Blok Zinciri Bileşenleri ve Uygulamaları Üzerine Bir Derleme

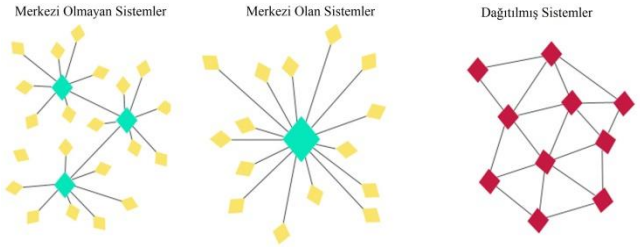
Sedat Akleylek[1], Kübra Seyhan[2]
[1,2]Ondokuz Mayıs Üniversitesi, Samsun, Türkiye
[1]*sedat.akleylek@bil.omu.edu.tr*, [2]*kubra.seyhan@bil.omu.edu.tr*

Özet. Blok zinciri teknolojisi, merkezi sistemlerin güvenilir aracıya duyduğu ihtiyaç sonucu daha güvenilir ve aracısız sistemlere olan arayış ile ortaya çıkmıştır. Blok zinciri teknolojisinin dağıtık ağ yapısı, uçtan-uca iletişim mantığı, içermiş olduğu özet değeri hesabı ve elektronik imzalama gibi kriptografik işlemler blok zinciri teknolojisini birçok çalışma alanı için tercih edilebilir kılmıştır.Enerji ve finans sektörleri, e-devlet teknolojisi, bulut depolama sistemleri gibi birçok alanda hızlı ve güvenli işlem yapmaya olanak sağlayan blok zinciri teknolojisi günümüzde işlemsel veri paylaşımı konusunda etkin bir şekilde kullanılmaktadır. Bu çalışmada blok zinciri teknolojisinin çalışma sistematiği açıklanarak teknolojininsahip olduğu özellikler kriptografik işlemler temel alınarak detaylandırılmıştır. Ayrıca blok zinciri teknolojisinin karakteristiği ve türlerine dair özellikler açıklanarak blok zinciri teknolojisinin özelliklerinden dolayı sistemlere sağlayacağı avantaj ve dezavantajlara yer verilmiştir. İzinli blok zinciri HyperledgerFabric ve izinsiz blok zinciri Bitcoin teknolojilerine dair araştırma sonuçları sunularak blok zinciri teknolojisinin bir sisteme uygunluğuna karar verilirken değerlendirilmesi gereken parametreler açıklanmıştır.Son olarak blok zinciri teknolojisine dair gelecek çalışmalara kaynaklık edecek, güncel gelişmeler sonucu ortaya çıkan bazı problemlere yer verilmiştir.

Anahtar Kelimeler: Blok Zinciri, Bitcoin, HyperledgerFabric

1. Giriş

Blok zinciri güvenilir olmayan katılımcıların bulunduğu geniş bir ağda merkezi olmayan ve işlemsel veri paylaşımı için gelişmekte olan bir teknoloji olarak değerlendirilir. Veri yapısı olarak blok zinciri, her bloğun küçük bir işlem listesi içerdiği sıralı bir blok yapısıdır[3]. Blok zinciri ismini her bir bloğun bir önceki bloğa kriptografik özet değeri ile bağlı olduğu zincir yapısından alır. İşlemler blok zincirinde bulunan her bir düğüm tarafından oluşturulabilir ve değiştirilebilir özelliktedir.Blok zincirleri dağıtılmış defter sistemleridir. Başka bir deyişle, bilgi tek ve merkezi bir veritabanında değil, potansiyel olarak sonsuz sayıda yerde saklanabilir. Blok zinciri veri depolama sağlarken şeffaflık ve bütünlük garantisi verir, güvenilir 3. tarafa olan ihtiyacı ortadan kaldırır. Bu özelliklerinden dolayı bir blok zinciri dağıtılmış bulut depolama, tedarik zinciri yönetimi, sağlık, mülkiyet ve telif dağıtımı, seçim oylarının kaydedilmesi gibi alanlarda ilgi görmeye başlamıştır [1]. Veritabanı sistemlerinde durumu veritabanına yazacak bir yazar belirlenir. Blok zincirinde ise belirlenen anlaşma protokolünde yer alan ve blok zincirinin büyümesine olanak sağlayabilen herhangi bir katılımcı veritabanındaki yazara karşılık gelir. Blok zincirindeki her bir yazar, bir blok içerisinde bulunan işlemleri biriktirebilir, ilgili bloğu zincire ekleyebilir ve ağda doğrulayıcı olarak görev yapabilir özelliktedir. Blok zincirinde bulunan okuyucu ise blok zincirini boyutunu değiştiremezken işlem oluşturma sürecine katılabilme özelliğine sahip olur. Ayrıca okuyucu, sadece blok zincirini okuyabilir, analiz edebilir ya da denetleyebilir özelliktedir [1]. Blok zinciri belirlenen ağda bulunan katılımcılar arasında yürütülen işlemleri kaydeden ve ağ üzerinde dağıtılan açık bir defter özelliği gösterir. Şekil 1'de dağıtılmış sistem bağlantılarının nasıl olduğu gösterilmiştir.



Şekil 1. Sistemler ve Ağ Bağlantıları

Ağdaki her bir işlem blok zincirine eklenmeden önce belirlenen anlaşma protokolüne göre ağda bulunan düğümler tarafından doğrulanır. Kayıtlı olarak belirlenen bilgiler değiştirilemez ve silinemez. Her işlemin geçmişi istenilen herhangi bir zamanda yeniden oluşturulabilir özelliktedir [2].

Literatürde yapılan çalışmalar incelendiğinde Wüst ve Gervais [1] nolu çalışmada blok zinciri türlerini analiz ederek bunların merkezi olarak yönetilen bir veritabanına göre karşılaştırmalarını analiz etmiştir. Ayrıca blok zinciri teknolojisinin probleme faydalı bir çözüm olup olmayacağını belirleyebilmek için bir yöntem sunmuştur. Bununla birlikte var olan bir problemin çözümünde hangi tür blok zincirinin tercih

DOI: 10.25045/NCInfoSec.2018.05

edilmesi gerektiğine dair fikirlerini yapılan çalışmada bildirmiştir.

[2] nolu çalışmada Gatteschi ve arkadaşları blok zinciri teknolojisinin çalışma sistematiğinin nasıl olduğu üzerinde durmuştur. Diğer çalışmalardan farklı olarak blok zincirinin sahip olduğu avantaj ve dezavantaj özelliklerine değinilmiştir. Ayrıca blok zincirinin evrimsel süreci ve potansiyel uygulama alanları konularının incelendiği gözlemlenmiştir.

Xu ve arkadaşları [3] nolu çalışmada blok zinciri teknolojisinin temel özellikleri ve sistemin çalışma mantığı üzerinde durmuştur. Ayrıca çeşitli blok zincirlerinin mimari açıdan önemli özelliklerini sağlayan bir model önerilmiştir.

Blok zincirinin web teknolojileri üzerindeki etkisi değerlendirildiğinde, English ve arkadaşları [4] nolu çalışmada anlamsal web ile ilgisi bağlamında blok zincir teknolojisinin objektif bir analizini yapmıştır. Ayrıca Bitcoin blok zincirinin fonksiyonel temellerinin tanımı konularına değinilmiştir.

Gaetani ve arkadaşları ise [5] nolu çalışmadabulut bilişim ortamlarının gerçek veri bütünlüğü ihtiyaçlarını ve blok zincir tabanlı sistemleri benimsemek için ele alınan araştırma sorunlarını açıklamıştır. Ayrıca bulut bilişim ortamları için etkili bir blok zinciri tabanlı sistem ön tasarımı önerilmiştir.

A. Motivasyon ve Amaç

Blok zinciri teknolojisinin sağlamış olduğu faydalar ve kriptografik özellikleri göz önüne alındığında birçok farklı uygulama alanında kendine yer bulmuştur. Enerji sektörü, ekonomi sektörü, e-devlet teknolojisi, bulut depolama, mülkiyet ve telif dağıtımı gibi alanlar blok zinciri teknolojisinin kendine yer bulduğu alanlara örnek olarak gösterilebilir. Birçok uygulama alanında kendisine yer bulan blok zinciri teknolojisine dair bilgi paylaşımını sağlamak bu çalışmada temel amaç olarak belirlenmiştir. Ayrıca yapılan bu çalışma ile blok zinciri teknolojisinin genel özellikleri, alt yapısı, çalışma sistematiği,blok zinciri teknolojisinin sağlamış olduğu avantaj ve dezavantajlar, blok zincirinin kriptografik anlamdaki bileşenleri, uygulama alanında kullanıma geçen çeşitli parametrelerinin detaylandırılmasıve blok zinciri teknolojisinin bir probleme uygunluğunu içeren bir derleme çalışması gerçekleştirilmiştir.

