MAKÜ FEBED
ISSN Online: 1309-2243
http://dergipark.gov.tr/makufebed
DOI: 10.29048/makufebed.365066

Mehmet Akif Ersoy Üniversitesi Fen Bilimleri Enstitüsü Dergisi 9(1): 75-82 (2018)
The Journal of Graduate School of Natural and Applied Sciences of Mehmet Akif Ersoy University 9(1): 75-82 (2018)

Derleme Makale / Review Paper

Blokzinciri Teknolojisi ve Yakın Gelecekteki Uygulama Alanları

İsmail KIRBAŞ

Mehmet Akif Ersoy Üniversitesi, Mühendislik-Mimarlık Fakültesi, Burdur

Geliş Tarihi (Received): 12.12.2017, Kabul Tarihi (Accepted): 19.02.2018
Sorumlu Yazar (Corresponding author): ismailkirbas@mehmetakif.edu.tr
+90 248 2132751 *+90 248 2132704*

ÖZ

Bu çalışmada günümüzde giderek değerlenen popüler halen sanal para uygulamalarının temelini oluşturan blokzinciri teknolojisi ele alınmıştır. Blokzinciri teknolojisi güvenilir bir merkez kullanımı zorunluluğunu gerektirmeyen dağıtık bir kayıt yönetim sistemi olarak tanımlanabilir. Çalışmamızda geleneksel alışveriş yöntemi ile blokzinciri yapısı arasındaki temel farklılıklar ve blokzinciri kavramını meydana getiren teknolojiler incelenmiştir. Ardından blokzinciri yapısını oluşturan blokların üretilmesi ve transfer işlemlerinin nasıl gerçekleştirildiği açıklanmıştır. Çalışmanın son bölümü ise yakın gelecekte kullanılması planlanan uygulama alanları hakkında bilgiler ve yazılım çözümlerine ayrılmıştır.

Anahtar Kelimeler: Blokzinciri, Dağıtık Hesap Defteri, Dağıtık Uzlaşma, Uygulama Alanları

Blockchain Technology and Its Application Areas in Near Future

ABSTRACT

In this study, Blockchain technology, which is becoming increasingly popular and is still the foundation of virtual money applications, has been considered. This technology can be described as a distributed record management system that does not require a trusted centre. In our study, we investigated the fundamental differences between the traditional transaction method and the technologies that bring about the concept of the blockchain. Then, it is explained how to make the blocks constituting the blockchain structure and how the transfer operations are performed. The last part of the study is devoted to software solutions and information about the application areas planned to be used in the near future.

Keywords: Blokchain, Distributed Ledger, Distributed Consensus, Application Areas

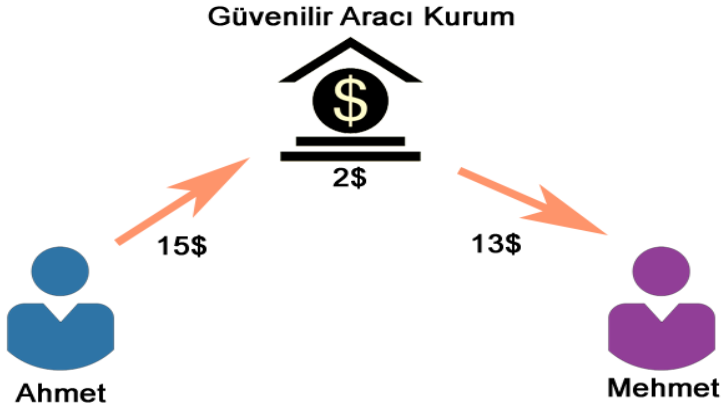
GİRİŞ

Günümüzde başta Bitcoin olmak üzere çok çeşitli sanal para birimlerinin üretilmesi ve borsalar üzerinden el değiştirmesinin yaygınlaşması ile tüm dünyada sanal paraya yatırım yapma oranı hızla artmaktadır. Sanal para alışverişinin temelini merkezi olmayan bir onaylama mekanizması oluşturmaktadır. Çalışmamızın konusu kripto-paranın da temelini oluşturan sayısal değerlerin güvenli alışverişini sağlayan blokzinciri kavramının incelenmesi ve yakın gelecekteki muhtemel uygulama alanlarının belirlenmesidir. Bitcoin (Nakamoto, 2008) sanal para birimi ile blokzinciri kavramları çoğu zaman birbiri ile karıştırılmaktadır. Bitcoin sahibine belli bir gizlilik sağlayarak merkezi bir otoritenin onayına ihtiyaç duymaksızın düşük iletim masrafları ile dünyanın her yerinde ödeme yapmayı sağlayan ve merkezi bir yönetime bağlı olmayan bir sanal kripto-paradır (Mukhopadhyay ve ark., 2016). Blokzinciri teknolojisi ise günümüzde yaygın olarak Bitcoin transferlerinde kullanı-

lan dağıtık bir kayıt yönetim sistemi olarak tanımlanabilir. Blokzinciri altyapısı sadece sanal para transferleri için oluşturulmamıştır. Bununla birlikte bir sayısal ya da fiziksel varlığın sahipliğinin izlenmesi ve bu varlıklar üzerinde gerçekleşecek işlemlerin takip edilmesi amacıyla da kullanılabilir. Çalışmamızda güncel bir örnek olması sebebiyle Bitcoin tarafından kullanılan blokzinciri sistemi ele alınacaktır.

