Blok Zincir

Blok zincir teknolojisinin arkasındaki fikir, 1991 yılında bilim adamları Stuart News ve W. Scott Stornetta tarafından dijital belgelerin zaman içinde geriye dönük olarak değiştirilemeyeceği bir hesaplama çözümü olarak tanımlanmaktadır. Sistem, depolama ve zaman damgalı belgeler için güvenli bir şifreli blok zinciri kullanmaktadır ve 1992'de Merkle ağaçlarının dâhil edilmesiyle, birkaç blok tek bir blokta toplanarak sistemi daha verimli hale getirmektedir. Ancak, bu teknoloji kullanılmamıştır.

Blok Zincir, merkezi olmayan bir işlemsel veri tabanı teknolojisidir. İlk olarak Bitcoin kripto para birimi bu teknolojiyi kullanmaya başlamıştır. Blok Zincir teknolojisinin geçmişi çok daha eski olmasına rağmen bu teknolojiye olan ilgi, Bitcoin'in 2008'de icat edilmesiyle birlikte ciddi artış göstermiştir. Blok Zincir teknolojisine olan ilgi, merkezi olmayan özelliklerinden kaynaklanmaktadır. Bunlar işlemlerin güvenliği, şeffaflığı ve işlemlerin herhangi bir üçüncü şahıs kontrolü olmaksızın veri bütünlüğünün sağlanmasıdır.

Kişiler veya şirketler arasındaki para işlemleri genellikle merkezileştirilir ve üçüncü bir tarafın kontrolünde yönetilir. Bir dijital ödeme veya para transferi işlemini gerçekleştirilmesi için bir banka veya kredi kartı sağlayıcısı gereklidir. Ayrıca, bu dış dâhiller her işlem için ücret alır. Benzer şekilde oyunlar, müzik, yazılım gibi diğer birçok alan için de benzer şekilde uygulanabilmektedir. Mevcut durumda bu süreç tamamen merkezi olarak yürütülmekte; tüm veri ve bilgiler, işlemde yer alan iki taraf dışında üçüncü bir şahıs tarafından kontrol edilip yönetilmektedir. Bu noktada blok zincir teknolojisi aracısız işlem imkânı ile çözüm olarak karşımıza çıkmaktadır. Blok Zincir teknolojisinin amacı işlemlerin ve verilerin herhangi bir üçüncü tarafın kontrolü altında olmadığı merkezi olmayan bir ortam yaratmaktır.

Blok Zincir, sürekli büyüyen veri kayıtlarının bir listesinin depolandığı ve düğümlerin (zincirlerin) birbirine eklenmesiyle doğrulama işleminin gerçekleştirildiği dağıtılmış bir veri tabanı çözümüdür. Veriler, gerçekleştirilen her bir işlemle ilgili bilgilerin kaydedildiği "Dağıtık Defter" içerisine kaydedilir. Blok Zincir ağında gerçekleştirilen işlemlerle ilgili bilgiler herkesle paylaşılır ve tüm düğümler tarafından kullanılabilir. Bu özellik, şeffaflık sağlamakta ve üçüncü bir dış dâhilin kontrolündeki merkezi sistemlerden farklılaşmaktadır. Ayrıca, Blok Zincir ağındaki tüm düğümler anonimdir, bu da diğer düğümlerin işlemleri doğrulamasını daha güvenli hale getirir.

Blok Zincir teknolojisi, alıcı ve satıcı tarafların üçüncü bir tarafın onaylamasına gerek kalmadan birbirleriyle doğrudan güvenli bir şekilde çalışmasını sağlar. Tüm işlemler, kriptografi kullanılarak dağıtılmış bir veri tabanında saklanır, böylece istemci ve sağlayıcı arasındaki bu alışveriş güvenli bir şekilde yapılabilir. Bu dağıtık yapıda, herhangi bir bloğun değiştirilebilmesi için ilgili değişikliklerin sistemdeki tüm bilgisayarlara kaydedilmesi gerekir.

Blok Zincir teknoloji kullanılarak oluşturulan ağa yapılacak herhangi bir siber saldırının başarılı olabilmesi için, bilgisayarların en az %50'sinden fazlasında doğrulanması gerekir, bu da olasılığı neredeyse imkânsız hale getirmektedir.

Literatürdeki başka kaynaklar da göstermektedir ki; blok zinciri, bilgi ve işlemlerin zaman damgalı olarak işlendiği, bloklarda saklandığı ve zincirlerde birbirine bağlandığı, eşler arası bir ağ üzerinden dağıtılarak kullanılan, merkezi olmayan bir veri tabanıdır.

Yeni bir işlem oluşturulduktan ve "blok" olarak eklendikten sonra, bir şifreleme karması tarafından güvence altına alınmadan ve ağın merkezi olmayan düğümlerinde depolanmadan önce, ağın çoğunluğu tarafından doğrulanmalı ve onaylanmalıdır. Daha sonra, her blok bir önceki bloğun karmasına sahiptir, bu yüzden bloklar bu karmalar ile bağlanmaktadır. Oluşan zincirde, doğrulama nedeniyle bilgiler artık değiştirilememektedir ve önceki işlemlerin değiştirilemez oluşu geçmişi temsil etmektedir. Aynı zamanda bir blok zincirde, bulunan iki blok arasına yeni bir blok yerleştirilememektedir.

Yapılan tanımlar ayrıntılarda da olsa farklılıklar göstermektedir. Genel bir tanım olarak Tian; "Blok zincirinin özünün, merkezi olmayan ve güvenilir yöntemlerle topluca tutulan güvenilir bir veri tabanının teknik bir planı" olduğunu belirtmektedir.

