YILDIZ TEKNİK ÜNİVERSİTESİ
KİMYA-METALÜRJİ FAKÜLTESİ
MATEMATİK MÜHENDİSLİĞİ BÖLÜMÜ

BİTİRME ÇALIŞMASI

BLOCKCHAIN TEKNOLOJİSİ

Tez Yöneticisi: Doç. Dr. Birol ASLANYÜREK

14052023 Aziz ÇOBAN

İstanbul, 2018

İÇİNDEKİLER Sayfa

ÖNSÖZ

Tarih boyunca bilim ve teknoloji sürekli gelişmiştir. İnsanlık her geçen yıl bir önceki neslin yaptığını geliştirmek ve ileriye gitmek için çalışmıştır. Hatta akıp giden bu zamanda sadece teknoloji ve bilim değil teknoloji ve bilimin gelişme hızı da eksponansiyel olarak artmıştır. Bunun sonucunda geçen zaman daha az olmasına rağmen bu kısa zaman içinde eskisine göre çok daha fazla yeni teknolojiler insanlığa kazandırılmıştır. Dünya bu şekilde ilerlerken özellikle ülkemiz gençlerinin üzerindeki sorumluluk günden güne artmaktadır. Karşımızda duran tüm bu gerçeklerin sonucunda özellikle son 10 yılda dünyayı kasıp kavuran, günümüzdeki teknoloji devlerinde çalışan yetkili insanların muhakkak değindiği, sadece değinmekle kalmayıp bu konu üzerinde çalışmalar yürüttükleri veya yürüteceklerini açıkladıkları "Blockchain" hakkında ülkemizde farkındalık ve kendi dilimizdeki kaynak azlığını üzülerek takip ettim. Bu sebeple, önümüzdeki süreçte dünyadaki birçok sistemin işleyişini değiştireceğine ve insanlığa yepyeni bir dünyanın kapılarını açacağına inandığım, hakkında her araştırma yaptığımda beni heyecanlandıran bu konu özelinde hem suya ufak bir taş atmak hem de duyduğum heyecanı somut bir sonuca dönüştürmek istedim.

Araştırma sürecim boyunca her zaman yanımda olan aileme, arkadaşlarıma ve günlük yaşantımızın alışmışlığı içinde kıymetini aslında çok da anlayamadığımız ve bu yüzden de etkin bir şekilde faydalanamadığımız ama bu süreçte her defasında aslında nasıl bir kıymet olduğunu anladığım "İnternet" buluşuna teşekkürlerimi bir borç bilirim.

ÖZET

Genellikle Blockchain teknolojisini açıklamak için onun ilk uygulaması olan dijital paralardan yani Bitcoin'den yola çıkılır. Buna karşın bu tanımlamanın kapsamadığı ve halen Blockchain olarak sınıflandırılan sistemler de mevcuttur. Alternatif olarak yapılan tanımlardan biri Ethereum kurucusu Vitalik Buterin'e aittir. Yaptığı tanımda:

"Blockchain, herhangi bir kişinin program yükleyebileceği, bu programların kendi kendine çalışmak üzere bırakılabileceği ve yüklenen programların anlık ve geçmiş tüm durumlarını herkesin görebileceği bir şekilde çalıştığı sihirli bir bilgisayardır. Bu bilgisayar, programların protokole uygun bir şekilde çalışmasını çok güçlü krpitografik yöntemlerle koruyarak garanti altına almıştır."

Buterin'in yaptığı bu tanım çok fazla teknik bir tanım olmamasına ve içinde Bitcoin barındırmamasına rağmen Blockchain teknolojisinin genel hatlarını güzel bir biçimde açıklamıştır. Standardizasyon alanlarını tanımlamak için ISO bünyesinde bir komite oluşturulmuştur. Bu kurum henüz resmi bir tanımlama yayınlamamıştır ancak Blockchain'i şu şekilde tanımlamıştır:

"Farklı kurumlar ve kişiler arasında paylaşılabilen, değiştirilemez bir ekonomik defterdir. Bu, işlemlerin şeffaf ve güvenli bir yol ile onaylanıp kayıt altına alındığı, aracı kurumlara duyulan ihtiyacı ortadan kaldıran ve şeffaf doğası sayesinde kendisine duyulan güveni artıran dijital bir platformdur."

Blockchain, üzerinde bulunduğu ağ boyunca dağıtık olan ve yapılan işlemlerin kaydedildiği bir defter veya vertabanıdır. Yapılan işlemlerin daha güvenli olmasını sağlamak için herhangi bir merkezi otorite liderliği altında değildir. Her işlem blok zincirine yeni bir blok eklemek için kompleks bir kriptografiyi çözen, ağ içindeki özel düğümler yani "madenciler" tarafından onaylanır. Her blok bir önceki blok içindeki bazı bilgileri barındırır. Bu yüzden tüm zincir kronolojik olarak sıralıdır ve değiştirmek neredeyse imkansızdır. Blok zinciri ağı içindeki işlemler ağ içindeki herkes tarafından görülebilir ve değiştirilemezdir. Bu tanım Blockchain'in tüm eklentilerini içinde barındıran en geniş tanımdır.

ABSTRACT

Many use Bitcoin as a starting point, explaining blockchain technology by its first application, cryptocurrency. However, there are systems that aren't captured very well by that definition, and that still are generally classified as blockchains. As for alternative definitions there is the one by Vitalik Buterin, the founder of Ethereum:

"A blockchain is a magic computer that anyone can upload programs to and leave the programs to self-execute, where the current and all previous states of every program are always publicly visible, and which carries a very strong cryptoeconomically secured guarantee that programs running on the chain will continue to execute in exactly the way that the blockchain protocol specifies."

The definition of blockchain made by Buterin is not very rigorous or technical, and is certainly not identical to Bitcoin, but manages to include many characteristics of blockchain systems. A technical committee has been formed within ISO to define areas for standardisation. They have yet to publish a formal definition but do describe blockchain as:

"*A shared, immutable ledger that can record transactions across different industries. It is a digital platform that records and verifies transactions in a transparent and secure way, removing the need for middlemen and increasing trust through its highly transparent nature."*

A blockchain is a distributed computing architecture where a computer is called a node if they are participating in the blockchain network. Every node has full knowledge of all the transactions that have occurred, information is shared. Transactions are grouped into blocks that are successively added to the distributed database. Only one block at a time can be added, and for a new block to be added it has to contain a mathematical proof that verifies that it follows in sequence from the previous block. The blocks are thus connected to each other in a chronological order. The above definition is a very wide one, encompassing almost all existing implementations of blockchains.

1. GİRİŞ

2008 küresel krizinde bankacılık ve finans sektörünü düzenleyen "merkezi" kurumlara büyük bir güvensizlik ortaya çıkmıştır. Çok ilginç bir tesadüf eseri mi yoksa özellikle mi seçilen bir zaman olduğu bilinmemekle beraber bu küresel krizde çok büyük ve güvenilen bankaların batmasından sadece birkaç ay sonra gerçek kimliği bilinmeyen, "Satoshi Nakamoto" takma adıyla bir kişi veya grup "Bitcoin: Eşten Eşe Elektronik Nakit Ödeme Sistemi" adıyla bir makale yayınladı. Blokchain, ilk olarak bu makalede Bitcoin'in tanımına uygun çalışması için gerekli olan bir teknoloji olarak karşımıza çıkmıştır. Ancak bugün biliyoruz ki Blockchain'e ait kavramsal temeller 90'lı yıllarda kaleme alınan 3 farklı makale ile atılmıştır. Bunlar;

1) Stuart Haber ve W. Scott Stornetta tarafından hazırlanan 1991 yılına ait olan ve belgelerin zaman damgası ile birlikte kripto imzalarla nasıl kullanılacağının anlatıldığı,

2) Ross Anderson tarafından hazırlanan, 1996 yılına ait olan ve kaydedilen güncellemelerin silinemeyeceği merkezi olmayan bir veri depolama sisteminin tanımlandığı,

3) Bruce Schneier ve John Kelsey tarafından hazırlanan 1998 yılına ait olan ve güvenilmeyen makineler üzerinde tutulan günlük dosyalarının içerdiği hassas bilgilerin korunması için şifrelemenin nasıl kullanılacağının açıklandığı makalelerdir.

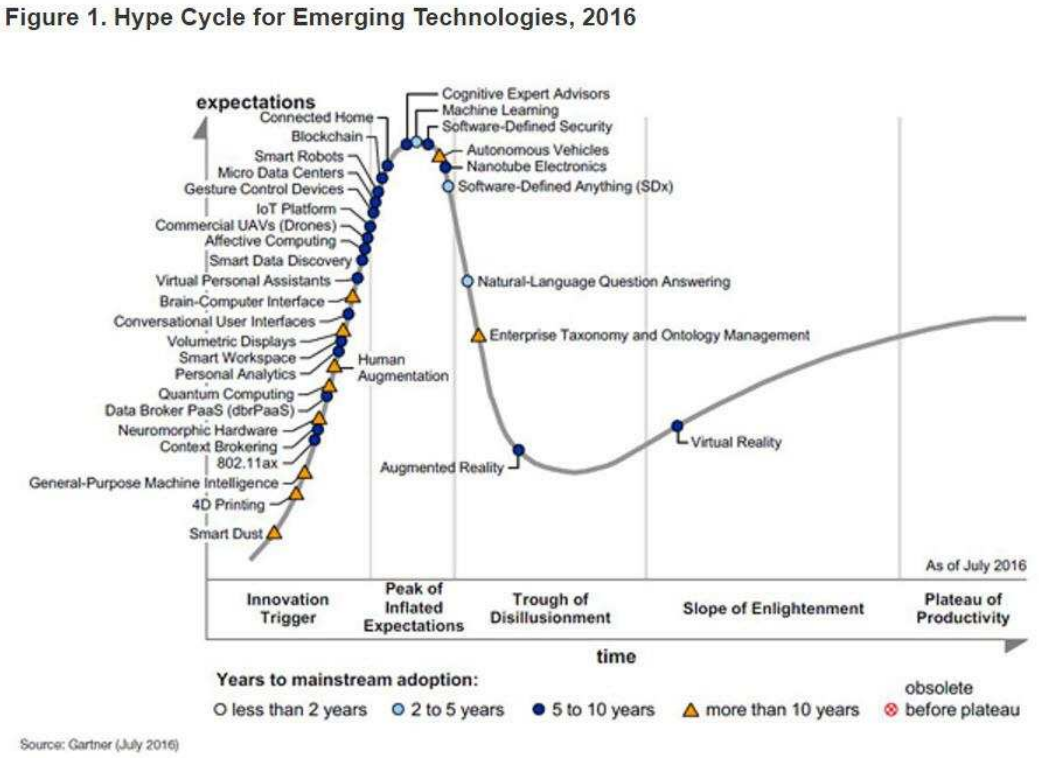
Satoshi Nakamoto, daha önce oluşturulan belli kavramları birleştirip inovasyon yaparak kendi deyimiyle "Chain of Blocks", sonradan genel olarak kabul gören ismiyle "Blockchain" teknolojisini hayatımıza katmıştır. Esas itibarı ile Blockchain, kayıtların dağıtılmış bir veritabanı, tüm yapılan işlemlerin herkese açık bir defteri veya ağa katılan tüm katılımcılar arasında çalıştırılan ve paylaşılan dijital olaylar olarak tanımlanabilir. Herkese açık olan bu defterdeki her işlem, sistem içindeki katılımcıların çoğunluğunun mutabakatı ile onaylanır. Yapılan bir veri girişi bir daha asla değiştirilemez. Blockchain, üzerinde yapılmış olan her işlemin mutlak ve onaylanmış kayıtlarını içerir.