DAĞITIK ONAY MEKANİZMASI

Günümüzde iki taraf arasında internet üzerinden gerçekleşen para alışverişlerinde alışveriş işlemi iki tarafın da güvendiği merkezi bir otorite aracılığıyla gerçekleştirilmekte ve gerçekleşen işlem otorite tarafından kayıt altında tutulmaktadır. Para transferleri resmi kurum ve kuruluşlar tarafından belirlenmiş yasalara göre gerçekleştirilir ve yapılan işlemler ülkelerin vergi denetimine tabidir. Şekil 1'de Ahmet güvenilir bir aracı kurum vasıtası ile Mehmet'e 15$ göndermek istemektedir. Güvenilir aracı kurum öncelikle Ahmet'in kimliğini tespit eder ve ardından Ahmet'in hesabında transfer işlemine yetecek bakiyenin olup olmadığını kontrol eder. Yeterli bakiye varsa bunu bloke eder. Mehmet'in kimliğini kontrol ederek Mehmet'e ait hesabın bakiyesini transfer edilecek bakiyeden kendi komisyonunu (örnekte 2$ olarak belirtilmiştir) keserek aktarır. İşlem güvenliğinin sorumluluğu güvenilir aracı kuruma aittir ve herhangi bir uyuşmazlık veya yasal itiraz halinde işlem geri alınabilir. Ülkeler arasında gerçekleşen bu tür para transferlerinin tamamlanması genellikle birkaç günü bulmaktadır. Günümüzde dünya üzerinde kullanılan kâğıt paraların sahibi ve yöneticisi devletlere ait merkez bankalarıdır. Kâğıt para ile ilgili yapılan tüm işlemler sahibi olan merkez bankası tarafından denetlenmektedir.



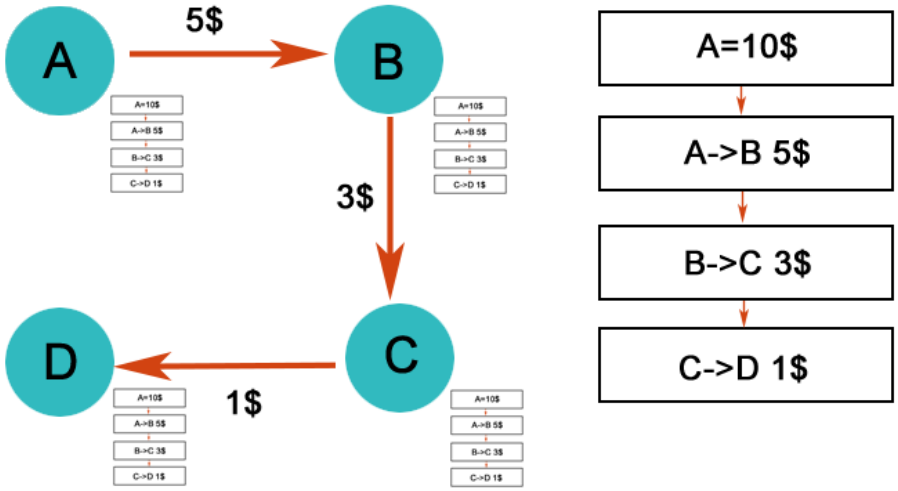
Şekil 1. Güvenilir kurum aracılığıyla gerçekleştirilen bir transfer işlemi modeli.

Blokzinciri yapısında alışverişi yapacak kişi veya kurumun kimliği önemli değildir. İşlemler elektronik cüzdanlar arasında gerçekleşir. İnternet üzerinden gerçekleştirilen sanalpara işlemlerinde taraflar arasında güvenli alışverişin sağlanabilmesi için asimetrik kriptografi teknikleri kullanılmaktadır. Bir elektronik cüzdanın açık ve gizli olmak üzere iki adet gizli anahtarı bulunur. Cüzdanın sahibi gizli anahtarı bilen kişidir. Gizli anahtar kaybolduğunda cüzdana yükleme yapılabilirken, cüzdandan harcama yapmak mümkün olmaz.

Blokzinciri altyapısı açık kaynak kodludur ve herhangi bir merkezi sistem tarafından yönetilmez. Sistemde güvenilir bir aracı yoktur ve işlem onay mekanizması dağıtıktır. Blokzinciri ağı üzerinde yer alan bilgisayarlar birer düğüm (node) olarak adlandırılırlar ve birbirleri ile uçtan uca bağlıdırlar. Blokzinciri ağı dinamiktir ve herhangi bir bilgisayar istediği zaman ağı terk edebilir veya dâhil olabilir. Ağ üzerinde gerçekleştirilen bütün alışveriş işlemleri küresel bir hesap defterinde (open ledger) tutulur. Bu hesap defterindeki kayıtlar tamamen şeffaftır ve tüm hareketler ağ üzerindeki düğümler tarafından takip edilebilir. Ağda yer alan düğümlerin hiçbiri güvenilir olmak zorunda değildir ve birbirlerine herhangi bir üstünlükleri yoktur.