Blok zincir teknolojisinin temel aldığı beş önemli unsur bulunmaktadır.

- *Dağıtık Veri Tabanı Yapısı:* Ağdaki her katılımcı, tarihçesi ile birlikte tüm verilere sahiptir. Tek bir kontrol noktası veya merkezi otorite yoktur.

- *Uçtan uça iletişim:* İletişim, merkezi bir düğüm yerine doğrudan eşler arasındadır. Her düğüm bilgileri depolar ve diğer tüm düğümlere iletir.

- *Pseudonymity:* Pseudonymity kavramı blok zincir ile birlikte oluşmuştur. Her işlem ve ilgili değeri, sisteme erişimi olan herkes tarafından görülebilir. Blok Zincir ağı üzerindeki her düğüm veya kullanıcının, onu tanımlayan benzersiz bir adresi vardır. Kullanıcılar anonim kalmayı veya başkalarına kimliklerini kanıtlamayı seçebilirler. İşlemler, blok zincir adresleri arasında gerçekleşir.

- *Kayıtların Değiştirilememezliği:* Veri tabanına bir işlem kaydedildikten ve hesaplar güncellendikten sonra, kendilerinden önce gelen her işlem kaydına bağlantıları sağlandığı için, kayıtların değiştirilebilmesi veya güncellenebilmesi mümkün değildir.

  Veri tabanındaki kaydın kalıcı, kronolojik olarak sıralı ve ağdaki diğer herkes tarafından kullanılabilir olmasını sağlamak için çeşitli hesaplama algoritmaları ve yaklaşımları kullanılır. Herhangi bir siber saldırının başarılı olabilmesi için, bilgisayarların en az %50'sinden fazlasında doğrulanması gerekir, bu da olasılığı neredeyse imkânsız hale getirmektedir.

- *Hesaplama mantığı:* Defterin dijital yapısı, blok zincir ağındaki işlemlerinin hesaplama mantığına bağlanabileceği ve özünde programlanabileceği anlamına gelir. Diğer bir ifadeyle, kullanıcılar düğümler arasındaki işlemleri otomatik olarak tetikleyen algoritmalar ve kurallar oluşturabilir.

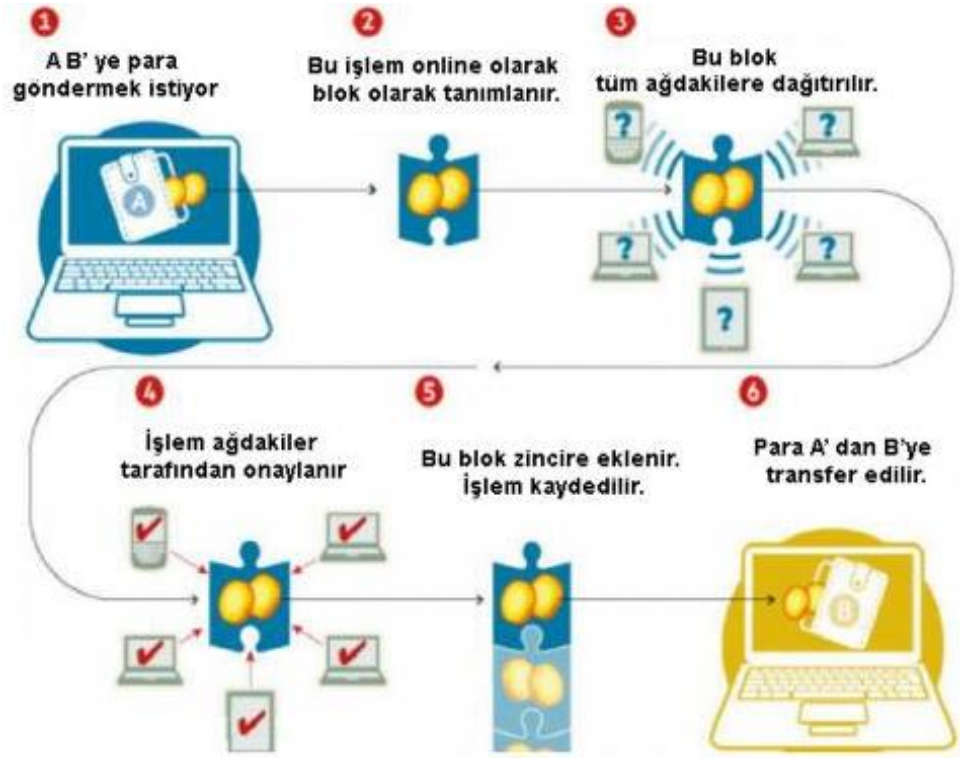
Tüm bu göz alıcı avantajlar göz önünde bulundurulduğunda birçok şirketin blok zincir teknolojisini kullanarak yeni uygulamalar geliştirmeye başladığı görülmektedir. Blok Zincir teknolojisinin siber tehditlere karşı güvenilirliği ve alıcı ile satıcı tarafın güvenli alışveriş yapma talepleri bir araya getirildiğinde blok zincir uygulama alanları ortaya çıkmaktadır.

Blok Zincir teknolojisi kullanılarak birçok farklı alanda uygulamalar geliştirilmektedir. Akıllı sözleşmeler, nesnelerin interneti (IoT) bu alanların en popülerleridir. Bugüne kadar hâlihazırda çok sayıda uygulama geliştirilmiş olup, önümüzdeki dönemde de uygulama sayısının artacağı öngörülmektedir.

