Haliç Üniversitesi Fen Bilimleri Dergisi 2022, 5/1: 43-72
DOI: 10.46373/hafebid.1000108

Blok Zinciri Platformları, Fikir Birliği Mekanizmaları ve Ağın Güvenlik Analizi

Mimar ASLAN[1*], Mustafa Cem KASAPBAŞI[2]

[1]İstanbul Ticaret Üniversitesi, Bilgisayar Mühendisliği, İstanbul, Türkiye
[2]İstanbul Ticaret Üniversitesi, Bilgisayar Mühendisliği, İstanbul, Türkiye
Orcid: 0000-0002-9001-6510, 0000-0001-6444-6659

Geliş Tarihi: 27.09.2021
***Sorumlu Yazar e mail:** mimar.aslan@gmail.com **Kabul Tarihi:** 04.01.2022

Atıf/Citation: Aslan, M., Kasapbaşı, M. C., "Blok Zinciri Platformları, Fikir Birliği Mekanizmaları ve Ağın Güvenlik Analizi", Haliç Üniversitesi Fen Bilimleri Dergisi 2022, 5/1: xx-xx.

Araştırma Makalesi/ ***Research Article***

Özet

Finans, sağlık, sosyal medya vb ortamlardaki insanların ihtiyacı olan güven problemine blok zinciri teknolojisi, şifreli algoritmalar ile çözümler sunmaktadır. Güven problemini çözen ve verileri dağıtık olarak kayıt altına alan ve her şeyi şeffaf olarak bizlere sunan blok zinciri bir devrim niteliğindedir. Blok zinciri, akıllı sözleşmeler sayesinde kurumsal projelerde de kullanılmaktadır. Kurumların arasında yeni nesil bir ağ olarak da adlandırılan blok zinciri ile birçok şeyin değişmesi beklenmektedir. İnternetin, mobil cihazların ve sensörlerin yaygınlaşmasıyla birlikte güven problemi her geçen gün daha da önem kazanmaktadır. Farklı amaçlara hizmet eden Ethereum, Cardano, EOS, Cosmos, Hyperledger gibi blok zincir platformları bulunmaktadır. Altyapılarında Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS) ve Directed Acyclic Graph (DAG) gibi farklı fikir birliği mekanizmalarını kullanmaktadırlar. Bu çalışmada blok zinciri platformları, altyapılarında kullandıkları mutabakat mekanizmaları ve blok zinciri ağının güvenliği incelenrek araştırılmıştır.

Anahtar Kelimeler: Blok zinciri, fikir birliği mekanizmaları, ağ güvenliği.

Blockchain Platforms, Consensus Mechanisms and Security Analysis of the Network

Abstract

Blockchain technology offers solutions with encrypted algorithms to the trust problem that people in finance, health, social media, etc. need. The blockchain is revolutionary given that it solves the problem of trust and records data in a distributed manner and presents everything to us transparently. It can also be used in corporate projects thanks to smart contracts. A lot of things are expected to change with Blockchain, which is also called a new generation network by institutions. With the widespread use of the Internet, mobile devices and sensors, the problem of trust is gaining more and more importance day by day. There are blockchain platforms such as Ethereum, Cardano, EOS, Cosmos, Hyperledger that serve different purposes. They use different consensus mechanisms such as Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS) and Directed Acyclic Graph (DAG) in their infrastructure. In this study, Blockchain platforms were investigated by using the consensus mechanisms they use in their infrastructure and the security of the blockchain network.

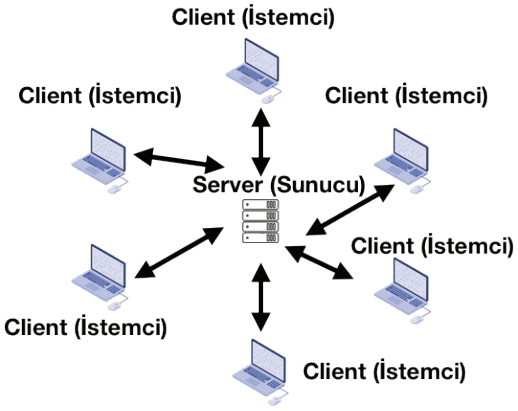
Keywords: Blockchain, consensus mechanisms, network security**.**

1. Giriş

Bu çalışmada en yaygın olarak kullanılan blok zinciri uygulama geliştirme platformları, altyapıda kullanılan doğrulama algoritmaları ve blok zincir ağının güvenlik analizi ele alınmaktadır. Daha önce yapılan çalışmalarda genelde blok zincirine ait bir ya da birkaç özellik incelenmektedir. Blok zincir ekosisteminin genel altyapısındaki çalışma mekanizmalarını ele alıp blok ağının değiştirilmeye karşı dayanıklılık gücünü deneysel testlerle sayısal olarak gösterme bu çalışmada hedeflenmiştir. Blok zinciri çoğu zaman kripto para Bitcoin (BTC) ile karıştırılmaktadır. Blok zinciri bir teknolojidir ve altyapı sunar. Bitcoin ise sadece bir blok zincir projesidir. Blok zincir altyapısını kullanarak kurumsal projeler geliştirmek de mümkündür. Blok zincirinin karakteristik özelliklerini incelendiğinde kayıt altına alınmış işlemlerin üzerinde daha sonradan bir değişiklik yapılamamaktadır. Gerçekleştirilen işlemler eşten eşedir ve birilerinin işlemler için aracılık etmesine de ihtiyaç

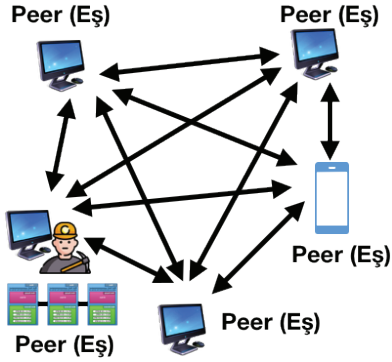
duyulmamaktadır. Yapılan işlemlerin hepsi ağdaki tüm makinelerde dağıtık olarak kaydedilmektedir. Blok zinciri sayesinde aracıların işlevselliğine gerek kalmamaktadır. Şahıslara ve kurumlara güvenme durumu son yıllarda ortaya çıkan finans ve sosyal medya platformlarında gözlenen skandallarla daha da tartışılır bir hale gelmiştir. Blok zinciri sayesinde güven problemi geri planda şifreli algoritmalarla sağlamaktadır. Blok zincirinin bir sahibi yoktur. Ağdaki herkes eşit haklara sahiptir ve ağa bağlı olarak çalışan makineler var olduğu sürece de sistem çalışmaya devam etmektedir. Blok zinciri teknolojisi şeffaftır. Yapılan işlemler şifrelenerek kayıt altına alınmakta ve asla kaybolmamaktadır [1]. Blok zinciri ağı herkesin görebileceği büyük bir veritabanıdır. Blok zinciri teknolojisini dijital ödeme, finans, sağlık, sigorta, borsa, tedarik zinciri, lojistik, nesnelerin interneti, mülkiyet tescili, devletin resmi belgelerinde, veri yönetiminde ve paylaşım ekonomisinin olduğu her yerde bir noter gibi kullanılmaktadır. Blok zincirinde her şey şeffaftır ve daima denetime açıktır. Ağ üzerinde gerçekleştirilen tüm işlemler kişi ya da kurum güvencesine ihtiyaç duymamaktadır. Algoritmalar, akıllı sözleşmelerle bu güveni garanti altına almaktadır [2].

1.1. Blok zinciri mimarisi



Şekil 1. Geleneksel client (istemci) ve server (sunucu) mimarisi

Blok zincirinde veriler kayıt altına alınırken Şekil 1'deki gibi geleneksel istemci sunucu mimarisi kullanılmaz. Bütün kayıtlar şifrelenmiştir ve ağa bağlı olan her bilgisayarda da bir kopyası bulunmaktadır. Blok zincirinde kalıcı hale getirilen tüm veriler önce doğrulanır, sonra şifrelenir, en sonda da kayıt altına alır [1].