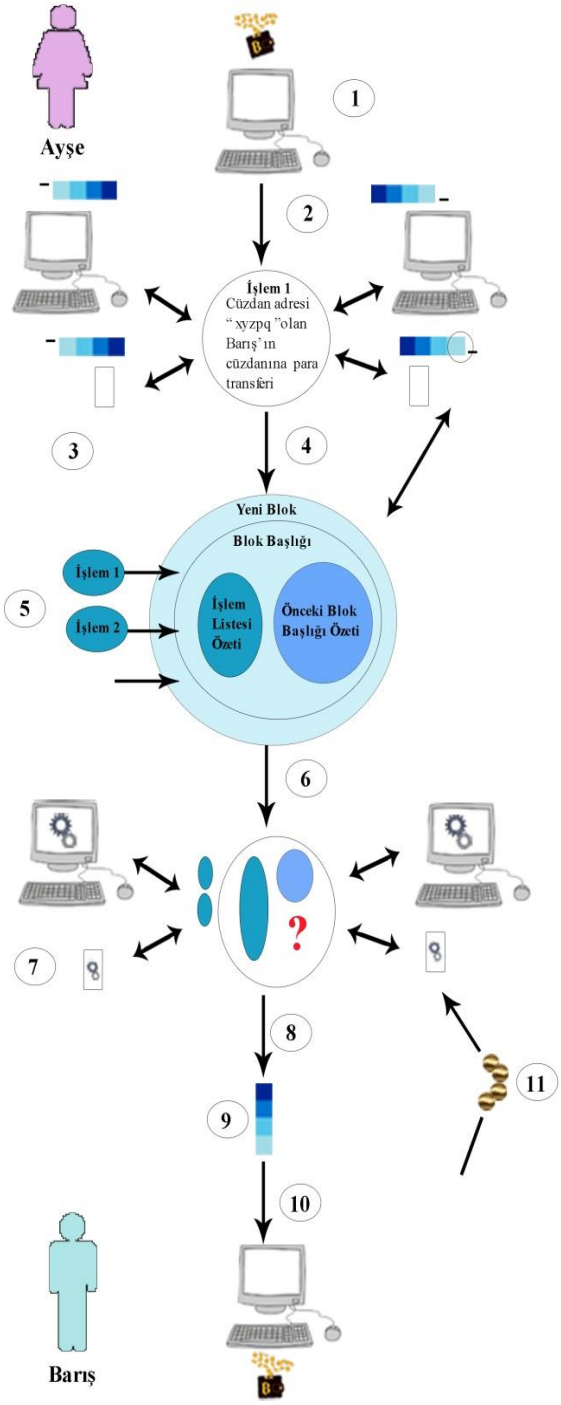
B. Organizasyon

Bu çalışmada, Bölüm 1’de blok zincirine dair çeşitli çevreler tarafından yapılan tanımlara değinilerek blok zinciri teknolojisinin alt yapısına dair bilgilereyer verilmiştir. Ayrıca literatürde incelenen çalışmalar hakkında özet bilgiler sunularak çalışmada amaçlanan yapı belirtilmiştir. Bölüm 2’de blok zinciri teknolojisinin çalışma sistematiği açıklanmıştır. Bölüm 3’de blok zincirinin temel özellikleri, sahip olduğu alt yapıdan kaynaklanan ilave özellikler, blok zinciri türleri ve blok zinciri teknolojisinin sağlamış olduğu avantaj ve dezavantajlara yer verilmiştir. Bölüm 4’te blok zinciri teknolojisinin bir probleme uygunluğu esnasında ölçüt olarak değerlendirilen parametrelere yer verilmiştir. Bölüm 5’te blok zinciri teknolojisinin sahip olduğu çeşitlenmeden kaynaklanan, iki farklı teknoloji olarak göz önüne çıkan, Bitcoinve HyperledgerFabric teknolojilerine dair bilgilendirme yapılmıştır. Bölüm 6’da ise gelecekte yapılması düşünülen çalışmalara kaynaklık edecek blok zincirine ait bazı problemlerden bahsedilmiştir.

2. Blok Zinciri Nasıl Çalışır?

Blok zincirin sürdürülebilirliği, işlemlerin geçerliliğini doğrulayan ve madencilik süreciyle yeni bloklara ekleyen bir düğüm ağıyla sağlanır. Blok zinciri veri yapısına yeni bloklar ekleme işlemine madencilik denir. Blok zinciri ağında, geçerli olan işlemleri bloklara ayırma ve bu işlemleri bloklara ekleme işlemini madencilergerçekleştirir. Tüm blok zincirinin birer kopyasının her bir düğüm tarafından tutulmasını sağlamak amacıyla yeni blok tüm ağa yayılır. Tüm ağ, blok zincirine katılacak olan son blok hakkında bir anlaşmaya varmayı amaçlar. Birbirinden farklı anlaşma mekanizmaları vardır ki bunlar iş ispatı ve çıkar ispatı anlaşma mekanizmalarıdır [3].

Karmaşık bir doğrulama mekanizması içeren bu sistemde, bir düğüm tarafından ağın çoğunun kontrol etmesi neredeyse imkânsızdır. Çünkü yanlış bir bloğun oluşturulması,matematik probleminin diğer düğümlerden önce çözülmesi ve sadece madencilik bloğunda %51 uzlaşma oldukça yüksek hesaplama gücü gerektirecektir. Her bir bloğun bir önceki bloğa ait özet değeri içermesi ile kayıtlı işlemlerde kötü niyetli değişikliklerin önlenmesi sağlanır. Bu ise herhangi bir işlemin değişmesinin onu içeren bloğu ve önceki bloklarında özetlerinin değiştirilmesinin gerekliliği ile sağlanır [2].Şekil 2’de blok zinciri mimarisinin genel çalışma adımları özetlenmiştir.



Şekil 2. Blok Zinciri Çalışma Adımları

1) Ayşe, Barış’a para transfer etmek ister.
2) Ayşe işlem mesajını ağa yayınlar.
3) Diğer düğümler, blok zincirinin yerel kopyalarını kullanarak Ayşe’nin parayı harcama hakkına sahip olup olmadığına bakar ve işlemin Ayşe tarafından onaylanıp onaylanmadığını kontrol eder.
4) Doğrulama işlemi gerçekleştirildikten sonra işlem bloğa eklenir.
5) Yeni blokişlem listesini, onun başlığını, önceki blok başlığının özetini ve içerilen işlemlerin özetini içerir.
6) Madencilik süreci başlar.
7) Düğümler matematiksel bir problemi çözmek için bir yarışma başlatır.
8) Yeni blok, blok zincirine eklenir.
9) Her bir düğüm sahip olduğu yerel kopyayı günceller.
10) Barış parayı alır.
11) Yarışmayı kazanan düğüm ödüllendirilir.

