T.C
İSTANBUL AYDIN ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BLOCK-CHAIN TEKNOLOJİSİ VE B2B FİNANS İŞLEMLERİNDE KULLANILABİLİRLİĞİ

YÜKSEK LİSANS TEZİ

Onur YILMAZ

Bilgisayar Mühendisliği Anabilim Dalı

Bilgisayar Mühendisliği Programı

HAZİRAN - 2019

T.C.
İSTANBUL AYDIN ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BLOCK-CHAIN TEKNOLOJİSİ VE B2B FİNANS İŞLEMLERİNDE KULLANILABİLİRLİĞİ

YÜKSEK LİSANS TEZİ

Onur YILMAZ
(Y1513.010040)

Bilgisayar Mühendisliği Ana Bilim Dalı

Bilgisayar Mühendisliği Programı

Tez Danışmanı: Dr. Öğr. Üyesi Mehmet Kamil TULGA

HAZİRAN- 2019

T.C.
İSTANBUL AYDIN ÜNİVERSİTESİ
FEN BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜ

Yüksek Lisans Tez Onay Belgesi

Enstitümüz Bilgisayar Mühendisliği Ana Bilim Dalı Bilgisayar Mühendisliği Tezli Yüksek Lisans Programı Y1513.010040 numaralı öğrencisi **Onur YILMAZ**' ın **"BLOCK-CHAİN TEKNOLOJİSİ VE B2B FİNANS İŞLEMLERİNDE KULLANILABİLİRLİĞİ"** adlı tez çalışması Enstitümüz Yönetim Kurulunun 12.06.2019 tarih ve 2019/12 sayılı kararıyla oluşturulan jüri tarafından Oybirliği ile Tezli Yüksek Lisans tezi olarak Kabul..edilmiştir.

Öğretim Üyesi Adı Soyadı	**İmzası**
Tez Savunma Tarihi : 04/07/2019	
1)Tez Danışmanı: Dr. Öğr. Üyesi Mehmet Kamil TULGA	.....
2) Jüri Üyesi : Prof. Dr. Ali GÜNEŞ	.....
3) Jüri Üyesi : Dr. Öğr. Üyesi Ferdi SÖNMEZ	.....

Not: Öğrencinin Tez savunmasında **Başarılı** olması halinde bu form **imzalanacaktır.** Aksi halde geçersizdir.

YEMİN METNİ

Yüksek Lisans tezi olarak sunduğum “Block-Chain Teknolojisi ve B2B Finans İşlemlerinde Kullanılabilirliği” adlı çalışmanın, tezin proje safhasından sonuçlanmasına kadarki bütün süreçlerde bilimsel ahlak ve geleneklere aykırı düşecek bir yardıma başvurulmaksızın yazıldığını ve yararlandığım eserlerin Bibliyografya’da gösterilenlerden oluştuğunu, bunlara atıf yapılarak yararlanılmış olduğunu belirtir ve onurumla beyan ederim. (…/…/20..)

Onur YILMAZ

Eşime ve Aileme,

ÖNSÖZ

Bu çalışmanın yürütülmesi sırasında zaman ayrımı yapmaksızın her zaman destek ve yardımcı olan, destek veren sözleriyle tüm olumsuzlukları ortadan kaldıran danışman hocam Dr. Mehmet Kamil Tulga'ya, yaptığı katkılar ve desteklerden dolayı Prof. Dr. Zafer Utlu'ya, teknik desteğe ihtiyaç duyduğumda yardımıma koşan, değerli bilgilerini benimle paylaşan sevgili hocam Dr. Kubilay Kaptan'a ve sevgili eşi Av. Rukiye Kaptan'a, çalışmanın sonuçlandırılmasında ki katkılarından dolayı Öğr. Gör. Arif Karabuğa'ya, güler yüzlülüğü ile etrafına pozitif enerji saçan sevgili hocam Öğr. Gör. Buket Dönmez'e, desteklerini her zaman dile getiren Nalan Üker ve Recep Üker'e, çalışmalara katkılarından dolayı meslektaşım Muhammed Cihad Turan'a, mesai arkadaşlarıma, gösterdiği büyük sabır ve desteklerinden dolayı eşim Fatma Yılmaz'a, tez yazım süresince kendilerine zaman ayıramadığım fakat her zaman bana destek olan sevgili anneme, babama, Yılmaz ve Bal ailesine teşekkür ederim.

Haziran 2019 Onur YILMAZ

İÇİNDEKİLER

Sayfa

KISALTMALAR

ATM : Bankamatik (Automated Teller Machine)
BDDK : Bankacılık Düzenleme ve Denetleme Kurumu
BIS : Uluslararası Ödemeler Bankası
BKM : Bankalararası Kart Merkezi A.Ş.
BTC : Bitcoin
B2B : Firmadan Firmaya Pazarlama (Bussiness to Bussiness)
CPU : Merkezi İşlem Birimi (Central Processing Unit)
DLT : Dağıtık Kayıt Teknolojisi (Distributed Ledger Technology)
EFT : Elektronik Fon Transferi
FINETECH : Finansal Teknoloji
KVKK : Kişisel Verileri Koruma Kanunu
GB : Gigabyte
IoT : Nesnelerin İnterneti (Internet of Things)
IT : Bilgi Teknolojileri (Information Technologies)
M.Ö. : Milattan Önce
PoW : İş Kanıtlanması (Proof of Work)
PoS : Pay Kanıtlaması (Proof of Stake)
POS : Satış Noktası (Point of Sale)
RSA : Ron Rivest, Adi Shamir ve Leonard Adleman Algoritması
SHA : Secure Hash Algorithm
SWIFT : Dünya Bankalararası Finansal İletişim Kurulu
TCMB : Türkiye Cumhuriyeti Merkez Bankası
QR : Hızlı Cevap (Quick Response)

ŞEKİL LİSTESİ

Sayfa

BLOCK-CHAIN TEKNOLOJİSİ VE
B2B FİNANS İŞLEMLERİNDE KULLANILABİLİRLİĞİ

ÖZET

İnternet hayatımıza girdiği günden bu yana hiç durmayan ve devamlı gelişen teknoloji olmuş ve hayatımızın önemli bir parçası haline gelmiştir. Bugün internet üzerine geliştirimler ve incelemeler halen devam etmekte ve teknolojisi devamlı gelişmektedir. Günlük hayatımızda işlerimizin çoğunu, sunucu sistemlerimizin kontrollerini, fabrikalarımızın ya da iş yerimizin kaynak yönetimini, tükettiğimiz gıdaları, banka hesaplarımızı ve harcamalarımızın çoğunu internet üzerinden kontrol etmekte ve yönetmekteyiz. Hayatımızda bu noktaya taşıdığımız internetin gelişmesiyle paralel olarak yeni güvenlik sistemleri de adını duyurmaya başlamıştır. İlk olarak Bitcoin ile kendisinden bahsedilen blokzinciri bu güvenlik ihtiyacının en büyük etkenlerinden biri olacaktır. Doğru anlaşıldığında ve kullanıldığında internet üzerinde daha kontrollü ve güvende olacağız. Blokzinciri sadece güvenlik alt yapısıyla değil, ortaya koyduğu mimari ile hiçbir merkezi otoriteye bağlı kalmadan işlemlerimizi doğrudan uçtan uca gerçekleştirebileceğiz. Bu yönüyle ve arkasındaki teknoloji ile internetten sonraki en büyük buluş olarak kabul görmektedir. Bu tez blokzinciri hakkında genel bilgiyi, teknolojinin arkasındaki detayları ve finans alanındaki etkileri ele almaktadır.

Anahtar Kelimeler : *Blokzincir, Bitcoin, kripto-para, kriptoloji*

BLOCKCHAIN TECHNOLOGY AND USABILITY IN B2B FINANCE

ABSTRACT

Since INTERNET has been introduced to civilian uses, it and applications on it has been developed continuously and has become an integral and important part of our everyday lives. To this day, numerous applications that use INTERNET as a common platform are being developed and its technology is being advanced to facilitate the various needs of these applications. Numerous tasks that we accomplish in our everyday lives, like securing our homes, managing the operations in our workplaces, buying and selling goods, making and receiving payments in our bank accounts are performed through the INTERNET. As different applications are performed on this unique international platform, the security needs for these various operations have taken precedence. It is widely believed that the BLOCKCHAIN paradigm that was first used successfully for the cryptocurrency Bitcoin, will be a solution for most data security needs. We believe that BLOCKCHAIN will not only provide security of data but also let users perform various tasks directly from one node to another, without the need and interference of a central authority. It is thus hailed by many as the most promising and wide-reaching technology since the inception of the INTERNET. This thesis first summarizes the general properties and technological details of BLOCKCHAIN and then addresses its potential impact in commercial and financial operations.

Keywords : *Blockchain, Bitcoin, Crypto-currency, Cryptology.*

1. GİRİŞ

1.1 Çalışma Konusu

Finans sistemindeki ödeme sistemleri ve kontrol mekanizmaları merkezi bir yönetime tabidir. Merkezi bir yönetime ve sunucuya bağlı kalmadan işlemleri gerçekleştirmek veri alışverişi yapmak ancak bir blokzinciri teknoloji ile sağlanabilir. Bu sistem A'dan B'ye herhangi bir veriyi hiçbir aracı ve merkezi bir sistem olmadan iletimine olanak sağlar. Bu çalışma bu sistemin gelişim sürecini arkasındaki teknolojiyi ve ileride bizleri nasıl etkileyeceğini ele almaktadır.

1.2 Tezin Amacı

Bu çalışma Bitcoin sayesinde adını bir kere de olsa duyurmuş olan fakat arka planında yatan teknolojiden çoğu insanın haberi olmayan ve ülkemizde Türkçe kaynakların azlığı sebebiyle araştırmanın güç olduğu Blokchain – Blokzinciri teknolojisini, yapısını ve hayatımıza kattığı yenilikleri kapsamaktadır. Blokzinciri yapısını incelemek ve finans alanında kullanılabilirliğini ele almaktır. Günümüze kadar kullandığımız geleneksel ve son teknolojik ürünlerden de kısaca bahsedilecektir. Blokzinciri ile geleneksel sistemlerin farkları karşılaştırılacak ve avantajları ile dezavantajları üzerinde durulacaktır. Bu çalışmayla beraber özellikle finans sektöründe geleneksel ekonomik düzeni değiştirecek olan blokzincirinin yapısı, özellikleri ve teknik detayları üzerinde odaklanılacaktır.

1.3 Literatür Araştırması

Tezde aşamalı olarak literatür incelemelerine yer verilmiştir. Blokzinciri alanında yapılan çalışmaların birçoğu incelenmiş ve bu tezde birleştirilmiştir. Finans sistemi ile bağlantılı olarak diğer ödeme sistemleri, para, kullanımı ve tarihi gelişiminden bahsedilmiştir. Ülkemizde uygulanan örnekleri ve oluşturulan çalışma kurulumları incelenmiş, çalışmalarında yer alınmış ve sonuçları bu tezde verilmiştir.

2. PARA NEDİR?

Devletler tarafından basılan ve diğer devletler tarafından kabul edilen mal ve hizmet alımı için kullanılan üzeri sayısal semboller olan bir satın alım aracıdır. Paralar kâğıt, madeni ve günümüzde dijital ya da sanal olabilir. Kabul görülen paraların her biri bir sembol ve kısaltmaya sahiptir. Para birimleri ISO 4217 standartlarına tabiidir. Eğer bulunulan ülkede Latin alfabesi kullanılmıyor ise üç basamaktan oluşan bir kod kullanılır bu koda göre Türk Lirasının numerik kodu 949'dur. Paranın geleneksel tanımına göre üç tane fonksiyonu olması gerekir (Bankacılık terimleri, 2016);

- Değişim aracı,
- Değerini saklama,
- Muhasebeleştirme.

2.1 Altın ve Gümüş

Evrende nadir bulunan elementler ekonomi ve piyasalar için her zaman değerli bir karşılığı olan araç olarak kullanılmıştır. Altın ve gümüş de bunlardan biridir. Altın ve gümüşün nadir bulunmasının sebebi bu elementlerin oluşması için iki nötron yıldızının çarpışması gerekliliğidir. Bu çarpışmadan meydana gelen birleşmeyle yoğun bir element bileşiğin oluşumu için gerekli koşullar sağlanmış olur (Achenbach, 2013).

2011 yılında Max Planck Enstitüsünde yapılan çalışmalar sonucunda iki nötron yıldızının çarpışması sonucu yaklaşık 735 katrilyon kilo altın maddesi oluştuğu belirlenmiştir (Halici, 2013).

Tüm bu özelliklerinin yanı sıra altın ve gümüş diğer elementlere göre kolay ayırt edici özelliklere sahiptir. Zehirli değildir, katı durumundadır, renklidir, parlamaz, yanmaz, radyo aktif değildir, oksitlenme oluşmaz, uzun süre saklanabilir, eritmesi zordur ve tabi ki en büyük özelliği nadir bulunur. Gümüşün altına göre özellikleri değişkendir, altına göre daha çok bulunur ve zamanla kararlamalara yol açabilir bu nedenle altın daha çok değerli konumdadır (Rowlatt, 2013).

2013 yılında yapılan çalışmalara göre insanlık tarihi boyunca 171 bin ton altın çıkarıldığı ve bu da ortalama kişi başına 24 gram altın düştüğü ortaya çıkarmıştır (Prior, 2013).

Altın ve gümüşün bu özellikleri onu tarih boyunca hep değerli kılmış ve bir ödeme aracı ya da takas aracı olarak kullanılmasını sağlamıştır. Büyük medeniyetler özellikle altını devlet parası olarak kullanmış ve üzerlerine sembollerini basmışlardır. M.Ö. 3000'lerde Antik Mısır'da para yerine altın çubuklar kullanılmıştır. Altının günümüzdeki kavramlara en yakın örneği ise M.Ö. 7nci yüzyılda Lidya'lılar basmış ve kullanmıştır.

Şekil 2.1 : Lidyaların bastığı altın sikke örneği

Kaynak: (Cartwright 2014)

2.2 Temsili Para

Çift metal para döneminde gümüşün değeri altının değerinden düşük olduğundan insanların günlük kullanımda gümüşü tercih etmesine ve altını ise bir yatırım aracı (yastık altı) olarak görmesine neden olmuştur. Bu oluşum sonucu gümüş sirkülasyonun artmasına daha çok talep görmesine neden oldu ve sonuç olarak kötü para gümüş iyi para olan altını piyasadan kovdu. Bu kanuna Gresham kanunu denir.

Günümüz para aracının yerine kullanılan metal elementlerin kullanımı, taşınması ve içeriğinin değiştirilmesi söz konusudur. Günümüz madeni paralar yerine eskiden kullanılan altın sikkelerin bir kısmının eritilmesi, şekillerinin bozulması ve kırpılması

ile ağırlığı ve değerini etkiliyor, değiştiriyordu. Bu gibi nedenler ile emtia para yani temsili para sistemine geçilmesi kaçılmaz oldu. Bu sistem altın ve gümüşler karşılığında belli bir değeri olan kâğıt paraları doğurdu.

Jiaozi, tarihimizdeki ilk temsili para ve banknot olarak kabul edilir (Şekil 2.2). 10.yüzyılda Song hanedanlığında Çin'de basılmıştır. Banknotun en solundaki simgeler mühürdür, ortasındaki yazılar değeri hakkında bilgi verirken en sağında ise bir alışveriş figürü resmedilmiştir (Chinese Ancient Currency, 2012).

Şekil 2.2 : Jiaozi ilk banknot para

Kaynak: (Chinese Ancient Currency, 2012)

Bu oluşum hareketinden sonra 1661 yılında Avrupa'da ilk para Stokholm Bankası tarafından basılmıştır (Sergii, M., 2008).

17 ve 19 yüzyıllar arasında kâğıt paralar güçlü otoriteler tarafından basılmış, kullanılmış ve kullanılmasına teşvik oluşturulmuştur. Sistem yine altına dayalı olduğundan ülkelerin basmış olduğu paraların değerleri sahip oldukları altına bağlıdır (Morah, 2019).

2.3 Dijital Para

Dijital para kavramının ilk örnekleri 1980 yılında Hollanda'da görülmüştür. Benzin istasyonlarında güvenli ödeme ve hırsızlıklara karşı önlem almak isteyen bazı benzin istasyonu sahipleri müşterilerine içlerinde belli bir para değeri olan kartlar dağıtmaya başladılar. Yine günümüzde çok sık kullandığımız kredi kartı ve banka kartının ödeme sistemleri olan POS, yine aynı tarihlerde yaşamış olan bir iş adamının müşterileri tarafından ödemelerin direk olarak kendi hesabına girmesini istemesi ve bu doğrultuda bankalara yaptığı baskı sonucu ortaya çıkmıştır (Griffith, 2014).

Dijital paraların diğer ödeme araçlarına göre farkı ve özelliği elektronik olarak saklanabilmesi ve transfer edebilmesidir. Kâğıt paralarının emtiası olarak kullanılır. Bankalarımızda bulunan kâğıt paralarımızın temsilidir. Ticaret esnasında ve alışverişte bu temsili miktarları bir banka aracılığı ile güven altına alırız. Günümüzde kağıt para ile yapılan ticaret ve alışverişler neredeyse azalmıştır. İnsanlar çalışmaları karşılığında hesaplarına dijital para olarak maaşlarını almakta ve yine tüm ödemelerini dijital olarak gerçekleştirmektedirler.

Amerikalı yazılım uzmanı David Chaum bir elektronik ödeme sistemi oluşturdu. Bu sistem merkezi olarak yönetilen bir ödeme sistemiydi. Tam anlamıyla bir para birimi değildi ama hesaplar arası kolay ve hızlı transferlere cevap veriyordu. DigiCash olan bu sistem 1998 yılında şirketin iflas etmesiyle kapatıldı. Bu iflas sonrası piyasada büyük bir boşluk oluştu ve bu boşluğu 2000 yılında Confinity ve x.com'un birleşmesi sonrası PayPal doldurdu. Paypal'ın asıl amacı otomatize olmuş sistemlerde dolandırıcılığı engellemektir (Griffith, 2014).