Bitcoin, Blockchain teknolojisine bağlı olarak çalışan ilk ve en popüler örnektir. Ayrıca her hangi bir devlet kontrolü olmadan milyarlarca dolarlık bir market oluşmasına olanak tanıdığı için de hakkında en çok tartışma yürütülen üründür. Blockchain'in ilk pratik uygulaması Bitcoin olduğu için Bitcoin'e değinilmeden yapılan her tanım eksik kalacaktır. Bu yüzden Blockchain haricinde Bitcoin'in de tanımı ve nasıl çalıştığına dair teknik bilgilere devam eden kısımlarda yer verilmiştir. Bitcoin hakkındaki tartışmalara karşın Blockchainn teknolojisinin kendisi, tartışmasız ve kusursuz olarak yıllardan beri çalışmakta ve dünyadaki finansal olan ve olmayan uygulamara başarılı bir şekilde entegre edilmiştir. Geçtiğimiz yıllarda Silikon Vadisi kapitalistlerinin duayeni olarak görülen Marc Andreessen, Blockchain'in dağıtık mutabakat modelini İnternet'ten beri yapılan en önemli buluş olarak listelemiştir. BNP Pariba şirketinde güvenlik servislerinin başında sorumlu olarak bulunan Johann Palychata ise Quintessence dergisinde yazdığı yazıda, dijital paralara olanak sağlayan yazılımın yani blok zinciri teknolojisinin, buhar makinesi ve içten yanmalı motorlar gibi finans dünyasını ve daha ötesini dönüştürebilecek potansiyele sahip bir buluş olarak düşünülmesi gerektiğini söylemiştir.

Günümüz dijital ekonomi sistemi mutlak bir otoriteye duyulan güven temeli üstüne kurulmuştur. Tüm dijital işlemler bize gerçeği söylemesi için birilerine güvenmemize dayanır. Bu bazen attığımız mailin iletildiğini bize söyleyen bir mail servis

sağlayıcısı veya uzak diyarlardaki sevdiklerimize gönderdiğimiz paranın iletildiğini bize söyleyen bir banka olabilir. Örnekler çoğaltılabilir. Aslında dijital dünyadaki hayatlarımızı, djital varlıklarımızın güvenliği ve gizliliği için üçüncü şahıslara güvenerek esasında pek de güvenilir olmayan bir şekilde yaşamaktayız. Çünkü bu üçüncü kaynaklar saldırıya uğrayabilir veya manipüle edilebilir. Blockchain teknolojisinin kullanışlı olduğu nokta tam burada başlamaktadır. Geçmişte ve yaşadığımız zamanda internet üzerinden yapılan ve dijital varlık içeren her bir işlemin gelecekte herhangi bir zaman içinde, doğruluğunu onaylayabilmesine olanak tanıyan "Dağıtık Mutabakat" yapısıyla dijital dünya için bir devrim olma potansiyeline sahiptir. Üstelik bunu, işlem içindeki varlıkların ve tarafların gizliliğinden ödün vermeden yapar. "Dağıtık Mutabakat" ve "kimliksizlik" Blockchain teknolojisinin iki önemli karakteristik özelliğidir. Blockchain, dijital ticaret işlemlerimizi yönetmek için sürekli artan internet kullanımı olan ve hayatımızdaki olayları veya kişisel verilerimizi paylaştığımız dijital ekonominin gelişimi noktasında bir lokomotif olma potansiyeline sahiptir.

Aşağıda gösterilen Gartner's teknoloji artım döngüsü grafiğine göre blockchain teknolojisi üstünde en çok beklenti bulunan yeniliklerin tepe noktasındadır. (Temmuz 2016) Ayrıca ana akım tarafından kullanımı için 5 ile 10 yıl arası bir adaptasyon zamanı öngörülmüştür.



Source: Gartner (August 2016)

Şekil 1.1 *Yeni çıkan teknolojilerin Gartner's artım döngüsü*

Blockchain'e olan ilgi kuvvetlenerek artmaktadır. Bazıları tarafından değersiz bir varlık veya bir takım saçmalık olarak addedilen kriptopara bakış açısı, bugün birçok dünya

çapında şirketin hakkında araştırmalar yapıp bunun için milyonlarca dolar ödenek ayırdığı ve pratik olarak hayata geçirip kullanmak istediği bir ürün haline dönüşmüştür. Basit bir Google trend araştırması, geçtiğimiz birkaç yılda Blockchain teknolojisine olan ilginin artışını göstermektedir.

Şekil 1.2 *Blockchain için Google'da yapılan arama grafiği*

Zaman geçtikçe farklı ürünlere ait blok zinciri türleri ortaya çıksa da bu çalışmada sadece Bitcoin'e ait ve aynı zamanda en yaygın olan blok zinciri incelenmiştir. İnceleme yapılırken daha çok teknik detaylara ve matematiksel altyapıya değinilmiştir.

Bu çalışmayla Blockchain üzerine oldukça sınırlı sayıda olan Türkçe kaynak havuzuna çok küçük bir damla da olsa katkıda bulunmak ve teknik detaylarıyla beraber konuyu olabildiğince açık ve herkesin öğrenebileceği bir şekilde anlatmak amaçlanmıştır.

2. BLOCKCHAIN TEKNOLOJİSİNE GİRİŞ

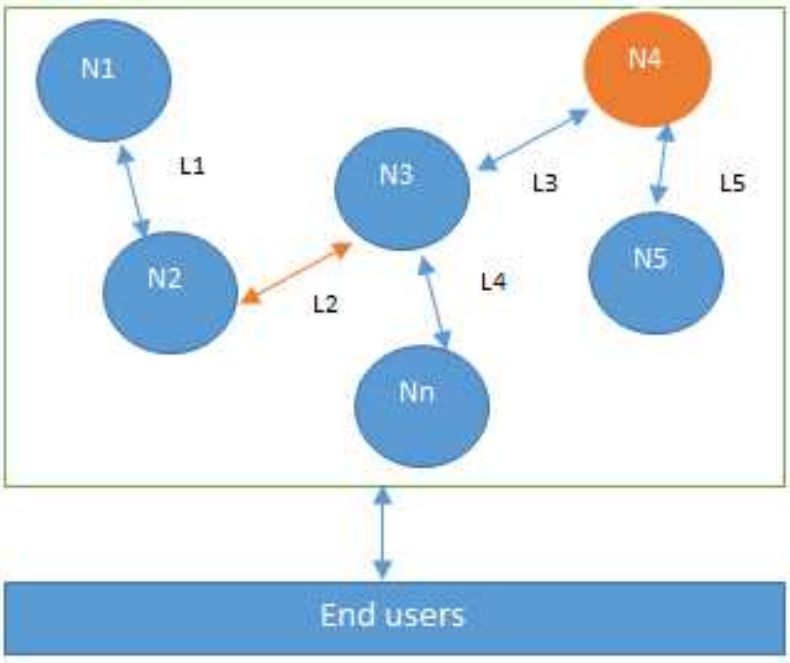
Bu bölümde Blockchain teknolojisini daha net bir şekilde kavramak için gerekli olan temel kavramların ve bazı teknik kavramların tanımlarına değinilmiştir. Ayrıca bazı blockchain tipleri de aktarılmıştır. Bu sebeple bu teknolojiyi daha önce hiç duymamış bir insan için bir giriş niteliğindedir.

2.1 Dağıtık Sistemler

Blockchain'i anlamak için dağıtık sistemler yapısını anlamak gereklidir çünkü temel olarak Blockchain teknolojisi özünde bir dağıtık sistemdir. Daha kesin tanımıyla merkeziyetsiz dağıtık sistemdir.

Dağıtık sistemler, iki veya daha fazla düğümün ortak bir neticeye ulaşmak için birbirleriyle koordineli bir şekilde çalışmasıyla oluşan programlama paradigmasıdır. Bunun yanında son kullanıcıların bunu tek bir mantıksal katman olarak görebileceği şekilde modellenmiştir.

Düğüm, dağıtık sistem içindeki bireysel oyuncular olarak tanımlanabilir. Tüm düğümler birbirlerinden mesaj almaya ve birbirlerine mesaj gönderme özelliğine sahiptir. Düğümler, dürüst, arızalı veya kötü niyetli olabilirler ve kendi hafızalarına ve işlemcilerine sahiptirler. Bir düğüm keyfi bir davranış sergileyebilir. Bunlar ayrıca "Bizans Düğümü" olarak bilinir. Bu keyfi davranış ağ işleyişine zarar veren, kasıtlı bir kötü niyet sonucunda olabilir. Ağ içinde beklenmeyen davranışlar gösteren her düğüm genellikle bizans düğümü olarak kategorize edilir. Bu terim beklenmeyen her davranışı ve kötü niyeti kapsar.



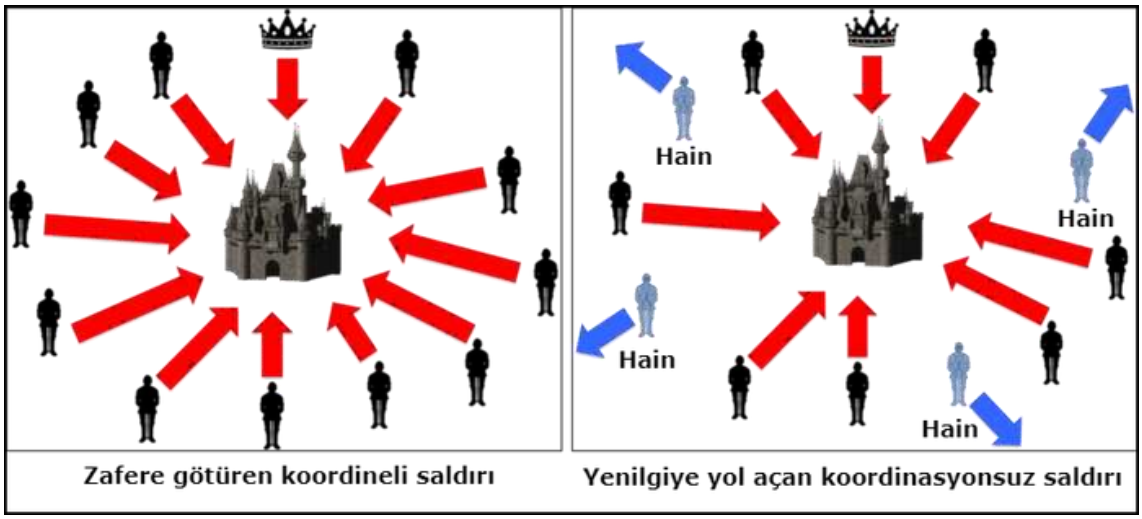
Şekil 2.1 *Dağıtık sistem modeli; N4, bizans düğümü, L2 ise kırılmış veya yavaş ağ bağlantısıdır.*

Dağıtık sistem dizaynının ana olayı düğümler arasındaki koordinasyon ve hata toleransıdır. Düğümlerden bazıları hatalı davransa veya ağ bağlantısı kopsa bile dağıtık sistem bu durumu tolere etmeli ve arzu edilen sonuca ulaşmak için hatasız şekilde çalışmaya devam etmelidir.

2.2 Bizans Generalleri Problemi

Dağıtık sistemler içindeki mutabakat mekanizmalarına değinmeden önce tarihteki olaylar, başarılı ve pratik mutabakat mekanizmalarının gelişimi için bir öncü olarak sunulabilir.

