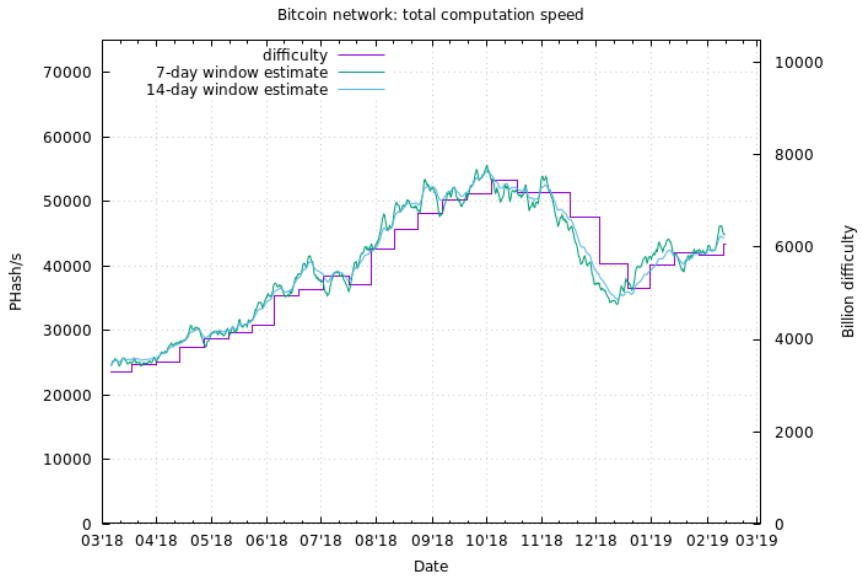
Her blok, gerçek onaltılık hedefi için paketlenmiş bir gösterimi saklar. Hedef, önceden tanımlanmış bir formül vasıtasıyla türetilir. Sistemde 32 bit olarak tutulan hedef değeri ile karşılaştırma işlemi için kullanılan 256 bit, aşağıdaki formül ile hesaplanarak bulunur. Örneğin, Bitcoin sisteminde 32 bit olan hedef değer 0x2004b30d olsun. Verilen bu değerin ilk iki onaltılık basamağı üs bilgisini, kalan altı basamak ise katsayı değerini gösterir. Bloğun doğrulanabilmesi için hedef değerin üs kısmı 0x20, katsayısı ise 0x04b30d olarak bulunur. Hedef değer 256 bit olarak aşağıdaki eşitlik kullanılarak hesaplanır. (Antonopoulos, 2014)

$$Hedef = Katsayı * 2^{8*(Üs-3)}$$

Bu eşitlik kullanıldığında 0x2004b30d değeri ile 256 bitlik onaltılık tabanda aşağıdaki sonuç elde edilir.

$$Hedef = 0x04b30d * 2^{0x08*(0x20-0x03)}$$

Bu işlem sonucunda, iş kanıtı probleminde karşılaştırma işlemi için kullanılacak hedef değer bulununmuş olur. Blok başlığı çift SHA-256 özet algortimasından gerçirilmesi ile elde edilen sonuç zorluk değeri ile karşılaştırılarak yeni üretilen bloğu doğrulama işlemi gerçekleşir. Mevcut zorluk seviyesini http://bitcoin.sipa.be/ adresinden görebilirsiniz.



Şekil 12.Zorluk seviyesi (http://bitcoin.be, 2019)

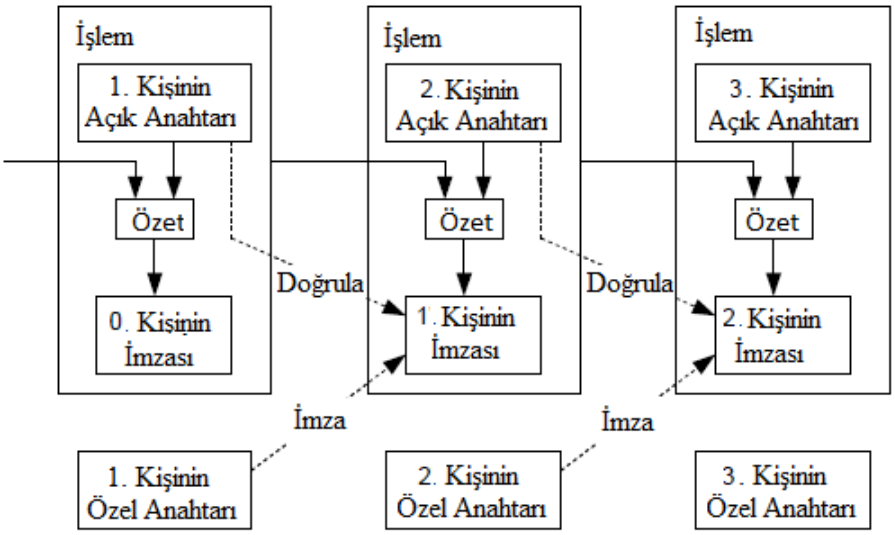
Nonce: Bloktaki bilgiler değiştirilmeden yeni bir özet elde etmek için bu alan kullanılır. Madenciler iş kanıtı problemini çözebilmek için bu alanı kullanır. Nonce değeri her denemede bir birim artırılır. Nonce değeri 0 ile2^{32}arasında değer alır.

Bu kadar nonce denemesi ile geçerli bir özet değeri bulunmaması durumunda bloğun zaman damgası güncellenerek yeni blok başlığı oluşturulur. Günümüzde madencilik için kullanılan cihazlar yüksek özet hesaplama hızına sahiptir. Zaman damgasını değiştirerek geçerli özet bulanamadığı durumda, bloğun içindeki bir işlem çıkartılarak yada bloğa yeni bir işlem ekleyerek geçerli özet bulmaya çalışılır.

2.3.İşlemler

Blokzincir ağında eşler arasındaki varlık transferlerine işlem denir. Blokzincir defterindeki işlemler blokta saklanır. Blokzincir üçüncü bir taraf olmadan transfer işlemlerini, doğru ve güvenli yapılabilmesi üzerine kurulmuştur. Bu sebeble işlemler blokzincir mimarisinin en temel ve en önemli yapı taşıdır. Bir bitcoin işlemi, bir değerin eşten eşe transfer edilmesini sağlar.

Her işlem sahibi, bir önceki işlemin dijital imzasını kullanarak işlemini imzalar ve bir sonrakine aktarır. Ödemeyi alan imzaları doğrulayarak sahiplik zincirini tamamlar.



Şekil 13. Blokzincir işlem yapısı (Nakamoto, 2008)

Bir önceki işlem sahibinin, daha önceki işlemleri imzalamamış olduğundan emin olmamız gerekmektedir. Bir işlemin olup olmadığını tanımlamanın tek yolu bütün işlemlerin bilinmesi ile olur. Merkezi otorite tabanlı sistemlerde, merkezi otorite bütün işlemlere hakimdir ve hangi işlemin ilk işlem olduğunun farkındadır. Bunu güvenilir bir otorite olmadan yapabilmek için ise, tüm işlemlerin halka açık olduğu ve tüm katılımcıların işlemlerin sırasını onaylayacakları bir sisteme ihtiyaç vardır. (Da, 1998)

Bloklar değişmezliklerini başlık özetlerinin hesaplanmasıyla garanti altına alır. Merkle ağaç yapısı ile blok içindeki bütün işlemlerin özet değeri alınarak merkle kökü elde edilir ve işlemlerin değişmemesi garanti altına alınmış olur. Böylelikle hem blokların hem de işlemlerin değişmediği garanti altına alınmış olur.

Bir bitcoin işlemi, girdi ve çıktı verilerinden oluşmaktadır. İşlem yapısı Tablo-3'te gösterilen alanlardan oluşmaktadır.

Alan	**Boyut**	**Açıklama**
Versiyon	4 Byte	İşlemin versiyon bilgisi
Girdi Sayısı	1-9 Byte	Girdi sayısı
Girdiler	-	Girdi verileri
Çıktı Sayısı	1-9 Byte	Çıktı Sayısı
Çıktılar	-	Çıktı verileri
Zaman Damgası	4 Byte	İşlem zamanı

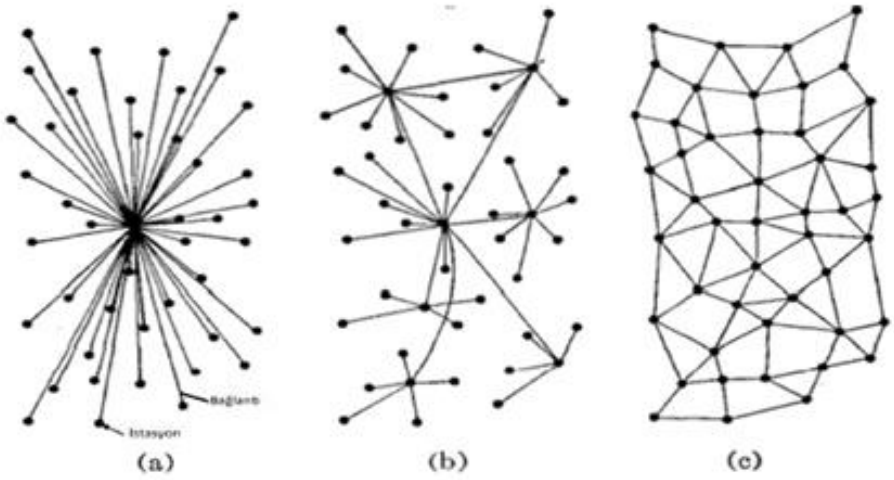
Tablo 3. İşlem veri yapısı

Bütün işlemler en az bir girdi ve bir çıktıdan oluşur. Bütün girdiler, kullanacağı parayı bir önceki çıktıdan alarak kullanır. Bütün çıktılar, sadece bir defa girdi olarak kullanılabilir. Bütün çıktılar, harcanmış veya harcanmamış (UTXO-Unspent Transaction Output) şeklinde sınıflandırılır. 20 bitcoininiz varsa bu UTXO kaydında ilk işleme kadar gidilip bütün işlemlerin taranarak bize ait olan ve harcayabileceğimiz bitcoin işlemlerini içeren miktarın toplandığı ve işlem sonucunun 20 bitcoin olduğu anlamına gelir. Önceki işlemlerin çıktısından 5 bitcoin'im var ve ödemem gereken 3 bitcoin ise kalan 2 bitcoin'i kendime transfer edebilirim. Bu işlem UTXO çıktısı üretilerek gerçekleştirilir.

Bir ödeme işleminin geçerli olabilmesi için, harcanmamış para içeren işlemlerden elde edilen paranın toplamı, harcanacak paraya eşit veya daha fazla olmalıdır. İşlem kaydına gelen para, çıkan paradan büyük olduğu durumda fazla olan miktar işlem komisyonu olarak o işlemleri blok içine alıp bloğu oluşturan madencilere verilir. Böylece mining işlemi özendirilir. Madenciler ayrıca ürettikleri her blok için ödül olarak verilen coin base transaction denilen miktarı da alırlar. Bir tür para basma işlemi olan coin base transaction işleminde girdi bilgisi bulunmamakta olup yalnızca çıktı bilgisi vardır.

İşlem kaydı çıktısında gönderilecek bitcoin miktarı ve bu miktarı kullanabilecek alıcının uyması gereken kurallar (ödemenin kim tarafından ve nasıl kullanılacağını belirleyen) ve alıcının adresi bulunur. İşlem çıktısında script alanı bu işlem için kullanılmaktadır.

2.4.Dağıtılmış Hesap Defteri



Şekil 14. Merkezi, çok merkezli ve dağıtık ağ yapıları (Baran, 1962)

Dağıtık Defter Teknolojisi(DLT), güvenilmez veya kötü niyetli (olumsuz ortam) olabilecek taraflara rağmen, merkezi operatör veya otorite olmayan bir ortamda çalışan çok taraflı sistemleri belirlemek için bir şemsiye terimi olarak tanımlanabilir. DLT'ler, verilerin, bilgisayarların veya katılımcıların dağıtık (distributed) bir ağda kaydedildiği, paylaşıldığı ve senkronize edildiği belirli veritabanı türleridir.

Blokzincir ve diğer dağıtık defter teknolojileri üçüncü bir şahıs veya aracılar olmadan (de-centralized) dijital veriyi taraflar arası coğrafi bağımsız dolaşımını güvenli bir şekilde sağlayan teknolojilerdir. Burada dolaşan dijital veri işletme birimi dijital para olabileceği gibi tarafların meta-verileri de olabilir. Örneğin; sigorta poliçeleri, sözleşmeler, arazi bilgileri, tıbbi kayıtlar, doğum ve evlilik sertifikaları, mal ve hizmet satın alma ve satma veya dijital biçimde çevrilebilen herhangi bir başka işlem veya varlık türünü temsil edebilir.

Ademi merkeziyetçilik için tüm tanımlarda, yinelenen tema, sistemin karar verme veya yönetimini sabit bir varlık kümesine bırakmak yerine, özgür ve açık katılım sağlayan ve canlı tartışmayı teşvik eden süreçler ve kurumlar olmasıdır.

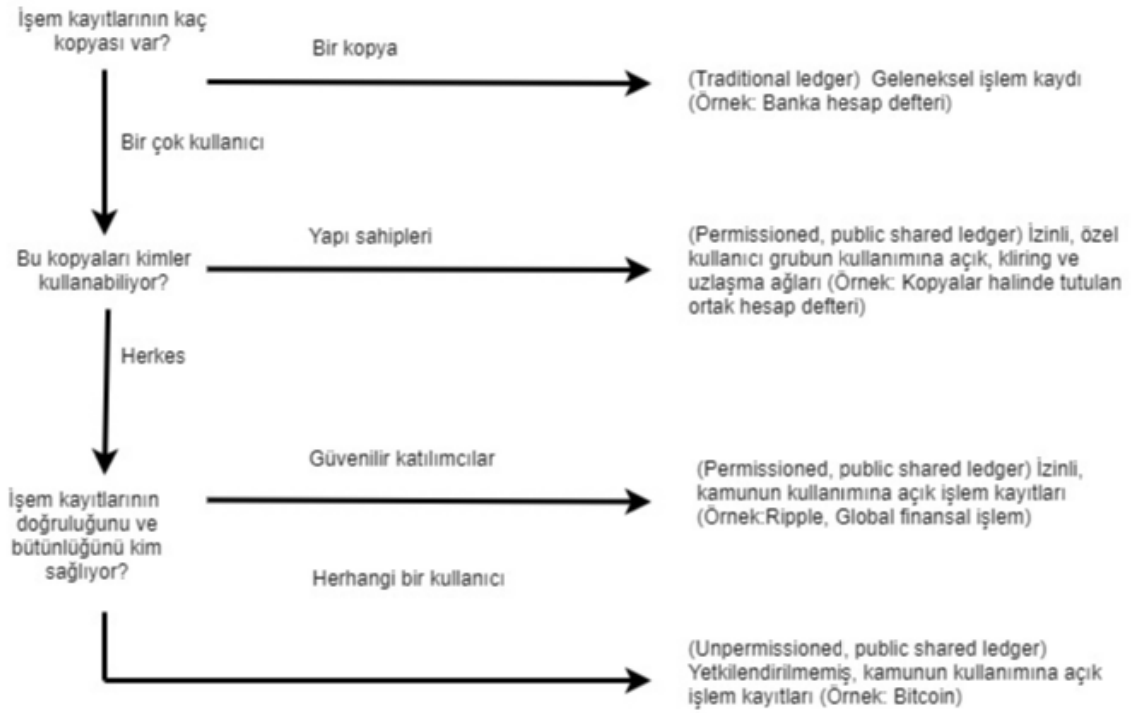
Bitcoin gibi, kamuya açık ve izin almayı gerektirmeyen ademi merkeziyet DDT sistemlerinde, tek bir taraf sistemi kapatamaz, defterleri manipüle edemez veya sansür

işlemleri gerçekleştiremez. Bu aynı zamanda esnekliği artırır ve bir bütün olarak ağ katılımcılarının kaybı da dahil olmak üzere sistemin her daim hayatta kalmasını sağlar.

Finansal teknolojilerin birçok destekçisi, DLT'nin yaygınlaşmasının sadece finansal piyasaların teknolojik mimarisinde değil, aynı zamanda finansal sistemin yapısında da köklü değişiklikler getireceğini öne sürmektedir. Federal Reserve ekibi tarafından sektör katılımcılarıyla gerçekleştirilen röportajlar sonucu toplanan bilgiler, şirketlerin DLT düzenlemelerini geliştirme ve uygulama çabalarının arkasında birkaç ortak motivasyona sahip olduklarını göstermektedir. DLT varlıkların muhafaza edilip depolama, yükümlülükleri yerine getirme şekli, sözleşmeleri yürürlüğe koyma ve risklerin yönetilmesi alanında olumlu köklü değişiklikler yapabilmesini olası olarak görmektedir. (Mills & diğerleri., 2016) Bu değişiklikler;

- Karmaşıklığı azaltmak (özellikle çok taraflı, sınır ötesi işlemlerde)
- İyileştirilmiş uçtan uca işlem hızı ile varlıkların ve fonların kullanılabilirliğini arttırmak
- Birden fazla kayıt tutma altyapısında mutabakat ihtiyacını azaltmak
- İşlem kaydında şeffaflığı ve değişmezliği arttırmak
- Dağıtılmış veri yönetimi vasıtasıyla ağ esnekliğini arttırmanın yansıra operasyonel ve finansal riskleri azaltmaktır.