Şekil 2'de A, B, C ve D olarak isimlendirilmiş 4 adet cüzdan bulunmaktadır. A cüzdanından başlangıçta 10$ değerinde bir bakiye bulunmaktadır. Ardından A cüzdanındaki 5$ B cüzdanına transfer edilir. B cüzdanındaki 3$ C cüzdanına, C cüzdanındaki 1$'da D cüzdanına transfer edilmiştir. Gerçekleştirilen tüm işlemler ardışık olmak zorundadır ve aynı anda birden fazla transfer gerçekleştirilemez. İşlemin yapılabilmesi için öncelikle gönderim yapmak isteyen cüzdanda yeterli bakiye olduğundan emin olunması gerekir. Yeterli bakiye varsa transfer isteği ağda bulunan bütün yakın düğümlere gönderilir, yakın düğümlerden en az 3 tanesi transfer işlemini onayladıktan sonra bu işlem küresel hesap defterine kayıt edilir ve ardından tüm düğümler küresel hesap defteri kayıtlarını günceller böylece onaylanmış tüm işlemlerin ağa bağlı düğümler tarafından senkroni-

ze edilmesi sağlanır. Onaylama ve güncelleme işlemi gerçekleştikten sonra değiştirilemez, iptal edilemez ve silinemez. Ancak tüm cüzdan kayıtları herkese açıktır ve takip edilebilir.



Şekil 2. Düğümler arasında para aktarımı işlemi ve küresel hesap defteri eşlemesi.

Blokzinciri teknolojisi ile eski merkezi ve dağıtık veritabanı sistemleri arasındaki belli parametrelere göre yapılan kıyaslama sonuçları Tablo 1'de verilmiştir. Bitcoin transfer işlemleri ile geleneksel banka modelinin belli özelliklere göre yapılan kıyaslaması Tablo 2'de verilmiştir.

Tablo 1. Blokzinciri ile eski merkezi ve dağıtık veritabanı karşılaştırması (Bozic ve ark., 2016)

Özellikler	Blokzinciri	Merkezi Veritabanı	Dağıtık Veritabanı
Kayıt bütünlüğü	Yüksek	Orta	Orta
Kullanılabilirlik	Yüksek	Düşük	Orta
Hata toleransı	Yüksek	Düşük	Yüksek
Gizlilik	Düşük	Yüksek	Orta
İşlem zamanı	Düşük	Yüksek	Orta
Güvenilmez düğümler arası işbirliği	Yüksek	Düşük	Düşük

Tablo 2. Bitcoin ile mevcut banka modelinin kıyaslanması (Tschorsch and Scheuermann, 2016).

Özellik	Banka Modeli	Bitcoin
Denetim	Merkez bankası	Uzlaşma
İşlem doğrulaması	Merkezi	Uzlaşma
Para Üretme	Krediler	Madencilik
Paranın değeri	Döviz kuru	İş ispatı, arz talep, güven
Paranın Kaynağı	Teoride sınırsız	Sınırlı sayıda
Para transferi	Aracılı, geri alınabilir	Doğrudan, geri alınamaz
Gizlilik	Uygulamaya bağlı	Belli ölçüde anonim
İşlem ücreti	Hesap ücreti, işlem ücreti	Teoride sabit işlem ücreti
İşlem süresi	Teorik olarak anlık, pratikte gün mertebesinde	Dakikalar mertebesinde

BLOKZİNCİRİ YAPISI

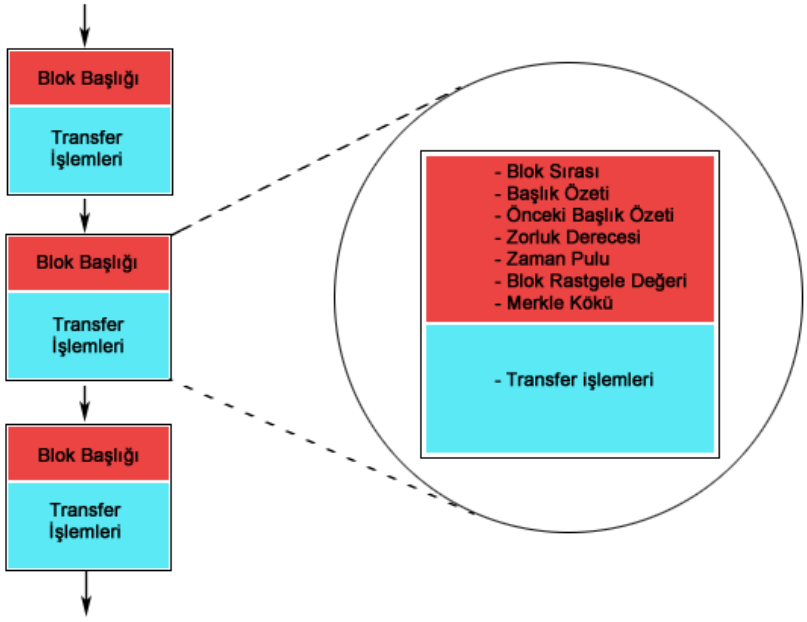
Şekil 2'de gösterilen transfer işlemleri 1MB büyüklüğünde bloklar halinde kayıt edilmektedir. Her kayıt bloğu birbirine ardışık olarak bağlıdır ve bir öncekinin sayısal imzasını taşır. Her blok kendi başlık bilgisi içerisinde hem kendisine hem de bağlı bulunduğu bloğa ait SHA-256 algoritması kullanılarak hazırlanmış iki adet kriptografik özet değerine (hash) sahiptir.