1962 Eylül ayında Paul Baran "Dağıtık İletişim Ağları Üzerine" adlı makalesiyle kriptografik imza fikrini tanıtmıştır. Ayrıca merkeziyetsiz ağlar konsepti ilk olarak bu makalede tanıtılmıştır. Daha sonra 1982'de Lamport et al. tarafından bir düşünce deneyi öne sürülmüştür. Bu deney Bizans ordusunun farklı kısımlarına liderlik eden ve bir şehre hücüm etmeyi veya geri çekilmeyi planlayan bir grup ordu generallerinden oluşur. Aralarında iletişim kurmalarının tek yolu bir ulak kullanmaktır. Komutanlar, kazanmak için aynı anda hücüm etmeye ihtiyaç duymaktadır. Bu yüzden komutanlar içinde bir hain olması halinde bile aynı anda hücüm pozisyonu almaya olanak sağlayan geçerli bir mekanizmaya ihtiyaç duyulmaktadır. Dağıtık sistemler ile benzer olarak ele alınırsa, generaller düğümler olarak, hainler kötü niyetli (Bizans) düğümleri olarak ve ulaklar ise düğümler arası iletişimi sağlayan kanallar veya bağlantılar olarak düşünülebilir.



Şekil 2.2 *Bizans Generalleri Problemi Modeli*

Bu problem 1999 yılında "Bizans Hata Toleransı" algoritmasını sunan Castro ve Lavrov tarafından çözülmüştür. Daha sonra 2009 yılında bu algoritmanın ilk pratik uygulması Bitcoin'in bir buluşu olarak "Proof of Work (PoW)" algoritması adıyla mutabakata ulaşmak için geliştirilen bir mekanizma olarak sunulmuştur.

2.3 Mutabakat

Mutabakat, aralarında güven ilişkisi bulunmayan düğümlerin verinin son hali konusunda aralarında anlaşmaya varma sürecidir. Mutabakata ulaşmak için farklı algoritma türleri kullanılabilir. İki düğüm arasında mutabakata varmak kolaydır (örneğin istemci-sunucu sistemleri) ancak dağıtık sistemlerdeki gibi birden çok düğüm katılımcı olduğunda ve bu düğümlerin tek bir değer üzerinde uzlaşması gerektiğinde bir mutabakata varmak olduka zorlaşmaktadır. Birden çok düğüm arasında mutabakata varılması konsepti dağıtık mutabakat olarak adlandırılır.

2.3.1 Mutabakat Mekanizmaları

Mutabakat mekanizması düğümlerin hepsinin veya çoğunun gerçekleştirdiği adımlardan kuruludur. 30 yıldan fazla zamandır bu konsept sektördeki bilgisayar bilimcileri ve akademiler tarafından araştırılmaktadır. Mutabakat mekanizmaları, son zamanlarda Bitcoin ve Blockchain'in doğuşu ile toplumun ilgisini çekmiştir.

Mutabakat mekanizmalarında istenen sonucu sağlamak için karşılanması gereken çeşitli gereklilikler vardır. Aşağıda bu gereklilikler kısa açıklamalarıyla verilmiştir:

- **Anlaşma:** Tüm düğümler aynı değer üzerinde uzlaşır.
- **Neticelendirme:** Tüm dürüst düğümler mutabakat sürecini sonlandırır ve eninde sonunda bir karara varır.
- **Geçerlilik:** Tüm dürüst düğümler arasında uzlaşılan veri değeri, başlangıçta en az bir dürüst düğüm tarafından sunulan değer ile aynı olmak zorundadır.
- **Hata Toleransı:** Mutabakat algoritması kusurlu veya kötü niyetl(Bizans) düğümleri varlığında dahi çalışabilmelidir.
- **Dürüstlük:** Bu, hiçbir düğümün birden fazla karar vermemesi üzerine kurulu bir gerekliliktir. Düğümler bir mutabakat döngüsünde sadece bir tek karar verir.

2.4 Blockchain'e Ait Çeşitli Teknik Tanımlar

Nereden bakıldığına bağlı olarak çeşitli Blockchain tanımları yapılabilir. Ticari olarak baktığınızda farklı, teknik olarak incelediğinizde farklı bir tanımla karşılaşılabilir. Blockchain, özünde kriptografik olarak korunan, sadece veri eklenebilen, içindeki verileri değiştirmenin neredeyse imkansız olduğu ve sadece ağ üzerindeki kişilerin mutabakatı ile güncellenebilen kişiden kişiye (peer-to-peer) dağıtık bir defterdir.

Ticari bakış açısıyla bakılırsa, kişilerin herhangi bir merkezi otoriteye güven duymadan ellerindeki değerli varlıkların ticaretini yapabildikleri bir platform olarak da tanımlanabilir. Bu, okuyucuların bir defa okumasıyla rahatlıkla anlayabileceği çok kuvvetli tsunamik bir potansiyeli olan Blockhain konseptidir.

2.4.1 Adresler

Adresler Blockchain üzerindeki işlemlerin, gönderici ve alıcısını simgeleyen emsalsiz belirteçlerdir(identifiers). Bir adres genellikle açık anahtartır. Bazı durumlarda özel anahtardan türetilebilir. Adresler aynı kullanıcı tarafından tekrar kullanabilir olmasına rağmen benzersizlerdir. Buna karşın pratikte kullanıcılar aynı adresi tekrar kullanmayıp

yeni bir adres üretirler. Bu yeni üretilen adres de diğerleri gibi benzersiz olacaktır. Bitcoin aslında takma adlı bir sistemdir. Genellikle kullanıcıların kimlikleri direkt olarak belirli değildir. Ancak bazı kimlik belirleme araştırmaları Bitcoin kullanıcılarının kimliklerinin başarılı bir şekilde belirlenebildiğini göstermiştir. Kimlik belirlemeden kaçınmak amacıyla önerilen iyi bir yöntem olarak kullanıcılar aynı adres sahibinden yapılan işlem bağlantısını göstermemek için her yapılan işlem için yeni bir adres üretirler.

2.4.2 İşlem

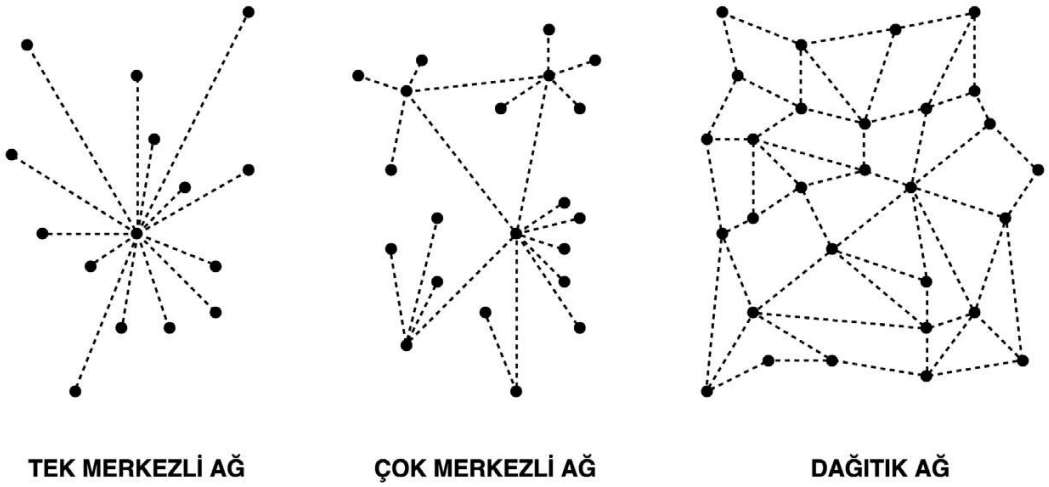
İşlem, Blockchain'in temel birimidir. İşlemler herhangi bir değerli varlığın bir adresten başka bir adrese transfer edilmesini temsil eder.

2.4.3 Blok

Bir blok birden çok işlemden ve bir önceki bloğa ait bazı bilgilerden (hash, zaman damgası, ve nonce değeri) oluşur.

2.4.4 Düğümler

Blockchain ağı içerisindeki bir düğüm aldığı role göre çeşitli fonksiyonları yerine getirir. Bir düğüm herhangi bir işlemi onaylanmak üzere ağa sunabilir ve başka bir işlemi onaylayabilir. Bunun yanında "madencilik" yaparak mutabakata yardımcı olabilir ve Blockchain ağının güvenliğini sağlayabilir. Düğümler ayrıca basit ödeme onaylaması gibi farklı işlemleri yerine getirebilir. Bunun haricinde yapılabilecek diğer fonksiyonlar tamamen düğümün ait olduğu Blockchain tipine ve ona verilen göreve bağlıdır.



Şekil 2.3 *Farklı Ağ Yapısı Tipleri*

Diyagramdaki her bir nokta bir düğümü, kesikli çizgiler ise iletişim kanallarını temsil etmektedir.

3. KRİPTOGRAFİ 101

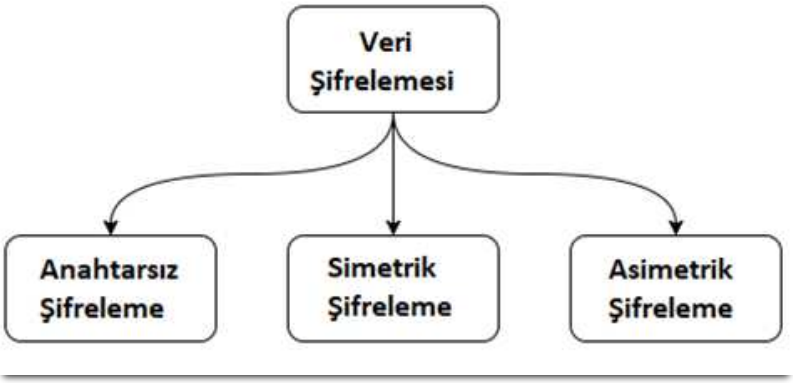
Bu kısımda kriptoloji biliminin bir alt dalı olan "kriptografi" hakkında giriş niteliğinde temel bilgiler ve Blockchain üzerinde kullanılan bazı kavramların tanımı ve nasıl çalıştkları hakkında bilgiler verilmiştir.

3.1 Kriptografiye Giriş

Kriptografi basit olarak verilerin şifrelenmesini ifade eder. Bu şifrelemeyi yaparken verilerin istenmeyen alıcıları için kullanışsız bir hale getirilmesini sağlar. Bu kapsamda verileri kullanışsız hale getirmek, üç temel aksiyonu engellemek anlamına gelir. Bu aksiyonlar, verideki bilgileri açığa çıkarmak, veriyi değiştirmek veya veriye yanlış bilgi ekleme girişimleridir. Bunlar sırasıyla gizlilik ve bütünlük problemleri olarak adlandırılır. Ek olarak, göndericinin sadece sonradan gönderenin kendisi olduğunu inkar etmek için bir veriyi şifreleyip gönderdiği bir durum farz edilebilir. "Reddedilemezlik" (non-repudiation) olarak adlandırılan, gönderilen spesifik bir verinin sonradan reddedilememe durumu kriptografinin bir diğer amacıdır. Temelinde kriptografi teorik bir kavramdır ancak hile yapmayı engellemek ve tespit etmek veya veriye ulaşımı engellemek için kullanılan geniş bir pratik kapsama sahiptir.

Veri şifrelemesi üç ana dal olarak sınıflandırılabilir;

1) Anahtarsız Şifreleme (Veri şifrelenirken herhangi bir anahtar kullanılmaz.)
2) Simetrik Şifreleme (Şifrelerken ve şifreyi çözerken tek bir anahtar kullanılır.)
3) Asimetrik Şifreleme (Şifrelerken ve şifreyi çözerken gerekli olan, birbirinden farklı olarak herkese açık (public) ve özel (private) anahtar kullanılır.)