Ayşe belirli miktarda kripto para birimini Barış’a göndermek istediğinde, kripto para bir adres ile tanımlanan dijital bir cüzdanda saklanır. Para aktarımının gerçekleşebilmesi için Ayşe göndermek istediği para miktarı ile birlikte Barış’ın cüzdan adresini belirtir ve işlemi bulunduğu ağa yayımlar. Cüzdan içerisinde saklanan gizli bilgiler kullanılarak işlem elektronik olarak imzalanır. Aynı zamanda işlemin Ayşe’nin cüzdanından geldiği ve başka herhangi biri tarafından değiştirilemeyeceğinin garantisi sağlanır. Ağda bulunan diğer düğümler elektronik imzayı analiz eder ve ilgili işlemin gerçekten Ayşe tarafından yapılıp yapılmadığının kontrolünü sağlar. Ayrıca blok zincirinin ağdaki tüm işlemleri saklayan yerel bir kopyasındaki bakiyesi hesaplanarak Ayşe’nin para harcama hakkına sahip olup olmadığı doğrulanır. Ayşe para gönderme işlemi yapabilecek durumda ise düğümler işlemi yeni bir bloğa ekler. Yeni blok onaylanacak olan tüm işlemlerin listesini içerirken yeni blok başlığı ise önceki blok başlığı ve önceki bloğa ait kriptografik özet değerini içerir. Oluşturulan yeni bloğun blok zincirine eklenebilmesi için düğümler madencilik işlemini başlatır.Madencilik işlemi, düğümlerin karmaşık bir matematik problemini çözebilmesi için gerçekleştirmiş oldukları rekabet olarak değerlendirilir. İş ispatı olarak adlandırılan bu süreç işlemlerin ve önceki blok başlığının bir araya getirilmesiyle birlikte verilen bir sonucu üreten düğümlerin rastgele bir değer bulmalarını gerektirmektedir. Düğüm olası bir çözümü gerçekleştirdiğinde hesapladığı sonucu diğer düğümlerle paylaşır ve sonucu denetler. Düğümlerin çoğunluğu sonuç üzerinde anlaşabilirse, blok geçerli kabul edilir ve blok zincirine eklenir. Her bir düğüm kendisinde bulunan yerel kopya blok zincirini günceller. Ayrıca kazanan düğüm bir işlem ücreti şeklinde ödüllendirilebilir.Madencilik sürecinin tamamlanması ile Barış, Ayşe’nin göndermiş olduğu parayı kendi cüzdanında gözlemleyecektir [2].

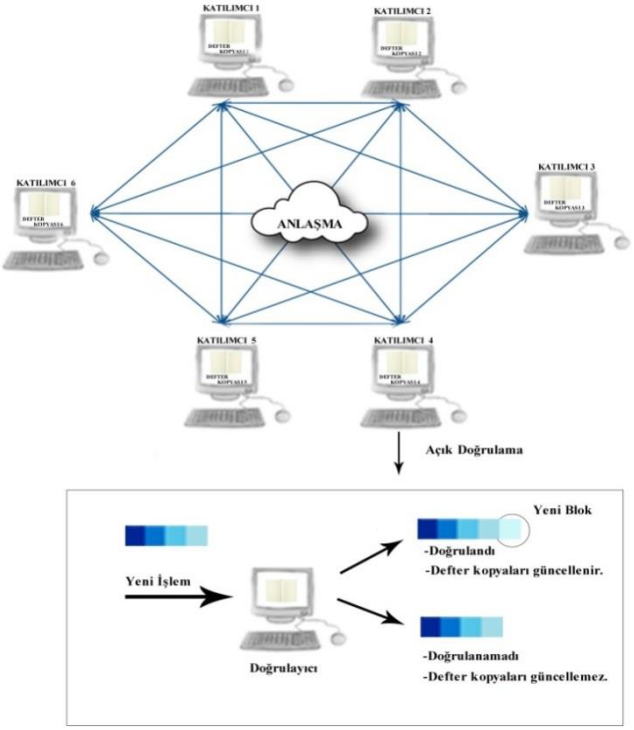
3. Blok Zinciri Arka Planı

A. Blok Zincirinin Temel Özellikleri

Değişmezlik, bütünlük, eşit haklar, şeffaflık ve tekrar edememezlik blok zinciri tarafından desteklenen 5 temel özelliktir. Kriptografik olarak imzalanmışdeğişmez işlemler zinciri olan blok zinciri, depolanmış olan verilerin inkâredilememesini sağlar. Kriptografik özellikler sayesinde verinin bütünlüğü, açık erişimin sağlanması, veri şeffaflığı gibi özellikler ağda bulunan her katılımcıya blok zincirine erişme ve blok zincirini işleme yeteneğini eşit oranda sağlar. Blok zincirine güven, ağ içerisinde bulunan düğümler arasındaki etkileşimlerden elde edilir. Blok zinciri ağında bulunan her bir katılımcı işlemleri kolaylaştırmak için güvenilir 3. taraf yerine blok zinciri ağının tamamına güvenir. Blok zincirinde verilerin boyutu, işlemlerin işlenme oranı ve veri aktarımındaki gecikme gibi ölçeklenebilirlik sınırları söz konusudur.Bir işlemin blok zinciri üzerinde yer aldığının sunulması ve bu durumun onaylanması arasındaki gecikme, anlaşma protokolü tarafından belirlenir [3].

B. Dağıtılmış Kayıt Defteri ve Merkezi Sistemlerin Sağlamış Olduğu Özellikler

1) *Açık Doğrulama:*Açık doğrulama ilesistemde bulunanherhangi birinin sistemin durumunu doğrulaması sağlanabilir. Dağıtılmış defterde kısıtlı bir katılımcı grubu olan doğrulayıcılar tarafından her bir durum geçişi onaylanırken her bir katılımcının durumu hakkında bilgi sızdırmaksızın genel halin açık doğrulaması yapılabilir. Herhangi bir gözlemci, defterin durumunun protokole göre değiştiğini doğrularken, tüm gözlemciler en azından belirli bir uzunluğa kadar defterin yerel bir kopyasına sahip olabilir. Blok zinciri teknolojisini geleneksel veritabanından ayıran özellik bütünlük ve şeffaflık ile sağlanan açık doğrulama özelliğidir. Merkezi bir sistemde farklı gözlemcilerin farklı görüşlere sahip olabilme özelliklerinden dolayı durum geçişlerinin doğru bir şekilde yürütüldüğü doğrulanmayabilir.Dolayısıyla merkezi sistemlerde gözlemcilerin doğrulamayı sağlayabilmesi için merkezi varlığa güvenmeleri gerekir [1]. Şekil 3’de blok zinciri teknolojisinin açık doğrulama özelliğini sağlarken kullanmış olduğu yapı resmedilmiştir.



Şekil 3. Blok Zinciri Açık Doğrulama

2) *Şeffaflık:*Blok zincirinde şeffaflık işlemlerin herkese açık olması gerekliliğinden kaynaklanmaktadır.Verilerin şeffaflığı ve verilerin durumunun güncellenmesi süreci açık doğrulama özelliği için bir gerekliliktir. Her bir katılımcının bilgiye olan şeffaflığı farklıdır. Dolayısıyla her bir katılımcı her bilgi parçasına erişemez [1]. Sistemin tamamen açık bir defter yapısına sahip olması, blok zinciri teknolojisinin şeffaflığı artırmasının kanıtı olarak gösterilmektedir. Blok zinciri teknolojisinde verilerin kelime tabanlı temsilinin kullanılması, kullanıcıların şeffaflık ve analiz yeteneğini artırıcı bir özellik olarak değerlendirilir [4].

3) *Gizlilik:* Gizlilik ve şeffaflık arasında doğal bir gerilim vardır. Tamamen şeffaf olan bir sistemde herkes herhangi bir bilgi parçasını görebilir bunun sonucu olarak gizlilik sağlanmaz. Tamamen gizli bir sistemin ise şeffaflık özelliği garanti edilemeyecektir. Bazı sistemlerde ise işlem geçişleri şeffaf iken özel gizlilik garantileri verilebilir. Örneğin dağıtılmış defterde ayrı ayrı her bir katılımcı hakkında bilgi verilmezken sistemin genel durumu herkese açıktır. Merkezi sistemlerde sistemin işleyişi için şeffaflık ve açık doğrulama gerekmediğinden gizliliği sağlamak kolay olur. Açık sistemlerde gizlilik, kriptografik teknikler kullanılarak sağlanır. Bununla birlikte düşük verimlilik maliyeti ortaya çıkar [1].

4) *Bütünlük:*Bilginin bütünlüğü sağlanıyorsa bilgi izni olmayan kişiler tarafından ele geçirilmemiştir ve değiştirilmemiştir. Bütünlük, açık doğrulama özelliği ile doğrudan bağlantılıdır. Herhangi bir sistemde açık doğrulama özelliği sağlanıyorsa, sistemde bulunan herkes, verilerin bütünlüğünü doğrulayabilir demektir [1]. İş ispatı tabanlı blok zincirleri, ağda bulunan tüm düğümlerde blok zincirinin bir kopyasının tutulmasından ve madencilik sürecinden kaynaklı veri bütünlüğünü sağlayan özelliklere sahiptir [5]. Blok zincirinin bir parçası olabilmek için tüm madencilerin içerik üzerinde anlaşma sağlamış olması gerekmektedir. Dolayısıyla pratik olarak reddedilemez ve kalıcıdır. Verilerin reddedilemez olması ve kalıcılığının sağlanması ile veri bütünlüğünün sağlanması ilişkili kavramlar olarak değerlendirilir [5].