Şekil 2. Dağıtık halde merkeziyetsiz peer to peer (eşten eşe) çalışan blok zincir mimarisi

Blok zincirinde merkezde duran ana bir sunucu ve karşı tarafta yer alan bir istemci bulunmamaktadır. Blok zincirinde Şekil 2'deki gibi merkezi olmayan dağıtık bir yaklaşım kullanılmaktadır. İşlemlerin geçmişini ağa dağıtılmış olarak paylaşılan bir deftere kaydeder, ağdaki tüm katılımcılar defter hakkında aynı görüşe sahiptir ve deftere yazılan bir veri bir daha asla değiştirilmemektedir [3]. Blok zinciri, şifrelenen verileri hem şeffaf hem de dağıtık olarak tutmaktadır. Ağa bağlı olan tüm birimlere node (düğüm) denilmektedir. Yapılmak istenen işlemleri doğrulayıp kayıt altına alan ve yeni bloklar oluşturup zincir ağına ekleyen birimlere madenci düğümler denir. Ağdaki her düğümün madenci olmasına gerek yoktur. Ağda bazı düğümlerin madenci olarak görev alması zincirin devamı ve tutarlılığı için yeterli olmaktadır. Madenci düğümler çok güçlü donanımlara sahip bilgisayarlardır. Özellikle ekran kartlarının yüksek kapasitelere sahip olması ağdaki işlemlerin doğrulanma aşamasını hızlandırmakta ve madenci düğüme daha

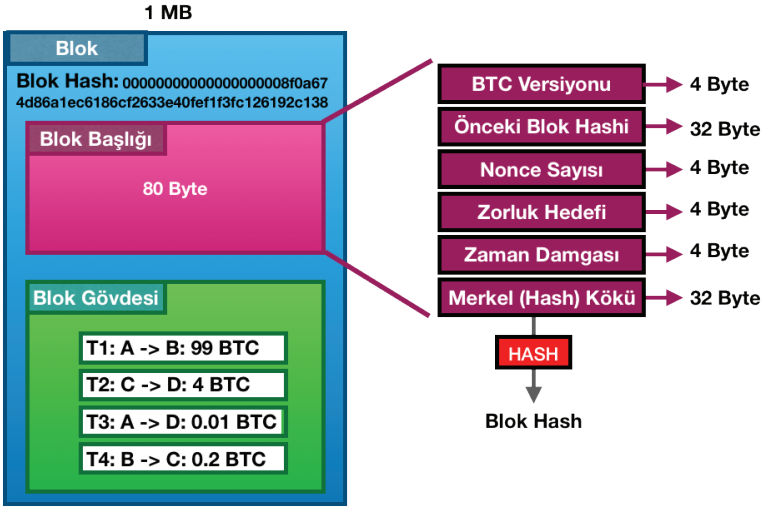
çok kazanç sağlamaktadır. Madenci bir makine blok zincir ağında gerçekleştirilen işlemlerin doğruluğunu devamlı olarak kontrol etmektedir. Bir madenci düğümün ağa bağlı, birden fazla makinesi olabilmektedir. Bu makineler, aralıksız olarak çalıştıklarından dolayı zamanla ısınmaktadı**r**lar ve çok elektrik enerjisi tüketmektedirler. Madenci düğüm tarafından doğrulanan işlemler bir blok haline getirilip blok zincir ağına dahil edilmektedir. Blok zinciri merkezi olmayan, şifreli, üst düzey güvenlikli bir teknolojidir. Ağdaki her bilgisayar eşit kabul edilmektedir ve ağdaki hiçbir düğümün diğerine karşı bir üstünlüğü yoktur.

Blok zinciri ile geliştirilen bir operasyonda yapılan işlemlerin hepsi eksiksiz kayıt altına alınmaktadır ve bir daha da değiştirilmemektedir. Bu sayede sürekli büyüyen tutarlı bir defter yapısı mevcuttur. Bu deftere yeni bir kayıt eklendiği zaman ağdaki tüm makinelere güncelleme bilgisi bildirilmektedir ve her bilgisayar tuttuğu deftere, gelen bu yeni kaydı ekleyerek verilerini güncellemektedir. Yazılan bilgiler kalıcıdır ve hiç kimse tarafından silinemez ve değiştirilemez [1]. Eğer üçüncü bir kişi zincirdeki bir veriyi değiştirmeye kalkışırsa, yapılan değişiklik hash fonksiyonları sayesinde anında fark edilerek zincirde değiştirilmiş olan o kısım ve sonrası geçersiz ilan edilmektedir. Ağın tutarlılığının tamamı, gelişmiş şifreli algoritmalarla korunduğundan denetlenme süreci her zaman otomatik olarak geri planda devam etmektedir. Daha önce doğrulaması yapılıp kaydedilmiş olan işlemlerin kronolojik sıralamasını isteyen herkes ağın kayıtlarını açıp görebilmektedir. Klasik istemci sunucu mimarisinde kredi kartı ile yapılan alışverişlerde geri planda her şey bankanın ve satış yapan kurumların sistemleri üzerinde devam etmektedir ve yapılan tüm işlemler sadece ilgili birkaç kurumun ve bankanın veritabanlarına yazılmaktadır. Blok zincir ağı üzerinde gerçekleştirilen alışverişlerde ise dağıtık olarak yer alan ve o ağa bağlı olan bütün bilgisayarlara yani düğümlere işlemler kaydedilerek yazılmaktadır. Ağdaki her düğümde kayıtların bir kopyası tutulmaktadır. Tüm işlem geçmişi blok zincirin üzerinde saklanmaktadır [4]. Şifreli, dağıtık ve şeffaf bir ağ mimarisine sahip olan blok zinciri sayesinde kurumlara, kişilere vb aracılara olan güven ihtiyacı artık ortadan kalkmaktadır.

1.2. Hash fonksiyonları

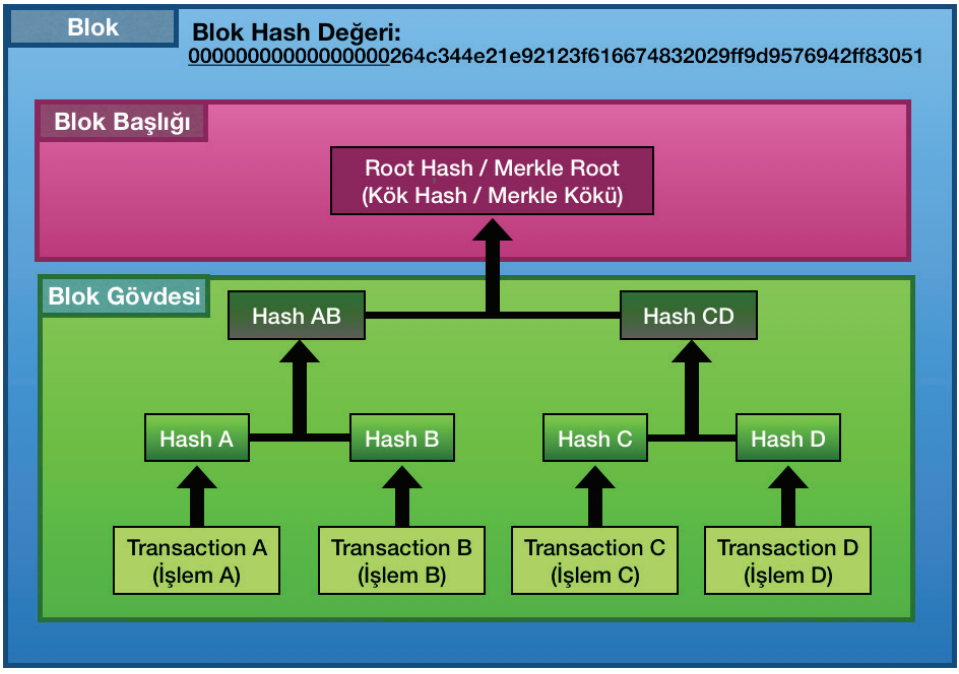
Şekil 3. Hash (özet) fonksiyonuna giren değer ve çıktısı.

Blok zincirinde hash fonksiyonları Şekil 3'teki gibi yapılan işlemlerin şifrelemesi için kullanılmaktadır. Hash fonksiyonunun girişine veri olarak yazı, video, resim ve başka dosya çeşitlerinin verilmesi mümkündür. Girişe ne verilirse verilsin, çıkıştaki digest (sonuç) değeri hep aynı uzunlukta ve benzersiz bir değer olmaktadır. Oluşturulan her hash değeri benzersiz bir parmak izidir. Hash fonksiyonuna aynı giriş değeri verildiği müddetçe hep aynı çıkış değeri elde edilmektedir. Giriş kısmındaki veride küçücük bir değişiklik bile yapılsa çıkıştaki sonuç değeri de anında değişmektedir. Blok zinciri platformlarında bir ağa daha önceden kaydedilmiş işlemlerin sonradan değişip değişmediğinin takibi altyapıda hash fonksiyonları ile yapılmaktadır.



