Blokzincir Teknolojisi

İçerik

- Dağıtık Sistemler (P2P, Bittorent)
- Para-Kripto Para
- Blokzincir Mekanizması
- Node-Block Yapısı
- Mining (PoW - Nonce – Halving - Ödül)
- Riskler ve Güvenlik

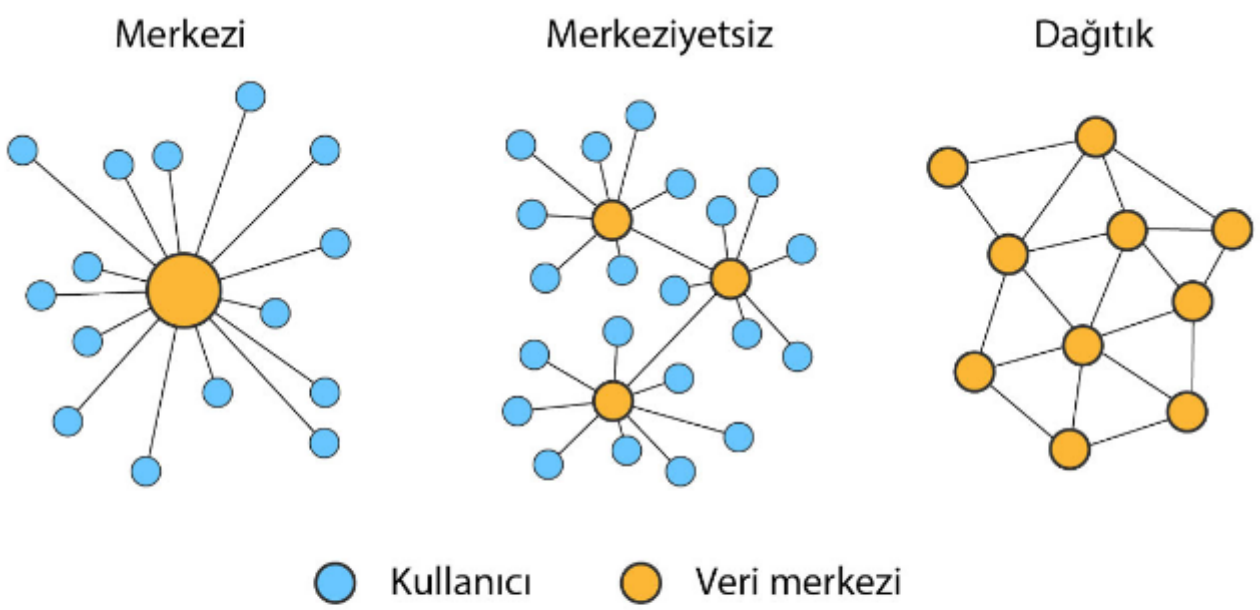
- https://tr.cointelegraph.com/ ile Siber Güvenlik ve Savunma (Şeref Sağıroğlu) kaynaklarından hazırlanmıştır.

DAĞITIK SİSTEMLER

Dağıtık Sistem

- Aynı veri kaydının, birbirleriyle iletişim halindeki farklı bilgisayarlar üzerinde saklanmasına dağıtık ağ ya da dağıtık sistem denir.
- Dağıtık ağ üzerindeki donanımlar, tek bilgisayar gibi davranırlar.
- Bu sayede bazı bilgisayarlarda teknik arıza meydana gelse bile, diğer üyelerde verilerin birer kopyası saklandığı için sistem aksamadan çalışmaya devam eder.

Merkezi-Merkeziyetsiz- Dağıtık



Sol: *Geleneksel ya da merkezi yapıda her kullanıcı aynı bilgisayara bağlanır.*

Orta: *Merkeziyetsiz yapılarda kullanıcılar, kendileri için en verimli sunucuya bağlanırlar.*

Sağ: *Dağıtık yapıda ise kullanıcılar aynı zamanda veri sağlayıcısıdırlar.*

Dağıtık Yapı

- Dağıtık yapı sayesinde verilerin sahipliği kurum ya da otoritede bulunmaz.
- Hak; ağdaki kullanıcılara demokratik biçimde teslim edilir.
- Kayıtlı veriler kimsenin tekelinde olmadığından, ağdaki tüm kullanıcılar erişim sağlayabilir, herkesin eşit hak iddia edebildiği bir ortam oluşur.