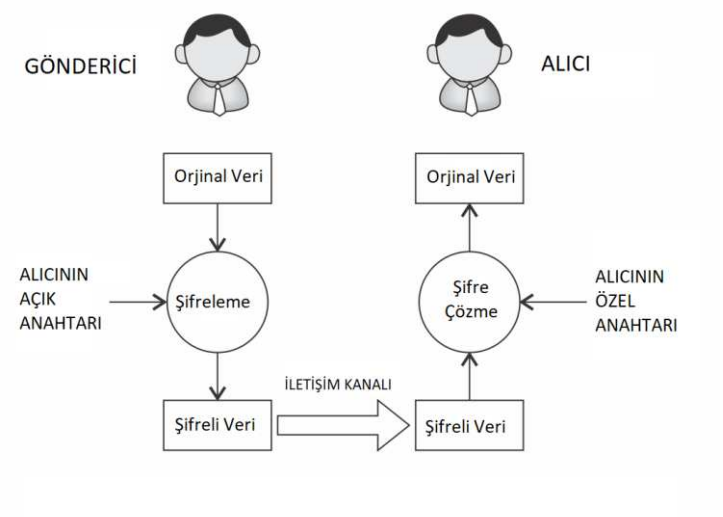
Şekil 3.1 *Veri Şifreleme Türleri*

3.2 Simetrik Şifreleme

Bir veriyi şifrelerken ve şifresini çözerken kullanılan anahtarın iki durumda aynı olduğu şifreleme türüne simetrik şifreleme denir. Bu özelliğinden dolayı paylaşımlı anahtar (shared key) şifrelemesi olarak da bilinir. Veri transferi öncesinde taraflar kendi arasında anahtarı belirlemeli veya var olan bir anahtar üstünde anlaşmalıdır. Bu sebeple gizli anahtar şifrelemesi de denmektedir.

3.3 Asimetrik Şifreleme

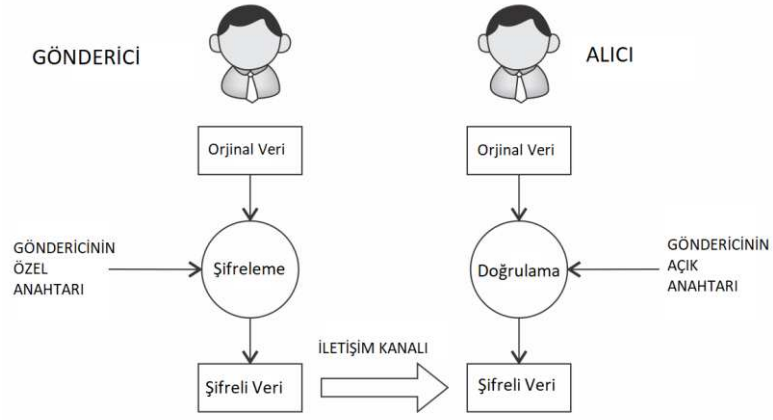
Asimetrik şifreleme, şifrelemeyi yaparken kullanılan anahtar ile şifrelemeyi çözerken kullanılan anahtarın birbirinden farklı olması esasına dayanır. "Özel Anahtar Şifrelemesi" olarak da bilinen bu teknikte, şifreleme ve şifre çözme işlemleri için sırasıyla bir açık ve bir özel anahtar kullanılır.



Şekil 3.2 *Açık/Özel Anahtar Kullanarak Şifreleme Ve Şifre Çözme*

Üstteki diyagram bir göndericinin verisini gönderici kişinin yani alıcının açık anahtarı ile şifreleyip kullandıkları ağ boyunca transfer ettikten sonra alıcının kendi özel anahtarı ile nasıl şifreyi çözüp veriyi okuduğunun açıklamaktadır. Bu şekilde özel anahtar alıcı tarafında saklı kalır ve şifreleme yapmak veya şifre çözmek için herhangi bir anahtar paylaşma gereği duyulmamaktadır.

Alt tarafta yer alan bir başka diyagram ise gelen bir mesajın alıcı tarafından doğruluğunun ve bütünlüğünün kanıtlanması için özel anahtar şifrelemesinin ne şekilde kullanılabildiğini göstermektedir. Bu modelde gönderici kendine ait özel anahtar ile veriyi imzalar ve kullanılan ağ boyunca bu veriyi alıcıya ulaştırır. Mesaj alıcı tarafına ulaştığında göndericinin açık anahtarı ile verinin doğruluğu ve bütünlüğü kanıtlanabilir. Bu modelde herhangi bir şifre çözme işlemi yapılmamıştır. Bu teknik yalnızca verinin kimliğini doğrulama ve verinin doğruluğunu kanıtlamak için kullanılır.



Şekil 3.3 *Açık/Özel Anahtar Kullanarak İmzalama Ve Doğrulama*

3.3 Açık(Public) ve Özel (Private) Anahtarlar

Açık anahtar kriptografisini anlamak için incelenmesi gereken ilk konsept açık ve özel anahtar kavramlarıdır.

Özel anahtar, adından da anlaşılacağı gibi temel olarak kullanıcılar tarafından gizli ve özel tutulan, rastgele üretilmiş karakter dizileridir. Özel anahtarların korunması gerekir ve hiçbir şekilde anahtara ulaşım izni verilmemelidir. Aksi taktirde bu anahtarlar mesajların şifresini çözmek için kullanıldığından tüm açık anahtar kriptografisi riske girmiş olur. Özel anahtarlar kullanılan algoritmaya bağlı olarak farklı uzunluklarda olabilirler.

Açık anahtar herkes tarafından görülebilen ve özel anahtar sahibi tarafından sunulan anahtar türüdür. Açık anahtar sahibine şifrelenmiş bir mesaj göndermek isteyen herkes, alıcı tarafından sunulan açık anahtarı kullanarak mesajını şifreleyip özel anahtar sahibine gönderebilir. Hiç kimse gönderilen mesajın şifresini çözemez çünkü açık anahtara karşılık gelen özel anahtar, gönderilmek istenen alıcıda gizli bir şekilde tutulmaktadır. Açık anahtar ile şifrelenmiş mesaj karşı tarafa ulaştığında alıcı kendinde bulunan özel anahtar ile bu mesajın şifresini çözebilir. Bunun yanında açık anahtarı sunan kişinin doğruluğunun kanıtlanması noktasında birkaç endişe de mevcuttur.

3.5 Özet(Hash) Fonksiyonları

Özet fonksiyonları, gelişigüzel uzunluktaki metinlerden sabit uzunlukta çıktılar üretmek için kullanılır. Özet fonksiyonları anahtarsız olarak çalışır ve veri bütünlüğünü sağlar. Algoritmalarına göre değişkenlik gösteren farklı özet fonksiyonu aileleri mevuttur. (MD, SHA1, SHA-256, SHA-3, vb.) Özet fonksiyonlarının ortak kullanım alanı dijital imzalama ve mesaj doğruluğunun kanıtlanma ihtiyacı doğduğu durumlardır. Özet fonksiyonlarının 3 adet güvenlik özelliği vardır. Bunlar;

1) Ön görüntü direnci
2) İkinci ön görüntü direnci
3) Çakışma direnci

olarak adlandırılır.

Özet fonksiyonkları uzun veya kısa farketmeksizin her uzunluktaki metni alır ve sabit uzunlukta sıkıştırılmış bir çıktı üretebilir. Çıktılar, 128-bit ve 512-bit olarak farklı boyutta çıktı üretebilir. Bu fonksiyonluk oldukça verimli ve hızlı tek yönlü çalışmaktadır. Mesaj boyutundan bağımsız olarak çok çabuk bir şekilde çıktı üretebilirler. Mesaj fazlasıyla büyük bir boyutta olduğunda verimlilik azalabilir ancak bu durumda dahi özet fonksiyonları, pratik kullanım için yeterli hıza sahiptir.

3.5.1 Ön Görüntü Direnci

$h(x) = y$ olarak bir fonksiyon ele alalım. Burada h, özet (hash) fonksiyonunu, x, girdiyi ve y ise oluşan özet çıktıyı temsil etmektedir. Birinci güvenlik özelliği y'nin kesinlikle ters işleme sokulamayacağını söylemektedir. Burada x, y'nin ön görüntüsü olarak tanımlandığından bu özellik "Ön Görüntü Direnci" adını almıştır. Tek yönlülük özelliği olarak tanımlanan kaynaklar da mevcuttur.

3.5.2 İkinci Ön Görüntü Direnci

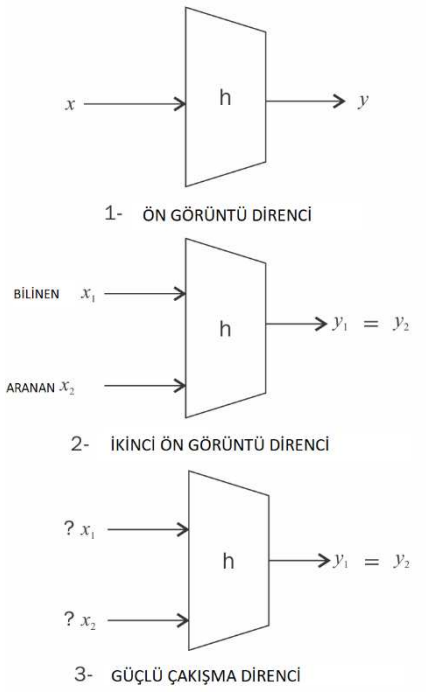
İkinci ön görüntü direnci özelliğine göre verilen *x* ve *h(x)* elemanları özelinde, başka bir mesaj *m* olarak tanımlanırsa $m \neq x$ olacak şekilde ve $h(m) = h(x)$ durumunu sağlayan bir *m* bulmak neredeyse imkansızdır. Bu özellik ayrıca zayıf çakışma direnci olarak da adlandırılır.

3.5.3 Çakışma Direnci

Çakışma direnci özelliği farklı iki mesaj girdisinin aynı özet çıktısı vermemesi gerektiğini söyler ($h(x) \neq h(z)$). Bu özellik ayrıca güçlü çakışma direnci olarak adlandırılır.

Özet fonksiyonları tanımları gereğince her zaman bazı çakışmalar barındıracaktır. Başka bir ifadeyle, iki farklı mesajın özet çıktısı aynı olabilir ancak matematiksel olarak bu çakışmaların bulunması neredeyse mümkün değildir. Tüm özet fonskiyonlarında arzu edilen konsept "Çığ Etkisi" konseptidir. Çığ etkisi, mesaj içindeki küçük bir değişikliğin -girdi içindeki tek bir harf bile olabilir- komple tüm özet çıktısının değişmesi olarak belirtilir.

Özet fonksiyonları genellikle yinelemeli bir yaklaşımla dizayn edilir. Bu methoda göre sıkışmış çıktıyı üretmek için girdi olarak gelen mesaj birçok defa bloklama (block-by-block) ilkesine göre sıkıştırılır. Yinelemeli özet fonksiyonların popüler tipi Merkle-Damgard yapısıdır. Bu yapı, gelen verinin eşit büyüklükteki bloklara bölünmesini ve daha sonra sıkıştırma fonksiyonları yardımıyla bu blokların yinelemeli bir tutumla doldurulması fikrine dayanır. Bloklar her seferinde metin boyutunun yarısına gelecek şekilde oluşturulur ve özet çıktı elde edilir.



