VERİ BİLİMİ DERGİSİ
www.dergipark.gov.tr/veri

Nesnelerin İnterneti Güvenliğinde Blok Zinciri Uygulamaları

İrfan KÖSESOY[1]*

[1]*Yalova Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği, Yalova*

Makale Bilgisi

Başvuru:
03/07/2019
Kabul:
13/07/2019

Özet

IoT cihazların askeri ve sivil alanda kullanımı yaygınlaşmakta, bununla birlikte her alana özgü cihaz sayısı ve buna paralel olarak üretilen veri miktarı da önemli ölçüde artmaktadır. IoT'nin hızla gelişmesi, cihazların ve cihazlar arasında paylaşılan verilerin güvenlik sorununu de beraberinde getirmektedir. Düşük bellek, düşük bilgi işlem gücü ve sınırlı pil ömrü IoT cihazlarının tipik özellikleridir. Cihazlar, heterojen yapıları ve kısıtlı kaynaklarından dolayı karmaşık ve maliyetli hesaplamalara sahip geleneksel güvenlik önlemleri ile korunamamaktadır. Başlangıçta sadece finansal değer transferi için tasarlanmış olan blok zinciri teknolojisi son yıllarda siber güvenlik alanında da kullanılmaya başlanmıştır. Blok zincirinin hata toleransı, kriptografik güvenlik avantajı ve ademi merkeziyetçi mimarisi gibi özellikleri sayesinde dünya genelinde birçok araştırmacı ve veri güvenlik analistini bu teknolojiyi IoT'nin güvenlik ve gizlilik problemlerini çözmek için nasıl kullanılabileceğine odakladı. Bu çalışmada, blok zincirinin IoT güvenliğinde karşılaşılan problemleri çözme potansiyeli analiz edildi. Bu amaçla IoT güvenliğinde karşılaşılan problemlerin neler olduğu, blok zinciri teknolojisinin nasıl işlediği ve literatürde blok zinciri teknolojisinin IoT güvenliğinde nasıl çözüm olarak önerildiği anlatılmıştır.

Anahtar Kelimeler: *Nesnelerin İnterneti, IoT, Blockchain, Siber Güvenlik*

Blockchain and IoT Security

Abstract

Use of IoT devices in military and civilian context is becoming more common, however, the number of devices specific to each field and the amount of data generated in proportion to it are also increasing significantly. The rapid development of IoT also brings the security issues of devices and the data shared between them. Low memory, low compute power, and limited battery life are typical features of IoT devices. Due to their heterogeneous structure and limited resources, devices cannot be protected by traditional security measures with complex and costly calculations. Originally designed for the transfer of financial value, blockchain technology has been used in cyber security in recent years. Because of its decentralized architecture, error tolerance and encryption security advantages such as pseudonymous identities, data integrity and authentication, researchers and security analysts around the world are focusing on blockchain to resolve IoT security and privacy issues. In this study, the potential of blockchain to solve problems encountered in IoT security is analyzed. To do this, the problems encountered in IoT security, how blockchain technology works and how blockchain technology is proposed as a solution to IoT security in literature are examined.

Keywords: Internet of Things, IoT, Blockchain, Cyber Security

İletişim e-posta: Irfan.kosesoy@yalova.edu.tr

1 Giriş

Elektronikte ve kablosuz iletişim teknolojilerindeki hızlı değişim, toplumda benzeri görülmemiş gelişmelere katkıda bulunmuştur. Bu gelişmeler birçok alana uygun olarak geliştirilen elektronik cihazlar, üretim maliyetlerindeki düşüş ve gerçek dünyadan dijital dünyaya bir paradigma kayması sayesinde yaşandı. İnsanların birbirleri ile ve yaşadıkları çevreyle olan iletişim şekli değişerek dünyayı daha iyi anlar hale geldi.

Nesnelerin İnterneti (IoT-Internet of Things), Kablosuz Algılayıcı Ağlardan (WSN), Radyo Frekansı Tanımlamasına (RFID) kadar, Internet üzerinden algılama, hareket etme ve iletişim kurma yeteneklerini sağlayan bir dizi teknoloji olarak ortaya çıkmıştır [1]. IoT, mevcut şehirleri akıllı şehirlere, elektrik şebekelerini akıllı şebekelere, evleri akıllı evlere dönüştürmede merkezi bir rol oynamaktadır. IoT kişisel kullanım dışında, hastanelerde ameliyat takibi, hava durumunun tespiti, araçların takibi ve kendi aralarında haberleşmesi, akıllı ulaşım sistemleri ile ulaşımın optimize edilmesi, tarımda verimliliğin arttırılması gibi toplumun spesifik ihtiyaçlarının karşılanmasında da önemli rol oynamaktadır. Çeşitli araştırma raporlarına göre, bağlı cihaz sayısının 2020 yılına kadar 20 ila 50 milyar arasında olacağı [1] ve global ekonomiye 7.1 trilyon dolar katkı sağlayacağı tahmin edilmektedir [2]. IoT'nin, günlük hayatta farklı endüstrilerde ve kişisel amaçlarla kullanımının bu denli yaygınlaşması ve hâlihazırda yapılan çalışmalar sonucu donanımsal teknolojide ve araçlar arası iletişimdeki bant genişliğinde yapılan iyileştirmelerle gelecekte daha önemli hale geleceği açıktır.