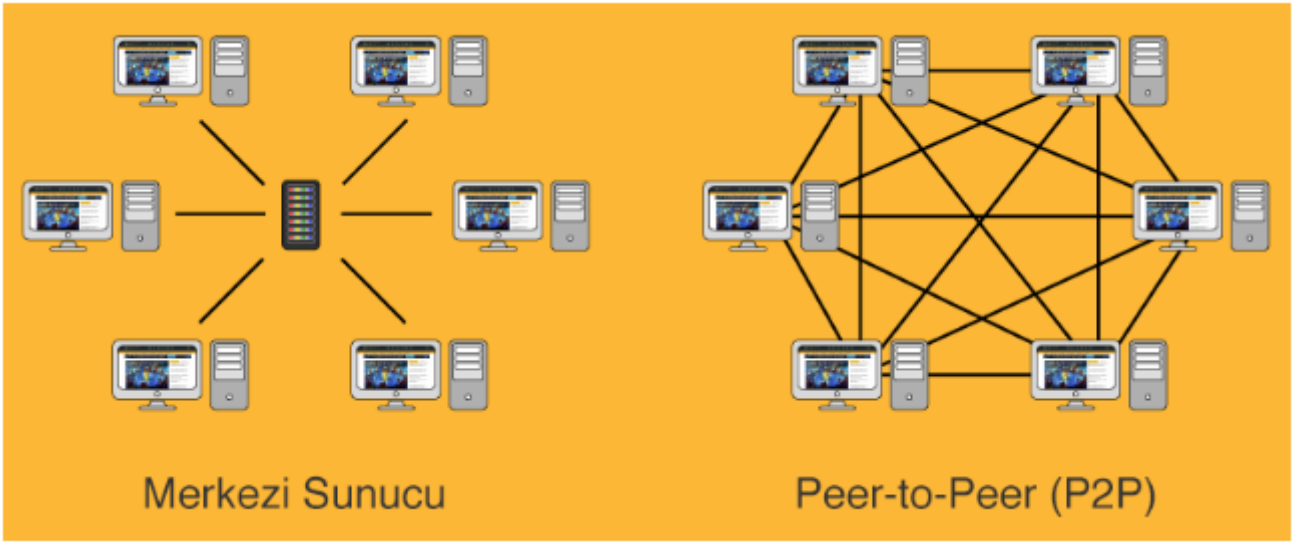
P2P Ağlar

- Merkezi kontrole ihtiyaç duymadan, iki veya daha fazla bilgisayarın veri paylaşmak amacıyla birbirine bağlandığı ağ protokolüne Peer-to-Peer ya da P2P denir.
- Eşler, merkezi kontrol olmadan kendilerine ait veri depolama donanımlarını ağın kullanımına açarlar.
- P2P ağlarında merkezi sunucu yapısına ihtiyaç yoktur. Eşler hem sağlayıcı, hem de tüketicidirler.
- Bilgisayarların doğrudan birbirine bağlandığı P2P ağ protokollerinde, her dosya tipini paylaşma olanağı bulunduğundan işlemler daima yasalara uygundur diyemeyiz.

Merkezi Sunucu

- Birçok hizmet sağlayıcı merkezi sunucu modelini tercih eder. Çünkü bu model, yönetici açısından kolaylık sağlar. Veriler merkezde birikir, bir sorun yaşandığında ana bilgisayar üzerinden çözüm sağlanır.
- Binlerce kullanıcının tek bilgisayara bağlanmaya çalışması sistemin çökmesine neden olur. "Denial-of-service attack" ya da bilinen kısaltmasıyla "DDoS" saldırılarına açıktır.