Birleşik Krallık Hükümeti Baş Bilim Danışmanı tarafından hazırlanan "Dağıtık Kayıt Teknolojisi: Blokzincirinin Ötesinde" raporunda dağıtık işlem kayıtları sınıflandırmasının nasıl olabileceği Şekil 15'de gösterilmiştir.



Şekil 15. Dağıtık işlem kayıtları sınıflandırılması (GOS, 2015)

Raporda tıpkı blokzincirinin kripto para birimlerinin ötesinde kullanım olanakları sağladığı gibi, dağıtık kayıt teknolojisinin de blokzincirinin ötesinde kullanım olanaklarının ekonomik faydalarını açığa çıkarmak, tanıtmak istenilmiştir. Dağıtık kayıt teknolojisi, hükümetin dolandırıcılık, yolsuzluk, hata ve kağıt yoğun süreçlerinin maliyetini azaltma olanağı sağlamaktadır. Bilgi paylaşımı, şeffaflık ve güven açısından hükümet ve vatandaş arasındaki ilişkiyi yeniden düzenleme potansiyeline sahiptir. Bir dağıtık kayıt teknolojisi düzenlemesinin açık ya da kapalı olmasına bakılmaksızın, katılımcılar (dolayısıyla bulundukları düğümler) izin verilen roller yada gerçekleştirmelerine izin verilen işlevler ile farklılıklar gösterebilmektedir.

2.5.Uzlaşma Yöntemleri

Dağıtık sistem üzerinde kayıt defterini tutan makinelerin herhangi bir işlemin geçerli olarak kabul edilebilmesi için sistemin geneli tarafından kabul edilmiş kurallara uygunluğunun kontrol edilmesi gerekir. Bu kontrol sürecine ve sonunda fikir birliğine varmaya mutabakat denir.

Bizans Generalleri Problemi: Araştırmacılar Leslie Lamport, Robert Shostak ve Marshall Pease'in 1982 yılında yayınladığı akademik makalesi ile anlatılan mantıksal bir ikilem olan, bizans generalleri problemine ait çözüm yolunu içerdiğinden bu şekilde isimlendirilmiştir.

Birden fazla kullanıcı, uygulama, sunucu veya diğer başka node ile oluşturulan dağıtık bir ortamda, güvenilmez aktörlerin ortama zarar verme riski vardır. Fikir birliğine olan ihtiyaç, aynı zamanda bizans hatalarını blokzinciri için önemli bir zorluk haline getirir. İşlem ağındaki üyelerden bazıları, işlemlerle ilgili diğer üyelere hatalı bilgi gönderdiği durumda blokzincirin güvenirliği bozulur ve işlem ağını düzeltmek için adım atabilcek merkezi bir otorite yoktur. İşlem ağına katılan hiç kimseye güvenmiyorsanız veya üylerden bazıları hatalı, yanıltıcı yada kötü niyetli işlem gönderdiği durumda ortaya çıkacak problemi çözmek için oluşturulan sisteme Bizans Hata Tolerans Sistemi denir. Bu sistem, belli bir alana dağılmış ve birbirlerine sinyaller gönderen değişik parçaların gelen çelişkili sinyaller karşısında nasıl doğru hareket etmeleri gerektiğini belirler. Sistem aşağıdaki kurallara bağlı olarak çalışır:

1. Oyuncuların en az 2/3'ü doğru çalışıyor olmalı.
2. Her bir parça kendisine gelen mesajlar içinde çoğunluğun gönderdiği mesajı uygular;
3. Sistem oyuncuların çoğunluğunun ilerlediği şekilde ilerler. (Burada önemli olan "doğru" bir sonuç çıkması değil "tutarlı bir" sonuç çıkması, ortada bir kararsızlık kalmaması)

Blokzincir genel olarak yukarıda bahsedilen Bizans Hata Tolerans sistemine bağlı "Mutabakat Mekanizması"nı kullanarak kendi aralarında uzlaşma sağlar.

İş İspatı(Proof of Work): 1997 yılında Adam Back e-mail gönderimi için kriptografik özet algortimalarını kullanarak Hashcash adında anti-spam uygulaması geliştirmiştir. (www.hashcash.org, 1997) E-mail gönderilmek istenildiği durumda, mail sunucusu daha önceden hesapladığı ve özetini bildigi bir kriptografik özet fonksiyonunu kullanıcın hesaplamasını ister. Özet fonksiyonun hesaplanma işlemi, yaklaşık bir saniye sürer ve her e-mail gönderilmeden önce hesaplanması gerekir. Hashcash, bu kullanımıyla, kriptografik özet fonksiyonunun, belli bir işi yaptığının kanıtı olarak kullanılmasına örnektir.

Bitcoin'de Hashcash temelli Proof of Work(PoW) kullanılır. Bu işlem "mining" olarak adlandırılır. Önceden belirlenmiş özelliklere uygun bir özet değeri bulmak için madenciler bütün ihtimalleri deneyerek bulmaya çalışırlar. İstenilen özelliği sağlayan özeti bulan ilk madenci, blokzincirdeki yeni bloğu üretir. Yapılan işlemler kurallara uygunsa, onaylar ve yaptığı işin karşılığında işlem komisyonları ve yeni üretilen bitcion ile ödüllendirilir. Özet fonksiyonunun çıktısı tamamıyla rassal olduğu için tüm madencilerin ödülü alma ihtimali vardır.

İş kanıtı, temelde SHA-256 gibi şifreleme algoritması ile dijital olarak imzalandığında, bu dijital imzanın belirli sayıda 0(sıfır) biti ile başlamasını arar. Bu format zorluk denilen bir değişkenle ayarlanır. Gerek duyulan ortalama iş, gerek duyulan sıfır bit sayısı ile üstel olur ve tek bir hash çalıştırılarak doğrulanabilir. Zorluk seviyesi arttıkça istenilen formata uygun özet değeri elde etmek daha da zorlaşmaktadır. Mevcut zorluk derecesi ile ilgili bilgiler https://blockchain.info/charts/hash-rate adresinde bulunabilir.

İş kanıtını, bloğun dijital imzasında istenen 0(sıfır) değerine ulaşana kadar arttırdığımız bir "nonce" değeri ile sağlanır. İşlemci iş kanıtını sağlayacak işlemleri bir kez yaptıktan sonra, aynı işlemler yapılmadan blok bir daha değiştirilemez. Sonraki bloklar zincire eklendikten sonra, önceki blok değiştirildiğinde, sonra gelen tüm blokların da aynı şekilde değiştirilmesi gerekir.

Son oluşturulmuş bloğa ait özete ve blokla ilgili diğer bilgilere https://www.blockchain.com/btc/block adresinden ulaşılabilinir.

İş kanıtı, aynı zamanda çoğunluğun kararının benimsenmesi sorununu da ortadan kaldırır. İş kanıtı, "bir bilgisayar bir oy" temeline dayanır. Çoğunluk kararı, en büyük kanıtlama çalışması eforuna sahip en uzun zincir tarafından temsil edilir. İşlemci gücünün büyük bir çoğunluğu dürüst düğümlerle kontrol edilirse, dürüst zincir en hızlı büyüyecek ve rakip zincirleri aşacaktır. Daha önce oluşturulmuş bir bloğu değiştirmeye çalışan saldırganın, o bloğun ardından gelen bütün blokları da değiştirmesi gerekecek, ve akabinde mevcutta dürüst düğümlerden kurulu bir zincirden daha uzun bir zincir oluşturması gerekecektir.

Zaman içinde artan donanım hızları ve artan düğüm sayısına uygun şekilde, her bir blok için iş kanıtı zorluk seviyesi hareketli ortalama metodu kullanılarak saatlik olarak yeniden hesaplanır. (Nakamoto, 2008)

Pay İspatı(Proof of Stake): İş ispatı ile madenciler aynı işlemleri yapmak için yarışırlar. Bununla birlikte, pay ispatı(PoS), işlemleri işlemek ve güvenceye almak için onaylayıcıları rastgele seçer. Pay ispatı sisteminde, onaylayıcılar madencilerin eşdeğeridir. Bir sonraki bloğu üretme görevi tamamen rassal bir fonksiyon ile madencilerden birisine verilir.

PoS yönteminde üretilen blok için madenci ödül kazanmaz. Sadece blok içindeki işlemlerinin komisyonunu kazanır. Bu sebeble bu yöntemle çalışan madencilere oluşturucu(forger) denir.

Pay ispatı kullanan sistemlerde genellikle üretilebilecek bütün kripto para miktarı ilk önce üretilir ve üye olan yatırımcılar sistemdeki paylarına göre kripto para alırlar. Daha sonra yeni ekleme yapılmaz. Sistemdeki pay, sahip olunan kripto para miktarına göre bulunur.

Onaycı sistemde ne kadar paya sahipse, blok oluşturma ihtimali o kadar yüksektir. Bir onaycının payı arttıkça, işlemleri doğrulamak için seçilme şansı da artar. Potansiyel ödül ile hile yapma riskleri arasındaki asimetrik fark, doğrulayıcıların her zaman dürüst kalmasını sağlar.

Sadece sahip olunan pay değeri kullanılması, yüksek pay sahibi üyeler için bir avantaj oluşturduğu için bloğu oluşturacak madenci bulunurken yaş(age) kavramı getirilmiştir. Bu yöntemle blok üretimi için kullanılan pay kapsamındaki kripto paralara ait yaş değeri sıfırlanır. Yaş değeri sıfırlanan paralar belirli bir süre sonra tekrar yaş değeri kazanmaya başlar. Yaş değeri blok üretilmesinde öncelik elde etmede avantaj olur. (Usta & Doğantekin, 2017)

PoS'un PoW'a karşı enerji tüketimi açısından çok büyük avantajı vardır. Bitcoin üretirken on binlerce madenci her bir blok üretimi için katrilyonlarca kez özet hesaplaması aynı anda yaparlar ve sadece bir blok üretilir. Ancak PoS yönteminde

seçilen bir tek madenci bu işlemi yapacaktır. Bu da devesa boyutta enerji tüketimini çok azaltacak bir durumdur.

2.6.Madencilik

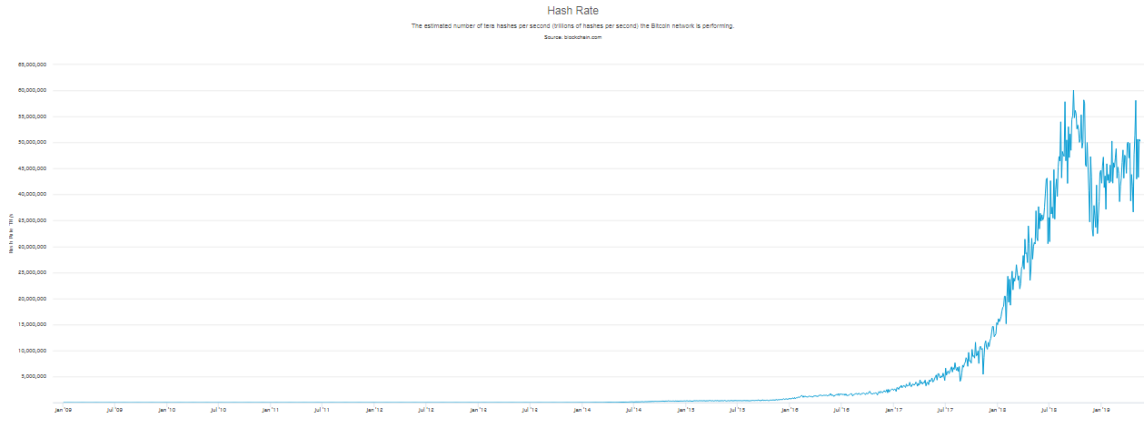
Bitcoin madenciliği, bitcoin para birimini oluşturma ve işlemleri doğrulama sürecidir. Mevcutta merkez bankaları tarafından basılan paranın aksine bitcoin matematiksel problemlerin çözülmesiyle oluşturulur. Madencilik, bitcoin geçmiş işlemleri içeren halka açık defteri tutarak deftere yeni işlemler ekleme işlemidir.

Madenciliğin temel rolü, bitcoin düğümlerinin güvenli ve saldırılara karşı dirençli hale gelmesini sağlamaktır. Enflasyondan kaçınmak amacıyla madenciler tarafından her gün keşfedilen blokların üretilme süresi sabit tutulacak şekilde tasarlanmıştır. Blokzincirindeki her bir bloğun geçerli sayılabilmesi için çalışma kanıtının olması gerekir. Bu çalışma kanıtı daha sonra her blok için ağdaki diğer tüm bitcoin düğümleri tarafından doğrulanır.

Madenciler, blokzincire yeni bir blok eklemek için zorluk değerini bulan ilk kişi olmaya çalışırlar. İnsanları madenciliğe teşvik etmek için, geçerli bir blok üretip zincire ekleyen madenciye yaptığı işin ödülü olarak işlem komisyonları ve yeni oluşturulan bitcoin ödülü verilmektedir. Madenicler sayesinde işlemler yapılmakta ve bloklar düzenli bir şekilde oluşturulmaktadır. (Boucher, Nascimento & Kritikos, 2017)

Madencilere verilen ödül 2009'da üretilen blok başına 50 bitcoin iken, verilen ödül her dört yılda bir yarıya düşürülerek günümüzde 12,5 bitcoin olmuştur. Bitcoin üretimi yaklaşık 2140 yılında tamamlanacaktır. Toplam bitcoin miktarı 21 milyon adet olacaktır.

Bitcoin madenciliğinde hash oranı bitcoin ağının işlemci gücünün ölçü birimidir. Bitcoin ağı güvenlik amacıyla yoğun matematiksel işlemler yapmaktadır. Ağın 10 TH/s hash oranına varması saniyede 10 trilyon hesap yapabilmesi anlamına gelmektedir. (Bitcoin.org, 2009) Bu işlemler küresel boyutta oldukça maliyetli bir hal almaktadır. Bir bitcoin işlemi gerçekleştirebilmek için tüketilen elektrik 223 kilowatt saattir. (digiconomist.net, 2017) Bu durum elektronik ödemeler alanındaki kullanımı için oldukça düşündürücüdür.



Şekil 16. Bitcoin ağının özetleme kapasitesi (https://blockchain.info, 2019)

2.7.Çatallanma

Blokzincir sistemleri mutabakat mekanizmasına göre çalışan sistemlerdir. Ağa dahil olan herkes değişiklik önerebilir. Önerilen değişiklik üzerine uzlaşma olmaması durumuna çatallanma denir. Çatallanmalar kalıcı ise bununla birlikte iki farklı para birimi, iki ayrı token oluşur.

Geliştiricilerin bir kısmı yeni kurallar koymak ve o kurallarla hareket ederek, yavaş, eski ya da blokzincirde gördükleri sorun her ne ise ondan kurtulmak ister ama blokzincir'in merkezi bir yapısı olmadığı için herkes, her zaman yeni olanı kabul etmek istemeyebilir. Eski kurallarla devam etmek isteyenler bir yolda, yeni kurallarla devam etmek isteyenler diğer yolda devam ederler. Blokzincir üzerinde coin sahibi olan kişiler, çatallanma sonrasında her iki coinede aynı miktarda sahip olur.

Yapılan bir önerinin kabul edilebilmesi için birçok kullanıcı tarafından da kabul edilmesi gerekmektedir. Burada çatalda oluşan iki zincirden hangisinin rağbet göreceği borsalar, kripto para sahipleri, madenciler ve piyasa tarafından kabul görüp görmemesiyle bağlantılı olarak gelişim gösterir.

Çatallanmalar basit ve zorunlu çatallanma olarak ikiye ayrırılır.

Basit Çatallanma: Geriye uyumlu olarak yapılan çatallanamaya basit çatallanma denir. Basit çatallanma özellikleri aşağıda belirtilmiştir.

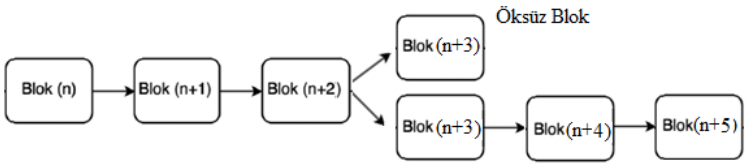
- Basit çatallanmalar (soft fork) tam düğümler tarafından uygulanan ve blokzincirin kurallarını sınırlayan protokol güncellemeleridir.
- Düğümlerin yazılımlarını güncellemesini gerektirmez.
- Geçici blokzincir bölünmelerine yol açabilirler.