IoT'nin hızla gelişmesi, cihazların ve cihazlar arasında paylaşılan verilerin güvenlik sorununu da beraberinde getirmektedir. Uygulama alanının kapsamı göz önüne alındığında, IoT ortamındaki güvenliğin kritiklik seviyesi değişmektedir. E-sağlık, altyapı kontrolü ve dronlar gibi uygulamalar tipik olarak can güvenliği etkilerine sahip olabilir, bu nedenle bu alanlarda güvenlik kaygıları olağanüstü ve baskındır. Örneğin ameliyat sırasında hastaya ilaç akışını düzenleyen cihazın işlevsiz kalması hastada kalıcı hasarlara veya ölüme sebep olabilir. Buna benzer hayati öneme sahip uygulamalar sebebiyle IoT cihazlarda güvenlik oldukça önemlidir. Geleneksel ağlar için geliştirilmiş hesaplama maliyeti yüksek güvenlik çözümleri donanımsal kısıtlardan dolayı IoT cihazlarına uygulanamamaktadır. IoT'de güvenliğin bir diğer zorluğu da farklı alanlar için geliştirilmiş donanımların yer aldığı heterojen ortamdır. Bu sebeplerden ötürü IoT için henüz global olarak kabul görmüş bir referans modeli oluşmamıştır.

IBM işletme enstitüsüne göre [3], IoT'nin geleceği için yönetim modelinin maliyetli ve dominant bir merkezi mimariden öz düzenlemeli ve özerk yönetimli bir modele dönüştürülmesi kritik öneme sahiptir. Böyle bir dönüşüm, ölçeklenebilirlik, düşük altyapı maliyeti, özerklik, güvenilir bir ortamda güvenli işlemler, kullanıcı odaklı gizlilik, erişim kontrolü ve ağ saldırılarına karşı dayanıklılık sağlayacaktır. Blok zinciri mimarisinin kendine özgü, şeffaflık, sağlamlık, denetlenebilirlik ve güvenlik gibi özellikleri vardır [4]. Bu bağlamda, blok zinciri mekanizması, sayılan ihtiyaçları karşılayan bir model olarak kabul edilebilir.

Blok zinciri başlangıçta Bitcoin şeklinde bir finansal işlem protokolü olarak düşünülmesine rağmen, şifrelenmiş takma kimlikler, ademi merkeziyetçilik, hata toleransı, veri bütünlüğü ve kimlik doğrulaması gibi özellikleri göz önüne alınarak, araştırmacılar ve güvenlik analistleri tarafından IoT'nin güvenlik ve gizlilik problemlerinin çözümünde kullanılabileceği düşünülmüştür. Bunun yanında yapılan çalışmalarda blok zincirinin kripto paralar için kullanılan halinin, işlem onaylarındaki gecikme, büyük depolama gereksinimi, yüksek hesaplama maliyeti ve enerji gereksinimi gibi sebeplerden dolayı, IoT ortamında güvenli ve verimli bir şekilde kullanılmadan önce derinlemesine değerlendirilmesi gerektiği sonucuna varılmıştır.

Bu çalışmada, blok zincirinin IoT güvenliğinde karşılaşılan problemleri çözme potansiyeli analiz edildi. Bu amaçla IoT güvenliğinde karşılaşılan problemlerin neler olduğu, blockchain teknolojisinin nasıl işlediği ve literatürde blok zinciri teknolojisinin IoT güvenliğine nasıl çözüm olarak önerildiği anlatılmıştır.

Makalenin geri kalanı şu şekilde organize edilmiştir: Bölüm 2'de, IoT mimarisi hakkında bilgi verilmiştir. IoT'nin tehdit ortamı ve sistemlerdeki güvenlik performans gereksinimleri anlatılmıştır. Bölüm 3'te blockchain teknolojisinde geçen kavramlar ve çalışma mekanizmasının nasıl olduğu gösterilmiştir. Bölüm 4'te blockchain teknolojisindeki gelişmeler ve IoT üzerindeki etkisi,

IoT güvenliğinde blockchainin nasıl kullanıldığı, uygulamada karşılaşılan güncel zorlukların neler olduğu anlatılmıştır.

2 IoT

Geleneksel ağlar ve IoT arasındaki en önemli fark, son cihazlarda mevcut olan kaynak seviyesidir [5]. IoT genellikle RFID ve sensör düğümleri gibi kısıtlı kaynağa sahip gömülü cihazları içerir. Düşük bellek, düşük bilgi işlem gücü ve sınırlı pil ömrü IoT cihazlarının tipik özellikleridir. Geleneksel ağlar ise, güçlü bilgisayarlar, sunucular, akıllı telefonlar gibi daha geniş kaynaklara sahip cihazları içermektedir. Bu nedenle geleneksel ağlar, herhangi bir kaynak gözetmeksizin karmaşık ve çok faktörlü güvenlik protokolleri ile güvence altına alınabilirken, IoT cihazların güvenliği için geliştirilecek algoritmaların pil ömrü, bellek ve işlemci kullanımı gibi kaynak tüketimini göz önünde bulundurması gerekmektedir. Geleneksel ağlar ve IoT arasındaki farklar tablo 1'de verilmiştir.

2.1 IoT'de güvenlik ve performans gereksinimleri

Gelecekte geliştirilecek IoT sistem ve cihazların belirli bir standartlara uygun olması gerekmektedir. Bu standartlar içerisinde dikkat edilmesi gereken en önemli iki başlık güvenlik ve performanstır. Makhdom ve arkadaşları [6]'da yaptıkları literatür taramasında güvenlik sorunları ve performans gereklerini sırasıyla şekil 1 ve şekil 2'deki gibi kategorize etmiştir.