Blok Zincir Teknolojisinin İşleyişi

Blok zincir teknolojisini 5 adımda inceleyebiliriz (Şekil 1). İki taraf arasında bir işlem gerçekleşmek üzere olunduğunda öncelikle kayıt defterinde bir teklif hazırlanmaktadır (1.Adım). Bu teklif önerilen işlem tarihini, saatini, gönderen bilgilerini, alıcı bilgilerini, varlık türü ve miktarı gibi temel bilgileri içermektedir. Önerilen işlem, kaydın bütünlüğünü ve orijinalliğini sağlayan benzersiz bir şifreleme imzası ile sağlanmaktadır (2. Adım), daha sonra işleme alma ve kimlik doğrulama için dağıtık vaziyetteki ağ bilgisayarlarına yayın yapılmaktadır (3. Adım). Bu bilgisayarlar işlemi işlemekte ve doğrulamaktadır (4. Adım) ve kimlik doğrulaması yapıldıktan sonra, işlem iki taraf arasındaki varlık transferini tamamlayan dijital deftere eklenmektedir (5. Adım).

Her yeni işlem, daha önce kaydedilen işlemlerle bağlantılıdır ve bu da blok zincirinde yapılan tüm işlemlerin eksiksiz, geri dönüşü olmayan ve doğrulanabilir bir geçmişi olmasını sağlamaktadır.



Şekil 1. Blok Zincir İşleyişi

Her bir blok içerisinde blok başlık özeti, blok sırası, bağlı bulunulan ve bir öncesinde yer alan bloğa ait başlığın özeti, bloğun oluştuğu zamana dair zaman pulu, zorluk değeri, rastgele değeri ve transfer işlemlerine ait değerler bulunmaktadır.

Tüm yapılan işlemler ağda bulunan diğer paydaşlar tarafından takip edilebilmektedir. Yapılan işlemlerin geçerliliği diğer paydaşlar tarafından onaylandıktan sonra işlemler bir araya getirilirler ve böylece yeni bloklar oluşturulur. İşlem gören blok bir önceki geçerliliği onaylanmış blokla ilişkilendirildikten sonra, ağdaki tüm paydaşlar bu yeni bloğu yerel veri tabanlarına ekleyerek senkronize olmaktadır.

Blok Zincir Teknolojisi ve Veri Akışı

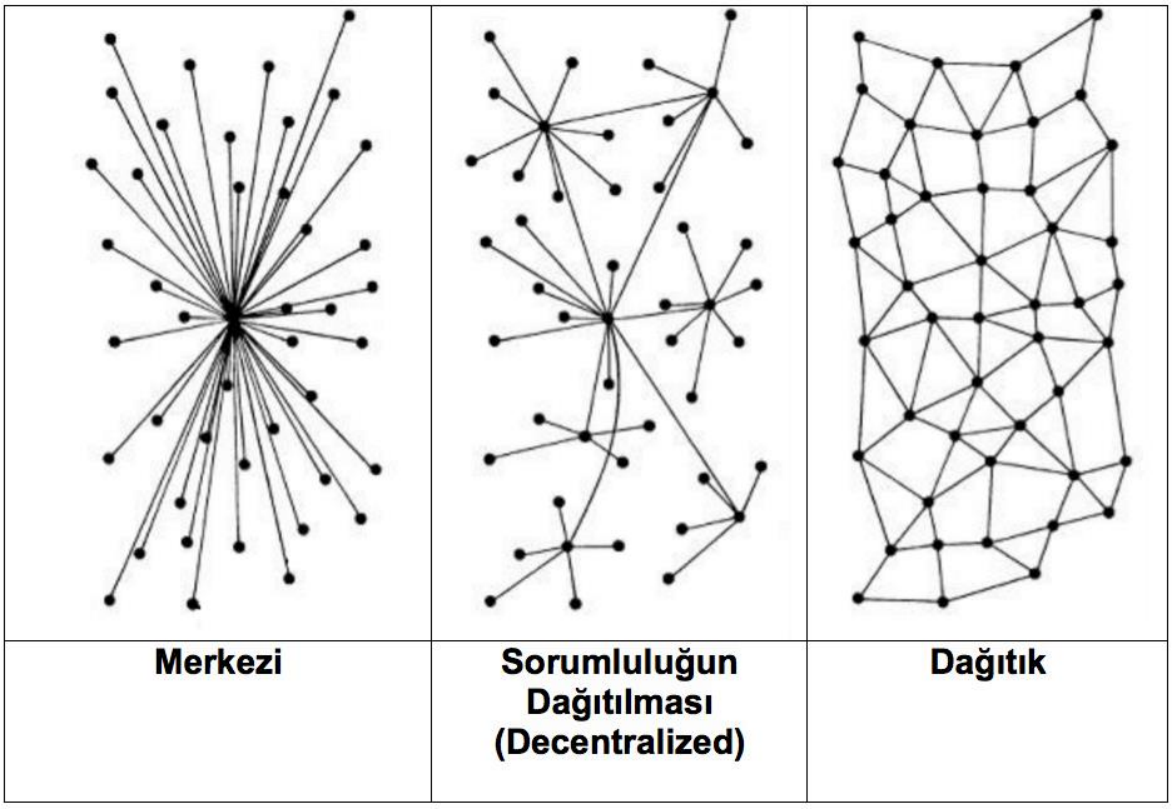
Blok zinciri teknolojisi, matematik bilimi ve kriptoloji kavramından yararlanarak merkezi bir otoriteye gerek duymadan ortaya çıkmış bir güven mekanizmasıdır. Basit bir ifadeyle, blok zinciri yapısı bir bilgisayar ağı gibi işlem görür ve burada bilgisayar sahipleri bu ağ yapısının temel yapı taşlarını oluşturur. Diğer bir deyişle bu teknoloji uçtan uca ağlar arasında gerçekleşen bütün işlemleri kapsayan verileri kaydeden bir açık ve dijital defterdir.