Zorunlu Çatallanma: Geriye uyumun sağlanamadığı çatallanamaya zorunlu çatallanma denir. Bu çatallanmada eski kurallara göre oluşturulmuş bir blok sadece eski versiyonda geçerli olur. Yeni kurallara göre oluşturulmuş blokda sadece yeni versiyon için de geçerlidir. Çatallanmadan sonra iki ayrı zincir rmeydana gelir ve birbirleri arasında etkileşim olamaz.

- Sert çatallanmalar (hard fork) düğümler tarafından uygulanan ve blokzincirin kurallarını değiştiren protokol güncellemeleridir.
- Düğümlerin yeni blokzincire adapte olması için yazılımlarını güncellemelerini gerektirir aksi halde düğümler eski zincire bağlı kalırlar.
- Yeni bir blokzincir ve kripto paranın ortaya çıkmasına neden olabilirler.

2.8. Yetim Blok

Bir madenci bloğu üretir üretmez yayınlar ve ödülü alır. Ancak benzer zamanlarda başka bir madenci de aynı sıradaki bloğu üretmiş olabilir. Bu blok da ağda yayılmaya başlar. Böylece sistemde en son blokları farklı olan iki zincir dolaşmaya başlar. Böyle bir durum sistem açısından bir sorun teşkil etmez. Çünkü her madenci yeni bloğu üretirken mevcut zincirin özet değerini kullanacaktır ve bu esnada karşısına iki farklı zincir çıkarsa hangi zincirin hesaplama zorluğu daha yüksek ise o zinciri esas kabul edecektir. Herkes bu kurala uyacağından bu farklı zincirlerden biri sistem tarafından dışlanacak, diğeri yaşamaya devam edecektir. Dışlanan zincirin son bloğu böylece geçerliğini yitirmiş olacaktır. Dışlanan bloğa Yetim Blok (Orphan) adı verilir.



Şekil 17. Yetim blok

Yetim bloğun içine alınmış işlemler tekrar işlem havuzuna bırakılır. Bitcoin transfer işlemlerinde işlem gerçekleşmiş olsa bile işlemin üzerinen 6 blok geçmesini beklemek yeterli güvence oluşturacaktır.

2.9.Blokzincir Platformları

Blokzincir, ilk olarak kripto para uygulaması olan bitcoin ile tanınmış ve yaygınlaşmış teknoloji olmasıyla birlikte, günümüzde blokzinciri ile proje geliştirebilmek için kullanabilceğimiz birçok blokzincir platformu vardır. Bu platformlar bir çok özelliğine göre sınıflandırılmaktadır. Örneğin, açık kaynak olmaları, fiyatlandırma şekli, kullanılan programlama dilleri veya blokzincir yapısı.

Sektörün blokzincir özelliklerini fark etmesinden sonra, blokzincir geliştirme platformlarına olan ilgili beklentilerin üzerinde artış göstermiştir. Blokzincir platformlarına olan ilginin artmasının bir değer nedeni de Initial Coin Offering(ICO) ların günden güne büyümesidir.

Yeni bir blokzincir platformu geliştirmek yerine geliştiricilerin ihtiyaçlarına uygun olan platforma odaklanabileceği geniş bir yelpazede blokzincir platformları mevcuttur. Başarılı bir blokzincir platformlarında olması gereken özellikler aşağıdaki gibidir.

1-Gizlilik: Blokzincir platformunun düzenleyici ve yasal ihtiyaçlar göz önünde bulundurulduğunda güçlü bir gizlilik özelliğine sahip olması gerekir.

2-Şeffaflık: Blokzincir üzerinde yapılan tüm işlemler anlık olarak herkes tarafından görülebilir ve böylece yapılan işlemler ilk bloktan itibaren takip edebilir. Blokzincirde bilgilerinin kontrol edilebilmesi için işlemlerin şeffaf olması gerekir.

3- Güvenilirlik: Merkezi olmayan bir sistem olduğu için tek bir noktadan yönetilmiyor ve herhangi bir kişi, kurum ya da hükümetin kontrolünde değildir. Tüm işlemler sistemdeki diğer katılımcılarla paylaşıldığı için veriler dağıtık şekildedir. Merkezi olmadığı için her hangi bir saldırı noktası bulunmaz. Üçüncü şahıslara ihtiyaç duyulmaz ve taraflar birbirlerine güvenmek zorunda değildir.

4-Operasyonel Maliyet: Aracıların ve komisyoncuların aradan çıkarılması ve manuel müdahalenin azaltılması ile operasyonel maliyetleri düşürür. Aynı zamanda kayıt tutma sistemi ile denetim maliyetlerini azaltır. DLT kullanıldığı için 3.parti yazılımlar üzerinde veritabanı bakım maliyetlerinin ve siber güvenlik endişelerinin önüne geçilir.

5-İşlem Maliyeti: Mevcut sistemlerde işlemlerin doğrulanması büyük bir iş gücü ve maliyet gerektirmektedir. Blokzincir platformlarında doğrulama sisteminin kullanılmasıyla işlem maliyetleri azaltır.

6-Süreklilik: Merkezi bir yapısı olmadığı için yılın her günü 7/24 işlem yapmak mümkündür. Tatil günleri çalışmama gibi prensipleri yoktur.

Çok kullanılan blokzincir platformlarına aşağıdaki platformlar örnek verilebilir.

Platform	**Sektör Odağı**	**Kayıt Tipi**	**Konsensüs Algoritması**	**Akıllı Sözleşme**	**Yönetim / Kontrol**
Ethereum	Çeşitli Sektörler	İzinsiz	İş İspatı	Evet	Etherum Geliştiricileri
Hyperledger Fabric	Çeşitli Sektörler	İzinli Ağ	Pluggable Framework	Evet	Linux Vakfı
R3 Corda	Finans	İzinli Ağ	Pluggable Framework	Evet	R3 Konsorsiyumu
Ripple	Finans	İzinli Ağ	Olasılık Oylama	Hayır	Ripple Labs
Quorum	Çeşitli Sektörler	İzinli Ağ	Çoğunluk Oylama	Hayır	Etherum Geliştiricileri ve JP Morgon Chase
Hyperledger Sawtooth	Çeşitli Sektörler	İzinli Ağ	PoET(Geçen Zamanın Kanıtı)	Evet	Linux Vakfı
EOS	Çeşitli Sektörler	İzinli Ağ	Pay İspatı	Evet	EOSIO Core Arbitration Forum(ECAF)
Hyperledger Iroha	Çeşitli Sektörler	İzinli Ağ	BFT(Bizans Hata Toleransı)	Evet	Linux Vakfı
OpenChain	Dijital Varlık Yönetimi	İzinli Ağ	Bölümlenmiş Konsensus	Evet	CoinPrism

Stellar	Finans	Halka Açık / Özel Ağ	Stellar Konsensus Protokol	Evet	Stellar Geliştirme Vakfı

Tablo 4. Blokzincir platformları

2.9.1.Etherum

Ethurum 2013 yılında rus asıllı kanadalı yazılımcı Vitalik Buterin tarafında açık kaynak kodlu olarak gelişilmiştir. Etherum akıllı sözleşmeler üzerine kurulu blokzincir platformudur. Akıllı sözleşmeler için Etherum sanal makinesi(EVM) ortamı bulundurur. Etherum günümüzde en olgunlaşmış ve esnek blokzincir platformlarından biridir. Geniş bir sektör tarafından kullanılır. Ethereum, geliştiricilerin yeni nesil merkezi olmayan uygulamalar yazmasını ve dağıtmasını mümkün kılan bir platformdur.

2.9.2.Hyperledger

2015 Aralık ayında Linux Foundation tarafından duyurulan ve 2016 yılında çıkan Hyperledger, açık kaynak kodlu bir blokzincir projesidir. Hyperledger kripto para değildir. Bitcoin veya başka herhangi bir kripto para birimini desteklemez. Hyperledger kendi web sitesinde şu şekilde tanımlanmıştır.

HyperLedger, sektörler arası blok zincir teknolojilerini ilerletmek için oluşturulan açık kaynak kodlu bir iş birliği girişimidir. Finans, bankacılık, nesnelerin interneti (IoT), tedarik zincirleri, imalat ve teknoloji liderlerinin bir araya geldiği ve Linux Vakfı'nın ev sahipliği yaptığı küresel bir iş birliğidir. (www.hyperledger.org, 2019)

Amaçları, kısaca, iş dünyasında şirket seviyesindeki işlemlerin idare edileceği blokzincir framework'leri geliştirmek; bu işlemler için hem ticari hem de teknik yönetimler tarafından desteklenen tarafsız, açık ve tamamen topluluk odaklı altyapılar sağlamak; insanları blokzincir fırsatları konusunda eğitmek ve bu projeleri geliştirecek teknik topluluklar kurmaktır.

Yine sitesinde blokzincir'den şu şekilde bahsediliyor: "Web'in kendisinden bu yana, bu kadar kapsamlı, geniş ve temel bir teknoloji vaad eden başka bir teknoloji

çıkmadı". Blokzincir, iş süreçlerini ve yasal kısıtlamaları düzenlerken merkezinde güven, hesap verebilirlik ve şeffaflık kuran yeni nesil işlem uygulamaları üretme potansiyeline sahiptir. (www.hyperledger.org, 2019)

Hyperledger karakteristikleri aşağıdaki gibidir.

- İzinli Ağ
- Mahremiyete Saygılı İşlemler
- Kripto Para Barındırmaması
- Programlanabilir oluşu

Hyperledger çatısı altında 13 proje bulunmaktadır. Bu projelerden ilk altısı Framework, diğer yedi tanesi ise Tool başlığı altında listelenmektedir.



Şekil 18. Hyperledger ekosistemi (www.hyperledger.org, 2019)

Frameworkler:

Burrow: Hyperledger Burrow, izin verilen bir akıllı sözleşme makinesidir.Aralık 2014'te piyasaya sürüldüğünde türünün ilk örneği olan Burrow, Ethereum Sanal Makinesi'nin (EVM) teknik özelliklerine kısmen izin verilen akıllı bir sözleşme tercümanı ile birlikte modüler bir blokzincir istemcisi sunmaktadır.

Fabric: Modüler bir yapıya sahip uygulamalar veya çözümler geliştirmek için, bir temel olarak tasarlanan Hyperledger Fabric, fikir birliği ve üyelik hizmetleri gibi bileşenlerin tak-çalıştır özellikli olmasını sağlar.

Grid: Hyperledger Grid, tedarik zinciri çözümleri oluşturmak için WebAssembly tabanlı bir projedir. Tedarik zinciri akıllı sözleşmelerinde ve müşteri ara yüzlerinde gelişmeyi hızlandırmak için bir dizi kitaplık, veri modeli ve SDK içerir.

Indy: Hyperledger Indy, merkeziyetçi kimlik için özel olarak tasarlanmış, dağıtılmış bir defterdir. Birlikte çalışabilirlik için bloklara veya diğer dağıtılmış defterlere dayanan bağımsız dijital kimlikleri oluşturmak ve kullanmak için araçlar, kütüphaneler ve yeniden kullanılabilir bileşenler sağlar.

Iroha: Hyperledger Iroha, kendi benzersiz fikir birliği ve sipariş servisi algoritmaları, zengin rol tabanlı izin modeli ve çoklu imza desteği ile kullanımı kolay, modüler dağıtılmış bir blok zinciri platformudur.

Sawtooth: Hyperledger Sawtooth, dağıtılmış defterleri oluşturmak, dağıtmak ve çalıştırmak için kullanılan modüler bir platformdur. Hyperledger Sawtooth, minimum kaynak tüketimi ile büyük dağıtılmış validator popülasyonlarını hedef alan yeni bir fikir birliği algoritması, Geçen Zamanın Kanıtı (PoET) içerir.

Araçlar:

Aries: Hyperledger Aries, blokzincir temelli, eşler arası etkileşimler için bir altyapıdır. Doğrulanabilir dijital kimlik bilgileri oluşturmaya, iletmeye ve depolamaya odaklanan girişimler ve çözümler için tasarlanmış ortak, yeniden kullanılabilir, birlikte çalışabilir bir araç kiti sağlar.

Caliper: Hyperledger Caliper, kullanıcıların belirli bir blokzincir uygulamasının performansını önceden tanımlanmış bir dizi kullanım durumuyla ölçmelerini sağlayan bir blokzincir kıyaslama aracıdır.

Cello: Hyperledger Cello, talep üzerine “hizmet olarak” dağıtım modelini blokzincir oluşturma, yönetme ve sonlandırma çabalarını azaltmak için blokzincir ekosistemine getirmeyi amaçlamaktadır.

Composer: Hyperledger Composer, blokzincir iş ağlarını kurmak, akıllı sözleşmelerin gelişimini ve dağıtılmış bir deftere konuşlandırılmasını hızlandırmak için bir işbirliği aracıdır.

Explorer: Hyperledger Explorer, blokları, işlemleri ve ilişkili verileri, ağ bilgilerini, zincir kodlarını ve işlem ailelerini ve defterde saklanan diğer ilgili bilgileri görüntüleyebilir, arayabilir, dağıtabilir veya sorgulayabilir.

Quilt: Hyperledger Quilt, öncelikli olarak bir ödeme protokolü olan ve dağıtılmış defterler ve dağıtılmamış defterler arasında değer aktarmak için tasarlanmış olan ve muhasebe sistemleri arasında birlikte çalışabilirlik sunar.

Ursa: Hyperledger Ursa, insanların (ve projelerin) diğer şifreleme çalışmalarını kopyalamaktan kaçınmalarını ve süreçte güvenliği artırmalarını sağlayan paylaşılan bir şifreleme kütüphanesidir.

2.9.3.R3 Corda

R3, 2015 yılında Corda adlı açık kaynaklı bir dağıtık defter platformu kuran dünyanın önde gelen finans kurumlarından oluşan bir konsorsiyumdur. İşletmelerin ticari işlemlerinde yüksek maliyeti kaldırarak doğrudan akıllı sözleşmelerle işlem yapmalarını sağlayan blokzinciri platformudur.

Kripto para birimi veya bütünleşik bir jetonu(token) yoktur. İzin verilen katılımcıların tüm ağa değil izin verilen verilere erişmesine sağlayan bir blokzinciridir. İzin verilen bir modda çalıştığı için gizliliği arttırır ve dijital kayıtlara ince ayarlı erişim kontrolü sunar.

2.9.4.Ripple

2012 yılında geliştirilmiştir. Ödeme sağlayıcıları, dijital varlık değişimlerini, bankaları ve şirketlerini, RippleNet adı verilen blokzinciri ağı üzerinden herhangi bir geri ödeme olmadan bağlamayı hedeflemektedir. Uluslar arası ödeme ve varlık transferine imkan verir. Gelişmiş blokzinciri teknolojisi üzerine inşa edilen ripple(XRP), düğümler arasında uzlaşmaya ulaşmak için olasılıklı oylama

kullandığından dolayı diğer blokzincir paltformlarına göre daha ölçeklenebilir ve daha hızlıdır.

Santander, American Express, MoneyGram International, SBI Holdings ve Deloitte gibi büyük markalar, Ripple'daki blokzincir'in potansiyelini test etmektedir ve mevcut finansal işlemlerini güvenli ve hızlı hale getirmek için ripple kullanmayı planlıyorlar.

2.9.5.Quorum

J.P. Morgan tarafından kurulmuştur ve Ethereum'un kurumsal odaklı bir versiyonudur. Diğer blokzincir platformlarından farklı olarak, saniyede yüzlerce işlemi işlemek için oy tabanlı algoritmalar kullanır. Yüksek işlem hacmi ve hız gerektiren işlemler için uygun bir platformdur.

Quorum platformu, Ethereum (ETH) Go istemcisi temel alınarak modellenmiştir ve Ethereum Blokzinciri üzerinde çalışır.

2.9.6.EOS

Haziran 2018'de Block.one tarafından başlatılan açık kaynaklı blokzincir platformudur. Dağıtılmış uygulamalar geliştirilmek için tasarlanmıştır. Platformun amacı, merkezi olmayan bir uygulama, kurumsal çözümlerin depolanması ve akıllı sözleşme yeteneği sunmaktır. Ethereum ve Bitcoin'in ölçeklenebilirlik sorunlarını çözmüştür ve tamamen ücretsizdir.

2.9.7.OpenChain

OpenChain platformu Open Assets'ın arkasındaki Coinprism tarafından geliştirilmiştir. OpenChain, dijital varlıkları güvenli ve ölçeklenebilir bir şekilde yönetmek isteyen kuruluşlar için açık kaynaklı bir blokzincir platformudur. Bitcoin'de kullanılan iş ispatı uzlaşma yönteminin aksine bölümlenmiş konsensusu kullanır. OpenChain'de madenci olmadığından, işlemler ücretsizdir.