5) *Fazlalık:* Merkezi sistemlerde genellikle farklı fiziksel sunuculardaki kopyalar ve yedeklemeler sonucu fazlalık oluşur. Blok zincirinde ise sistemde bulunan yazma özelliğine sahip katılımcılar arasındaki çoğaltma yoluyla fazlalık ortaya çıkar [1].

6) *Güven kaynağı:*Güven kaynağı ilesistemde bulunan en yüksek otorite temsil edilir. Bu otorite ilgili sisteme okuma/yazma erişimini verme ve iptal etme yetkisine sahip olacaktır [1].

C. Blok Zinciri Teknolojisinin Kriptografik Parametreleri

Blok zinciri teknolojisi kullanıcı kimliklerini korumak amacıyla kriptografik özelliklerden yararlanır. İşlemlerin güvenli bir şekilde yapılmasını garanti ederken depolanan tüm bilgilerin güvenliğini sağlar. Blok zincirinde açık anahtar şifrelemesi yaklaşımı kullanılır. Asimetrik kriptografi olarak da bilinen bu yöntemde bilgi herkesle paylaşılabilecek bir açık anahtar aracılığıyla aktarılır. Şifreleme ve şifre çözme için tek bir anahtar kullanmak yerine ortak anahtar ve gizli anahtar olmak üzere iki anahtar kullanılır. Blok zinciri teknolojisinde iş ispatı mekanizması ile sistemde bulunan defter kopyalarının tüm katılımcılarda bulunması sağlanarak verinin bütünlüğü garanti edilir.Ayrıca açık anahtar şifreleme ile verilerin bütünlüğünü güvence altına alan bir elektronik imza üretilir. Elektronik imzanın üretimi bir kullanıcının özel anahtarını, matematiksel bir algoritma aracılığıyla imzalamak istedikleri verilerle birleştirilerek yapılmaktadır. Bu yaklaşım ile asıl veriler elektronik imzanın bir parçası haline gelir. Veride meydana gelecek en küçük değişiklik imzayı da değiştireceğinden blok zinciri ile verinin doğruluğu garanti edilebilir ve değişmezliği sağlanmış olur. Özetleme algoritmaları ise blok zincirinde bulunan işlem ayrıntılarını içeren blok verilerinin değiştirilmediğini ve verilerin bütünlüğünün korunduğunu garanti etmek için kullanılır. Blok zinciri tabanlı teknolojilerde özetleme algoritması olarak SHA-256 algoritması kullanılmaktadır. ECDSA ve eliptik eğri dâhil farklı şifreleme türleri ise blok zincirinde işlemleri doğrulamak için kullanmaktadır. Katılımcılar arasında gerçekleşen bir işlem sırasında üretilen elektronik imzayı doğrulayan ECDSA algoritmasıile işlem verilerinin değiştirilmediğinin kanıtlanması sağlanır [14].

D. Blok Zinciri Teknolojisinin Avantaj ve Dezavantajları [2]

Avantajları:

1) Blok zincirinde, ağda bulunan her bir düğüm tarafından paylaşılan bir depo hizmeti sunulur. Ağda bulunan herkes veriye erişebilir ve işlemleri görüntüleyebilir. Düğümlerde bulunan verilerin depolanması ile beklenmedik olaylarda veri kaybının önüne geçilmiş olur.

2) Blok zinciri herkes tarafından okunabilen ve yazılabilen kısacası erişimin sağlanabildiği dünya çapında bir veri deposu olarak değerlendirilir.

3) Blok zinciri teknolojisinde değişmezlik garanti edilir. Başka bir ifadeyle, istenmeyen kişiler tarafından veri silinemez veya değiştirilemez.

4) Sistemde bulunan herkesin ağda bulunan işlemlerin önceki ve şu anki durumlarına dair bilgiler edinebilmesi özelliği ile blok zinciri teknolojisinde şeffaflık özelliği garanti edilir.

5) Blok zinciri teknolojisinde görevlerin dağıtılması ile merkeziotoriteye ihtiyaç ortadan kalkar.

6) Blok zinciri teknolojisinde elektronik imza ve doğrulama ile her bir düğümarasında aracılara ihtiyaç duymadan güven sağlanır.

Dezavantajları:

1) Blok zinciri teknolojisinde bulunan madencilik işlemi pahalı donanım gerektirir. Ayrıca bilgi işlem gücünün büyük bir kısmınınboşa harcandığı gözlemlenir.

2) Blok zinciri teknolojisinde veri çoğaltma alanına ihtiyaç duyulur. Blok zincirinde her bir düğümün blok zincirinin yerel bir kopyasını içermesi sistemi performans olarak veritabanı sistemleri ile karşılaştırılamaz hale getirir.

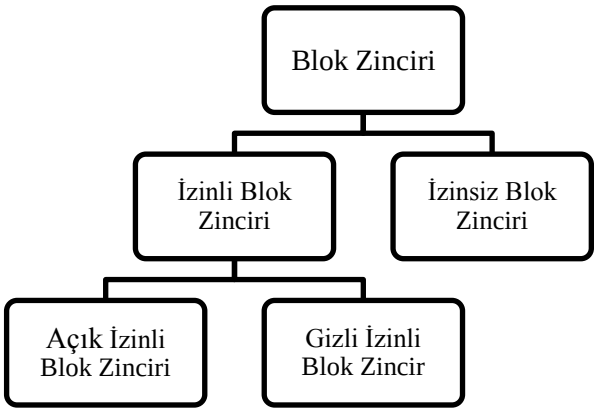
3) Blok zinciri teknolojisinin garanti ettiği şeffaflık ile ağda bulunan her bir düğüm, blok zincirinin yerel bir kopyasını saklayıp içeriğine erişebildiği için kullanıcıların gizliliğine ve itibarına zarar verebilir.

4) Blok zincirine bilginin eklenmesi yavaştır.

5) Akıllı sözleşmelerde kodlar herkesin kullanımına açık olduğu ve oluşturulduktan sonra kendi kişiliklerini kazandıkları için istenmeyen kişiler için erişilebilir özelliğe sahip olur. Akıllı sözleşmeler blok zincirinde saklandıkları için değiştirilemez özelliğe sahip olurlar. İstenmeyen kişiler tarafından yapılan değişiklikleri gidermek için geliştiricilerin yeni sözleşmeler oluşturmaları ve tüm verileri, işaretçileri eskiden yeni hale aktarmaları gerekmektedir.

E. Blok Zinciri Çeşitleri:

Blok zinciri teknolojisinin sağlamış olduğu çeşitli özellikler dikkate alındığında teknolojinin iki ana grup altında değerlendirildiği gözlemlenir. Şekil 4’de blok zinciri teknolojisinin alt ana grupları özetlenmiştir.



Şekil 4. Blok Zinciri Türleri

1. İzinsiz Blok Zinciri: Herhangi bir düğümün ağa istediği zaman okuyucu ya da yazar olarak katılabildiği ve ayrılabildiği blok zinciri türüdür. Her bir durum değişikliği doğrulayıcılar tarafından doğrulanır. Üyelikleri yöneten, izinsiz okuyucuları ya da yazarları yasaklayabilen merkezi bir varlık yoktur. Merkezi bir varlığın olmaması yazılı içeriğin ağda bulunan herhangi bir düğüm tarafından okunabileceği anlamına gelir. İzinsiz blok zinciri yapısında uygulamalar onay ve güvene gerek duyulmadan ağa eklenebilir. İzinsiz blok zincirine örnek olarak Bitcoin ve Ethereum gösterilebilir [1].

*2. İzinli Blok Zinciri:*Blok üyelerinin yazma ve okuma işlemlerine katılma haklarını sağlayan merkezi bir varlık vardır. Gizlilik ve kapsülleme özelliklerini sağlayabilmek için okuyucu ve yazar birbirleriyle bağlantılı olan paralel blok zincirlerinde çalışabilir. Ayrıcablok zinciri ağına erişme özelliği olan kişileri yönetmek için bir erişim kontrol katmanı kullanılır. İzinli bir blok zinciri, benzerliklerini merkezi bir veritabanı ile paylaşır. Bu durum ise bir blok zincirinin merkezi bir veritabanından daha uygun olup olmadığı sorusunu ortaya çıkarır. İzinli blok zincirinde işlemlerin doğrulanması sırasında her düğüme güvenilmez. Sınırlı sayıda okuyucu ve yazarı yetkilendiren, sadece izin verilen bir grup varlığın okuma ve yazma yapabildiği sözde izinli blok zincirleri kısa süre önce önerilmiştir. İzinli blok zincirine örnek olarak ise HyperledgerFabricve R3 Corda örnek verilebilir [1].