Merkezi Veri Tabanı (Centralized Database) tüm verilerin tek bir mantıksal merkezde toplandığı veri tabanıdır. Bu sayede veri iletişimi yöntemleri ile bilgisayarlar arasında fiziksel olarak yaygınlaşmaktadır. Fakat verilerin tek bir merkezde olması siber güvenlik açısından oldukça riskli olmaktadır.

Merkezi Olmayan Veri Tabanı (Decentralized Database) verilerin belirli bir sınıflandırmaya göre farklı veri tabanlarına ayrılarak depolandığı veri tabanıdır. Verilere ulaşmak için çeşitli yönlendirmeler kullanılmaktadır ve bu nedenle merkezi veri tabanına kıyasla hem daha güvenli hem de daha az iş yükü getiren bir tür olmaktadır.

Dağıtık Veri Tabanı (Distributed Database) verilerin parçalara ayrılarak farklı sunucularda barındırıldığı veri tabanıdır. Aynı anda daha fazla veri işlenebildiği ve istekleri daha hızlı karşıladığı için dağıtık yapılar en verimli veri tabanı çeşidi olmaktadır. Güvenlik açısından dağıtık yapılar diğer türlere göre bir adım öndedir çünkü verilerin tamamının ele geçirilmesi için tüm sunucuların art niyetli kişilerin eline geçmesi gerekmektedir.

Şekil 2'de Merkezi, Merkezi Olmayan ve Dağıtık Yapılar görsel olarak verilmiştir.



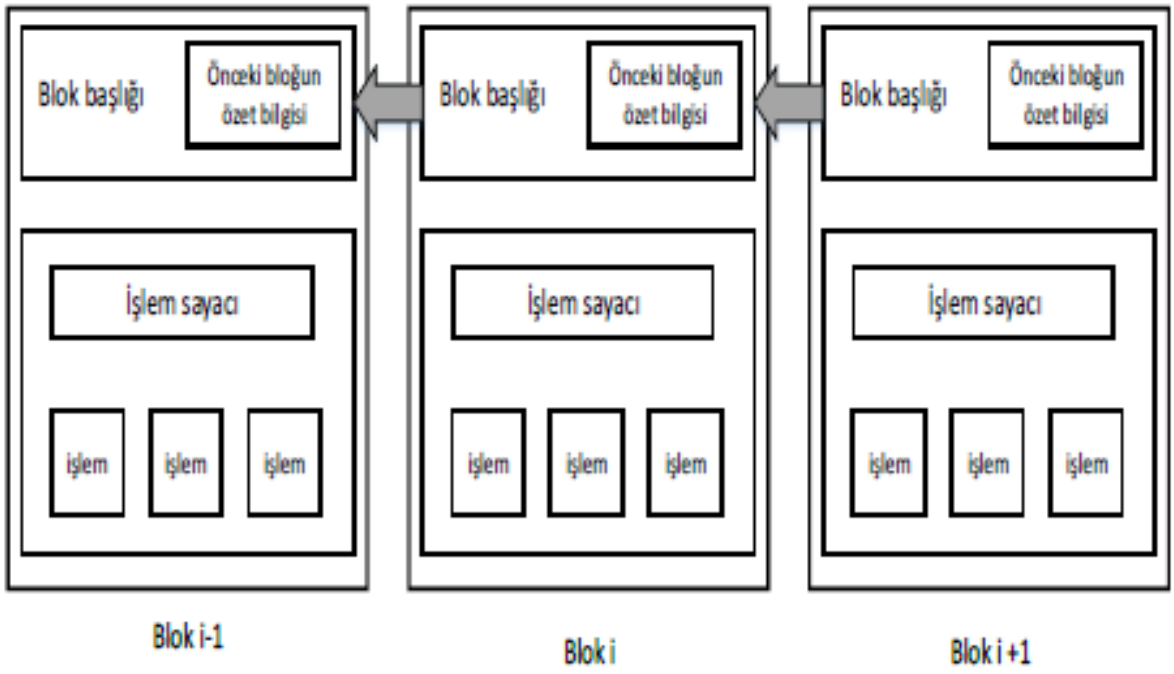
Şekil 2. Merkezi, Merkezi Olmayan ve Dağıtık Yapılar

Merkezi bir sisteme bağlı olmayan blok zincir ağında, madenciler sistemin bağlı olduğu kurallar çerçevesinde eşit şartlarda varlığını sürdürmeye ve veri paylaşımı yapmaya devam edebilmektedir. Bu zincirde herhangi bir madencinin girmiş olduğu hatalı veya eksik veri bütün ağı etkilemez. Çoğunluk eğer ağın kural yapısına göre hareket ederse sistem bozulmadan devam etmektedir.

Blok zinciri altyapısı açık kaynak kodludur ve herhangi bir merkezi sistem tarafından yönetilmemektedir. Sistemde güvenilir bir aracı yoktur ve işlem onay mekanizması dağıtıktır. Blok zinciri ağı üzerinde yer alan bilgisayarlar birer düğüm (node) olarak adlandırılmakta ve birbirleri ile uçtan uca bağlı olmaktadırlar. Ağda yer alan düğümlerin hiçbiri güvenilir olmak zorunda değildir ve birbirlerine herhangi bir üstünlükleri yoktur.

