Blokzinciri Tabanlı Siber Güvenlik Sistemleri

Article *in* ULUSLARARASI BİLGİ GÜVENLİĞİ MÜHENDİSLİĞİ DERGİSİ · December 2017

DOI: 10.18640/ubgmd.373297

2 authors:

Enis Karaarslan
Mugla Üniversitesi
80 PUBLICATIONS **175** CITATIONS
SEE PROFILE

Muhammet Fatih Akbaş
Izmir Katip Celebi Universitesi
11 PUBLICATIONS **27** CITATIONS
SEE PROFILE

BLOKZİNCİRİ TABANLI SİBER GÜVENLİK SİSTEMLERİ

Enis Karaarslan[1], Muhammet Fatih Akbaş[2]
[1]Muğla Sıtkı Koçman Üniversitesi, Bilgisayar Mühendisliği Bölümü, Muğla, Türkiye
[2]İzmir Kâtip Çelebi Üniversitesi, Bilgi İşlem Daire Başkanlığı, İzmir, Türkiye
enis.karaarslan@mu.edu.tr, mfatih.akbas@ikc.edu.tr

ÖZET

Kripto paralar (cryptocurrency), eşler arası (Peer-to-Peer) mimaride birbirine bağlı madenci düğümü adı verilen bilgisayarlara ve blokzinciri yapısında tutulan kayıt sistemine dayanmaktadır. Bu sistemler sadece bir para birimi sağlamamakta, bu altyapılar üzerinde çeşitli 'merkezi olmayan' (decentralized), dağıtık (distributed) sistemler/yazılımlar tasarlanmaktadır. Bu çalışmada blokzinciri sisteminin nasıl çalıştığı, sağladığı veri bütünlüğü, kullanılabilirlik, mahremiyet gibi güvenlik servisleri ve hata toleransı incelenmektedir. Blokzinciri yapısının; nesnelerin interneti (Internet of Things), akıllı şehirler, kişisel verilerin korunması, bilgisayar ağları için kullanımı gibi siber güvenlik konularındaki çalışmalar ele alınmaktadır. Blokzinciri uygulamalarındaki temel sorunlara ve olası çözümler gözden geçirilmiştir. Bu tür çözümlerin ağ güvenliğinde kullanımına dair önerilere yer verilmiştir.

Anahtar Kelimeler: Blokzinciri, Siber Güvenlik, Kripto Para

BLOCKCHAIN BASED CYBER SECURITY SYSTEMS

ABSTRACT

Cryptocurrency relies on the computers called miner nodes which are interconnected with Peer-to-Peer (P2P) architecture and the record system that is held in a blockchain structure. These systems do not only provide a currency; various decentralized, distributed systems/softwares can be designed on these infrastructures. This study examines how blockchain system works, investigates the provided security services like data integrity, availability, privacy and fault-tolerance. The studies of using blockchain structure in cyber security issues like protecting the Internet of Things (IoT), smart cities, computer networks and the privacy of the personal data is covered. Basic problems in the blockchain applications and possible solutions are discussed. Ideas for the use of such solutions in the network security are addressed.

Keywords: Blockchain, Cyber Security, Cryptocurrency

I. GİRİŞ (INTRODUCTION)

Bitcoin (BTC), bilindiği üzere P2P protokolünü kullanan ve merkezi olmayan bir dijital paradır. 2008 senesinde duyurulmuş ve 2009 senesinden beri aktiftir. Protokol çalışması [1] Satoshi Nakamoto adıyla yayınlanmasına rağmen, bu çalışmanın bilinmeyen kişi(ler) tarafından geliştirildiğine inanılmaktadır. Hiçbir finans kurumunun yönetmediği Bitcoin'in başarısı, alternatif bozukluk (altcoin) adı verilen türevleri ile devam etmiştir.

Makalenin hazırlandığı anda; bu tür paraların geçerli olduğu Coin Market Cap [2] borsasında işlemde olan 1325 farklı kripto para bulunmaktadır.

Kripto paralar, yapılan işlemleri P2P protokolü ile birbirine bağlı bilgisayarlar üzerinde blokzinciri yapısında tutmaktadır. Ethereum gibi birçok kripto para, sağladıkları API'ler aracılığı ile kendi altyapı ve para birimlerini kullanan başka yazılımların da geliştirilmesi için ortamlar sağlamaktadır. Ethereum [3] projesi kendisini bir blokzinciri uygulama platformu olarak tanımlamakta ve durdurulamaz uygulamalar geliştirilebileceğini öne sürmektedir.