Merkezi Sunucu - P2P



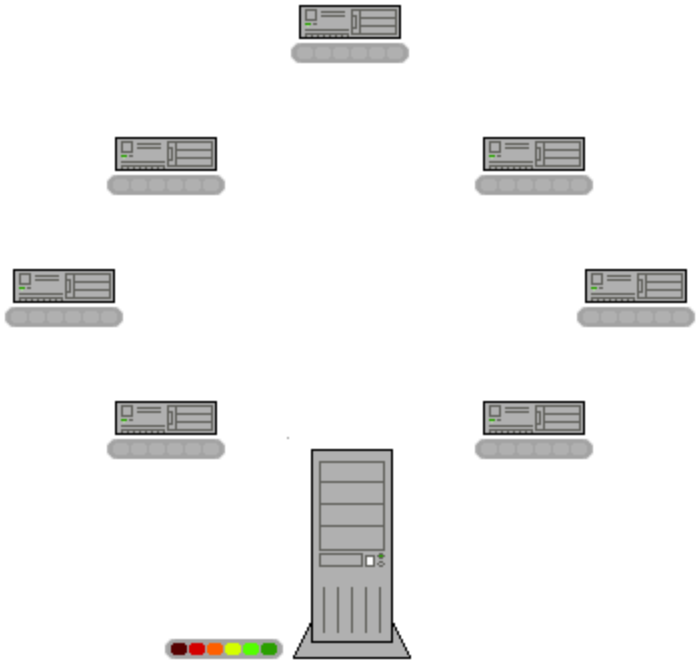
P2P Ağlar ve Bittorent

- Kullanıcı, ihtiyaç duyduğu veriye sahip olan bilgisayar hangisiyse, doğrudan ona bağlanıp veriye erişir. Dosyayı edindikten sonra ağa bağlı kalmaya devam ederse, kendisi de sağlayıcıya dönüşür.
- Tahmin edileceği üzere P2P sisteminin idaresi oldukça zordur. Sistemdeki işlemlerin takip edilmesi, kullanıcının nereye bağlandığını ve neyi transfer ettiğini izlenmek imkansıza yakındır.
- Yüzlerce bilgisayar az sayıda bilgisayara bağlanmak isteyecek ve darboğaz oluşacaktır.
- BitTorrent protokolü, yavaşlama ve darboğaz sorunu olmadan büyük boyutlu dosyaların ağdaki tüm kullanıcılara paylaşılmasına imkan sağlıyor.

Bittorent

- Tanımlama dosyaları (.torrent) sayesinde kullanıcıların birbirlerine bağlanmalarına ve büyük boyutlu dosyaları paylaşmalarına imkan tanıyan takas protokolüne BitTorrent denir.
- BitTorrent protokolünün gücü, dosyanın tamamı indirilmeden de paylaşılmaya başlamasında yatar. Dolayısıyla ağda ne kadar çok kullanıcı varsa, dosya parçasına erişim o kadar kolay ve bağlantı hızı o kadar fazladır.
- Merkezi sunucu yapılarının aksine BitTorrent protokolünde, bağlı kullanıcı sayısı arttıkça dosyaya erişim kolaylaşır, bağlantı hızı yükselir.

P2P Mantığı



Kaynak dosya, parçalara ayrılarak erişime açılır. Her bilgisayar, indirdiği parçayı diğerlerine paylaşır. Kullanıcı, ihtiyacı olan veriyi, o parçaya sahip ağdaki herhangi kullanıcıdan alabilir.

PARA-KRİPTO PARA

Para Çeşitleri

- **Emtia Para:** Emtia para, değeri yapıldığı üründen kaynaklanan paralara denmektedir. Altın Gümüş gibi
- **Temsili Para:** Değerli metallerin para olarak kullanımında zamanla ortaya çıkan birçok zorluktan dolayı, zaman içerisinde emtia para sistemi altına dayalı temsili para sistemine dönüşmüştür. Banknot gibi
- **İtibari Para:** Şekil açısından temsili paralara benzeyen ancak altın veya gümüşe dayalı olmayan itibari paralar. Dolar, Petrol gibi
- **Dijital Para:** Elektronik olarak saklanan ve transfer edilebilen paralardır. (Kağıt parayı temsil eder)
- **Sanal Para:** Herhangi bir merkez bankası, kredi kuruluşu veya e-para kuruluşu tarafından ihraç edilmediği halde, dijital paraya benzeyen ancak kağıt parayı temsil etmeyen sanal paralar ortaya çıkmıştır.
- **Kripto-Para:** Son yıllarda kriptografik/şifreli oldukları için güvenli işlem yapmaya ve ek sanal para arzına olanak sağlayan kripto-paralar hem alternatif para birimi ve dijitaldirler hem de sanal paradırlar.

Bitcoin

- Bitcoin, Ağ üyeleri çok sayıda işlemci ve elektrik gerektiren son derece karmaşık yineleme işleminde, birbirlerinin onaylarını doğrulamak ve işlemlerin geçerliliği için herhangi bir üçüncü tarafın güvenilirliğine itimat etmek zorunda kalmadan anlaşmazlıkları bertaraf eden bir mülkiyet ve işlem defteri çıkarmak için işlem gücü harcarlar.
- Bitcoin %100 doğrulama ve %0 güven üzerine kurulmuştur

Dünyada Bitcoin

- Alman Federal Finansal Denetleme Otoritesi (BaFin), Belçika Merkez Bankası ve Fransa Merkez Bankası, Bitcoin'in gözetiminin herhangi bir meşru otorite tarafından yapılmaması, fiyatının aşırı dalgalanma yaşaması, kara para aklama ve terörün finansmanında kullanılması ve taşıdığı siber güvenlik riskleri konusunda uyarılarda bulunmuşlardır.
- Finlandiya Merkez Bankası, İsveç Merkez Bankası Bitcoin'in para birimi olarak kabul edilemeyeceğini belirtmişlerdir.
- Fransız Maliye Bakanlığı 2014 yılında yayımladığı yasal bir düzenleme ile kripto para birimlerine ilişkin hesapların kullanımına kimlik doğrulama zorunluluğu getirmiş, kazanılan gelirleri ise vergiye bağlamıştır.
- Çin Merkez Bankası 2013 yılında bir duyuru yayımlayarak, finansal kuruluşların Bitcoin ile alışveriş yapmamaları gerektiğini belirtmiştir.
- Türkiye'de kripto para alımı, satımı ve kullanımı hiçbir yasa ile düzenlenmemiştir ve 6493 Sayılı Kanun'a göre kripto paralar e-para olarak kabul edilemezler. Dolayısıyla, aslında bu para birimlerinin kullanımı yasak değildir.