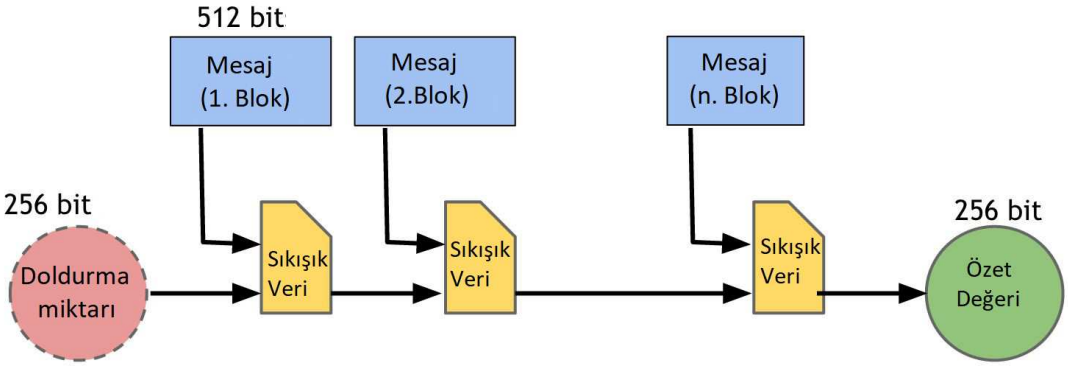
Şekil 3.4 *Özet Fonksiyonlarının 3 Adet Güvenlik Özelliği*

3.5.4 SHA-256 Güvenli Özetleme Algoritması (Secure Hash Algorithms)

Daha önce özet fonksiyonlarının birçok tipi olduğu belirtilmiştir. Çalışma kapsamında Bitcoin Blockchain'inde kullanılan özet fonksiyonu yani SHA-256 algoritması hakkında bilgiler verilmiştir.

Öncelikle özet fonksiyonlarda keyfi uzunluktaki girdilerle çalışıldığı tekrar hatırlanmalıdır. Her boyutta girdi fonksiyona sokulabilir. Bununla birlikte sabit uzunluktaki girdilerle çalışan bir özet fonksiyonu oluştuabildiğimiz sürece bu fonksiyonu rastgele uzunluktaki girişler için de çalışabilen bir fonksiyona dönüştürmek için genel bir yöntem mevcuttur. Bu yönteme **Merkle-Damgard transformasyonu** denmektedir. SHA-256 bu yöntemi kullanan en popüler özet fonksiyonlarından biridir. Ortak terminolojide sabit uzunlukla çalışan ve çakışma direnci özelliğini barındıran fonksiyonlara "sıkıştırma fonksiyonu (compression function)" denir.

Aşağıdaki diyagramda 768-bit mesaj girdisi olan bir SHA-256 fonksiyonunun 512-bit büyüklükteki bloklar ile 256-bit büyüklüğünde bir özet değeri üretmek için sıkıştırma fonksiyonunu kullanım şekli gösterilmiştir.



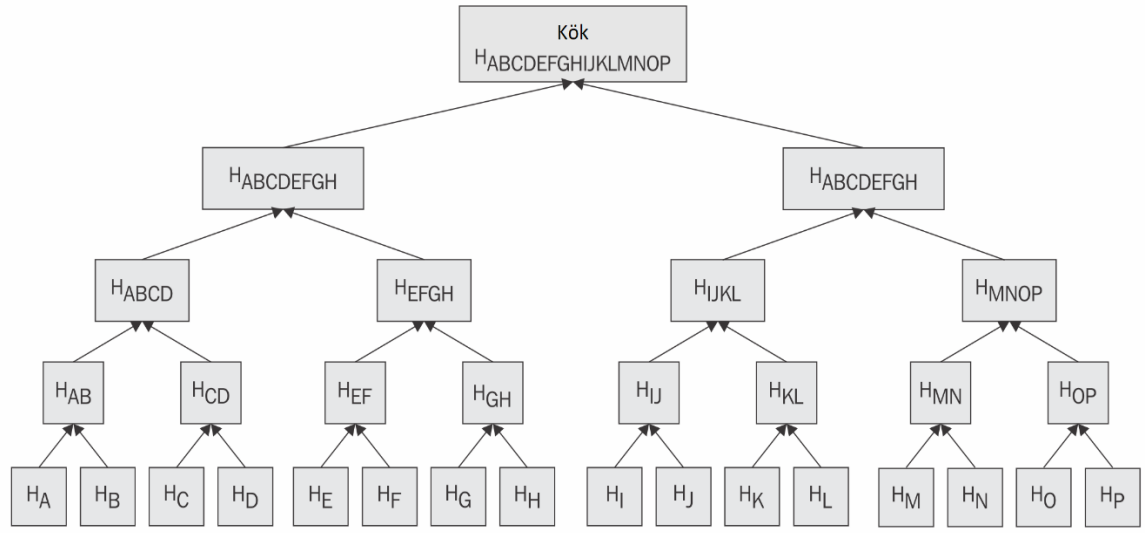
Şekil 3.5 *SHA-256'nın Sıkıştırma Prensibi*

SHA-256 sabit uzunluklu çakışma direnci özelliğine sahip bir sıkıştırma fonksiyonunu rastgele uzunluklu girişleri kabul eden bir özet fonksiyonuna dönüştürmek için Merkle-Damgard dönüşümünü kullanır. Girdilerin 512-bit'in bir katı olması için boşlukları doldurulur. Örneğin bir veri 768-bit büyüklüğünde ise başlangıçta 256-bit ile doldurulup çıktı olarak 256-bit çıktı elde edilir. Algoritma sonuçları sabit uzunlukta olduğundan teorik olrak farklı veriler için çıktıların çakışması mümkün gözükebilir. SHA-256 algoritması kapsamında çıktı kümesinin içinde 2^{256} farklı değer olabilir. Bu ise yaklaşık olarak 10^{77} sayısına tekabül etmektedir. Görünür evrendedeki atom sayısının 10^{80} civarında olduğu düşünüldüğünde 2^{256} sayısının büyüklüğü hakkında fikir vermektedir. Bu sebeple bu ihtimalin gerçekleşmesi oldukça zor olacaktır.

3.6 Merkle Ağaç Yapıları

Merkle ağaç yapısı *Ralph Merkle* tarafından tanıtılmıştır. Merkle ağaçları büyük verilerin güvenliğini ve doğruluğunu verimli bir şekilde onaylanmasını sağlamaktadır. Bu yapıda ikili (binary) bir ağaç yapısı oluşturulup en alt seviyeye veri içindeki parçalar yerleştirilir. Daha sonra en alt seviyeden yukarı doğru tek bir kök değer elde etmek için bu parçaların

özet değerleri alınır. Tek bir özet değere ulaşılana kadar bu işleme devam edilir. Bu değere "Merkle Kök Değeri" adı verilir.



Şekil 3.6 *Merkle Ağaç Yapısı*

3.7 Dijital İmzalama

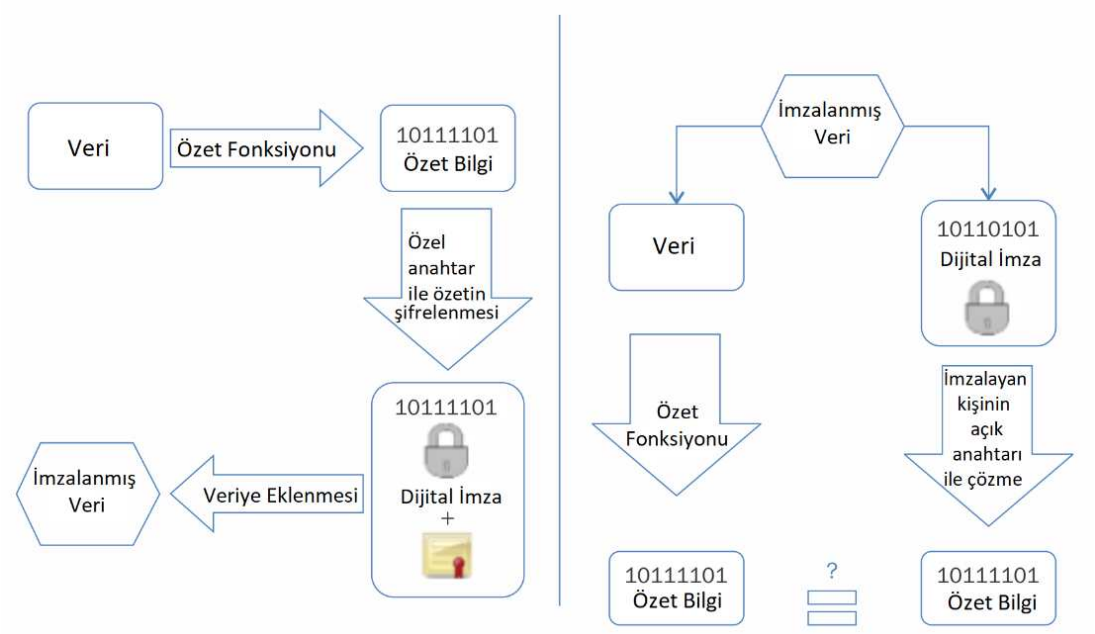
Kriptografide veri doğruluğunu onaylamak ve reddedilemezliği sağlamak için dijital imzalama yöntemi kullanılır. Başka bir ifadeyle belirli bir kişinin veya makinenin gönderdiği mesajın gönderen kişiye özel olduğunu teminat altına almak için dijital bir imza gereklidir. Bu yaklaşım, eski zamanlarda gönderilen mektupların gönderen kişiye özel bir mühür ile damgalanmasına veya kendi elleriyle imzalamasına benzetilebilir. Dijital imzalama, el yazması mektuplara kıyasla muhtemeken daha fazla bir şekilde veriye kesinlik katan ve gönderenin kimliğini doğru biçimde belirleyen bir dijital imzalama methodudur. Resmi olarak bu method mesajın gönderildiğini kanıtlar, gönderen kişinin sonradan gönderdiğini inkar edememesini ve gönderenin kimliğini garanti altına alır. Bu işlem aşağıda belirtilen adımlardan oluşur:

- Gönderici bir özetleme algoritması (SHA-256) kullanarak mesajın özet değerini oluşturur. Bu adım, alıcı tarafında verinin değiştirilmediğinin ispatlanmasını sağladığı için önemlidir.
- Oluşturulan bu özet değer göndericiye ait olan özel anahtar ile imzalanır. Burada özel anahtar sadece imzalayan tarafta olduğundan imzanın ve imzalanan verinin doğruluğu kanıtlanmış olur.
- Gönderici mesajıyla birlikte hazırladığı imzasını karşı tarafa gönderir.
- Alıcı mesajı aldığında kendisi de mesajın bir özet değerini oluşturur.
- Mesaja gönderici tarafından eklenen imzalı özet bilgiyi göndericinin açık anahtarı ile çözümler.
- Alıcı, kendi oluşturduğu özet bilgi ile karşı tarafın açık anahtarı ile çözümlediği özet bilgiyi karşılaştırır.
- Eğer iki özel bilgi tamamen birbirleri ile aynıysa gönderen kişi doğrudur ve gönderdiği bilgi değiştirilmemiştir.

Dijital imzaların ayrıca üç önemli özelliği vardır:

1) Dijital imzaların gerçekliği alıcı taraf tarafından doğrulanabilir.
2) Özel anahtar kullanarak imzalama işlevini yalnızca mesajın göndericisi yerine getirebilir. Başka bir ifade ile legal gönderici tarafından üretilen imzalanmış mesajı o kişiden başka hiçkimse üretemez.
3) Dijital imza bir mesajdan ayrılamaz ve başka mesajlar için kullanılamaz.

Daha iyi anlaşılması açısından dijital imzalama operasyonun aşamaları diyagramda gösterilmiştir.



Dijital İmzalama (Solda) ve Onaylama Süreci (Sağda)

4. BLOCKCHAIN: NASIL ÇALIŞIR?

Çalışmanın bu bölümünde Bitcoin protokolü teknik detayları ile tanıtılmış ve Blockchain sisteminin yapıtaşları tek tek incelenip teknik olarak nasıl çalıştıkları belirtilmiştir.

