FBU-DAE 2021
1 (2) : 110-118

YENİ NESİL VERİ GÜVENLİĞİ BAĞLAMINDA DAĞITIK SİSTEMLER ÜZERİNDE BLOCKCHAIN KULLANIMI VE BITCOIN UYGULAMASI

USE OF BLOCKCHAIN ON DISTRIBUTGED SYSTEMS AND IMPLEMENTATION OF BITCOIN, IN THE CONTEXT OF DATA SECURITY

Alparslan HORASAN *, Turgut PURA **, Ferdi SÖNMEZ ***

*
Bilişim Güvenliği Teknolojisi Programı, İstanbul Gedik Üniversitesi, İstanbul / Türkiye

Programme of Information Security Technology, İstanbul Gedik University, Istanbul / Turkey

ORCID: 0000-0003-0978-2953

**
Bilişim Güvenliği Teknolojisi Programı, İstanbul Gedik Üniversitesi, İstanbul / Türkiye

Programme of Information Security Technology, İstanbul Gedik University, Istanbul / Turkey

ORCID: 0000-0002-4108-8518

***
Bilgisayar Mühendisliği Bölümü, Fenerbahçe Üniversitesi, İstanbul / Türkiye

Department of Computer Engineering, Fenerbahçe University, Istanbul / Turkey

ORCID: 0000-0002-5761-3866

ÖZET

Bitcoin, 2008 yılında ortaya çıkan elektronik kripto para birimidir. 2009 yılında ilk Bitcoin'in tasarlanmasından günümüze kadar teknolojinin ilerlemesi ve halkın yoğun ilgisi ile hızlı bir gelişme göstermiştir. Uçtan Uca (Peer-to-Peer) bir mimariye sahip olan kripto paralar, bilgisayarlar üzerinde blok zinciri (Blockchain) yapısında tutulan bir teknoloji kullanmaktadır. Bu yapı, dağıtık (distributed) ve merkezi olmayan (decentralized) bir şekilde oluşturulmuştur. Bu nedenle, yapı üzerinde, verinin korunması ve bütünlüğü, hata payı, kullanıcı güvenliği incelemeyi gerektirmektedir. Bitcoin, bu 10 yıllık zaman diliminde yoğun ilgi görmüş ve kullanıcılar tarafından yatırım aracı olarak kabul edilmiştir. Bu da gelecek yıllarda da Bitcoin'in alt yapısını oluşturan blok zincirinin birçok alanda kullanılacağını göstermektedir. Bu araştırmada, Bitcoin'in tarihçesi, nasıl üretildiği ve satın alındığı, güvenliği, Bitcoin cüzdanı (wallet) ve blok zincir kavramları incelenerek güvenlik analizi gerçekleştirmek amaçlanmıştır.

Keywords: Bitcoin, Blockchain, Bitcoin Cüzdanı

ABSTRACT

Bitcoin was first proposed in 2008 as a cryptocurrency. After the design of the first bitcoin in 2009, with the technological developments and intense public interest, it showed a fast improvement in its sector. Having a Peer–to–Peer infrastructure, cryptocurrencies use a technology named as Blockchain. This infrastructure has a distributed and decentralized nature. For this reason, protecting the data and its integrity, the margin of the error and protecting users must be investigated in detail. Bitcoin has drawn a big attention in this 10 year time period and has been used as investment tool. This also shows that being the infrastructure of bitcoin, blockchain is going to be used in many areas in the coming years. In this study, the history of bitcoin, how it is produced, bought, its security, bitcoin wallet and blockchain concepts are investigated and security analysis is conducted.

Anahtar Kelimeler: Bitcoin, Blockchain, Bitcoin Wallet

1. GİRİŞ

Bitcoin (BTC) özellikle son 10 yılda teknolojinin durdurulamayacak bir hızla gelişmesiyle birlikte ortaya çıkan elektronik bir para birimidir. Süreç, 2008 yılında Satoshi Nakamoto adlı bir kişinin kapalı bir mail grubuna 8 sayfalık bir makale göndermesiyle başlamıştır. 2009 yılına geldiğimizde ise ilk Bitcoin ortaya çıkmıştır (Ankalkoti ve Santhosh, 2017).

Bitcoin üretilmesi aşamasında Bitcoin Madenciliği kavramı ortaya çıkmıştır. Bitcoin ağındaki tüm kullanıcılara "madenci" denilmektedir (Gültekin ve Bulut, 2016). Madencilik yalnızca bitcoin elde etmek için değil aynı zamanda Blockchain özelliklerden birisi olan ve merkezi olmama özelliğine sahip (decentralized) hesap defterini de tutmaya yaramaktadır. Madenciliğin ortaya çıkmasındaki en büyük sebep sistemin tek bir merkezden kontrol edilmemesi ve dolayısıyla kontrolü bir bedel karşılığında sağlayacak kişilere ihtiyaç duyulmasıdır (Durğay ve Karaarslan, 2018).