Bitcoin ve P2P

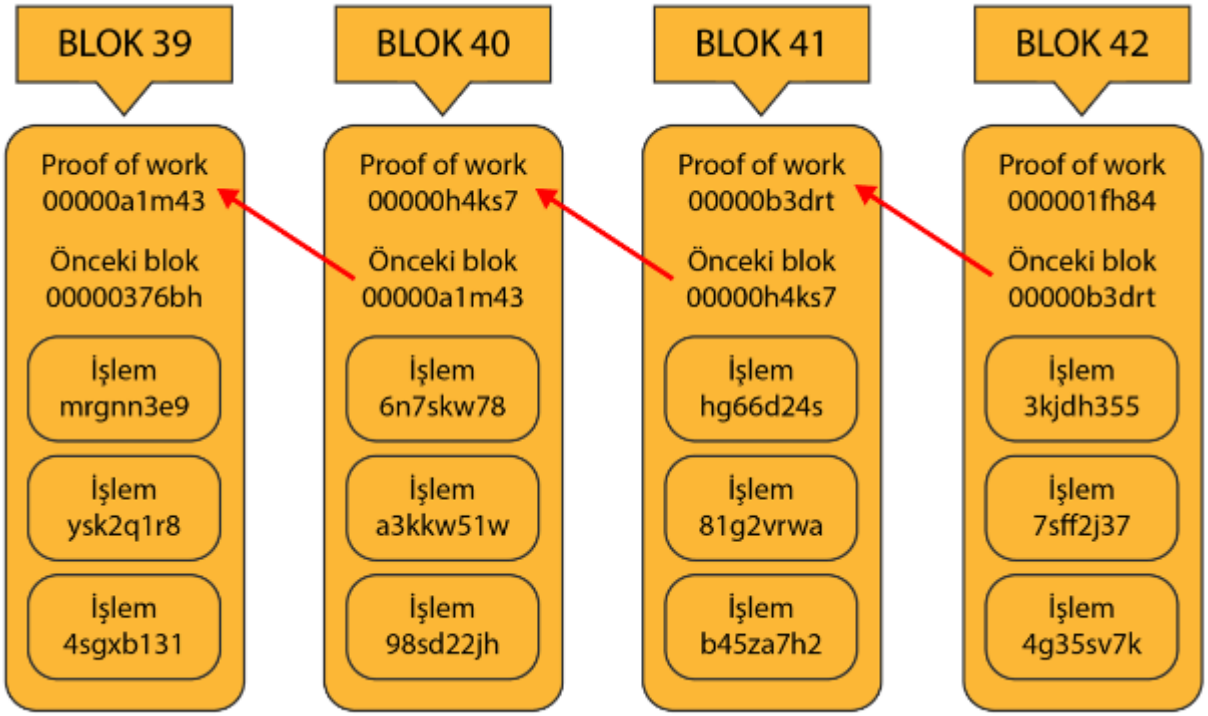
- Kullanıcılar, dijital imzalı mesajlar aracılığıyla BTC gönderir veya alırlar. Tüm işlemler dağıtık defter üzerine kaydedilir ve ağa bağlı kullanıcılar tarafından defterdeki kayıtların doğruluğu kontrol altında tutulur.
- Bitcoin ağında "node" ismi verilen, veri doğruluğunu ve bütünlüğünü sağlayan bilgisayarlar bulunur. Node'lar, diledikleri zaman ağa dahil olur veya ayrılırlar. Blockchain üzerindeki kayıtların birer örneğini ellerinde tutan node'lar verilerin bozulmadığına dair güvenlik mekanizması oluştururlar.
- Dileyen herkes Bitcoin.org adresinden Bitcoin Core dosyasını indirerek ağa destek verebilir.

BLOKZİNCİR

Blokzincir Teknolojisi

- Bitcoin isimli ilk kripto para birimini dünyaya tanıtan Satoshi Nakamoto lakaplı kişi ya da grup tarafından 2008 yılında blockchain'in icat edildiği biliniyor.
- Herhangi bir merkez ya da otoriteye ihtiyaç duymadan, verilerin dağıtık ağ üzerinde saklandığı kayıt teknolojisine blockchain ya da blok zinciri denir.
- İlk kripto para birimi Bitcoin ile hayatımıza giren blockchain, eski verilerde düzenleme olanağı sunmaz.
- Dolayısıyla geleneksel veri tabanları gibi değil, işlemlerin ardı sıra listelendiği dijital bir kayıt defteri şeklinde çalışır.