Özetleme algoritmasının birbirine yakın girdiler için bile benzersiz çıktılar ürete-bilmesi ve çıktıdan girdinin tahmin edilememesi sistem güvenliği açısından son derece önemlidir. Örneğin SHA-256 özetleme algoritması kullanılarak "merhaba" ifadesi özetlendiğinde "7fdc9f4717c5fe66df286c700fab969b4d6209d03aa846 24c5f8f58c17c9c058" şeklinde bir çıktı üretilirken giriş ifadesine sadece bir nokta ekleyip "merhaba." şekline dönüştürdüğümüzde daha önceki ifadeye pek de benzer olmayan "dfd9dad4ed172b61cf303165caae7135e9e66bb69d6c 52e383a8728cf8360108" ifadesi elde edilmektedir. Taraflar arasında güvenli iletişimin sağlanabilmesi için Bitcoin blokzinciri üzerinde eliptik eğri Diffie-Hellman anahtar değişimi metodu kullanılır (Franco, 2015).

Özet değerler takip edilerek en son bloktan ilk bloğa kadar geri gidilebilmektedir. Bir bloğa bağlı birden fazla blok olmamalıdır, eğer böyle bir durum meydana gelirse bu duruma çatallaşma (fork) adı verilir ve çatallaşmanın olduğu yer tespit edilerek kısa zincir yok edilir ve blokzinciri oluşumuna uzun zincir üzerinden devam edilir.

Bağlı bulunan bloğun başlık bilgisi içerisinde herhangi bir değişiklik yapılırsa bu durum iki bloğun başlık özetlerinde uyuşmazlığa sebep olacağından ve bu durum en baştaki düğüme kadar geri götürülme ihtiyacı doğuracağından imkânsız olarak kabul edilir. Böylelikle yapılan işlemler üzerinde geriye dönük düzeltme ve silme işleminin yapılması engellenmiş olur. Bu özellik blokzinciri mekanizmasını en güçlü güvenlik özelliğidir (Singh ve Singh, 2016).

Şekil 3'te birbirine bağlı ardışık bloklardan oluşan blokzinciri yapısı ve bir bloğa ait detaylı bilgi yer almaktadır. Buna göre başlık yapısı içerisinde blok sırası, blok başlık özeti, bağlı bulunan bloğa ait başlık özeti, bloğun üretildiği zamana ait zaman damgası değeri, blok rastgele değeri ve transfer işlemlerine ait Merkle kökü değeri bulunur (Antonopoulos, 2014).



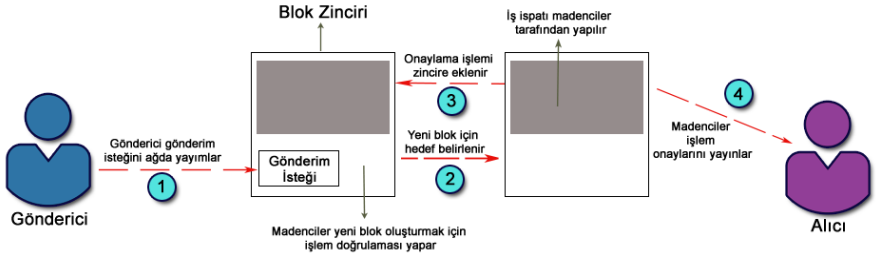
Şekil 3. Blokzinciri ve blokzincirini oluşturan blok yapısı.

Bir blok içerisinde en az bir işlem yer alır ve bir blok 1 MB boyutundadır. Blok üst bilgisi 80 Byte uzunluğundadır ve bloğa ilişkin bilgileri içermektedir. Her bir transfer işlemi en az 250 Byte uzunluğundadır ve bir blokta ortalama 350-500 arası işlem bilgisi yer alır (Çarkacıoğlu, 2016).

Alışveriş işlemlerinin tamamı ağda yer alan tüm taraflar tarafından takip edilebilir. İşlemlerin geçerliliği onaylandıktan sonra bir araya getirilirler ve böylece bloklar oluşturulur.