F. Blok Zinciri Karakteristiği

- Blok zinciri düzenli olarak büyüyebilme özelliğine sahiptir [1].
- Blok zincirinde bulunan her blok, özet değeri ile önceki bloğa bağlıdır. Her blok kendi başlık bilgisi içerisinde, kendisine ve bağlı bulunduğu bloğa ait kriptografik özetleme algoritması kullanılarak hazırlanmış iki adet özet değeri içermektedir. Özet değerlerini her bir bloğun içermesi ile blok zincirinde daha önceden yapılmış olan işlemlerin silinmesinin ve değiştirilmesininönüne geçilir [3].
- Blok zinciri merkezi olmayan bir kayıt sistemidir. Normal sistemlerde veri tek bir merkezde saklanırken blok zinciri yapısında veri ağın tamamında tutulur [1].
- Blok zincirinde yapılan işlemler, ağda bulunan tüm düğümlere yayımlanır. İşlemler tek düğüm değil de birden fazla düğüm tarafından onaylanır ve sonunda zincire eklenir özellikte olmalıdır [1].
- Blok zinciri teknolojisi ile bütünlüğü korunan veri depolaması sağlanırken işlem şeffaflığı garanti edilir [4].
- Blok zinciri dağıtık kayıt defteri yapısını kullanır. Bu yapıda her bir düğüm dağıtık kayıt defterinin bir kopyasına sahip olur ve ihtiyaç olduğu durumda güncelleme işlemi yapar. Her bir kayıt işlemi bağımsız olarak yapılır. Basit bir veritabanı yapısıdır [1].
- Blok zincirinde tüm işlem geçmişine herkes erişebilir. İşlemlerin geçmişlerine erişim ile sanal paranın geçerliliği kontrol edilebilir [3].
- Blok zincirinde iletişim merkezi bir bağlantıdan değil taraflar arasında doğrudan gerçekleşir [1].
- Blok zinciri mimarisinde her bir işlem ve işleme verilen değer sisteme erişebilme yetkisine sahip olan herkes için açık olur [1].
- Açık anahtarlı şifreleme ve elektronik imzalar blok zincirinde hesapların tanınmasında ve başlatılan işlemlerin yetkilendirilmesinde kullanılır. Blok zincirinde işlemler işlev çağrılarının parametrelerini ve sonuçlarını depolayan veri paketleri olarak değerlendirilir. İşlemlerin bütünlüğü algoritma tabanlı kurallar ve kriptografik teknikler ile kontrol edilir [3].

4. Bir Sistem İçin Blok Zinciri Teknolojisinin Uygunluğu

Sistemin ihtiyaç duyduğu gereksinimler bugünün ilişkili veritabanları tarafından karşılanıyorsa, blok zincirini kullanmak anlamsız olacaktır. Oracle ve MySQL gibi sistemlerin arkasında onlarca yıllık gelişim vardır. Bu teknolojiler trilyonlarca sorgu çalıştıran milyonlarca sunucuya dağıtılmıştır. En kapsamlı, test edilmiş, hataları ayıklanmış ve optimize kodlar içerdikleri için saniyede binlerce işlemi yapabilme özelliğine sahiptirler.Ancak bu durum blok zincirinin işe yaramadığına bir kanıtı olarak gösterilemez [2]. Bir probleme çözüm olarak blok zinciri teknolojisi kullanılmak istendiğinde sistemin sağlaması gereken özellikler şu şekilde değerlendirilebilir:

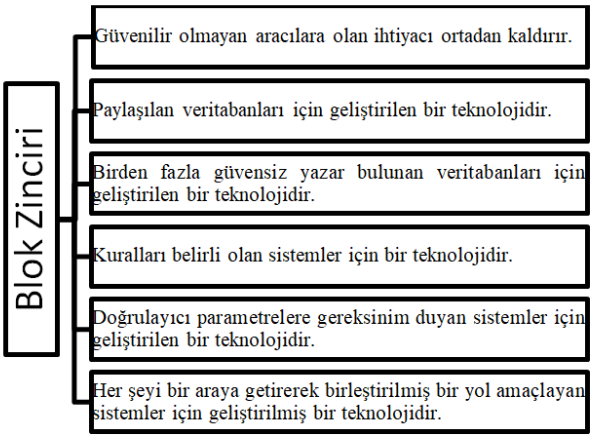
- Eğer sistemin veriyi depolamaya ihtiyacı yoksa veritabanı ya da veri bloğu olarak blok zincirine ihtiyaç duyulmamaktadır [1].
- Sadece bir tane yazar (blok zinciri sistemindeki anlaşmaya bağlı belirlenen katılımcı) varsa, blok zinciri ek garantiler sağlamayacaktır. Çıktı ve gecikme açısından veritabanı daha iyi performans sağlayacaktır [1].
- Paylaşılan bir veritabanına sahip olmak gerekliyse doğru çözüm blok zinciri teknolojisindedir [2].
- Verinin yazılması sırasında birden fazla tarafa ihtiyaç varsa blok zinciri doğru çözüm olacaktır [2].
- Olması muhtemel olan yazarlara güvenilmiyorsa blok zinciri bu sistemin ihtiyacını karşılayacaktır [2]. Sistemde bulunan yazarlar birbirlerine karşılıklı olarak güveniyorsa, yazma erişimi olan paylaşılan bir veritabanı en iyi çözümdür. Sistemde bulunan yazarlar birbirlerine karşılıklı olarak güvenmiyorsa, yazma erişimi olan izinli blok zinciri en iyi çözümdür [1].
- Güvenilir 3. tarafa ihtiyaç var mı? Güvenilir 3. taraf varsa iki seçenek vardır. Eğer güvenilir 3. taraf, her zaman çevrimiçi ise, yazma işlemleri ona devredilebilir ve durum geçişleri için doğrulama işlevleri güvenilir 3. tarafa devredilebilir. Eğer güvenilir 3. taraf genellikle çevrimdışı ise güvenilir 3. taraf sistemin bütün yazarlarının bilindiği izinli blok zinciri ayarında bir sertifika yetkilisi olarak işlev görecektir [1].
- İşlemlerin birbirleri ile bağlantısının nasıl olduğu görülebilir özellikte olmalı mıdır? Cevap hayırsa blok zinciri teknolojisini kullanmak anlamsız olacaktır [2].

Tüm bu parametreler göze alındığında ilgili sisteme blok zinciri teknolojisinin uygunluğunun belirlenmesi esnasında Tablo 1’deki parametreler dikkate alınarak çözüme karar verilmelidir.

Tablo 1. Blok Zinciri Teknolojisinin Problem İçin Uygunluğuna Karar Verirken Değerlendirilen Parametreleri Gösteren Tablo

	Hayır	Evet
Sistemde birden fazla yazara ihtiyaç var mı?	1	0
Paylaşılan veritabanı ihtiyacı söz konusu mu?	1	0
Verilerin yazılması sırasında birden fazla tarafa ihtiyaç duyulacak mı?	1	0
Güvenilir aracı ihtiyacı ortadan kaldırılmalı mı?	1	0
Güvenilir aracıların doğrulanması gerekli midir?	1	0
Sistemde bulunan potansiyel yazarlar güvenilmez mi?	1	0
İşlemlerin birbirleri ile bağlantısının nasıl olduğu görülebilir özellikte olmalı mıdır?	1	0

Bir sistem tasarlanırken gereksinimler doğrultusunda Tablo 1’de belirlenen parametrelere ait değerler “0” olduğu sürece blok zinciri teknolojisini kullanmak mantıklı olacaktır. 0’dan farklı her değer için çeşitli değerlendirme ölçütleri göz önüne alınarak diğer veri depolama teknolojileri seçilmelidir. Tablo 1 ve sistemin sağlaması gereken şartların genel olarak değerlendirilmesi Şekil 5 ile resmedilmiştir.