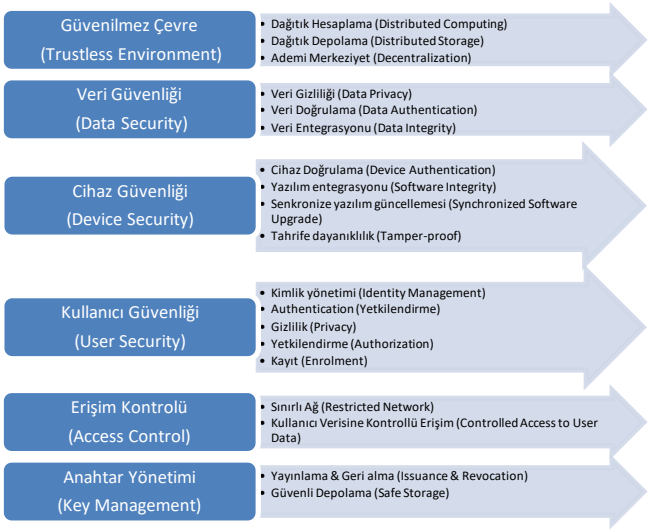
IoT sisteminin en temel güvenlik gereksinimi güvenilmez bir ortamda çalışabilir olmasıdır. IoT uygulamalarının çoğu sensör verilerine dayanmaktadır. Bu nedenle, veri manipülasyonuna ve yetkisiz paylaşıma karşı güvenlik gereklidir. Ayrıca, çevre sensörleri (sıcaklık, nem, gaz vb.), güvenlik kameraları ve kamuya açık alanlarda fazla koruma olmadan konuşlandırılan akıllı trafik sistemi sensörleri gibi IoT cihazlarının çoğu fiziksel olarak tehlikeye açıktır [7], [8]. Bu nedenle, IoT cihazında yüklü olan kodun ve cihazlar arasında paylaşılan verilerin bütünlüğü sağlanmadıkça, IoT sisteminde hiçbir işlemin güvenli olduğu düşünülemez [9]. Bu nedenle, cihaz güvenliği üreticilerin ve güvenlik araştırmacılarının dikkat etmesi gereken bir diğer önemli unsurdur. IoT sistemlerinin ağı, düğümlerin bozulmasına ve kötü amaçlı yazılım saldırılarına karşı korumak için, cihazları ağa eklemeden önce doğrulaması gerekir. Benzer şekilde, cihazlara yüklenen kodun bütünlüğünü doğrulamak için sık sık kontroller yapılmalıdır. Cihaz yazılımı hakkında herhangi bir şüphenin olması durumunda, güvenli yazılım güncellemesi gerçekleştirilinceye kadar ilgili düğüm geçici olarak iptal edilmelidir.

IoT aygıtları yazılım ve donanımlarda oluşabilecek tahriflere karşı dirençli (temper-resistant) olmalıdır. Donanımlarda bellek, güç ve hesaplama kaynaklarının yetersiz olması nedeniyle yüksek kriptografik güvenlik önlemi alınamamaktadır. Bu nedenle ağın güvenliği için daha hafif güvenlik protokolleri kullanılmalıdır. Bir diğer önemli gereklilik kayıt, kimlik yönetimi, kimlik doğrulama ve yetkilendirme dâhil olmak üzere kullanıcı

Tablo 1. IoT ve Geleneksel ağların karşılaştırılması

IoT	**Geleneksel Ağ**
• Düşük bellek, düşük işlem gücü ve sınırlı pil ömrüne sahip gömülü sistem cihazlardır. • İnternete ve ağ geçidi cihazlara 802.15.4, 802.11a / b / g / n / p, LoRa , ZigBee, NB-IoT ve SigFox gibi düşük bant genişliği ve güce sahip sistemlerle bağlanır. • Çok farlı veri içeriği ve formatı vardır. • Çeşitlilikten dolayı standart bir güvenlik protokolü geliştirmek zordur. • Bilgisayar tabanlı güvenlik yaklaşımı, kaynak kısıtı olan IoT cihazlarına uygulanamaz. • Tehditlere karşı yeterli güvenlik önlemi yoktur. Kullanıcıların güvenliği ve gizliliği ile ilgile tehditler vardır. • Dünya genelinde IoT çözümlerinde tutarlılık ve standardizasyon eksikliği vardır.	• PC, sunucu, akıllı telefon gibi daha geniş kaynağa sahip cihazlar bağlanır. • Fiber optik, DSL / ADSL, WiFi, 4G ve LTE gibi daha güvenli ve daha hızlı kablolu/kablosuz ortamlar üzerinden iletişim kurar. • Neredeyse aynı işletim sistemine ve veri formatına sahiptirler. • Güvenlik tasarımına bakarsak, güvenlik duvarlarına, IDS/IPS'ye dayanan statik ağ çevre korumasının bir karışımı ile korunur ve son cihazlar, anti virüs ve güvenlik/yazılım yamaları gibi ana bilgisayar tabanlı yaklaşımlarla güvence altına alınır.

güvenliğidir. Güvenli bir IoT sistemi, ağa ve kullanıcı verilerine yetkisiz erişime karşı da korunmalıdır.



Şekil 1. IoT sistemlerde güvenlik gereksinimleri

IoT sistemlerinin çoğunun gerçek zamanlı veri paylaşımına bağlı olması nedeniyle sistemin performans verimliliği, güvenliği kadar önemlidir. IoT sistemlerde istenen performans gereksinimlerinin bazıları Şekil 2'de verilmiştir. Gelecekteki IoT sistemlerini insan hatalarına karşı korumak için, sistemi kendi kendini düzenleyen ve yöneten şekilde tasarlamak gerekir. Verimli bir IoT sistemi, düşük bellek, düşük güç tüketimi ve düşük hesaplama yeteneği gibi son cihazların kısıtlı kaynaklarına hitap etmelidir. Ancak, performans verimliliğinde artış yapmak uğruna, sistemin güvenliği tehlikeye atılmamalıdır.