Geçerli bir blok teşkil edilebilmesi için öncelikle işlem gücüne dayalı bir bulmacanın çözülmesi istenir. Burada hedef bir özet fonksiyonunun tam karşılığını bulmak

yerine belli bir yaklaşık değerin elde edilmesidir. Bu kavrama iş ispatı (proof of work) adı verilmektedir. Bulmacayı çözmeye katılanlardan biri bu değeri (nonce) bulduğunda üzerinde çalışılan blok bir önceki geçerli blokla ilişkilendirilir ve ağ üzerinde yayılır. Ardından ağdaki tüm taraflar yeni bloğu yerel veritabanlarına ekleyerek senkronize olurlar. Açıklanan işleyiş Şekil 4 üzerinde görülmektedir. Bulmaca çözme yaklaşımı ile ilgili olarak Gray ve Kiayia (2015)'ın çalışmasına göz atılabilir.



Şekil 4. Transfer işlemi ve blokzincirine eklenme aşamaları.

Söz konusu bulmacanın hesaplama metotları ile çözümü oldukça güçtür ve çok fazla sayıda deneme yapmayı gerektirir. Bitcoin blokzinciri özetleme fonksiyonu olarak SHA-256'yı kullanır. Özet fonksiyonunun geriye doğru çözümlenebilmesi için aynı anda çok sayıda değerin denemesi gerekir. Bulmacanın zorluğu belirlenen hedef değere göre değişmektedir. Hedef değerin değeri azaldıkça daha az çözüm mümkün hale gelir ve daha zorlu bir bulmaca oluşturulmuş olur. Örneğin başlangıcında 40 adet sıfır bulunan bir özetin çözülebilmesi için 240 adet denemenin yapılması gerekir. Bulmacayı ilk çözen olma ihtimali hesaplama gücüyle doğru orantılıdır.

Kararlılığın sağlanması ve kabul edilebilir bekleme sürelerinin belirlenebilmesi amacıyla hedef değer ve dolayısı ile zorluk derecesi her 2.016 blokta yeniden belirlenir. Burada hedef bekleme süresi her bir blok için 10 dakika şeklindedir. Bir örnek üzerinden açıklamak istersek Ahmet'in Mehmet'e Bitcoin transfer etmek istediğini varsayalım. Bu durumda transfer isteği ağ üzerinde yer alan Cemal ve diğerleri tarafından da fark edilir. Bu isteği duyan katılımcılar transfer isteğini kendi yerel veritabanlarına kayıt ederler. Cemal bu ve bununla beraber onay aşamasında olan diğer transferlerin geçerli olduğunu onaylamak isterse bulmacayı çözme işlemi-ne katılır ve bulmacayı ilk çözen olursa geçerli bir blok oluşturur. Çözümün geçerliliği diğer katılımcılar tarafından onaylandıktan sonra blok oluşturmanın karşılığı olan ödülü de Bitcoin cinsinden elde etmiş olur. Böylece Ahmet'ten Mehmet'e transfer işlemi onaylanarak blok zincirine eklenmiş olur.

Blokzincirine yeni blokların eklenmesi işlemine madencilik adı verilir. Bu işlemi yapan katılımcılar da madenci olarak adlandırılırlar. Madenciler blokzincirinin kaydının tutulması ve transfer işlemlerinin yapılabilmesi için elzemdirler. Bitcoin için başlangıçtaki blok oluşturma ödülü 50 Bitcoin olarak belirlenmiştir ve her 210.000 blokta ödül yarılanır. Bu yaklaşık olarak 4 yıllık bir süreye tekabül eder. Yarılanma 2140 yılına kadar devam edecektir.

Transfer işlemlerinin gerçekleşebilmesi için tarafların kim olduğunun belli olması gerekmektedir. Ancak taraflar gizliliklerinin sağlanabilmesi amacıyla kişisel bilgilerini vermek zorunda değildirler. Bu amaçla tarafları adresleyebilmek için hesap cüzdanları kullanılır. Bir cüzdan aslında açık ve gizli anahtara sahip bir adresten oluşur. Cüzdan adresi SHA-256 özetleme algoritması ve açık anahtar kullanılarak oluşturulur. Adresler Base58 kodlama sistemini kullanır. Örnek bir cüzdan adresi "1ELiFNCg6v1wnc6cxTrY4m1MNDC5e5Vb1B" şeklinde ise bu adresin gizli anahtarı "5JNbVn7tXtkAp5rYagA9ZPaGDBCRueqycsyxTugpW CSTNLntXUz" şeklinde olur. Cüzdanın sahibi cüzdana ait gizli anahtarı bilen herhangi bir kişidir. Burada yasal bir ilişkilendirme ve hak sahipliği söz konusu değildir. Bu sebeple gizli anahtarın gizliliğinin korunması en önemli noktalardan biridir. Bir cüzdan üzerinden harcama yapabilmek için işlemlerin gizli anahtar kullanılarak imzalanması gerektiğinden gizli tutulması gerekir. Bir cüzdana gönderim yapılabilmesi içinse sadece adresinin bilinmesi yeterlidir. Bu konuyla ilgili olarak Möser ve ark. (2016) tarafından hazırlanan, gizli kriptografik anahtarların güvenliğinin artırılması konusundaki çalışmasına göz atılabilir.