Sadeleştirilmiş Bloklar



Sadeleştirilmiş blockchain yapısı. Veriler giriş tarihine göre art arda sıralanır. Her blok kendinden önceki blokun şifrelenmiş kodunu içinde barındırarak değişikliklere karşı güvenlik sağlar.

Hash

- Her blok içinde işlem bilgileri ve önceki blokun şifrelenmiş özet kodu (hash) bulunur.
- Her blok, kendilerinden öncekine şifreli biçimde bağlı olduğundan, herhangi birinde değişiklik yapılması, sonraki tüm bloklarda değişiklik meydana getirir. Bu sayede verilerin asla değiştirilmediğinden emin olunur.
- Özet fonksiyon (hash) oluşturmak için SHA-256 ismi verilen şifreleme sistemi kullanılır. SHA-256 standardı; girdi verisi bir harften de ibaret olsa, yüzlerce sayfalık roman uzunluğunda da olsa daima on altılık sayı sisteminde 64 karakterlik çıktı sunar.

Çalışma Mantığı

- Ağa destek veren, node* isimli gönüllü katılımcılar tarafından blokların ve şifreleme bilgilerinin kontrolü yapılır. Yeterli onay alınması durumunda blok, zincire eklenir.
- Gerçekleşen işlemin ardından madenci, kullanılan konsensüs yapısına uygun biçimde ödül kazanır. Bitcoin ağından örnek verecek olursak, bu yazının hazırlandığı Haziran 2020 tarihi itibarıyla oluşturulan her blok başına madenciye 6,25 BTC ödül verilmektedir.
- 11 Mayıs 2020'de gerçekleşen Bitcoin blok ödülü yarılanması işlemi (halving) öncesi bu tutar 12,5 BTC idi.

NODE – BLOCK

Node nedir?

- Açık blockchain ağlarına gönüllü biçimde bağlanan, gerçekleşen işlemler ve oluşturulan bloklar hakkında bilgi yayılmasına yardımcı olan bilgisayarlara node (düğüm) denir.
- Node'lar şu kontrolleri yapar:
  - Kurallara uygun miktarda coin üretildi mi?
  - Transferler uygun biçimde imzalandı mı?
  - Bloklar doğru veri formatında mı?
  - Çifte harcama (double spend) yapıldı mı?
- Yetkili node'lar, konsensüs kurallarına uymayan işlemleri geçersiz kılma yetkisine sahiptir.

Light Node

- Blockchain’deki işlemlerin doğruluğunu sağlamak üzere, blokların sadece başlık (header) bilgilerini barındıran düğümlere “light node (hafif düğüm)” ismi verilir.
- Hafif düğümler, işlemleri doğrulamak için Simplified Payment Verification (SPV) adlı yöntemi kullanır.
- Light node'ların kurulumu, bakımı ve çalıştırılması kolaydır ama full node'lara doğrudan bağlıdırlar.

Full Node

- Blockchain üzerinde gerçekleşen tüm işlemlerin depolandığı, kurallara uygun biçimde denetlendiği ve doğrulandığı bilgisayarlara full node (tam düğüm) denir.
- Gereksinimleri daha yüksek olduğundan az sayıdadırlar. Light node'lara kıyasla daha yüksek donanıma ihtiyaç duyarlar.
- **Full node'lar, konsensüs kurallarına uymayan her işlemi geçersiz kılma yetkisine sahiptir.**
- Bilgisayarınızı full node'a dönüştürmek isterseniz, bitcoin.org indir adresinden Bitcoin Core dosyasını indirerek ağa destek verebilirsiniz.
- **Bitcoin ağının devamlılığını sağlayan full node'lar ayda ortalama 200 GB upload, 20 GB download yapıyor.**

Block Yapısı

- Blokların içinde; blok numarası, blok başlığı, önceki bloktaki verilere ait özet fonksiyon (hash), bloktaki verilere ait özet şifre ve zaman damgası gibi temel öğeler bulunur.
- Blok içindeki verilerin büyük kısmı madencilik işleminin yapıldığı esnada ağ tarafından sunulmaktadır.
- Bitcoin ağındaki madencinin görevi, Proof-of-Work** konsensüs algoritmasına uygun biçimde blok verisini şifrelemektir.
- Yüksek miktarda işlem gücü gerektiren bu görevi başarıyla yerine getiren ilk madenci, bloku oluşturmaya ve konsensüs yapısında belirtilen ödülü elde etmeye hak kazanır.