Bu makalede, ikinci bölümde P2P ve blokzinciri temelli bu mimarinin nasıl çalıştığı ve öğeleri ele alınacaktır. Üçüncü bölümde, sistemin güvenilirliği ele alınacaktır. Dördüncü bölümde, bu mimarinin hangi güvenlik servislerini sağladığı belirtilecektir.

Beşinci bölümde, bu yapının siber güvenlik için kullanımına dair akademik çalışmalardan örnekler verilecektir. Altıncı bölümde, blokzinciri sistemlerindeki sorunlar ele alınacak ve bunları çözmeye yönelik yeni yaklaşımlara değinilecektir.

II. BLOKZİNCİRİ SİSTEMLERİ (BLOCKCHAIN SYSTEMS)

Bazı sistemlerde farklılıklar olmakla birlikte, BTC Mimarisi [1] yaygın olarak diğer alternatif bozukluk sistemlerde de kullanılmaktadır. Temel kavramlar aşağıda tanımlanmıştır:

- **Blokzinciri:** Blokzinciri, zamana göre sıralanmış ve sürekli büyüyen bir veri yapısıdır. Bloklar, yapılan işlem(ler)i ve bir önceki blokun adresini tutarlar. Blokzinciri, işlemlerin değiştirilemez listesinin tutulduğu bir kayıt defteridir (ledger). Ethereum'un kullandığı bloklarda çalıştırılabilir kod da bu blok içerisinde tutulmaktadır.
- **Akıllı Anlaşma (Smart Contract):** Ethereum projesi ile blokzincirinde akıllı anlaşmalar yapmak mümkündür. Bu anlaşmalarla; değer tutan, veri kaydeden ve çeşitli hesaplama görevleri için bloklara çalıştırabilir kod ekleyen uygulamaların geliştirilmesi mümkün olmaktadır.
- **Madenci Düğüm (Mining Node):** İşlemlerin gerçekleşmesini sağlayan bilgisayarlardır. Önceleri işlemci gücü kullanılırken, ekran kartlarındaki işlemcilerin veya bu iş için üretilmiş özel kartların kullanılması söz konusu olmuştur.
- **Madencilik Gücü:** Hash işlemleri çoğunlukla ekran kartlarının işlemcileri üzerinde GPU hesaplama gerçekleştirilmekte ve H/s (saniyede hash hesaplama) birimi ile Kilo-Mega-Giga (bin, milyon, milyar) biriminden güçleri tanımlanmaktadır. Bir ekran kartı Mh/s güçlerinde çalışmakta, makinelere takılan çoklu kartlarla yüksek madencilik güçlerine ulaşılabilmektedir.
- **Konsensus Protokolleri:** Blokzincirlerinin bütün düğümlerde aynı olabilmesi için kimin değişiklik yapacağını belirleyen kurallar bütünüdür. PoW ve PoS yaklaşımlarından söz etmek mümkündür. Çalıştığının Kanıtı (Proof of Work, PoW), her düğümün değişiklik önerisi yapabilme hakkı kazanmak için öncelikle çözmesi gereken bir bulmaca gibidir. Başkalarının çözmesinin zor olduğu ama işleyen tarafından kolaylıkla doğrulanabilecek bir değerdir. PoS (Proof of Stake), PoW'deki hesaplama yerine, sisteminde sahip olduğu zenginliğe (kripto para) göre bloğu yaratacak olanın seçildiği bir yaklaşımdır.
- **Hesap:** Her makine veya kullanıcıya özgü o kripto para birimini tutmaya yarayan tekil (unique) bir hesaptır.

Örneğin:
a94f5374fce5edbc8e2a8697c15331677e6ebf0b

Sistemin temel özellikleri:

- İşlemler merkezi değildir,
- İşlemler P2P ağda tüm düğümlere yayınlanır (broadcast),
- İşlemler birden fazla düğüm tarafından onaylanır ve sonunda blokzincire eklenir,
- Sistemdeki bütün hesaplar halka açıktır (public) ama anonimdir. Hesap ID'si aynı zamanda açık anahtar (public key) olarak kullanılır,
- Madenci düğümler, işlemleri bloklar olarak toparlar.