PayPal, BDKK tarafından sistemlerini Türkiye Cumhuriyeti devleti sınırları içerisinde tutmadığı gerekçesiyle lisansları durdurulmuştur (Dalkılınç, 2016).

2.4 Sanal Para

Sanal paraları dijital paradan ayıran en büyük özelliği temsil ettiği bir fiziksel paranın olmamasıdır. Sanal paranın literatürde tanımı için karmaşa vardır.

2012'de Avrupa Merkez Bankası'nın yaptığı tanıma göre "genellikle geliştiricileri tarafından kontrol edilen, sınırlı sanal grup üyeleri tarafından benimsenip kullanılan, düzenlenmemiş/regüle edilmemiş, dijital paradır".

Şubat 2015'te revize edilen tanıma göre “Herhangi bir merkez bankası, kredi kuruluşu veya e-para kuruluşu tarafından ihraç edilmediği halde, bazı durumlarda paranın yerine kullanılabilen bir değerin dijital temsilidir”.

2014'te Avrupa Bankacılık Otoritesi'nin tanımına göre “Bir merkez bankası veya kamu otoritesi tarafından ihraç edilmediği halde, doğal olarak veya yasal kişiler tarafından ödeme, transfer, saklama ve elektronik transfer şekli için kabul gören, karşılığının olması da şart olmayan değerin dijital temsilidir”.

Amerikan Hazine Bakanlığı'na göre sanal para; “Gerçek paranın tüm özelliklerini taşımadığı halde, bazı ortamlarda para gibi kullanılabilen değişim medyasıdır” (European Central Bank, 2015).

2.5 Kripto Para (Şifreli Para)

Kriptolojik ve belli bir şifreleme sistematiği ile güvence altına alınmış hem dijital hem de sanal paralardır (Graydon, 2014).

Kripto-paralar çok sık Bitcoin ve diğer sistemler ile karıştırılır. Dijital ve sanal paralar devlet kontrolündedir ve ulusal para birimine bağlıdırlar. Merkezi bir otorite tarafından yönetilir ve düzenlenir. Bitcoin ise hiçbir merkezi sisteme tabi olmayan kendisi bir para birimdir. Hiçbir otorite tarafından denetlenemez (Rotman, 2014).

Bu tezin ana konusu olan Blokzincir teknolojisi, Bitcoin para biriminin alt yapısıdır. Genelde Blokzincir’de Bitcoin ile çok kez karıştırılır.

3. KAREKOD SİSTEMİ

Karekod bir barkod sistemidir. Beyaz bir zemin üzerinde yer alan bazı grafiksel kodlamalar sonucu dijital ve mobil sistemler tarafından okunabilir içeriklerdir. Karekod sistemi ile günlük hayatımızda birçok işlerimiz kolaylaştırabiliriz. Geleneksel doğrusal barkod sistemlerine göre iki boyutlu özelliği sayesinde içerisinde çok sayıda veri barındırabilir (Şekil 3.1).

Şekil 3.1 : Doğrusal ve iki boyutlu barkod içerik örnekleri

Kaynak: Yazar

İki boyutlu karekodlar içerisinde 7.090 nümerik, 4.291 karakter barındırabilir (What is a QR Code? 2017). İlk olarak 1994 yılında Japonya'da Denso Wave tarafından iki boyutlu yapıda tanıtılmıştır ve yine ilk olarak aynı yıl içerisinde Japon bir otomotiv fabrikasında motorlara işlenerek kullanılmıştır. Araç üzerindeki sistem parçalarının kolay takibi bu sayede işlem hızları artmıştır (What's a QR Code? 2015). Ülkemizde ilk örneklerini ilaç kutularının üzerinde yer almasıyla görüyoruz. Bu sistem ile büyük ilgi görmesi karekod sistemini geliştirmiştir. Diğer ürün ve ambalajlarda kullanılması neredeyse zorunlu hale gelmiştir.

Karekod sistemleri içerisinde sayı ve metin barındırabilirler. Karekodlar iki boyutudur. Geleneksel barkod sistemlerine göre karekodlar çok daha fazla miktarda harf ve sayı barındırabilmekte ve barkodların onda biri oranına kadar küçültülerek kullanılabilme imkânına sahiptirler. Belli bir orana kadar bozulma aralığına sahiptir bu nedenler bozulmuş karekodlar kolaylıkla okunabilir, içerlerine bu oran kullanılarak şekil ve logolar yerleştirilebilir. Karekodların birçok çeşitleri vardır. (Şekil 3.2)

Şekil 3.2 : İki boyutlu barkod çeşitleri

Kaynak: (Karekod (QR Kod) Nedir? 2018)

Günümüzde karekodlar eğitim amaçlı olarak çok yaygın olarak kullanılmaktadır. Soruların açıklamaları ve cevapları içerlerine gömülüdür. Aynı mantık ile basılı yayınların görsel içerikleri dergi ve gazetelerde karekodlara yerleştirilir. İş ilanları, iletişim aracı, mail yönlendirmesi, telefon araması ve uzun internet bağlantı adresine erişim için kullanılmaktadır.

Bu sistemlerin yanında finans sektöründe de karekod oldukça yayın kullanılmaktadır. Ödeme sistemlerinde, ATM makinelerinde mobil telefonlar tarafından okunarak ve hızlı onaylanarak yayın kullanılmaktadır. İçeriğinin hızlı ve kolay değiştirilebilir olması güvenlik olarak tercih edilmesine ve ikili doğrulamaya (two factor authantication) olanak sağlamaktadır.

Karekod sistemleri Blokzincir ve Bitcoin sistemlerinde de yaygın olarak kullanılmaktadır. Ödeme ve işlem geçişlerinde (transactions) karekod sisteminden yararlanılır.

4. BITCOIN

4.1 Bitcoin Nedir?

Günümüzde teknoloji ve finans yönünden en yaygın ve en çok konularından biri olan Bitcoin'i (BTC) aslında hem dijital para hem de sanal para olarak tanımlayabiliriz. Banka hesaplarımızda bulunan ve sanal ortamlarda yaptığımız alışveriş işlemlerinde kullandığımız kredi kartları bunlarda sanal ve dijital paradır. Bitcoin'i tanımlamak istersek aslında şifreli (kripto) para diyebiliriz (Sagona Stophel, 2015). Şifreli paranın anlamı hesaplarımızda kullandığımız şifrelerimiz değil, sunucularda tutulan kayıtların şifrelenmiş olmasıdır.

Şekil 4.1 : Bitcoin logoları

Kaynak: (Promotional Graphics, 2015)

Bitcoin TL, Amerikan Doları, Euro veya başka paralara dönüştürülebilinir (Granger, 2016). Normal para gibi insanlar dilerse BTC gönderebilirler, BTC satın alabilir ve takas yapabilirler.

Bitcoin'in diğer sanal ve dijital paralardan farkı vardır. Basit bir senaryo yazalım. Bir adet ekmek almak istiyorsunuz. Sizde nakit para var, satıcıda ise ekmek. Belirli bir ortama giderek nakdinizi elden teslim edersiniz. Satıcı eğer bir sorun yoksa nakdi alır, kabul eder ve ekmeği size teslim eder. Fakat burada bir sorun var, ödemeyi yapan ve ödemeyi alan kişi aynı ortamda yan yana olmalıdır. Günümüz internet ve e-ticaret dünyasında bu pekte hoş karşılanmayacak durum haline gelmektedir.

Bitcoin'de ise işler bu şekilde ilerlemiyor. Yukarıdaki örnek senaryoda olduğu gibi sanki yüz yüze alışveriş yapıyormuşçasına ödeme yapılabilir. Benzer işlemi geleneksel EFT veya Havale yöntemiyle de yapabilirsiniz elbette fakat EFT veya Havale yaptığınızda mutlaka arada bir aracı kurum kullanmak durumundasınız. Bankalarınız, alışveriş yaptığınız karşı tarafın bankası, onların bağlı olduğu kurumlar, kuruluşlar ve devletler. Kişisel bilgileriniz paylaşılıyor, işlemler zaman alıyor çünkü birileri tarafından doğrulanması gerekiyor ve üstüne de maliyetini ödüyorsunuz. Bitcoin'de ise merkezi bir yönetim sistemi yoktur. İki kişi arasında merkezi bir banka ya da devlet yoktur. Dağıtık bir sisteme sahiptirler bu nedenle kırılması ve çalınması, işlemin yapıldığı ve kaydedildiği bilgisayarlara saldırı yapılması söz konusu değildir. Arz edilen veya edilecek miktar bellidir. Bu nedenle devletlerin yaptığı gibi gelir yaratmak için para basılamaz.

Bitcoin Ağustos 2009'de Satoshi tarafından yayınlanan 9 sayfalık bir makale ile devrimini başlatmıştır. Fakat halen bu kişi ya da kişiler hakkında detaylı bilgi bilmemekteyiz.

4.2 Bitcoin Hakkında Eleştiriler

Bitcoine karşı yapılan itirazlar ve kabul edilemezlikler, takip edilemiyor olmasından ve yer altı ekonomisinde kullanılıyor olmasından kaynaklıdır. Bitcoin'de yapılan işlemler isimsizdir. İşlemlerin ne zaman yapıldığını takip etmek mümkün olsa da kimler arasında yapıldığı belirsizdir.

Derin web denen internetin diğer tarafında kendini gösteren Silkroad adlı site 2011 yılında kuruldu. Site üzerinde birçok illegal ürünler satıldı, illegal videolar gösterildi. İşlemlerin tümü Bitcoin ile yapıldı. Bu Bitcoin'in adının kirlenmesine sebep oldu. Herkes tarafından illegal işlemlerde kullanılan bir araç olarak düşünülmesine sebep oldu (Silk Road Nedir? Bitcoin ile Bağlantısı Nedir? 2017).

Aslında Bitcoin'e gösterilen en büyük direnç ve tepki mevcut ticaret yapısını ve yukarıda belirttiğimiz düzeni bozması konumunda olmasıdır. Devletler tarafından kontrol edilemiyor olması da ayrıca en büyük tepkidir.

4.3 Bitcoin'in Geleneksel Para Sistemlerinden Farkları

Bitcoin sisteminin günlük hayatımızda kullandığımız geleneksel para birimleri ve diğer ödeme araçlarından bazı farkları vardır. Bu farklılıkları paranın özelliklerine göre karşılaştırma yapabiliriz.

- Kabul edilebilirlik, BTC için bu özellik gün geçtikçe artmaktadır. Önceden olmasa da günümüzde BTC'e güven artmaktadır.
- Değerinin istikrarlı kalması, bu özellik BTC için en büyük problemdir ve paranın yerine geçmesine en engel etkendir. Çünkü BTC değerleri çok farklılık göstermektedir. Paranın yerine geçebilmesi için fiyatlarındaki artış ve inişler dengeli olmalıdır.
- Taşınabilirlik, bu özellik BTC için en güçlü yönüdür. Günümüzdeki hiçbir değer (para, bankadaki para vb.) BTC ile rekabet edemez. Günümüzde paranızı istediğiniz zaman istediğiniz başka bir noktaya taşıma imkanınız var fakat bu işlem için hem büyük komisyonlar ödersiniz hem de uzun zamanlarınıza mal olur. BTC için bu sorunlar yoktur.
- Bölünebilirlik, Türk Lirasından örnek verirsek kullandığımız paralarda en küçük birim kuruşlardır. BTC bölünebilirlik konusunda çok gelişmiştir. Kuruşun kuruşunun kuruşu bile mevcuttur. 1 BTC 100 milyona bölüne bilir ve buna satoshi denir.
- Ömürlülük, günümüzde kullandığımız paralar yıpranmakta ve hatta tedavülden kalkmaktadır. BTC için böyle bir sorun yoktur. Yıllar geçse de coinleriniz eskimez ve yıpranmaz.

4.4 Bitcoin Kullanarak Maliyetsiz Para Transferi

Eğer bu konuyu birkaç yıl önce ele alıyor olsaydık cevabı çok netti, evet. Fakat günümüzde artan işlem hacimleri ve talepler bu konuda BTC'e sıkıntılar yaratmaktadır ve BTC'in en büyük sıkıntısı haline gelmiştir. Geliştirilen yan ve destekleyici algoritmalar ile bu sorundan kurtulmaya çalışılsa da sorunlar halen devam etmektedir.

BTC’de oluşturulan her bir blok 1MB ile sınırlıdır. Bu içerisinde barındıracak verinin sınırlı olması anlamına gelmektedir. Her bir blok üretimi de yaklaşık 10 dakika süreceğinden BTC için saniyede 3-4 arası işlem hızı ortaya çıkmaktadır. Bu geçen süre VISA için saniye de 1.667 adettir. İşlemleri hızlandırmak için komisyon ödemek durumunda kalırsınız. Bu sorunlardan dolayı BTC bu özelliğinden şimdilik uzaklaşmıştır.

4.5 Bitcoin’in Ana Problemleri

Yukarıdaki yazılarımız aklımıza gelirse iki konu hemen karşımıza çıkıyor, birincisi değerinin çok büyük dalgalı halde olması diğeri ise üretim zamanı ve doğurduğu maliyetler; örneğin elektrik masrafı.

Satoshi 2008’de BTC’i tasarlarken belki kendisinin de ön göremediği en büyük sorun elektrik masrafıdır. Madencilerin 10 dakikada BTC üretmelerindeki çabaları ve yarışmaları çok büyük rekabetler getirmektedir. Bu da birçok güçlü bilgisayarın çalıştırılması ve onların da soğutulması sorununu ortaya çıkarmaktadır.

4.6 Bitcoin Madenciliği

Sisteme gelen yeni bir Bitcoin talebini karşılamak ve güvenli bir Bitcoin üretmek için madenciler kullanılır. Bu yöntem ile çifte harcamalar engellenir. Bitcoin transfer işlemlerini madenciler kayıt altına alır. Bitcoin sistemindeki güven mercihinin ana temeli madencilerdir. Madenciler tarafından yazılan bir işlem onaylanmış olarak kabul edilir.

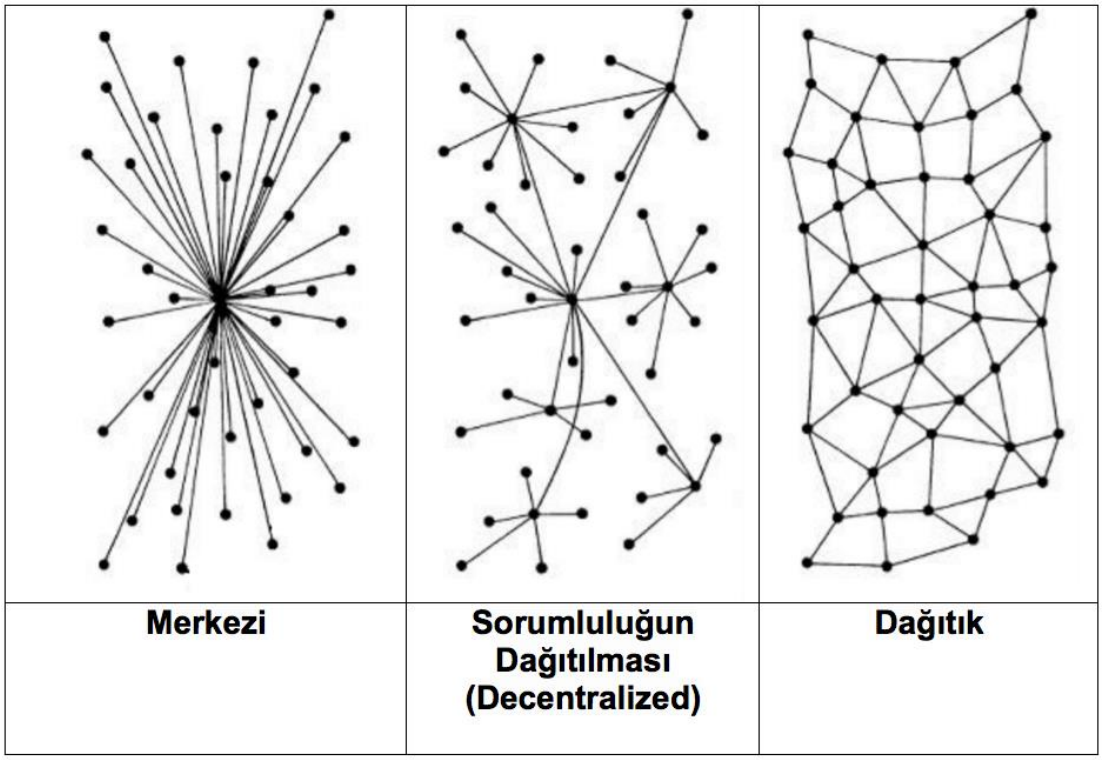
Bitcoin madenciliği tabiki uzun ve derin bir konudur, birçok çeşidi vardır. Bu tezin asıl konusu Blokzinciri olduğundan bu kısımlara girilmemiştir.

Genel olarak blokzinciri için gerekli olan zorluk derecesini madenciler çözer ve bir nonce değeri oluştururlar. Bu kavramlara ileriki bölümlerde geniş yer verilecektir. Üretilen nonce değeri, iş ispatını yaptıktan sonra, bunu ağ üzerinde yayar, bunu alan diğer uçlar bloğu pek çok kontrolden geçirir, madencinin dürüst olduğu kanıtlanırsa, Blokzincir'e bulunan son blok eklenir.

Madencilerin asıl amacı zorlu matematiksel işlemleri doğru bir zorluk derecesine tabii tutarak hesaplamaktır. Hesaplamalar çok fazla elektrik ve kaynak tüketmektedir. Bu nedenle madencilik yapan kişi ve firmalar kaynaklarını devamlı olarak geliştirirler. Bu rekabet Bitcoin sistemi ekstra olarak güvenli kılmaya yarar. Madenciler yaptıkları çalışma ve sonuç doğrultusunda karlığı olarak Bitcoin ile ödüllendirilirler (Köse B., 2019).