Blok Zinciri Mimarisi

Blok zinciri, defteri kebir gibi gerçekleşen tüm işlemlerin kayıtlarının tutulduğu sıralı bloklardan oluşmaktadır. Blok zinciri yapısının bir örneği Şekil 3' te gösterilmektedir. Bir blok sadece bir ana bloğa sahiptir ve her bloğun üst bilgisinde önceki bloğun özet bilgisi yer almaktadır. Blok zincirinin ilk bloğu, bir ana bloğu olmayan genesis blok olarak adlandırılır.



Şekil 3. Blok Zinciri Yapısı

Blok (Block)

Bir blok Şekil 4'te gösterildiği gibi bir başlık ve bir gövdeden oluşmaktadır. Blok başlığında bulunan bilgiler şu şekildedir;

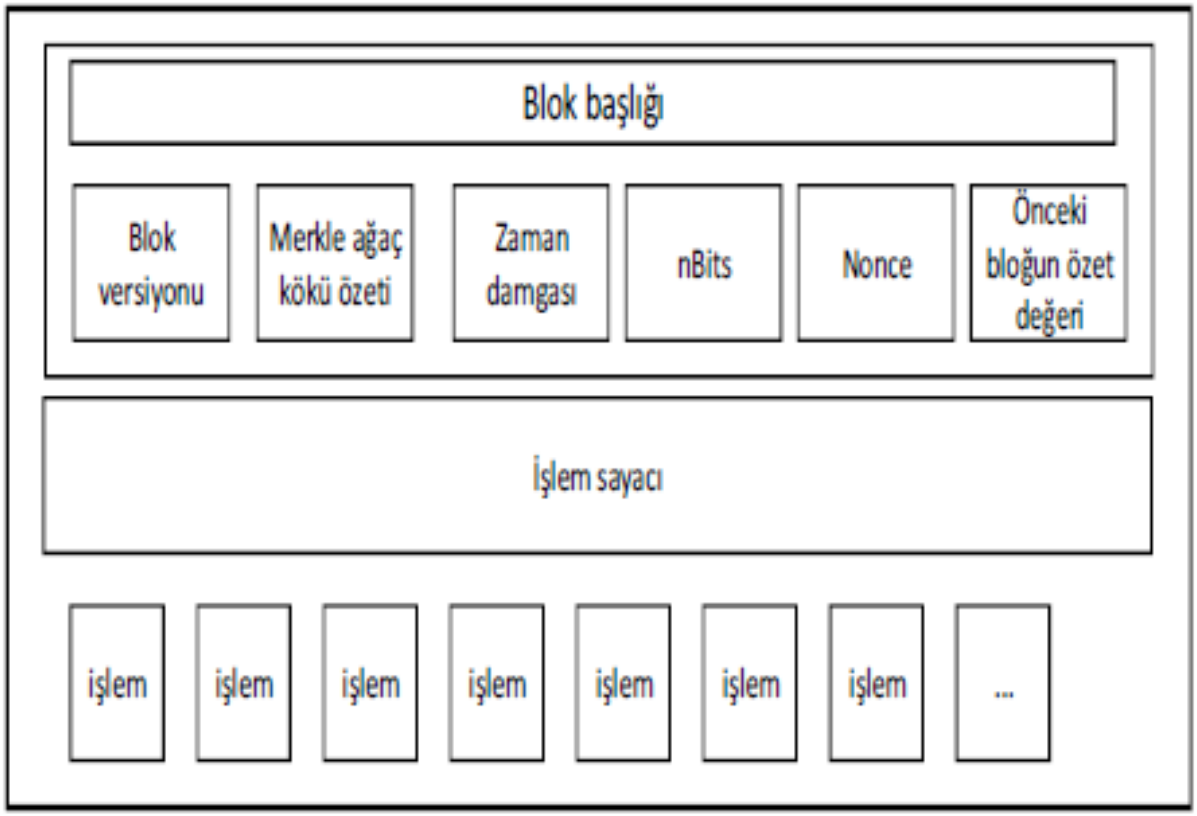
- Blok versiyonu, hangi blok doğrulama kurallarının uygulanacağını belirler.
- Merkle ağaç kökü özeti, bloktaki tüm işlem kayıtlarının özet değerini tutmaktadır.

- Zaman damgası, 1 Ocak 1970 tarihinden beri evrensel zamanda saniye olarak geçerli zaman bilgisini tutmaktadır.

- Nbit, geçerli bir blok özet değeri için eşik değer bilgisi içermektedir.

- Nonce, genellikle 0 ile başlayan her bir hesaplama için artan 4 byte boyutunda bir alandır.

- Önceki blok özet değeri alanında zincirde bir önceki bloğa karşılık gelen 256 bit boyutunda bir özet değer tutulmaktadır.



Şekil 4. Blok Yapısı

Blok gövdesi, gerçekleşen işlem kayıtlarından ve bir işlem sayacından oluşmaktadır. Bir bloğun içerebileceği maksimum işlem sayısı, blok büyüklüğüne ve her bir işlemin büyüklüğüne bağlı olarak değişebilmektedir. Blok zincirinde işlemlerin doğrulanmasını onaylamak için asimetrik bir şifreleme mekanizmasına dayalı dijital imza kullanılmaktadır.