Bitcoin içeriği

BITCOIN BLOK İÇERİĞİ			
Sihirli sayı		4 byte	"0xD9B4BEF9" şeklinde sabit değer
Yükseklik		4 byte	Blok numarası
BAŞLIK (HEADER)	Versiyon	4 byte	Kullanılan güncel sürüm
	Önceki başlık	32 byte	Önceki blokun başlık özeti (hash)
	Merkle kökü	32 byte	İşlemlerin özet değeri (hash)
	Zaman damgası	4 byte	1 Ocak 1970'ten itibaren geçen süre
	Zorluk	4 byte	Ağın zorluk bilgisi
	Nonce	4 byte	Ağ zorluğuna göre ayarlanmış rastgele sayı
İşlem sayısı		1-9 byte	Belirli uzunlukta tam sayı değeri (integer)
İşlemler		-	Bloktaki transferlerin listesi

MINING (POW - NONCE – HALVING)

Proof Of Work (PoW)

- Bilgisayarın, belirlenen bir iş için emek sarf ettiğini ispatladığı yönteme Proof-of-Work (PoW) denir.
- Madenciler, hash kodunun başında belirlenen adette sıfır oluşturabilmek için "nonce" ismi verilen rastgele sayıyı bulmak için pek çok deneme yaparlar. Brute force ismi verilen, doğru sonucu bulana kadar tekrar tekrar deneme yöntemi ile bu işlemi sürdürürler.
- Doğru "nonce" sayısını bulan ve hash kodunun başında belirtilen adette sıfır elde eden ilk madenci hedefine ulaşır.

Nonce

- "Number Only Used Once (Yalnızca Bir Kez Kullanılan Sayı)" ifadesinin kısaltılmış hali olan nonce, yetkilendirme amacıyla kullanılan ve rastgele üretilen sayıdır.
- Bitcoin madenciliği, astronomik ölçekte işlem gücü gerektiriyor. Bitcoin madenciliğindeki bu büyük uğraş, blok ödülünü kazanmak için…
- ***Hatırlatma:*** *11 Mayıs 2020'de gerçekleşen Bitcoin blok ödülü yarılanması (halving) işlemiyle, madenci ödülleri 6,25 BTC'ye indirildi.*

Halving

- Bitcoin'in (BTC) arzı sınırlı. Toplam 21 milyon adet BTC çıkarıldığı zaman üretim de duracak. Dijital altın olarak adlandırılan Bitcoin, 21 milyona ulaştığında tüm BTC'ler çıkarılmış ve dolaşıma sokulmuş olacak.
- An itibarıyla maksimum Bitcoin arzının kabaca yüzde 85'ine denk gelen, 18 milyondan fazla BTC dolaşımda bulunuyor.
- Bitcoin blockchain ağında oluşturulan her 210.000 blokta bir madencilere verilen BTC ödülü yarı yarıya azalıyor. BTC üretmek de bir o kadar zorlaşıyor. Yaklaşık 4 yıla denk gelen bu yarılanma işlemine Bitcoin halving ya da Bitcoin blok ödülü yarılanması deniyor.

Halving Tarihleri

- 28 Kasım 2012'de gerçekleşti. O zamana kadar oluşturulan bloklar için 50 BTC ödenirken, 210 bininci bloktan itibaren 25 BTC ödenmeye başlandı.
- 9 Temmuz 2016 tarihinde yaşandı. 420.000 numaralı blok oluşturulduğu andan itibaren her üretilen blok karşılığında 25 BTC yerine 12,5 BTC kazanılmaya başlandı.
- *11 Mayıs 2020'de gerçekleşen Bitcoin blok ödülü yarılanması (halving) işlemiyle, madenci ödülleri 6,25 BTC'ye indirildi.*

Bitcoin Geleceği

- Nakamoto, sınırlı arz sayesinde satın alma gücünün asla yok olmamasını hedefledi.
- Bitcoin blok ödüllerinin yarılanması ise hem ağın sürdürülebilirliğini sağlıyor hem de teorik olarak fiyatların artmasına vesile oluyor. Sınırlı arzı olan ve üretilmesi güçleşen emtianın değerinin de artması bekleniyor.
- 21 milyonuncu BTC'nin 2140 yılında çıkarılması bekleniyor.
- Son Bitcoin çıkarıldığında madencilere sadece 1 Satoshi, yani 0,00000001 BTC ödül verilecek. Bu noktadan itibaren artık blok ödülü verilmeyecek. Bunun yerine işlem başına madencilerin aldıkları işlem komisyonları geçerli olacak.