5. BLOKZİNCİRİ

Adını özellikle Bitcoin ile beraber duyuran ve son zamanlarda herkes tarafından merak edilen blokzinciri dağıtık bir hash veritabanı sistemidir. Hiçbir merkezi yönetime bağlı olmadan çalışmasını sürdürebilen sistem, birçok kurum ve devlet tarafından bu nedenle kabul görmezken son zamanlarda devletlerin özelleştirdiği sistemler ile kapalı blokzinciri uygulamaları da gündeme gelmiştir. Merkezi bir yönetime tabii olmaması ve dağıtık bir sistem (DLT, Distributed Legder Technology) ile çalışıyor (Şekil: 5.1) dolayı blokzinciri ekstra güvenlik sistemleri ile desteklendiğinde daha da güçlü bir yapıya gelmektedir.

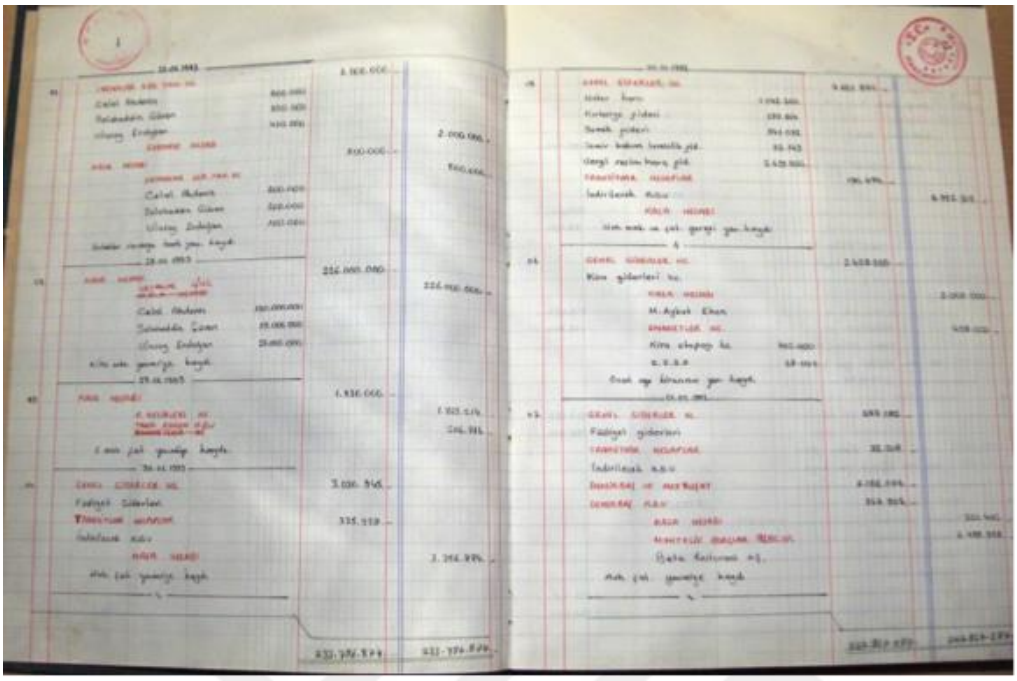


Şekil 5.1 : Merkezi, Merkezi Olmayan ve Dağıtık Mimariler

Kaynak: (Blokzinciri, 2018)

Dağıtık kayıt teknolojisi blokzincirinin çalışma yapısının temelidir. Bu temeli kullanmak zorundayız diye bir durum yoktur. İstenilirse merkezi ya da sorumluluğun dağıtılması teknolojileri de kullanılır. Fakat blokzincirini güçlü yapan ve şeffaflığını sağlayan yapı dağıtık teknoloji ile sağlanır. Dağıtık sistem bir muhasebe kayıt defteri

(Şekil: 5.2) gibi çalışır. Böylelikle birbirini tanımayan kişi ve sistemler arasında bir güven oluşturur.



Şekil 5.2 : Merkezi, Merkezi Olmayan ve Dağıtık Mimariler

Kaynak: (Blokzinciri, 2018)

Bu güveni sağlamak için bir merkeze ya da otoriteye bağlı olmak durumunda kalmayız. Sisteme dahil olan tüm aygılar üzerinde yapılan tüm işlemler (transactions) kayıt altına alınır. Böylelikle şeffaflık ve inkar edilemezlik sağlanmış olunur.

5.1 Blokzinciri Nedir?

Bitcoin'nin nakit paraya oranla güçlü yanlarını yapısını ve en popüler kripto para olmasını ele aldık. Şimdi ise onun bu kadar popüler olmasındaki başrol yapıyı ele alacağız. Günümüzde çok popüler bir konu hale gelmesi sadece para olarak değil tüm verilerin de güvenli transferinin sağlanması bir algoritma tarafından gerçekleşmektedir, Blokzinciri algoritması. Birçok kesim tarafından BTC ile karıştırılsa da BTC'nin alt yapısıdır Blokzinciri. Adını ilk olarak 2009 yılında Bitcoin isimli takma bir yazar adı ile yayınlanan makale ile duyduk. (Nakamoto, S. 2008)

Blokzinciri kullandığımız veritabanları ve bulut yazılımlara yeni bir devrim ve yenilikçilik getirmiştir. Uzmanlara göre blokzinciri sistemi hayatımızı internetin buluşundan sonra değiştiren bir diğer teknoloji olacaktır. Blokzinciri en doğru tanım ile yazılım mimarisidir. En büyük özellikleri BTC ile elbette benzerdir. Ödemeleri yüz yüze ve fiziksel bağımlıkları ortadan kaldırarak yapılabilmesi, aracıları ortadan kaldırması, kırılamıyor olması gibi birçok özelliği vardır. Bu bölümde blokzincirinin özelliklerini ve yapısını ele alacağım. Ethereum'un mucidi Vitalik Buterin blokzincirinin tanımını şöyle yapıyor: "Bu öyle sihirli bir bilgisayar ki isteyen herkes program yükleyebilir ve bu programları kendi başlarına çalışması için bırakabilir; bu bilgisayarda ayrıca her bir programın mevcut ve geçmiş bütün durumları her zaman herkes tarafından görülebilir; aynı zamanda bu bilgisayar zincirdeki programların Blokzincir protokolünün tam olarak belirttiği şekilde işlemeye devam edeceğini kripto-ekonomik olarak güvenceye alınmış bir garanti taşımaktadır."

Blokzinciri özünde veritabanı sistemidir. Veriler peş peşe sıralı olacak şekilde belli bir kurala dayalı olarak bloklar halinde kayıt ediliyor. Her bir bloğun zaman damgası vardır. Bir blok dolunca başka bir bloğun üretimi devam ediyor. Bloklar birbirine özel bir hash ile bağlı bu da zinciri oluşturuyor, ismi de buradan gelmektedir.

Çok basit bir örnekle aslında herkes tarafından görülebilen ve kaydedilen muhasebe defteri olarak düşünebiliriz. Tek fark bu deftere kayıt edilebilir fakat hiçbir kayıt değiştirilemez ve silinemez. Gerçekleşen her bir blok işlemi tüm kişiler tarafından kayıt edilir. Böylelikle ileride çıkabilecek anlaşmazlıklar ve inkarlar çok kolay ve doğru bir şekilde çözülmektedir.

Blokzinciri dağıtık bir yapıya sahiptir. Her bir bloğun kendi özellikleri vardır. Büyüklüğü, kayıtların nasıl saklanacağı, blok dolunca ne olacağı, blok arası bağlantılar, nasıl dağıtılacağı, nasıl saklanacağı gibi özellikleri barındırır.

Blokzinciri sadece bir finans ve ödeme aracı değil, merkezi kontrol gerektirmeyen diğer tüm sistemler için kullanılabilir ve geliştirilebilir bir algoritmadır. Bu nedenle blokzinciri birçok yeni fırsatlar açacakken birçok merkezi sistemi de iptal edecektir.

5.2 Blokzincirinin Temel Özellikleri

Blokzinciri kendisine ait özellikleri barındırır. Bu özellikler;

- Herkes tarafından görüntülenebilen açık bir veri sistemidir. Herkes istediği zaman yapıya ulaşabilir, bilgileri görüntüleyebilir.
- Hiçbir veri aynı sırada bulunmamaktadır. Her bilgi sıralı bir şekilde bir hash sistemi ile birbirine bağlıdır ve her biri zaman damgasına sahiptir. Verilerde herhangi bir değişiklik zaman damgası ve hash özet bilgisini değiştireceğinden yapı bozulacaktır. Zincire dahil edilmeyecektir. Böylelikle zincir güvenliği sağlanacaktır.
- Tüm işlemler herkes tarafından kontrol edilebilir ama değiştirilemez veya silinemez. Eğer talep edilirse tüm kayıtları bilgisayarınızda barındırabilir ve bir kopyasını tutabilirsiniz.
- Merkezi bir yönetime sahip değildir. Bu da güvenlik zafiyetlerini ortadan kaldırmaktadır. Geleneksel yapıda merkezi bir sunucuya yapılacak bir saldırıdan etkilenmek gibi bir durum blokzincirinde söz konusu değildir.

5.3 Blokzinciri Kim Tutar?

Blokzincirinin kayıt defteri herkes tarafından görüntülenebilir ve indirilebilirdir. İstenirse bu defter kayıtlarını bilgisayarınıza indirebilir ve akışları kontrol edebilir hatta katkıda bulunabilirsiniz. Hesap defterinin büyüklüğü 95GB'ı aşmış durumdadır. Bu verilerin tamamını tutan bilgisayarlara tam uç adı verilir. Yalnız bu uçlar defterin tamamını tutmak durumundadırlar (Arıcan ve diğerleri, 2018)

http://blockchain.info web sitesi tam bir uç noktadır ve bu web sitesini kullanılarak anlık ya da tarihsel işlemleri inceleme yapmak mümkündür.

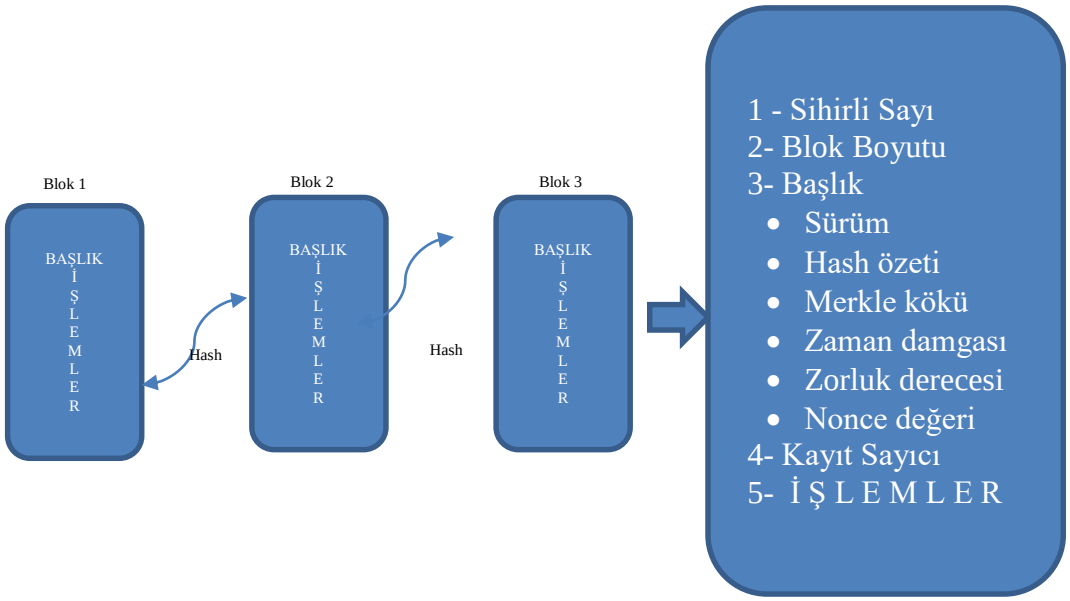
Uç birimlerdeki bloklar onaylanmış ve iş ispatı yapılmış (iş ispatı 45. sayfada detaylı anlatılmıştır.) işlemlerdir. Nadir de olsa kendi uç birimlerinizde bulunan bloklar diğer uç birimlerdekilerle farklılık gösterebilir. Bu bir güvenlik zafiyeti değildir. Bu sorun kısa sürede bir eşitleme ile düzeltilir ve tüm uç birimler aynı eşitliğe sahip olmuş olur.

5.4 Blokzincir Veri Yapısı

Gerçekleşen her bir işlem belli bir yapıdaki bloklara kayıt edilir. Bu işlemlere transaction denir. Her bir dolan blok yerine yeni bir hash üretilerek başka bir blok oluşturulur. Bloklar birbirine bağlanırken bir önceki bloğun hash özeti alınır. Böylelikle veri bütünlüğü korunmuş olunur. Zincir sistemindeki ilk bloğun bir öncesi olmadığından sistem yaratıcısı tarafından bir değer atanır bu genellikle 256 adet 0'dır. Bu ilk bloğun adı Genesis Blok'tur (Nakamoto, S. 2008).

Her bir önceki bloğa "Ebeveyn blok (parent block)" denir. Her bir bloğun sadece bir tane ebeveyn bloğu vardır. Her bir ebeveyn bloğun ise birden fazla yavru bloğu (child block) olabilir. Her blok kendinden bir önceki ve sonraki blok ile hash özeti ile bağlıdır, bu bağlılık zinciri oluşturur (Şekil: 5.3). Bloğun 5 alanı vardır;

- Sihirli Sayı - 4 byte,
- Blok Boyutu - 4 byte,
- Blok Başlığı - 80 byte,
- Kayıt Sayıcı - 1-9 byte,
- Kayıtlar - değişken.



Şekil 5.3 : Blok yapısı

Kaynak: Yazar

Sihirli sayı 0xD9B4BEF9'dur ve her zaman sabittir. Bu alan, veritabanı okurken devamında bilgilerin blok halinde olduğunu belirtir.

Blok boyutu ise başlangıç ve sonunu belli etmek için kadar byte olduğunu tutar.

Blok başlığı içerisinde 6 adet özellik barındırır. Şekil içine yazalım

1. Sürüm: Güncellemelerin takibi için kullanılır, 4 byte.
2. Önceki hash özeti: Bir önceki blok bağlantısını tutar, 32 byte.
3. Merkle kökü hashi: Merkle ağacının kökünün hash özeti, 32byte.
4. Zaman damgası: Saniye cinsinden bloğun oluşturulma zamanı, 4 byte.
5. Zorluk derecesi: Bloğun iş ispatının zorluk derecesi, 4 byte.
6. Nonce değeri: PoW yapılabilmesi için kullanılan sayaç, 4 byte.

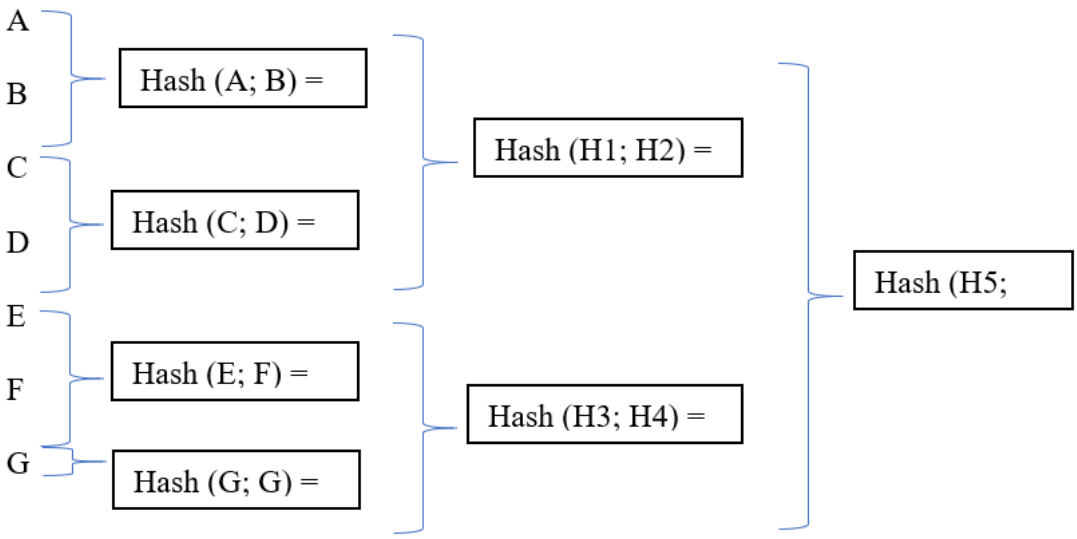
Yukarıdaki maddeleri tek tek ele almak istiyorum çünkü bu tanımlamalar blokların temelini oluşturmaktadır.

Sürüm: Bu alanda blok hakkında bazı önemli bilgiler ediniriz. Bloğun hangi kurallara dayalı oluşturulduğu, yapısı, uzunluğu, kayıtların şekli ve yazım kuralları zaman içerisinde değişebilir. Sürüm bilgisi hangi kurallara dayalı olduğu bilgisini tutar böylelikle ileride bir gün geçmiş kayıtlar arandığında o sürümdeki kurallar geçerli olur.

Önceli hash özeti: Zincir birbirine bağlı bloklardan oluşuyordu, bir blok oluştururken özet bir hash üretilir ve bu değer bir sonraki bloğun hash değerine eklenir. Böylelikle verilerdeki en ufak bir değişiklik bir diğerini ve o da diğerini olacak şekilde tüm zinciri etkilemiş olur.

Merkle kökü: Blok içerisinde kayıt edilen işlemler ikişerli gruplar halinde tutulur. İkişerli grupların da hash değeri alınır, en sonunda son iki tane kalıp onlarında hash değeri alınınca merkle kökü oluşturulmuş olur.

İkişerli hesaplanan hash değerlerine merkle kökü ağacı denir. Kayıtlar ikişerli hashendiğinden eğer tüm kayıtlar tek olursa son kayıt kendisiyle hashlenerek sonuç olarak çift bir merkle kökü oluşturulmuş olur. Örneğin, aşağıda A, B, C, D, E, F ve G için 7 adet işlem olsun ve bunların merkle kökünü bulalım. (Şekil: 5.4)



Şekil 5.4 : Merkle kökü yapısı

Kaynak: Yazar

Yukarıdaki örnekte G işlemi tek olduğundan kendisi ile hashlenerek çift hash elde edilmektedir. A, B, C, D, E, F ve G merkle yapraklarını H1, H2, H3, H4, H5 merkle dallarını ve son olarak hashlenen H5 ve H6 ise merkle kökünü temsil eder.