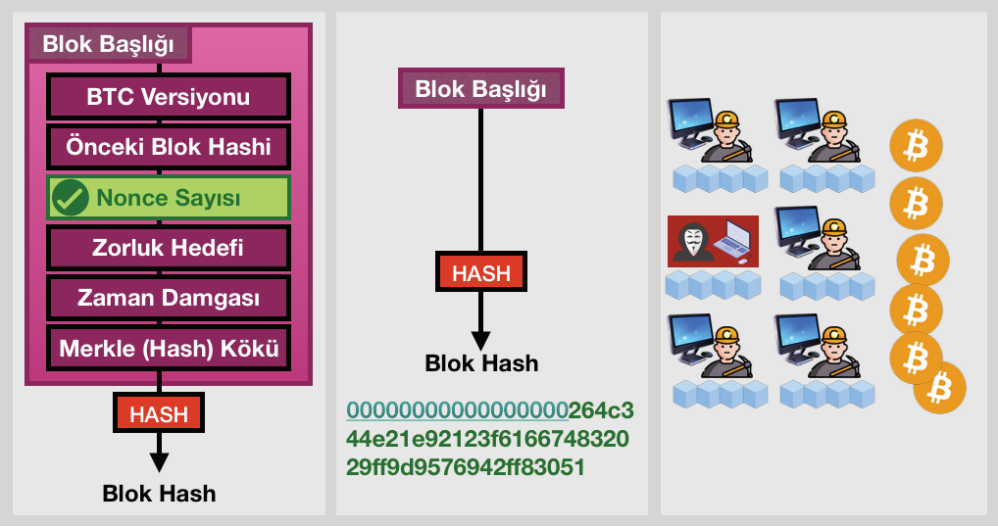
Şekil 4. Bitcoin blok zinciri ağındaki yer alan bir bloğun başlık ve gövde kısımları.

Blok zincir ağının üzerinde Şekil 4'teki gibi gerçekleştirilen her işlem ve her blok için benzersiz hash kodu değerleri oluşturulmaktadır. Blok zinciri platformlarının kullandıkları kripto paraların mimari tasarımları birbirinden farklı olduğundan altyapılarında SHA2, SHA3, Keccak gibi hash algoritmalarını kullanabilmektedirler. Blok zincirine eklenmek için oluşturulan yeni blok aslında sadece bir kutudur. Blok içerisinde başlık, gövde kısmı ve hash değerleri bulunmaktadır. Bloklar belirli bir işlem depolama kapasitesine sahiptir. Bitcoin bloğunun kapasitesi 1 MB'tır. Blok zincir tabanlı kripto para birimlerinde her blok bir önceki bloğun hash değerini içermektedir ve bu sayede blok içindeki işlemlerin manipüle edilmesini zorlaştırmaktadır [5]. Her bloğun başlık ve gövde kısmının arasında şifreli bir ilişki bağı kurulmaktadır. Blok gövdesi sadece veri alanıdır ve içerisinde doğrulaması yapılmış işlemler yer almaktadır. Ağdaki her madenci düğüm, yapılan işlemlerden bazılarını alıp onaylamakta ve kendine ait bir blok içerisinde bunları biriktirmektedir. Bloğun başlık kısmında ağın versiyonu, bir önceki bloğa ait hash değeri, nonce sayısı (tek seferlik kullanılan), zorluk hedefi, oluşturulma zamanı, merkle hash kökü değeri yer almaktadır.



Şekil 5. İşlemlerin hash fonksiyonuna girdikten sonra merkle kök değerini oluşturma aşamaları.

Bloğun gövde kısmında yer alan tüm işlemlerin hash çıktısına merkle kökü değeri denilmektedir. Blok gövdesinde Şekil 5'te gösterildiği gibi doğrulaması yapılan işlemler önce tek tek, sonra da ikili ikili olarak sıra ile hash fonksiyonuna sokulmaktadır. En son çıkan hash değeri merkle kökü olmaktadır.



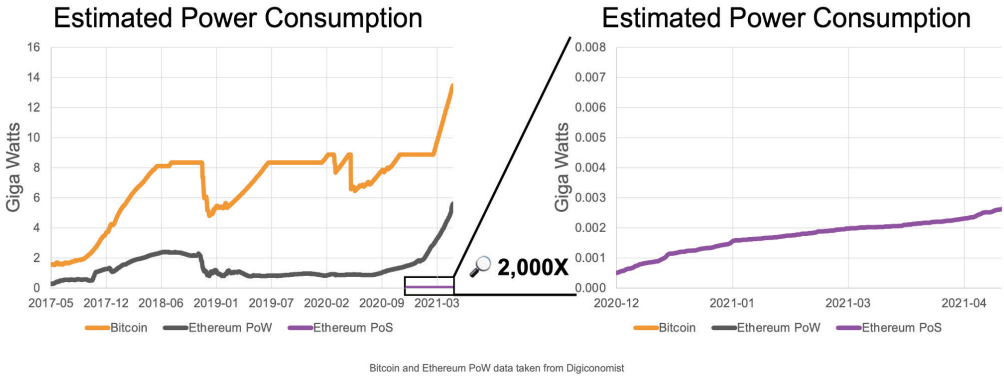
Şekil 6. Blok gövdesindeki nonce sayısının araştırılması.

Blok başlığı ve gövdesi merkle kökü ile birbirine bağlanmaktadır. Şekil 6'da gösterildiği gibi madenci tarafından blok zincirine eklenmek istenilen yeni bloğun hash değerini blok versiyonu, önceki bloğun hash değeri, nonce sayısı, zorluk hedefi, zaman damgası ve merkle kökünün hash fonksiyonuna girişinin sonucu belirlemektedir. Blok zincir ağına yeni bir blok eklemek için altyapıda bir sayı tahmin etme oyunu düzenlenmektedir. Ağdaki madenci düğümler bu yeni bloğun üstünde yer alması gereken nonce sayı değerini tahmin etmek için yarış aşamasına geçmektedirler. Nonce sayı değerini ilk bulan madenci yeni bloğu kendi zincirine ekleme hakkını elde etmekte ve bir miktar kripto para ödülünü kazanmaktadır. Ağdaki diğer madenciler ise bulunan bu nonce sayısını kontrol ederek zincirlerine yeni bloğu eklemektedirler. Bir madenci düğümün ağdaki görevi, yapılan işlemlerin geçerliliğinin doğrulanması, onların hash fonksiyonuna sokulması, yeni bloğa ait nonce değerinin bulunması ve zincire yeni bloğun eklenmesidir. PoW, PoS ve DPoS doğrulama mekanizmalarını kullanılan blok zincir ağlarının algoritmalarında yarış ve rekabet ortamı yer almaktadır.

1.3 Blok zinciri fikir birliği mekanizmaları

Blok zincirinde yapılan bir işlemi doğrulamak ve aynı işlemin tekrarının önüne geçmek için kontrolü sağlayan bir fikir birliği mekanizmasına ihtiyaç duyulmaktadır. Blok zinciri teknolojisinde birden fazla doğrulama mekanizması mevcuttur. Fikir birliği mekanizmaları literatürde mutabakat, doğrulama ve konsensüs terimleri ile ifade edilmektedir [6]. Kullanılan bir mutabakat algoritması sayesinde yapılan bir işlem, kripto para kayıt defterine güvenli olarak kaydedilmektedir. Proof of Work (PoW) mutabakat algoritması Bitcoin ile birlikte öne çıkıp tanınmaktadır. PoW mekanizması, ağdaki işlemlerin doğrulanıp yeni blokların eklenmesini sağlamak için çok güçlü donanımlara sahip madenci düğümlere ihtiyaç duymaktadır. Farklı doğrulama mekanizmalarını kullanan çeşitli blok zincir tabanlı geliştirme platformları da bulunmaktadır. Blok zincirinin altyapısında en yaygın olarak Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS) ve Direct Acyclic Graph (DAG) mekanizmaları kullanılmaktadır. Fikir birliği mekanizması, ağdaki işlemlerinin güvenilirliğini ve tutarlılığını garanti altına almaktadır. İlk ve en meşhur blok zinciri projesi olan Bitcoin, konsensüs mekanizması olarak PoW'u kullanmaktadır [6]. PoW, Bitcoin'in öncülük ettiği blok zincirindeki en klasik fikir birliği mekanizmasıdır [7]. Diğer bir kripto para olan Ethereum, konsensüs mekanizması olarak PoW'u kullanır ama en kısa zamanda PoS mimarisine geçiş yapmayı hedeflemektedir [8]. PoS mekanizmasında bir madenci düğümün çok üst düzey donanımlara sahip olması bir önem arz etmemektedir. Madenci düğüm, doğrulama yapmak istediği blok zincir ağının kripto parasına ne kadar çok yatırım yapıp onu cüzdanında bolca bulundurursa yeni bir blok ekleme şansını da o kadar çok arttırmaktadır. Bitcoin ve Ethereum kripto paralarının yaygınlaşmaları ile birlikte blok zinciri ağları üzerinde yapılan işlemlerin sayısı da katlanarak artmaktadır. Bu işlemlerin doğrulanma aşamasındaki bekleme sürelerinin azaltılması için mimarilerde iyileştirilme ihtiyacı doğmaktadır. Bu ihtiyacı karşılamak için DAG tabanlı

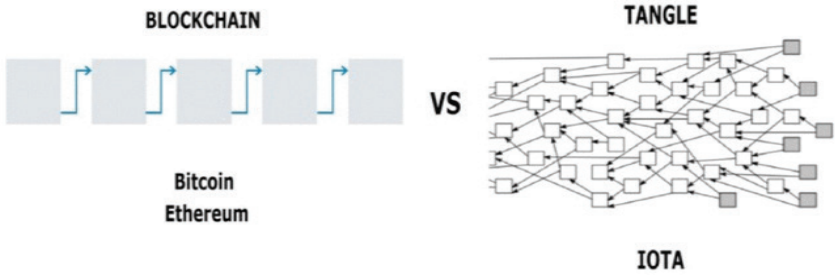
blok zincir, IOTA projesi geliştirilmiştir. Tangle, DAG altyapısını kullanan ve IoT sistemlerindeki işlemlerin kısa zamanda doğrulanmasını sağlayan bir blok zinciri platformudur [9].