Örnek Blok

- Astronomik işlem gücü harcıyor olsalar da, madencilerin yaptıkları iş aslında basit bir sayıyı bulmak, yani nonce değerini…
- Blockchain.com sitesi üzerinden, Bitcoin ağında oluşturulmuş herhangi bir bloka ait bilgi ekranına girdiğimizde şuna benzer bir görüntüyle karşılaşıyoruz:

Örnek Blok

Hash	00000000000000000007beef62d08dd723c4342bdf89dcf1fe77ca6208f081ba
Confirmations	2
Timestamp	2020-05-30 08:56
Height	632276
Miner	F2Pool
Number of Transactions	2,917
Difficulty	15,138,043,247,082.88
Merkle root	3437b844e1dfe1db50e36498b39ee15d5a0d3b603d62d297a87086a928b90a2f
Version	0x20000000
Bits	387,094,518
Weight	3,998,764 WU
Size	1,293,790 bytes
Nonce	3,719,213,695
Transaction Volume	5519.61929761 BTC
Block Reward	6.25000000 BTC
Fee Reward	0.61968993 BTC

Örnek Blok

- Dikkat ederseniz hash verisinin ilk 19 hanesi sıfırdan oluşuyor. Bu rastlantı değil. Hatta, Bitcoin madenciliğinin bu denli zor olmasının asıl sebebi bile denilebilir.
- Çünkü madenciler, farklı "nonce" değerlerini kullanarak, başında bu kadar sıfır bulunan hash kodunu oluşturmak için bu denli uğraşıyorlar.
- Yukarıda örneğini verdiğimiz bloku oluşturan madenci (F2Pool), hash verisinin başında 19 adet sıfır oluşturabilmek için nonce değerinin 3.719.213.695 olduğunu belirlemiş.

N değeri?

- Blok içinde yer alması gereken tüm verileri SHA-256 formatına dönüştürmek gayet basit bir işlem.
- Ancak Proof of Work konsensüs mekanizması, önümüze kalın bir set çekiyor ve önemli bir şart koşuyor:
- **Öyle bir hash kodu oluşturun ki, başında 'n' adet sıfır olsun.**
- Burada bahsedilen 'n' değeri ağın zorluğuna göre değişiyor.
- Zorluk seviyesi, Bitcoin madenciliği yapan işlemci miktarına ya da başka ifade ile hash oranına (hash rate) bağlı olarak güncelleniyor.
- Her 2.106 blokta bir düzeltme yapılan Bitcoin ağ zorluğu, her blokun ortalama 10 dakikada oluşmasını sağlayacak biçimde ayarlanıyor.

Demo

- Eldeki verileri SHA-256 formatında hash koduna dönüştürürken, başında 'n' adet sıfır oluşmasını beklemek inanılmaz derecede düşük bir ihtimal.
- Art arda on binlerce kez zar atıp her defasında 6 gelmesini beklemek bile daha olası.
- Blok içindeki transfer verileri, blok numarası, önceki blokun hash kodu, zorluk seviyesi, işlem adedi gibi veriler sabit olduğundan madencinin elinde tek değişken kalıyor: nonce.

Demo

https://andersbrownworth.com/blockchain/block

RİSKLER VE GÜVENLİK

Güvenlik

- Bitcoin ağındaki madencilik işlemleri, kaba tabir yapacak olursak kulağı tersten göstermeye benziyor.
- Hesaplanması basit transfer dökümlerini, son derece zorlu bir hesaba dönüştürerek astronomik ölçüde işlem gücü harcanmaya dayalı bir sistem.
- Ancak bunun mantıklı bir açıklaması var: blok ödülü…
- Ağ zorluğunun, blok oluşturmak için gereken işlem gücünün artması aslında Bitcoin ekosistemi için iyi bir durum.
- Zorluk ne kadar artarsa, o kadar çok madenci işlem gücünü Bitcoin ağına ayırıyor demektir.
- Ağın işlem gücünün artması ise Bitcoin'in sağlamlığını ve güvenirliğini artırır.

Riskler

Risk	Sebep	Etki Aralığı
Gizli Anahtar Güvenliği	Genel anahtar şifreleme şeması	Blok Zincir 1.0 ve 2.0
%51 Güvenlik Açığı	Konsensus mekanizması	
İllegal Faaliyetler	Kripto para birimi uygulaması	
İşlem Gizliliği Sorunu	İşlem tasarım hatası	
Çift Harcama	İşlem doğrulama mekanizması	
Zeki Sözleşmedeki Güvenlik Zaafları	Zeki Sözleşme Uygulaması	Blok Zincir 2.0
Düşük Fiyatlı İşlemler	Program yazma hatası	
Optimize Edilmemiş Zeki Sözleşme	EVM tasarım hatası	

Gizli Anahtar Güvenliği

- Anahtarlar Bitcoin cüzdanlarına erişmek için gerekli olan özgün alfanümerik şifrelerdir. Anahtarı kaybetmeniz cüzdanınızı da kaybetmeniz anlamına geliyor.
- Blokzincir teknolojisinde, kullanıcının gizli anahtarı yine kullanıcı tarafından üretilmektedir ve bu anahtar blokzincirde kullanıcının kimlik ve güvenlik bilgisi olarak kabul edilmektedir.
- Kullanıcının kendisi tarafından üretilen bu gizli anahtarın kaybolması veya çalınması durumunda, bu anahtarın kurtarılması bir daha mümkün olmamaktadır.
- Kötü niyetli kişiler tarafından kullanıcının gizli anahtarının çalınması durumunda, kullanıcının blokzincir hesabı bu kişilerin kontrolüne geçebilmektedir.