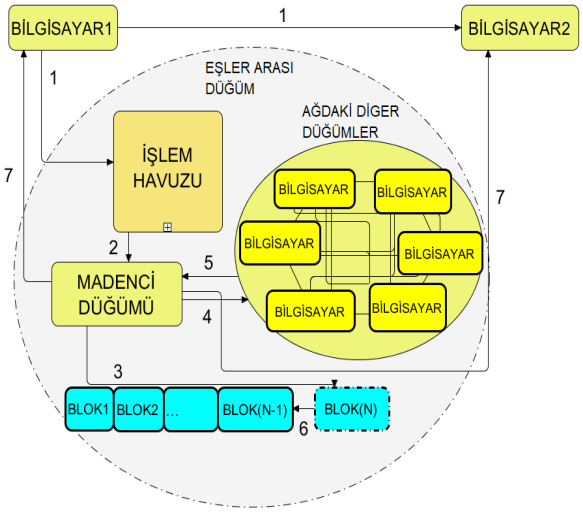
Blokzinciri uygulamasında madenci adı verilen sistemler, şu ana kadarki bütün işlemleri içeren bütün blokzincirini tutarlar. Bloğu oluşturacak düğümün seçimi konsensus protokolü ile gerçekleştirilir. Blokzinciri yapısı kullanan bir uygulama aracılığı ile Bilgisayar1 ve Bilgisayar2 makineleri arasında bir işlem yapılacağı bir senaryodaki yeni bloğun oluşturulması ve blokzincirine eklenmesi Şekil 1'de gösterilmiştir. İşlem aşamaları şekilde gösterilen numaralarla aşağıdaki gibidir:

1. Bilgisayar1 yapılacak işlemi Bilgisayar2 de dâhil olmak üzere eşler arası ağda yayınlar,
2. Sistemde işlem havuzunun (mining pool) kullanımı seçimli olabilmekte, işlemler yayınla öğrenilebilmektedir. Doğrulanmamış işlemler, düğümler tarafından çağırılır,
3. Ağda kullanılan protokole göre, n adet işlem toplu olarak bir bloğa yazılabilir. Düğümler tarafından yeni blok oluşturulur,
4. Doğrulama için eşler arası ağdaki bilgisayarlara yayın yapılır,
5. Doğrulama bilgisinin tamamlandığı bilgisi ağ içerisinde iletilir,
6. Eşler arası ağda konsensus protokolü ile bir madenci düğümü seçilir. Seçilen madenci düğümü, yeni bloğu blokzincirine ekler,
7. Talep edilen işlemin tamamlandığı bilgisi, işlemi gerçekleştiren makinelere iletilir.

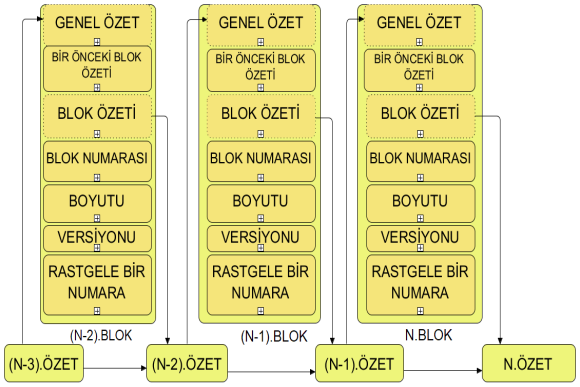
Bloklar, hash (özet) değeri ile önceki bloklara bağlanmaktadır. Bu süreçte önceki bloklardaki özet değerinden genel özet değeri oluşturulmaktadır. Aynı zamanda bir önceki bloğun özeti de tutulmaktadır. Blok içerisinde ise; 4 işlemin toplanarak bir bloğa yazılması durumunda alınan özetlerden kök özet (Merkle ağacının) oluşturulması Şekil 3'de gösterilmiştir.

Blokzinciri tabanlı uygulamaların geliştirilmesi için çeşitli altyapı çalışmaları bulunmaktadır. Linux Foundation tarafından yürütülen Hyperledger [4], 27 organizasyonun destek verdiği bir açık kaynak projesidir. Bunun yanı sıra farklı kripto paraları altyapıları da çeşitli API'ler sağlamaktadır. Örneğin; Ethereum blokzinciri platformu, akıllı anlaşmalar ile altyapıları üzerinde çeşitli uygulamaların çalıştırılmasına izin vermektedir. Solidity [5] gibi