Bitcoin madenciliği ilk zamanlar bilgisayarların işlemcileri (CPU) ile yapılabilmekteydi. Fakat sisteme dahil olan madencilerin sayısının artması ile birlikte yüksek performansa sahip bilgisayarlara ihtiyaç duyulmaya başlanmıştır (Nakamoto, 2008). Buna bağlı olarak,

bilgisayarların işlemcileri yerine 1000 kat daha hızlı çalışabilen miner cihazlar kullanılmaya başlamıştır. Çünkü ne kadar hızlı ve performansı yüksek bir cihaz kullanılırsa BTC madenciliğinin de o kadar iyi olacağı öngörülmektedir (Barber, Boyen, Shi ve Uzun, 2012). Fakat madencilik yapan kişilerin sayısının artmasıyla birlikte sadece performans yeterli olmamaya başlamıştır. Bunun sonucunda, aynı kripto paranın madenciliğini yapan kişiler bir zincire bağlanarak bir madencilik havuzu oluşturmuş ya da mevcut bir bitcoin havuzuna dahil olmuşlardır. Böylelikle, işlem gücü bağlı olduğu diğer madencilerle birleştirilmiş ve BTC üretme şansı artmıştır (Bradbury, 2013). Bitcoin'in ilgili olaylardaki tepkilerini modellemek, Bitcoin piyasalarının davranışını anlamak için büyük önem taşımaktadır (Li, Chen ve Dong, 2021).

CPU madenciliğinden sonra ekran kartı işlemcisi (GPU- Graphics Processing Unit) madenciliği başlamıştır (Jiang, Li, Lu, Hong, Guan, Xiong ve Wang, 2021). GPU'lar, CPU'lara göre daha verimli ve yüksek performanslı çalışmaktadırlar (Anish Dev, 2014). Çünkü, GPU'lar, floating point hesaplamalarında daha verimli ve BTC üretmek için gerekli olan işlemlerin, yoğun olarak bu hesaplamaları kullanmalarıdır. Bu nedenle, kullanıcılar çok geniş kapsamlı GPU madenciliği rig'leri (özel bilgisayarlar) kurmuşlardır. Rig'ler birden fazla ekran kartının bir bilgisayara bağlı ya da birden çok bilgisayarın gücünden bir havuz oluşturulmasıyla elde edilen bir yapıdır (Maurer, Nelms ve Swartz, 2013). Bu yapı 2013 yılına kadar kullanılmaya devam etmiştir. 2013 yılından sonra ASIC madenciliği (Application-Specific Integrated Circuit- Uygulamaya Özgü Tümleşik Devreler) kavramı ortaya çıkmıştır.

ASIC'ler, sadece yerine getirilmesi istenen görevi gerçekleştirmek üzere üretilmiş işlemcilerdir. ASIC, GPU'lara göre hem hızlı hem de verimlidir (Ahamad, Nair ve Varghese, 2013). Bu nedenle, 2013 yılından itibaren ASIC işlemciler kullanılmaktadır.

BTC'nin alışveriş, para transferi ya da yatırım amaçlı kullanım alanlarının olduğu gözlenmektedir. Bu bakımdan, bir ticari işletme olan bankaların en önemli amaçlarından birisi oluşturan karlılık (Sönmez, Zontul ve Bülbül, 2015) kapsamında başvurduğu veya aracı olduğu faaliyetlerden para transferi ve yatırım yönetimi işlemlerine çok önemli bir rakip olarak ön plana çıkmaktadır.

Alışveriş amaçlı kullanılan BTC için cüzdan (wallet) oluşturulması gerekmektedir. Cüzdan, kripto paraları depolayabilmek amacıyla oluşturulan sanal belleklere verilen isimdir (Hurlburt ve Bojanova, 2014). Bu kısımda her kripto paranın protokolleri ve algoritmaları farklı olmasından ötürü, her kripto para ayrı bir cüzdana sahip olacağı bilinmelidir. Tek bir cüzdan ile bütün kripto paralar kontrol edilemez. Bitcoin yatırım amaçlı kullanılacak ise cüzdan oluşturmaya gerek bulunmamaktadır. Parayı depolamak için kripto para borsaları kullanılır. Bitcoin cüzdanları 5 farklı çeşittedir (Karaarslan, 2017):

- Masaüstü Cüzdanları (Bitcoin Core, Electrum, Armory)
- Web Cüzdanları (Blockchain Wallet, Coinbase)
- Mobil Cüzdanlar (Simple Bitcoin, Electrum Mobile, Bither)
- Hardware Cüzdanlar (Legder, Trezor)
- Paper Wallet (Kağıt Cüzdan)

Bitcoin sisteminde yapılan ödemelerin doğrulanması için açık anahtarlı şifreleme (asimetrik şifreleme), noktadan-noktaya ağ bağlantısı ve proof-of-work gibi teknolojiler kullanılır (Kirbaş, 2018). Bitcoinler ödemeyi yapan adresten alıcı adrese şifrelenmiş olarak ve imzalanarak gönderilir. Her işlemin ağa duyurulumu yapılır ve blok zincirinde yerini alır. Böylece eklenen bitcoinler birden fazla kere kullanılamaz (Rotman, 2014). Bitcoin bu teknolojileri kullanarak, herkesin kullanabileceği hızlı ve son derece güvenilir bir ödeme ağı sağlamaktadır.