İşlem/Hesap Hareketi

Bilgi bloklarının içerisinde tutulan veriler, hesap defter girişini ya da hesap hareket kayıtlarını (işlemleri) temsil etmektedir. Her hesap hareketinin dijital olarak imzalanarak gerçekliğinin korunması sağlanmaktadır. Böylece kayıt üzerinde kimse değişiklik yapamaz ve verinin güvenilir olduğu varsayılır. Blok zincir ağında terminaller arasındaki varlık transferlerinin kayıtlarına işlem denir. Bu işlemler blokların gövdesinde saklanır. Temel olarak bir işlem; Toplam Miktar, Girdi Listesi, Çıktı Listesi, Özet Değeri bilgilerinden meydana gelir;

- Toplam miktar, transfer edilecek dijital varlıkların toplam miktarı bilgisini tutar,

- Girdi listesi bilgi olarak transfer edilecek varlıkların listesini, miktarlarını ve gönderici hesap adresini tutar,

- Çıktı listesi bilgi olarak transfer edilecek varlıkların miktarlarını, alıcı adresini ve yeni sahiplerini tutar,

- Özet Değer, işlem içeriğinin hesaplanmış kriptografik özet değeridir. Özet değer kullanılarak, saklı anahtar ile işlemler imzalanır ve göndericinin açık anahtarı kullanılarak doğrulanır.

Hesap Adresleri

Blok zincirinde yer alan bir işlemde, gönderici ve alıcının hesap adresleri yer almaktadır. Sisteme dâhil olan her yeni kullanıcı için yeni bir adres üretilir. Bu adresler blok zincir sisteminde kullanıcıların kimlikleri niteliğindedir. Kullanıcının açık anahtarları kullanılarak hesap adresleri oluşturulur.

Bu adreslerde, dijital bir varlığın sahiplik bilgisi tutulur. Bir kullanıcının sahip olduğu dijital varlığı kullanarak işlem yapabilmesi için, o hesaba ait saklı anahtarının olması gerekir. Çünkü işlemlerin, kullanıcının saklı anahtarı ile imzalanmış olması gerekmektedir. Yaratılan bu işlemin doğrulanmasında hesap adresinden oluşturulan açık anahtar kullanılmaktadır.

Kayıt Defteri/Hesap Defteri

Veriler, her terminalde yer alan herkese açık hesap defterlerinde tutulmaktadır. Bu hesap defterleri içerisinde blok zincir ağında oluşturulan ve doğrulanan işlemler yer almaktadır. Sistem güvenliği, dijital hesap defterlerinin bir altyapı ya da ağ üzerinde dağıtılmasıyla sağlanmaktadır. Altyapıdaki bu ek katmanlar, bir hesap hareketinin durumu ile ilgili istenilen her an mutabakat sağlanabilmesi amacına hizmet etmektedir. Her katmanda, gerçekliği korunan hesap defterlerinin kopyası yer almaktadır.

Sisteme yeni bir hesap hareketi geldiğinde ya da mevcut bir işlemde değişiklik yapıldığında, altyapıda yer alan tüm kayıtlarda belirli bir algoritma çalışarak bu yeni işlemin doğruluğunu kontrol etmektedir. Hesap defterleri kopyalarının çoğunluğu bu kaydın doğruluğunu onaylarsa, yeni bir blok sisteme dâhil edilmektedir. Eğer sistemdeki kopyaların çoğunluğu yeni işlemi reddederse, bu hesap hareketi sistem üzerine kaydedilemeyecektir. Bu dağıtık sistem sayesinde, Blok zinciri merkezi bir yapı ile kontrol edilmeden etkili bir şekilde çalışmaktadır.

Cüzdan

Kişilerin saklı anahtarları çok önemlidir. Dijital varlıkların güvenliği için bu anahtarın çok sağlam ve güvenli bir şekilde saklanması gerekmektedir. Cüzdan, bu anahtarların saklandığı uygulamalardır. Cüzdanlar, ek olarak kullanıcıya ait dijital varlık bilgilerini ve açık anahtarı da gösterir. Uygulama, yerel diskler üzerinde ya da bulut içerisinde yer alır.

Kriptografik Hash Fonsiyonu

Kriptografi, kısaca bir verinin şifrelenmesi anlamına gelmektedir. Bu şifreleme işlemi, karmaşık olan birçok gelişmiş matematiksel tekniği kullanan derin bir akademik araştırma alanını kapsamaktadır. Burada bilinmesi gereken ilk şifreleme tekniği temel bir şifreleme olan hash işlevidir. Hash birçok kaynak ve uygulamada İngilizce olarak kullanılsa da Türkçe karşılığı itibariyle bilişim dünyasında özetleme olarak ifade edilmektedir. MD-5, SHA-1, SHA-2, SHA-3, BLAKE gibi farklı özetleme algoritmaları bulunmaktadır. Bir hash, üç temel özelliğe sahip matematiksel yöntemdir.

- Girdi verileri herhangi bir boyutta herhangi bir dize olabilir,
- Sabit boyutta bir çıktı üretmektedir. Örneğin; 64, 128, 256 bit çıktı boyutu,
- Verimli olarak hesaplanabilmektedir. Sezgisel olarak, belirli bir girdi dizgesi için, hash çıktısının makul bir süre içerisinde ne olduğunu bulabileceğiniz anlamına gelmektedir.