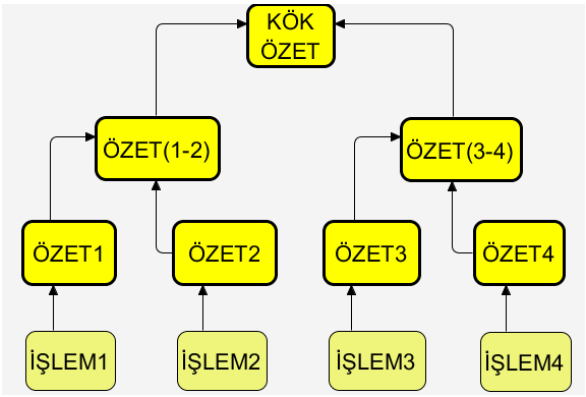
yüksek düzeyli dillerle Ethereum Sanal Makinesi (Ethereum Virtual Machine) üzerinde akıllı anlaşmalar geliştirmek mümkündür.



Şekil 1. Blokzinciri tabanlı uygulamada yeni bloğun zincire eklenme süreci



Şekil 2. Blokzinciri yapısı



Şekil 3. Merkle ağacının oluşturulması

III.SİSTEMİN GÜVENİLİRLİĞİ (RELIABILITY OF THE SYSTEM)

Saldırganların sistemi ele geçirmesi için, ağdaki düğümlerin çoğunluğunu ele geçirmesi gerekmektedir. Düğümlerin dağıtık olması, bu olasılığı da oldukça düşürmektedir.

Blokzinciri yapısında hash fonksiyonları aktif olarak kullanılmaktadır. Her blok, bir önceki bloğun sağlamasını (hash) tutar. Hash fonksiyonu olarak farklı algoritmalar da kullanılmakla birlikte, BTC SHA256 algoritmasını kullanmaktadır. Sistemdeki bir işlemi değiştirmek, zincirdeki tüm blokları da hesaplamayı gerektirecektir ki bu da muazzam bir işlem gücüne gereksinim duyacaktır. Zincirdeki her değiştireceği blok için diğer düğümleri de ikna etmesi ve bunun için de PoW hesaplamalarını gerçekleştirebilmesi gerekecektir. Bu da %51 saldırısı olarak tanımlanmaktadır, çünkü bunun için ağdaki bütün düğümlerin madencilik işlemci gücünün en az %51'ine sahip olması gerekecektir. Saldırı teorik olarak mümkün olsa da pratikte bu tür bir saldırı olası değildir ve etkisinin kısa süreceği ifade edilmektedir [6]. PoS kullanıldığında ise, saldırganın bütün kripto paranın en az %51'ine sahip olması gerekecektir ki Ethereum'da sadece konsorsiyumun elinde bulunan bir güçtür.

IV.GÜVENLİK SERVİSLERİ (SECURITY SERVICES)

Güvenlik servisleri açısından blokzincirinin, merkezi ve dağıtık veritabanlarından farkı Tablo 1'de [7] verilmiştir. Blokzinciri ile veri bütünlüğü (data integrity), kullanılabilirliği (availability) servisleri ve hata toleransı (fault tolerance) en iyi şekilde verilebilmektedir. Blokzinciri tabanlı sistemler, gizlilik (confidentiality) servisini hedeflememektedir.

TABLO 1. BLOKZİNCİRİ İLE MERKEZİ / DAĞITIK VERİTABANLARINDAKİ GÜVENLİK SERVİSLERİNİN KIYASLANMASI [7]

	Blokzinciri	Merkezi Veritabanı	Dağıtık Veritabanı
Kayıtların Bütünlüğü	Yüksek	Orta	Orta
Kullanılabilirliği	Yüksek	Düşük	Orta
Hata Toleransı	Yüksek	Düşük	Yüksek
Gizlilik	Düşük	Yüksek	Orta

İşlemi gerçekleştiren makinelerin bütün kayıtları ortada olsa da kime ait olduklarının belirli olmamasından dolayı mahremiyet (privacy) tabanlı servisler de verilebilmektedir.

V. SİBER GÜVENLİK İÇİN KULLANIMI (USAGE FOR THE CYBER SECURITY)

Yeni teknolojiler beraberinde yeni güvenlik tehditlerini getirmektedir. IoT, akıllı şehirler gibi popüler kavramların sağladığı yararların yanı sıra bilgi güvenliği konusunun iyi bir şekilde gözden geçirilmesi gerekmektedir. P2P tabanlı ve dağıtık blokzinciri mimarisi ile siber güvenlik için mahremiyet ve bütünlük başta olmak üzere çeşitli

güvenlik servisleri sağlayacak çözümler yapmak mümkündür. Blokzinciri, kriptografik algoritmalar, dijital imzalar ve özet fonksiyonları gibi güvenlik yöntemlerini kullanmaktadır. Bankacılık sektörü, finans kuruluşları, sağlık hizmetleri, elektronik oylama, IoT ve bilgisayar ağları için kullanımı söz konusudur. Güvenlik ve mahremiyet alanı üzerine yapılan çalışmalarda blokzinciri tabanlı yaklaşımların kullanımı gelecek vaat etmektedir [8].