Güvenlik yönüyle Bitcoin'nin yapısında her yapılan işlem şifrelenmekte ve kayıt hafızasında depolanmaktadır. Bilgisayarın hacklenmesi ya da kullanıcı hatası olarak cüzdanın şifresini çaldırmak sistemin güvenlik problemi olarak görülmektedir (Krombholz, Judmayer, Gusenbauer ve Weippl, 2016).

Blockchain yapısını incelediğimizde şifreli işlemlerin takip edildiği, dağınık bir veri tabanı olarak tanımlabilir (Crosby, Pattanayak, Verma ve Kalyanaraman, 2016). Zincirleme sistem olan blockhain, blokların zincir sistemi ile bağlı olması sayesinde işlem takibi yapılabilir ve kesinlikle bu bloklar kırılamaz. Blok zincirleri, aslında dijital defterlerdir (Hepkorucu ve Genç, 2017). Bu defterin her bir birimi bir "blok" niteliğindedir ve bu bloklar, oluşturuldukları sırayı hiç bozmadan dizilirler. Yani defterdeki her bir sayfa gibidir. Bir sayfanın sırasını değiştirmek mümkün olmadığı gibi, ortak köke bağlı blok zinciri halkalarının yerini de değiştirmek mümkün değildir. Blokları düzenlemek zor olmasının yanı sıra, ağda meydana gelen herhangi bir değişikliğin de onaylanması gerekir. Bu süreç birden fazla bilgisayardan gelecek onayla gerçekleşir ve bu da güvenlik açısından önemli bir avantajdır (Hurlburt ve Bojanova, 2014). Siber güvenlik saldırılarının dikkate değer bir bölümünü oluşturan finansal dolandırıcılık, sigorta dolandırıcılığı gibi alanlardaki anormal davranışların gerçekleşmesi önünde özellikle ele alınması gereken konulardan birisi olarak da ön plana çıkmaktadır (Sonmez vd., 2018). Bununla birlikte, anormallik tespiti konusunda çeşitli çalışmalar olmasına rağmen (Signorini, Pontecorvi, Kanoun ve Pietro, 2020; Zhang, Liu, Wang ve Wan, 2020) özellikle blok zinciri tabanlı sistemleri hedefleyen saldırılara karşı önlemlerin ele alan çalışmaların artması da gereklidir.

Blockchain, birçok blok yapısının bir araya gelmesinden oluşmuştur. Her blok içerisinde, kendi blok yapısına ait veriler ve verilerin güvenliği için bir hash kodu barındırır. Ayrıca her blok ait olduğu zincirin üzerindeki bir önceki blok yapısının hash kodunu da kendi blok yapısına dahil eder (Al-Rakhami ve Al-Mashari, 2021). Böylece tüm bloklar zincir üzerinde hem kendi hash kodunu hem de bağlı olduğu bir önceki blok yapısının hash koduna sahip olmuş olur. Bunun nedeni herhangi bir blok yapısı üzerindeki verinin değiştirilmesini engellemektir. Eğer bir blok üzerinde veri değişirse, zincir üzerindeki tüm bloklar bundan etkilenecektir.

Bu çalışmada, bitcoin için blockchain temelli mimarinin çalışma yapısı incelenecektir. Sistemin güvenliği incelenecektir. Blockchain yapısı için daha önceden uygulanmış örnekler denenecek ve sistemdeki sorunlar tespit edilip yeni yaklaşımlarda bulunulacaktır.

2. HASH OLUŞUMU VE YAPISI

Blockchain'e başlamadan önce blockchain'in anahtar elemanlarını incelemek gerekmektedir. Blockchain'in temelini oluşturan SHA256 hash olarak adlandırılan yapının ne olduğu kavranmalıdır. Hash, rastgele harf ve karakterlerden oluşan bir dizidir. Diğer bir ifadeyle hash, dijital bir verinin parmak izi olarak tanımlanabilir. "E3d0eD254……" hash yapına bir örnektir. Başka bir örnekle hash yapısını incelediğimizde; "Ahmet" 'in karşılığı olarak bir hash'i oluşturduğumuzda, veri alanına bir karakter girildiğinde hash'in değiştiğini görebiliriz.