Şekil 5. Sistemler için Blok Zinciri

Blok zinciri kullanan bir sistem tasarlanırken bazı şartların sağlanması gerekmektedir. Bu şartlar:

*1) Veritabanı:*Blok zincirleri paylaşılan veritabanları için bir teknolojidir.

*2) Birden fazla yazar:*Blok zincirleri birden fazla yazara sahip veritabanları için bir teknolojidir. Başka bir deyişle, veritabanını değiştiren işlemleri üreten birden fazla varlığın olması gerekmektedir. Birçok durumda yazarlar aynı zamanda veritabanının bir kopyasını ve düğümler arası geçiş işlemlerini içermelidir.

3) Güven Yokluğu: Blok zincirleri, birden fazla güvensiz yazar bulunan veritabanları için geliştirilmiş bir teknolojidir. Veritabanına birden fazla varlığın yazma izni varsa, bu varlıklar arasında belirli bir dereceye kadar güvensizliğin var olması gerekir.

4) Aracısızlaşma: Temelde hedeflenen amaç birden fazla güvenilir yazara sahip olan bir veritabanını etkinleştirmektir. Bunun sağlanmasında genel kullanılan yaklaşım güvenilir 3. taraftır. Bu yaklaşımda yazarlar birbirlerine güvenmezler ancak tüm yazarların güvendiği bir aracı belirlenir. Blok zincirleri ise güvenilir olmayan aracılara olan ihtiyacı ortadan kaldırır. Blok zincirinde işlemleri ve kaynakları doğrulamak için merkezi bir varlığa ihtiyaç yoktur. Bir işlemin tanımı, yetki belgesi ve geçerlilik kanıtını içerecek şekilde genişletilir. Böylece her bir işlem, veritabanının bir kopyasını tutan her bir düğüm tarafından bağımsız olarak işlenebilir ve doğrulanabilir hale getirilir.

5) İşlem Etkileşimi: Farklı yazarlar tarafından oluşturulan işlemler genellikle birbirine bağlıdır. Örneğin, Ayşe’nin Barış’a bir miktar para gönderdiğini ve Barış’ın bir kısmını Ali'ye gönderdiği varsayıldığında Barış’ın işlemi Ayşe’nin hesabına bağlıdır ve Ayşe’nin hesabını kontrol etmeden Barış’ın işleminin doğrulanmasının bir yolu yoktur. Bunun sonucu olarak, işlemler tek ve paylaşılan veritabanına ait olur. Kısacası blok zinciri her şeyi bir araya getirerek birleştirilmiş bir yol sağlar.

6) Kuralların Belirlenmesi: Birden fazla birbirine güvenmeyen yazar tarafından doğrudan değiştirilen bir veritabanı varsa, veritabanı gerçekleştirilen işlemleri kısıtlayan birtakım kurallar içermelidir. Bu kurallar geleneksel veritabanı sistemlerinin içerdiği kurallardan farklıdır. Her bir işlem, ağdaki her bir düğüm tarafından bu kurallara göre kontrol edilmelidir ve başarısız olanlar reddedilmelidir.

*7) Doğrulayıcıların belirlenmesi:*Bir blok zincirinin temel işlevi yetkili son işlem kaydını yapmaktır. Bu kaydın yapılmasının temel sebebi yeni eklenen düğümlerin veritabanının içeriğini başka bir düğüme güvenmeye gerek olmadan sıfırdan hesaplamasını sağlamaktır. Ayrıca, bazı düğümlerin sistem kesintisi veya iletişim aksaklığı nedeniyle bazı işlemleri kaçırma olasılığını ele alırken iki işlemin çatışma içinde olmasının mümkün olduğu durumlarda, sadece birinin kabul edilmesine olanak sağlar. Hangi anlaşma şeması kullanılırsa kullanılsın, doğrulama düğümleri geleneksel bir merkezi veritabanının sahibinden çok daha az güce sahiptir. Doğrulayıcılar, işlemleri ihlal edemez veya veritabanının kurallarını değiştiremez.

5. Uygulama Bakımından Blok Zinciri

A. İzinli Blok Zinciri Olarak HyperledgerFabric:

HyperledgerFabric, Bitcoin ve diğer mevcut ağların adreslediği temel dijital paranın ötesindeki iş uygulamaları için tasarlanmış izinli blok zincir platformudur [7]. HyperledgerFabric ilk olarak DigitalAsset ve IBM tarafından sağlanmıştır. Açık blok zinciri ürün ve hizmetlerini geliştirmek için farklı kuruluşlardan birçok mühendis HyperledgerFabric projesine katkıda bulunmuştur [8]. Kurumsal içeriklerde kullanılmak üzere tasarlanan HyperledgerFabric açık kaynaklı, dağıtımlı defter platformudur. Fabric mimarisi bankacılık, finans, sigorta, sağlık hizmetleri, insan kaynakları, tedarik zinciri ve dijital müzik dağıtımı dahil olmak üzere geniş bir yelpazede sanayi kullanımı vakaları için yenilik, çok yönlülük ve optimizasyon sağlayan son derece modüler ve yapılandırılabilir bir yapıya sahiptir. Fabric izin verilen bir yapı olduğundan katılımcılar anonim ve dolayısıyla tamamen güvenilmez değildir. Katılımcılar birbirlerine tam olarak güvenmese de katılımcılar arasında güvenin ne olduğu konusunda kurulu bir model söz konusudur. Anlaşmazlıkları ele alabilmek için yasal bir anlaşma bulunmaktadır [9].

HyperledgerFabric yapısında bilinmeyen kimliklerin ağa katılmasına izin veren, işlemleri doğrulamak ve ağı güvenli hale getirmek için “iş ispatı” gibi protokoller gerektiren sistemlerden ziyade, bir HyperledgerFabric ağının üyeleri güvenilir bir “Üyelik Servis Sağlayıcısı” aracılığıyla sisteme kayıt olurlar.HyperledgerFabric ayrıca çeşitli takılabilir seçenekler sunar. Defter verileri çoklu formatta saklanabilirve farklı Üyelik Servis Sağlayıcısı sistemleri desteklenebilir.HyperledgerFabric aynı zamanda kanal oluşturma yeteneğini de sunar. Eğer iki katılımcı bir kanal oluşturuyorsa, o katılımcıların bu kanal için her birinde defterin kopyaları vardır [11]. Modüler yapısı, blok zincir çözümlerinin gizliliğini, esnekliğini en üst düzeye çıkarır. HyperledgerFabric, işlemin gerçekleşmesini üç aşamaya ayıran modüler bir mimari üzerine kurulmuştur. Bu yapıdağıtık mantık işleme ve anlaşma, işlem siparişi, işlem doğrulama ve taahhüdü yapısıdır. Bu ayrım ile düğüm türleri arasında daha az güven ve doğrulama düzeyi sağlanır. Ayrıca ağ ölçeklendirilebilirliği ve performansı en iyi duruma getirilir.HyperledgerFabric'te desteklenen kanallar,

DOI: 10.25045/NCInfoSec.2018.01

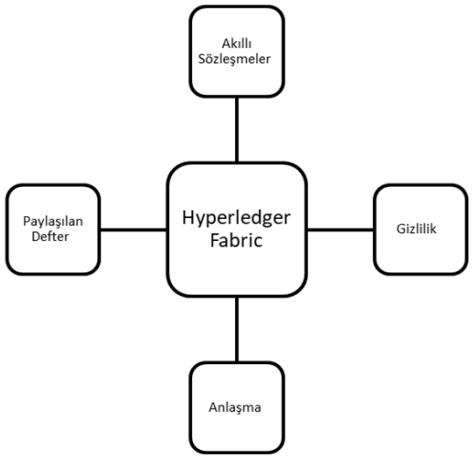
verilerin yalnızca bilmesi gereken taraflara gitmesine izin verir [10].

1) HyperledgerFabric Modelinin sağladığı özellikler:

- İzinli blok zinciridir.
- Dağıtımlı defter platformu özelliği gösterir.
- Akıllı sözleşmeleri destekler.
- Katılımcılar anonim ve dolayısıyla tamamen güvenilmez değildir.
- Üyelik Servis Sağlayıcısı desteği vardır.
- Çeşitli takılabilir seçenekler sunar.
- Defter verileri çoklu formatta saklanabilir.
- Farklı Üyelik Servis Sağlayıcıları desteklenebilir.
- Kanal oluşturma yeteneği sunar.
- Modüler yapısı, blok zincir çözümlerinin gizliliğini, esnekliğini en üst düzeye çıkarır.
- Ayrıca ağ ölçeklendirilebilirliği ve performansı en iyi duruma getirilir.