Conoscenti ve arkadaşlarının literatür çalışmasında [9], blokzinciri teknolojisinin kullanıldığı durumlar incelenmektedir. Blokzinciri teknolojisinin bütünlük (integrity), anonimlik (anonymity) ve uyarlanabilirlik (adaptability) özelliklerini etkileyen unsurlar ele alınmaktadır. Blokzinciri teknolojisinin veri depolama yönetimi, malların ve verilerin ticareti, kimlik denetimi ve değerlendirme sistemleri gibi kategorilerde kullanıldığı belirtilmektedir.

Huh ve arkadaşlarının çalışmasında [10], IoT cihazlarının yönetimi için blokzinciri teknolojisinin kullanımı önerilmektedir. Platform olarak Ethereum'un seçildiği bu çalışmada, Ethereum'un akıllı anlaşması kullanılarak IoT cihazlarının davranışlarını belirleyen kodlar yazılmaktadır. Kimlik doğrulama amaçlı (authentication) kullanılan açık anahtarlı altyapı (Public Key Infrastructure, PKI) ile saldırganların Ethereum platformu üzerinde bulunan yönetim sistemini kontrol altına almasının önüne geçilmektedir. Anahtarların yönetimi için RSA kripto sistemi kullanılmaktadır. Açık anahtarlar (public keys) Ethereum'da, gizli anahtarlar (private keys) uçlardaki IoT cihazlarda saklanmaktadır.

Birçok nesnenin/cihazın birbirleriyle etkileşim halinde olduğu bir IoT ortamında hassas veriler söz konusu olmaktadır. Böylesine bir ortamda cihazlar arasındaki iletişimin ve hassas verilerin korunması gerekmektedir. Bu yüzden IoT güvenliği konusunun önemi her geçen gün artmaktadır. Dorri ve arkadaşlarının çalışmasında [11], IoT güvenliği ve mahremiyet için blokzinciri yaklaşımı önerilmekte ve akıllı evler için durum çalışması sunulmaktadır. Çalışmada önerilen çözümün DDoS ve Linking saldırılarına karşı etkinliği de analiz edilmektedir.

Biswas ve arkadaşlarının çalışmasında [12], akıllı şehirlerdeki güvenlik tehditlerine karşı koruma sağlamak ve akıllı şehirleri daha güvenli bir hale getirmek için blokzinciri teknolojisinin kullanımı ele alınmıştır. Akıllı şehirlerde bulunan cihazlarla blokzinciri teknolojisinin entegrasyonunun dağıtık bir ortamda güvenli veri iletişimini sağlayacağı ifade edilmektedir.

Blokzinciri teknolojisi işlemsel olarak maliyetlidir ve yüksek bant genişliğine gereksinim duyulmaktadır. Bu gereksinimler birçok IoT cihazı için uygun değildir. IoT'de blokzinciri teknolojisinin uygulanması; yüksek enerji tüketimi, ölçeklenebilirlik ve işleme zamanı gibi nedenlerden çok kolay değildir. Dorri ve arkadaşlarının bir diğer çalışmasında [13], IoT için iyileştirilmiş yeni bir blokzinciri mimarisi önerilmektedir. Bu çalışmada, Bitcoin'in altyapısını oluşturan klasik blokzinciri kullanımının getirdiği yükleri ortadan kaldırmak için hafif (lightweight) bir blokzinciri mimarisi kullanımından bahsedilmektedir. Önerilen çözüm, merkezi konumda ve özel olan değiştirilemez bir kayıt defterinden (Immutable Ledger, IL) ve merkezi olmayan konumda ve herkese açık (public) blokzincirinden oluşan hiyerarşik bir mimariye sahiptir. IL, ek yükü azaltmak için IoT'nin yerel ağ seviyesinde çalışmaktadır. Blokzinciri ise daha güçlü bir güven için daha üst seviyedeki uç cihazlarda bulunmaktadır. IoT için iyileştirilmiş bu blokzinciri mimarisi, güvenlik ve mahremiyet özelliklerini içinde barındırmakta olup blok onayı işleme zamanını azaltmak için PoW yerine dağıtık güven yöntemini kullanmaktadır. Madencilik süreci yoktur, bu da bazı gecikmeleri ortadan kaldırmaktadır. Simülasyon sonuçları, önerilen yöntemin düşük oranda paket ve işlem yükü getirdiğini göstermektedir. Servis reddi saldırısı (Denial of Service, DoS), modifikasyon saldırısı (modification attack), düşürme saldırısı (dropping attack) ve ekleme saldırısı (appending attack) gibi bazı saldırı türlerine karşı da yöntemin başarısı ölçülmüştür.

