TOBB EKONOMİ VE TEKNOLOJİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

HİSSE İSPATI TABANLI BLOKZİNCİR SİSTEMLERİNİN TEKNİK BİR ANALİZİ

YÜKSEK LİSANS TEZİ

Yunus Çağrı YURDAKUL

Bilgisayar Mühendisliği Anabilim Dalı

Tez Danışmanı: Prof. Dr. Ali Aydın SELÇUK

AĞUSTOS 2019

Fen Bilimleri Enstitüsü Onayı

……..
Prof. Dr. Osman EROĞUL
Müdür

Bu tezin Yüksek Lisans derecesinin tüm gereksinimlerini sağladığını onaylarım.

……
Prof. Dr. Oğuz ERGİN
Anabilimdalı Başkanı

TOBB ETÜ, Fen Bilimleri Enstitüsü'nün 151111013 numaralı Yüksek Lisans Öğrencisi **Yunus Çağrı Yurdakul**'un ilgili yönetmeliklerin belirlediği gerekli tüm şartları yerine getirdikten sonra hazırladığı **"Hisse İspatı Tabanlı Blokzincir Sistemlerinin Teknik Bir Analizi"** başlıklı tezi **08.08.2019** tarihinde aşağıda imzaları olan jüri tarafından kabul edilmiştir.

Tez Danışmanı : **Prof. Dr. Ali Aydın SELÇUK** .....
TOBB Ekonomi ve Teknoloji Üniversitesi

Jüri Üyeleri : **Doç. Dr. Ahmet Burak CAN (Başkan)** .....
Hacettepe Üniversitesi

Dr. Öğr. Üyesi Mücahid KUTLU .....
TOBB Ekonomi ve Teknoloji Üniversitesi

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, alıntı yapılan kaynaklara eksiksiz atıf yapıldığını, referansların tam olarak belirtildiğini ve ayrıca bu tezin TOBB ETÜ Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırlandığını bildiririm.

Yunus Çağrı Yurdakul

ÖZET

Yüksek Lisans Tezi

HİSSE İSPATI TABANLI BLOKZİNCİR SİSTEMLERİNİN TEKNİK BİR ANALİZİ

Yunus Çağrı Yurdakul

TOBB Ekonomi ve Teknoloji Üniveritesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

Danışman: Prof. Dr. Ali Aydın Selçuk

Tarih: Ağustos 2019

Emek ispatı (PoW) tabanlı sistemler, fazla enerji tüketiminden dolayı uzun süreli sistemler olmayacaklardır. Bu durumu düzeltmek için yeni bir fikir birliği protokolü sunuldu. Hisse ispatı (PoS) protokolü. Bu fikir birliği mekanizması, kullanıcıların özet gücü yerine zincirdeki hisse miktarını kullanmaktadır. Fakat bu protokolünde kendine has problemleri vardır. Bunlardan biri ortaya konan bir şey olamam problemidir. Kullanıcılar karşılarına çıkan her bloğu oylayabilirler ve bunu yaparken hiçbir şey kaybetmezler. Bu durum çifte harcama problemine neden olabilmektedir. Bu tezde, üç fikir birliği protokolü incelenecektir. Blok yapıları, onaylama metotları, kontrol noktası mekanizmaları ve cezalandırma sistemleri incelenip analiz edilecektir. Bu üç uygulamanın kullanıcıları, onaylayıcı olabilmek için zincirde hisse bulundurmak zorundadırlar. Bu hisselerinin miktarına bağlı olarak, blok işleme oranlarını arttırırlar. Bir PoS sistemi, bunu sağlayabilmek için şu bileşenlere sahip olmalıdır. Özetleme algoritması, blokları birbirine bağlaması için gereklidir. Eklenen blokların oluşturduğu

zincirin bozulması durumunda ana zincir seçimini yapacak bir protokol önceden belirlenmiş olması gerekmektedir. Bu zincirdeki blok verilerinin tüm kullanıcılarda bulunması gerekmektedir ve bu veriler düzenli olarak güncellenmelidir. Blokları eklerken, hatalı blokların eklenmemesi için bir fikir birliği protokolü belirlenmelidir. Her blok birden fazla transfer bilgisini içerebilmelidir. Bu tutulan verilerin boyutunu azaltacaktır ve transferlerin onaylanmasını hızlandıracaktır. Bu blok işleme protokolü güncellenebilmelidir. Bu güncelleme, eski veri yapısını bozmamalıdır. Eski veriler yeni protokolde de kullanılabilmelidir. Hangi transfer, hangi kullanıcıya ait belirlenebilmelidir. Kullanıcılar protokol ihlallerinde cezalandırılmalıdırlar. Bu ceza sistemi, kullanıcıları daha dürüst olmaya zorlayacaktır. Belli bloklar, kontrol noktası olarak belirlenmelidir. Hata durumunda, sistemin yanlış işlemeye zorlanması durumunda uygulamanın bu noktaya geri dönüp, buradan işlemlerine devam etmesi sağlanmalıdır.