Cüzdanlar genel olarak sıcak ve soğuk olmak üzere iki farklı yapıda olabilirler. Bunlardan ilki soğuk cüzdan (cold storage) olarak adlandırılır. Soğuk cüzdan kavramı, cüzdana ait bilgilerin internete bağlı bir bilgisayar veya sunucuda depolanması yerine, çalınma ve saldırı riskini minimize etmek amacıyla çevrimiçi olmayan bir cüzdan adresinde tutulmasıdır. Bu cüzdan adresi basılı bir kâğıtta tutulabileceği gibi bu amaç için özel olarak geliştirilmiş donanımlar da kullanılabilir. Şekil 5'te bu amaçla geliştirilmiş bir cüzdan donanımı yer almaktadır. Sıcak cüzdan ise internete bağlı sunucular veya bilgisayarlar üzerinde tutulan ve çevrimiçi olarak erişilebilen cüzdanlardır. Burada güvenlik açısından en büyük sorumluluğu çevrimiçi kripto-para borsaları veya çevrimiçi

cüzdan hizmeti veren firmalar üstlenir. Hesap bilgilerinin kaybolması veya cüzdan servisinin kapatılması halinde hesaplara erişim mümkün olmaz.

Şekil 5. Çevrimdışı cüzdan (cold wallet) örneği.

BLOKZİNCİRİ TEKNOLOJİSİ İÇİN UYGULAMA ALANLARI

Blokzinciri teknolojisi açık blokzincirleri ve özel blokzincirleri şeklinde iki bölüme ayrılabilir. Bu ana kadar açıklanan blokzinciri yapısı açık Blokzinciri yapısı için geçerlidir. Özel blok zinciri yaklaşımında izin yapısı söz konusudur ve ağdaki her öğe blokzincirine doğrudan katılamaz ve bloğun işleyişine müdahale edemez. Yine özel blokzincirlerinde iş ispatı yapısı yer almayabilir, işlem zamanı, ağ gecikmesi ve güvenlik gibi özellikler açık blokzinciri sistemlerinden farklılıklar gösterir (Bozic ve ark., 2016).

Blokzinciri teknolojisi başta Bitcoin gibi sanal para birimlerinin altyapısı üzerinde kullanılmak üzere geliştirilmiş olsa da günümüzde finans, sağlık, gayrimenkul, tedarik zinciri, hükümet kurumları ve telekomünikasyon gibi birbirinden farklı sektörlerde kullanılma potansiyeline sahiptir. Blokzinciri yapısı için para kullanımı zorunlu değildir ve sayısal olarak ifade edilebilen herhangi bir değer transferinde veya sahiplik işlemlerinde kullanılabilir.

Sözleşme dâhilinde gerçekleştirilen bir alışveriş işleminde genellikle bir arabulucu, alışverişte bulunan tüm tarafların şartlara uymasını sağlar. Blokzinciri, sadece üçüncü şahıslara olan ihtiyacı ortadan kaldırmakla kalmamakta; aynı zamanda, tüm defter katılımcılarının akıllı sözleşmeler yardımıyla sözleşme detaylarını bilmesini ve koşulların yerine getirilmesinden sonra sözleşme şartlarının otomatik olarak uygulanmasını sağlamaktadır.

Blokzinciri ve ilgili teknolojilerin geliştirilmesi ile ilgili açık kaynak kodlu çalışmalar da bulunmaktadır. Bunların başında Linux Foundation tarafından desteklenen ve geliştiriciler için bir şemsiye proje olan “Hyperledger” gelmektedir. Hyperledger 2015 Aralık ayında 17 farklı firmanın katılımı ile oluşturulmuştur ve halen 130’un üzerinde üyeye sahiptir. Bu projenin amacı açık kaynak kodlu blokzinciri projelerinin geliştirilmesi için sağlam ve verimli standartların belirlenmesidir. Bunula birlikte modüler bir blokzinciri yapısı oluşturulacak ve geliştirilecek arayüzler vasıtasıyla birbirinden farklı küresel hesap defterleri ile bağlantılar kurulabilecektir (Gupta, 2017).

Özellikle denetim ve güvenliğin tek elden sağlanmasının zor olduğu uygulama alanlarında dağıtık yapıdaki ve güvenilir bir merkez kurmanın maliyetinin yüksek olduğu durumlarda blokzinciri yaklaşımı avantajlı hale gelmektedir.