Kişisel verilerin korunması ve mahremiyet amacıyla da blokzincirinin kullanımı mümkündür. Bilindiği üzere, üçüncü parti yazılımları veya servisleri çok fazla miktarda kişisel ve hassas verileri toplamaktadır. Zyskind ve arkadaşlarının çalışmasında [14], blokzinciri tabanlı ve blokzinciri tabanlı olmayan depolama alanlarının birleştirildiği mahremiyet odaklı bir kişisel veri yönetimi platformu sunulmuştur.

Kişisel sağlık verilerinin tutulduğu elektronik sağlık kayıtlarına erişim denetim altında tutulmalıdır. Azaria ve arkadaşlarının çalışmasında [15], MedRec adını verdikleri blokzinciri çözümü tabanlı kayıt yönetim sistemi önerilmiştir. Hastaların, geniş kapsamlı ve değiştirilemez bir sağlık kaydına sahip olması ve bu kayda farklı sağlık kurumlarından kolaylıkla erişebilmesi hedeflenmiştir. Sistem, araştırmacı ve sağlık otoriterilerinin madenci olarak sisteme katkıda bulunması için anonim verileri bir ödül olarak vermeyi öngörmektedir. Madenci makineleri PoW ile sistemin güvenilirliğini sağlayacaktır.

Watanabe ve arkadaşlarının çalışmasında [16], dijital haklar gibi sözleşmelerin yönetiminin daha güvenli hale getirilmesi için yeni bir mekanizma önerilmektedir. Bu mekanizma, güvenilirlik skorunu (credibility score) kullanan yeni bir konsensus metoduna sahiptir. Bu yöntem ile birlikte proof-of-stake (PoS) yöntemi bir arada kullanılarak hibrit bir blokzinciri yapısı ortaya çıkmaktadır. Saldırganın kaynakları ele geçirmesinin önüne geçmesini

sağlamakta ve blokzincirini daha güvenli bir hale getirmektedir.

Bilgisayar ağları için kullanımına dair bazı çalışmalardan da söz etmek mümkündür. Gelecekte blokzinciri tabanlı DNS ve blokzinciri tabanlı internet söz konusu olabilecektir. DNSChain [17]; özgür, güvenli ve dağıtık bir DNS çözümü olarak ortaya atılmıştır. SecureChain [18], ağ cihazlarının yapılandırma dosyalarının ve log kayıtlarının saklanmasına yönelik bir yaklaşımdır. Log kayıtlarının daha güvenli bir mimaride tutulması; değiştirilemezlik ve inkâr edilemezlik ilkesinin sağlanması hedeflenmektedir.

İlgi çekici bir başka çalışmada, Barnas [19]; yeni bir siber savunma yaklaşımı modelinin gerektiğini belirtmiş ve ülke ulusal güvenliği için blokzincirinin kullanımına dair çeşitli önerilerde bulunmuştur. Blokzinciri ile değiştirilemez kayıtların oluşturulabileceği ve sistemde zayıflık takibi yerine değişiklikleri izlemenin daha etkin olacağı belirtilmiştir. Tedarik zinciri yönetiminde kullanımı ile aygıt yazılımlarının (firmware) takip edilebileceği belirtilmiştir. İletişim altyapısına saldırı yapıldığında, dağıtık mimarisinin ve güvenlik protokollerinin sayesinde iletişimin devamını sağlayabilen altyapıların kurulabileceğine değinilmiştir.