Anahtar Kelimeler: Kripto para, Blokzincir, Emek ispatı, Hisse İspatı, Nxt, Casper

ABSTRACT

Master of Science

TECHNICAL ANALYSIS OF PROOF OF STAKE BASED BLOCKCHAIN SYSTEMS

Yunus Çağrı Yurdakul

TOBB University of Economics and Technology
Institute of Natural and Applied Sciences
Computer Engineering Science Programme

Supervisor: Prof. Dr. Ali Aydın Selçuk

Date: August 2019

Proof-of-work (PoW) based blockchain systems are not long-term solutions because of their high energy consumption problem. To eliminate this issue, a new consensus protocol is introduced; proofof-stake (PoS). This consensus mechanism depends on the peers' stake on the blockchain. However, this solution comes with new problems, one of them is the nothing-at-stake problem. The problem is due to the fact that clients can vote for any block on every fork they encounter because they don't lose anything by doing that, which creates an opportunity for double-spending, which in turn may cause more vulnerability. In this study, three PoS-based cryptocurrency protocols are analysed; PeerCoin, Nxt and Ethereum's Casper in terms of how they secure the integrity of blockchain. Block structures, validation methods, checkpoint mechanism and penalty methods of all these three systems are investigated and compared. As a result, a generic design space of PoS system for solving the problem. The clients of all three systems need to have a stake on the blockchain to become a validator and they bet on with their stakes to validate next transaction blocks. The system should have these components to provide such consensus. Hashing protocol, to connect blocks to

each other. Main chain protocol to correct the chain. The consensus mechanism should be updateable and the update should not ignore the old data. The system must have digital signature to determine the ownership of the transactions. The system must have a punishing and checkpoint protocol.

Keywords: Cryptocurrency, Blockchain, Proof of Work, Proof of Stake, PeerCoin, Nxt, Casper

TEŞEKKÜR

Çalışmalarım boyunca değerli yardım ve katkılarıyla beni yönlendiren hocam Prof. Dr. Ali Aydın SELÇUK'a, kıymetli tecrübelerinden faydalandığım TOBB Ekonomi ve Teknoloji Üniversitesi Bilgisayar Mühendisliği Bölümü öğretim üyelerine, destekleriyle her zaman yanımda olan aileme ve arkadaşlarıma çok teşekkür ederim.

İÇİNDEKİLER

ŞEKİL LİSTESİ

Sayfa

ÇİZELGE LİSTESİ

Sayfa

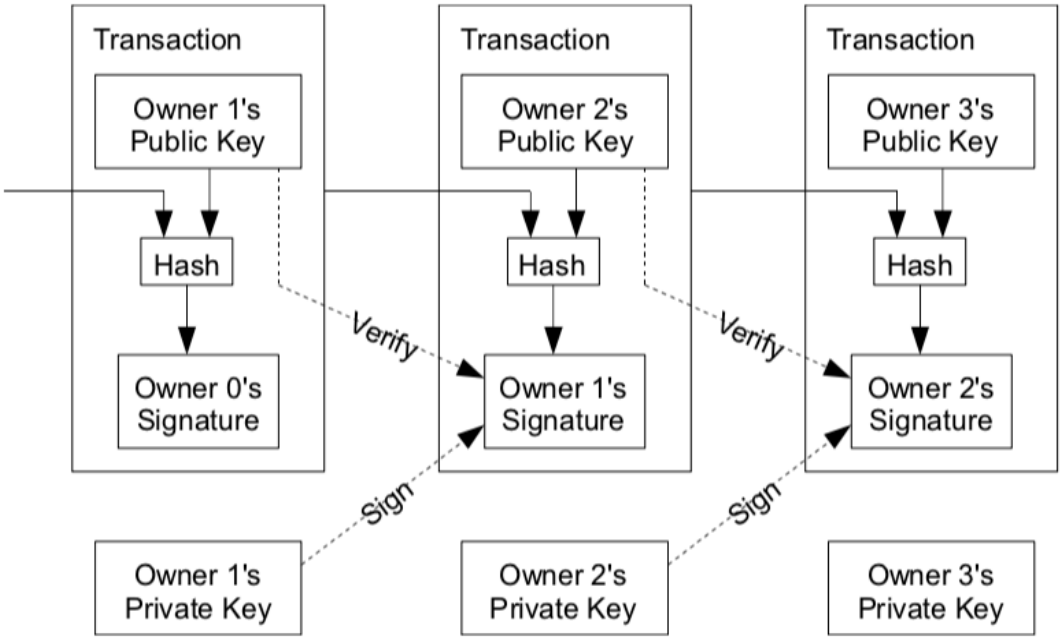
KISALTMALAR

PoW **:** Proof-of-Work
PoS **:** Proof-of-Stake
DPoS **:** Delegated Proof-of-Stake
NaS : Nothing-at-Stake
DDoS : Distributed Denail of Service
BFT : Byzantium Fault Tolerance
P2P : Peer to Peer