Merkle kökü bloklar için en önemli unsurdur ve iki ana görevi vardır. Birinci görevi ikili kayıtların hashlenmesinden oluştuğu için kayıtların birinde olan değişiklik merkle köküdeki hashleri de değiştirecek ve işlem güvenliği kolay tespit edilecektir. Diğer önemli görevi ise işlem teyidinin hızlı bir şekilde yapılmasını sağlamaktır (Yücel, M., 2017).

Zaman damgası: Zincirdeki bloğun üretim zamanını zaman damgası ile belirtilir. Epoch formatında işlenir. 1 Ocak 1970'den bu yana kaç saniye geçtiği şeklinde tutulur. Zaman damgası için 4byte yer belirtilir. Burada ileride yaşanabilecek ufak bir problemden bahsetmek istiyorum. 4byte, 32bittir. İlk bit sayının pozitif negatif durumunu tuttuğuna göre geriye kalan bitlerle yazılabilecek en büyük sayı 2.147.483.647'dir. Bu sayıyı hesapladığımızda 19 Ocak 2038 tarihine ulaşmış oluyoruz. Buna aslında bilgisayar dünyasında Y2038 problemi denir. 2038 yılına kadar UNIX'in 4byte zaman formatı kullanan kalmayacaktır düşüncesinden dolayı çok önemsenmez. Fakat yaşanan bir büyük problem örneği vardır.

3 Aralık 2014 tarihinde Youtube'da yayınlanan Gangnam Style videosunun izlenme sayısı 32 bitte tutulabilecek en büyük sayıyı geçince sistemlerin çökmesine ve kısa sürede olsa ulaşılmamasına neden olmuştur (Yumrutepe B., 2014). Bu nedenle ne kadar önemsenmezse de erkenden önlem almak gereklidir.

Zorluk derecesi: Blokzincirinde hesaplanan bloklar aslında zorluk derecesi hesaplananlar anlamına gelir. Her bir blok ortalama 10 dakika hesaplanacak ve zorluk derecesi olacak şekilde ayarlanır. Eğer blok çok kolay oluştuysa zaman damgası ve nonce değerleri değiştirilerek zorlukların arttırılması hedeflenir.

Nonce değeri: Bilgisayar dünyasında tek kullanımlık sayı anlamına gelen nonce blokzinciri için en önemli etkenlerden biridir. Blokzincirlerin hash özetlerinden bahsetmiştik. Bu hash değeri belli bir kurala dayalı olarak çalışır. Örneğin kural ilk 16 hanesinin 0 olması olsun. Blokzincirinin içerdiği değerler değiştirilmeyecekti bu nedenle bu kurala erişmemizi sağlayan başka bir değer olmalı. Bu değer noncedır. Nonce değeri her defasında bir arttırılarak kurala ulaşmaya çalışılır. Eğer ilk defasında ve 10 dakika altında bulunduysa zorluk derecesi değiştirilerek yeniden hesaplama yapılır. Bu nonce değerlerinin üretimi zahmetli ve maliyetlidir. Bu işlemi ileride ele alacağım madenciler denen bilgisayarlar gerçekleştirilir.

5.5 Hash Sistemi

Hash kriptolojinin bir konusu olmasına rağmen aslında bir tür şifreleme değildir. Daha çok verinin parmak izi diyebiliriz. Bir metnin, müzik dosyasının, resmin veya yazının özgünlüğünü kanıtlamak için kullanılır. Secure Hash Algorithm – SHA elinizde nasıl bir veri olursa olsun ortaya çıkaracağı özet hep aynı uzunluktadır. Eğer belge üzerinde en ufak bir değişiklik yaparsanız özette değişeceğinden özgünlüğü de değişmiş olur.

5.6 Açık ve Özel Anahtar Kavramları

Bilgi sistemlerinde güvenliğin iki yönü vardır; gizlilik ve doğruluk. Bu nedenle kriptolojide asimetrik ve simetrik şifreleme kullanılır. Simetrik sistemlerde hem şifrelemek hem de şifreyi açmak için tek anahtar mevcut iken, asimetrik sistemlerde ise (kripto paralarda tercihen bu sistem kullanılır) anahtarın başkanın eline geçmesi ihtimaline karşı iki adet anahtar üretilir. Bu anahtarlar birbirine matematiksel olarak bağlıdır. Bu anahtarlardan biri açık (public), diğeri ise özel (private) anahtardır. Özel anahtarlar şifreyi açmak için kullanılır, açık anahtar ise şifrelemek için kullanılır. Açık anahtar ile özel anahtar arasındaki matematiksel bağlılık tek yönlüdür, açık anahtarı kullanarak oluşturulan şifrenin özel anahtar tarafından açılması çok kolaydır. Fakat açık anahtar kullanılarak özel anahtar üretmeye çalışmak oldukça zordur ve 2256 ihtimali vardır.

Buraya kadar anlattıklarımızı basit bir örnekle pekiştirmek gerekirse; örneğin Onur posta kutusuna Cihad'tan gelecek gizli bir belge bekliyor. Bunun için Onur öncelikle kapı numarasını 3214 ve posta kutusunu 32, Cihad ile paylaşır (açık anahtar). Cihad elindeki 3214 ve 32 bilgisi ile kapıya ve posta kutusuna ulaşır içerisine gizli belgeyi koyar ve yeniden kapatır. Onur elindeki özel anahtarla posta kutusunu açar ve belgeye ulaşır. Bu yöntemler başka hiç kimse belgeye ulaşamaz.

Yukarıdaki örneğin tersini yani dijital imzayı da düşünürsek; Onur'un göndereceği belgenin diğer kişiler tarafından görünmesinde sorun yok ama göndericinin kendisi olduğunu bilinmemesini istesin. Bu sefer kendi elindeki özel anahtarı ile postayı açar içerisine belgeyi yerleştirir. Cihad elindeki açık anahtar bilgisi ile posta kutusuna erişir, kutunun açık olduğunu görür ve belgenin Onur tarafından mutlaka konulmuş olduğunu fark eder ve belgeye ulaşır.

Açık ve özel anahtar deyince akla ilk gelen RSA algoritması oluyor. RSA 1970'li yıllarda Ron Rivest, Adi Sahamir ve Leonard Adleman tarafından yayınlanmıştır. (Şeker E., 2008) RSA verileri şifrelemek için kullanılmaya uygun değildir, oldukça yavaştır. Bu nedenle blokzincirinde SHA algoritması kullanılır. RSA sadece verilerin güvenli şekilde dolaşmasını sağlayan anahtarları şifrelemek için kullanılır.

RSA temelinde olabildiğinde büyük iki asal sayılar kullanır ve mod tabanlı işlemler gerçekleştirir. RSA çalışma mantığı;

- İki büyük asal sayı seçilir q ve p,
- q ve p çarpılarak n değeri hesaplanır ve bu mod olur,
- n değeri için Totient fonksiyonu hesaplanır, q-1 ve p-1 ile çarpımından bulunur,
- 1'den büyük totient n den küçük bir asal sayı seçilir. Bu açık anahtardır. Bu sayı ile totient aralarında asaldır,
- d mod totient 1 olacak şekilde bir sayı hesaplanır, bu sayı özel anahtar olacaktır.

Örnek olarak;

- p=61 ve q=53 için (işlemlerin kolaylığı için küçük asal sayılar seçilmiştir.),
- n = p.q = 3233,
- Totient fonksiyonu $\varphi(n) = (p-1)(q-1) = 3120$,
- e > 1 => e = 17 (3120 ile aralarında asal), açık anahtar olarak belirlenir,
- de ≡ 1 mod(n), d=2753 (17*2753 = 46801 = 1+15*3120),

Bu hesaplamalar sonucunda karşı tarafa gönderilecek mesaj 321 olsun. 321^{17} mod 3233 = 1476 olarak şifreli metin elde edilir. Şifreli metin olan 1476 karşı tarafa iletilir. Karşı taraf elindeki özel anahtar 2753 ile işlemin tersini yapar. 1476^{2753} mod 3233 = 321 sayısı elde edilir.

5.7 Hash Özeti ve SHA256

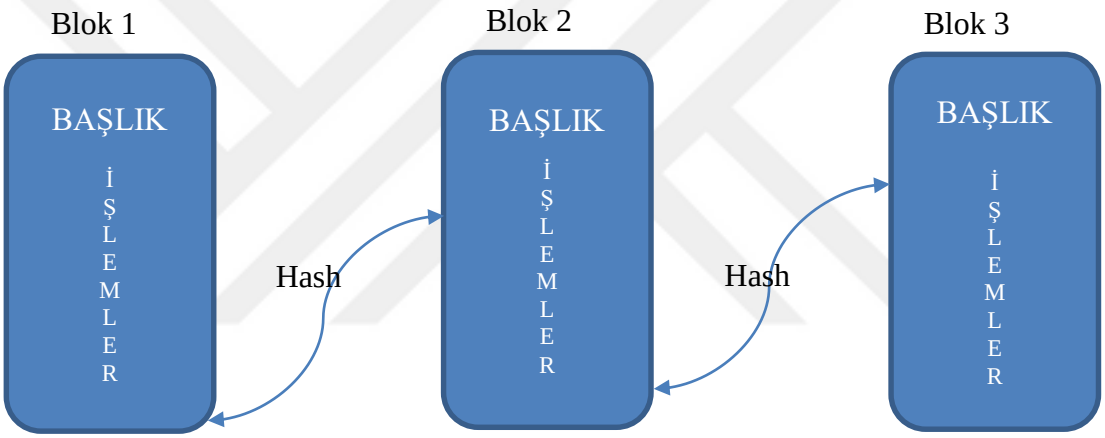
Hash konusu blokzinciri ile tam olarak bağlantılıdır. Hash kısaca parmak izidir. Kriptolojide şifreleme ile çok karıştırılsa da aslında şifreleme değil bir özettir. Hash belli bir uzunluktaki veriyi özel bir algoritma yöntemine göre sabit bir uzunluktaki değere çevirir. Buradaki veri 'A' harfi de olsa 500 sayfalık bir kitapta olsa aynı uzunlukta özeti olması şarttır.

Günümüzde 20'nin üzerinde hash algoritması mevcuttur. Bu algoritmalardan en popüler olanı SHA hash grubundan SHA256'dır. Çıktı olarak 256 bitlik veri üretir.

Kabul edilebilir bir hash algoritması aşağıdaki beş özelliği barındırmalıdır.

1. Aynı girdiler mutlaka aynı veri sonucu özetini üretmelidir.
2. Çıktı özetleri hızlı bir şekilde üretilmelidir.
3. Çıktı özeti kullanılarak verinin orijinali bulunamamalıdır.
4. En ufak değişikliklerde özet değeri mutlaka değişmelidir.
5. Farklı veri girişleri aynı özet değerlerini üretmemeli.

Hash konusu blokzinciri için en önemli konudur. Her bir blok birbirine hash özet değeri ile bağlıdır. Blok zincirinde içerisindeki bilgilerle üretilen hash değeri bir sonraki içinde kullanılır (Şekil 5.5). Yani bir blok içerisinde olan değişiklik diğer zincirde bulunan tüm özetleri değiştirdiğinden zincir yapısının bozulmasına ve haliyle okunamaz durumuna getirilmesini sağlayacaktır.



Şekil 5.5 : Blokların birbirine bağlantısı.

Kaynak: Yazar

5.8 Blokzincir Madencilik Algoritmaları

Blokzinciri sisteminde blokların üretimi için aynı Bitcoinlerde olduğu gibi birkaç çeşit madencilik algoritması vardır. Bunlardan en popüler ve Bitcoin ile beraber kullanılan proof of work – iş ispatı ve proof of stake – varlık ispatı en popüler ve kabul gören algoritmalardır. Bu algoritmalar haricinde kullanılan başka madencilik algoritmaları da vardır.

5.8.1 Proof of work – İşlem ispatı algoritmasi

Bitcoin sisteminde olduğu gibi blokzincirinde blokların üretimi sırasında her bir blok belli bir zorluk derecesine sahiptir. Bu zorluk derecesi nonce denilen bir rasgele oluşturulan bir sayı ile belirlenir ve oluşturulan hash sistemi belli bir kurala tabii tutularak oluşturulur. Örneğin bir hash özetinin zorluk derecesi 10 dakika olmalıdır. Eğer bu derecenin altında kalırsa yeni bir rasgele sayı üretimi yapılır. Bu nedenle yeni kriterler için yeni matematiksel hesaplamalar gerektirir. İşlem gücünü baz alan bu sistemin temeli elektronik postalarda spam maillerin kontrolünü sağlayan sistem olan hash cache algoritmasıdır. İşlem gücü algoritması herkes tarafından kontrol edilen ve açık olan sistemler için en kabul gören algoritmadır.

5.8.2 Proof of stake –Varlık ispatı algoritması

Bu sistem proof of work gibi çalışmaz. Madenciler kendi aralarında yarışmalar ve kendilerine ayrılmış belli bir para miktarını kazanırlar. Aslında günümüzde kullanılan faiz sisteminin bir çeşididir.

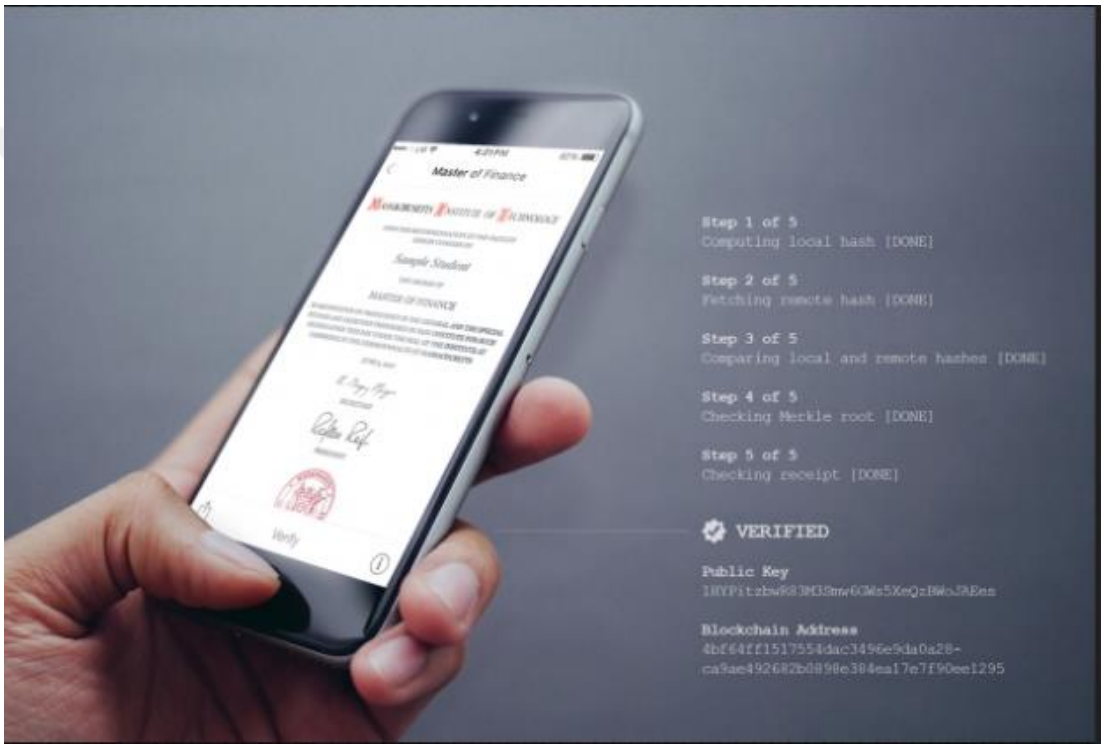
5.9 Blokzincirinde Güvenlik

Blokzincirinde güvenlik konusu iki farklı çeşitte incelenmelidir. Kapalı sistem, açık sistem. Kapalı sistemlerde zaten dışarıdan bir müdahale söz konusu olmayacağından açık sistemlere baktığımızda buradaki güvenlik yapısı verilere ulaşmayı engellemek, işlemlerin gizliliği değildir. Bunun aksine blokzinciri şeffaflık istediğinden tüm kayıtları göstermelidir. Blokzincirinde güvenlik ile bahsedilen konu dağıtık olan verilerin birebir aynı olması ve kayıtların değiştirilmemesidir. Zaten kayıtlar birbirlerine hash ile bağlı olduğundan bu durum gerçekleştiğinde tüm verilerin içeriğine ulaşamıyor olacağız.

Diğer en büyük güvenli özelliği ise merkezi bir sistem olmamasıdır. Veriler dağıtık düzende ve birçok bilgisayar ve sunucu tarafından tutulduğundan hackerlar verilere ulaşabilmesi için %51 denen sistemdeki bilgisayarların yarısından fazlasını aynı anda ele geçirmek durumundadır.

5.10 Blokzinciri Kullanım Alanları

Blokzinciri teknolojisinin en yoğun kullanım alanı günümüzde hiç şüphesiz ki başta Bitcoin olmak üzere kripto paralardır. Blokzinciri teknolojisi başka birçok alanda kullanıma açık ve kullanıldığı takdirde güveni artırıcı ve bağımlılıkları azaltacağı yapıya sahiptir. Amerika'da önde gelen ve önemli üniversite kuruluşları diplomalarını artık blokzinciri teknolojisiyle vermektedir. Massachusetts Teknolojisi Enstitüsü (MIT) 2017 yılında blokzinciri teknolojisi ile diploma verdiklerini duyurdu (Şekil: 5.6).



Şekil 5.6 : MIT Dijital Diploma Çalışma Mantığı

Kaynak: (Durant, E 2017)

Ülkemizde 2018 yılında çalışmalarına hız katan TÜBİTAK BİLGEM, Blokzincir Araştırma Ağı (BAĞ) kurarak üniversiteler arasında akademik araştırma, bilimsel geliştirme ve bilgi paylaşımı sağlamayı hedeflemektedir (Blokzincir teknolojisi, 2017). Üniversitelerin çalışmalarının yanı sıra blokzinciri teknolojisi başka birçok alanda faaliyet göstermektedir.