VI. SORUNLAR VE YENİ YAKLAŞIMLAR (ISSUES AND NEW APPROACHES)

Blokzinciri sistemlerinde, işlemlerin kayıtlarının tutulduğu blokların büyümesi ve bunun sonucunda yaşanan performans sorunları, büyük miktarlarda madenci düğümü kuran ve bir nevi fabrikalara dönüşen şirketlerin sistemi domine etme riski ve yüksek elektrik harcamaları gibi sorunlardan söz etmek mümkündür. O'Dwyer ve arkadaşlarının 2014'deki çalışmasında [20], Bitcoin altyapısının elektrik harcamasının İrlanda'nın elektrik tüketimi olan 3 GW'a yaklaştığı tahmin edilmiştir. Blokzinciri sistemlerinin yaygın kullanımında çok daha fazla elektrik harcamasının olacağı ve 4000 GW'ı aşabileceği tahmin edilmektedir. Bu da Amerika'nın toplam elektrik harcamasının iki katıdır [21].

Bu sistemlerdeki sorunlara farklı yaklaşımlarla çözüm bulunmaya çalışılmaktadır. Daha hızlı ve ölçeklenebilir bir çözüm olan Lightning Network [22] çözümü önerilmiştir. Dağıtık konsensusun sağlanması için PoW yaklaşımı yerine PoS yaklaşımı tartışılmakta ve bazı kripto paralar tarafından kullanılmaktadır. Böylece matematiksel problem çözmek için harcanan işlemci gücü yerine rastsal seçim [23] veya madencilerin sistemde bulundurduğu kripto para değerinin kullanımı [24] söz konusu olabilecektir. PoS ile sistemin çok daha az elektrik harcaması ve çok daha hızlı çalışmasının söz konusu olacağı iddia edilmektedir [23].

VII. SONUÇ (CONCLUSION)

Kripto paralar sadece farklı bir ekonomi yaratmakla kalmamakta, aynı zamanda kullandıkları P2P ağları ve blokzinciri yapısına dayalı mimarileri ile siber güvenlik için yeni çözüm önerilerine ilham olmaktadır. Blokzinciri yapısına dayanan bu mimari ile veri bütünlüğü, mahremiyeti, kullanılabilirliği güvenlik servislerinin ve hata toleransının sağlandığı etkin çözümler geliştirilebilmektedir.

Blokzinciri sistemleri ile siber güvenlik çözümlerinin etkinleştirilmesine yönelik çalışmalar gerçekleştirilebilir. Bu sistemlerin; IoT, akıllı şehirler ve bilgisayar ağlarının siber güvenliği için ve kişisel verilerin korunmasında kullanımına dair çalışmaların belli başlıları bu makalede sunulmuştur.

Blokzinciri tabanlı siber güvenlik sistemlerinin ele geçirilmesinin diğer çözümlere göre daha zor olduğunu da söylemek mümkündür. Saldırganın ağdaki madencilik gücünün en az %51'ini elinde tutması veya yazılım değişikliği için madenci düğümlerinin çoğunluğunu ikna etmesinin gerekmesi bu teknolojinin siber güvenlik sistemlerinde kullanımının önemini ortaya koymaktadır.

Blokzinciri sistemlerinde aşılması gereken sorunlar bulunmaktadır. Bunlardan en önemlisi; işlemlerin kayıtlarının tutulduğu blokların büyümesi ve bunun sonucunda yaşanan performans sorunlarıdır. Bunun yanı sıra, bu sistemlerin ihtiyaç duyduğu yüksek işlemci gücü ve yüksek elektrik sarfiyatı da önemli bir etmendir. Büyük miktarlarda madenci düğümü kuran kurumların sistemi domine etme riski de bulunmaktadır.

Lightning Network gibi daha hızlı ve ölçeklenebilir yeni ağların kurulması, P2P ağında hangi düğümün kaydı yapacağının seçiminde daha az enerji gerektiren PoS yaklaşımının kullanımı gibi yeni yaklaşımlar ortaya çıkmaktadır.

Blokzinciri teknolojisine dayanan siber güvenlik önlemlerinin çalışılması ve geliştirilmesi gerektiğini düşünüyoruz. MSKÜ Blokzinciri Araştırma Grubu (http://wiki.netseclab.mu.edu.tr/index.php?title=MSKU_BcRG) bünyesinde bu tür blokzinciri tabanlı sistemlerin simülasyonu ve denemelerinin gerçekleştirilmesi hedeflenmektedir.

TEŞEKKÜR (ACKNOWLEDGEMENTS)

MSKÜ Blokzinciri Araştırma Grubundan Fatih Teke'ye katkılarından ve yaptığı test çalışmalarından dolayı teşekkür ederiz.

KAYNAKLAR (REFERENCES)

[1]. S. Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System". 2008.

https://bitcoin.org/bitcoin.pdf (Türkçesi: http://bitcoin-turkiye.net/bitcoin-makale.pdf) (Erişim Tarihi: 30.08.2017).