4.1 Bitcoin: Eşten Eşe Elektronik Para Sistemi

Blokchain teknolojisi, kimliği bilinmeyen ve Satoshi Nakamoto adını kullanan bir kişi veya grup tarafından 2008 yılında yayınlanan "Bitcoin: Eşten Eşe Elektronik Para Sistemi" isimli makalede tanıtılan Bitcoin isimli dijital para ile ayrılamaz bir biçimde bağlıdır. Bu makalede Nakamoto, on yıllardır üzerinde çalışılan Merkle Ağaçları, Hash Fonksiyonları, Açık Anahtar Şifrelemesi ve Dijital İmzalar gibi kavramları, herhangi bir aracı kuruma güvenmeyi gerektirmeden dijital varlıkların transfer edilmesine olanak tanıyan ve bugün dijital paralar olarak bilinen eşten eşe ödeme sisteminin taslağını oluşturmak için bir araya getirip harmanlamıştır. Bu kriptografik bileşenlerin oluşturduğu alaşım daha sonraları bilinen şekliyle Blockchain teknolojisidir.

Bitcoin'in ele aldığı en önemli konu, çift harcama yani bir paranın birden çok defa harcanması probleminin pratik bir çözümü ile birlikte sunduğu mükemmel Bizans Generalleri Problemi çözümüdür. Normal olarak bu problem bankalar veya güvenilen üçüncü parti aracı kurumlar tarafından çözülmüştür fakat Nakamoto, tüm işlemlerin veritabanında kronojik olarak gösterildiğini garanti altına alan zaman damgalı bir sunucu(server) fikrini ortaya atmıştır. Ayrıca yazar hangi zincirin doğru zincir olduğunu belirlemek üzere bir mutabakat mekanizması kurmak için İş Kanıtı (Proof-of-Work) algoritmasını önermiştir. Bu algoritma, kullanıcıların işlemleri onaylama noktasında dürüst olmalarını teşvik eden bir sistem meydana getirmiştir. Temel olarak bu sistem, sahte bir işlem yapmanın bedelini potansiyel kazanç için harcanan bedelden daha pahalı hale getirmiştir. Blockchain üzerinde uygun bir mutabakat sistemi olmasaydı blockchain sistemine bir güven olmazdı ve herhangi bir kullanıcı sistemdeki tüm işlem kayıtlarına erişebildiğinden bu kayıt geçmişini istediği gibi değiştirip geçerli olan zincir olarak yayınlayabilirdi.

4.2 İşlemler

İşlemler Blockchain ekosisteminin çekirdeğinde yer alır. İşlemler bir adresten diğerine birkaç adet bitcoin göndermek kadar basit veya işlemin gerektirdiği şartlara bağlı olarak oldukça kompleks bir yapıya sahip olabilirler. Her işlem en bir adet girdi ve bir adet çıktıdan oluşur. İşlemin girdileri, daha önceki başka işlemlerin çıktılarıdır. Başka bir deyişle, bir işlemdeki girdiler, daha önceki işlemlerin henüz harcanmamış olan çıktılarıdır. Eğer bir işlem yeni bir para yaratan işlemse herhangi bir girdi olmaz ve bu yüzden herhangi bir dijital imzaya gerek yoktur. Eğer bir işlem başka bir kullanıcı adresine bitcoin gönderiyorsa, göndericinin özel anahtarı ile imzalanmasına ve gönderilen dijital paranın kaynağını göstermek için bir önceki işlemin referans olarak gösterilmesi gerekmektedir. Aslında paralar Satoshi olarak temsil edilen, harcanmayan işlem çıktılarıdır. (0.00000001 BTC = 1 Satoshi)

Bir işlemin yaşam döngüsü aşağıdaki adımlardan oluşur:

1) Bir kullanıcı cüzdan yazılımı veya başka bir arayüz olarak işlem gönderir.
2) Cüzdan yazılımı göndericinin özel anahtarı ile işlemi imzalar.

3) İşlem Bitcoin ağı boyunca yayınlanır.
4) Madenci düğümler bir sonraki eklenecek bloğa bu işlemi ekler.
5) Madencilik işlemi başlar ve bir madenci İş kanıtı(PoW) problemini çözdüğünü ve yeni bir blok eklediğini ağ boyunca duyurana dek devam eder.
6) Diğer düğümler bu bloğu onaylar ve bloğu tüm ağa yayarlar. Ayrıca işlemi sağlamak amacıyla onaylama işlemi başlar.
7) Son olarak onaylama işlemleri alıcının cüzdanında belirir ve daha sonra yaklaşık olarak 6 onaydan sonra işlem bitmiş kabul edilir ve onaylanır. 6 onay sayısı önerilen adet olmasına karşın tek bir onaydan sonra dahi işlem bitmiş kabul edilebilir. Beklemenin arkasındaki kilit fikir çift harcama olasılığını fiilen elemiş olmaktır.

4.2.1 Temel Para İşlemleri (Coinbase Transactions)

Temel para işlemi, her zaman madenciler tarafından yapılan ve bir bloktaki ilk işleme verilen isimdir. Yeni paralar üretmek için kullanılır. Bu işlem türü içinde temel para işleminin girdisi olarak davranan, *coinbase* olarak adlandırılan özel bir alan mevcuttur. Ayrıca bu işlemler 100-byte büyüklüğe kadar keyfi bir veri tutup saklayabilme özelliğine sahiptir. Örneğin Blokchain üzerindeki başlangıç bloğunda Times gazetesinden alınan çok meşhur bir yorum satırı bulunmaktadır:

"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"

("Başbakan, bankalar için ikinci kurtarma paketinin eşiğinde.")

Bu mesaj başlangıç bloğunun 3 Ocak 2009 tarihinden önce eklenmediğinin kanıtıdır.

4.2.2 İşlem Komisyonu Ve İşlemlerin Onaylanması

Işlem komisyonları madenciler tarafından tahsil edilir. Komisyon miktarı yapılmak istenen işlemin boyutuna bağlı olarak değişkenlik gösterir. İşlem komisyonları girdilerin toplamı ve çıktıların toplamı arasındaki fark ile hesaplanır. Komisyonlar madencileri işlemleri onaylama ve yeni bloklar oluşturmaya teşvik etmek için kullanılır. Tüm işlemler hafıza havuzu (memory pool) adı verilen yerde son bulur. Burada madenciler, işlemleri öncelik sıralarına göre önerilen yeni bloğa eklerler. Örneğin öncelik konusuna komisyon açısından bakıldığında, yüksek komisyonlu işlemler madenciler için her zaman daha önceliklidir. Komisyonlar işlem tiplerine göre değişkenlik gösterebilir. Bunun için gönderim işlemleri ve bloğa katılma işlemleri gibi farklı işlem tipleri için farklı komisyon miktarları ödenir. Bitcoin protokolünde komisyonlar sabitlenmemiştir ve zorunlu değildir. Komisyonsuz işlemler dahi zamana geldiğinde onay işlemine sokulabilir ancak bu çok fazla zaman alacaktır. Çıktıların değerlerinin toplamı, girdilerin değerlerinin toplamında büyükse işlem reddedilir.

Bitcoin ağı uçtan uca bir ağdır. Her Bitcoin ucu işleme başladığında birkaç başka uçla iletişime başlar. Uçlar arasında bir üstünlük yoktur. Bitcoin işlemleri ve bloklar birbirleri arasında paylaşılır. Yeni bir işlem doğrulandığında her uç bunu bağlı olduğu uçlara gönderir. Bu şekilde onaylanan bir işlem 3-4 saniye içinde tüm uçlara ulaşmış olur. Uçlar bu işlemleri ve blokları alır almaz kendileri de doğrularlar. Bu şekilde ağa yapılacak olan potansiyel bir saldırı geçersiz sayılmış olur.

Bir işlemin çıktısı başka bir işlemin girdisi olabildiğinden, işlemler birbirine dede-baba-torun ilişkisi içinde bağlıdır. Ancak Bitcoin ağı herhangi bir kısıtlama olmayan bir ağ olduğundan bazı durumlarda el alt işlem (torun) diğerlerinden önce sistem

tarafından onaylanabilir. Bu durumda işlemlerin bağlı olduğu ilk işlem (dede) onaylanana kadar diğer işlemler bekletilir. Sistemin şişmesinin önüne geçebilmek için bekletilecek işlem sayısı sınırlıdır.

4.3 Bir Bloğun Yapısı

Daha önceki bölümlerde de bahsedildiği gibi Blockchain yapısı birbirleri ile ilişkili bloklardan oluşan bir zincir gibi düşünülebilir. Bu zincir kronolojik şekilde dizilmiştir. Her blok içindeki işlemlere ve kayıt bilgilerine ait bazı önemli bilgiler barındırır. Bir bloğun yapısı aşağıdaki gibidir.

Bayt	**Eleman İsmi**	**Açıklaması**
80	Blok başlığı	Bu kısım blok başlığı içindeki bilgileri tutar.
Değişken	İşlem sayıcı	Bu kısım blok içindeki işlemlerin sayısını tutar.
Değişken	İşlemler	Blok içindeki tüm işlemler bu alandadır.

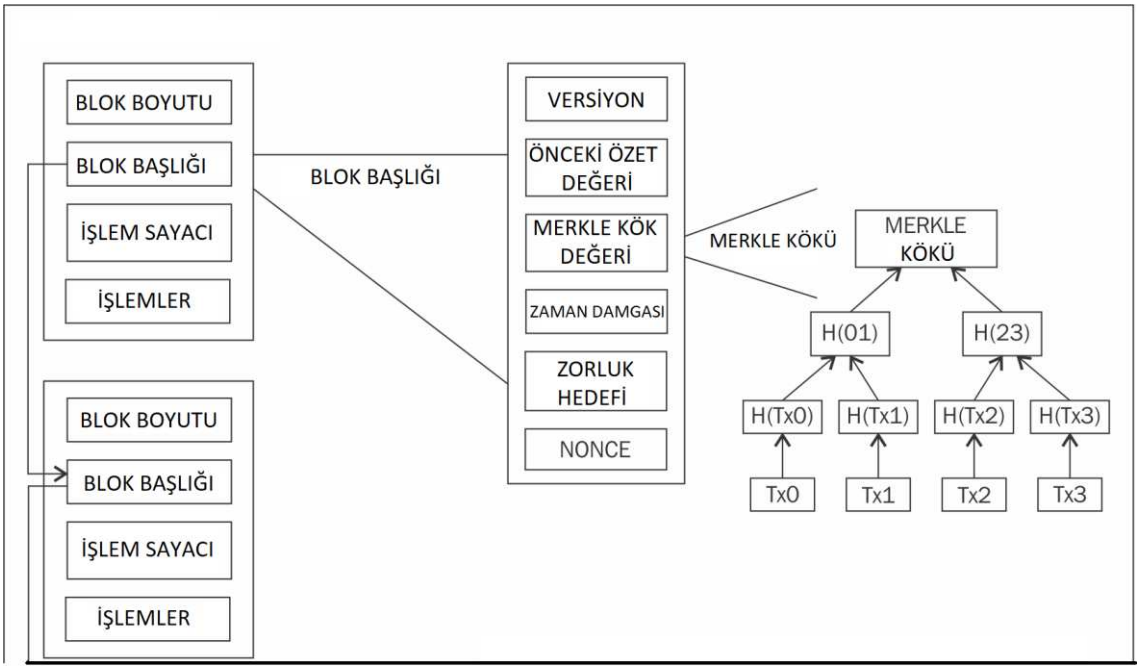
4.3.1 Blok Başlığının Yapısı

Blok başlığı her blokta bulunmak zorunda olan ve içinde versiyon numarası, önceki bloğun özet değeri, merkle kök özet değeri, zaman damgası, zorluk hedefi, ve bloğun nonce değerini barındırır.

Bayt	**İsim**	**Açıklaması**
4	Versiyon numarası	Blok onaylama işlemi için uyulması gereken kuralı gösteren blok versiyon numarasıdır.
32	Önceki blok başlık özeti	Bir önceki bloğun başlığına ait SHA256 özet bilgisidir.
32	Merkle kök özet değeri	Blok içindeki tüm işlemlerin SHA256 merkle kök özet değeridir.
4	Zaman damgası	Bu kısım bloğun yaklaşık olarak üretildiği andaki zamanı barındırır. Daha açık olarak, bu madencinin başlığın özetini çıkardığı andaki zamanın bilgisidir. Yani madencinin bakış açısına göre bir zamandır.
4	Zorluk hedefi	Bloğun zorluk hedefini barındırır.