2.9.8.Stellar

Stellar, değer aktarımlarını yapabilmek için kullanılan blokzincir platformudur. Finansal işlemlerin kaydedilmesi için Stellar Konsensüs Protokolü (SCP) kullanılır. Kanıtlanabilir güvenlik özelliğine sahip olan SCP, yanlış düğümler veya bölümlenme durumunda bir uzlaşmaya varılana kadar ağın ilerlemesini durdurur. İş ispatı ve pay ispatı algoritmalarına kıyasla, SCP finansal ve bilgi işlem gereksinimlerine sahip olup, giriş engelini azaltmakta ve finansal sistemi yeni katılımcılara açmaktadır.

TransferTo, NaoBTC, RippleFox ve ICICI Bank gibi birçok şirket, sınır ötesi para transferlerini sağlamak için Stellar paltformunu kullanmaktadır.

2.10.Blokzincir Uygulama Alanları

Blokzincir merkezi otoriteye güven sorunu yaşayan birçok farklı sektörde kullanılabilecektir. Kripto para blokzinciri teknolojisinin en önemli kullanım alanıdır. Günümüzde yaklaşık 2000 adet kripto para olduğu bilinmektedir. Genel olarak blokzincirin uygulama alanları şunlardır;

1. Kripto para
2. Dijital kimlik uygulamaları
3. Fon toplama işlemleri
4. Akıllı sözleşmeler
5. Para transferleri
6. Değerli belgelerin oluşturulması ve saklanması
7. Pasaport işlemleri
8. Sosyal güvenlik sistemleri
9. Bağış sistemleri
10. Müşteri tanıma işlemleri(KYC)
11. E-Ticaret ve ödemeler
12. Tedarik zinciri yönetimi
13. Kayıt sistemleri
14. Takas yönetimi
15. Doküman yönetimi
16. Oy kullanma

17. Vergi sistemi
18. Ödeme sistemleri
19. Telif kayıt sistemleri
20. Sigorta işlemleri
21. Tapu işlemleri
22. Yetkilendirme ve doğrulama işlemleri
23. Sağlık sistemleri
24. Noter İşlemleri

BÖLÜM 3. KİMLİK DOĞRULAMA METOTLARI

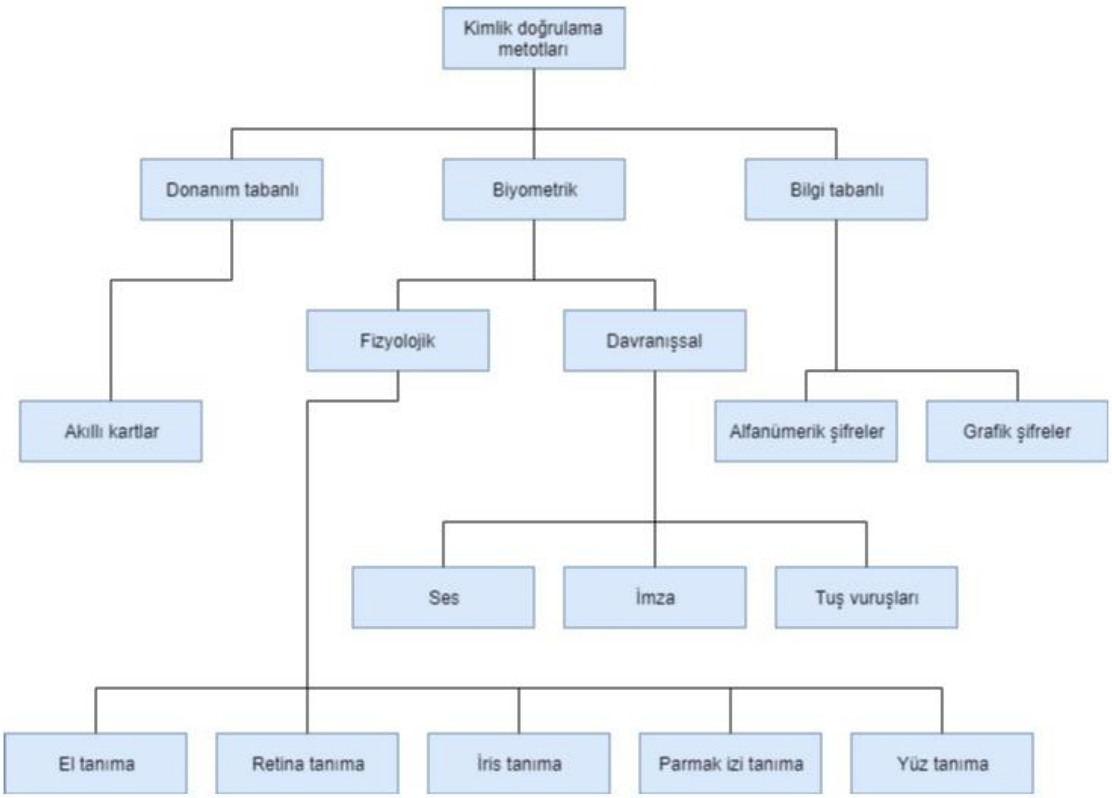
Kimlik doğrulama, bir kişinin veya bir uygulamanın gerçekte iddia ettiği kişi veya uygulama olduğunun tespit edilmesi amacıyla yapılan işlemlere denir. Kimlik doğrulama tasarımları ise, bir kullanıcıyı ya da uzaktaki bir sunucuyu güvenli olmayan ağlar üzerinden tanıyıp doğrulama yapabilen mekanizmalardır. Doğrulama mekanizmasında kullanılan üç temel teknik vardır. (Woodward. D., 2003)

- Genellikle kişi tarafından bilinen şifreler ya da tek kullanımlık şifreler (TKŞ): Şifrelerin ve kişisel kimlik numaralarının en basit uygulamaları, tüm doğrulama mekanizmalarının en önemlilerinden sayılmaktadır.
- Sadece kişi tarafından kullanılan özel donanımlar: Akıllı kartlar ve şifre fişleri gibi fiziksel doğrulama cihazları, şifrelerle ilgili belli zayıflığı gidermek için geliştirilmiştir. Kartların ve fişlerin esas faydası, şifreleri paylaşmada olduğu gibi aynı özgürlükle paylaşılamamalarıdır.
- Biyometriğe karşılık gelen, fiziksel özellikler ya da kişisel niteliklere bağlı olan yöntemler: Yaygın biyometrik doğrulama teknikleri bir kullanıcının parmak izi, eller, gözler, yüz ya da ses ölçüler ve o kişiye ait başka özelliklerle eşleştirmeye çalıştırmayı hedef edinir.

Bir başka kimlik doğrulama yöntemi de çok faktörlü kimlik doğrulama yöntemidir. Bu doğrulamada yönteminde 3 farklı unsur kullanılabilmektedir; sahip olunan şey, bilinen bir şey ve kişiye ait biyometrik bir özellik. Çok faktörlü doğrulama bir bireyin fiziksel bir olanağa erişme ya da bir bilgi sistemi içindeki veriye erişme hakkını belirlemek için kullanılır. Daha iyi ve güçlü bir kimlik doğrulama yapmak için çeşitli metotların birleştirilmesiyle gerçekleştirilir. Örneğin ATM makinesini kullandığınız zaman banka kartınızı yerleştirmeniz ve daha sonra PIN kodunu girmeniz gerekir. Banka kartı sahip olduğun bir şeye karşılık gelir, sadece sahibi tarafından bilinen PIN kodu ise bildiğin bir şeye karşılık gelir. Daha sonra hesap profiline ulaşabilirsin ve parayı çekebilirsin. Çok faktörlü kimlik doğrulama metodunu kullanarak doğrulama daha güvenilir olabilir. Özel bir doğrulama metodunun başarısı teknolojiden daha fazlasına dayanır. Ayrıca uygun politikalara, prosedürlere ve kontrollere dayanır. Etkili ve güçlü bir doğrulama metodu müşteri kabulü, güvenli performans, büyümeyi sağlama ölçeği ve var olan sistemler ve gelecek planlarıyla

karşılıklı kullanılabilirliğe sahip olmalıdır. (http://www.webcitation.org, 2014) Üç farklı unsurdan herhangi ikisinin kullanıldığı çözümler 2-faktör kimlik doğrulama, her üç unsurun kullanıldığı çözümler 3-faktör kimlik doğrulama olarak sınıflandırılır.

Kimlik doğrulama yöntemleri genel olarak üç bölüme ayrılır. Bunlar, donanım tabanlı kimlik doğrulama, biyometrik kimlik doğrulama ve bilgi tabanlı kimlik doğrulama yöntemidir.



Şekil 19. Kimlik doğrulama metotların sınıflandırılması (Khan, 2011)

3.1.Donanım Tabanlı Kimlik Doğrulama

Donanım tabanlı kimlik doğrulama yönteminde kullanıcılar tarafından taşınan akıllı kart ya da program kilidi gibi sisteme özel fiziksel bir nesne ile kendilerini sisteme tanıtırlar. Bu yönteme akıllı kartlar, personel kartları örnek olarak verilebilir. Bu kartlar kimlik doğrulama sistemlerinde kullanılmaktadır ve her kişinin bilgileri bu kartlarda kayıtlıdır. Bu kart kimin elinde ise onun bilgilerinden faydalanır ve istediği işlemleri yapabilir.

3.2.Biyometrik Kimlik Doğrulama

Biyometri, kişinin fiziksel ya da davranışsal özelliklerini analiz ederek kimlik doğrulaması yapan bir bilimdir. Bu özellikler; kişiye özgü olan ve aynı zamanda kişiden kişiye kolayca aktarılamayacak kadar güvenilir, hayatın başlangıcından sonuna kadar değişmeyen kalıcı bir yapıdadır. Bu nedenle değiştirilmesi zordur. (Jain A. K., 2006)

Halihazırda kullanılmakta olan biyometrik tanıma sistemleri iki grupta incelenmektedir.

Fizyolojik Sistemler: Fizyolojik biyometrik insan vücudunun özelliklerinden toplanan veri bakımından, kimlikleri tanımlamak için algoritmaları ve diğer metotları kullanır. Bu sistemde, parmak izi, el geometrisi, iris ve retina tarama, yüz geometrisi ve kan damarları kullanılır. (Rejman-Greene, 2001)

Davranışsal Sistemler: Biyometri, biyolojik verileri, yani bireyin kişisel bir nitelik ya da davranışını analiz ederek kimliğini doğrulama bilimidir. Bu yöntemde insana ait ses, imza ve yürüyüş gibi davranışları kimlik doğrulamada kullanılır. Hayatımızda büyük önem taşıyan biyometrik tabanlı doğrulama, güvenilir kimlik doğrulaması için güçlü bir metottur. (Khan, 2011)

3.3.Bilgi Tabanlı Kimlik Doğrulama

Bu yöntemde kullanıcılar kendi şifrelerini genellikle kolay hatırlayabilecekleri şekilde oluştururlar. Alfanümerik kimlik doğrulamasında kolay belirlenen şifreler kötü niyetli saldırganlar tarafından farklı algoritmalar kullanarak basit bir şekilde kırılabilir. Başka yönden bakıldığında alfanümerik şifrelerde kullanılan özel karakterler, büyük ve küçük harften oluşan şifrelerde ve aynı zamanda uzun olan şifrelerin kırılması da daha zor ve daha güvenlidir. Bu şekilde oluşan şifrelerin tek sıkıntısı, kullanıcılar tarafından ezberlenmesi zor ve kullanıcılar tarafından pek tercih edilmemesidir. Yeni geliştirilen sistemlerde artık bu tür şifrelerin kullanılması zorunlu kılınmaktadır ama kullanıcılarda bu durumda şifrelerini bir yere yazarak kendi şifrelerini kaydedebilirler. Bu bir tehdit sayılmaktadır. Güvenlik sistemlerininde sadece süreçler, kurallar, algoritmalar, protokoller ve donanımsal faktörlerle birlikte, kullanıcı faktörü unutulmamalıdır. Bir

yöntemin arka tarafta bulunan güvenlik önlemleri ne kadar güçlü olursa olsun kullanıcının ihmali o yöntemi güvensiz hale getirebilir. (Bicakci, 2010)

Alfanümerik şifreler: Alfanümerik şifrelerinde güvenlik zafiyetleri ve bazı problemleri olsada halen en yaygın kullanılan şifre yöntemlerinden sayılmaktadır. Alfanümerik şifrelerin daha güvenli olması için genellikle uzun olması ve özel karakterlerin ve büyük ve küçük harflerden oluşması gerekmektedir. Kullanıcıların birçok sistemde kullandıkları farklı kullanıcı adı ve şifreleri güvenli bir şekilde saklanmalıdır, çünkü farklı saldırılara maruz kalıp çözülebilirler. (Kuo, 2006)

Grafik şifreler: Grafik şifreler, grafiksel resimlerin üzerinde işaretlenen noktalardan oluşmakta olup veya bir dizi imgenin arasından sıralı bir şekilde birkaç tanesini tanıma tekniğine dayanmaktadır. Bu kimlik doğrulama yönteminde resimdeki herhangi bir noktayı işaretlemek veya hatırlamak gizli bir şekilde şifre sahibine aittir ve bu bilgiler gizlidir. Grafik kimlik doğrulama sistemlerinde genellikle sistem kullanıcısına hatırlaması ve tanıması daha kolay olan farklı yöntemler geliştirmişlerdir. (Paivio, 1968) Grafik şifreleme tekniği, "tanıma" ve "hatırlama" temeline dayanan iki kategoriye ayrılır.

BÖLÜM 4. BLOKZİNCİR TABANLI GELİŞRİRİLEN KİMLİK DOĞRULAMA UYGULAMALARI

Blokzincir şu anda bazı değişik uygulamalar için test edilmektedir. Kimlik yönetimi ile ilgili olan paltformlar ve son yıllarda hızla artan girişimlerden bazıları aşağıda özetlenmiştir.

4.1.The CivicApp

2015 yılında Palo Alto da kurulan Civic, bireysel kullanıcılara ve işletmelere dijital kimlikleri üzerindeki güçlerini korumak için araçlarla donatılmış, blokzincir tabanlı ekosistem sunmaktadır.

Civic, dış sitelere ve uygulamalara erişmek isteyenler için tanıtım paneli sunmaktadır. Kullanıcı adı, şifre, üçüncü taraf kimlik doğrulayıcı veya fiziksel donanım belirteci olmadan çok faktörlü kimlik doğrulama sağlamak için mobil cihazlarda blokzincir ve biyometri kullanan bir kimlik platformudur. Civic platformunu bir tampon olarak kullanarak, kullanıcılar giriş ve şifre gerektirmeden web üzerindeki güvenilmeyen konumlara erişebilirler.

Civic'e girilen tüm kimlik bilgileri tamamen şifrelenmiştir; bu nedenle, her türlü siteye giriş yapmak için platformu kullanmasına rağmen, kullanılan bilgiler gizli ve dış tehditlerden uzak tutulmuştur.

CivicApp, kullanıcıların bilgilerinin gerçek zamanlı olarak kullanımını onaylamalarını ve doğrulamalarını sağlar. Bu uygulama aynı zamanda kuruluşların kimlik doğrulama sürecini hızlandırmasına ve maliyetleri düşürmesine yardımcı olmaktadır.

Kişi uygulamayı akıllı telefonuna indirebilir ve sanal bir kimlik kartı gibi kullanabilir. Bir devlet kurumu gibi Civic Kimlik Ortakları, güvenilir bir kimlik doğrulama otoritesi olarak hareket etmektedir. Bunların tümü blokzincir üzerinden yapıldığından, Civic verileri tek bir hacklenebilir sunucuda saklamaz. Kullanıcılar, hesaplarına, akıllı telefonlarını kaybettikleri takdirde ek bir güvenlik düzeyi sağlayan biyometrik doğrulama (parmak izi veya 3B yüz tanıma) yoluyla da erişirler. Örneğin bir

kullanıcının yeni bir banka hesabı için kimlik kanıtı sunması gerektiğinde, banka kişinin kimliğini bu uygulama üzerinden doğrulayabilir.

4.2.SecureKey and IBM Blockchain

Civic'e benzer bir fikir, Kanada'da IBM Blokzincir üzerine kurulu (Linux Vakfı'nın açık kaynaklı Hyperledger Fabric v1.0'ı üzerine inşa edilmiştir.) bir dijital kimlik ağı olan SecureKey ile uygulanmaktadır. 2018'den başlayarak, Kanadalılar yeni banka hesaplarına, ehliyetlere ve yardımcı programlara kaydolmak için akıllı telefonlarını kullanarak kimliklerini daha hızlı bir şekilde doğrulayabilecekler.

Kullanıcıların kimliklerini bir banka veya kredi ajansı gibi güvenilir bir kaynak aracılığıyla önceden doğrulaması gerekir, ancak bir doğrulamanın tüm kimlik doğrulama sürecini tekrar geçmesine gerek kalmadan diğer hizmetlere hızlı bir şekilde kaydolabilir.