Bir kriptografik işlem özet fonksiyonun da $H{:}\{0,1\}* \rightarrow \{0,1\}n$ herhangi bir istenilen uzunluktaki mesaj olan M için n bitlik bir sabit uzunlukta hash değerini hesaplayan bir fonksiyondur. Kriptografik hash fonksiyonu, dijital imza şemaları, kimlik doğrulama kodları, parola işlem özet fonksiyonları ve içerik adresli depolama da dâhil olmak üzere pek çok uygulamada kullanılan temel bir kriptografi yöntemidir. Bu uygulamaların birçoğunun güvenliği veya düzgün işleyişi, kırılmasının (çarpışmaların bulunmasının) pratik olarak mümkün olmadığı varsayımına dayanmaktadır. Güvenli Hash Algoritması (SHA-Secure Hash Algorithm), bir dizi kriptografik hash işlevinden oluşmaktadır.

Özetle kriptografik hash, bir metin veya veri dosyası için bir imza gibidir. SHA-2 Hash Algoritmasının, 6 farklı fonksiyonundan biri olan ve yüksek güvenliğe sahip olanı SHA-256 algoritmasıdır. Bu algoritmada farklı boyut ve büyüklükteki yazı, sayı veya değişik formattaki bilgisayar dosyası verileri, tek yönlü olmak üzere standart büyüklükte, 256 bit (32 byte-64 hexadecimal) boyutunda özetleme değerlerine dönüştürülmektedir. Aynı veri için hesaplanan SHA-256 değeri her zaman aynı sonucu vermektedir ve sadece veri de değişikliği olması durumunda sonuç özetleme değeri değişmektedir.

Merkle Tree (Ağacı)

İngilizce ifadesiyle Merkle Tree, Merkle Root veya Root Hash, Türkçe ifadesiyle ise Merkle Ağacı, Merkle Kökü veya Kök Özet tanımları aynı anlamda kullanılmaktadır. Genel anlamda, Merkle Ağacı büyük veri yığınlarının bir araya getirilip özet olarak gösterilmesi ve bunun güvenli bir şekilde doğruluğunun sağlanabilmesidir.

Çalışma prensibi açısından bir ağacın yapısına benzemektedir. Ağacın yaprakları veri bloklarını temsil etmekte, bu veri blokları özetleme fonksiyonundan geçirilerek özet değerleri oluşmakta ve bunlar da ağacın dallarını temsil etmektedir. Oluşan özet değerlerde tekrar özetleme fonksiyonlarından geçirilerek yeni özet değerler elde edilir. Bu döngü aynı şekilde devam ederek en son kök özet değerine ulaşılır. Bu da ağacın köküne ulaşmak olarak yorumlanmaktadır.

Blok Zinciri Sistemlerinin Sınıflandırması

Mevcut blok zinciri sistemleri Genel Blok zinciri, Özel Blok zinciri ve Konsorsiyum Blok zinciri olmak üzere üç kategoride sınıflandırılmıştır.

Genel (Public) Blok zinciri: Genel Blok zinciri, çeşitli kurumlara bağlı ya da bağımsız kişilerin katılımına, kayıt eklemesine ve madencilik yapmasına imkân veren açık bir platform sunmaktadır. Bu tür blok zincirlerinde herhangi bir kısıtlama yoktur ve bu yüzden izinsiz blok zinciri olarak da adlandırılır. Genel Blok zincirleri tamamen açık ve şeffaftır ve herhangi bir özel doğrulayıcı düğüm barındırmamaktadır.

Blok zincirinde isteyen herkesin tüm zincir verilerini indirip madenciliğe başlayabilmesi, zincirin birçok aktif kopyasının olmasını sağlamaktadır. Bu da blok zincirin güvenliğini ve tutarlılığını arttırmaktadır. Bu şekilde herhangi bir kontrol mekanizması olmayan dağıtık yapılarda mevcut ağdaki veri boyutunun büyümesinden dolayı zincirde bir değişiklik yapılması sırasında uzlaşma protokollerine çok iş düşmektedir.

Özel (Private) Blok zinciri: Bir ya da birkaç organizasyondaki kişiler arasında paylaşım ve veri alışverişini sağlayan, bir kişi ya da grup tarafından yönetilen blok zinciri yapılarına Özel Blok zinciri denmektedir. Özel bir izni olmayan kişilerin zincire katılamadıkları için izinli blok zinciri olarak da adlandırılabilir.

Ağa bir düğümün katılımı ve erişimi, ağı yöneten grup tarafından belirlenen kurallara göre yapılmaktadır. Bu da blok zincirinin merkezi olmayan ve şeffaf yapısına uygunluğu azaltmaktadır.

Konsorsiyum (Consortium) Blok zinciri: Konsorsiyum Blok zinciri, blok doğrulama ve uzlaşma işlemlerinde tek bir organizasyonun yerine önceden belirlenmiş bir grup düğümün karar verici olarak yer aldığı kısmen özel ve izinli bir blok zinciri olarak tanımlanabilir. Kimlerin ağa katılabileceğine ve kimlerin madencilik yapabileceğine bu düğümler karar vermektedir.

Blok doğrulaması için, bir bloğun sadece yetkili düğümler tarafından imzalanmışsa geçerli sayıldığı çoklu bir imza şeması kullanılır. Ağın herkese açık olması ya da sınırlı olmasına ve ağdaki herkesin veri okuma ve yazma işlemlerine sahip olma durumlarına bir konsorsiyum tarafından karar verilir.