Şekil 7. Bitcoin PoW, Ethereum PoW ve Ethereum PoS fikir birliği mekanizmalarının yıllara göre enerji tüketimi kıyaslaması [10]

PoW mekanizması, çevre dostu değildir ve çalışırken çok fazla enerji tüketmektedir [8]. PoS, daha küçük bir karbon ayak izine sahiptir. PoS mekanizmasında yüksek güçte madencilik çiftliklerine ihtiyaç duyulmamaktadır ve harcanan elektrik miktarı, PoW mekanizmasına kıyasla çok daha düşük olmaktadır. Ethereum PoW ile çalışmaktadır ama PoS altyapısına geçmeyi hedeflemektedir [11]. Bitcoin PoW, Ethereum PoW ve Ethereum PoS mekanizmalarının güç tüketimi kıyaslaması Şekil 7'de verilmiştir. PoS mekanizması, madenci düğümlerin nonce sayısını tahmin ederken ortaya koydukları rekabetin süresini azaltmak ve daha az kaynak tüketimini sağlanmak için o ağa ait kripto para varlığına sahip olma miktarını öne çıkarmaktadır. Ağdaki madencilerin cüzdan hesabında o ağa ait kripto para varlığından kimlerde daha çok varsa yeni bloğu eklemesi için o düğümlere öncelik verilmektedir. Seçilen madenciler, kendi aralarında yarışırlar ve nonce sayısını bulan ilk madenci, yeni bloğu ekleme hakkını elde ederek kripto para ödülünün sahibi olmaktadır. DPoS yapı olarak PoS konsensüs

mekanizmasına benzemektedir ama yeni bir bloğu eklemek isteyen madenci düğümler o ağdaki kişiler tarafından özgürce seçilmektedir. DPoS konsensüs mekanizmasında her düğüm bir adaydır. Her düğüm oylama yoluyla birkaç aracı düğümü seçmektedir. Aracı bir düğüm bloğu oluşturup belirlenen programa göre doğrulama için sıraya almaktadır [12]. PoS kullanan ağlarda sadece zengin madenciler ödülleri kazanmaktadır. Bu sorunu gidermek için DPoS mekanizması yeni bir çözüm sunmaktadır. DPoS mutabakat algoritması, PoS mekanizmasına oldukça benzemektedir ama ağdaki kişiler, yeni bloğu eklemek isteyen aday düğümlerini bizzat kendileri seçebilmektedir. Hisse sahipleri, sistemi kendileri adına denetleyecek birkaç delege ve şahit için oy kullanma hakkına sahiptirler. Delegeler ve şahitler, işlemlerin doğrulanması ve yeni blokların oluşturulmasında vazife almaktadır [13]. Yeni bloğu ekleyen düğüm tarafından kazanılan ödül ise kendisine oy verip onu seçen kişilerle pay edilmektedir. PoW, PoS, DPoS mekanizmalarını kullanan blok zincir ağlarında yeni bir blok oluşturmak için madenciler yarışıp rekabet etmektedir. DAG mekanizmasında böyle bir yarış süreci yoktur ve tüm işlemler birbiriyle bağlantılı olarak sürdürülmektedir.



Şekil 8. Tangle (IOTA) blok zinciri ağına yeni blok eklenme örneği [14]

Tangle (IOTA), DAG tabanlı çalışan ilk blok zinciridir. IOTA, mikro ödeme desteği ve işlem ücreti olmaması gibi temel özellikleri ile nesnelerin interneti (IoT) uygulamalarını desteklemek için umut verici bir platform olarak kabul edilmektedir [15]. DAG, IoT ve mikro

işlemler için önerilmektedir. IOTA ağının büyüme ve blokların bağlantı kurma türü Şekil 8'de gösterilmektedir. DAG mekanizması çalışma esnasında ağdan rastgele 2 tane onaylanmamış işlemi seçip doğruladıktan sonra ağdaki tepe noktasını güncellenmektedir. Son adımda ise işlemlerin toplam ağırlıkları hesaplanmaktadır [16]. Blok zinciri altyapılarında PoW, PoS, DPoS ve DAG fikir birliği algoritmaları çok yaygın olarak kullanılmaktadır. Bu konsensüs mekanizmalarının da kısıtları mevcuttur [17].

1.4. Blok zinciri uygulama geliştirme platformları

Blok zinciri tabanlı çalışan uygulamaları geliştirmek için birçok yardımcı platform vardır. Bu platformlarda akıllı sözleşmeler kullanılmaktadır. En çok öne çıkan platformlar alt başlıklarda açıklanmaktadır.

1.4.1. Ethereum

Bitcoin, akıllı sözleşmeleri olmayan 1. Nesil bir blok zinciri projesidir ve sadece kripto para olarak kullanılmaktadır. Blok zincirinin 2. Nesil projesi olan Ethereum bu kalıbı kırarak blok zincirinde akıllı sözleşmelerin kullanımı fırsatını sunmaktadır [18]. Akıllı sözleşmelerin amacı, taraflar arasındaki işlemleri şifreli algoritmalarla şeffaf ve güvenli olarak otomatikleştirmektir [19]. Tarafların arasında hiç kimse ve hiçbir kurum aracı olarak girmemektedir. Akıllı sözleşmeler, yazılmış talimatları sırasıyla yerine getirerek çalıştırmaktadır. Yapılan tüm işlemler blok zincir ağına şeffaf olarak kaydedilmektedir. Akıllı sözleşmeler sayesinde herkes merkezi olmayan uygulamalarını decentralized applications (dapps) oluşturup kolayca kullanabilmektedir [20]. Dapps uygulamalarının kodu, onu kullanan herkese açık olarak paylaşılmaktadır. Uygulama işlem yaparken üzerinde çalıştığı ağa ait kripto parayı kullanmaktadır. Remix IDE üzerinde akıllı sözleşmeler Solidity programlama dili ile geliştirildikten sonra Ethereum Virtual Machine

(EVM) ağına eklenip çalıştırılmaktadır [21]. Ethereum platformu, Ether (ETH) adında kendine ait kripto parasına sahiptir. Akıllı sözleşmeler her çalıştırıldığında bir işlem ücreti ödenmektedir.

1.4.2. Cosmos

Bitcoin ve Ethereum gibi farklı blok zincir ağları birbiri ile doğrudan iletişim kuramamaktadır. Blok zincir ağları yaygınlaştıkça paralel olarak birlikte çalışabilecek ağlara da ihtiyaç duyulmuştur. Farklı blok zincirlerinin birlikte çalışmasını sağlamak için Cosmos platformu doğmuştur [22]. Cosmos, altyapı mimarileri bambaşka olan ağlarının hepsini birbiriyle konuşturmayı hedeflemektir. Cosmos platformu, işlemleri gerçekleştirirken ATOM adında kendi ait kripto parasını kullanmaktadır.

1.4.3. Cardano

Cardano, 3. Nesil bir blok zinciridir. Ölçeklenebilirlik ve birlikte çalışabilirlik getirmeye odaklanmaktadır. Cardano ile akıllı sözleşmeler geliştirilmektedir [23]. Akıllı sözleşmeleri kodlarken Plutus yazılım dilini kullanılmaktadır. Düğümlerin ağ hakkında fikir birliğine ulaşması için altyapısında Ouroboros adında yeni bir algoritma mekanizması kullanmaktadır. Cardano platformu çalışırken ADA adında kendine ait kripto parasını kullanmaktadır.