Şekil 2. IoT sistemlerde performans gereksinimleri

3 Blok Zinciri

Bilgi teknolojilerinde kullanıcılar arasında güvenli veri akışı, özellikle sanal paraların internet üzerinden aktarıldığı finansal sistemler açısından oldukça önemlidir. Bu tarz sistemlerde veriler karmaşık bir doğrulama ve denetleme mekanizması kullanılarak sağlanmaktadır. Satoshi Nakamoto 2008 yılında yaptığı çalışmada [10], günümüzde başta finans sektörü olmak üzere birçok alanda büyük etki yaratan iki radikal kavram önerdi. Bunlardan ilki, herhangi bir merkezi otorite veya finansal kuruluştan destek almadan değerini koruyan sanal bir kripto para birimi olan Bitcoin'dir. Bitcoin, merkezi olmayan, denetlenebilir ve doğrulanabilir P2P (peer to peer) ağ üzerinde, toplu ve güvenilir bir şekilde tutulmaktadır. Kavramlardan ikincisi de popülerliği şifreli para biriminin kendisinden bile ileri giden blok zinciri (blockchain) algoritmasıdır. blok zinciri algoritmasının en önemli özelliği birbirini tanımayan dolayısıyla güvenmeyen kişiler arasında güvenli veri transferine olanak sağlamasıdır. Bitcoinin icadından sonra blok zincirinin farklı versiyonları kullanılarak binlerce farklı kripto para birimi ortaya çıkmıştır. Bu yayının yazıldığı tarih itibariyle kripto paraların piyasa hacmi 290 milyar dolara yaklaşmıştır. 2009 dan sonra kripto paraların arka planında güvenli satışın yapılmasını sağlayan blok zinciri algoritması hatasız çalışmaktadır. Bu güne kadar kripto paralarda yaşanan güvenlik sorunları blok zinciri algoritmasından değil kullanıcı taraflı hatalardan kaynaklanmaktadır.

Blok zinciri çoğaltılmış ve bir ağın üyeleri arasında paylaşılan dağıtılmış bir veri yapısıdır [4]. Dolayısıyla sadece kripto paralar için değil farklı alanlara da uygulanabilir yapıdadır. Kripto paralarda güvenli olarak uygulandığı görüldükten sonra finans sektörü dışında, başta siber güvenlik olmak üzere, dijital oylama, müzik, sigortacılık, emlak, sağlık, kamu hizmeti gibi birçok alanda uygulanmakta veya uygulanması konusunda araştırmalar yoğun bir şekilde devam etmektedir.

3.1 Temel Kavramlar

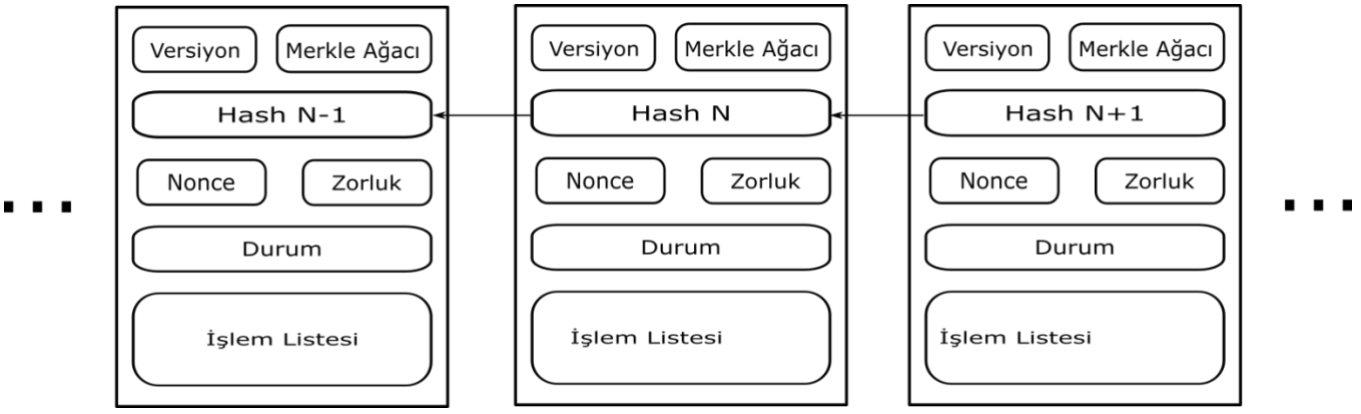
Blok zinciri, bir veri tabanı gibi düşünülebilir. En bilindik veri tabanı olan ilişkisel veri tabanında veriler tablolar içinde satır ve sütunlar halinde tutulur. İlişkisel veri tabanında bir veya birden fazla tablonun ilişkilendirilmesi ile veri tabanı oluşturulur. Verilere, bu veri tabanı üzerinden ulaşılır, sorgular aracılığıyla ekleme, silme güncelleme işlemleri yapılır. Blok zincirini de verilerin bloklar içinde tutulduğu ve birbirine