Yine dağıtık bir yapı gösteren Nesnelerin İnterneti uygulamaları için özellikle güvenlik amaçlı olarak bünyelerinde dışarıdan gelecek ataklara karşı bir güvenlik duvarı yazılımı bulunmayan kısıtlı kaynaklara sahip cihazlar için blokzinciri uygulamaları üzerinden güvenli mesajlaşma imkânı sağlanabilir. Yazılım güncellemelerinin uzaktan güvenli bir şekilde yapılabilmesi gömülü sistemler içerisine üretici tarafından bir akıllı sözleşme yazılımı yerleştirilebilir (Christidis ve Devetsikiotis, 2016; Samaniego ve Deters, 2016). Akıllı sözleşme bir işi yöneten sözleşme ve kurallar dizisidir. Bir işlemin parçası olarak blokzinciri üzerinde saklanır ve otomatik olarak yürütülür. Akıllı sözleşmeler kısmi ya da tam olarak kendi kendini yürütebilir olarak düzenlenebilir. Bu özellikleri ile geleneksel sözleşmelere göre daha

düşük maliyete, işlem zamanına ve daha yüksek güvenliğe sahiptirler.

Tedarik zinciri yönetiminde güvenilir belli bir merkezin onayına ihtiyaç duymaksızın işlemler ortak bir blokzinciri üzerinde gerçekleştirilip teslim aşaması sonrasındaki ödemeler otomatik hale getirilebilir. Bu işlemlerin takibi blokzinciri teknolojisi ile her aşamada taraflar tarafından şeffaf olarak izlenebilir. Sistem içerisinde yer alan taraflardan birinin kayıtları silmesi veya geriye dönük olarak değiştirilebilmesi mümkün değildir (Watanabe ve ark., 2015).

Enerji sektörü ele alındığında nesnelerin interneti ile blokzinciri uyumu ile makinelerin önceden tanımlanmış akıllı sözleşmeler doğrultusunda enerji satışı ve alımı yapabilmesi mümkün hale gelmektedir.

Sağlık alanında hastalara ait tıbbi kayıtların tutulması, taraflar arasında güvenli bir şekilde transfer edilmesi, ilaç sahtekârlığının tespit edilmesi ve önlenmesi konularında faydalanılabilir. Estonya hükümeti 2011 yılında Guardtime adlı bir proje başlatmış ve sağlık platformunu blokzinciri teknolojisi üzerinde çalışır hale getirmiştir (Mettler, 2016).

Tarımda ve zirai uygulamalarda yetiştirme, ilaçlama ve paketleme süreçlerinin takibinde ve onaylanmasında RFID sistemleri ile birlikte dağıtık veritabanı temelli güvenlik yaklaşımları kullanılmaktadır (Tian, 2016).

İçerik sağlayıcılar açısından bakıldığında üretilen içeriğe ait kullanım ve tekrardan üretim hakları da blokzinciri teknolojisinden faydalanılarak takip ve kontrol altında tutulabilir. Kullanım kısıtlamaları akıllı sözleşmeler ile teminat altına alınarak taraflar arasında içerik paylaşımı sağlanabilir.

Blokzinciri teknolojisinin bir diğer uygulama alanı müzik sektörü olabilir. Müzik endüstrisindeki kilit sorunlar sahiplik hakları, telif hakkı dağıtımı ve şeffaflıktır. Dijital müzik endüstrisi mülkiyet haklarını göz ardı ederken üretimden para kazanmaya odaklanır. Blokzinciri ve akıllı sözleşmeler teknolojisi, müzik haklarının merkezi ve kapsamlı bir veritabanını oluşturarak bu sorunu çözebilir. Aynı zamanda, sanatçıların şahsına ait telif hakları ve gerçek zamanlı dağıtımları tüm ilgili kişilere etiketlerle defter üzerinden şeffaf bir şekilde aktarılabilir. Sanatçılara, sözleşmenin belirtilen şartlarına göre dijital para birimi ile ödeme yapılabilir.

Devlet işlerinde pek çok farklı uygulama için blokzinciri teknolojisinden faydalanılabilir. Bunların başında kimlik, pasaport, doğum belgesi, evlilik cüzdanı, tapu kaydı gibi değerli evrakların ve resmi sertifikaların şifrelenmesi ve yönetimi gelmektedir. Blockzinciri teknolojisi resmi belge ve dokümanları şifreleyerek ve vatandaşları bu kritik bilgiye erişebilmek için yetkilendirerek kayıt tutmayı daha güvenilir hale getirebilir.

Alan adı yönetim sistemlerinde de blokzinciri teknolojisi kullanılarak alan adı sahipliği ve taraflar arasında devir işlemleri gerçekleştirilebilir. Birden fazla tarafın işbirliğini gerektiren yazılım geliştirme sektöründe de taraflar arasında yapılacak işlemlerin akıllı sözleşme transferleri ile sıralı ve çoklu onaylama sistemi ile otomatikleştirilerek takip ve idare edilmesi de mümkündür. Xu ve arkadaşları (Xu ve ark., 2017) çalışmalarında yazılım mimarilerinin tasarım ve değerlendirilmesinde blokzincirleri ve blok zinciri tabanlı sistemlerin sınıflandırma ve karşılaştırmasını yapmışlardır.