1.4.4. EOS

EOS platformu merkezi olmayan bir işletim sistemidir. Blok zinciri üzerinde çalışan merkezi olmayan uygulamaları çalıştırıp desteklemektedir. Saniyede milyonlarca işlem yapma yeteneğine sahip bir platform olmayı ve blok zincirindeki işlem ücretlerini de tamamen ortadan kaldırmayı hedeflemektedir. EOS için akıllı sözleşmeler, C++ yazılım dili ile geliştirilmektedir. EOS, çok hızlı okuma ve yazma

işlemleri gerçekleştirmek için depolama alanı olarak disk yerine RAM kullanmaktadır [24]. DPoS konsensüs mekanizmasını ile çalışmaktadır [20]. DPoS ağdaki kullanıcıların kendi temsilcilerini seçmesine izin vermektedir. Seçilen bir temsilci, blok zincir ağına yeni bir blok ekleme hakkına sahip olmaktadır. Ekleme işleminden sonra kazanılan ödül ise kendisini seçen kişilerin hisselerine orantılı olarak paylaştırılmaktadır. EOS platformunun kendine ait kripto parası platformla aynı adı taşıyan EOS'tur.

1.4.5. Hyperledger

Ethereum, Cardano, Cosmos ve EOS platformları kendi kripto para birimlerine ve kendi blok zincir ağlarına sahiptirler. Hyperledger platformunun ise kendine ait bir kripto para birimi yoktur. Hyperledger Linux vakfı tarafından geliştirilmiş açık kaynaklı bir projedir [3]. Hyperledger, kurumların kendilerine ait hızlı, ölçeklenebilir ve yüksek performanslı blok zinciri ağlarını oluşturmalarını amaçlamaktadır. Hyperledger platformunda akıllı sözleşmeler Chaincode yazılım dili ile geliştirilmektedir [25]. Blok zincir uygulama geliştirme platformları Tablo 1'de kıyaslamalı olarak verilmektedir.

Tablo 1. Blok zincir uygulama geliştirme platformları.

	Ethereum	Cardano	EOS	Cosmos	Hyperledger
Kripto para birimi	ETH	ADA	EOS	ATOM	-
Sahibi (Firma/vakıf)	Ethereum vakfı	Cardano vakfı, IOHK, Emurgo	Block One	Interchain vakfi	Linux vakfı
Amacı	Dünyanın merkeziyetsiz blok zincir tabanlı süper bilgisayarı olmak.	Bilimsel olarak desteklenen akıllı sözleşme platformu olmak.	Endüstriyel ölçekli dapps uygulamaları için ölçeklenebilir bir platform olmak.	Birlikte çalışabilirliği sağlayıp blok zincirlerinin arasındaki internet olmak.	İşletmelerin kendi yerel özel blok zincir ağlarını oluşturmalarını sağlamak.
Fikir birliği, (mutabakat, doğrulama, konsensus) mekanizması	PoW ve PoS	Ouroboros	DPoS	Tendermint	Practical Byzantine Fault Tolerance (PBFT) pratik Bizans hata toleransı
Akıllı sözleşme kodlama dili	Solidity	Plutus	C++	Java, Javascript, Swift	Chaincode
Saniye cinsinden ağa yeni bir bloğun eklenme süresi	14	20	3	7	1

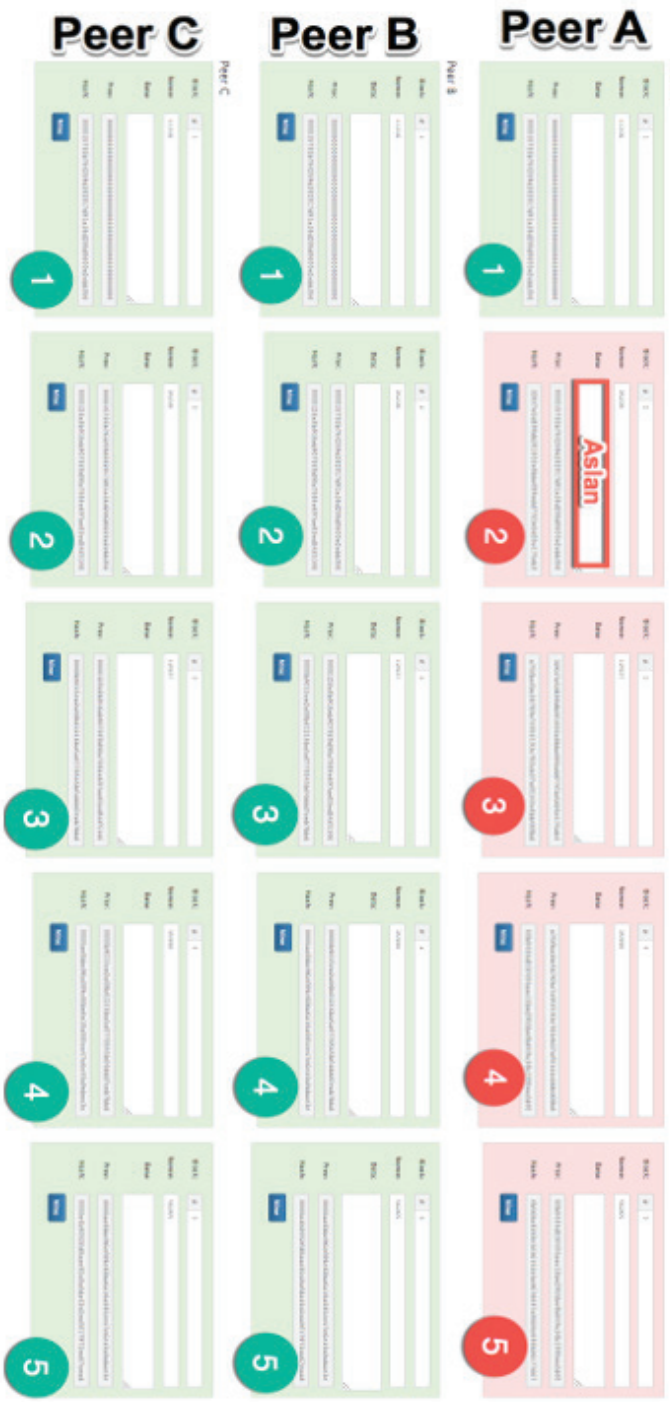
Bu çalışmada blok zincirlerine eklenen her bir blok ile güvenliğin nasıl sağlandığı, arada değişmesinin olasılığı, yani bir değişiklik (saldırı) yapılması olasılığı hakkında analitik olarak bir hesaplama sunulacaktır. Eklenen her bir bloğun dolaylı olarak güvenliği nasıl etkilediği araştırılacaktır.

2. Materyal ve Metot

Bu çalışma kapsamında blok zincir ağının güvenlik analizleri açıklanacaktır. Bu amaçla blok zinciri mimarileri, doğrulama mekanizmaları ve uygulama geliştirme platformları açıklanmaktadır. Bir saldırganın blok zincir yapısını değiştirmek için yerine getirmesi gerekenler ve ortaya koyacağı efor, teorik modeller ile gösterilerek saldırının gerçekleştirilmesinin zorluk derecesi hesaplanmıştır.

2.1. Blok zinciri ağının güvenlik analizi

Blok zincirinde herkesin kabul ettiği güvenilir zincir, dürüst zincirdir [26]. Ağdaki tüm peer (eş) düğümler bu doğrulanmış zincirin bir kopyasını kendisine almaktadır. Bu çalışmada blok zincirini değiştirip onu ele geçirmek isteyen kötü niyetli kişinin ağa saldırdığı bir senaryo incelenmektedir. Saldırgan kişi, ağda daha önce hiç yapılmamış bir işlemi yapılmış gibi bir bloğun içine kendi verilerini yerleştirip ağa eklemeye çalışsa bile bunu başarması çok zordur çünkü ağdaki doğrulama mekanizması, blok zinciri üzerinde sonradan yapılan bir değişimin tüm ağ tarafından yeniden onay almasını istemektedir.



Şekil 9. Ağdaki peer (eş) A isimli zincirindeki bir blok değiştirilme durumu.