bağlandığı bir veri tabanı olarak düşünebiliriz. Ancak verilerin tutulmasında ve ulaşılmasında farklı bir yöntem uygulanır. Blok zinciri, yüksek verim, merkezi olmayan kontrol, düşük gecikme süresi, değişmez veri ve dahili güvenlik gibi özellikleri ile ön plana çıkar. Burada blok zincirini klasik veri tabanından ayıran en önemli özellik merkezi olmayan yapıdır. Blok zinciri kopyası, birbirine p2p ağı ile bağlı birden fazla bilgisayar üzerinde tutulur. Yani veriler bir merkez veya sunucu yerine dağıtık olarak tutulur. Ağa bağlı her düğüm belli aralıklarla blok zincirini günceller. Güncelleme yapıya bir dizi kriptografik ve matematik işlem sonucunda yeni bloğun veya bloklardan birine yeni işlemin eklenmesi anlamına gelir. Ağ içerisinde işlemi gerçekleştiren düğüm, blok zincirinin kopyasını tutan diğer tüm düğümlere bilgi verir. Ağdaki düğümlerin her biri benzer matematiksel ve kriptografik işlemi kullanarak veriyi ekler. Ancak verinin blok zincir içine dahil edilmesi için onaylanması gerekir. Onaylama işlemi ağa bağlı düğümlerin mutabakatı (consensus) ile sağlanır. İki düğümün mutabık olması yapılan matematiksel işlem sonrası aynı sonucu elde etmeleri anlamına gelmektedir. Bu aşamada farklı mutabakat yöntemleri kullanılabilmektedir (PoW, PoS .. vb.). PoW (Proof of Work) algoritmasında demokratik bir yol izlenerek ağa bağlı düğümlerin çoğunluğunun (%51) işleme onay vermesi durumunda işlem blok zincirine eklenir, aksi durumda reddedilir. Blok zinciri teknolojisini daha iyi anlamak için buraya kadar geçen önemli kavramlara daha detaylı bakalım.

3.1.1 Blok (block)

Blok, kabaca verilerin tutulduğu veri listesi ve başlık kısmından oluşur. Şekil 3'te blokla ilgili detaylar ve blokların birbirine hash kodu ile nasıl bağlandığı gösterilmiştir. Blok detaylarına geçmeden önce blokların kimliğini belirlemede ve düğümler arasındaki mutabakatın sağlanmasında önemli yeri olan hash kodunun nasıl üretildiğini anlamak gerekir.

Hash kodu bilinen şifreleme fonksiyonlarının en güvenlileri arasında yer alan SHA-256 (Secure Hash Algorithm) algoritması kullanılarak üretilir. İsmin sonunda yer alan 256 sayısı, algoritmanın şifreleme sonucunda ürettiği 256 bitlik sayısal değeri (32 bayt) ifade etmektedir. Buna göre algoritma 2^{256} farklı ikili sayı dizisi oluşturabilir. Girilen her karakter dizisini boyuttan bağımsız olarak sabit uzunlukta, ve her seferinde aynı sonucu döndürecek şekilde şifreler. Algoritmanın güçlü yanlarından biri de birbirine çok yakın karakter dizilileri için çok farklı sonuçlar üretmesidir. Örneğin "blokzinciri" kelimesi için üretilen hash kodu "e96e2639a9190006a89c253f2b940b67dd8b403d984047d79b2adbf7962789eb" iken "blokzincir" kelimesi için dönen hash kodu "94bddc04cf4fa84e9a76d619603421a1678048ccd439888f2d8e29a7ae6add5c" olmaktadır. Ayrıca hash kodundan yola çıkarak şifrelenmek istenen metne ulaşmak neredeyse imkânsızdır. Yani üretilen şifreden yola çıkarak orijinal metne ulaşılamamaktadır.



Şekil 3. Blok yapısı ve blokların birbirine bağlanma biçimi. İlk blok (genesis) dışında blokların her biri bir önceki bloğa işaret eder.

Blok zincirinde ilk blok kendinden önceye işaret etmez ve özel olarak "genesis" diye adlandırılır. Daha sonraki blokların her biri bir önceki bloğun hash kodu aracılığıyla zincire eklenir. Blok içinde yer alan bazı kısımlar aşağıda kısaca açıklanmıştır.

Hash: Bloğun tüm bilgilerinin şifrelenmesi sonucu oluşturulan ve bloğu temsil eden 32 baytlık kimlik bilgisi.

Versiyon numarası: Bloğun versiyon numarasını gösteren 4 baytlık bilgi.

Önceki Hash: Bloklar arası bağlantının sağlanması için tutulan önceki bloğun 32 baytlık hash bilgisi. Blokları arası işaretçi görevi görür.

Zaman damgası (time stamp): Blok oluşturulurken bloğa eklenen 4 baytlık zaman bilgisi.

Merkle ağacı: İşlemlere ait 32 baytlık hash bilgisidir. Blok içerisindeki tüm işlemler hash kodu üretilerek ikili bir ağaca yerleştirilir. Daha sonra ikili ağacın düğümleri birleştirilerek tekrar hash kodu üretilir. Bu işlem kök hash kodu üretilene kadar tekrar edilir ve son hash kodu blok içine eklenir.

Nonce: Blok oluşturmak ve farklı hash hesaplamaları için kullanılan 4 baytlık değer.

3.1.2 İşlem (Transaction)

Bloklar içinde tutulan veri kayıtlarıdır. Bitcoin üzerinden düşünecek olursak, kullanıcılar arasında transfer edilen dijital paralara ait hesap bilgileridir. Block zinciri kullandığı kriptografi ve matematiksel fonksiyonlar sayesinde işlemlerin değişmezliğini garantiler. İşlemlerin değişmezliği blok içerisinde iki aşamalı kontrolden geçer; ilk aşama blok içerisinde işlemlerin de dâhil olduğu tüm bilgilerin birleştirilmesi ile elde edilen hash kodudur. İkinci aşama merkle ağacı yoluyla sadece işlemlerden elde edilen hash kodudur. Her iki hash kodu da veri güvenliğinde kullanılmaktadır.

3.1.3 Madencilik (miner)

Bloğa yeni işlem ekleme ve sonrasında bunun diğer düğümler tarafından onaylanması için ağdaki tüm birimlere yayınlama işlemidir. Madencilik, madenci düğümler tarafından yapılır. Madencilik yapılırken karmaşık matematiksel fonksiyonlar çözülmeye çalışılır. Bu da yoğun hesaplama gerektiren bir iştir. Bitcoin madencileri yaptıkları işlem başına bahşiş (transaction fee) almaktadır. Verilen bu bahşiş daha çok kişinin madenci olmasını sağlamakta dolayısıyla sistemi daha güvenli hale getirmektedir.