Kanada'nın önde gelen bankalarının yanı sıra Kanada Dijital Kimlik ve Kimlik Doğrulama Konseyi ve Gelişmiş Veri Analizi için Komuta Kontrol ve Birlikte Çalışabilirlik Merkezi tarafından desteklenen proje, vatandaşların verilerini özel olarak paylaşmasına ve yalnızca hizmete erişmek için gereken verileri paylaşmasına izin vermektedir.

4.3.MONI

Benzer bir çizgide, Avrupa'daki sığınmacılar, MONI adlı Finlandiya'daki girişim tarafından geliştirilen ön ödemeli ve blokzincir tabanlı Mastercard alabilirler.

Kart, blokta bulunan benzersiz bir dijital kimliğe bağlı, bir banka hesabı ve bir de kimlik kartı gibi davranmaktadır. Resmi belgeleri olmayanlar için MONI faturalarını ödemelerini, yiyecek satın almalarını ve iş bulmalarını sağlar. Göçmenlik Hizmetleri işlemleri izleyebilir, ancak bu işlemlerle ilgili yalnızca ortak anahtarlar görünebilir. Hesap sahipleri dışında hesaplara hiç kimse doğrudan erişemez. MONI uygulaması, tüm kredi kartı ve hesaplarını uygulamaya bağlayabilen gezginler tarafından da kullanılabilir. Yurtdışında MONI kartı çalınırsa veya akıllı telefonlarını kaybederse,

işlemleri izleyebilir ve kartı herhangi bir web tarayıcısından online olarak tamamen engelleyebilirler.

4.4.E-Stonia

Nispeten küçük bir nüfusa sahip olan Estonya, dijital hükümet için örnek gösterilecek bir ülkedir. Oylama ve vergi dahil olmak üzere, hükümetle ilgili tüm işlemleri çevrimiçi hale getiren sistem Estonya kimlik kartıdır.

Blokzincir destekli kimlik kartı, Estonyalıların bankacılık ve tıbbi reçete gibi e-hizmetlere dijital imzasıyla erişmelerini sağlıyor. Kimliği doğrulamak için artık bir devlet dairesinde sırada beklemeyi ortadan kalkmıştır.

Yazılım, işletim sistemleri ve teknik mimari şu anda diğer ülkelerin benzer hizmetler oluşturmalarına yardımcı olmak için ücretsiz olarak sunulmaktadır. Ayrıca, bu kimlik kartı işlevselliklerinin bir kısmını herhangi bir ülkenin sakinlerine yayan bir e-vize programı sunmaktadırlar.

4.5.Kimlic

2017 yılında kurulan Estonya merkezli girişim Kimlic, Quorum blokzincirinin desteklediği ve Google Play aracılığıyla erişilebilen merkezi olmayan bir kimlik doğrulama ekosistemidir. Parola'sız tanımlama işlemleri blokzincir teknolojisi ile sağlanır ve şirketlerin daha verimli süreçler için Müşteri Tanılama(KYC) verilerini kolayca, güvenli bir şekilde aktarmalarını sağlar.

Kimlic uygulaması kimliğinizi herhangi bir işletmeye kanıtlama imkanı sunar. Artık yinelenen müşteri tanıtma süreç ve işlemlerini ortadan kaldırır.

Parolasız kimlik doğrulama teknolojisi sayesinde kimlik verileriniz ve belgeleriniz güvenli bir şekilde aktarılır. Kimlik bilgilerinizi ve belgelerinizi cep telefonunuzdan doğrudan şirketlere aktarabilirsiniz. Yeni müşterinin kimliğini dakikalar içinde doğrulamaya veya önceden onaylanmış kullanıcıların işlemlerin hızlıca yapılmasına olanak tanır. Tüm bilgiler doğrudan bir kullanıcının mobil cihazından bir işletmeye, yol boyunca hassas bir şekilde durmaksızın aktarılır.

4.6.Persona

Persona blokzincir üzerine kurulu sıfır bilgi kimlik yönetim sistemidir. 2017 yılında kurulan Romanya merkezli platform, kullanıcıların üçüncü şahıslarla herhangi bir veri paylaşmadan kimliklerini kanıtlamalarını sağlamak için blokzincir protokollerini kullanarak bu gizliliği sürdürmektedir.

Persona, bireylerin paylaşmak istedikleri ayrıntılarla, kiminle paylaştıkları ve ne kadar süre kalacaklarını belirleyebilecekleri merkezi olmayan bir uygulama olarak tasarlanmıştır.

Persona, toplumu bir doğrulama biçimi olarak benimser. Bir kullanıcı kimliğini Persona ağında onayladıktan sonra, diğer kullanıcıların kimliklerini doğrulayıcı olarak hareket edebilir.

Ağda, % 90 onaylamaya ulaşmak için 16 kişinin onayı gerekiyor; diğer % 10 ise, kullanıcının istediği bir finans kurumu aracılığıyla onaylamak için bir finansal işlemden gelmelidir.

Kapsamı müşteriyi güçlendirmek ve ona kişisel verileri üzerindeki kontrolün yanı sıra kendi özel detaylarına erişimin güvenliğini sağlamaktır.

4.7.Object Tech

2016 yılında kurulan Object Tech, bireysel güvenli dijital vizelere yardımcı olmak için blokzincir destekli bağımsız kimlik sistemleri kullanıyor. AB destekli Object Tech ekibi, dijital pasaportların seyahat edenlerin uçaklarından kolayca çıkmalarını ya da yasal olarak seyahat ettiklerini doğrulamak zorunda kalmadan doğrudan bir taksi ya da kiralık araca binmelerini sağlayan bir gelecek öngörüyor. Dijital kimlik, seyahat eden kullanıcıları “izler”, kanıt işlevi gören doğrulanabilir bir defter oluşturur. Object Tech, sistemlerinin en yüksek gizlilik ve güvenlik standartlarına uygun olduğunu ve aynı zamanda vizyonunun geleceğin akıllı şehirleri ve toplulukları ile aynı doğrultuda olduğunu belirtmektedir.

4.8.SelfKey

SelfKey, entegre finansal hizmetler pazarı için blokzincir tabanlı olarak 2017 yılında kurulan bir dijital kimlik sistemidir. Özerk kimlik, SelfKey'in merkezindedir.

SelfKey, kullanıcıların kimlikleri ile ilgili tüm yönlerini kontrol altına almalarını sağlayacak sistemleri sunarak, diğer amaçların yanı sıra kripto para birimi yönetimi, finansal yatırım ve göç işlemlerinde kırılganlığı azaltmayı amaçlamaktadır.

Bireylerin ve şirketlerin dijital kimliklerini almalarını, kontrol etmelerini ve yönetmelerini sağlayan, dijital kimlik platformu oluşturmayı amaçlamaktadır. Dahası, kullanıcılar kimliklerini doğrulayabilir, kimlik belgelerini noterden alabilir ve yatırım, banka hesapları ve diğer hizmetlerle vatandaşlık ve ikamet imkanlarına erişebilirler.

Bu amaca ulaşmak için platform; kişisel olarak tanımlayıcı varlıkları ve belgeleri dijital olarak koruyan Kimlik Cüzdanı; çeşitli kimlikle ilgili hizmetlerin karşılaştırılması ve bunlara erişim için SelfKey Marketplace ve kullanıcıların SelfKey platformundaki diğer varlıkların yanı sıra noter ve doğrulama hizmetleri için ödeme yapmalarını sağlayan KEY Token gibi araçları içermektedir.

Çoğunlukla Asya pazarına odaklanmaktadırlar.

4.9.OVCODE

OVCODE, geliştirici merkezli, bireylerin, şirketlerin, kurumların ve hükümetlerin mevcut sistemleri blokzincir teknolojisi ile entegre olacak şekilde kolayca yükseltmelerini sağlayan doğrulama motorudur.

OVCODE, kullanıcılarının varlıklarına ilişkin blokzincir teknolojisini kullanan verilerin orijinalliğini, güvenilirliğini ve bütünlüğünü doğrulamaya odaklanmış, ödüllü patentli bir blokzincir teknolojisidir. Bu varlıklar dijital varlıklar, maddi olmayan duran varlıklar veya fiziksel varlıklar olabilir. OVCODE İsviçre, Güney Kore ve Filipinler'de güncel operasyonları bulunan İsviçre, Zürih'te kurulan bir girişimdir.

4.10.Authenteq

Authenteq, kullanıcıların kimliklerini doğrulamalarını ve bir blokzincir içinde şifreli olarak depolanan kendi dijital dijital kimliklerini oluşturmalarını sağlayan otomatik bir kimlik doğrulama ve gizlilik platformudur. Herhangi bir kişisel kullanıcı bilgisi, kullanıcıya aittir ve kullanıcı tarafından kontrol edilir ve Authenteq de dahil hiç kimse tarafından erişilemez. Authenteq ID ile, kullanıcılar talep doğrulama API kullanarak kimliklerini veya kimliğinin bir kısmını üçüncü taraflara doğrulamayı seçebilirler. İlk kayıt işlemi 60 saniyenin altında bir sürede gerçekleşir ve bundan sonra bir şifreye ihtiyaç duymadan doğrulama işlemi 3 saniyeden kısa sürer.

Authenteq ile, ister çevrimiçi bir pazar yeri, ister çevrimiçi bahis, finansal hizmet ve yakın zamanda ICO (İlk Dijital Para Arzı) veya jeton satış olsun, hemen her türlü çevrimiçi hizmetten faydalınabilir.

BÖLÜM 5. HYPERLEDGER INDY İLE DİJİTAL KİMLİK DOĞRULAMA UYGULAMASI

Uygulama geliştirilirken blokzincir teknolojisi olarak hyperledger indy aşağıdaki özelliklerden dolayı tercih edilmiştir.

Kimlik Doğrulaması: Hyperledger, izinli bir blokzincirdir ve kimlik yönetim modülü ile kimlik doğrulaması konusunda yardımcı olmaktadır.

Veri Gizliliği: Hyperledger kullanarak belirli bir kullanıcı grubuna özel yetki verebilirsiniz.

Mimari: Hyperledger'ın modüler mimarisi, geliştiricilerin ihtiyacı olan veya kullanmak istediği modülleri kullanmasına imkan sağlamaktadır.

Dil Seçenekleri: Hyperledger Java, Go ve NodeJS ile geliştirme yapmamıza imkan vermektedir.

Ücretsiz: İşlem yapmak için veya blokzincir üzerine veri tutmak için lisans veya ödeme yapmanıza gerek yoktur.

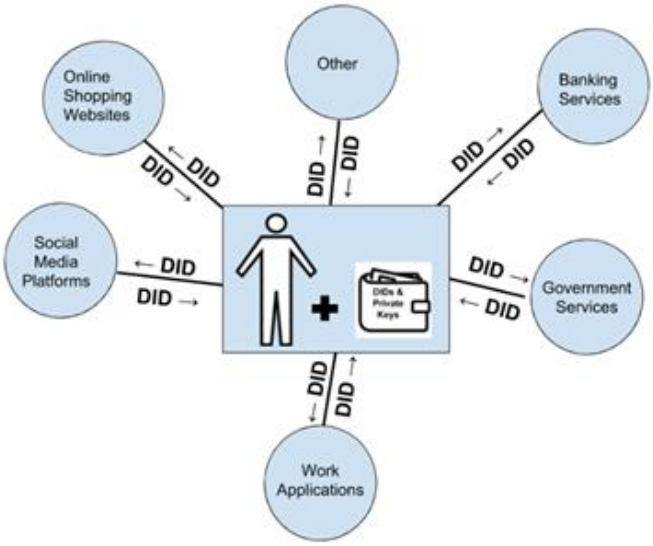
Hız: Public blokzincirler, ölçeklenebilirlik problemi sebebiyle yaşanan hız sorunları yüzünden pek tercih edilmiyor. Bu durumda devreye Hyperledger ve diğer izinli blokzincirler tercih ediliyor.

5.1.Temel Kavramlar

Hyperledger Indy, kim olduğunuzu başkalarına kanıtlamak için kullanabileceğiniz blokzincir tabanlı bir uygulamadır. Indy, kullanımı kolay, güven sağlayan ve gizliliği artıran bir mekanizma kullanarak internete bir kimlik katmanı ekler. Örneğin, hükümet, banka veya kurum gibi bilgilerinizi kontrol etmenizi sağlayan merkezi olmayan bir sistemdir.

Dağıtılmış Tanımlayıcılar(DID): Kullanıcı ve hizmetin web sitesi gibi iki kimlik arasında güvenli iletişim kurabilmesi için Dağıtılmış Tanımlayıcı(DID) kullanır. DID'ler, herhangi bir merkezi otoriteden bağımsız olarak, sahipleri tarafından oluşturulan, dünya genelinde benzersiz tanımlayıcılardır.

İnternette sahip olduğunuz her ilişki için bir tane olmak üzere bir çok DID'e sahip oluruz. DID'leri açık/özel anahtar çiftleri şeklinde güçlü şifreleme ile desteklenen, kullanıcı kimliği/şifre çifti olarak düşünebiliriz. Ayrıca, ilişkinin her iki tarafının da diğerleriyle iletişim kurması için DID'ler kullanılır.



Şekil 20. Dağıtılmış tanımlayıcı (www.hyperledger.org, 2019)

Kullanıcılar, dağıtılmış tanımlayıcı(DID) oluşturabilir ve bu DID'leri başkalarıyla güvenli bir şekilde iletişim kurmak için kullanabilir.

Agent ve Cüzdanlar: Sistemde birçok dağıtılmış tanımlayıcı(DID) oluştuğunda, bir kişinin oluşturduğu veya aldığı tüm DID'leri yönetmek için bellek ve kağıt parçalarının yeterli olmadığı açıktır. Hyperledger Indy, "Agent" terimini, diğer varlıklarla etkileşimde bulunan, DID'ler ve ilgili bilgiler için (özel anahtarlar dahil) bir veri deposu olarak "Cüzdan" terimini kullanır. Örneğin, bir kişinin akıllı cihazlarında bir mobil agent uygulaması olabilirken, kurumunların bulut sunucusunda çalışan bir kurumsal agent uygulaması olabilir. Tüm agentların kimlik verilerini depolamak için güvenli bir cüzdanı vardır. Agent'lar kimlik sahipleri tarafından kontrol edilir.

Hyperledger Indy Kayıt Defteri: Dağıtılmış tanımlayıcı(DID) oluşturan bir kişi veya kurum oluşturduğu DID'i Hyperledger Indy kayıt defterine yayınlar. Kayıt defterindeki DID ve ilişkili bilgiler daha sonra aranabilir fakat genel anahtarlarla ilişkilendirilmiş özel anahtarlar DID'nin sahibi tarafından cüzdanında tutulur. Özel anahtarlar korunduğu

sürece DID başkası tarafından kullanılamaz. Blokzincir teknolojisine dayanan merkezi olmayan bir sistemin kullanılması, kullanıcılara DID'lerini merkezi otorite olmadan güvenli bir şekilde kullanma olanağı sağlar.

Dağıtılmış tanımlayıcı(DID) kullanımı ile aşağıdaki problemlere çözüm üretmiş oluruz.

- Kullanıcılar kendi dağıtılmış tanımlayıcılarını(DID) tanımlar ve bu DID'i, onları tanımlamak için kullanılacak bir servise verir. Bu, merkezi tanımlayıcılar tarafından yaratılan sorunları giderir. DID'ler kullanıcı tarafından kontrol edilir.
- Agentlar ve cüzdanlar, şifre yöneticileri gibi davranır ve kullanıcıların sitelere ve servislere erişmelerini kolaylaştırır.
- Kullanıcı her servis için farklı bir DID kullandığından, kimlikleri ile servis arası ilişkilendirilemez.
- Kullanıcı ve servis DID'leri kullanarak iletişim kurabildiklerinden, bir kullanıcının bir e-posta adresi sağlamasına gerek yoktur
- Servis, kullanıcıya hizmetin yanı sıra ilişkileri için bir DID verir; böylece kullanıcı, servisle konuştuğundan emin olabilir.

Doğrulanabilir Kimlik Bilgileri: Hyperledger indy, kendimizle ilgili kimlik özellikleri (adımız, yaşımız, banka hesap numarası, derece, doğum yeri vb.) sağlamanın güvenilir bir yolunu sağlayan "Doğrulanabilir Kimlik Bilgileri" adlı yeni bir W3C standardını destekler.

Kimlik bilgileri, ehliyet, pasaport veya üniversite dereceleri gibi, bize gerektiğinde başkalarına göstermek için kullanabileceğimiz bir düzenleyici otorite tarafından verilen bilgilerdir. Doğrulanabilir kimlik bilgileri, kriptografik olarak işlenen kağıt kimlik bilgilerinin dijital eşdeğeridir ve kimlik bilgilerini isteyen aşağıdaki bilgilerden kesin bir şekilde emin olabilir.