Kamu hizmet alanlarında da çok etin kullanım alanları vardır. Güven unsurunun ve şeffaflığın olduğu ortamlarda oylama, kontratlar, dijital kimlik, vergi sistemleri ve ödemeler gibi sistemlerde de kullanılmaktadır (Cognizant, 2016). Bu çalışmalara bazı ülkeler (İsviçre, İngiltere, Dubai, Singapur vd.) öncülük etmişlerdir.

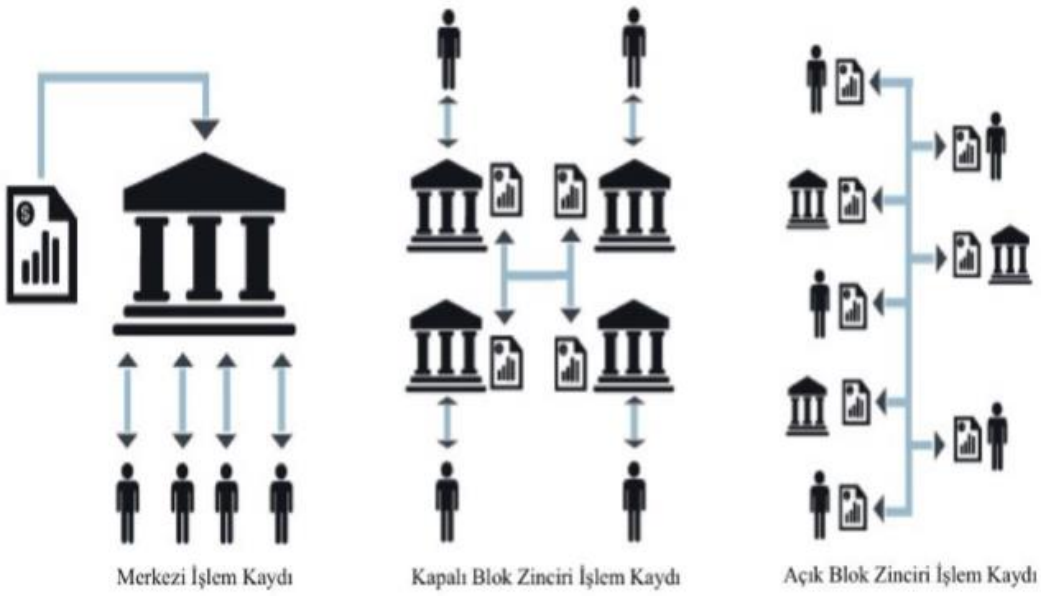
Sanayi sektörünün yoğun çalışma süreci olan ve Endüstri 4.0 çalışmalarıyla adını yaygınlaştıran nesnelerin interneti (Internet of Things) ile beraber güvenlik önemi artmıştır. İnternete bağlı olan cihazların veri paylaşımındaki güvenlikte blokzinciri önemli bir rol oynamaktadır.

5.11 Blokzincir Teknolojileri, Yöntemleri ve İş Modelleri

Blokzinciri en belirgin özelliği ile dağıtık sistemler üzerinde kurulmuş, test edilmiş ve kullanılmaktadır. Blokzinciri teknolojisinin dağıtık sistemlerde ya da merkezi olmayan sistemlerde kullanılması zorunlu değildir.

Blokzinciri teknolojisini kullanarak sistem oluştururken çalışma yöntemini ve mimarisini kendinize, kurumunuza ya da çalışma yöntemine göre şekillendirmek mümkündür. Fakat bununla birlikte bazı gereksimleri de karşılıyor mu diye kontrol etmek gerekir. Bazı mimarilerde örneğin, veriler birden fazla kullanıcı tarafından yazılmayacaksa, kullanıcılar ya da kurumlar arasında bir güven mekanizmasının kurulmasına gerek yoksa blokzinciri teknolojisi kullanılmak zorunda değildir (Blokzincir teknolojisi, 2017).

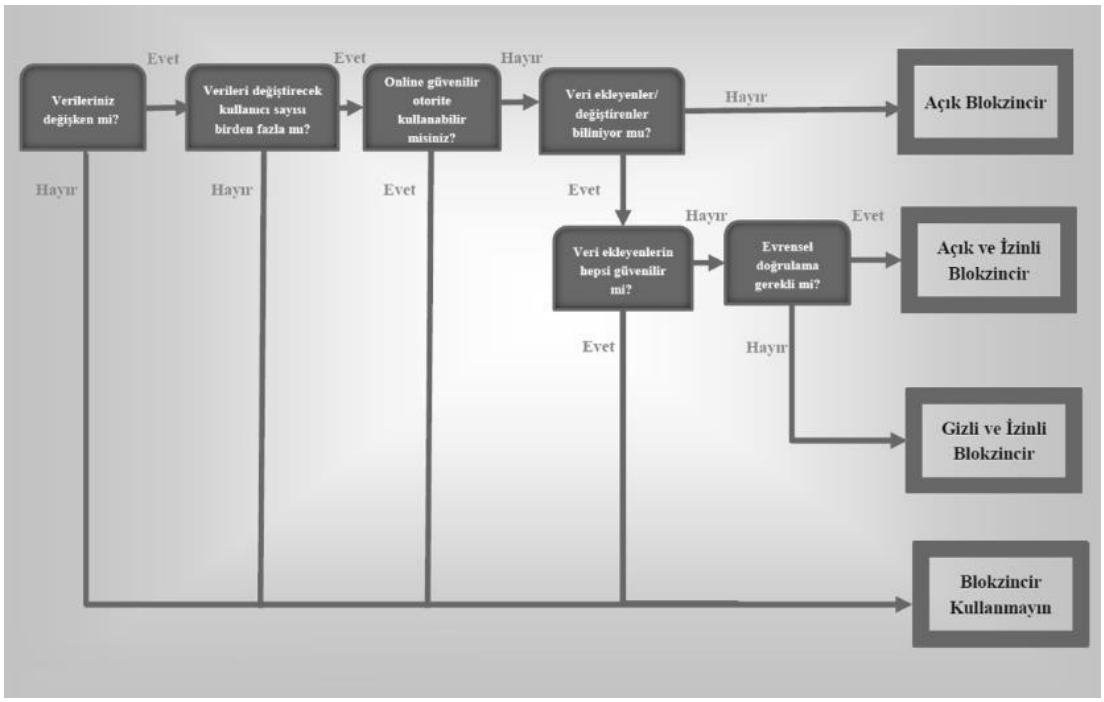
Günümüzde özellikle kamusal ve finans alanındaki sistemler merkezi mimari ile çalışmaktadır. Blokzinciri teknolojisini elinizdeki iş modeline göre kapalı ya da açık blokzincir kaydı olmak üzere uygulayabiliriz (Şekil: 5.7).



Şekil 5.7 : Merkezi İşlem Kayıtları, Kapalı ve Açık Blok Zinciri İşlem Kayıtları

Kaynak: (Lanka Business Online, 2016)

İş modellimizi oluşturmadan önce bazı soruları yanıtlayarak mimarinize karar verebilirsiniz (Şekil: 5.8).



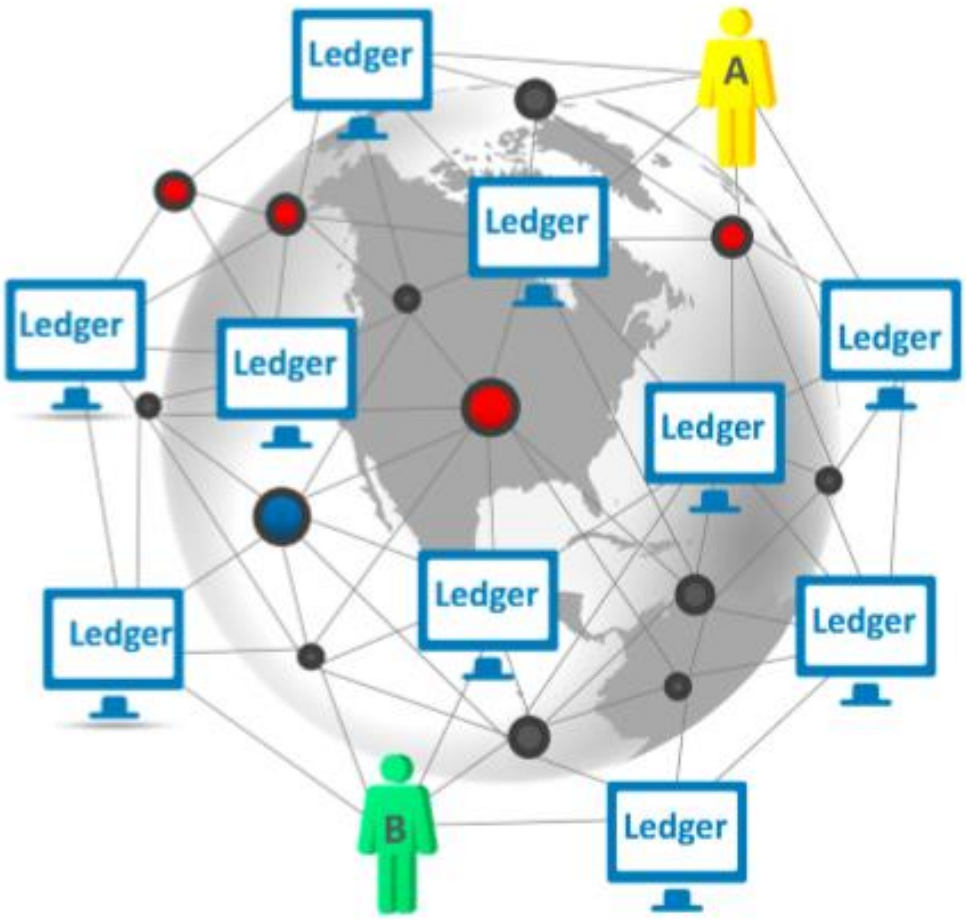
Şekil 5.8 : Blokzincir İş Modeli Karar Ağacı

Kaynak: (Blokzincir teknolojisi, 2017)

5.11.1 Açık Blokzincir Teknolojisi

Hiçbir merkezi kişi veya sisteme bağlı olmaksızın herkesin sistem üzerinde veri okuyabildiği ve yazabildiği sistemlere açık blokzincir denilmektedir. Bu zincire dahil olan her kişi veya kurum herkesin sahip olduğu haklara sahip olurlar. Bu hak zincir içeriğindeki kayıtların görüntülenmesini ve veri yazabileceği anlamına gelir.

Bu mimaride gönderici ile aracı arasındaki tüm işlemler diğer sisteme dahil olan kişiler ya da kurumlar tarafından da kayıt altına alınır ve görüntülenebilir. İşlem doğrulu bu düğüm noktalarıyla sağlanır. (Şekil: 5.9)



Şekil 5.9 : Açık Blokzinciri Gösterim Örneği

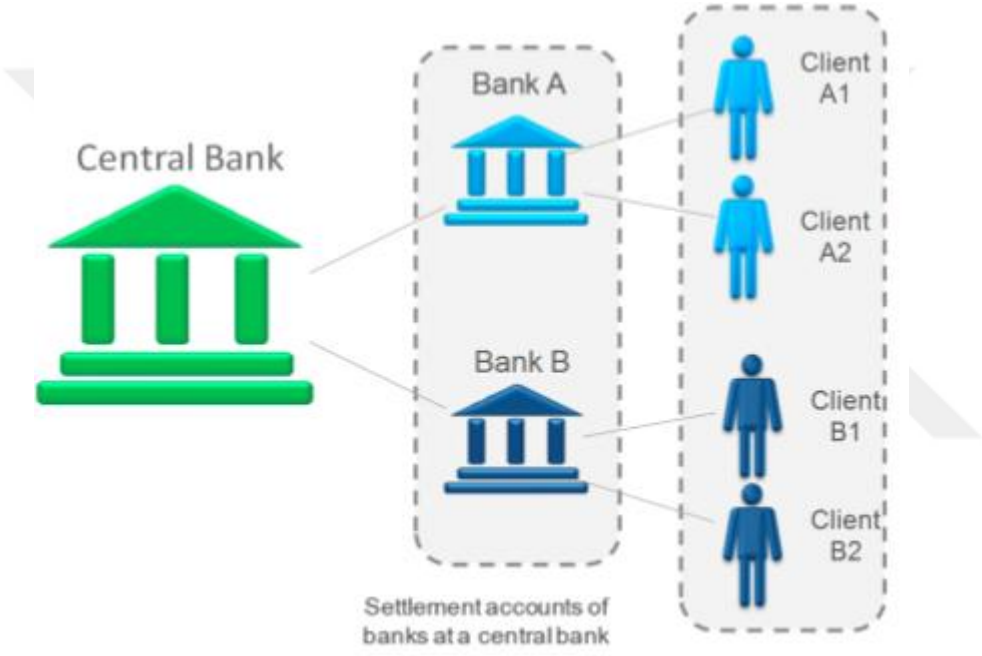
Kaynak: (He, D. ve diğerleri, 2016)

Blokzincirinin oluşmasını için gerekli olan matematiksel hesabı BTC'de olduğu gibi bu düğümler sağlar. Düğümlerden biri yanlış bir bilgi ya da hile yapmak isterse sistemdeki diğer tüm düğüm noktalarını ikna etmek durumundadır.

5.11.2 Kapalı Blokzincir Teknolojisi

Bu sistem daha çok kamu alanlarında kullanılır. Kapalı sistemlerde kullanıcıların kim olduğu ve yetkileri bilinir. Örneğin devletin birimleri kendi aralarında yaptıkları blokzincir uygulamalarında bu yöntemi tercih ederler. Bu sistemde her veri herkes tarafından okunmaz ve sadece yetkili olan birimler sisteme kayıt yazabilir.

Bu sistem daha çok tercih edilse de saldırıya daha açık olan yöntemdir. Merkezi sistemler barındırdığı için tehditlere karşı savunmasızdır. Merkezlere yapılacak olan bir saldırıda ya manipülasyonda veriler okunamaz olsa bile sistem kullanılmaz duruma gelebilir (Blockchain technology, 2017).



Şekil 5.10 : Kapalı Blokzincir Gösterim Örneği

Kaynak: (He, D. ve diğerleri, 2016)

Şekil 5.10'da kapalı bir merkezi bağımlılığı olan blokzinciri yapısı gösterilmiştir. Buradaki örneği açıklarsak, A1'den A2'ye gönderilen bir parayı A bankası merkezi bir otorite olarak doğrular. Bunun için A1 ve A2'nin tüm kişisel bilgileri, hesap bilgilerini tutar. Güven merkezi A bankasıdır.

A2'den B1'e gönderilen bir miktar para öncelikle merkez bankasına iletilir. Merkez bankası A bankasından A2'nin göndereceği tutarı çeker ve B bankasına iletir. B bankası da gelen parayı B1'e iletir.

Böylelikle tüm bilgilerimizi birkaç nokta üzerinden paylaşıyor oluruz ve bu merkezi sistemlere güvenmek zorunda kalırız.

Bankalararası Kart Merkezi verilerine göre 2018 yılında ülkemizde kullanılan kredi kartlarının sayısı 66.304.603'dir (POS, ATM, kart sayıları 2018). Kredi kartları genelde VISA ya da MASTER kart olarak ikiye ayrılır ya da birlikte kullanılır. VISA ve MASTER kartlar teorik olarak bir ödeme sistemi türüdür. Yapısal olarak aynı görevi görürler ve birbirlerine karşı rakiptirler. Eğer cebinizde bir VISA kredi kartı taşıyorsanız, 4.000'den fazla merkezi düğümü olan ve merkezi İngiltere'de bulunan bir sistemin parçasısınız anlamına gelir ve tüm bilgileriniz buralarda da kopyalanmıştır (Mastercard ve Visa nedir, farkları nelerdir? 2013)

5.12 Blokzinciri Uygulamalarında Zorluklar ve Riskler

Blokzinciri uygulamaları ve barındırdığı güvenlik yapısı ile ne kadar ilgi çekse de uygulama alanlarında bazı zorluklara ve risklere sahiptir. Geleneksel veri gönderme ya da para transferi ile karşılaştırıldığında, blokzincirinin gelişim ve dolaşım hızının arttırılması için daha çok çalışılması gerekildiği kaçınılmazdır.

Blokların oluşturulması için yapılacak matematiksel işlemlerin zorluğu uzun hesaplamalar yüksek miktarda enerji ve kaynak kullanımına neden olmaktadır. Bu sistem her ne kadar rekabetçiliği ve güvenliği artırırsa da günümüz koşullarında zorlayıcı bir engeldir. Bu nedenle blokzinciri madencileri sürekli olarak rakiplerine karşı kaynaklarını güncel tutma ve geliştirmek zorundadır.

BTC gibi yaygın kullanılan açık blokzinciri sistemlerinde örneklerini gördüğümüz özel anahtar saklama sorunu bir diğer etkendir. Kullanıcılar eğer özel anahtarlarını unuturlarsa BTC hesaplarına ve işlemlerine erişemezler. Bu nedenle birçok kullanıcı üçüncü bir dijital cüzdana güvenerek gizli anahtarlarını orada sakladılar ve 2016 yılında Bitfinex dolandırıcılığı olarak adlandırılan saldırıda 120.000 BTC kullanıcıların cüzdanlarından çalınmıştır (İnanç, B 2017). Bu rakam günümüzde 5.336.594,66 TL etmektedir. 1 BTC = 44.471,62 TL (kur zamanı: 17.05.2019 – 14:32)

Blok oluşturmadaki zorluklar ve blokzincirine dahil edilmesinde geçen süreler, açık blokzinciri sistemlerinde işlem performansını da çok yüksek seviyede etkilemektedir. BTC saniyede 3-4 işlem gerçekleştirilirken, geleneksel kredi kartı ödeme sistemi olan VISA saniyede 1,667 işlem gerçekleştirilebilmektedir (Bitcoin vs Visa transactions per second, 2018).

Blokzinciri teknolojisin önündeki bir diğer engel ise dijital dönüşümün şart olması. Kapalı veya açık sistemlerde kullanılmak istendiği takdirde şirketler mutalaka dijitalleşme sürecini tamamlamış olmak durumundadır. Bu da bazı şirketlerin stratejik çalışmalarını gözden geçirilmesine ve kurum kültürünün yenilenmesine ve yüksek yatırımlara neden olacağından caydırıcı bir madde olarak kendini korumaktadır.