3.1.4 Konsensüs Mekanizması

Konsensüs mekanizması, ağ üzerine dağılmış blokzinciri kopyalarının ağdaki tüm düğümler tarafından onaylaması için kullanılır. Blok zincirinde yapılacak herhangi bir değişiklik tüm düğümlere iletilir ve düğümlerden gelen yanıta göre onaylanır veya reddedilir. Birçok konsensüs mekanizması vardır. Ancak bunlar arasında en çok kullanılanları PoS (Proof of Stake) ve PoW (Proof of Work) mekanizmalarıdır. Bu mekanizmalar arasındaki en önemli fark işlem onayında kullandıkları oylama ve ödüllendirme şekilleridir [11]. PoW, bitcoinin de dahil olduğu bir çok kripto para tarafından kullanılmaktadır. PoW makanizmasına göre yapılan madencilik, yüksek enerji tüketimi ve işlem süresi gerektirmektedir. PoS, PoW ile kıyaslandığında daha düşük maliyet ve düşük enerji tüketimine ihtiyaç duyar.

4 IoT ve Blok zinciri

IoT, gittikçe artan güvenlik ve gizlilik sorunlarını çözmek için blok zincirin güçlü güvenlik altyapısını kullanabilir. Örneğin, heterojen IoT cihazları arasında güvenli veri paylaşımının zorluğu ve veri güvenilirliğinin garantisi, verilerin değişmezliğini garanti eden ortak blok zinciri platformu ile karşılanabilir. Bu nedenle, blok zinciri, merkezi olmayan mimarisi ile çoğunlukla güvenilmeyen bir ortamda çalışan IoT sistemler için ideal bir çözümler sunar.

Geçtiğimiz yıllarda, bulut bilişim teknolojileri, IoT'ye bilgiyi analiz etmek, işlemek ve onu gerçek zamanlı eylemlere ve bilgilere dönüştürmek için gerekli işlevselliği sağlamaya katkıda bulunmuştur [1]. Bulut bilişim ve benzer mantıkla çalışan merkezi mimariler, IoT'nin gelişimine büyük katkı sağlamıştır. Ancak bu mimarilerin güvenlik ve gizlilik konularındaki savunmaları endişe vericidir. Veri manipülasyonu konusunda, bulut servis sağlayıcısının bulutta ve ilgili servislerde depolanan veriler üzerinde kontrolü olduğu için güvenilir bir taraf olması gerekir. Bulut sağlayıcının kullanıcı verilerini değiştirme ihtimali vardır [12]. Oysa blok zinciri, ağdaki tüm madenci ve tam düğümlerin, blok zincirinin aynı kopyasını koruyacak şekilde düzenlenir ve güven, tüm ağ düğümleri arasında dağıtılır. Dolayısıyla, bir cihazın blok zinciri verilerini kötü bir amaçla değiştirmesi durumunda, sistem bunu reddeder ve blok zinciri durumu değiştirilmeden kalır. Ayrıca, tek başarısızlık noktası problemi olarak sayılan, yazılım hataları, siber saldırılar, güç sorunları, soğutma gibi sorunlar nedeniyle bulut sunucularının devre dışı kalma ihtimalleri vardır [13]. Blok zincirinde ise, veriler birçok düğümde çoğaltılır ve birkaç düğümde oluşabilecek sorunlar blok zinciri hizmetlerini bozmaz. Blok zinciri bu nedenle veri güvenliği ve ulaşılabilirlik açısından oldukça kullanışlıdır.

Bununla birlikte, blok zinciri verilerin tüm madenciler ve tam düğümlerde tutulmasını zorunlu kılar. Örneğin bu yazının hazırlandığı tarih itibarı ile bitcoin blok zinciri 226 GB boyutuna ulaşmıştır [14]. IoT'de, bu zorluk daha belirgindir, örneğin akıllı bir şehir IoT senaryosunda, yüz binlerce IoT düğümünden gelen sensör verileri blok zinciri boyutunda hızlı bir artışa sebep olacaktır, dolayısıyla IoT cihazlarının bu veriyi kullanması zorlaşacaktır [6].

IoT, cihazların güvenliği, yönetimi kapsamında merkezi mimari ve blok zincirinin ayrı ayrı avantaj ve dezavantajları vardır. Merkezi ve dağıtık mimarilerin IoT güvenliği ve yönetimi konusunda var olan eksikliklerin giderilmesi üzerine çalışmalar devam etmektedir. Şu an için blok zincirinin veya bulut teknolojisinin bilinen IoT problemlerine göre ayrı ayrı veya birlikte kullanılabileceği yerler belirlenip blok zinciri, bulut veya hibrit çözümler sunularak çözümler geliştirilebilir.

4.1 Literatür Özeti

Dünyadaki araştırmacılar ve yenilikçiler blok zinciri teknolojisinin IoT ortamına uygulanması için çalışmalar yürütmektedir. Bu çalışmalarda özellikle blok zincirinin ademi merkeziyetçi kontrol, değişmezlik, kriptografik güvenlik, hata toleransı, veri bütünlüğü, kimlik doğrulama ve akıllı sözleşmeler yapabilme gibi faydalarından yararlanmak amaçlanmaktadır. Bu bölümde bu amaçla yapılan bazı çalışmalar incelenmiştir.

Biswas ve Muthukkumarasamy [15]'de yaptıkları çalışmada, akıllı şehir varlıkları arasında güvenli iletişim için blok zinciri tabanlı bir framework önerdiler. Yazarlar, blok zincirin akıllı şehirdeki cihazlarla entegrasyonunun, tüm cihazların güvenli bir şekilde iletişim kurabilecekleri ortak bir platform sağlayacağını iddia etmektedirler. Ayrıca, blok zincirin veri erişimi ve veri bütünlüğü saldırılarını önleyebileceği ifade edilmektedir.