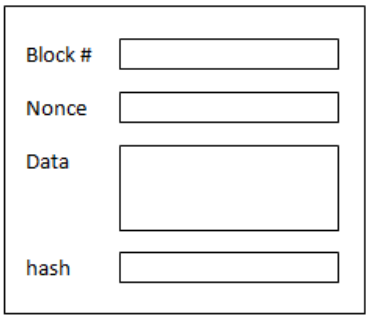
Veri	Hash
a	94c142ab…
ah	47ab87CD…
ahm	49cd98BA…
ahmet	19eab2de…

Tablo 1. Veri ve Hash

"Ahmet" hash'i "19eab2de…" olarak yapılandırılmıştır. Elimizdeki veriye bir harf eklendiğinde hash'in değiştiği görülmektedir. Eğer "Ahmet" 'i silip tekrar yazarsak "Ahmet" 'e karşılık gelen hash'in "19ea…" ile başladığını görürüz. "Ahmet"'in hash karşılığı her zaman aynı olacaktır. Bu bağlamda Ahmet'in parmak izi bu hash kodu olacaktır. Değişik veriler kullansak da üretilen hash dizisi aynı olacaktır. Verilerimizin "Ahmet, Mehmet, Ali, Veli" olduğunu düşünelim, oluşacak hash dizisindeki eleman sayısı aynı olacaktır. Bu hash dizisini önceden tahmin etmek mümkün değildir. Ancak veri aynı şekilde tekrar edildiğinde hash dizisi aynı olacaktır.

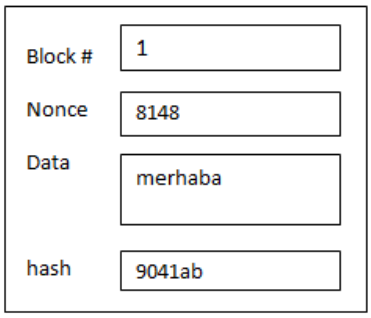
3. BLOCK YAPISINA HASH UYGULAMA

Hash dizisini block üzerinde uygulanabilmektedir. Bunun için öncelikle block yapısını kavramamız gerekmektedir.



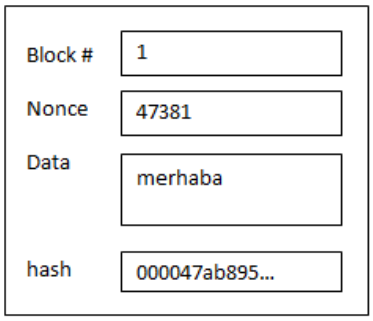
Şekil 1. Block Ekranı

Data ve hash kavramları block üzerinde 4 alana çıkmış durumdadır. Hash, bu durumda sadece data alanındaki veriyi değil tüm blocktaki verilerin dikkate alınması ile oluşturulan bir dizidir. Bu dizi "0000F57…" ile başlamaktadır. Bu 4 sıfıra bakarak block'un imzalanmış olduğunu kabul edilmektedir. Bu 3 veri alanındaki (Block #, Nonce, Data) verilerden herhangi biri değiştirildiğinde buna uygun olarak hash dizisi de değişmektedir. Data alanına herhangi bir karakter girildiğinde hash dizisinin artık "0000" ile başlamadığı görülür. Bu durumda block geçersiz hale gelir. Sonuç olarak bu block geçersiz ve imzalanmamış bir block olarak kabul edilmektedir.



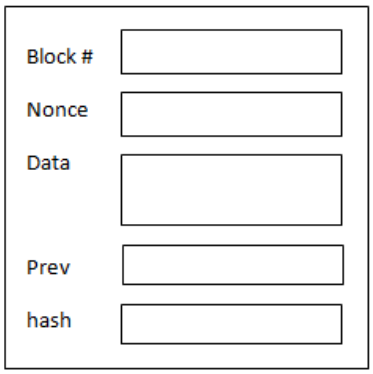
Şekil 2. Data ve Hash Ekranı

Bu işlem sırasında "Nonce" alanı devreye girer. Bu alan, hash dizisi "0000" ile başlayacak şekilde belirlenebilmektedir. Bu işlemi yapmak için Nonce alanındaki veriyi 1'den başlayarak belirleyebiliriz. 1, 2, 3, 4 ile denediğimizde hash dizisinin hiçbir zaman "0000" ile başlamadığı görülmektedir. "Nonce" alanındaki veriyi elle düzenlemek mümkün değildir. Bunu defalarca denesek bile "0000" ile başlayan bir hash dizisi üretme ihtimali çok düşüktür. Bu yüzden devreye "Mine" madencilik işlemi devreye girmektedir. Bu işlemde "None" alanındaki tüm muhtemel veriler denenerek "0000" ile başlayan bir hash dizisi oluşturulacaktır. "Mine" işlemiyle yeni bir "Nonce" kodu bulunur ve buna uygun olarak "0000" ile başlayan bir hash dizisi üretilir.



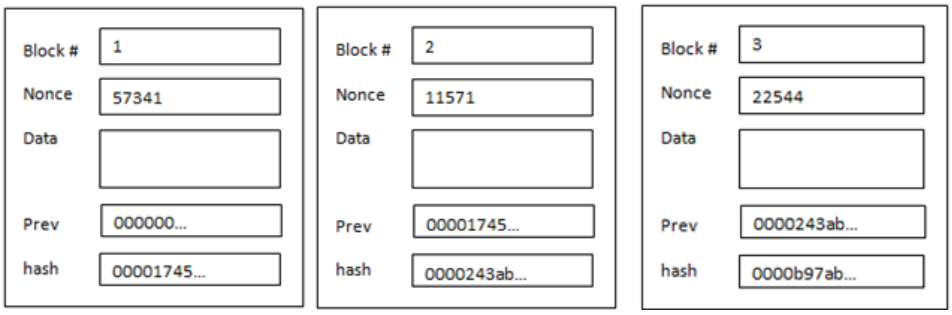
Şekil 3. Nonce Yapısı

Bu dizi "0000" ile başladığı için geçerli ve imzalanmış bir dizi durumundadır. Bir block ile ilgili işlemler tamamlanmış olur. Eğer 1'den fazla block üzerinde çalışacaksak "Block Chain – Blok Zinciri" olarak birbirine bağlanması gerekmektedir. Bu blokların birbirine bağlanması için, blocklara bir önceki (prev) alanı eklenmelidir. Bu Şekil 4'te gösterilmektedir.