	Genel Blokzincir	Konsorsiyum Blokzincir	Özel Blokzincir
Uzlaşma sağlayıcılar	Bütün madenciler	Seçilmiş düğümler	Bir organizasyon
Okuma izinleri	Açık	Açık veya izinli olabilir	Açık veya izinli olabilir
Verimlilik	Düşük	Yüksek	Yüksek
Merkeziyetçilik	Hayır	Kısmen	Evet
Uzlaşma işlemlerine katılım	İzinsiz	İzinli	İzinli

Tablo 1. Genel, Özel ve Konsorsiyum Blok Zincirlerinin karşılaştırılması

Tablo 1'de Genel, Özel ve Konsorsiyum blok zincirlerinin uzlaşma sağlayıcılar, katılımcıların veri okuma izinleri, verimlilik, merkeziyetçilik ve uzlaşma işlemlerine katılım durumlarına göre karşılaştırılmasına yer verilmiştir.

Blok Zincir Kullanım Alanları

Blok zincirin uygulama alanlarının bankacılık, borsa, akıllı sözleşmeler, tıp, eğitim, ağ teknolojisi, nesnelerin interneti, havayolu taşımacılığı ürün tedariki ve lojistiği olduğunu söyleyebiliriz.

Bu açıdan bakıldığı zaman her geçen gün uygulama alanı artan blok zinciri teknolojisini tedarik zinciri süreçlerine uygulamak ve tedarik zinciri performansını arttırmak amaçlanmaktadır. Şekil 5'de blok zincirin uygulama alanları belirli başlıklar altında kapsamlı bir şekilde gösterilmiştir.

Şekil 5. Blok Zinciri Uygulama Alanları

Blok zinciri teknolojisi ile ilgili bahsedilen açıklamaları genel olarak değerlendirmek gerekirse bu teknoloji mevcut iş akışlarının karmaşıklığını yönetebilecek ve ürün güvenliği ve sürdürülebilirliği konusunda erişilebilir bilgi sağlayabilecek bir dijital kayıt tutma mekanizmasıdır.

Blok zincirin küresel iş akışlarında izlenebilirlik, şeffaflık ve daha iyi koordinasyon oluşturarak iş dönüşümünü sağlama ve sürdürülebilirliği arttırma potansiyeli üzerine yapılan birçok araştırma mevcuttur. Ayrıca bu teknolojinin kullanım yaygınlığı arttıkça taraflar arasındaki işlem maliyetlerinin de büyük ölçüde azalarak iyileşeceği öngörülmektedir.

Gelişim süreci devam eden Blok Zincir'in Şekil 6'da teknolojisinin ortaya çıkışından başlayarak yakın gelecekteki gelişim evreleri ve hangi boyutlara ulaşacağı gösterilmiştir.

Şekil 6. Blok Zinciri Teknolojisinin Geleceği

Blok zincirinin avantajları;

- Verilerin bir kopyası tüm paydaşlar tarafından kaydedilir, herkes bu verilere erişebilir ve yapılan işlemleri görebilir. Verilerin bu şekilde saklanması sayesinde veri kaybı ve veri tahribatı önlenir.

- Dijital imza ve doğrulamalar sayesinde aracılara ihtiyaç duymadan paydaşlarını birbirine güvenmesini sağlanır.

- Herkes hem kendi işleminin durumunu hem de blokzincirindeki tüm işlemlerin ayrıntılarını görebilir, bu şekilde şeffaflık sağlanmış olur.

- Blokzinciri üzerindeki veriler değiştirilemez veya silinemez.

- Merkezi bir otorite olmadan çalışabilir, bu dağıtık yapısı sayesinde kontrol edilemez, iptal edilemez veya kapatılamaz.

- Akıllı sözleşmeler sayesinde belirli faaliyetler otomatikleştirilebilir.

Blok zincirin dezavantajları;

- Uzlaşma protokolü olarak proof of work (işin ispatı) kullanılan blok zincirlerinde çok fazla enerji tüketilmekte ve çok pahalı bilgisayar sistemleri çalıştırılmaktadır.

- Blok zincirindeki tüm veriler her bir düğümde ayrı ayrı saklanmaktadır ve her bir işlem sonrası bu düğümlerdeki verilerin tutarlılığı sağlanmaktadır.

  Örneğin zincire bir blok eklemek Bitcoin zincirinde 10- 60 dakika Ethereum zincirinde ise 15 saniye zaman almaktadır. Bu nedenle geleneksel veri tabanları ile performans bakımından kıyaslandığında yetersiz kalmaktadır.

- Ağdaki her bir düğümün tüm verilerin bir kopyasını saklayabilmesi ve içeriğine erişebilmesi, kullanıcıların mahremiyetine zarar verebilir.

- Akıllı sözleşmeler bir kez oluşturulduktan sonra değiştirilemez ve blok zincirinde herkesin erişimine açık halde saklanır. Bu da akıllı sözleşmeleri kötü niyetli saldırılara karşı savunmasız bırakabilir.

Kaynaklar

Mendi, A. F. (2021). Blokzincir Uygulamaları ve Gelecek Öngörüleri. *GSI Journals Serie C: Advancements in Information Sciences and Technologies*, *4*(1), 76-88.

Örnekler, Ş. (2021). Tedarik zincirinde blok zincir teknolojisi ve uygulamaları.

Tanrıverdi, M., Uysal, M., & Üstündağ, M. T. (2019). Blokzinciri teknolojisi nedir? ne değildir?: alanyazın incelemesi. *Bilişim Teknolojileri Dergisi*, *12*(3), 203-217.

Tektaş, B., & Kırbaç, G. (2020). Lojistik Sektöründe Blokzinciri Teknolojisinin Kullanılmasına Yönelik Bir Vaka Analizi İncelemesi Ve Lojistik Şirketi Uygulaması. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, *25*(3), 343-356.