4	Nonce	Madencilerin zorluk hedefine uygun bir hash üretmek için tekrar tekrar değiştirdiği gelişigüzel bir numaradır.

Daha açıklayıcı olması açısından bir sonraki diyagramda gösterildiği gibi, Blockchain her bloğun kendinden bir sıra önce gelen blok ile bir önceki bloğun başlığının özet değerini referans olarak tutması vasıtasıyla birbirlerine bağlanan bir blok zinciridir. Bu bağlanma kuralı, işlemlerin bulunduğu blok ve o bloktan önce gelen her bir bloğun değiştirilmeden hiçbir bloğa ait işlemin değiştirilemeyeceğini garanti altına alır. Bir önceki bloğa bağlanmayan yalnızca tek bir blok vardır. Bu bloğa başlangıç bloğu (genesis block) adı verilir.



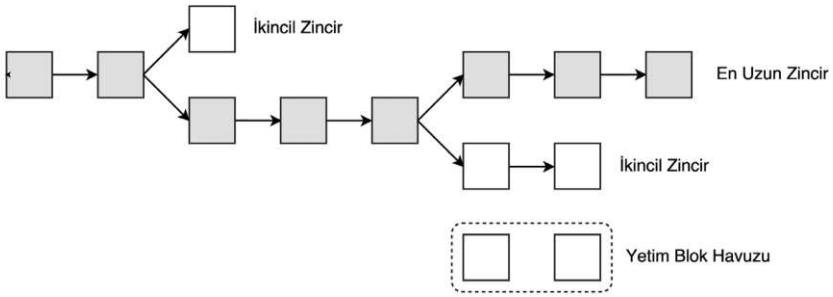
Şekil 4.1 *Blok zinciri, bloklar, blok başlığı ve işlemlerin basit bir görünümü.*

4.4 Blokların Güvenliği ve Çatallanmalar

Bitcoin protokolü işlem onaylama sürecinde katı kurallar uygulayarak ve madencilik ile çifte harcama girişimlerine güvenlik sağlamaktadır. Bloklar, yalnıza katı kurallardan onay aldıktan sonra ve başarılı bir İş Kanıtı (PoW) çözümünden sonra blok zincirine eklenir. Belirli bir bloktan önceki blok sayısına "Blok Yüksekliği" adı verilir. Bu çalışma hazırlandığı sırada blok zincirinin yüksekliği 527354'tür. İş Kanıtı Blokchain'in güvenliği için kullanılmaktadır. Her blok temel para işlemi dışında bir veya birden fazla işlem barındırır. Bitcoin sisteminde İş Kanıtı ispatını yapan ve bulduğu bloğu zincire ekleten madenciye ödül verilmektedir. Temel para işlemi bu kanıtı yapan madenciye ödül olarak verilen paranın işlemidir. Ancak ödülü kazanan madenci en az 100 blok, yaklaşık 17 saat kazandığı bitcoinleri harcayamaz. Çünkü madencinin ürettiği blok, eş zamanlı olarak başka bir madenci tarafından da üretilmiş olabilir ve bu bloğun çalışmanın ilerki kısımlarında açıklanmış olan öksüz bloklardan biri olma ihtimali vardır. Sadece bloğunu zincire ekletebilen madenci ödül alabilir.

Aranan nonce değeri bir madenci tarafıından bulunan ve diğer madenciler halen nonce değerini bulmak için üzerinde çalıştıklara bloklara “bayat blok” adı verilir. Bayat denmesinin sebebi artık üzerinde çalışılmasına gerek duyulmaması kaynaklıdır.

Normal olarak blok zincirinde her bloğu takip eden yalnızca bir blok olabilir. Bazı durumlarda, aynı anda birden çok madenci blok üretir. Bu blokların içerikleri farklı olabilir. Ağdaki diğer düğümler ilk aldıkları bloğu onaylarlar. Her düğüm farklı bir bloğun doğrulayacağından çatallaşma meydana gelir. Fakat uzun vadede Bitcoin protokolü gereği, otomatik olarak en uzun zincir geçerli sayılacağından çatalın diğer ucundaki bloklar “yetim bloklar” olarak adlandırılır.

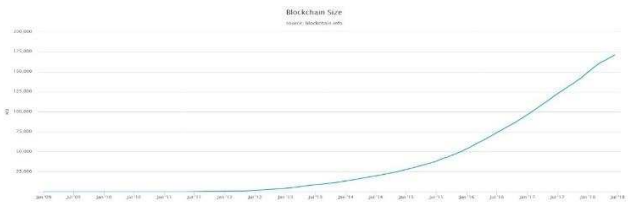


Şekil 4.2 *Yetim Blokları Ve En Uzun Zinciri Gösteren Diyagram*

Bitcoin protokülünün dağıtık yapısının doğası gereği, bazı durumlarda ağ normal olarak çatallanabilir. İki düğümün aynı anda geçerli bir bloğu duyurması durumunda, farklı işlemlere sahip iki bloğun bulunduğu bir durum ortaya çıkabilir. Bu arzu edilen bir durum değildir ancak yalnıza en uzun zinciri kabul ederek Bitcoin ağı tarafından üstesinden gelinebilir. Bu durumda küçük zincir, yetim olarak kabul edilir. Eğer kötü niyetli bir kişi ağ içindeki hesaplama gücünün %51’ini kontrol etmeyi başarabilirse, kendi istediği işlem geçmişine ait olan versiyonu ağa dayatabilir.

Blockchain üzerindeki çatallanmalar Bitcoin protokolü içindeki değişimlere bir giriş olarak meydana gelebilir. Tercihi çatallanma (Soft Fork) durumlarında yalnızca geçmişte onaylanan bloklar artık geçersiz kabul edilir bu şekilde zaman ilerledikçe yeni versiyona ait bloklar %51 üstünlüğü ele geçireceğinden bütün zincir yeni versiyona geçmiş sayılır. Tercihi çatallanma gündeme geldiğinde yeni protokol özelliklerinden yararlanmak için yalnızca madencilerin güncellenmesi gerekmektedir. Planlanmış güncellemeler muhakkak bir çatal oluşturmaz çünkü tüm kullanıcılar önceden güncellenmiştir. Öte yandan mecburi çatallanma (Hard Fork) durumlarında diğer tüm blokları geçersiz sayar ve tüm kullanıcıların güncellenmesini gerekli kılar. Yeni işlem tipleri gibi güncellemeler tercihi çatallanma ile eklenir ancak blok yapısı değişikliği veya büyük çaplı protokol değişiklikleri mecburi çatallanma ile sonuçlanır.

Blok zinciri bu çalışma hazırlandığı sırada yaklaşık olarak 171.1 GB gibi bir boyuta sahiptir.

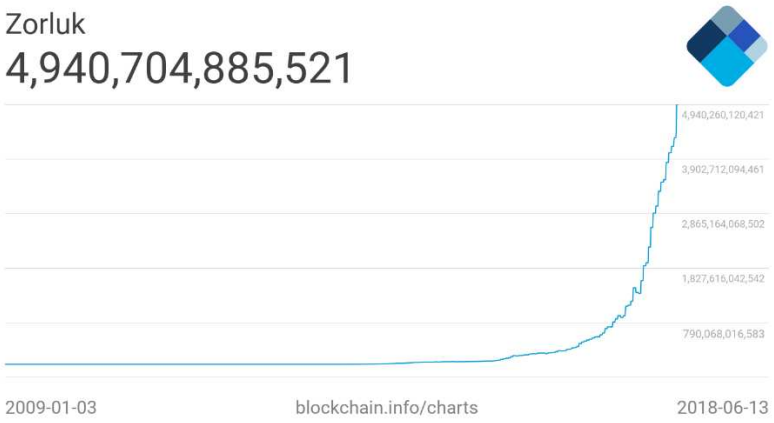


Şekil 4.3 *Tüm Zamanların Blok Zinciri Boyut Değişimi*

Yeni bloklar neredeyse her 10 dakikada bir zincire eklenmeye devam etmekte ve ağ zorluğu zincire eklenen blok sayısının istikrarını sürdürmek için her 2016 blokta bir dinamik olarak güncellenmek üzere ayarlanmıştır. Ağ zorluğu şu şekilde hesaplanmaktadır:

*Hedef Zorluk = Önceki Zorluk * Geçen Zaman/2016 * 10 Dakika*

Burada önceki zorluk eski zorluk oranını, geçen zaman ise 2016 blok üretmek için geçen zamanı temsil eder. Ağ zorluğu temel olarak madenciler tarafından bir blok üretmenin ne kadar zor olduğunu gösterir. Bir başka deyişle özet değeri bulmacasının zorluğunu belirtir.



Şekil 4.4 *Tüm Zamanların Blokchain Zorluk Grafiği*

4.5 Madencilik

Madencilik, Blockchain'e yeni bloklar ekleme yoluyla ilerleyen yoğun kaynak (resource-intensive) gerektiren bir süreçtir. Madencilik sürecinde madenci düğümler tarafından onaylanan işlemleri barındıran bloklar blok zincirine eklenirler. Bu süreç madenciler tarafından bir bloğun onayı için gereken kaynağın harcandığını garanti altına almak için yoğun kaynak gerektiren şekilde dizayn edilmiştir. Yeni paralar madencilerin gerekli işlem gücü kaynağını harcamasıyla üretilir. Bu süreç bitcoin ekosistemine daha fazla dijital para eklerken ayrıca sistemi dolandırıcılardan ve çifte harcama saldırılarından da korumaktadır.

Yaklaşık olarak yeni bir blok 10 dakikada üretilir. Madenciler yeni bir blok ürettiklerinde ürettikleri bloğa karşılık bir ödül kazanırlar. Bu ödül o bloktaki ilk işlem olarak eklenir ve dağıtılır (Coinbase Transaction). Ayrıca bloklarına ekledikleri işlemler için de işlem komisyon ücreti alabilirler. Yeni bloklar yaklaşık olarak sabit bir oranda üretilir. Ayrıca üretilen bitcoin oranı her 210,000 blokta yani yaklaşık olarak her 4 yılda bir yarı yarıya azalmaktadır. Bitcoin ilk ortaya çıktığında her blok için ödül olarak 50 bitcoin dağıtılmaktaydı. Daha sonra 2012 yılında bu sayı 25 bitcoin, 2016 Temmuz'da ise 12.5 bitcoin seviyesine düşürülmüştür. Bundan sonraki azalma tahminen 4 Temmuz 2016 tarihinde olacak ve verilen ödül 6.25 bitcoin olarak güncellenecektir.

Her gün yaklaşık olarak 144 blok üretilmektedir ve bu günde 1,728 bitcoin üretildiği anlamına gelmektedir. Günlük üretilen 144 adet blok sayısının sabit olmasına karşın bir gün içinde üretilen bitcoin sayısı günden güne değişebilir. Bitcoin arzı sınırlıdır ve 2140 yılında toplamda 21 milyon adet üretilmesiyle sona erecektir ve o tarihten sonra

herhangi bir bitcoin üretmek mümkün olmayacaktır. Buna karşın bitcoin madencileri işlem komisyonlarından gelir elde etmeye devam edebilecektir.