- Bilgileri kim verdi
- Bilgilerin, iddiaları sunan kimliğe verildiğini
- Bilgilerin tahrif edilmediğini
- Kimlik bilgilerinin kurum tarafından iptal edilmediğini

Doğrulanabilir kimlik bilgileri için veri akışı, kağıt belgelerle aynıdır. Kurumlar, kimlik bilgilerini sahiblerine verir ve sahibleri bunları istediği zaman kullanabilirler. Indy'deki ispat ve ispat talepleri, doğrulanabilir kimlik bilgileri'nin sahibi ile doğrulayıcı arasında gerçekleşen işlemlerdir. Kimlik bilgilerini veren kurum, doğrulanabilir kimlik modelinin çok önemli bir niteliği olan ispat sürecine dahil değildir.(Yaşımızı kanıtlamak için kimliğimiz her kullanışımızı devletin bilmesini gerek yoktur.)

Doğrulanabilir kimlik bilgileri ve kullanımları, gerçek dünyadakileri taklit eder. Doğrulanabilir kimlik bilgileri bu modeli alır ve güvenilir bir şekilde çevrimiçi hale getirir.

Seçici Açıklama ve Sıfır Bilgi Kanıtları(ZKP): Hyperledger Indy, taleplerin kanıtlanmasında gelişmiş özellikler sunar. Spesifik olarak, istemlerin seçici bir şekilde açıklanabileceği, yani bir kimlik bilgilerinden sadece bazı veri öğelerinin bir kanıt olarak sağlandığı anlamına gelir. Sıfır bilgi kanıtları(ZKP), temel verileri sunmadan bir bilgi parçasının kanıtlanmasına izin verir. Örneğin doğum tarihine bakarak, bir kişinin, doğum tarihi ve adı da dahil herhangi bir bilgiyi açıklamadan, belirli bir yaştan büyük olup olmadığı kanıtlanabilir.

Doğrulanabilir kimlik bilgileri kullanımın faydaları;

- Dijital kanıt olmadan kimlik numaralarının olması hiçbir değere sahip olmayacaktır. Veri ihlallerinin değerini ve etkisini azaltır
- Çalışanın eğitim kimlik bilgilerini dijital olarak onaylayan bir işveren. İşveren, sertifikayı verenin uygun şekilde akredite edilmiş bir kurum olup olmadığını inceleyebilir.
- Mali müşavir ile bağlantı kuran bir kişi, danışmanın kimlik bilgilerini uygun devlet düzenleyicisi ile doğrulayabilir.
- Her serviste aynı bilgileri tekrar tekrar yazmak yerine (örneğin adres) adresini içeren bir doğrulanabilir kimlik ile sağlayabilir.
- Bir uzman çevrimiçi olarak hem endüstri kuruluşlarında mevcut üyeliğe sahip olduğunu hem de sigortasını kanıtlayabilir.

Bu işlemlerin tümü, günümüzde sıklıkla yüz yüze etkileşimler gerektiren, güvenilmez kağıt işlemleriyle yapılmaktadır. Doğrulanabilir kimlikler ile işlemler hızlı ve daha güvenlidir. Ayrıca kullanıcı doğrulanabilir kimliği elinde tuttuğu için, her bir işlem için gerektiği kadarını paylaşır.

Blokzincir, doğrulanabilir kimlik ve kanıtların yayınlanması ile Indy'de kilit rol oynar. Doğrulanabilir kimlikler özel bilgi içerdiklerinden, doğrulanabilir kimliklerin kendileri blokzincirde saklanmaz. Doğrulanabilir kimlik sahibinin cüzdanında saklanır. Bununla birlikte, doğrulanabilir kimliklerin kullanılması için gerekli olan bilgiler şema, ihraç sahibinin DID'i ve iptal edilmediğine dair bilgilerin tamamı Indy blok zincirinde saklanır. Bu güvenli bir şekilde, doğrulanabilir kimliklerin, kimlik bilgilerini ve talep alış verişinde kullanılacak kimliklerin sahibinin özel cüzdanında kişisel bilgileri korurken kullanmasını sağlar.

Gizlilik: Hyperledger Indy ‘nin gizlilikle ilgili özellikleri aşağıdaki gibidir;

- Sahip olunan işletme tarafından yaratılan ve kontrol edilen dağıtılmış tanımlayıcılar(DID)
- Her ilişki için DID'lerin kullanımı, hizmet arası korelasyonun önlenmesi
- İleti oluşturucudan alıcıya eşler arası, uçtan uca şifreleme
- Sahipleri tarafından tutulan ve yalnızca gerektiğinde kullanılan doğrulanabilir kimlik
- Doğrulanabilir kimlik verilerinin seçici kullanımı. Sadece gerekli verilerin gösterilmesi
- Kimiliği veren kurum ile iletişim kurmaya gerek kalmadan doğrulanabilir kimlik kullanımı

Blokzincir Türü: Indy, herkesin blokzincir'in (public) içeriğini görebileceği şekilde çalıştırılmak üzere tasarlanmıştır, ancak yalnızca "Stewards" olarak bilinen önceden onaylanmış katılımcıların doğrulama işlemine katılmasına izin verilir. Indy'nin genel bir ağ olarak çalışmak üzere tasarlanmış olmasına rağmen, Indy yalnızca ağı kullananların erişebileceği özel bir ağ olarak çalıştırılabilir.

Blockchain Konsensüs Algoritması: Tüm blokzincir uygulamalarında olduğu gibi, Hyperledger Indy, zincire eklenen bir sonraki bloğun içeriğine karar vermek için bir

fikir birliği algoritması kullanır. Spesifik olarak Indy, Yedekli Bizans Hata Toleransı (RBFT) algoritmasının bir uygulaması olan Plenum'u kullanır. Plenum, ideal koşullarda diğer BFT algoritmalarına benzer performans gösterir ancak ağda problem meydana geldiğinde performansı diğer algoritmalara göre (% 3-78) düşer. Ayrıca, Indy'nin fikir birliği algoritmasının altında yatan şey ağın düğümleri arasında güvenli ve sağlam bir mesajlaşma sistemidir. Bu, Indy'nin genel güvenliğini arttırır.

Indy ağında kabul edilebilir eşzamanlı düğüm başarısızlığı sayısı, Indy'nin Plenum konsensüs algoritmasının önemli bir parametresidir. F düğümü arızalarından kurtulabilen bir Plenum ağı en az 3F + 1 düğümüne sahip olmalıdır. Bir düğümün kaybına dayanabilecek minimum ağ (F=1) için en az 4 düğüme sahip olmalıdır. Bununla birlikte, ağa çok fazla düğüm eklemek de sorunludur, düğümler ne kadar fazla olursa, fikir birliğine varmak o kadar uzun sürer.

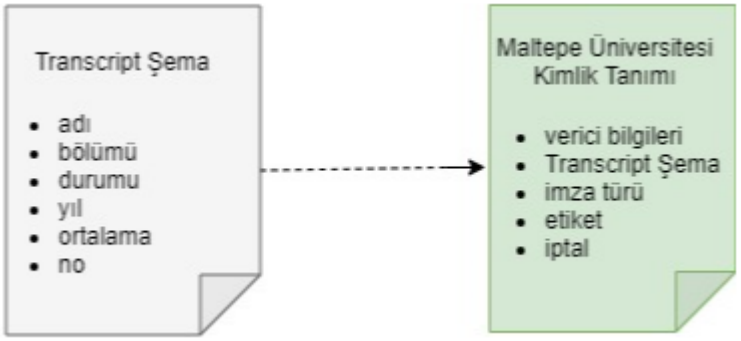
5.2.Kimlik Doğrulama Uygulaması

Bu bölümde geliştilen uygulumanın nasıl çalıştığını göstereceğiz. Kurgusal olarak Maltepe Üniversitesi mezunu olan Elif, Doruk A.Ş şirketindeki bir işe başvurmak için, Maltepe Üniversitesindeki transkriptini iş başvurusunda eğitiminin kanıtı olarak kullanmak istiyor. Bunu ortaya çıkarmak için gereken kimlik ve güven etkileşimi bugün dünyada dağınık, yavaş, mahremiyeti ihlal ediyor ve sahtekarlığa açıktır.

Elif, Doruk A.Ş'deki işe başvurabilmesi için Maltepe Üniversitesinin verdiği yeni ve taşınabilir bir kimliğe ihtiyacı olacak ve Elif'in izni olmadan hiç kimse bu kimliği kullanamayacaktır. Bu özerk ve özdeş bir kimliktir. Elif transkript alabilmesi için Maltepe Üniversitesine bir bağlantı isteği talebinde bulunur ve Maltepe Üniversitesi ile bağlantı kurma isteğini kabul edip etmediği sorulacaktır. Sonrasında Elif, Maltepe Üniverstesiden aldığı kimlik(transkript) ile Doruk A.Ş deki işe başvuracaktır. İşlem adımları aşağıdaki gibi gerçekleşir.

Adım 1: Şemaların oluşturulması: Şemalar, devlet veya yetkili kurumlar tarafından düzenlenmekte ve blokzincire kaydedilmektedir. Şemalar herkes tarafından erişilebilmektedir.

Adım 2: Kimlik Tanımlarının oluşturulması: Kimlik belgesi verecek olan kurumlar daha önce oluştulan şemaları referans olarak kendi kimlik tanımlarını oluştururlar. Kimlik bilgisi tanımı, kullandığı şemayı ve ayrıca kimlik bilgisi tanımını veren kişi hakkında gerekli bilgileri içerir. Oluşturulan kimlik tanımları blokzincire kaydedilir.

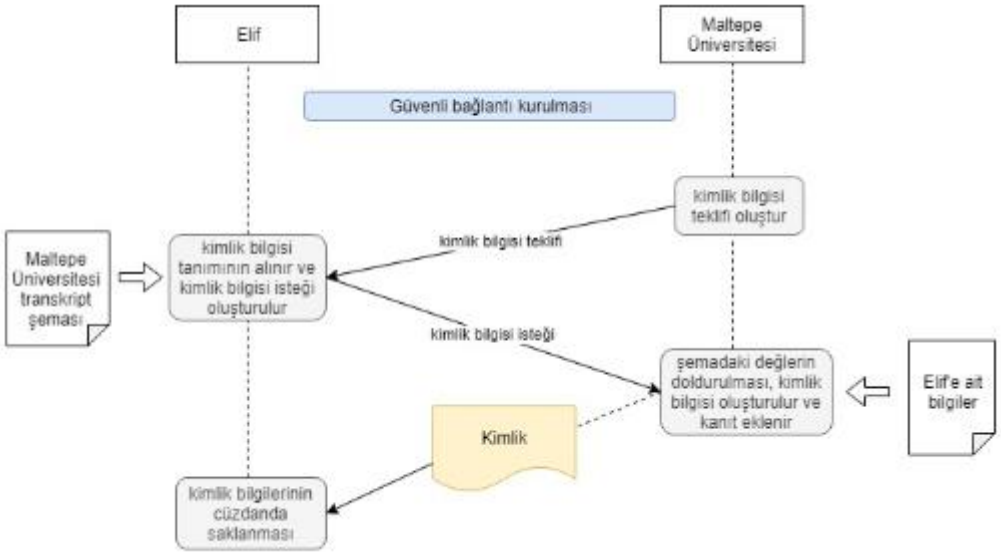


Şekil 21.Şema ve kimlik tanımı arasındaki ilişki

Örneğimizde, Elif, Maltepe Üniversitesinden bir transkript(kimlik belgesi) alıyor ve daha sonra işe başvururken Doruk A.Ş'ye eğitiminin yeterlilik belgesi olarak veriyor.

Adım 3: Elif'in, Maltepe Üniversitesinden transkript alması:

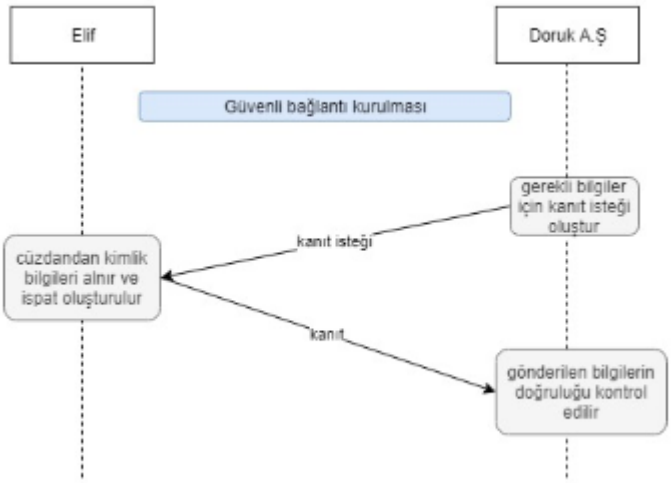
- Maltepe Üniversitesi ve Elif arasında bağlantı kurulması için Elif, Maltepe Üniversitesine bağlantığı isteği gönderir.
- Maltepe Üniversitesi, Elif'e kimlik bilgisi teklifi oluşturur ve gönderir.
- Elif, blokzincirden Maltepe Üniverstesine ait kimlik tanımını alır, kimlik isteği oluşturur ve Maltepe Üniversitesine gönderir.
- Maltepe Üniversitesi, Elif için kimlik bilgisi oluşturur. Oluşturulan kimlik içerisinde, Maltepe Üniversitesine ait kimlik tanımında yer alan bilgiler bulunur. Elif daha sonra bu bilgileri Doruk A.Ş tarafından istendiğinde eğitimin kanıtı olarak kullanır.
- Elif kimlik bilgisini alır ve kendi cüzdanında saklar.



Şekil 22.Elif'in transkript alması

Adım 4: Doruk A.Ş'nin, Elif'ten eğitim bilgilerini istemesi

- Doruk A.Ş ve Elif arasında bağlantı kurulması için Elif, Doruk A.Ş ye bağlantığı isteği gönderirir.
- Doruk A.Ş kendisi için gerekli olan bilgileri içeren prova talebi oluşturur. Bu durumda Doruk A.Ş, Maltepe Üniversitesin verdiği bilgileri eğitimin kanıtı olarak istemiş olur.
- Elif, kanıt isteğini alır ve Maltepe Üniverstesinden aldığı transkripte dayanarak ispat oluşturur. İspat içerisinde Doruk A.Ş'nin kanıt isteğini karşılaycak bilgiler vardır.
- Doruk A.Ş, kanıtı Elif'den alır. Kanıt içinde Doruk A.Ş için gerekli olan bilgileri görür ve bu bilgilerin Maltepe Üniversitesinden geldiğini doğrular.
- Doruk A.Ş bu kanıtı kabul eder.



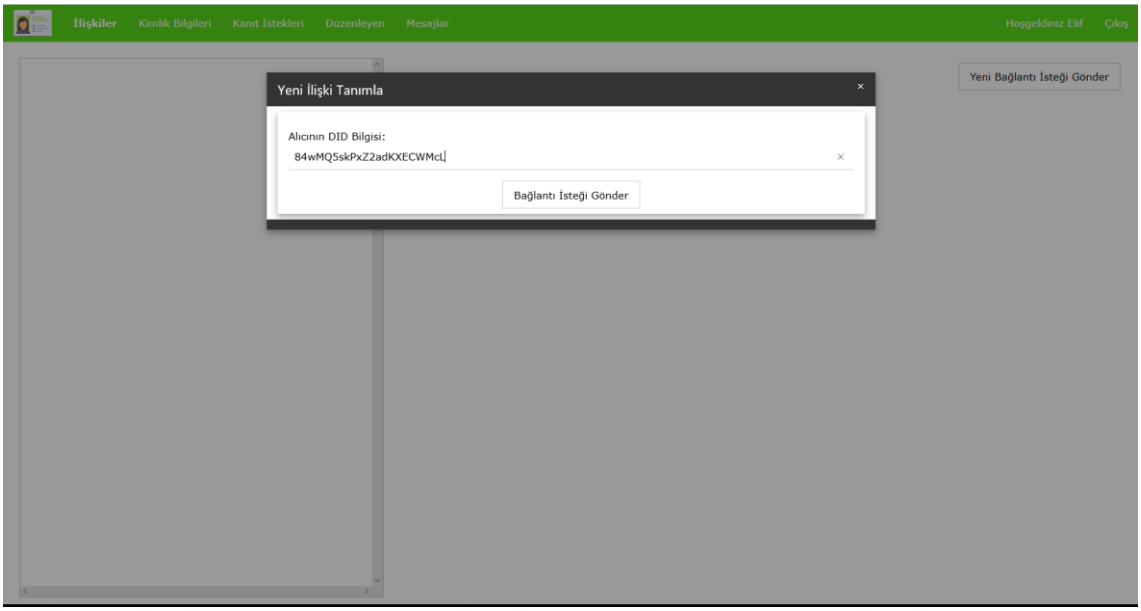
Şekil 23.Elif, Doruk A.Ş için ispat oluşturması

Tüm bu süreçte blokzincirde, merkezi olmayan tanımlayıcılar, verinym ve doğrulama anahtaları saklanır. Ayrıca hem kimlik bilgisi tanımları hem de kimlik bilgileri ile belirtilen öğelerin yapısını tanımlayan şemalar da blokzincirde saklanır. Bir şemanın üzerine inşa edilen kimlik tanımı ve ayrıca kanıtın oluşturulması için vericinin bilgileri herkesin erişimine açıktır. Blokzincirde herkese açık bir şekilde saklanan bilgiler kanıt oluşturulurken güven kaynağı sağlar.