Şekil 4. Prev Alanı

Prev alanındaki hash dizisi bir önceki block'un hash dizisidir. Zincirdeki her block geriye doğru bir önceki blok'u işaret eder. Bir block zinciri Şekil 5'te gösterilmiştir.



Şekil 5. Blok Zinciri

İlk block'un önceki (prev) alanında tümü sıfırlardan oluşan bir dizi olduğu görülmektedir. Bu dizi, block'un başlangıç block'u olduğunu göstermektedir.

Bu blocklar üzerinde değişiklik yapıldığında yapı değişmektedir. Bu bir örnek ile açıklandığında: 3 no'lu block'taki veriler üzerinde bir değişiklik yaptığımızda o block'un hash dizisi değişecektir. Bu durumda block geçersiz hala gelmektedir. Data alanına "Merhaba" verisi girildiğinde hash dizisi buna uygun olarak değişir.

İlk aşamada madencilik (mine) yapıldığı için hash dizisi "0000" ile başlamadığından blok geçersiz duruma gelecektir. Bu durumda "Mine" yapılarak block geçerli hale getirilebilir. Ancak 2 no'lu blokta bir değişiklik yapıldığında, 2 no'lu block'un hashini değiştirecektir. Bir sonraki yeni 3 no'lu blocktaki "Prev" alanındaki hash dizisinde de block'un bir önceki hash'i bulunduğundan 2 ve 3 no'lu blocklar geçersiz hale gelir. Block zincirinde yüzlerce block olduğunu ele aldığımızda zincirin herhangi bir yerinde, bir block üzerinde yapılacak değişiklik o blok'un ve kendinden sonra gelen blockları geçersiz hale getirir. Bir önceki blocklar bundan etkilenmeyecektir. Bu block zinciri üzerinde sadece son block üzerinde değişiklik yapıldığında diğer blocklar etkilenmeyecektir.

Zincir içindeki herhangi bir blockta yapılan değişiklik kendinden sonra gelen blockları geçersiz duruma düşürecektir. Son blockta "Mine" madencilik ile "0000" olarak başlayan geçerli bir block oluşturmak mümkündür. Bu nedenle zincirdeki son blocklar değiştirilmeye açık tehlikeli blocklardır. Ancak kendinden sonra yeni bir block eklendiğinde tehlikesiz hale gelecektir. Aradaki ya da baştaki bir block'u değiştirdiğimizde ise yine "Mine" madencilik ile o block'u geçerli hale getirmemiz mümkündür. Hash dizimiz "0000" ile başlamış olacaktır. Ancak kendinden sonra gelen block geçersiz duruma düşecektir. Bunun nedeni o block'un hash dizisinin içinde prevdeki verilerin de bulunmasıdır. Prev yani önceki block'un hash'i değişitiğinde o block'un hash'i de değişecektir. Bu durumda madencilik (mine) ile yeni hash üreterek söz konusu block'u geçerli hale getirmek mümkün olacaktır.

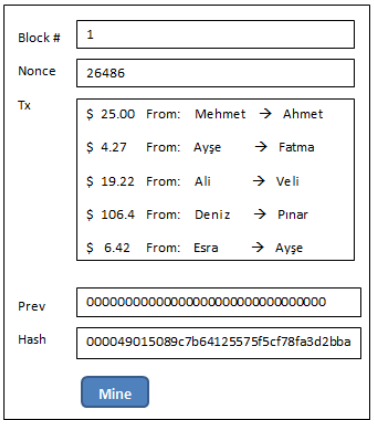
Sonuç olarak zincir içinde herhangi bir blockta en küçük bir değişiklik yapıldığında o block ve kendinden sonra gelen blocklarda madencilik yapılması ve tüm blokların geçerli hale getirilmesi gerekmektedir. Her bir madenciliğin belirli bir zaman aldığı düşünüldüğünde bu işlemin çok zaman alacağı kesindir. Eğer zincirdeki son blockta bir değişiklik yapılırsa sadece o block için madencilikle hash üretme söz konusuyken, zincirin ortasındaki bir

blockta değişiklik yapıldığında o block ve kendinden sonra gelen blocklarda madenciliğin yapılması gerekmektedir.