2) HyperledgerFabric modeli karakteristiği[11]:

HyperledgerFabric sisteminin sağladığı özellikler Şekil 6’da özetlenmiştir:



Şekil 6. HyperledgerFabric Teknolojisi Özellikleri

a) *Paylaşılan Defter**:***HyperledgerFabric, iki bileşeni içeren bir defter alt sistemine sahiptir. Bu bileşenler; dünya durumu ve işlem kaydıdır. Her bir katılımcının, ait oldukları her HyperledgerFabric ağına ait defterin bir kopyası vardır.

b) *Akıllı Sözleşmeler:*HyperledgerFabric akıllı sözleşmeler, zincir kodunda yazılır ve bu uygulamanın defter ile etkileşime girmesi gerektiğinde, blok zincirine harici bir uygulama tarafından çağrılır. Çoğu durumda, zincir kodu yalnızca defterin veritabanı bileşeniyle, dünya durumuyla ve işlem günlüğüyle etkileşime girmez. Zincir kodu çeşitli programlama dillerinde uygulanabilir özelliktedir.

c) *Gizlilik:*Bir ağın ihtiyaçlarına bağlı olarak, bir İşten-İşe ağdaki katılımcılar, paylaştıkları bilgi hakkında son derece hassas olabilirler. Diğer ağlar için gizlilik en önemli konu olmayacaktır. HyperledgerFabric, gizliliğin önemli bir operasyonel gereksinim olduğu ve nispeten açık olan ağları destekler.

d) *Anlaşma:*HyperledgerFabric, ağ başlatıcılarının, katılımcılar arasında var olan ilişkileri en iyi temsil eden bir anlaşma mekanizması seçmesine izin verecek şekilde tasarlanmıştır.

B. İzinsiz Blok Zinciri Olarak Bitcoin

Bitcoin, dijital para ekosisteminin temelini oluşturan kavram ve teknolojilerin bir araya getirilmesidir. Bitcoin ağında bulunan katılımcılar arasında değer kaydetmek ve aktarmak için Bitcoin denilen para birimleri kullanılır. Bitcoin kullanıcıları birbirleriyle internet üzerinden etkileşme özelliğine sahiptir. Açık kaynak yazılımı olarak kullanılabilen Bitcoin protokol yığını, çok çeşitli bilgi işlem cihazlarında çalıştırılabilir özelliktedir. Geleneksel para birimleriyle yapılabilen tüm işlemler Bitcoin teknolojisi ile yapılabilmektedir. Bu teknoloji, Bitcoin ağının güvenliğini sağlamak için şifreleme ve elektronik imzalamaya dayalı özellikler içermektedir. Bitcoin hızlı, güvenli ve sınırsız olduğu için internet kullanımında mükemmel bir para birimi olarak değerlendirilmektedir. Geleneksel para birimlerinin aksine tamamen sanal olan Bitcoin, anahtar değerler sayesinde ağda işlemlerin sahibinin kanıtlanmasına izin verebilen bir yapıya sahiptir. Bu anahtar değerler genellikle her bir kullanıcının bilgisayarında saklanmaktadır. İşlemlerin kilitlerinin açılmasına olanak sağlayan anahtarların bulundurulması Bitcoinlerin harcanılabilmesi için tek ön koşuldur [12].

Bitcoin’in tamamen dağıtılmış eşler arası bir sistem olması merkezi sunucu veya kontrol noktasına olan ihtiyacı ortadan kaldırır. Bitcoinler, “madencilik” adı verilen ve zor bir soruna çözüm arayışında olan bir süreçle yaratılır. Bitcoin ağındaki herhangi bir katılımcı (Bitcoin protokol kümesini çalıştıran herhangi bir aygıt), bu soruna çözüm bulmaya çalışmak için bilgisayarının işlem gücünü kullanarak bir madenci olarak çalışabilir. Bitcoin protokolü, ağ üzerindeki madencilik işlevini düzenleyen yerleşik algoritmalar içerir. Madencilerin çözmesi gereken problemin zorluğu dinamik olarak ayarlanır. Protokol ayrıca, her 4 yılda bir yeni Bitcoinlerin oluşturulduğu oranı yarıya indirir ve toplam 21 milyon jeton olarak Bitcoin sayısını sınırlar. Sonuç olarak, dolaşımdaki Bitcoin sayısı, 2140 yılına kadar 21

milyona ulaşan, kolayca tahmin edilebilen bir eğriyi yakından takip etmektedir. Bitcoin'in düşüş oranının azalması nedeniyle, uzun vadede, Bitcoin para birimi deflasyonisttir. Ayrıca, Bitcoin beklenen ihraç oranının üzerinde ve ötesinde yeni para basmak suretiyle şişirilmez özelliktedir [12].

Bitcoin'in sahipliği; dijital anahtarlar, Bitcoin adresleri ve elektronik imzalar aracılığıyla kurulmaktadır. Dijital anahtarlar aslında ağda saklanmaz, bunun yerine bir dosyada son kullanıcılar tarafından veya bir cüzdan olarak adlandırılan basit bir veritabanında depolanır. Her Bitcoin işlemi, yalnızca geçerli dijital anahtarlarla oluşturulabilen blok zincirine dâhil edilmek üzere geçerli bir imza gerektirir. Bu nedenle dijital anahtarların bir kopyasına sahip olan herkes bu hesaptaki Bitcoin kontrolüne sahip olur. Anahtarlar, özel (gizli) ve ortak anahtardan oluşan çiftler halinde gelir. Bu dijital anahtarlar, Bitcoin kullanıcıları tarafından çok nadir görülür. Çoğunlukla, cüzdan dosyasında saklanır ve Bitcoin cüzdan yazılımı tarafından yönetilir [13].

1) *Bitcoin’in Çalışma Mantığı:*

Barış, Ayşe’ye Bitcoin transfer etmek istiyor. Barış’ın Ayşe’ye gönderim yapabilmesi için, Bitcoin tam ya da hafif istemci yazılımını çalıştıran akıllı telefon, tablet veya bilgisayar gibi bir cihazın yanı sıra, Barış’ın özel anahtarı ve Ayşe’nin Bitcoin adresini içeren 2 adet bilgiye ihtiyaç duyulur. Ağda bulunan herhangi bir kullanıcı bir Bitcoin adresine para gönderebilir. Fakat yalnızca özel anahtar kullanılarak oluşturulan benzersiz imza ile Bitcoinlerhesaptan serbest bırakılabilir. Barış yapılacak olan işlemin elektronik olarak imzalanması için bir şifreleme anahtarı kullanır ve bu paraların sahibi olduğunu kanıtlar. Barış ağda bir işlem yayınladığında, ağdaki tüm madencilere bu yeni işlem hakkında bilgi veren bir uyarı gönderilir.Madenciler, elektronik imzaların doğru olduğunu ve Barış'ın işlemleri tamamlamak için yeterli Bitcoin’e sahip olup olmadığını kontrol ederler. Ayrıca madenciler ağda bulunan ve Barış’ın işlemi de dâhil beklemedeki tüm işlemleri paketlemek için yarışırlar ve sonuçta ortaya çıkan bloğu işlerler. Madenciler ilgili bloğun özet değerini oluştururlar ve eğer sonuç belirli bir sıfır sayısı ile başlamazsa özetleme işlevi yeni bir rastgele sayı kullanarak geri döner. Gerekli özet değeri başlangıçta belirli ancak rastgele sayıda bir sıfır değerine sahip olmalıdır. İstenmeyen tahmin durumunun doğru sayıda sıfır ile üretileceği tahmin edilemez. Dolayısıyla madenciler istenen özet değerini bulmak için farklı anahtarlar kullanarak denemeye devam ederler. Madenci, doğru sayıda sıfır ile bir özet değer bulduğunda ağda duyurulur ve hem Barış hem de Ayşe’den başarılı işlem hakkında bir onay alınır. Diğer madenciler kabullerini iletirler ve ağda bulunan bir sonraki bloğu keşfetmeye başlar. Bitcoin protokolü kazanan madenciyi, teşvik olarak yeni basılmış Bitcoin seti ile ödüllendirir ve özetlenmiş blok açık defterde yayımlanır. Barış’ın işleminin blok zincirine eklenmesiyle, Barış ve Ayşe’nin her biri Bitcoin’inAyşe’ye devredildiğini gösteren ilk teyidini alır. İşlem süresi değerlendirildiğinde, geçerli ağın yükü ve Barış tarafından yapılan işlemin içerdiği işlem ücreti öne çıkar. Ancak asgari olarak yaklaşık 10 dakika sürecektir [13].