Kişisel hiçbir bilgi blokzincirde saklanmaz. Kimlik bilgileri eşler arası bağlantı yoluyla iletilir ve bu bilgiler doğrulanmış şifreleme ile güvence altına alınır. Paylaşılan bilgiler yalnızca iki tarafça bilinir. Bu nedenle, hiçbir kimlik bilgisi kamuya açıklanmazken, blokzincirdeki bilgiler ispat üzerinde güçlü bir güven sağlar.

İşlemlere ait uygulama adımları ve ekran görüntüleri aşağıdaki gibi gerçekleşir.

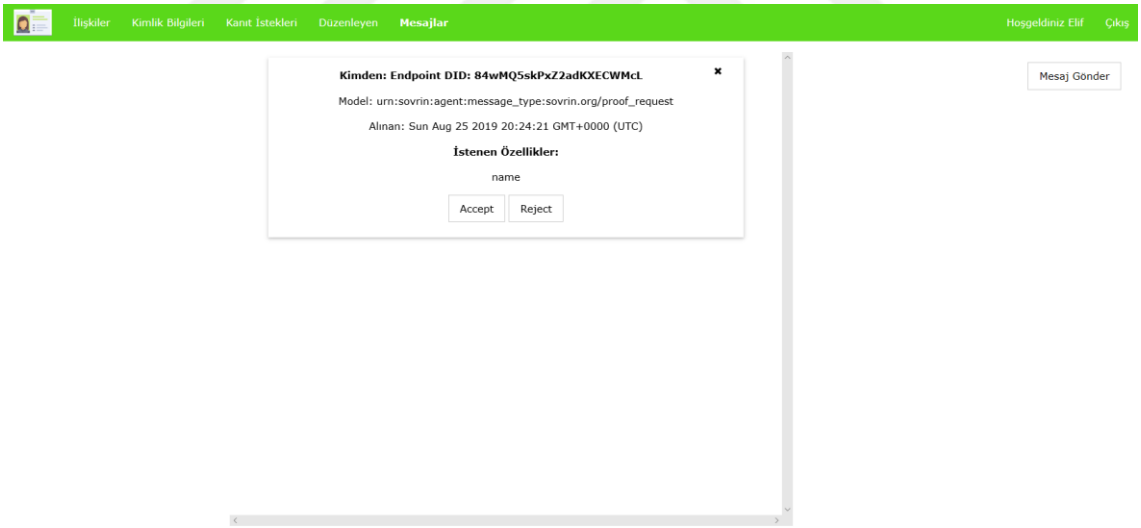
1. Elif, Maltepe Üniversitesinden kimlik(transkript) almak için Maltepe Üniverstesine bağlantığı isteği gönderir.



Şekil 24.Elif'in Maltepe Üniversitesine bağlantı isteği göndermesi

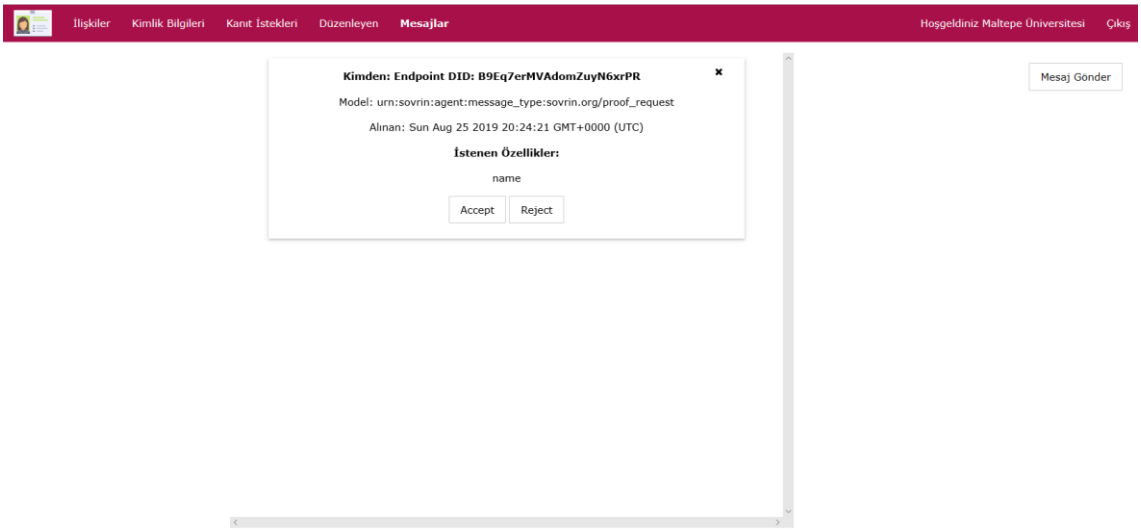
2. Hem Elif hem de Maltepe Üniversitesi bağlantığı isteğini kabul eder.

Elif'in sayfası:



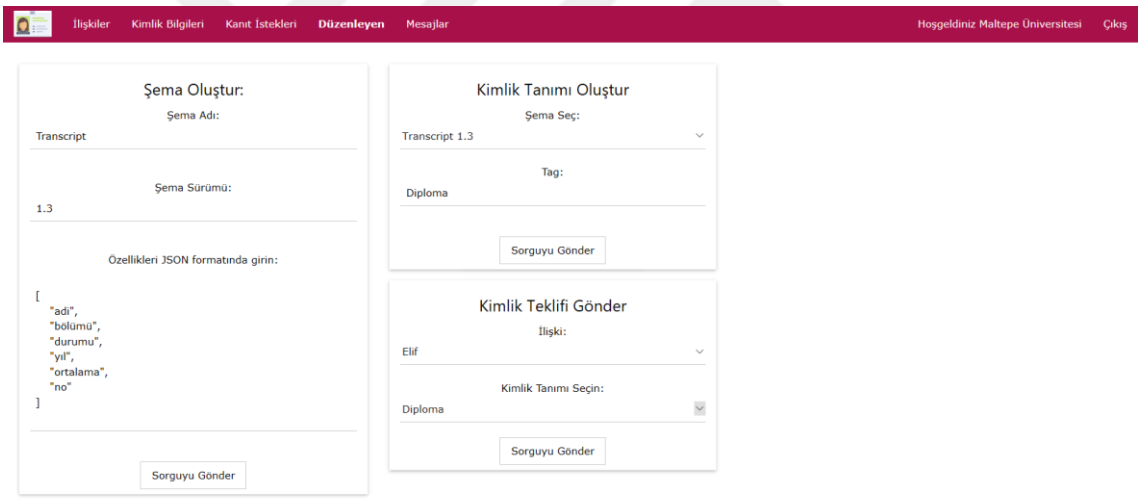
Şekil 25. Elif için Maltepe Üniversitesi ile ilişki onayı

Maltepe Üniversitesinin sayfası:



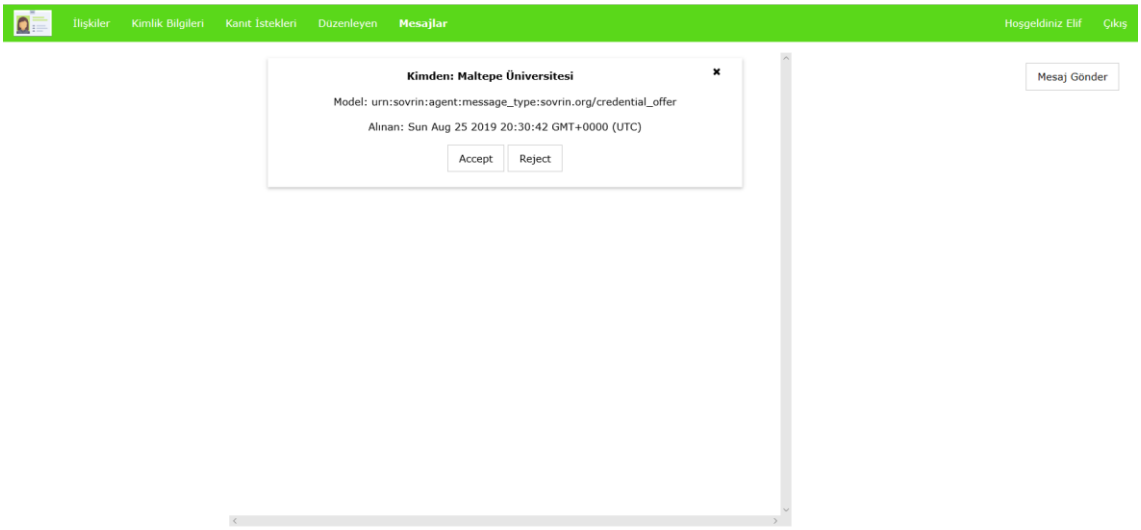
Şekil 26. Maltepe Üniversitesi için Elif ile ilişki onayı

3. Maltepe Üniversitesi, Elif için kimlik teklifi gönderir.



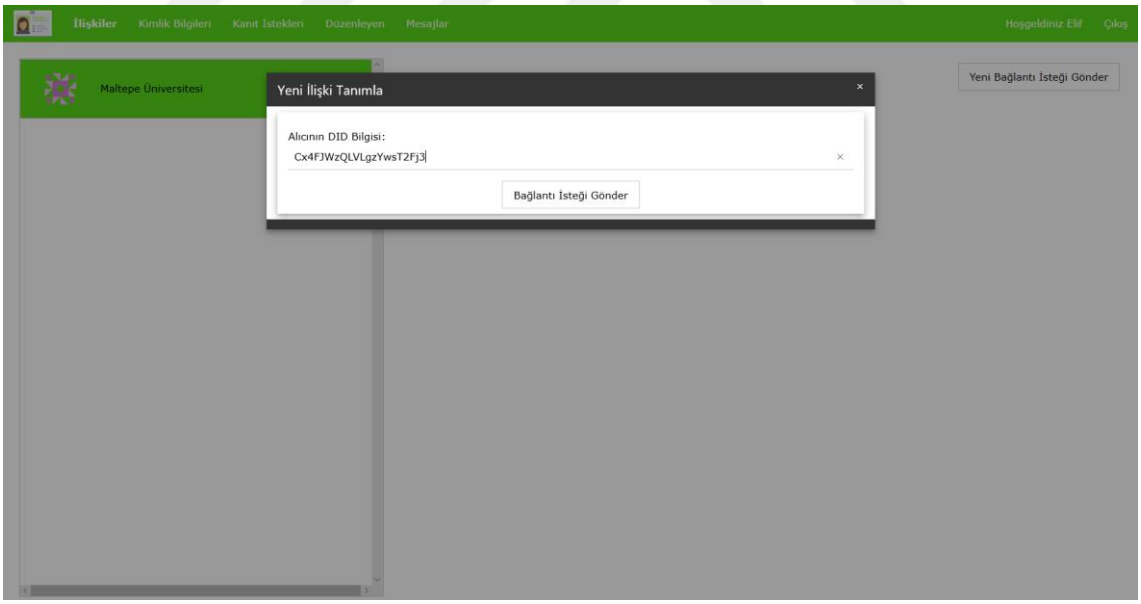
Şekil 27. Maltepe Üniversitesinin kimlik teklifi göndermesi

4. Elif, Maltepe Üniversitesinin oluşturduğu kimliği kabul eder.



Şekil 28. Elif'in kimliği kabul etmesi

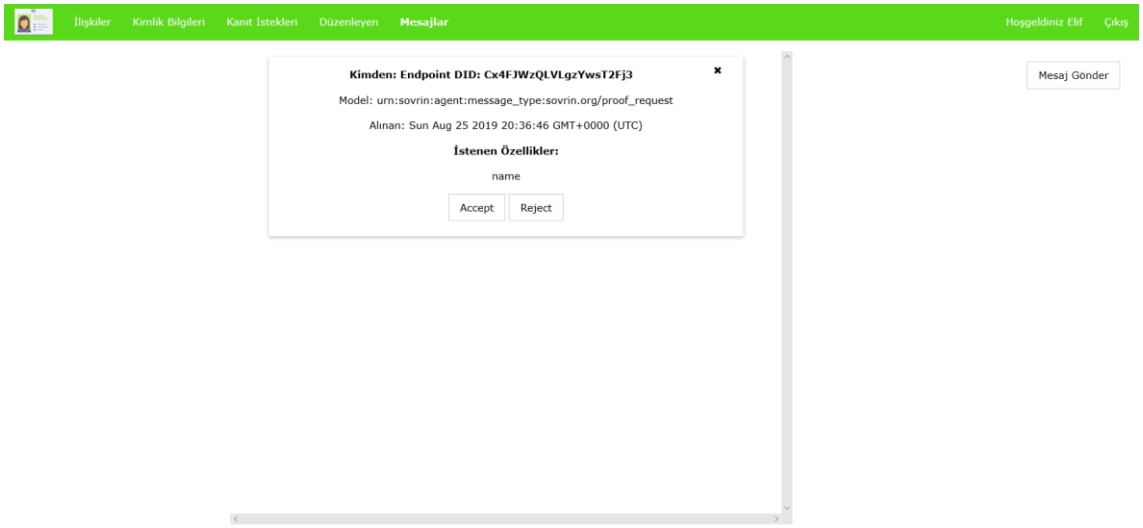
5. Elif, Doruk A.Ş deki işe başvuruda bulunur.



Şekil 29. Elif'in Doruk A.Ş'ye bağlantı isteği göndermesi

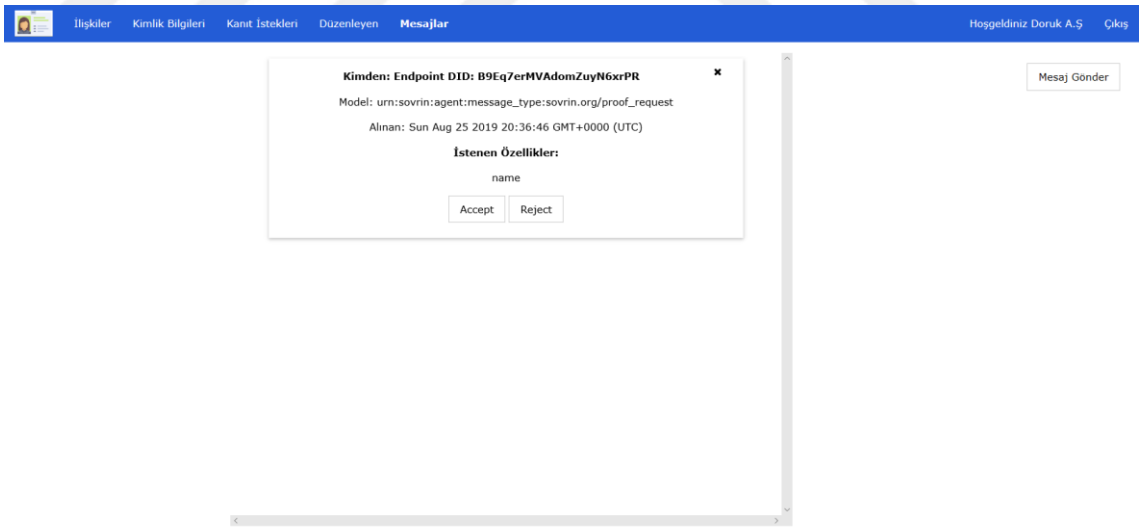
6. Hem Elif hem de Doruk A.Ş bağlantı isteğini kabul eder.