[2]. CryptoCurrency Market Capitalizations. https://coinmarketcap.com/currencies/views/all (Erişim Tarihi: 05.12.2017).

[3]. Ethereum. https://www.ethereum.org (Erişim Tarihi: 30.08.2017).

[4]. Hyperledger. https://www.hyperledger.org (Erişim Tarihi: 30.08.2017).

[5]. Solidity Tutorial. http://solidity.readthedocs.io/en/latest (Erişim Tarihi: 30.08.2017).

[6]. 51% Attack. https://learncryptography.com/cryptocurrency/51-attack (Erişim Tarihi: 30.08.2017).

[7]. N. Bozic, G. Pujolle ve S. Secci. "A Tutorial on Blockchain and Applications to Secure Network Control-Planes". IEEE 3rd Smart Cloud Networks & Systems (SCNS), s. 1-8, 2016.

[8]. H. Halpin ve M. Piekarska. "Introduction to Security and Privacy on the Blockchain". IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), s. 1-3, 2017.

[9]. M. Conoscenti, A. Vetro ve J.C. De Martin. "Blockchain for the Internet of Things: a Systematic Literature Review". IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), s. 1-6, 2016.

[10]. S. Huh, S. Cho ve S. Kim. "Managing IoT Devices using Blockchain Platform". IEEE 19th International Conference on Advanced Communication Technology (ICACT), s. 464-467, 2017.

[11]. A. Dorri, S.S. Kanhere, R. Jurdak ve P. Gauravaram. "Blockchain for IoT Security and Privacy: The Case Study of a Smart Home". IEEE 2nd PERCOM Workshop On Security Privacy And Trust In The Internet of Things, 2017.

[12]. K. Biswas ve V. Muthukkumarasamy. "Securing Smart Cities Using Blockchain Technology". IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC-SmartCity-DSS), s. 1392-1393, 2016.

[13]. A. Dorri, S.S. Kanhere ve R. Jurdak. "Towards an Optimized BlockChain for IoT". ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI '17), s. 173-178, 2017.

[14]. G. Zyskind, O. Nathan ve A.S. Pentland. "Decentralizing Privacy: Using Blockchain to Protect Personal Data". IEEE Security and Privacy Workshops (SPW), s. 180-184, 2015.

[15]. A. Azaria, A. Ekblaw, T. Vieira ve A. Lippman. "MedRec: Using Blockchain for Medical Data Access and Permission Management". IEEE 2nd International Conference on Open and Big Data (OBD), s. 25-30, 2016.

[16]. H. Watanbe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu ve J. Kishigami. "Blockchain Contract: Securing a Blockchain Applied to Smart Contracts". IEEE International Conference on Consumer Electronics (ICCE), s. 467-468, 2016.

[17]. S. Singh ve N. Singh. "Blockchain: Future of Financial and Cyber Security". IEEE 2nd International Conference on Contemporary Computing and Informatics (IC3I), s. 463-467, 2016.

[18]. SecureChain: A Blockchain Security Gateway for SDN. http://www.reply.com/en/content/securechain (Erişim Tarihi: 30.08.2017).

[19]. N.B. Barnas. "Blockchains in National Defense: Trustworthy Systems in a Trustless World". A Research Report Submitted to the Faculty In Partial Fulfillment of the Graduation Requirements, Air University, 2016.

[20]. K.J. O'Dwyer ve D. Malone. "Bitcoin Mining and its Energy Footprint". 25th IET Irish Signals & Systems Conference and China - Ireland International Conference on Information and Communications Technologies (ISSC 2014 / CIICT 2014), 2014.

[21]. The Bitcoin and Blockchain: Energy Hogs. https://theconversation.com/the-bitcoin-and-blockchain-energy-hogs-77761 (Erişim Tarihi: 30.08.2017).

[22]. J. Poon ve T. Dryja. "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments". 2016. DRAFT Version 0.5.9.2. https://lightning.network/lightning-network-paper.pdf (Erişim Tarihi: 30.08.2017).

[23]. Could a Blockchain-based Electricity Network Change the Energy Market? https://www.theguardian.com/sustainable-business/2017/jul/13/could-a-blockchain-based-electricity-network-change-the-energy-market (Erişim Tarihi: 30.08.2017).

[24]. Proof of Work vs Proof of Stake: Basic Mining Guide. https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake (Erişim Tarihi: 30.08.2017).