2) *Bitcoin Çalışma Adımları*

Bitcoin teknolojisi ile para transferi işlemleri sırasında kullanılan temel yaklaşım Şekil 7’da resmedilmiştir.

Şekil 7. Bitcoin Çalışma Modeli

Ayşe ve Barış arasında gerçekleşen transfer sırasında izlenen adımlar şu şekilde özetlenebilmektedir:

1) Barış 3. taraf cüzdan yazılımı kullanarak bir Bitcoin ödeme başlatır.
2) Ödeme işlemi ve diğer bekleyen işlemler dünya çapındaBitcoin ağında yayınlanır.
3) Madenciler birkaç yüz işlem toplar ve bunları bir blokta birleştirir.
4) Madenciler bloğu her on dakikada bir işleyecek şekilde tamamlar veya ağda bir blok çıkarırlar.
5) Kazanan madenci, tüm bloğa yeni bloğu yayar, bu işlemi blok zincirinde kaydeder ve teşvik amaçlı Bitcoin ile ödüllendirilir.
6) Ayşe, Bitcoin'in gelip gelmediğini görmek için cüzdan yazılımını kullanarak kontrolü sağlar

6. Sonuç ve Gelecek Çalışmalar

Yapılan bu çalışmada blok zinciri teknolojisine dair kabul görülmüş çeşitli çevreler tarafından yapılan tanımlara ve teknolojinin içermiş olduğu alt yapıya dair bilgilendirmeler yapılmıştır. Ayrıca teknolojinin sahip olduğu özellikler ve bu özelliklerin teknolojiye

kazandırmış olduğu avantaj ve dezavantajlar hakkında genel bir değerlendirme sunulmuştur. Çeşitli özelliklerinden dolayı alt dallara ayrılabilir yapıda olan blok zinciri teknolojisinin çeşitleri hakkında bilgilendirmeler yapılmıştır. Bu alt dallardan izinli blok zinciri teknolojisi olarak değerlendirilen HyperledgerFabric ve izinsiz blok zinciri olarak değerlendirilen Bitcoin teknolojileri ve bu teknolojilerin çalışma sistematikleri hakkında bir özet sunulmuştur. Yapılan bu çalışmada özellikle blok zinciri teknolojisinin kriptografik anlamdaki değerinden bahsedilerek hangi durumlarda blok zinciri teknolojisinin kullanılması gerektiğine dair bir yol gösterilmiştir.

Blok zinciri teknolojisinin genel yapısı incelendiğinde bazı açık problemlerin var olduğu gözlemlenmiştir.Bu problemler şu şekilde özetlenebilir:

Problem 1: Gelişen teknolojinin bir ürünü olarak ortaya çıkan ve var olan sistemlerin çözülebilmesine imkân sağlayan kuantum hesaplayıcılar sonrasında blok zincirindeki güvenlik nasıl olacaktır?

Problem 2: Sistemlerin genel çalışma yaklaşımları düşünüldüğünde kötü niyetli kullanıcıları ya da işlemleri anlamak için ek bileşenlere ihtiyaç duyulmaktadır. Blok zinciri teknolojisinde bu bileşenler nasıl belirlenmelidir?

Problem 3: Blok zinciri teknolojisinin sağlamış olduğu özellikler dikkate alındığında teknolojinin sağlamış olduğu parametreler insanlık kullanımına dair nasıl iyileştirilebilir?

Problem 4: Blok zinciri teknolojisinin dezavantajı olarak değerlendirilen verinin belirli bir noktaya kadar büyümesi hangi parametrelerle ve nasıl iyileştirilmelidir?

Problem 5:Aynı iki katılımcının blok üretmesi durumunda bu iki katılımcıdan hangisinin popüler olduğu içermiş olduğu blok sayısı ile belirlenmektedir. Popüler olan katılımcının seçilmesi durumu adillik kavramı düşünüldüğünde nasıl iyileştirilmelidir?

Blok zinciri teknolojisine ait belirlenen açık problemlerin nasıl çözüleceğine dair ilgili yaklaşımlar gelecekte yapılması planlanan çalışmalar olarak değerlendirilmektedir.

KAYNAKÇA

[1] K.Wüst, A. Gervais, Do you need blockchain?, IACR CryptologyePrint Archive, 2017, pp. 375.

[2] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamaria, To blockchain or not to blockchain: That is the question, IEEE IT Professional, 20(2),2018, pp. 62-74.

[3] X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L.Bass, C. Pautasso, and P. Rimba, A taxonomy of blockchain-based systems for architecture design, IEEE International Conference on Software Architecture (ISCA), 2017, pp. 243-252.

[4] M. English, S. Auer, and J. Domingue, Blockchain technologies & the semantic web: a framework for symbiotic development, In Computer Science Conference for Universityof Bonn Students, 2016, pp. 47-61.

[5] E. Gaetani, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, Blockchain-based database to ensure data integrity in cloud computing environments, In Italian Conference on Cybersecurity (ITA-SEC),1816, 2017.

[6] G. Greenspan, Avoiding the pointless blockchain project, 2015. https://www.multichain.com/blog/2015/ 11/avoiding-pointless-blockchain-project/(Erişim Tarihi: 26.07.2018)

[7] J. Sousa, A. Bessani, and M. Vukolić, A byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform, arXivpreprint arXiv:1709.06921, 2017.

[8] Hyperledger Fabric. https://www.hyperledger.org/ projects/fabric(Erişim Tarihi: 26.07.2018)

[9] Hyperledger Fabric. https://hyperledger-fabric.readthedocs.io/en/release-1.2/whatis.html(Erişim Tarihi:26.07.2018)

[10] S. W. Cocco, G. Singh, Top 6 Technical Advantages Of Hyperledger Fabric For Blockchain Networks, 2018. https://www.ibm.com/developerworks/cloud/library/cl-top-technical-advantages-of-hyperledger-fabric-for-blockchain-networks/index.html (Erişim Tarihi:19.07.2018)

[11] Hyperledger Fabric. https://media.readthedocs.org/pdf/hyperledger-fabric/latest/hyperledger-fabric.pdf(Erişim Tarihi: 26.07.2018)

[12] A. M. Antonopoulos, “Mastering Bitcoin: unlocking digital cryptocurrencies,” O’Reilly Media, Inc., 2014.

[13] M. Conti, C. Lal, S. Ruj et al., A survey on security and privacy issues of bitcoin, IEEE Communications Surveys&Tutorials, 2018.

[14] J. H. Park, J. H. Park, Blockchain security in cloud computing: use cases, challenges, and solutions, Symmetry, 9(8), 2017, pp.164.

FIGHT AGAINST PLAGIARISM AS AN IMPORTANT ASPECT OF INFORMATION SECURITY

Sedat Akleylek[1], Kübra Seyhan[2]
[1,2]Ondokuz May University, Samsun, Turkey
[1]*sedat.akleylek@bil.omu.edu.tr, kubra.seyhan@bil.omu.edu.tr*

Abstract. Blockchain technology has emerged as a result of the need for trusted mediator in centralized systems and the search for more reliable and efficient systems. Features of blockchain technology such as distributed network structure, end-to-end communication logic, hash value calculation and and cryptographic operations such as digital signature have made blockchain technology preferable for many work areas. Blockchain technology, which enables fast and secure transactions in many areas such as energy and finance sectors, e-government technology and cloud storage systems, is now effectively used in transactional data sharing. In this study, the principles of blockchain technology is explained and the properties of this are detailed based on cryptographic operations. Furthermore, the characteristics of blockchain technology are given and the advantages and disadvantages of blockchain technology are discussed. The research results of Hyperledger Fabric for permissioned blockchain and the unauthorized cryptocoin (for example Bitcoin) technologies are presented and their parameters are evaluated when deciding the suitability of blockchain technology for a system are explained. Finally, some problems related to the future of blockchain technology, which will cause the source of some recent developments, are discussed.

Keywords: Blockchain, Bitcoin, Hyperledger Fabric.