Ali Dorri ve Raja Jurdak [16]'deki çalışmalarında akıllı evler için tasarlanmış blok zinciri tabanlı hafif bir güvenlik mimarisi önerdiler. Akıllı evdeki blok zinciri uygulaması, geleneksel bir Bitcoin blok zincirinden birçok yönden farklıdır. Bitcoin blok zincirinden farklı olarak, akıllı evdeki yerel blok zinciri, sahibi tarafından merkezi olarak yönetilmektedir. Ayrıca, bu mimari bir politika başlığı (policy header) ile ağ sahibinin evinde olan tüm işlemleri kontrol etmesini sağlamaktadır.

[17]'daki yazarlar blok zincirinin endüstriyel IoT (IIoT) ile kullanılması için bir framework önerdiler. Bu framework, IIoT araçlarının bulut ve blok zinciri ağıyla haberleşmesini sağlamaktadır. Her IIoT cihazı, hem bulut hem de Ethereum blok zinciri için kontrol ve iletişim ara yüzü özelliklerine sahip tek kartlı bir bilgisayarla (SBC) donatılmıştır. IIoT cihazları depolama ve analiz yapmak üzere buluta veri göndermek, işlemleri blok zincir ağındaki diğer cihazlara gönderip almak ve akıllı sözleşmeleri tetiklemek üzere tasarlanmıştır.

VANET (Vehicular ad-hoc network) araçlar arası haberleşme ağıdır. Geleneksel VANET merkezi yönetim mimarisine göre çalışır. Merkezi yönetim nedeniyle tek başarısızlık noktası (single point of failure), kullanıcı gizliliği zaafı gibi sakıncaları vardır. Bu tür sorunlardan kaçınmak için Leiding ve ark. [18]'de merkezi olmayan, kendi kendini yöneten Ethereum blok zinciri tabanlı bir VANET önerdiler.

[19]'da IoT cihaz erişim kontrolü için blok zincir tabanlı bir çözüm olan "ControlChain" önerildi. Bu çalışmada Bitcoin blok zinciri ile aynı prensipler kullanılmakta ve IoT kontrolünün farklı yönlerini ele almak için çoklu blok zincirinin kullanılabileceği söylenmektedir.

[20]'de özellikle giyilebilir IoT araçları ve son kullanıcılar arasında veri gizliliğini koruyan blok zinciri tabanlı bir ağ geçidi önerildi. Kullanıcıların cihaz tercihleri şifrelenerek, sadece kullanıcı tarafından geri getirilecek şekilde blok zincirinde tutuldu.

[21]'de IoT üzerinde veri transferi, erişimi ve gizliliği gibi konulara odaklanıldı. Bu konularda güvenlik çözümleri sunmak için ethereum platformu kullanılarak blok zinciri tabanlı yöntemler önerildi.

4.2 Potansiyel blok zincir çözümleri

Bu bölümde blok zincirinin IoT'de kullanılabileceği bazı alanlar açıklanmıştır.

4.2.1 Adres Alanı

Blok zinciri 128-bit adres alanına sahip olan IPv6'ya karşın 160 bit adres alanına sahiptir [22]. Blok zinciri adresi 20 bayttır veya ECDSA (Elliptic Curve Digital Signature Algorithm) tarafından genel anahtardan üretilen 160 bitlik bir hash değerdir. 160 bitlik adres ile blockchain, yaklaşık 1.46×10^{48} IoT aygıtını adresleyebilir. Blok zinciri ile IANA (Internet Assigned Numbers Authority) gibi IPv4 ve IPv6 adreslerinin tahsis edilmesini yöneten merkezi bir otoriteye ihtiyaç duyulmamaktadır. Ayrıca, blok zinciri IPv6 dan 4.3 milyar daha fazla adresleme

olanağı sağlar. Dolayısıyla blok zinciri, IPv6'dan daha ölçeklenebilir bir çözüm olarak düşünülebilir. IoT cihazların düşük bellek ve hasaplama kapasitesi düşünüldüğünde, bu cihazların IPv6 yığınını çalıştırmaya uygun olmayacağını da söyleyebiliriz.

4.2.2 Veri Bütünlüğü ve Entegrasyonu

Blok zinciri ağına bağlı IoT cihazları tarafından iletilen tekil bir anahtara sahip veriler, ağ tarafından doğrulanmaktadır. Böylece iletilen verilerin doğrulanması ve bütünlüğü sağlanmaktadır. Ayrıca, bir IoT cihazında yapılan tüm işlemler veya gerçekleştirilen transferler ağa dağıtılmış olan blok zincirine kaydedilmekte ve güvenli bir şekilde takip edilmektedir.

4.2.3 Kimlik Doğrulama, Yetkilendirme ve Gizlilik

Blok zincirinde yer alan akıllı sözleşmeler (smart contracts), bir IoT Cihazına merkezi olmayan kimlik doğrulama yeteneği kazandırır. Ayrıca akıllı sözleşmeler, Role Dayalı Erişim Yönetimi (RBAC), OAuth 2.0, OpenID, OMA DM ve LWM2M gibi geleneksel yetkilendirme protokolleriyle karşılaştırıldığında, bağlı IoT cihazlarına daha etkili bir yetkilendirme erişim kuralı sağlayabilir. Bu protokoller bugünlerde IoT cihazının doğrulanması, yetkilendirilmesi ve yönetimi için yaygın olarak kullanılmaktadır. Akıllı sözleşmeler kullanarak kişi, grup veya makinelerin verilere erişim süresi, koşulu ve durumu belirlenip veri gizliliği sağlanabilir. Akıllı sözleşmeler ayrıca, kimlerin IoT yazılımını veya donanımını güncelleme, yükseltme, yama oluşturma, cihazı sıfırlama, bir servis veya onarım isteği başlatma yetkisi olduğunu detaylı olarak açıklar.