Blok zinciri Şekil 9'daki gibi dağıtık olarak tutulduğundan yapılan bir değişiklik sadece saldırganın kendi makinesinde yer alan zincirin üzerinde geçerli olacaktır. Ağdaki diğer düğümlerde çalışan konsensüs mekanizması tarafından denetleme yapılırken bu değişiklik anında fark edilecektir ve o düğüm ağın tamamında dürüst olmayan bir düğüm olarak ilan edilecektir. Blok zincirine saldıran bir kişi daha önce zincire eklenmiş olan bir bloğun içinde yer alan bir işlemi değiştirirse değişiklik yapılan o bloktan itibaren ne kadar blok varsa içindeki işlemlerle birlikte hepsinin yeniden tek tek doğrulanması gerekmektedir. Saldırgan kişi, daha doğrulamalarını bitirmeden diğer düğümler onun zincirinde yapılan değişikliği çok kısa zamanda denetleyip fark edecektir ve saldırganın tüm çabası da boşa gidecektir. Blok zincirine saldırmak isteyenler için en iyi fırsat ağa en son blok ekleneceği zaman dilimidir. Ağa en son blok eklenirken dürüst zincir ile saldırgan kişinin zinciri aynı uzunluktadır ve yeni bir bloğun eklenilmesi için aralarında bir binom yarışı yapılmaktadır. Saldırgan düğüm eğer başarılı olup da sadece kendi zincirine yeni bir blok ekleyebilirse o zaman ağdaki en uzun zincire sahip olmaktadır ama saldırganın ağın tamamını ele geçirmesi için bu çabası da yeterli olmamaktadır. Blok zinciri dağıtık halde tutulduğundan ağın %51'ne de bloğunu eklettirmesi gerekmektedir. Ağın %51'ine hakim olunmadan ağdaki tüm zincirlerin değiştirilmesi imkansızdır! Madenciler arasında blok ekleme yarışını kaybedenin eklemeye çalıştığı bloğun içindeki tüm işlemler madenci havuzuna iade edilmektedir. Eklenmeyen bloğa yetim blok denilmektedir. Blok zincir ağına saldıran kötü niyetli birinin bir açığı yakalama olasılığı, kumarbazın iflası problemine çok benzemektedir [26]. Kumarbazın iflası problemi, bir Markov zinciridir ve geçiş olasılıklarının bilindiği varsayıldığında kaybetme ve kazanma olasılıkları tam olarak hesaplanabilmektedir [27]. Kumarbaz, oyuna borçla başlamaktadır ve sonsuz bir krediye sahiptir. Rakibiyle başa baş bir seviyeye gelebilmek için istediği kadar deneme yapabildiği bir oyunu oynamaktadır. Rakibini yakalayıp onu geçme olasılığı aynen blok ağına saldıran birinin dürüst zincirin uzunluğunu yakaladıktan sonra yeni bir bloğu ekleyerek onu geçme olasılığı gibidir [28].

p: Dürüst olan bir madencinin yeni geçerli bir bloğu bulup onu ağa ekleme olasılığıdır.

q: Dürüst olmayan saldırgan bir madencinin yeni geçerli bir bloğu bulma olasılığıdır.

q_z: Saldırgan bir madencinin z tane blok geriden gelerek dürüst düğüm sayısını yakalayıp yeni bir bloğu ekleme olasılığıdır.

z: Ağa eklenen en son bloğun ardından eklenmesi beklenen diğer yeni blokların sayısıdır.

1.Durum

$$q_z = \{1, \quad p \leq q\} \tag{1}$$

2.Durum

$$q_z = \{ (p/q)^2, \quad p > q \} \tag{2}$$

Burada p > q olduğunu kabul edersek saldırganın yakalaması gereken blok sayısı arttıkça olasılık da katlanarak azalmaktadır. Saldırgan kişi eğer şanslıysa yeni bir bloğu bulup eklemektedir ve ağı ele geçirme şansı daha da artmaktadır. Aksi halde zincirini uzatamaz ve yarışı kaybederek başarısız olmaktadır. Yeni bir işlem yapıldığında alıcı taraftaki kişinin veriler üzerinde bir değiştirme yapamayacağından emin olmak için ne kadar zaman beklemesi gerektiğini incelenmelidir. Saldırgan kişi bir ödeme işlemi gerçekleştirdikten sonra yaptığı ödemeyi yine kendisine geri döndürmek isterse alıcı taraftaki kişi bunu doğrulama mekanizmaları sayesinde fark etmektedir. Saldırgan kişi bunun daima çok geç fark edilmesini ümit etmektedir. Alıcı taraf, yeni bir anahtar çifti üretmekte ve gönderen tarafa da açık anahtarını vermektedir. Karşı tarafa göndereceği anahtarı, kendi özel anahtarı ile imzalamakta ve bu mesaj ancak açık anahtar ile okunmaktadır. Anahtarlar sayesinde gönderme yapan tarafın yaptığı işlemler onay almadan yeni bir bloğun içine konulmamaktadır. Bu sayede doğrulmamış bir işlemin ağa eklenilmesi de engellenmektedir. Saldırgan, bir işlemi karşı tarafa

gönderdikten hemen sonra dürüst zincirlere alternatif başka bir zincir oluşturmaya çalışmaktadır. Alıcı taraf ise yeni bir bloğun eklenmesini ve ondan sonra ise z tane bloğun daha ağa dahil edilmesini beklemektedir. Normal dürüst bir düğümün yeni bir bloğu ağa ekleyebilmesi için diğer madencilerden de doğrulama onaylarını almak için biraz bekletilmesi gerekmektedir. Kötü niyetli kişinin ağda başarılı olarak ilerleme elde etme potansiyeli poisson dağılımı ile gösterilmektedir.

$$\lambda = z\frac{q}{p} \tag{3}$$

Saldırgan tarafın normal zincire yetişebilme ihtimalini hesaplamak için zinciri belirli bir yerden yakalayabilme olasılığını ve oradan ilerleme durumu poisson yoğunluğu ile çarpılmaktadır.

1.Durum

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \{ (q/p)^{(z-k)}, \quad k \leq z \} \tag{4}$$

2. Durum

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \{ 1, \quad k > z \} \tag{5}$$

Blok zincir ağındaki sonsuz dağılım kuyruğunun toplamı çıkarılarak formül oluşturulmaktadır.

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \{ 1 - (q/p)^{(z-k)} \} \tag{6}$$

3. Bulgular

Ethereum, Cosmos, Cardano, EOS, Hyperledger blok zinciri platformlarıdır. Her blok zinciri platformu farklı bir amaca hizmet etmektedir. Geri planda yapılan işlemlerin ağda geçerli olabilmesi için de en az bir tane doğrulama mekanizmasına ihtiyaç duyulmaktadır. En yaygın olarak PoW, PoS, DPoS ve DAG mekanizmaları kullanılmaktadır. PoW

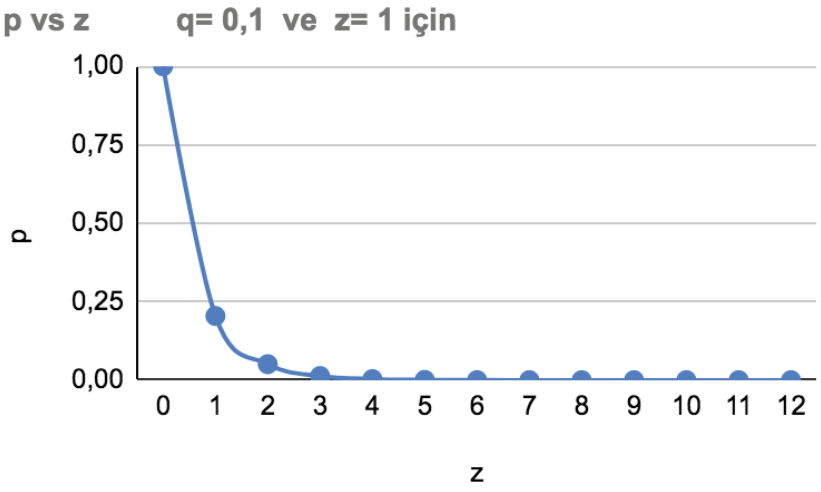
PoS, DPoS mimarileri tek ve büyük bir zincir yapısında tasarlanmaktadır. Zincir büyüdükçe yönetimleri zorlaşmakta ve ciddi gecikmeler yaşanmaktadır. DAG mekanizması ağırlıkların birikimine göre çalışır ve mimarisinde yeni işlemler zincire kolayca dahil edilmektedir. Yapılan analizler, blok zincir altyapılarının kurulu olmasını gerektirmektedir. Bu altyapıların analizleri bu sebeple makalede verildiği gibi teorik modeller üzerinde yapılabilmektedir. PoW, PoS, DPoS ve DAG doğrulama mekanizmalarını alıp birkaç bilgisayara kurup her biri için test blok zincir ağı oluşturarak başka yönlerden özel analizler yapılmak istense bile bu sistemler milyarlarca dolarlık dev kripto para platformların altyapı mimarilerindeki ticari projeler olarak yer aldığından kodlarının tamamına erişmek mümkün olamaz.

Blok zincirini ele geçirmeye çalışan kötü niyetli saldırgan kişiler elbette olacaktır. Ağa saldırı düzenleyen birinin ağı ele geçirmesi blok zincirinin dağıtık mimari yapısı sayesinde ve ağdaki diğer madenci düğümlerinde çalışan denetleme mekanizma algoritmaları sebebiyle çok zordur.