Blokzinciri teknolojisi özellikle açık sistem olarak kullanılacaksa ciddi bir yazılım zafiyeti anlamına gelebilir. Bu teknoloji daha çok yenidir. Bu nedenle birçok kullanım alanında "deney" ya da "demo" olarak adlandırılır. Açıkları ve saldırı alanları tespit edilmemiş olabilir. Fakat kapalı sistemler bu sorun daha da az olacaktır.

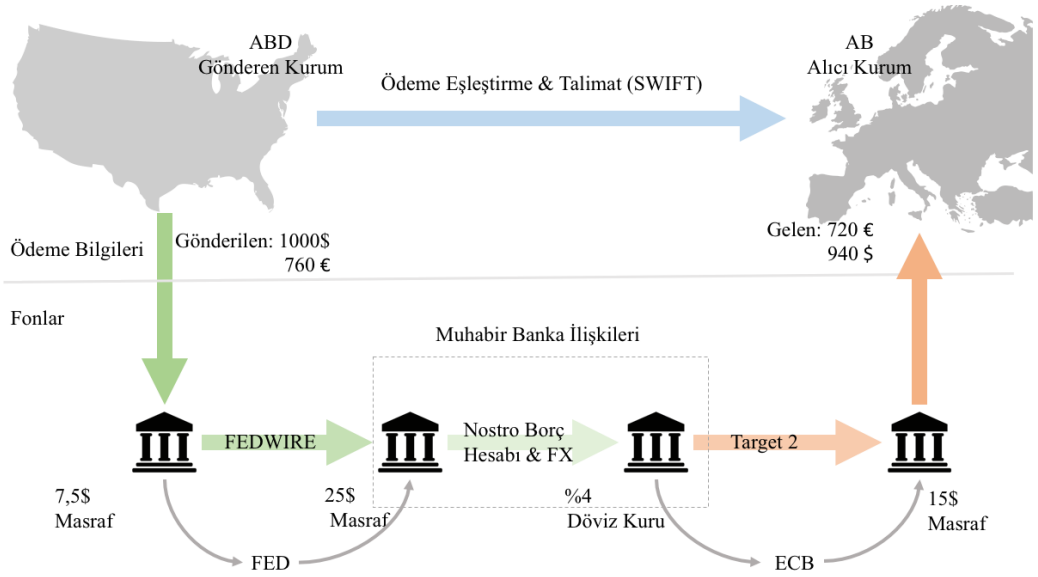
Son yıllarda kendinden söz ettiren ve şu an kurumların bilgi işlem departmanlarını meşkul eden bir diğer konu Kişisel Verilerin Koruma Kanunu (KVKK)'dur. KVKK ile blokzinciri birçok alanda çakışmaktadır. Blokzincirinde verilerin değiştirilemeyeceği ve silinmeyeceği ele alınmıştı fakat KVKK kişi isterse sistemden verisini silebilir maddesini barındırır. Bir başka örnek ile miras bırakma hakkı BTC gibi kripto işlemlerinde imkansız durumdadır. Eğer özel anahtar kaybolursa ya da devredilmezse başka bir kişiye o cüzdanın içerisindeki miktar ya da işlemler başkası tarafından erişilemez. Bu sebeple bazı merkezi kapalı sistemler kurulmuştur. Bu sistemler blokzinciri ya da BTC gibi kripto paraları sizin adınıza saklar ve ölümüzden sonra mirascılarınıza devreder.

6. B2B FİNANS İŞLEMLERİNDE KULLANILABİLİRLİĞİ

Uluslararası veya ulusal ticaret işlemlerinde merkezi ve aracı firmalar arasında rekabet ve hız yarışı devam ederken, hiçbir merkezi otoriteye bağlı kalmadan tamamen dağıtık bir sistemde blokzinciri teknolojisi yeni bir düzen getirmektedir. Birbirini hiç tanımayan iki ticari veya kamu kurumu mali işler yapmak durumunda kaldığında geleneksel teknolojide araya bir dizi merkezi otoriteye girer ve paranın dolışım kuvveti ile orantılı birçok farklı maliyet doğurur. Blokzinciri tabanlı bir finans sistemi ortadaki tüm merkezi otoriteleri ortadan kaldırır ve üçüncü hiçbir sisteme bağlı kalmaksızın neredeyse sıfıra yakın bir maliyet ile işlemlerini gerçekleştirebilir (Economist, 2015).

Blokzinciri kullanıcılar için şu an sadece internet üzerindeki bir dijital para sistemi olarak görülmektedir. IoT teknolojisi gibi B2B işlemlerini de birbirine bağlayabilecek yapıdadır. Çalışmaları günümüzün en önemli alanlardan biri olduğu için para ve ödeme sistemleri üzerinde yoğunlaşmıştır. B2B işlemlerde kullanıldığı takdirde uluslararası ya da ulusal düzeyde para transferinde maliyetler azalacak günler süren transfer işlemleri gerçek zamanlı düzeyine gelecektir. Bu süreç kullanıcılar tarafından şeffaf bir şekilde istenilirse izlenebilecektir.

Blokzincirinde işlemler sadece B2B para transferi ya da diğer finans işlemlerini kapsamaz. BTC'de programlanabilir paranın gücünü gördük. Bu sadece parada değil programlanabilir mülkiyet, sözleşmeler, kontratlar gibi birçok sistemi de kapsar. B2B sistemlerde etkileşim olan her adımda güven ve şeffaflık sağlar.



Şekil 6.1 : Paranın uluslararası trafiği

Kaynak: (Ripple 2014)

B2B uluslararası işlemlerde gönderilen bir değer para yaklaşık %6-7 oranında değer kaybeder ve bu oran aracı firmalara verilir (Şekil: 6.1). ABD'de yerleşik bir kurum Avrupa'da yerleşik bir kuruma para transfer etmek istediğinde aracı banka ve mutabakat sistemleri (FEDWIRE) devreye girer ve bu hem ek masraflara yol açar hem de ulaşım süresini arttırır. Eğer aracı olarak bir banka kullanılmak istenmez, daha hızlı ve başka bir merkezi otorite kullanılmak istenilirse para transferi maliyeti %10 oranını geçmektedir.

Hiçbir merkezi olmayan ve tamamen eşler arasında finansal işlemleri gerçekleştiren BTC ve benzeri sistemler yeni bir B2B işlemler zincirini oluşturmuş ve yeni bir çağ açmıştır. Blokzinciri teknolojisinden aldığı güçle kendisinden söz ettiren ve başarılı finansal işlemlere imza atan BTC hızla gelişmekte ve kullanılmaktadır. Merkez bir otorite ile kontrol edilemediği için devletler tarafından kabul görmese ve illegal sayılsa da sistemi ve BTC para birimi tanıyan ve destekleyen devletlerin sayısı gün geçtikçe artmaktadır. Bu nedenle blokzincirinden etkilenecek her türlü sistem yeni teknolojik ve hukuki düzenlemeler ile yeniden tasarlanmalıdır.

Blokzincirinin B2B finans işlemlerinde kullanılabilirliğinin yanında başka birçok sistem için de kullanılması mümkündür. Yine B2B işlemler için, sözleşmeler, emtialar, harcama kayıtları, müşteri kayıtları, silah ruhsatları, arazi kayıtları, tabu kayıtları, suç kayıtları, pasaportlar, oylama sistemleri, insan kaynakları bilgileri, yazılım lisansları ve benzeri birçok alanda kullanılabilirdir.

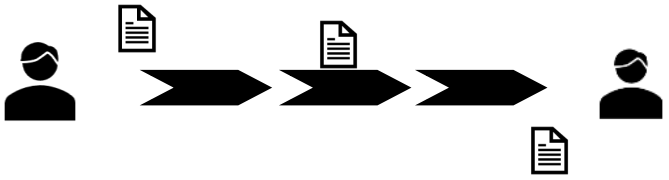
6.1 B2B Para Transferinde Blokzinciri

Bugün kullandığımız mevcut finansal işlemlerde paralar sürtünme kuvvetine maruz kalmaktadır. Bu işleme finansda "çarklardaki kum taneleri – sands in the wheel" denir. Blokzinciri bu süreci en aza indirir hatta ortadan kaldırır. A kişisinden B kişisine ister ulusal düzeyde isterse uluslararası düzeyde para veya başka bir değer transferinde hiçbir başka değer ödemek durumunda kalınmaz.

Bunu internet devrimleri tarafından incelemek gerekirse; birinci internet devrimi öncesinde Türkiye'de ikamet eden A kişisinden Avrupa'da ikamet eden B kişisine gönderilen bir bilgi ortalama $70 maliyetle ve yaklaşık 10 gün süreyle iletilmekteydi. Bunun yanında bilginin bir kopyası A'da bir kopyası B'de ve en az bir kopyası ise taşıma firmasında bulunmaktaydı (Şekil: 6.2).

Şekil 6.2 : Birinci internet devrimi öncesi bilgi paylaşımı

Birinci internet devrimi sonrasında Türkiye'de ikamet eden A kişisinden Avrupa'da ikamet eden B kişisine gönderilen bir bilgi sıfır maliyetle ve yaklaşık 10 saniye süreyle iletilmekteydi. Uçtan uca bir paylaşım olsa da paylaşım yapılan ortama bir en az bir kopyası bırakılmaktadır. (Şekil: 6.3).



Şekil 6.3 : Birinci internet devrimi sonrası bilgi paylaşımı

İkinci internet devrimi öncesi Türkiye'de ikamet eden A kişisinden Avrupa'da ikamet eden B kişisine gönderilen bir değer (para vb.) banka gibi bir aracı kullanılarak gönderilen değerin yaklaşık %6-7 oranında maliyetle ve yaklaşık 2 gün süreyle iletilmektedir. Merkezi bir yapıya güven ve bağlılık olduğundan tüm kopyalar bırakılmaktadır ve güven merkezi işlemi gerçekleştiren ortamdır. (Şekil: 6.4).

Şekil 6.4 : İkinci internet devrimi öncesi değer (para) paylaşımı

İkinci internet devrimi sonrası Türkiye'de ikamet eden A kişisinden Avrupa'da ikamet eden B kişisine gönderilen bir değer (para vb.) banka gibi bir aracı ve merkezi bir yapı kullanmadan direkt olarak uçtan uca gönderim yapılması mümkündür. Böyle bir işlemde üçüncü hiçbir kurum ve şahısa şahsi bilgiler ve işlemin bilgileri paylaşılmayacak, %1'den az maliyet ve yaklaşık 10 dakika süreyle (blokların zorluk derecesi) gerçekleştirilir. (Şekil: 6.5).

Şekil 6.5 : İkinci internet devrimi sonrası değer (para) paylaşımı

Blokzinciri teknolojisi ile yazılmış olan herhangi bir X değer gönderimi altyapısı ile paranın dolaşım hızı belirgin bir düzeyde azalıyor. Daha hızlı ve güvenli değer transferi gerçekleşmiş oluyor.

6.2 Blokzincirinin B2B Finans İşlemlerinde Bankacılığa Etkileri

Bankalar genel olarak şirket ve kurumların tasarruf fazlalığını kaynağa alıp fon üreten ve ihtiyacı olana bu fondan kredi sağlayıp kar eden kurumlardır. Aynı zamanda iki kurumun veya kişinin arasındaki alışverişin merkezi olarak hem güven unsurudur hem de aktarımı sağlar ve bunun için de aradaki işlem üzerinden yüzde kazanır. Bankalar yüzyıllardır faaliyetlerini sürdürüyor, gelişen teknolojiye göre şekilleniyorlar. Eğer böyle bir düzen olmasaydı kurumların fonlarını kim tutacaktı? veya güvenmediğimiz birine fonumuzun aktarımı için aracı olmasını isteyebilecek miydik? bu soruların cevabı birçok kişi için tabi ki hayır.

Günümüz teknolojisinin getirdiğini noktada Blokzinciri hiçbir merkezi güven noktasına ihtiyaç duymamaktadır. İki kurum ya da kişi arasında hiçbir güven olması gerek yoktur. Birbirini tanımayan iki nokta arasında güvenli değer aktarımı sağlamaktadır. Bu sistem bankacılık sektörünü tamamen ortadan kaldıracak diyemeyiz ama oldukça azaltacağı kesindir. Günümüzde uluslararası banka markaları şimdiden blokzinciri için kollarını sıvadı bile. Teknoloji ile beraber kendini yenileyen ve geride kalmayan banka markaları bu sistemin nimetlerinden yararlanacak ve varlıklarını sürdürecektir.

Bankacılığın mevcut sistemini incelediğimizde menkul kıymetler işlemlerindeki takas ve ödemeler neredeyse 1-2 gün sürmekte, EFT işlemleri artık son derece hızlansa da komisyonlar alınmakta ve bu işlemleri her ne kadar bazı bankalar ücretsiz olduğu söylense de yıllık aidat ödemelerimizle bizden almakta, SWIFT işlemlerinde 3-4 gün süren işlemler olmakta ve yüksek komisyonlar almakta, özellikle SWIFT döviz işlemlerinde 3-4 gün süren para transferi sırasında para üzerinde ne gibi işlemler olduğu gönderici ve alıcı bilmemekteyiz (Yılmaz, D. 2018).

Yukarıda belirtmiş olduğum etkiler gönderici ve alıcı üzerindeki etkileri. Banka kurumlarının da yararlanabileceği özellikler vardır. Bölümün başında belirttiğim gibi bankalar kendini bu sisteme adapte ettiğinde takip etmekle yükümlü olduğu bir dizi işlemden kurtulmuş olacaktır. Günümüz bankacılık sistemi her ne kadar online ekranlar üzerinden sağlansa da belge trafiği ihtiyacı duyulmaktadır. Bankalar günlük yedeklerini hatta afet yedeği dedilen başka hata ve şehir üzerinde tutulan yedeklerini de alsalar bile merkezi yönetime tabidirler. Her gün artan saldırı çeşitleri ve sayıları ile kendilerini devamlı güncel tutmaya çalışsalar da banka sistemlerine yapılan saldırıları ve manipüle girişimlerini basında duyuyoruz.

Bankalar bünyelerine her geçen gün yeni IT güvenlik sistemleri eklemekte ve ekipler kurmaktadır. Blokzinciri teknolojisi ile beraber bu zorlukları aşıyoruz. Güvenlik maliyetlerimiz ve zafiyetlerimiz en az seviyelere çekilmektedir.

Tüm bankacılık sistemini blokzinciri teknolojisine bırakılması kabul edilemez bir yapı olur. Günümüz bankacılık sisteminin blokzinciri sistemine göre yetersizliğinden bahsetmiyorum. Bankalar son derece güvenli sisteme sahiptir fakat blokzinciri teknolojisi ile müşteri kalitesi artacak, güvenlik zafiyetleri ortadan kalkacak ve en önemlisi B2B işlemlerinde şeffaflık en yüksek seviyede ve uçtan uca gerçekleşecektir.

6.3 Ülkelere Göre B2B Finans ve Diğer İşlemlerde Blokzinciri Kullanımı

Blokzincirinin, Bitcoin kripto paranın alt yapısı olduğundan bahsetmiştik. Kapalı blokzinciri yapıları tasarlanırken bazı ülkeler BTC ile işlemlerini sürdürmeye başladı. Bu gelişmeler blokzincirinin yaygınlaşması ve doğru anlaşılmasının önünü açmaktadır. BTC'i ve blokzincirini tanımaya ve benimsemeye başlayan ülke sayısı gittikçe artmaktadır. Blokzinciri teknolojisine sadece B2B finansal işlemlerde değil herhangi A ve B noktası arasındaki tüm işlemleriyle ele aldığımızda bugün aslında hiç de kötü konumda değiliz.

Bir Afrika ülkesi olan Sierra Leone, ülke seçimlerinde blokzinciri teknolojisini kullanan ve başarılı olan ilk ülke oldu. Oylar blokzinciri teknolojisi kullanılarak kripto-hashlendi ve daha sonrasında sayılarak oylama işlemi tamamlandı. Bu çalışmayı İsviçreli bir firma gerçekleştirdi (Pollock D. 2018).

Estonya Hükümeti blokzincir teknolojisini ülkesindeki sağlık sisteminde kullanılmak üzere çalışmalara başladığını duyurdu. Bu sistem ile yaklaşık 1 milyon verinin güvenliği ve sistem içerisinde B2B ödemeleri blokzincir teknolojisi ile sağlanacak. Aynı zamanda kendi kripto parasını da üretmek için çalışmalara başladılar.

İsviçre'de BTC ve blokzinciri teknolojisi çok yaygın olarak kullanılmaktadır. Zug şehrinde 200 CHF'ye kadar olan ödemelerede BTC kullanılıyor. Ülkenin önde gelen demiryolu şirketlerinden SBB biletlerini BTC ile satmaya başladı ve aynı zamanda şirket akıllı kontratları da blokzinciri teknolojisi ile gerçekleştiriyor.

İsveç Finansal Denetçi Otoritesi, BTC'i ödeme sistemi olarak yasallaştırdı.

Dubai 2020 yılında tüm devlet online işlemlerini blokzinciri teknolojisi ile yapacağını duyurdu (Blockchain 2019).

Hollanda ve Finlandiya özellikle bankacılık işlemlerinin güvenliğini arttırmak için sistemlerini blokzincir teknolojisine göre yeniden şekillendiriyor.

İngiltere BTC ile yapılan alışverişlerde vergi uygulamaya başladı. Buda resmi olarak BTC işlemlerini tanıdığı anlamına geliyor.