4.2.4 Güvenli İletişim

IoT uygulama iletişim protokolleri HTTP, MQTT, CoAP veya XMPP, hatta yönlendirme ile ilgili RPL ve 6LoWPAN protokolleri bile tasarım açısından güvenli değildir. Bu tür protokollerin, güvenli iletişim sağlaması için DTLS veya TLS gibi diğer güvenlik protokolleri ile kullanılması gerekir. Benzer şekilde, yönlendirmede, IPSec tipik olarak RPL ve 6LoWPAN protokollerinin güvenliğinde kullanılır. DTLS, TLS, IPSec , TinyTLS protokolleri, hesaplama ve bellek gereksinimleri bakımından ağır ve karmaşıktır. Blok zinciri ile anahtar yönetimi ve dağıtımı tamamen ortadan kaldırılmıştır, çünkü her IoT cihazı bir kez kendilerine ait bir GUID (Global Unique Identifier) ve asimetrik anahtar çiftine sahip olduktan sonra ağa bağlanmaktadır. Bu aynı zamanda, DTLS gibi diğer protokollerin veri iletişimi sırasında PKI sertifikalarının yönetimine ve değişimine olan ihtiyacı ortadan kaldırmaktadır.

5 Sonuç

Bu çalışmada, son yıllarda kripto paralar sayesinde çok popüler olan ve çalışma mantığı incelendiğinde siber güvenlik, eğitim, sağlık, müzik gibi bir çok alanda var olan problemlere çözüm üretebileceği düşünülen blok zinciri teknolojisi incelendi. Gene günümüzde popülerliği gittikçe artan ve neredeyse günlük hayatımızın her alanın da karşımıza çıkan IoT güvenliğinde ve işleyişinde yaşanan sorunlara değinildi. IoT'nin işleyiş ve güvenlik sorunlarından bazılarının blok zinciri teknolojisi ile nasıl çözülebileceğine değinildi.

Kaynaklar

[1] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Futur. Gener. Comput. Syst.*, vol. 88, pp. 173–190, Nov. 2018.

[2] D. Lund, C. MacGillivray, V. Turner, and M. Morales, "Worldwide and regional internet of things (IoT) 2014–2020 forecast : A virtuous circle of proven value and demand," 2014.

[3] P. Brody and V. Pureswaran, "Device democracy: Saving the future of the internet of things," *IBM, Sept.*, 2014.

[4] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*. 2016.

[5] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," *Wirel. Networks*, 2014.

[6] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, "Blockchain's adoption in IoT: The challenges, and a way forward," *J. Netw. Comput. Appl.*, vol. 125, pp. 251–279, Jan. 2019.

[7] O. Arias, J. Wurm, K. Hoang, and Y. Jin, "Privacy and Security in Internet of Things and Wearable Devices," *IEEE Trans. Multi-Scale Comput. Syst.*, 2015.

[8] B. Balamurugan and D. Biswas, "Security in Network Layer of IoT: Possible Measures to Preclude," in *Security Breaches and Threat Prevention in the Internet of Things*, IGI Global, 2017, pp. 46–75.

[9] A. Sadeghi, F. Lahouti, and M. Zorzi, "Constellation Shaping and LDPC Coding in a Bidirectional Full Duplex Communication," in *2015 IEEE Global Communications Conference (GLOBECOM)*, 2015, pp. 1–6.

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

[11] J. J. Sikorski, J. Haughton, and M. Kraft,

"Blockchain technology in the chemical industry: Machine-to-machine electricity market," *Appl. Energy*, 2017.

[12] 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 *CEUR Workshop Proceedings*, 2017.

[13] N. Kshetri, "Can Blockchain Strengthen the Internet of Things?," *IT Prof.*, 2017.

[14] "No Title." [Online]. Available: https://www.blockchain.com/charts/blocks-size. [Accessed: 30-Jun-2019].

[15] K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain technology," in *Proceedings - 18th IEEE International Conference on High Performance Computing and Communications, 14th IEEE International Conference on Smart City and 2nd IEEE International Conference on Data Science and Systems, HPCC/SmartCity/DSS 2016*, 2017.

[16] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internet of things: Challenges and Solutions," 2016.

[17] A. Bahga and V. K. Madisetti, "Blockchain Platform for Industrial Internet of Things," *J. Softw. Eng. Appl.*, 2016.

[18] B. Leiding, P. Memarmoshrefi, and D. Hogrefe, "Self-managed and blockchain-based vehicular ad-hoc networks," 2016.

[19] O. J. A. Pinno, A. R. A. Gregio, and L. C. E. De Bona, "ControlChain: Blockchain as a Central Enabler for Access Control Authorizations in the IoT," in *2017 IEEE Global Communications Conference, GLOBECOM 2017 - Proceedings*, 2018.

[20] S. C. Cha, J. F. Chen, C. Su, and K. H. Yeh, "A Blockchain Connected Gateway for BLE-Based Devices in the Internet of Things," *IEEE Access*, 2018.

[21] Z. Huang, X. Su, Y. Zhang, C. Shi, H. Zhang, and L. Xie, "A decentralized solution for IoT data trusted exchange based-on blockchain," in *2017 3rd IEEE International Conference on Computer and Communications, ICCC 2017*, 2018.

[22] A. M. Antonopoulos, *Mastering Bitcoin: unlocking digital cryptocurrencies*. " O'Reilly Media, Inc.," 2014.