Tablo 2. Ağı ele geçirmeye çalışan bir düğümün yeni ve geçerli bir bloğu bulma olasılığının değeri q= 0,1 yeni bir bloktan sonra eklenilmesi beklenen blok sayısı z=1

z (blok sayısı)	p (ekleme olasılığı)
0	1
1	0,2045873
2	0,0509779
3	0,0131722
4	0,0034552
5	0,0009137
6	0,0002428
7	0,0000647
8	0,0000173
9	0,0000046
10	0,0000012
11	0,0000003
12	0,0000001

Ağa eklenen yeni bir bloğun ardından zincire eklenilmesi beklenen daha başka kaç tane yeni blok varsa Tablo 2'de onların sayı değeri z olarak gösterilmektedir. Eklenen 3. bloktan sonra blok zincir ağını kırmak sıfıra doğru yaklaşmaktadır ve 12. bloktan sonra da zinciri kırmak neredeyse imkânsız bir hal almaktadır. Zincire eklenen z tane blok sayısı ne kadar artarsa zinciri değiştirmek de o kadar zorlaşmaktadır.



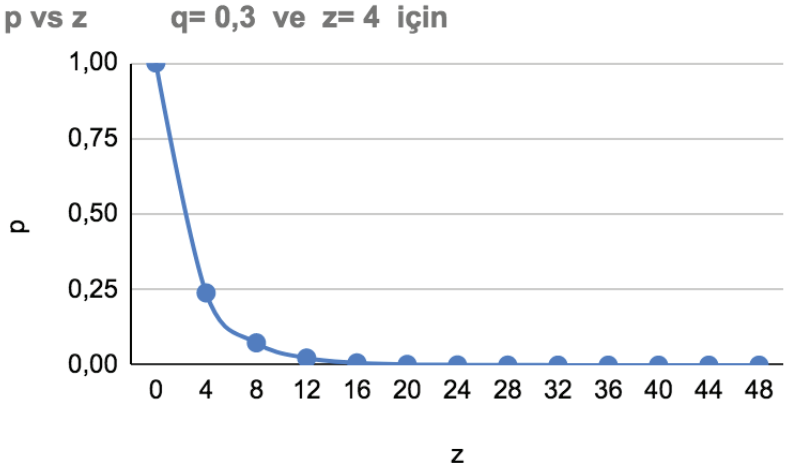
Şekil 10. Saldırgan kişinin zincire en son eklenen bloktan itibaren saldırıp başarılı olma durumu.

Ağa sadece 1 tane blok eklendikten sonra zincirin değiştirilme olasılığının sonuçları Şekil 10'da gösterilmektedir. Saldırgan kişiye zincire en son bloktan itibaren saldırıp ele geçirilme imkanı sağlanmasına rağmen, blok zinciri ağının kırılma olasılığı, yeni bloklar eklendikçe azalmaktadır.

Tablo 3. Ağı ele geçirmeye çalışan bir düğümün yeni ve geçerli bir bloğu bulma olasılığı değeri q=0,3 yeni bir bloktan sonra eklenilmesi beklenen blok sayısı ise z=4

z (blok sayısı)	p (ekleme olasılığı)
0	1
4	0,2391269
8	0,0739244
12	0,0235840
16	0,0076219
20	0,0024804
24	0,0008106
28	0,0002657
32	0,0000873
36	0,0000287
40	0,0000095
44	0,0000031
48	0,0000010

Tablo 3'teki değerlere göre blok zinciri ağı çok yoğun bir saldırı testine tabi tutulmaktadır ama saldırgan düğümün yine de başarılı olamayıp ağı ele geçiremediği açıkça görülmektedir.



Şekil 11. Saldırgan kişinin zincire en son eklenen 4. bloktan itibaren saldırıp başarılı olma durumu.

Saldırgan kişinin yeni bir blok ekleme şansı 3 kat daha arttırılıp ve zincire en son eklenen 4 bloktan sonra saldırıp zinciri değiştirme fırsatı verildi. 48. bloktan itibaren ağın artık kırılıp ele geçirilme olasılığının neredeyse sıfır doğru yaklaştığı Şekil 11'de gösterilmektedir.

4. Tartışma

PoW, PoS ve DPoS madencilerin yarışa ve rekabete dayalı doğrulama yaptıkları mekanizmadır [7]. Fikir birliği mekanizmalarından en yaygın olarak kullanılan PoW çok enerji, PoS ise daha az enerji tüketmektedir [8]. PoW, PoS ve DPoS altyapılarında hash algoritmalarını kullanmaktadır. PoW'da madencilere ihtiyaç varken PoS'ta yüksek güçte madencilik çiftliklerine ihtiyaç yoktur [10]. Ethereum, PoW ile çalışmaktadır ama PoS altyapısına geçmeyi hedeflemektedir, bunu başarınca ~%99,95 daha az enerji kullanacaktır. Bu çalışmada, PoS fikir birliği mekanizması ve onu daha ileriye taşıyacak olan DPoS ile de kıyaslaması yapılmaktadır. PoS, blok zincir ağına ait kripto paradan elinde en çok bulunduran sadece zengin madencilere kazanma önceliği tanırken DPoS ağdaki kişilere oy hakkı verip adil bir seçim yaklaşımını önermektedir. PoS'ta madenci düğümler arasında bir seçim yoktur ama DPoS ile blok üreticileri seçimle belirlenmektedir. Bu sayede ağdaki madencilerin kazançları dengelenmektedir. Fikir birliği mekanizmalarından DAG da incelenmiştir ve ağır hash hesaplamaları yerine, yeni bir işlemin onaylanmasını kullanılmaktadır. Yapılan bir önceki işlemin onay verilme referansı dikkate alınmakta ve ağa yeni bloklar eklenerek büyütülmektedir. Fikir birliği mekanizmalarının amacı yapılan işlemleri doğrulamak ve ağa yeni bir blok eklemektir.

Tablo 5. Blok zinciri ağının dayanıklılık kıyası.

Saldırı durumu	z (eklenen blok sayısı)	p (ekleme olasılığı)
Öncesi	10	0,0000012
Sonrası	12	0,0000001

Bitcoin blok zincirine yapılan ciddi bir saldırıda 10 bloğa kadar ağın dayanıklılığına garanti verirken (z=10 p=0,0000012) [26], bu çalışmada Tablo 5'te dayanıklılık seviyesi için blok sayısını 12 bloğa kadar çıkarılması sağlanmaktadır (z=12 p=0,0000001).

Tablo 6. Blok zinciri ağına yeni bir blok ekleme denetim sıklığı 5 blokta bir.

Değerlendirme sıklığı (5 blok)	z (eklenen blok sayısı)	p (ekleme olasılığı)
1. Denetim	5	0,1773523
2. Denetim	10	0,0416605
3. Denetim	15	0,0101008

Tablo 7. Blok zinciri ağına yeni bir blok ekleme denetim sıklığı 4 blokta bir.

Değerlendirme sıklığı (4 blok)	z (eklenen blok sayısı)	p (ekleme olasılığı)
1. Denetim	4	0,2391269
2. Denetim	8	0,0739244
3. Denetim	12	0,0235840
4. Denetim	16	0,0076219

Dürüst olmayan saldırgan bir madencinin yeni ve geçerli bir bloğu bulma olasılığı Tablo 6'da Bitcoin blok zincirinde 5 blokta bir değerlendirilirken (z=5 p=0,1773523 z=10 p=0,0416605 z=15 p=0,0101008) bu çalışmada, saldırgana daha müsamahalı davranarak Tablo 7'de her 4 blokta bir yeni ve doğrulanmış bir blok bulma olasılığı fırsatı tanınmakta ve sonrasında veriler kıyaslanmaktadır. (z=4 p=0,2391269 z=8 p=0,0739244 z=12 p=0,0235840 z=16 p=0,0076219). Yapılan saldırı girişimleri açıkça göstermektedir ki blok zincir ağını kırmak eklenen birkaç bloktan sonra çok zordur. Ağa yeni bir blok ekleyerek zincirin ele geçirilme teşebbüslerinin ne kadar çetin ve zahmetli bir süreç olduğunu yapılan testlerin neticesinde açıkça görülmektedir. Ağa eklenen yeni bloklardan sonra zincire belirli bir noktadan saldırıp kırma olasılığının da çok düşük olduğunu elde edilen sonuçlar göstermektedir. Ağa saldırı yapıldığında geçerli olan dürüst bir zincirin yerini

alabilmek için ondan daha uzun bir zincire ulaşılması gerekmektedir. Dürüst zincirin uzunluğunu geçme olasılıklarının yer aldığı bölgelerin çok sınırlı olduğunu yapılan saldırı denemeleri neticesinde görülmektedir.

Tablo 8. Blok zinciri ağına eklenen blokların sayısı arttıkça ağın değiştirilme zorluğunun kıyası.

Zincirin orta kısımlardan değiştirilme durumu	z (eklenen blok sayısı)	p (ekleme olasılığı)
1. Durum	3	0,0131722
2. Durum	48	0,0000010

Blok zincirine Tablo 8'deki gibi eklenen yeni 3 bloktan sonra (z=3 p=0,0131722) dürüst zinciri yakalayıp değiştirme fırsatı zamanla azalmaktadır. Bu şans, 48 yeni blok eklendikten sonra (z=48 p=0,0000010) olmaktadır. Blok zincir ağının kırılıp değiştirilme olasılığı bu aşamadan sonra artık sıfıra yaklaşmaktadır.