4. BLOCKLARI GEÇERLİ HALE GETİRMEK

Blockları geçerli hale getirmek için Dağıtık sistem devreye girmektedir. Zincirin kopyası binlerce bilgisayar üzerinde tutulmaktadır. Bir bilgisayardaki blocklar üzerinde değişiklik yapılırsa zincirin kopyası binlerce bilgisayarda bulunduğundan nasıl bir yöntemle söz konusu blocklar geçersiz kabul edileceği incelenir. Bunu denemek için 3 farklı bilgisayarda tutulan zincir kopyalarını ele alalım. Her bir bilgisayardaki hash kodlarının birbiriyle yeknesaklık göstermesi gerekmektedir. Örnek olarak 2 no'lu bilgisayardaki zincirdeki sondan ikinci blocktaki verileri değiştirip tekrar madencilik ile o block'u ve kendinden sonra gelen block geçerli hale getirilir. Bu durumda 3 bilgisayardaki tüm blocklar geçerli blocklar durumundadır. Ancak 1 ve 3 no'lu bilgisayarlardaki son blokların hashlerinin aynı olduğunu görmek mümkündür. Çünkü 1 ve 3 no'lu bilgisayarlardaki blokların üzerinde herhangi bir değişiklik yapılmamıştır. 2 no'lu bilgisayardaki son block'un hash kodu ise diğerlerinden farklı olacaktır. 1 no'lu bilgisayardaki zincirin son blockunun hash'i "00004be…" ve 3 no'lu bilgisayardaki zincirin son blockunun hash'i "00004be…" ile 2 no'lu bilgisayardaki son blockun hash'i farklıdır ("00005ca…" olabilir). İlk olarak bakıldığında tüm blokların hash'i "000…" ile başlamaktadır. Ancak bu hash diğer bilgisayarlardaki hashlerden farklıdır. Burada çoğunluğun durumu geçerli olduğu için 2 no'lu bilgisayardaki zincir geçersiz kabul edilir. Zincirler binlerce bilgisayara dağılsa da çok çabuk bir şekilde bir zincirdeki bir blockun bozulduğunu görmeleri mümkündür. Block zincirlerinde 400 – 500 bin block bulunabilir. Tamamen dağıtık bir yapıda ve bugünkü ağ teknolojisi ile bozulmuş blokların belirlenmesi çok kısa bir zaman almaktadır. Ayrıca block zincirindeki blocklarda değişiklik yapılıp yapılmadığını anlamak için tüm blockları kontrol etmeye gerek yoktur. Son block kontrol edildiğinde block zincirinde bir değişiklik yapılıp yapılmadığı anlaşılmaktadır. Eğer zincir içindeki herhangi bir blocktaki veriler değiştirildiyse son blocka bakarak bunu tespit etmek mümkündür. Bu durumda son blockun hash'i "0000" ile başlamak yerine başla karakterlerle başlayacaktır. Bu da sağlam zincirlerden farklı olacaktır.

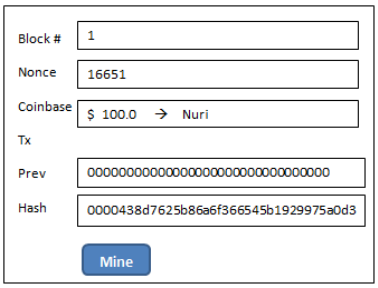
Blockchain bu işleyişi bakımından kullanışlı bir yapıda değildir. Veri alanına bazı veriler girerek hash üzerinde örneklemeler yaptık. Aslında amaç blok zincirleri üzerinden bir işlem yapmak, bir servis vermektir. Bu işlem ve servislere Token adı verilmektedir (Findikli ve Saygin, 2021).



Şekil 6. Blockchain Yapısı

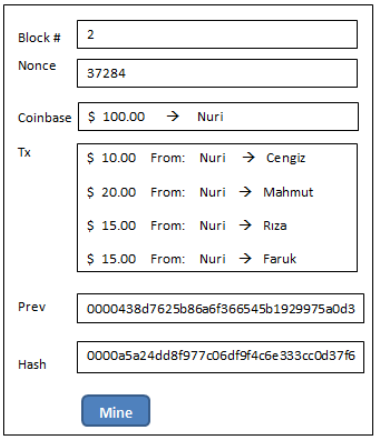
Şekil 6'daki gibi token Mehmet'ten Ahmet'e $25.00 ve Ayşe'den Fatma'ya $4.27 aktarılmıştır. Bir blocktaki işlemlere token (transaction) denmektedir. Data bölümünde tokenlar yer almaktadır. Diğer bütün kavramlar aynı şekilde devam etmektedir. 1 no'lu bilgisayarda 2.blocktaki bir tokenda bir değişiklik yapıldığında o block'un ve kendinden sonra gelen blocklarının hash'i bozulacaktır. Zincir içinde herhangi bir blockta değişiklik yapıldığında ve en son block'a bakıldığında hash'in "0000" ile başlamadığı görülecektir. Değişiklik yaptığımız block'a tekrar gidip ilk haline getirdiğimizde hash kodlarının ilk haline geldiği görülür.