SONUÇ VE DEĞERLENDİRME

Çalışmamızda sanal para birimi Bitcoin'in fikir olarak ortaya atıldığı 2008 yılından günümüze kadar artarak gelen popülerliğinin altında yer alan temel mekanizma olan blokzinciri teknolojisi ele alınmış ve örnekler üzerinden geleneksel sistemlerden farklılıkları üzerinde durulmuştur. Çalışmamızın en temel amacı, blokzinciri kavramı ve muhtemel uygulama alanları hakkında yazılım geliştirme potansiyellerini ortaya çıkarmak ve bu konuda literatüre katkıda bulunmaktır.

Blokzinciri teknolojisi sadece bir sanal para birimi için geliştirilmiş bir teknolojik altyapı değildir. Aynı zamanda sayısal dünyada ifade edilebilen her tür değerin güvenilir bir merkezi yapıya ihtiyaç duymadan el değiştirmesini ve yapılan tüm işlemlerin bütün paydaşlar tarafından takip edilebilmesini mümkün hale getiren bir yapıdır. Yapılan işlemlerde takip edilebilirlik, şeffaflık, geriye dönük düzeltme ve silme yapılamaması gibi özellikler işlem güvenliğini artırıcı unsurlar olarak öne çıkmaktadır.

Günümüzde de pek çok kurum ve kuruluşun ilgisini çeken ve üzerinde araştırmaların yapıldığı bu teknoloji önümüzdeki yıllarda dağıtık yapıda işlem yapılan pek çok sektörde kullanıma geçerek günlük hayatımızın vazgeçilmez bir parçası olma yolunda hızla ilerlemektedir.

BİLGİLENDİRME

Bu çalışma, International Advanced Researches & Engineering Congress-2017 kapsamında sözlü bildiri olarak sunulmuş ve özet olarak bildiri kitapçığında yayınlanmıştır (Kirbaş, 2017).

KAYNAKLAR

Antonopoulos, A.M. (2014). Mastering Bitcoin: Unlocking Digital Cryptocurrencies, 1st ed. O'Reilly Media.

Bozic, N., Pujolle, G., Secci, S. (2016). A tutorial on blockchain and applications to secure network control-planes, in: 2016 3rd Smart Cloud Networks Systems (SCNS), 1–8.

Çarkacıoğlu, A. (2016). Kripto-para Bitcoin. Sermaye Piyasası Kurulu Araştırma Dairesi.

Christidis, K., Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. IEEE Access 4, 2292–2303.

Franco, P. (2015). Understanding Bitcoin: Cryptography, Engineering and Economics, 1st ed. Wiley.

Garay, J., Kiayias, A., Leonardos, N. (2015). The Bitcoin Backbone Protocol: Analysis and Applications, in: Advances in Cryptology - EUROCRYPT 2015: 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, Proceedings, Part II. Springer Berlin Heidelberg, Berlin, Heidelberg, 281–310.

Gupta, M. (2017). Blockchain for dummies, IBM Limited Edition. ed. John Wiley & Sons, Inc.

Kirbaş, İ. (2017). Blockchain Technology and Its Application Areas in Near Future. International Advanced Researches & Engineering Congress, Osmaniye Korkut Ata University, Osmaniye, Turkiye.

Mettler, M. (2016). Blockchain technology in healthcare: The revolution starts here, in: 2016 IEEE 18th International Conference on E-Health Networking, Applications and Services (Healthcom), 1–3.

Möser, M., Eyal, I., Gün E. (2016). Financial Cryptography and Data Security: FC 2016 International Workshops, BITCOIN, VOTING, and WAHC, Revised Selected Papers. Springer Berlin Heidelberg, Berlin, Heidelberg, 126–141.

Mukhopadhyay, U., Skjellum, A., Hambolu, O., Oakley, J., Yu, L., Brooks, R. (2016). A brief survey of Cryptocurrency systems, in: 2016 14th Annual Conference on Privacy, Security and Trust (PST), 745–752.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system (Technical Report). www.bitcoin.org.

Samaniego, M., Deters, R. (2016). Blockchain as a Service for IoT, in: 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 433–436.

Singh, S., Singh, N. (2016). Blockchain: Future of financial and cyber security, in: 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I), 463–467.

Tian, F. (2016). An agri-food supply chain traceability system for China based on RFID blockchain technology, in: 2016 13th International Conference on Service Systems and Service Management (ICSSSM), 1–6.

Tschorsch, F., Scheuermann, B. (2016). Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. IEEE Commun. Surv. Tutor. 18: 2084–2123.

Watanabe, H., Fujimura, S., Nakadaira, A., Miyazaki, Y., Akutsu, A., Kishigami, J.J. (2015). Blockchain contract: A complete consensus using blockchain, in: 2015 IEEE 4th Global Conference on Consumer Electronics (GCCE), 577–578.

Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C., Rimba, P. (2017). A Taxonomy of Blockchain-Based Systems for Architecture Design, in: 2017 IEEE International Conference on Software Architecture (ICSA), 243–252.