5. Sonuçlar

Bu çalışmada önce Ethereum, Cosmos, Cardano, EOS, Hyperledger blok zincir platformları ve hizmet amaçları kıyaslanmıştır. Blok zincir ağının büyümesi ile saldırgan kişinin düğümleri ele geçirilmesinin zorluğunun üstel olarak arttığı sayısal olarak gösterilmiştir. Aynı zamanda bu çalışmada blok zincir tabanlı platformların altyapılarında kullandıkları konsensüs mekanizmalarının çalıştıkları ağın verimliliğini doğrudan etkilediği de gösterilmiştir. Fikir birliği algoritmalarının ağdaki işlemleri doğrulama yaklaşımlarının o blok zincir ağın performansı için de çok önemli olduğu gösterilmiştir. Blok zincir teknolojisi, insanlara herhangi bir otoriteye güvenerek ona bağımlı olmadan yepyeni merkeziyetsiz bir mimari ile verileri daha güvenli, son derece şeffaf ve dağıtık olarak saklama imkânını sağlamaktadır.

Kaynaklar

[1] Yaga, D., Mell, P., Roby, N., & Scarfone, K. Blockchain technology overview. arXiv preprint arXiv:1906.11078, (2019, June), doi: 10.6028/NIST.IR.8202

[2] Seijas, P. L., Thompson, S. J., & McAdams, D. Scripting smart contracts for distributed ledger technology. IACR Cryptology ePrint Archive, (2016, December), 1156.

[3] Benhamouda, F., Halevi, S., & Halevi, T. Supporting private data on hyperledger fabric with secure multiparty computation. IBM Journal of Research and Development, 63(2/3), 3-1. (2019, April), doi: 10.1147/JRD.2019.2913621.

[4] Yermack, D. Blockchain technology's potential in the financial system. 2019 Financial Market's Conference. (2019, May).

[5] Yang, X., Chen, Y., & Chen, X. Effective scheme against 51% attack on proof-of-work blockchain with history weighted information. In *2019 IEEE International Conference on Blockchain (Blockchain)* (2019, July), (pp. 261-265). IEEE, doi: 10.1109/Blockchain.2019.00041.

[6] Jiang, Y., & Lian, Z. High performance and scalable Byzantine fault tolerance. In *2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)* (2019, March), (pp. 1195-1202). IEEE, doi: 10.1109/ITNEC.2019.8728972.

[7] Cao, B., Zhang, Z., Feng, D., Zhang, S., Zhang, L., Peng, M., & Li, Y. Performance analysis and comparison of PoW, PoS and DAG based blockchains. Digital Communications and Networks, (2020, November), 6(4), 480-485, doi: 10.1016/j.dcan.2019.12.001.

[8] Košt'ál, K., Krupa, T., Gembec, M., Vereš, I., Ries, M., & Kotuliak, I. On transition between PoW and PoS. In *2018 International Symposium ELMAR* (2018, September), (pp. 207-210). IEEE, doi: 10.23919/ELMAR.2018.8534642.

[9] Sagirlar, G., Carminati, B., Ferrari, E., Sheehan, J. D., & Ragnoli, E. Hybrid-iot: Hybrid blockchain architecture for internet of things-pow sub-blockchains. In *2018 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)* (2018, July), (pp. 1007-1016). IEEE, doi: 10.1109/Cybermatics_2018.2018.00189.

[10] Ethereum Foundation. A country's worth of power, no more! Ethereum Foundation Blog. https://blog.ethereum.org/2021/05/18/country-power-no-more/ , (2021, May 18), (Erişim Tarihi: 28 Ağustos 2021).

[11] Supreet, Y., Vasudev, P., Pavitra, H., Naravani, M., & Narayan, D. G. Performance Evaluation of Consensus Algorithms in Private Blockchain Networks. In *2020 International Conference on Advances in Computing, Communication & Materials (ICACCM)* (2020, August), (pp. 449-453). IEEE, doi: 10.1109/ICACCM50413.2020.9213019.

[12] Xu, G., Liu, Y., & Khan, P. W. Improvement of the DPoS consensus mechanism in Blockchain based on vague sets. *IEEE Transactions on Industrial Informatics*, (2019, November), *16*(6), 4252-4259. doi: 10.1109/TII.2019.2955719.

[13] Chen, Y., & Liu, F. Improvement of DPoS Consensus Mechanism in Collaborative Governance of Network Public Opinion. In *2021 4th International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE)* (2021, March), (pp. 483-488). IEEE, doi: 10.1109/AEMCSE51986.2021.00105.

[14] Bhandary, M., Parmar, M., & Ambawade, D. Securing Logs of a System-An IoTA Tangle Use Case. In *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)* (2020, July), (pp. 697-702). IEEE, doi: 10.1109/ICESC48915.2020.9155563.

[15] Guo, F., Xiao, X., Hecker, A., & Dustdar, S. Characterizing IOTA Tangle with Empirical Data. In *GLOBECOM 2020-2020 IEEE Global Communications Conference* (2020, December), (pp. 1-6). IEEE, doi: 10.1109/GLOBECOM42002.2020.9322220.

[16] Wang, T., Wang, Q., Shen, Z., Jia, Z., & Shao, Z. Understanding Intrinsic Characteristics and System Implications of DAG-based Blockchain. In *2020 IEEE International Conference on Embedded Software and Systems (ICESS)* (2020, December), (pp. 1-6). IEEE, doi: 10.1109/ICESS49830.2020.9301563.

[17] Zhao, L., & Yu, J. Evaluating DAG-based blockchains for IoT. In *2019 18th IEEE international conference on trust, security and privacy in computing and communications/13th IEEE international conference on big data science And engineering (TrustCom/BigDataSE)* (2019, August), (pp. 507-513). IEEE, doi: 10.1109/TrustCom/BigDataSE.2019.00074.

[18] Vujičić, D., Jagodić, D., & Ranđić, S. Blockchain technology, bitcoin, and Ethereum: A brief overview. In 2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH) (2018, March), (pp. 1-6). IEEE, doi: 10.1109/INFOTEH.2018.8345547.

[19] Tonev, I. Energy Trading Web Platform Based on the Ethereum Smart Contracts and Blockchain. In *2020 12th Electrical Engineering Faculty Conference (BulEF)* (2020, September), (pp. 1-4). IEEE, doi: 10.1109/BulEF51036.2020.9326010.

[20] Mishra, R. A., Kalla, A., Singh, N. A., & Liyanage, M. Implementation and analysis of blockchain based dapp for secure sharing of students' credentials. In 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC) (2020, January), (pp. 1-2). IEEE, doi: 10.1109/CCNC46108.2020.9045196.

[21] Aung, Y. N., & Tantidham, T. Ethereum-based emergency service for smart home system: smart contract implementation. In *2019 21st International Conference on Advanced Communication Technology (ICACT)* (2019, February), (pp. 147-152). IEEE, doi: 10.23919/ICACT.2019.8701987.

[22] Dong, S., Yang, H., Yuan, J., Jiao, L., Yu, A., & Zhang, J. Blockchain-based cross-domain authentication strategy for trusted access to mobile devices in the IoT. In *2020 International Wireless Communications and Mobile Computing (IWCMC)* (2020, June), (pp. 1610-1612). IEEE, doi: 10.1109/IWCMC48107.2020.9148358.

[23] Worley, C., & Skjellum, A. Blockchain tradeoffs and challenges for current and emerging applications: generalization, fragmentation, sidechains, and scalability. In *2018 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)* (2018, July), (pp. 1582-1587). IEEE, doi: 10.1109/Cybermatics_2018.2018.00265.

[24] Dernayka, I., & Chehab, A. Blockchain Development Platforms: Performance Comparison. In *2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS)* (2021, April), (pp. 1-6). IEEE, doi: 10.1109/NTMS49979.2021.9432669.

[25] Nguyen, T. S. L., Jourjon, G., Potop-Butucaru, M., & Thai, K. Impact of network delays on Hyperledger Fabric. arXiv preprint arXiv:1903.08856, (2019, April), doi: 10.1109/INFCOMW.2019.8845168.

[26] Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, (2008, October), 21260.

[27] Akbarzadeh, N., & Tekin, C. Gambler's ruin bandit problem. In *2016 54th Annual Allerton Conference on Communication, Control, and Computing (Allerton)* (2016, September), (pp. 1236-1243). IEEE, doi: 10.1109/ALLERTON.2016.7852376.

[28] Feller, W. An introduction to probability theory and its applications. (1957), Wiley.