1. GİRİŞ

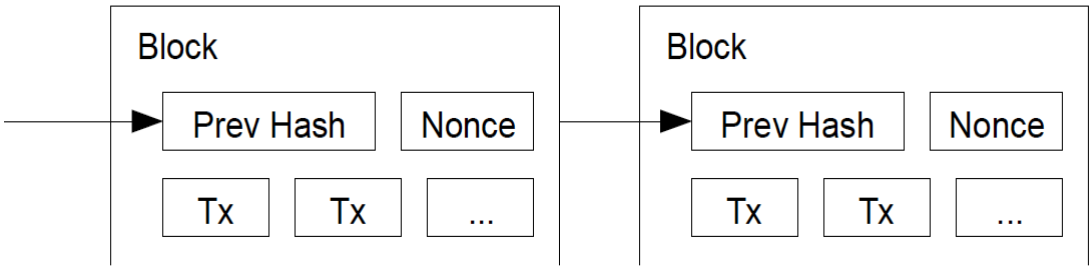
Kripto para; belli şifreleme kuralları kullanılarak, güvenli bir şekilde üretilip ve transfer edilen bir sanal para birimidir. Bu sanal para birimi, itibari bir para birimi gibi hükümetlerin koyduğu yasalar tarafından yönetilmez [1], yani güvenliği merkezi bir kurum tarafından sağlanmaz [2].

Merkezi olmayan sanal para için sunulan ilk sistem, 2008 yılında, Satoshi Nakatomo tarafından, elektronik para transfer sistemi olan Bitcoin ile sunuldu. 2009 yılında kullanılmaya başlayan bu sistemde para transferi merkezi bir finansal kurum olmadan, eşler arasında sağlanıyor [3]. Fakat arada güveni sağlayan bir kurum olmayınca, kullanıcıların kendi aralarında güven ortamını sağlaması gerekmektedir. Burada dijital imzalar çözümün bir parçasını oluşturmaktadır.



Şekil 1.1: Bitcoin dijital imzalama ve imza doğrulama modeli [3].

Bitcoin sistemi aslında dijital imzaların oluşturduğu bir zincirdir. Şekil 1.1'de görüldüğü gibi; bir kullanıcı, başka bir kullanıcıya para transferi yapmaya çalıştığı zaman, kendi gizli anahtarıyla, önceki transferin özetini ve diğer kullanıcın açık anahtarını imzalar ve transfer bilgilerine ekler. Parayı alacak olan kişi bu transferin geçerliliğini bu imza ile doğrulayabilir. Fakat burada kullanıcı, parayı gönderen kullanıcının aynı ödemeyi başkasına yapıldığını doğrulayamaz. Yani aynı para iki kez harcanabilir. Buna çift-harcama [4] problemi denir. Bu yüzden, alacaklı kişinin, kendisine gelen paranın, gönderici tarafından daha önce başkası için imzalandığını kontrol etmesi gerekmektedir. Bunu yapabilmek için tüm para transferlerinin açık bir şekilde gerçekleşmesi [5] ve bu sistemi kullanan kullanıcıların ortak bir zincirde karar kılmaları gerekmektedir. Ortak bir zincir kullanımı için her transfer, sitemi kullanan diğer kullanıcıları tarafından da kabul edilmelidir. Bunun için kullanıcıların çoğunluğu yeterlidir. Bitcoin, transfer işlemlerinin onaylanması için Adam Back'in HashCash [6] sistemine benzer bir protokol sunmaktadır. Bu protokolün adı emek ispatı (PoW) protokolüdür [3].



Şekil 1.2: Emek ispatı protokolü [3].

Emek ispatı sistemi, transferi onaylayacak kullanıcılara bir bulmaca sormaktadır. Bu bulmacada kullanıcılar belli özet değerine ulaşmak zorundadırlar. Bu özet değeri belli sayıda 0 değeri ile başlamalıdır. Bu değere formül 1.1'i kullanarak ulaşılır. Şekil 1.2'de görüldüğü gibi, bu değere ulaşmak için kullanıcılar bir sefer kullanılan bir sayı tutmak zorundadırlar. Bu sayı sürekli arttırılarak veya rastgele seçilerek bu özet değeri hesaplanır. İstenilen değere ulaştığında transfer verilerini içeren blok zincire işlenir. Sonrasında yapılan transfer blokları, bu blok üzerinden sırasıyla aynı işlemlerden geçerek devam eder.

$$T > H(V, P, M, t, n, N) \quad (1.1)$$

Formül 1.1'de T, ulaşılması gereken özet değeridir. Çizelge 1.1'de formülde kullanılan verilerin açıklaması yapılmıştır.