4.5.1 Madencilerin Görevleri

Yeni bir düğüm ağa katıldığında diğer düğümlerden geçmiş blokların dökümünü talep etmek suretiyle kendi kullandığı cihaza indirir. Ancak bu sadece madencilerin görevi değildir. Yalnızca madenci düğümlere ait olan görevler aşağıda belirtilen maddelerdir:

- **İşlem Onayı:** Ağ üstünde yayınlanmış işlemlerin dijital imzaları ve çıktıları tam düğümler tarafından soruşturulur ve doğrulanır.
- **Blok Onayı:** Madenciler ve tam düğümler tarafından alınan bloklar belirli kurallara göre değerlendirilerek onaylanma işlemine başlanır. Bu kurallar blok içindeki her işlemin onaylanmasını ve bunun yanında bloğa ait nonce değerinin doğrulanmasını gerektirir.
- **Yeni Blok Üretmek:** Madenciler ağ içinde yayılmış olan işlemleri onları onayladıktan sonra bir araya getirerek yeni bir blok önerisi sunar.
- **İş Kanıtını Gerçekleştirmek:** Bu görev madencilik sürecinin kalbidir ve madencilerin hesaba dayalı bir bulmacayı çözmesi yoluyla geçerli bir blok buldukları kısımdır. Blok başlığı 32-bit büyüklüğünde bir nonce alanı içerir ve madenciler daha önceden hesaplanan zorluk değerinden küçük olan bir özet değeri bulana dek nonce değerini tekrar tekrar değiştirmesi gerekir.
- **Getirme Ödülü:** Bir düğüm, bilmeceyi çözdüğünde derhal sonuçları bütün ağ boyunca yayar ve diğer düğümler bunu onaylayıp geçerli bir blok olarak kabul ederler. Burada küçük bir olasılıkla yeni üretilen blok, neredeyse aynı anda bulunan başka bir blokla çakıştığı için diğer düğümler tarafından onay alamayabilir. Ancak onaylandığında madenci 12.5 (2018 yılına göre) bitcoin ve ilgili işlem komisyonları ile ödüllendirilir.

4.6 İş Kanıtı Algoritması (Proof-of-Work)

İşlemlerin doğru ve kesin bir şekilde onayının gerektiği, güvene dayalı bir ekosisteme sahip olmayan bir ortamda Bitcoin transferi yapılması amaçlandığından beri mutabakat algoritmaları, Blockchain teknolojisiyle oldukça ilgili bir hale gelmiştir. Mutabakat algoritmalarının amacı içinde herhangi bir şekilde geçersiz ve çelişkili işlem içermeyen tek bir adet işlem geçmişinin varlığını garanti altına almaktır.

Blockchain ağı üzerindeki düğümler yeni eklenen blok içindeki işlemlerden ve emirlerden emin olmak durumundadır. Aksi halde, bireysel olarak ortaya çıkmış blok zincir copyaları türer ve bu durum yeni çatallanmalar ile son bulur. Düğümler farklı dünyaların bakış açısına sahip olacak ve bu çatallanma çözülmedikçe, ağ tek ve benzersiz bir yetkili kronolojiyi sürdüremeyecektir. Bu yüzden tüm Blockchain ağlarında tek bir yetkili uzun zincir yaratmak için dağıtık mutabakat mekanizması gerekmektedir. Bu mekanizma Blockchain ağının tipine göre değişkenlik gösterebilir. İdeal senaryoda, tüm onaylama yetkisine sahip düğümler, bir sonraki blok için işlemleri oylar ve çoğunluğun verdiği karara göre devam edilir. Buna karşın açık bir ağda herhangi bir kişi ağa katılabilir ve bu durum Sybil saldırılarına açık kapı bıraktığından felaket şeklinde sonuçlara yol açabilir. Sybil saldırısı, tek bir rakibin ağdaki birden çok düğümü kontrol ettiği bir saldırı türüdür.

Bitcoin, pahalı bir hesaplama işlemi ile madencilik yaparak bu probleme bir çözüm getirmiştir. Bu sayede tek bir düğümün hesaplama gücü sınırlı olduğundan ağ üzerindeki

başka kişilerin kimliğine bürünmek herhangi bir işe yaramayacaktır. Hesaplama gücü ile yapılan bu işe İş Kanıtı denmektedir.

İş kanıtı algoritmasında her bloğa ait bir zorluk hedefi vardır. Bu bloktan önceki bloğun özet değeri, o andaki bloğun içindeki işlemler ve nonce değeri toplu olarak hash fonksiyonuna sokulur. Fonksiyondan çıkan değerin bloğa ait zorluk hedefine eşit veya küçük olması beklenir. Hash fonksiyonunun çıktısı eşit olarak dağıtıldığından kesin bir sonuca ulaşmanın kolay olacağı bir şekilde blok oluşturmak imkansızdır. Bu yüzden ağ içindeki madenci bilgisayarlar arasında doğru nonce değerini bulmak için bir yarış meydana gelir. Hedefe ulaşıldığında, hedefe ulaşan madenci bunu ağ boyunca yayar ve diğer katılımcılar işlemleri onaylar. Eğer yeterli sayıda doğrulayıcı düğüm işlemleri eklenebilir uygunlukta bulursa işlemlerin olduğu blok zincire eklenmeye kabul edilir. Özetle algoritma şu adımlardan oluşmaktadır:

- Bir önceki bloğun özet değeri ağ içinden alınır.
- Potansiyel işlemler bir blok içinde birleştirilerek ağ boyunca yayılır.
- SHA256 kullanılarak blok başlığının özet değeri, önceki bloğun özet değeri ve nonce değerinin özeti alınır.
- Hash fonksiyonun çıktısı o andaki zorluk hedefinden küçükse süreç durur.
- Hash fonksiyonun çıktısı o andaki zorluk hedefinden büyük ise, aynı işlem nonce değeri artırılarak devam edilir. Bitcoin ağındaki hash oranı (saniyede çıkarılan özet sayısı) arttıkça toplamda 32-bit büyüklüğünde olan nonce değeri çok hızlı şekilde tüketilir. Bu sorunu gidermek için ekstra nonce çözümü eklenmiştir. Her blok içinde olan temel para işlemi (coinbase transaction) madencilere daha geniş bir nonce aralığı sağlamak için ekstra bir nonce kaynağı kullanır.
- Madencilik zorluğu zaman geçtikçe artmıştır. Bitcoin üretmek için eskiden bir laptop CPU'su yeterli olurken şimdi ise bu matematik problemini çözmek için sadece bu işe özel tesis edilmiş madencilik merkezleri gerekmektedir.

Buradaki amaç herhangi bir kişiye veya kuruma gereğinden fazla güç vermemek olduğundan, bir bloğun geçerliliği için yapılacak oylamada harcanak olan kaynağın sınırlı olması tercih edilmiştir. Buradaki sınırlı kaynak işlem gücüdür. Yılar geçtikçe Moore yasasına göre ve bulut işlemcilerden dolayı işlem gücü gittikçe ucuzlayacağından ve daha ulaşılabilir olacağından bu matematiksel problemin zorluğu kendinden bir önce gelen problemin çözüm süresine ve sıklığına göre düzenlenmiştir. İş kanıtı mekanizmasına yöneltilen ortak eleştiri harcanan işlem gücünün aynı zamanda yüksek miktarlarda enerji harcamak demek olduğudur. Madencilik faaliyetini sadece kışın yapan ve cihazlardan çıkan ısıyla evini ısıtan madenciler de mevcuttur.

Şekil 4.5 *Moore Yasası*

5. SONUÇLAR VE ÖNERİLER

Bu bitirme çalışması ile Blockchain'i daha önce hiç duymamış birinin okuduktan sonra gerek temel kavramlar konusunda gerek teknik kavramlar konusunda nitelikli bilgiye ulaşması amaçlanmıştır. Bu doğrultuda çalışmanın sonucunda tüm temel kavramlar ve çoğu kaynakta üstünkörü olarak geçilen teknik kavramları detaylarıyla birlikte açıklanmıştır. Gerek arkasındaki matematiksel ve kriptografik güçten, gerekse sistem işleyişi açısından Blockchain teknolojisinin ne kadar büyük bir potansiyel olduğu ve yeni bir çığır açmak üzere olduğu görülmüştür. Bu büyük potansiyele karşın gerçek hayata uygulamaları açısından henüz yolun çok başında olduğu da ortadadır. Bu çalışmada anlatılanların dışında "akıllı kontratlar", "proof-of stake" mekanizması gibi gerçekten oldukça etkileyici ve devrim niteliğinde konu başlıkları da bulunmaktadır. Ancak bu çalışmanın yalınlığı açısından ele alınmamıştır. Diğer taraftan Blockchain teknolojisinin tüm bu güzelliklerine ve ilgi çekici yapısına rağmen hala geliştirmeye muhtaç yanları ve barındırdığı riskler de mevcuttur. Bu sebeple bir konu ele alınırken tüm yönleriyle ele alınmalı ve değerlendirilmelidir.

Malesef ülkemiz, yeni teknolojileri yakalama öğrenme ve bunun üzerinde ürün geliştirme konusunda biraz yavaş kalmaktadır. Türkçe kaynak azlığı da buna sebep olmuştur. Bu sebepten bu çalışmanın dışında kalan ve oldukça büyük potansiyele sahip Blockchain'in diğer konu başlıklarının da kesinlikle okunup araştırmasını öneririm. Zira bazı teknolojilerin artık ne olduğunu öğrenme kısmını halledip, acilen bu teknoloji kullanılılarak nasıl ürün geliştirilir? Bu teknoloji sayesinde hangi problemlere çözüm bulunabilir? gibi sorular sormanın vakti gelmiştir.

KAYNAKLAR

[1] Bashir, I. (2017), Mastering Blockchain, Packt Yayınları, Birmingham.

[2] Bergquist, J. (2017), Blokchain Technology and Smart Contracts, Master Tezi, Upsala Üniversitesi

[3] Doğantekin, S. ve Usta, A. (2017), Blockchain 101, Kapital Medya Hizmetleri, İstanbul.

[4] Survey on Blockchain Technologies and Related Services, (2016), Araştırma Raporu, Nomura Research Institute, (Japonya)

[5] Christidis, K. ve Devetsikiotis, M. (2016), "Blockchains and Smart Contracts for the Internet of Things", IEEE Access, Special Section On The Plethora Of Resarch In Internet Of Things, Volume 4, pp.2292-2303.

[6] Crosby, M. ve Pattanayak, P. et. (2016), "Blockchain Technology: Beyond Bitcoin", AIR, Issue No:2, pp. 6-19

[7] Wall, E. ve Malm, G. (2016), Using Blockchain Technology and Smart Contracts to Create a Distrubuted Securities Depository, Master Tezi, Lund Üniversitesi Elektrik ve Bilgi Teknolojieri Departmanı

[8] Narayanan, A. ve Bonneau, J. (2016), Princeton Üniversitesi Yayınları, New Jersey

[9] Songara, A. ve Chouhan, L. (2017), Blockchain: A Decentralized Technique for Securing Internet of Things, Master Tezi, Department of Computer Science and Engineering National Institute of Technology Hamirpur, Hamirpur

[10] Nakamoto, S. (2008), Bitcoin: A Peer-to-Peer-Electronic Cash System

[11] Ellervee, A. (2017), A Reference Model for Blockchain-Based Distributed Ledger Technology, Master Tezi, University of Tartu Institute of Computer Science Software Enginerring Curriculum, Tartu

[12] Çarkacıoğlu, A. (2016), Kripto-Para Bitcoin, Araştırma Raporu Sermaye Piyasası Kurulu Araştırma Dairesi, İstanbul

ÖZGEÇMİŞ

Ad Soyad:	Aziz ÇOBAN
Doğum Tarihi:	17.08.1996
Doğum Yeri:	İstanbul
Üniversite/Bölüm:	Yıldız Teknik Üniversitesi / Matematik Mühendisliği
Lise:	Üsküdar Ahmet Keleşoğlu Anadolu Lisesi
Staj Yaptığı Yerler:	6Gen Global Yazılım Ltd. Şti.
E-mail:	aziizcoban@gmail.com