%51 Attack

- Kötü niyetli kişilerin kayıtlı verilerde değişiklik yapabilmeleri için ağın yarısından fazlasını ele geçirmeleri gerekir. %51 saldırısı (Attack 51%) ismi verilen bu yöntemi uygulamak içinse astronomik ölçüde bilgi işlem gücüne ihtiyaç vardır.
- Bir kişi ya da kurumun böylesi işlem gücüne sahip olması için, dünyadaki tüm Bitcoin madencilerin sahip oldukları donanımın yarısından fazlasına tek başına hükmetmesi gerekir.
- Teorik olarak ağın hash oranının çoğunluğunu elinde tutan kişi, işlem onay gücüne sahip olur ve çift harcama yapabilir.
- Fakat gerçekleştirilmiş işlemleri geri çevirme gücüne sahip değildirler.
- Olmayan coin'in yaratılması gibi bir durum da söz konusu değildir.

Örnek

- 2014 yılının ocak ayında, “ghash.io” isimli madencilik havuzu bitcoin hesaplama gücünün %42’sine ulaşmıştır.
- Bu olaydan sonra, bir dizi madenci gönüllü olarak havuzdan ayrılmıştır

Double Spending

- Aynı coin ile birden fazla transfer gerçekleştirme girişimine çift harcama denir.
- Normal şartlarda ağ içerisinde düğümler (node) her işlemi doğruladıkları için çift harcamaya karşı koruma sağlarlar.
- Ancak %51 saldırı gerçekleştirilmesi durumunda, onay gücünün çoğunluğu saldırganın elinde olduğu için son işlem bloku geçersiz sayılarak aynı coin ile bir kez daha işlem yapılması mümkün olabilir.

%51 Attack için Gereksinim

- GoBitcoin.io sitesindeki verilere göre Bitcoin ağına %51 saldırısı yapmak için 24 Nisan 2020 itibarıyla 17,5 milyar dolarlık madencilik donanımına ihtiyaç var.
- Bahsi geçen madencilik donanımını çalıştırmak için günde yaklaşık 12 milyon dolarlık elektrik tüketmek gerekiyor.
- Bunca madencilik donanımını kurmak ve güvenliğini sağlamak için tahminen yüzlerce hatta binlerce hektarlık kapalı depoya ihtiyaç var.
- Tüm bu donanımların kurulması, bakımının yapılması ve tabii ki güvenliğinin sağlanması için de on binlerce personel gerekli.

Altcoinlere %51 Attack

- Bitcoin ağının hash gücü astronomik ölçüde olduğundan %51 saldırısı imkansıza yakın olsa da işlem hacmi düşük olan coin'lere bu tip saldırılar yapmak söz konusu.
- 27 Ocak 2020 tarihinde bildirildiği üzere, Bitcoin Gold ağı (BTG) %51 saldırısına uğradı ve 70.000 doların üzerinde BTG'nin iki kez harcanmasına neden oldu.
- Bitcoin'den hard fork işlemi ayrılarak oluşan kripto para birimine, 23 ve 24 Ocak tarihlerinde 10 bloktan fazla düzenleme yapıldı.
- Halving den sonra BCH madenci gücünde yüzde 80'den fazla eksilme oldu.

Zeki Sözleşme Zaafiyetleri

- Blokzincir mekanizmasında çeşitli programlar yürütülmektedir. Bu kullanılan programların barındırdığı hatalardan ve/veya zaaflardan ötürü, zeki sözleşmeler de dolaylı olarak güvenlik zaafları barındırabilir.
- Yapılan bir çalışmada, zeki sözleşmelerde ortaya çıkabilecek 12 farklı güvenlik zafiyeti incelenmiştir ve bu güvenlik zafiyetlerinin hangi sebepten ötürü ve hangi seviyede ortaya çıktıkları belirtilmiştir.
- Ethereum zeki sözleşmelerdeki hataları tespit etmek için açık kaynak kodlu bir program olan “Oyente” geliştirilmiştir
- Solidity ve Assembly dili ile yazılır.
- ‘Kod Kanundur’ prensibine göre çalışır.
- 3 temel ögesi vardır. imzacı, anlaşmanın konusu, şartlar (kurallar, ödüller , cezalar) matematiksel olarak tanımlanıp kodlanmalı.

Cüzdan

- Cüzdan olarak online cüzdan veya bilgisayarınızın sabit diskinde bulunacak olan yazılım cüzdanı olarak iki ana gruba ayrılabilecek birçok seçenek mevcut.
- İki seçenek de yüzde yüz güvenli değil; online cüzdanın hacker saldırısına uğraması mümkünken sabit diskinizin de bozulma ihtimali var.

SON