Bu aşamada sadece Mehmet'in Ahmet'e 25 dolar gönderdiği belirtilmektedir. Mehmet'in 25 doları olup olmadığı ile ilgilenilmemektedir. Yani bir banka hesabı gibi düşünülmektedir. Burada Mehmet'in 25 doları olup olmadığı düşünülebilir. Bu durumda da "Coinbase" işlemleri devreye girmektedir. Şekil 7'de gösterilmektedir.



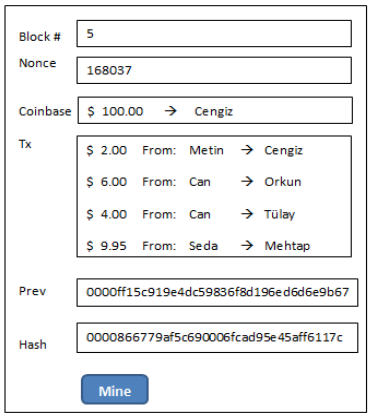
Şekil 7. Blockchain Coinbase Yapısı

Bu durumda blocklara "coinbase" alanı eklenmiş durumdadır. Bu alanı bir banka hesabı gibi düşünebiliriz. Şekilde de görüldüğü gibi Nuri'ye 100 dolar verilmektedir. Nuri'nin hesabında artık 100 dolar bulunmaktadır. İlk blockta herhangi bir işlem (transaction) söz konusu değildir.



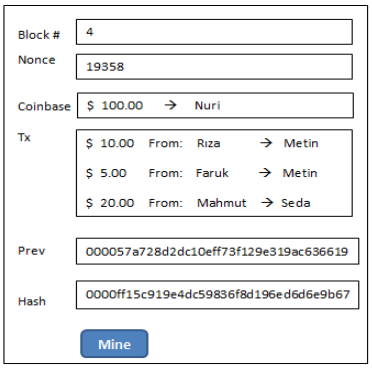
Şekil 8. Blockchain Coinbase Yapısı

Şekil 8'de görünen blockta 100 dolar daha Nuri'nin hesabına yatırılmamış olarak gözükmektedir. Bu blockta ise işlemler bulunmaktadır. Bu işlemlerin hepsi Nuri'den başka kimseye gönderilmemiştir. Nuri, Cengiz'e 10 dolar göndermiştir. Paranın olduğu ve hesabında en azından 100 dolar vardır. Bu durumda yapılacak olan para transferleri bir kişinin sahip olduğu paradan fazla olmayacaktır.



Şekil 9. Blockchain Yapısı

Şekil 9'da Metin, Cengiz'e 2 dolar göndermektedir. Burada düşünülmesi gereken nokta Metin'in 2 dolarının olup olmamasıdır.



Şekil 10. Blockchain Yapısı

Şekil 10'daki 4 no'lu blocka gidildiğinde Rıza'nın Metin'e 10 dolar gönderdiği görülmektedir. Bu durumda Rıza, Cengiz'e 2 dolar gönderebilecektir. Her blockta önceki (prev) kodunun olması bir önceki blocklara gidişi kolaylaştırmaktadır. Böylelikle paranın kaynağını takip etmeyi kolaylaştırmaktadır.

5. SONUÇ

Çalışmada incelenen temel yapı blockchain'dir. Blockchain temelli bir mimarinin çalışma yapısı incelendiğinde, bloklardan oluşan ve zincir yapısına sahip olan, şifrelenmiş işlemlerin denetlenmesine olanak sağlayan dağıtık yapıdaki bir veritabanı sistemidir. Blockchain yapısının kripto para üzerinde kullanımı söz konusudur. Uçtan Uca bir mimariye sahip olan kripto paralar, bilgisayarlar üzerinde blok zinciri yapısında tutulan bir teknoloji kullanmaktadır. Bu yapı, dağıtık (distributed) ve merkezi olmayan (decentralized) bir şekilde oluşturulmuştur. Güvenlik açısından Bitcoin'nin mimarisinde her yapılan işlem şifrelenmektedir. Bu işlemler kayıt hafızasında depolanmaktadır. Mimarinin güvenlik problemi olarak bilgisayarın hacklenmesi ya da kullanıcı hatası olarak cüzdan şifresini çaldırması olarak görülmektedir. Blok zincirleri, aslında dijital bir defter olarak tanımlanmaktadır. Bir defter sayfasının sırasını değiştirmek mümkün olmadığı gibi, ortak köke bağlı blok zinciri halkalarının yerini de değiştirmek mümkün olmamaktadır. Blokları düzenlemenin zor olmasının yanı sıra, ağda meydana gelen herhangi bir değişikliğin de onaylanması gerekmektedir. Bu süreç birden fazla bilgisayardan gelecek onayla gerçekleşmektedir ve bu da güvenlik açısından önemli bir avantaj olarak görülmektedir. Block zincirleri binlerce bilgisayarda kopyalanmış durumdadır. Bir blok veriyle dolduğunda, kalıcı bir kayıt haline gelebilmesi için, oldukça karmaşık bir işlem gerçekleştirilir. Her blok, her iki bloğun içeriğine başvuran bir kodla, bir sonraki bloğa bağlanmaktadır. Bir kopyadaki, bir block üzerindeki bir veri değiştirildiğinde, o blok ve sonraki bloklar geçersiz duruma gelmektedir. Aynı zamanda diğer kopyalarda da çelişkili duruma gelmektedir. Bu bağlamda, işlemsel (transactional) süreçler için uygun olacağı düşünülmektedir.