Elif'in sayfası:



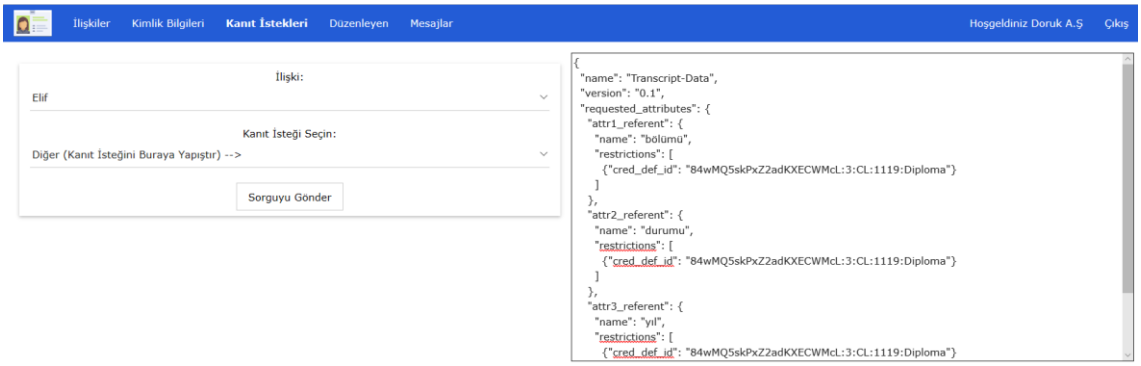
Şekil 30. Elif için Doruk A.Ş ile ilişki onayı

Doruk A.Ş'nin sayfası:



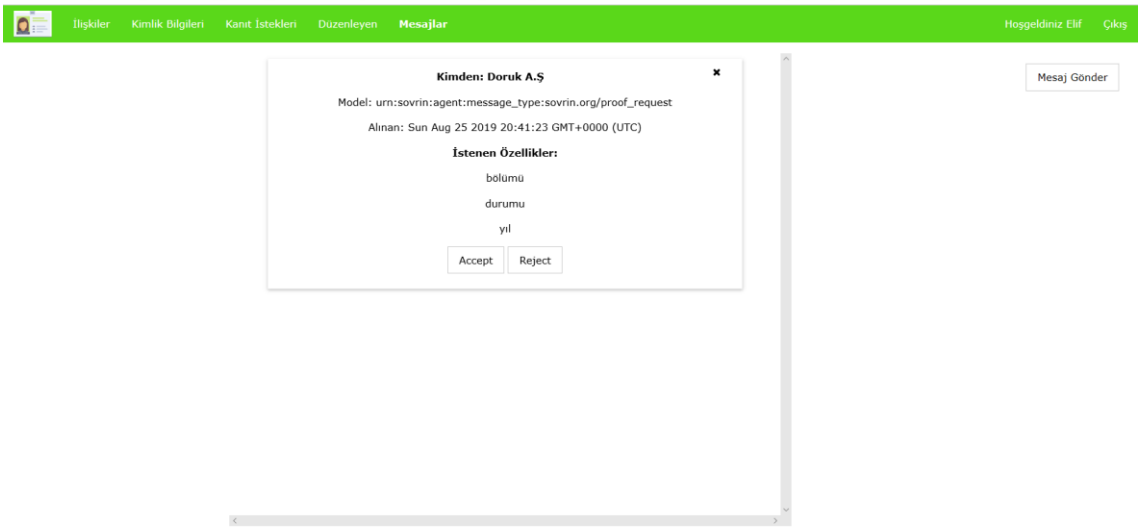
Şekil 31. Doruk A.Ş için Elif ile ilişki onayı

7. Doruk A.Ş kimlik bilgilerini ister.



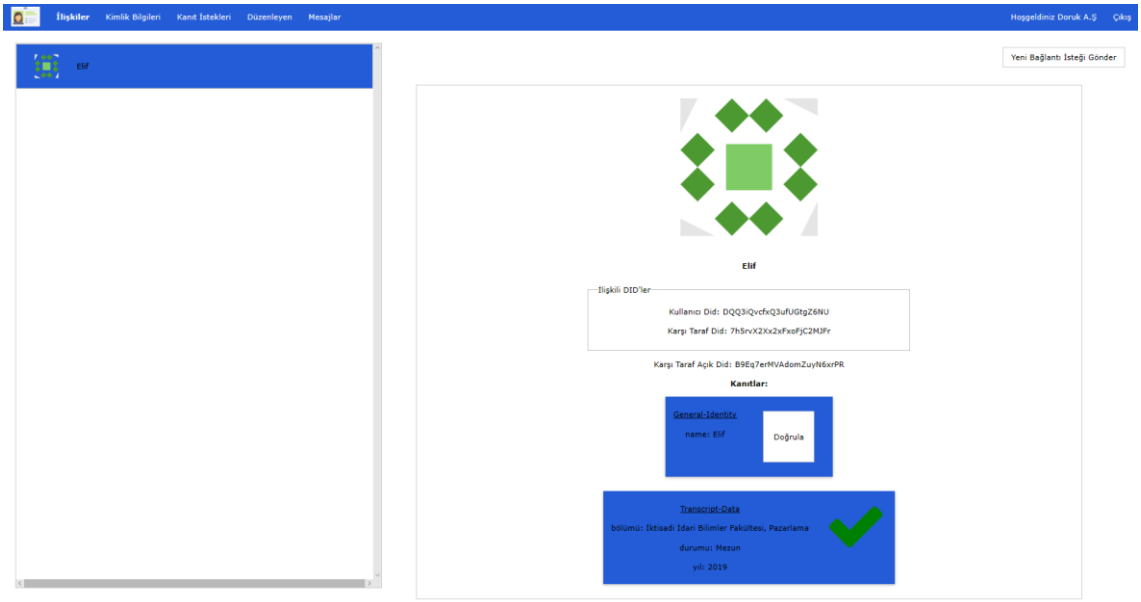
Şekil 32. Doruk A.Ş'nin kimlik bilgilerini istemesi

8. Elif Doruk A.Ş den gelen isteği onaylar



Şekil 33. Elif'in Doruk A.Ş ile kimlik bilgilerini paylaşması

9. Doruk A.Ş, Elif'e ait transcript bilgilerini doğrular.



Şekil 34. Doruk A.Ş, Elif'e ait kimlik bilgilerini doğrulması

BÖLÜM 6. SONUÇ

İnsanlar doğumla birlike verilen nüfus cüzdanına ek olarak, sosyal, eğitim ve iş hayatı gibi kazandığı statülere ait bir çok farklı kimliğe de sahiptir.

Kimlik doğrulama, bir kişinin veya bir uygulamanın gerçekte iddia ettiği kişi veya uygulama olduğunun tespit edilmesi amacıyla yapılan işlemler sürecidir. Günümüzde bu süreç kağıt üzerinde gerçekleştirilmektedir. Eğitim, sağlık, finansal işlemler ve abonelik işlemleri gibi bir çok işlemde kimliğimizin fotokopisi istenir. Böylelikle paylaşılmaması gereken bir çok bilgi yetkisiz kişilerle paylaşılmış olur. Kağıt üzerinde yapılan işlemler hataya açıktır. Aynı zamanda evrak sahteciliği gibi güvenlik zafiyetini beraberinde getirir.

Günümüzde kimlikle ilgili en büyük sorun güvendir. Herhangi bir web sayfasına üye olduğumuzda kimliğimizle ilgili bir çok bilgi istenir. Bu bilgiler siteler arasında ilişkilendirilir ve hakkımızda çıkarımlar yapılmasına izin veririr. Google, Facebook, Amazon gibi bir çok büyük şirket kullanıcı verisinin satılması yada çalınması ile ilgili işlemlere maruz kalmaktadır. Aynı zamanda merkezi veritabanları bilgisayar korsanlarının açık hedefidir. Kullanıcı verilerinin ihlali ile ilgili sık sık haberler çıkmaktadır.

Blokzincir, merkezi olmayan yapısı ile güvenilir bir üçüncü tarafa ihtiyaç duyulan bir çok sektörde kullanılabilcek bir teknolojidir. Blokzincirde herhangi bir kullanıcının işlem sırasında karşı tarafa veya merkez bir aracıya güvenmesi gerekmemektedir. Bitcoin başarılı bir şekilde uygulanması ile blokzincire olan güven ve blokzincirin kullanım yaygınlığı giderek artmaktadır.

Yapılan bu çalışma ile kimlik doğrulama işlemlerinde blokzincir teknolojisinin kullanılması önerilmiştir. Kişinin kimliğinin sahibi olduğu, kimlik bilgilerini paylaşırken sadece gerektiği kadar bilginin paylaşıldığı ve kazandığı statülerden elde ettiği kimliği ihtiyaç duyduğu yerlerde kullanabileceği bir yapı oluşturulmaya çalışılmıştır. Kimlik bilgilerinin kişinin kontrolünde olması ile merkezi yapıların zayıflıkları ortadan kalkacağı düşünülmektedir.

Blokzincir, gelişme potansiyeli yüksek bir teknoloji olmakla birlikte her yeni teknloijinin gelişim aşamasında yaşadığı riskler, zayıflılıklar ve kullanımı ile ilgili

zorluklar içermektedir. Ayrıca merkezi olmayan dijital kimlik sisteminin yaygınlaşabilmesi için, teknik altyapı, kimlik stadandartları, hukuki boyutu, yaşam döngüsü gibi konularının kamu ve özel paydaşlarla birlikte oluşturulması gerekmektedir.

KAYNAKÇA

Antonopoulos, M.Andreas. *"Mastering Bitcoin", O'Reilly, 330 s.* 2014.

Balcısoy, Erşen. *Yüksek performanslı bitcoin madenciliği için SHA256 özet algoritmasının eniyilenmesi, TOBB Ekonomi ve Teknoloji Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi*. Ankara, 2017.

Baran, P. *On Distributed Cominications Networks. The Rand Corporation (Vol.1). Santa Monica. Erişim adresi: http://pages.cs.wisc.edu/~akella/CS740/F08/740-Papers/Bar64.pdf.* 1962.

Başak, Mustafa. *Elektronik kimlik uygulamaları için tasarlanmış akıllı kart işletim sistemi ve gelişmiş güvenlik yöntemi, İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi*. İstanbul, 2014.

Beck, R., J. S. Czepluch, N. Lollike & S. Malone. *"Blockchainthe Gateway to Trust-Free Cryptographic Transactions". European Conference on Information Systems , 153.* 2016.

Bicakci, K. *"Kullanışlı Güvenlik için Temel Prensipler", 4. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, Ankara, Türkiye, 102-107*. 2010.

Bitcoin.org. "Bitcoin - Open Source P2P Money. Erişim tarihi: Haziran, 2017,Erişim adresi: https://bitcoin.org/," 2009.

Boucher, P., S. Nascimento & M Kritikos. *How blockchain technology could change our lives, 28. Brussels: European Parliamentary Research Service. Erişim adresi: https://doi.org/10.2861/926645*. 2017.

Crosby, M., P. Pattanayak, S. Verma & V. Kalyanaraman. *"Blockchain technology: Beyond bitcoin. Applied Innovation", 2, 6-10*. 2016.

Çarkacıoğlu, Abdurrahman. *"Kripto-Para Bitcoin", 330 s*. 2014.

Da, W. *"b-money," http://www.weidai.com/bmoney.txt*. 1998.

digiconomist.net. "Bitcoin Energy Consumption Index - Digiconomist. Retrieved October 9, 2017, Erişim tarihi: Eylül, 2017, Erişim adresi: https://digiconomist.-net/bitcoin-energy-consumption#assumptions," 2017.

Dulaney, E. *"CompTIA Security+ Study Guide: Exam SY0-301", Sybex, 5th Ed., Hoboken NJ, 307-309*. USA, 2011.

Eren, A Murat. *Açık anahtarlı kriptografi, Penguence Sayı:2*. 2005.

GOS. "(Government Office of Science). Distributed Ledger Technology: Beyond Block Chain. London: Government Office for Science, 1–88. Erişim adresi: https://www.gov.uk-/government/publications/distributed-ledger-technologyblackett-review," 2015.

Gronbaek, H. *Blockchain 2.0, Smart Contracts and Challenges. Erişim adresi: https://www.twobirds.com/en/news/articles/2016/uk/blockchain-2-0--smartcontracts-and-challenges*. 2016.

http://bitcoin.be. "http://bitcoin.sipa.be/," 2019.

http://www.webcitation.org. "Federal Financial Institutions Examination Council. Authentication in an Internet Banking Environment.. 2014-10-06. URL:http://www.e-janco.com/Downloadfiles/banking_guidance.pdf," 2014.

https://blockchain.info. "https://blockchain.info/tr/charts/hash-rate," 2019.

"https://blockchain.info/charts/hash-rate," [t.y.].

https://blokzincir.bilgem.tubitak.gov.tr. *https://blokzincir.bilgem.tubitak.gov.tr/blok-zincir.html*. [t.y.].

Jain A. K., Ross A., Pankanti S. *Biometrics: a tool for information security, IEEE Transactions on Information Forensics and Security, vol.1, no.2, 125-143*. 2006.

Kakıcı, Ahmet. *Biyometrik Tanıma Sistemleri. Erişim Tarihi: 01 Mayıs 2013, http://www.ahmetkakici.com/genel/biyometrik-tanima-sistemleri*. 2013.

Khan, W. Z., Aalsalem, M. Y. and Xiang, Y. *A graphical password based system for small mobile devices," Australia (8) 145-150*. 2011.

Kuo, C., Romanosky, S. and Cranor, L. F. *"Human selection of mnemonic phrase-based passwords" in Proceedings of the Second Symposium on Usable Privacy and Security, Pittsburgh, PA, USA, 67-78*. 2006.

Mills, D., K. Wang, B. Malone, A. Ravi, J. Marquardt, C. Chen & M. Baird. "Distributed Ledger Technology in Payments, Clearing, and Settlement. Finance and Economics Discussion Series, 2016(95), 1–36. Washington: Board of Governors of the Federal Reserve System, Erişim adresi: https://doi.org/10.17016/FEDS.2016.095," 2016.

Murat, Mehmet. *Blockchain ile güvenli elektronik sağlık sistemi*. 2014.

Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf*. 2008.

Narayanan, A., J. Bonneau, E. Felten, A. Miller & Goldfeder. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. New Jersey: Princeton University, 2016.

Paivio, A., Rogers, T. B. and Smythe, P. C. *"Why are pictures easier to recall than words?" Psychonomic Science, (11), 137-138*. 1968.

Pinna, A. & W. Ruttenberg. *Distributed Ledger Technologies in Securites Post-Trading. European Central Bank: Occasional Paper Series. Frankfurt am Main.https://doi.org/10.2866/270533*. 2016.

Price, R. *The 21 Companies That Control Bitcoin, Business Insider UK, http://uk.businessinsider.com/bitcoin-pools-miners-ranked-2015-7*. 2015.

Rejman-Greene, M. *"Biometrics—real identities for a virtual world" BT Technology Journal, (19), 115-121.]*. 2001.

Shannon, Caulde E. *"Communication Theory of Secrecy Systems", A Mathematical Theory of Cryptography 657-715*. Newyork, 1946.

Stallings, William. *Cryptography and Network Security Principles and PracticeSecond Edition, Prentice Hall*. 2000.

Swan, M. *Blockchain Blueprınt For A New Economy. (Tim McGovern, Ed.) (1.Baskı). Sebastopol: O'Reilly Media, Inc.* 2015.

The Economist. "The Trust Machine. New York: The Economist Online. Erişim tarihi: Haziran, 2017, Erişim adresi: https://www.economist.com/news/leaders-/21677-198-technology-behind-bitcoin-could-transform-how-economy-workstrust-machine.," 2015.

Usta, Ahmet & Serkan Doğantekin. *Blockchain 101*. İstanbul, 2017.

WEF, Survey Report, Shift, Deep. *Technology Tipping Points and Societal Impact. Geneva: World Economic Forum. Erişim adresi: http://www3.weforum-.org/docs/WEF_GAC15_Technological_Tipping_-Points_report_2015.pdf*. 2015.

Woodward. D., Orlans, N. M. and Higgins, P. T. *Biometrics:identity assurance in the information age: McGraw-Hill/Osborne, New York, 434.* 2003.

www.businessinsider.com. "http://www.businessinsider.com/bitcoin-technology-blockchain-only-halfway-through-its-evolution-2018-1," 2018.

www.cbronline.com. "https://www.cbronline.com/news/global-data-breaches-2018," 2018.

www.hashcash.org. "http://www.hashcash.org/papers/announce.txt," 1997.

www.hyperledger.org. "https://github.com/hyperledger/hyperledger/wiki/Whitepaper-WG. hyperledger.org," 2016.

www.hyperledger.org. "https://hyperledger-indy.readthedocs.io," 2019.

www.hyperledger.org. "https://www.hyperledger.org," 2019.

"www.kamusm.gov.tr," 2018.

www.tubitak.gov.tr. "https://blokzincir.bilgem.tubitak.gov.tr/blok-zincir.html," 2019.

Yaga, D., P. Mell, N. Roby & K. Scarfone. *Blockchain technology overview. Alındığı tarih: 01.03.2018, adres: https://csrc.nist.gov/publications/ detail/nistir/8202/draft. (s.23)*. 2018.

Yerlikaya, Tarık. *Yeni şifreleme algoritmalarının analizi, Trakya Üniversitesi*. 2006.

Yıldırım, Mustafa. "Kablosuz ağlarda erişim güvenliği ve kimlik doğrulama, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi," 2014.

Yüksel, Ali Umut. "Tek kullanımlık (atılabilir) kimlik doğrulamalı anahtar değişimi yazılım uygulamasının geliştirilmesi, Hacettepe Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi," 2006.