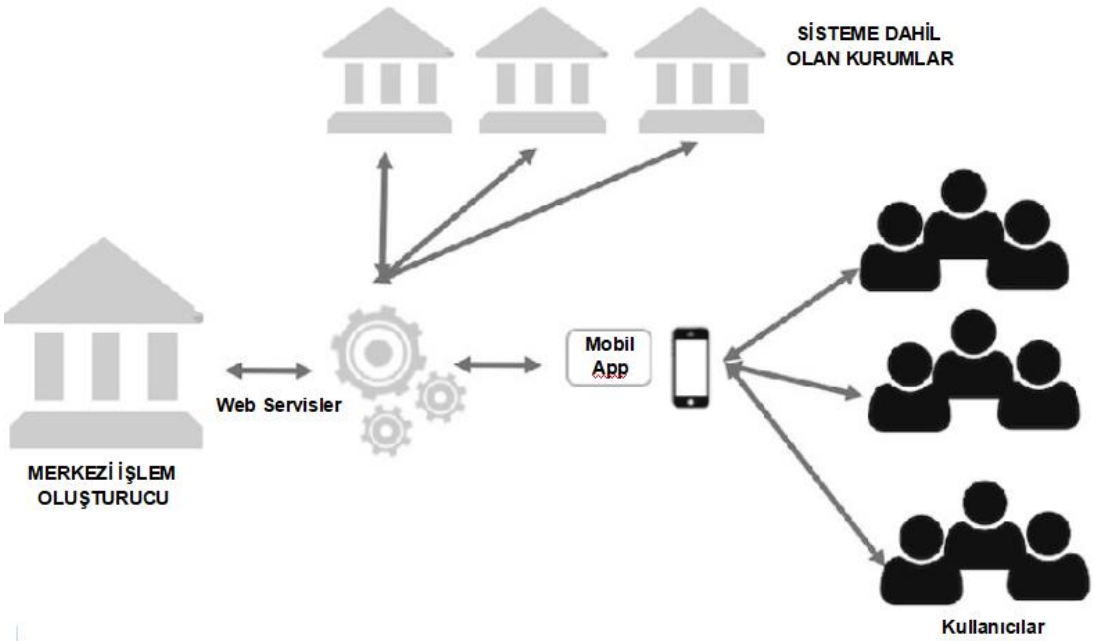
Rusya sadece BTC'e değil diğer kripto paralarla da ilgileniyor. Ethereum ile yakinen ilgilenen ülke kendi kripto parası üzerinde de çalıştığını ve aynı zamanda kendi para biriminin bir kısmını da kripto paraya dönüştüreceğini duyurdu.

6.4 Kapalı Blokzinciri B2B Finans Sistemi ve Örnek Uygulama

Bu çalışamada blokzinciri teknolojisinin başından günümüze kadar gelişimini, finans sektöründeki etkileri ve geleneksel sistemi ile farklarını ele aldık. Açık blokzincir teknolojisindeki devlet baskıları ve önündeki engeller ve artan blok sayısına bağlı olarak sistemin yavaşlaması neticesinde kapalı ve devlet kontrolünde sistemler geliştirilmelidir. Bu sisteme örnek olması açısından bir uygulama gerçekleştirilmiştir.

6.4.1 Sistemin Genel Yapısı

Sistem birkaç kurumun bir araya gelmesiyle oluşturulmuş bir kapalı blokzinciri olarak kurgulanmıştır. Bitcoin'de bulunan nonce oluşturma ve mining maliyetlerini düşürmek için gönderilecek değerin onayını merkezi bir sistem üzerinden hesaplanıp hashlenen veri ile diğer sisteme dahil yapılara web servis kullanılarak dağıtılacak bir kapalı dağıtık sistem oluşturulmaya çalışılmıştır (Şekil 6.6).



Şekil 6.6 : Uygulama Örneğinin Genel Yapısı

Kaynak: Yazar

Tasarlanan sistem açık bir blokzinciri olmadığından ve blok oluşturmayı zora sokan süreleri arttıran PoW ve PoS madencilik işlemleri olmadan merkezi bir kurum tarafından oluşturulan zincir hash sistemi kullanılmıştır. Bu hash datası sisteme dahil olan diğer kurumlara web servisler üzerinden dağıtılmaktadır. Olası sistem manipüle ve saldırılara karşı dirençlidir. Bütünlük, kullanılabilirlik, hata toleransı yüksek, gizlilik seviyesi düşüktür. Herkese açık bir web sayfasından tüm işlemler görüntülenebilir. Bir kayıt bloluğu hangi aşamalardan geçtiği izlenebilir fakat içeriği sadece ilgili iki noktayı kapsar.

Örnekteki sistem ile sistemdeki var olan datayı değiştirebilmek için var olan tüm veriler üzerinden hash hesaplaması yapılması gerekmektedir. En az sistemin %51'ne sahip olması durumunda sistem tehlikeye girer.

6.4.2 Uygulamanın Amacı ve Sistem Bileşenleri

Uygulama A noktasından B noktasına örnek olarak tasarlanan bir değerin aktarılmasını kapsar. Bu değer bir miktar para olarak kabul edilmiştir. Bu paranın değeri sisteme dahil olarak kurumlarla bağlantılıdır. Kullanıcı sisteminde tanımlı paranın değerini sistem üzerindeki kurumlarda kullanabilir.

Uygulamanın ana amacı kapalı sistemlerde ve güvenilir kurumlarla beraber çalışıldığında sistem performasını ölçmek, madencilik yapmadan blokzincir uygulamasını çalıştırmak ve olabilirliği konusunda yorumlar yapabilmektir.

Uygulama kapsamında bir merkezi micro web servis üreten sistem tasarlanmıştır. Bu sistem Microsoft yazılım dili ile kodlanmıştır. İlk gelen isteği yaptığı kontroller sonrasında uygunluğu ile geri döndürmek ve sistem akışını sağlamaktır.

İşlemleri gerçekleştirebilmek için bir adet android mobil uygulama gerçekleştirilmiştir. Hesap bilgileri, işlem talepleri, karekod üretme ve işlemler mobil uygulama üzerinden gerçekleştirilir.

Doğrulanan her işlem diğer partner kurumlara bir önceki zincirin özet hash bilgisi ile bağlanarak iletilir.

Sistemin genel incelenmesi ve işlemlerin takibi için PHP web programlama dili ile bir izleme sayfası kodlanmıştır.

6.4.3 Kayıt Bloklarının Oluşturulması

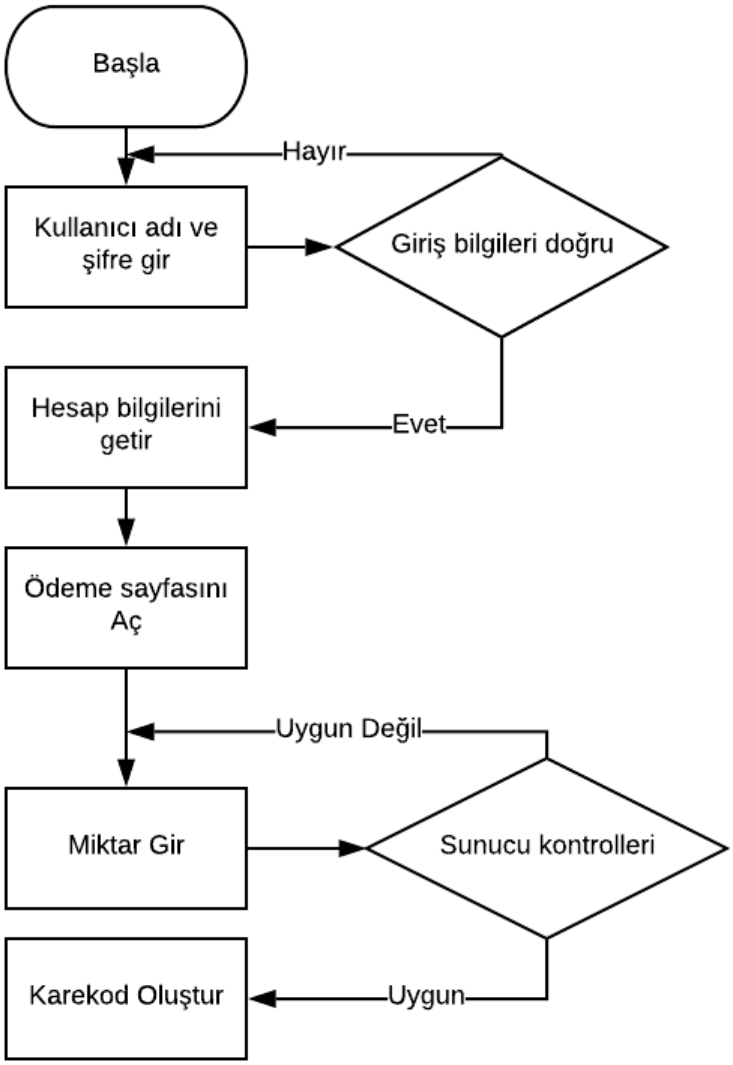
Kişiler sisteme dahil olabilmesi için resmi bilgileriyle kayıtlı olması gerekmektedir. Kendilerine verilen kullanıcı adı ve şifre ile sisteme giriş yaparlar. Bu çalışmada kullanıcının kayıt süreçleri ve kayıt yetkilendirilmesi ele alınmamıştır. Bu adımlar ayrı bir süreçtir ve oluşturulan kapalı sisteme dahil olan kurumların ortak kararı ile belirlenmelidir. Kullanıcılar sisteme kayıtlı ve yetkilendirilmiş olarak kabul edilmiş ana odak noktası blok oluşturulup blokların birbirine bağlanması ve A'dan B'ye aktarılmasıdır. Böylelikle B2B finans işlemlerinde kullanılabilirliği ölçülecektir.

A kullanıcısı ve B kullanıcısı işleme başlamak için sisteme girerler. A kullanıcısı sistemindeki tanımlanmış veya var olan sahip olduğu değeri görebilir ve B kullanıcısına aktarmak için aktarım menüsüne girer. Bir miktar yazar ve ödeme arzı oluşturur. Eğer sistemde aktif açık bir ödeme talebi yok ise talebi kabul edilir. Web servis ana sunucuya ulaşarak gerekli kontrolleri sağlatır. Sunucu A kullanıcısının talebini karşılar, değer kontrolü yapar ve bu işlemi gerçekleştirebilmesi için izin oluşturur ve geriye hash döndürür. Bu hash 60 saniye için sistemde açık tutulur. Eğer 60 saniyede karekod karşılanmazsa sunucu isteği iptal eder. 60 saniye içerisinde A kullanıcısı yeni bir karekod oluşturamaz ya da bir önceki iptal edebilir. B kullanıcısı,

A kullanıcısının oluşturduğu hashli karekodu okutur. Yine web servisler aracılığı ile gerekli kontroller sağlanır, A kullanıcısının değer kontrolleri, karekodun geçerlilik süreleri yeniden kontrol edilerek A'dan B'ye değer aktarımı yapılır. A kullanıcısı ve B kullanıcısı işlem sonrasında bilgilendirilir. İşlem kapalı dağıtık yapı içerisindeki son bloğun özet bilgisi yazılarak kayıt edilir ve sisteme dahil olan tüm kurumlara anons edilir.

Şekil 6.7 : Uygulama ekranları (giriş, ana ekran, istek oluşturma ve karekod)

Kaynak: Yazar



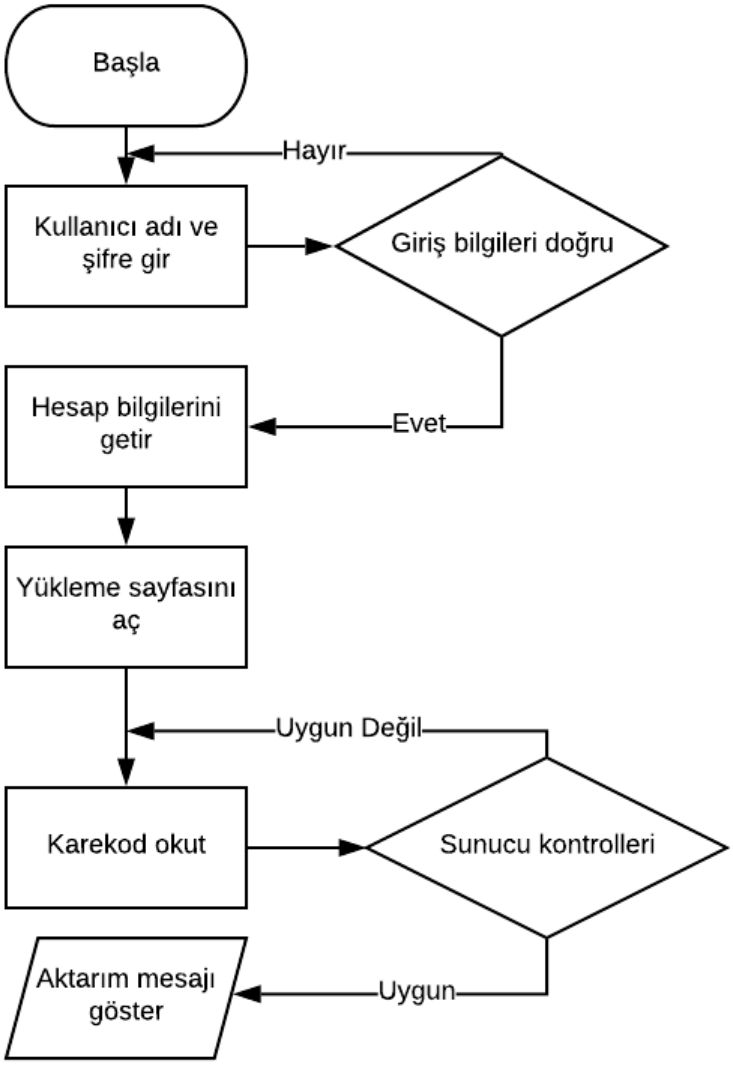
Şekil 6.8 : Karekod oluşturma temel algoritması

Kaynak: Yazar

Şekil 6.7'deki uygulama ekranlarını kullanarak kullanıcı A Şekil 6.8'de gösterilen algoritma ile karekod oluşturur. Sunucu kontrolleri aşamasında yapılan işlem sırası şu şekildedir;

- A kullanıcın yeterli miktarı var mı?
- A kullanıcının göndermek istediği miktar, bakiyesini karşılıyor mu?
- A kullanıcısının aktif talebi var mı? (Sorgu olmaması durumunda çalışacaktır)

B kullanıcı oluşturulan karekod okutarak hesabına değeri alır. Bunun için Şekil 6.9'deki algoritma kullanılır.



Şekil 6.9 : Karekod okuma temel algoritması

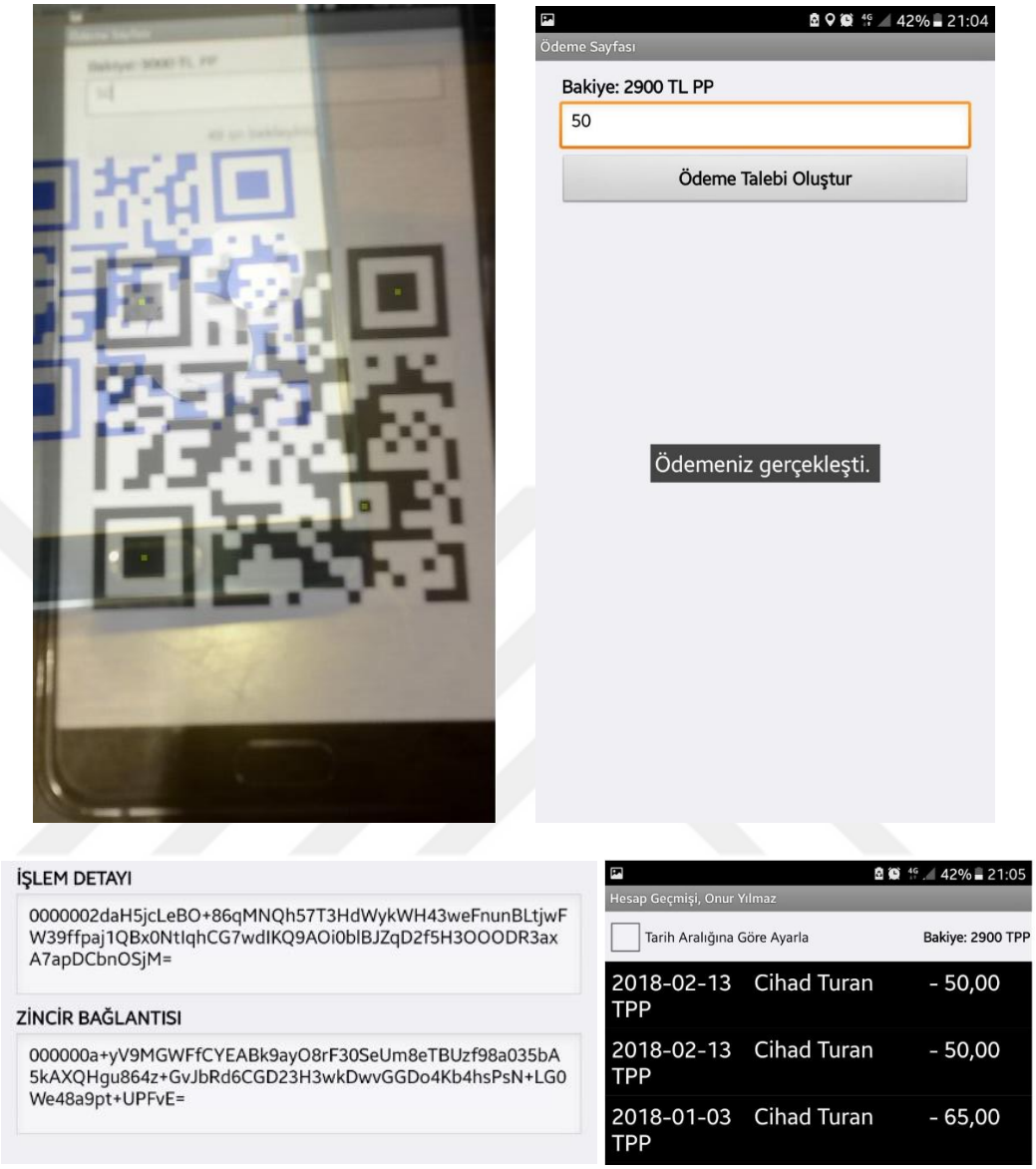
Kaynak: Yazar

Sunucu kontrollerinin bu aşamasında da aşağıdaki sıra ile işlem yapılır;

- A kullanıcısı tarafından oluşturulan karekod halen geçerli mi?
- A kullanıcısın bakiye durumu ve göndermek istediği miktar doğru mu?