KAYNAKLAR

Ahamad, S., Nair, M., & Varghese, B. (2013, December). A survey on crypto currencies. In 4th International Conference on Advances in Computer Science, AETACS (pp. 42-48). Citeseer.

Al-Rakhami, M. S., & Al-Mashari, M. (2021). A Blockchain-Based Trust Model for the Internet of Things Supply Chain Management. Sensors, 21(5), 1759.

Ankalkoti, P., & Santhosh, S. G. (2017). A relative study on bitcoin mining. Imperial Journal of Interdisciplinary Research (IJIR), 3(5), 1757-1761.

Barber, S., Boyen, X., Shi, E., & Uzun, E. (2012, February). Bitter to better—how to make bitcoin a better currency. In International conference on financial cryptography and data security (pp. 399-414). Springer, Berlin, Heidelberg.

Bradbury, D. (2013). The problem with Bitcoin. Computer Fraud & Security, 2013(11), 5-8.

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. Applied Innovation, 2(6-10), 71.

Dev, J. A. (2014, May). Bitcoin mining acceleration and performance quantification. In 2014 IEEE 27th Canadian conference on electrical and computer engineering (CCECE) (pp. 1-6). IEEE.

Durğay, Z., & Karaarslan, E. (2018). Blokzinciri Teknolojisinin E-Devlet Uygulamalarında Kullanımı: Ön İnceleme. Akademik Bilişim Konferansı, Karabük.

Findikli, S., & Saygin, E. P. (2021). Müsteri Vatandaslik Baglaminda Taraftar Tokenlari. Third Sector Social Economic Review, 56(1), 57-71.

Gültekin, Y., & Bulut, Y. (2016). Bitcoin ekonomisi: Bitcoin eko-sisteminden doğan yeni sektörler ve analizi. Adnan Menderes Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 3(3), 82-92.

Hepkorucu, A., & Sevdanur, G. E. N. Ç. (2017). FİNANSAL VARLIK OLARAK BİTCOİN'İN İNCELENMESİ VE BİRİM KÖK YAPISI ÜZERİNE BİR UYGULAMA. Osmaniye Korkut Ata Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 1(2), 47-58.

Hurlburt, G. F., & Bojanova, I. (2014). Bitcoin: benefit or curse?. It Professional, 16(3), 10-15.

Jiang, S., Li, Y., Lu, Q., Hong, Y., Guan, D., Xiong, Y., & Wang, S. (2021). Policy assessments for the carbon emission flows and sustainability of Bitcoin blockchain operation in China. Nature communications, 12(1), 1-10.

Maurer, B., Nelms, T. C., & Swartz, L. (2013). "When perhaps the real problem is money itself!": the practical materiality of Bitcoin. Social semiotics, 23(2), 261-277.

Karaarslan, E. Neden Herkes Blokzinciri Teknolojisini Konuşuyor?, http://dergi.bmo.org.tr/teknoloji/nedenherkes-blok-zinciri-teknolojisini-konusuyor, 2017.

KIRBAŞ, İ. (2018). Blokzinciri teknolojisi ve yakın gelecekteki uygulama alanları. Mehmet Akif Ersoy Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 9(1), 75-82.

Krombholz, K., Judmayer, A., Gusenbauer, M., & Weippl, E. (2016, February). The other side of the coin: User experiences with bitcoin security and privacy. In International conference on financial cryptography and data security (pp. 555-580). Springer, Berlin, Heidelberg.

Li, Z., Chen, L., & Dong, H. (2021). What are bitcoin market reactions to its-related events?. International Review of Economics & Finance, 73, 1-10.

Nakamoto, S. (2019). Bitcoin: A peer-to-peer electronic cash system. Manubot.

Rotman, S. (2014). Bitcoin versus electronic money.

Signorini, M., Pontecorvi, M., Kanoun, W., & Di Pietro, R. (2020). BAD: a Blockchain Anomaly Detection solution. IEEE Access, 8, 173481-173490.

SÖNMEZ, F., ZONTUL, M., & BÜLBÜL, Ş. (2015). Mevduat bankalarının karlılığının yapay sinir ağları ile tahmini: Bir yazılım modeli tasarımı. BDDK Bankacılık ve Finansal Piyasalar Dergisi, 9(1), 9-46.

Sönmez, F., Zontul, M., Kaynar, O., & Tutar, H. (2018). Anomaly detection using data mining methods in it systems: a decision support application. Sakarya Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 22(4), 1109-1123.

Zhang, R., Zhang, G., Liu, L., Wang, C., & Wan, S. (2020). Anomaly detection in bitcoin information networks with multi-constrained meta path. Journal of Systems Architecture, 110, 101829.