Eğer bu soruların hepsi karşılanıyorsa blok oluşturulur. Blok boyutu, oluşturma zamanı, oluşturma yeri, A kullanıcısı bilgisi, B kullanıcısı bilgisi, aktarım miktarı belli bir kuralla göre hashlenir ve blok özeti alınır. Bir önceki bloğun hash özeti ile beraber

sistemde var olan kurumlara anons edilir. Eğer bir önceki blok oluşmamışsa, ilk kayıt ise 256 adet 0 yazılarak zincir başlangıç bloğu oluşturulur.



Şekil 6.10 : B kullanıcısının okuma işlemi ve A kullanıcısının onay mesajı ekranı

Kaynak: Yazar

Kullanıcı uygulama üzerinden ilgili işlem detayını kontrol edebilir. İşlem detayı ve bağlantılı olduğu zincir hash bilgisini görebilir fakat sadece kendi bilgilerini okuyabilir.

6.4.4 Uygulama Sonuçları

Uygulama kısıtlı denemelere tabi tutulmuştur. Blokzinciri sisteminin tam anlamıyla test edilebilmesi için gerekli çoğunlukta düğüm noktalarına ve kullanıcıya ihtiyaç vardır. Bu nedenle uygulama sadece blokzinciri alt yapısı ile verileri birbirine belirli bir kural çerçevesinde bağlayıp, yine belirli bir kurala dayalı şekilde hash üretmenin mümkün olduğunu göstermiştir. Madencilerin birbiri ile yarıştığı açık kripto para sistemlerindeki yaşanan blok oluşturma zorlukları ve artan sürelerin önüne kapalı ve kontrol edilebilir sistemlerle geçebilmektedir. Devlet kurumlarının sisteme dahil edilmesiyle daha güvenli olacağı düşünülen sistemde yine bankarın da barınmasıyla sistem çok kararlı ve güvenli çalışacaktır.

Bitcoin'de olduğu gibi 10 dakika blok oluşturma zorluğu sisteme entegre edilmemiş ve madenciler kullanılmamıştır. Belirli bir kurala dayalı olarak ana merkez sunucu hash üretmektedir. Bu hash versiyon sürüm bilgisi ile sisteme kayıt edilir. İlerideki güvenlik geliştirimleri ile sürüm kontrolü yapılarak önceden oluşturulan blok verilerine ulaşım kolaylaşacaktır.

Yapılan testlerde sunucu cevapları ve kullanıcı talepleri ortalama 876 mili saniyede çalıştığını göstermektedir.

Örnek uygulama laboratuvar ortamına taşınmalı ve sanal sunucular üzerinde testler gerçekleştirilerek similasyonu gerçekleştirilmelidir. Daha sonrasında sistem ihtiyaçları ve fiziki donanım ihtiyaçları maliyetleri ortaya çıkacaktır.

Bu kısıtlı uygulama bile böyle bir sistemin güvenliği konusunda üzerinde çalışılması gerektiği çok konu olduğunu göstermektedir. Ana sunucu kim olacaktır? A'dan B'ye gönderilecek değer ne olacaktır? Eğer para olacak ise ana yükleme merkezleri nasıl çalışacaktır? Yeni bir coin mi üretilecektir yoksa geleneksel paranın temsili olarak mı tasarlanacaktır? Gerçek değere dönüştürümler nasıl olacaktır?

Bu sorulara verilecek doğru cevaplar, kurumlar arası birliktelik ve devlet ile güçlü bir yapı oluşturulup kapalı sistemler üzerinde geliştirilen B2B finans ve diğer tüm bilgi paylaşımları başarılı olacaktır.

7. SONUÇLAR VE ÖNERİLER

Bu araştırma tezi tarihten bu yana paranın tanımlarına ve gelişimlerine yer vermiştir. Adını Bitcoin ile duyuran ve internetten sonra en büyük yazılım icadı olarak kabul gören Blokzinciri teknolojisi ve teknik detayları hakkında bilgiler verilmiştir. Karmaşık yazılımsal terimlerle ya da matematiksel işlemlerle anlatmaktansa en yalın ve temel bilgilerle aktarılmıştır. Blokzincir teknolojisi birçok alanda kabul gördüğü gibi B2B finansal işlemlerde büyük özellikler sunmaktadır. Blokzinciri üzerinde yasal düzenlemeler devamlı geliştirilmektedir. Sisteme devletlerin ve uluslararası politikaların dahil olmasıyla beraber artan akademik çalışmalar yasal düzenlemelere karşı eleştirilere ve geliştirimlere olumlu yönde neden olacaktır. Araştırma süresince örnek bir uygulama geliştirilip, blokzinciri teknolojisinin B2B finans işlemlerinde kullanılabilirliğinin mümkün olduğunu göstermiştir. Kurumlar kendi blok kurallarını ve kamu kurumlarında katılmasıyla güçlü ve son derece güvenli sistemler oluşturabilirler.

Blokzincir teknolojisi internetten sonraki en büyük buluş olarak kabul görse de teknoloji hem dünya hem de ülkemiz adına henüz çok yenidir. İnternetin ilk kullanıldığı günleri hatırlarsak bugünkü durumuna yaklaşık 30 yılda gelmiştir. Halen internet üzerindeki eksikliklerimiz ve geliştirimlerimiz devam etmektedir.

Her ne kadar güvenlik konusunda çığır açacak bir sistem olsa da içerisinde barındırdığı riskleri ve açıkları unutmamak gerekir. Bu riskler ve caydırıcı nedenler tezde yer verilmiştir. Fakat bu nedenler bizleri yıldırmamalı ve ülkemiz bu teknolojinin gerisinde kalmamalıdır. Blokzinciri teknolojisi ucu açık bir yazılım sistemidir. Bu açıkları kapatacak riskleri ve engelleri kapatacak yazılım modelleri geliştirilebilir ve uygulamaya konulabilir.

Dağıtık bir mimariye sahip olan blokzinciri teknolojisini işletmeler, üniversiteler ya da devlet kurumları tek başlarına girmemelidir. Mutlaka işbirlikleri oluşturulmalı kapalı sistemler üzerinde durulmalı ve geniş bir network çalışması ele alınmalıdır.

Blokzinciri kullanmak isteyen özel ya da kamu kurumları mutlaka kendi iş birliklerini kurmalı ya da var olan bir sisteme dahil olmalılardır.

Elinizdeki sistemi ya da kurmak istediğiniz mimarinin gerçekten bir blokzincirine ihtiyacı olacak mı? sorusuna cevap aranmalıdır. Teknolojiyi sadece kullanmak için geliştirmek kurumunuzu bir süre sonra yanlış stratejilere sokabilir.

Blokzincir teknolojisini sadece bankacılık ya da finans işlemlerde kullanılabilirliğini ele alırsak konuyu çok daraltmış oluruz ve tam anlamıyla verim alamayız. Bu teknoloji dijitalleşme sürecinin tümünü kapsamaktadır. Ödeme sistemleri bunun sadece içerisinde dahil olan bir parçasıdır.

Bu teknolojinin kullanılmasının yaygınlaşmasıyla beraber geleneksel sistemler üzerindeki etkileri görülecek ve ölçülebilecek duruma gelecektir. Blokzinciri sistemi birçok alanda akademik araştırma alanı açmıştır.

Yüzyıllardır alışkın olduğumuz ödeme sistemlerine bambaşka bir alan sunan kripto paralar ve arkasındaki blokzinciri teknolojisi ne kadar yaygınlaşırsa güvenirliği ve kullanım alanları artacaktır. Ülkemiz blokzinciri teknolojisini yakinen takip etmeli ve geliştirimlerden geri kalmamalıdır. Birkaç üniversitenin ve teknoloji merkezinin başlatmış olduğu gibi akademik alanda blokzinciri teknolojisi ders olarak gösterilmeli ve üzerine yapılacak çalışmalar desteklenmelidir.

KAYNAKLAR

Achenbach, J. (2016). Origin of gold is likely in rare neutron star collisions. Amerika Birleşik Devletleri: The Washington Post

Arıcan, E., Yücememiş, B., Işıl, G. ve Omağ, A. (2018). Bitcoin for Dummies. Ankara: Nobel Yaşam Yayınevi.

Sagona Stophel, K. (2015). Bitcoin 101: How to get started with the new trend in virtual currencies. White Paper: Thomson Reuters

Sergii, M. (2008). History of the Weksel: Bill of Exchange and Promissory Note, Amerika Birleşik Devletleri: Xlibris

İnternet Kaynakları:

Bankacılık Terimleri 2016, erişim: 15 Şubat 2019, <http://bankalar.org/bankacılık - terimleri>

Bitcoin vs Visa transactions per second 2018, erişim: 06 Mayıs 2019, <https://altcointoday.com/bitcoin-ethereum-vs-visa-paypal-transactions-per-second/>

Blockchain 2019, Smart Dubai, erişim: 06 Temmuz 2019, <https://www.smartdubai.ae/initiatives/blockchain>

Blockchain Technology 2017, erişim: 15 Ağustos 2017, <https://www.bafin.de/EN/Aufsicht/FinTech/Blockchain/blockchain_artikel_en.html>

Blokzincir Teknolojisi 2017, erişim: 05 Mayıs 2019, <https://blokzincir.bilgem.tubitak.gov.tr/bz-calistay/blok-zincir.html>

Blokzinciri 2018, erişim: 05 Mayıs 2019, < https://blokzincir.tubitak.gov.tr/bz-calistay/blok-zincir.html>

Cartwright, M. 2014, *Gold in Antiquity*, yayım tarihi, 4 Nisan, Ancient History Encyclopedia, erişim tarihi: 10 Mart 2019, <https://www.ancient.eu/gold/>

Chinese Ancient Currency 2012, Erişim: 15.01.2019, <http://www.ichina.org/news.asp?type=1&id=1195>

Cognizant, 2016, Blockchain in Banking: A Measured Approach, erişim tarihi: 05.05.2019, <https://www.cognizant.com/whitepapers/Blockchain-inBanking-A-Measured-Approach-codex1809.pdf >

Dalkılınç, S. 2016, Kanuna uygun olmadığından PayPal'ın lisans başvurusu onaylanmadı, erişim tarihi: 02 Haziran, Anadolu Ajansı, erişim tarihi: 10.04.2019, < https://www.aa.com.tr/tr/ekonomi/kanuna-uygun-olmadigindan-paypalin-lisans-basvurusu-onaylanmadi/582825>

Durant, E. 2017, Digital Diploma debuts at MIT, yayım tarihi, 17 Ekim, MIT News, erişim tarihi: 10.05.2019, < https://www.weusecoins.com/what-is-cryptocurrency/>

Economist 2015, Trust Machine, Erişim: 04.04.2019, Economist Online. < https://www.economist.com/news/leaders/21677-198-technology-behind-bitcoin could-transform-how-economy-workstrust-machine.>

European Central Bank 2015, erişim tarihi: 14.04.2019, <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>

Granger, S. 2016, Everything You Need To Know In The Ultimate Guide To What Is Cryptocurrency, yayım tarihi, 16 Kasım, We use coins, erişim tarihi: 10.04.2019, < https://www.weusecoins.com/what-is-cryptocurrency/>

Graydon, C. 2014, What is cryptocurrency? tarihi, 16 Eylül, CCN, erişim tarihi: 10.04.2019, < https://www.ccn.com/cryptocurrency>

Griffith, K. 2014, A Quick History of Cryptocurrencies BBTC Before Bitcoinyayım tarihi, 16 Nisan, Bitcoin Magazine, erişim tarihi: 05.04.2019, < https://bitcoinmagazine.com/articles/quick-history-cryptocurrencies-bbtc-bitcoin-1397682630/>

Halici, N. 2013, Altın nasıl oluşuyor? yayım tarihi, 17 Temmuz, Deutsche Welle, erişim tarihi: 20.03.2019, < https://www.dw.com/en/about-dw/profile/s-30688>

He, D., Habermeier, K., Leckow, R., Haksar, V., Almeida, Y., … Jagatsing, K. (2016), Virtual Currencies and Beyond: Initial Considerations Internatıonal Monetary Fund Monetary and Capital Markets, Legal, and Strategy and Policy Review Departments Virtual Currencies and Beyond: Initial Considerations. IMF. Erişim adresi: https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf.

İnanç, B. 2017, 31 milyon Dolar'lık kripto para soygunu, yayım tarihi, 23 Kasım, Dünya Halleri, erişim tarihi: 02.05.2019, <https://www.dunyahalleri.com/31-milyon-dolarlik-kripto-para-soygunu/>

Karekod (QR Kod) Nedir? 2018, Erişim: 10.05.2019, <http://www.cngmedya.com/karekod-qr-kod-nedir-nasil-kullanilir-cesitleri-nelerdir/>

Köse, B. 2019, Bitcoin madenciliği nihayet yüz güldürüyor, yayım yarihi: 21 Nisan, Uzman Coin, erişim tarihi: 20.05.2019, <https://uzmancoin.com/bitcoin-madenciler-kazanc/>

Lanka Business Online 2016, Erişim tarihi: Haziran, 2017, Erişim adresi: http://www.lankabusinessonline.com/opinion-blockchain-cryptoeceonomics-and-the-disintermediation-of-trust/.

Mastercard ve Visa nedir, farkları nelerdir? 2013, Erişim: 05.05.2019, < http://www.kredibulteni.com/kredi-kartlari/mastercard-ve-visa-nedir-farklari-nelerdir>

Morah, C. 2019, What is the gold standard? yayım tarihi, 3 Şubat, Investopedia, erişim tarihi: 02.03.2019, <https://www.investopedia.com/ask/answers/09/gold-standard.asp>

Nakamoto, S. 2008, Bitcoin: A Peer-to-Peer Electronic Cash System. Journal for General Philosophy of Science, yayım tarihi: 2018, erişim tarihi: 05.03.2019, <https://bitcoin.org/bitcoin.pdf>

POS, ATM, kart sayıları 2018, Erişim: 05.05.2019, <https://bkm.com.tr/pos-atm-kart-sayilari/>

Pollock, D. 2018, Who Created the Story of Sierra Leone's Blockchain Election? yayım tarihi, 29 Mart, Coin Telegraph, erişim tarihi: 06.07.2019, < https://cointelegraph.com/news/sierra-leones-fake-blockchain-election-hasnt-damaged-the-technologys-reputation>

Prior, E. 2013, How much gold is there in the world? yayım tarihi, 1 Aralık, BBC News, erişim tarihi: 15.03.2019, <https://www.bbc.com/news/magazine-21969100>

Promotional graphics 2015, erişim tarihi: 15.02.2019, < https://en.bitcoin.it/wiki/Promotional_graphics>

Ripple 2014, A Deep Dive for Finance Professionals, Erişim: 05.05.2019 <http://www.the-blockchain.com/docs/Ripple Protocol-Deep>

Rotman, S. 2014, Bitcoin Versus Electronic Money tarihi, 01 Ocak, The Word Bank, erişim tarihi: 15.04.2019, <https://openknowledge.worldbank.org/handle/10986/18418>

Rowlatt, J. 2013, Altın neden değerli? yayım tarihi, 9 Aralık, BBC News, erişim tarihi: 15.03.2019, <https://www.bbc.com/turkce/haberler/2013/12/131209_altin_neden_degerli>

Silk Road Nedir? Bitcoin ile Bağlantısı Nedir? 2017, Erişim: 12.05.2019, <https://www.senhesapla.com/blog/silk-road-nedir-bitcoin-ile-baglantisi-nedir/>

Şeker, E. 2007, RSA, yayım tarihi, 19 Mart, erişim tarihi, 20 Mayıs 2019, <http://bilgisayarkavramlari.sadievrenseker.com/2008/03/19/rsa/>

What is a QR Code? 2017, Erişim: 10.05.2019, <https://www.qrcode.com/en/about/>

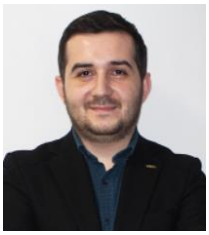
What's a QR Code? 2015, Erişim: 05.05.2019, <https://www.the-qrcode-generator.com/>

Yılmaz, D. 2018, SWIFT nedir? SWIFT kodu ve ücretleri hakkında bilmemiz gerekenler, 12 Aralık, Yurtdışı Forex, erişim tarihi: 07.07.2019, <https://www.yurtdisiforex.co/swift-nedir/>

Yumrutepe, B. 2017, Gangnam Style Youtube Sayacını Bozdu, 04 Aralık, Shift Delete, erişim tarihi: 17.05.2019, <https://shiftdelete.net/gangnam-style-youtube-sayacini-bozdu-56474>

Yücel, M. 2017, Merkle Root Merkle Kök Ağacı, yayım tarihi, 25 Aralık, Medium Medium (MM), erişim tarihi: 10.05.2019, < https://medium.com/blockchainturk/merkle-root-merkle-k%C3%B6k-a%C4%9Fac%C4%B1-5fade59dadb6>

ÖZGEÇMİŞ



Ad-Soyad **:** Onur YILMAZ

Doğum Tarihi ve Yeri: 03/02/1990 İstanbul

E-posta **:** me@onurylmz.com

ÖĞRENİM DURUMU:

- **Ön Lisans** **:** 2011, İstanbul Aydın Üniversitesi, Meslek Yüksekokulu, Bilgisayar Programcılığı (Türkçe - İ.Ö.)
- **Lisans** **:** 2014, İstanbul Arel Üniversitesi, Mühendislik ve Mimarlık Fakültesi, Bilgisayar Mühendisliği (İngilizce)

MESLEKİ DENEYİM VE ÖDÜLLER:

Yıl	**Kurum**	**Görevi**
2012-2015	İstanbul Aydın Üniversitesi	Teknik Projeler Uzmanı
2015-2018	Uluslararası Mavi Hilal Vakfı	IT Direktör ve Yazılım Uzmanı
2018-devam	Gedik Holding	Yazılım Koordinatörü

TEZDEN TÜRETİLEN YAYINLAR, SUNUMLAR VE PATENTLER:

DİĞER YAYINLAR, SUNUMLAR VE PATENTLER:

TEZDEN TÜRETİLEN YAYINLAR/SUNUMLAR