Çizelge 1.1: Bitcoin blok başlığı [11].

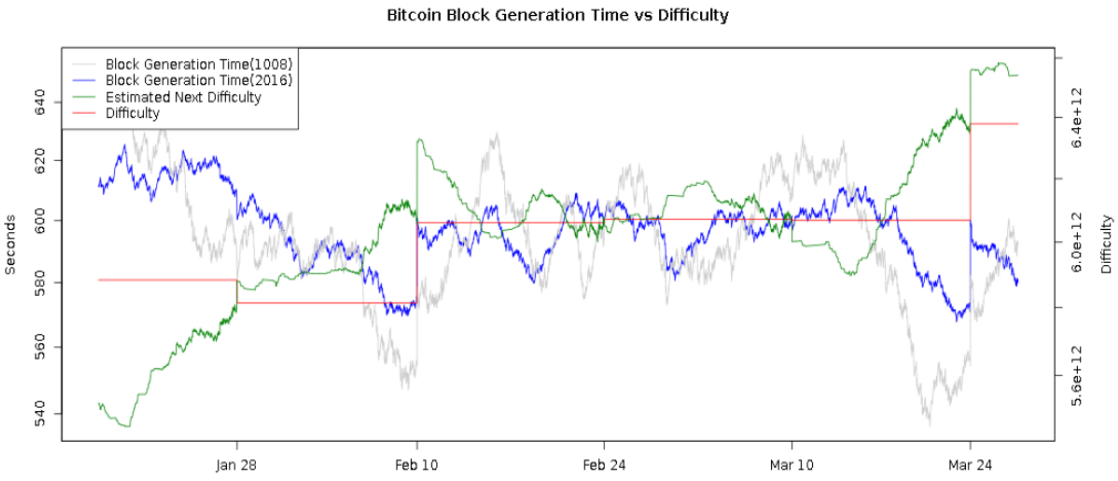
Bayt	Formül Değeri	Adı	Veri Türü	Açıklama
4	V	Versiyon	int32_t	Blok versiyonu. Her versiyon kendine ait kuralları içermektedir. 4 blok versiyon türü vardır.
32	P	Önceki bloğun özet değeri	char[32]	Önceki blok başlığının SHA216 özet değeri.
32	M	Merkle Root özet değeri [13,14]	char[32]	Merkle root değeri, tüm transfer verilerinin özet değerinden oluşmaktadır (bu blok da dahil). Bu değer zincirin bütünlüğünü sağlar.
4	t	Zaman	uint32_t	Özet hesaplamaya başlanan zaman. 11 blok önceki zaman değerinden büyük olması gerekmektedir.
4	n	nBits	uint32_t	Hedef özetteki başlangıç 0 değeri sayısı.
4	N	Tek kullanımlık sayı	uint32_t	Hedef özet değerine ulaşmamız için kullanılan tek kullanımlık sayı değeri.

Emek ispatında kazaman olmak için aslında N değerini bulmak gerekmektedir. Bu değer bulunduktan sonra ağa bildirilir ve zincire eklenir. Buna madencilik adı verilmiştir.

Bitcoin zorluk derecesi, kullanıcılar tarafından kontrol edilmektedir. Bu değer formül 1.1'deki T değeridir. Fakat bu değer madencilerin hızına ve o an ki T değerine bağlıdır. Zorluk derecesi; D'nin T ile olan ilişkisi aşağıdaki formül 1.2'de gösterilmiştir. Tmax, o ana kadarki en yüksek hedef değeridir.

$$D = \frac{Tmax}{T} \quad (1.2)$$

Bu zorluk derecesi her 2016 blokta bir değişmektedir. Yeni zorluğu hesaplamak için son 2016 blok kullanılır. Bu blokların oluşma süresinden tüm Bitcoin ağının özet oranı çıkarılır. Şekil 1.3'de zorluk derecesi değişim grafiğini göstermektedir. Mavi ile gösterilen, her 2016'ncı bloğun ortalama oluşma süresi, gri ile gösterilen ise her 1008'inci bloğun ortalama oluşma süresini göstermektedir. Yeşil ile belirtilen grafik tahmini zorluk derecesi ve kırmızı ile gösterilen is zorluk derecesini göstermektedir.



Şekil 1.3: Son iki aydaki Bitcoin zorluk derecesi değişimi. [15].

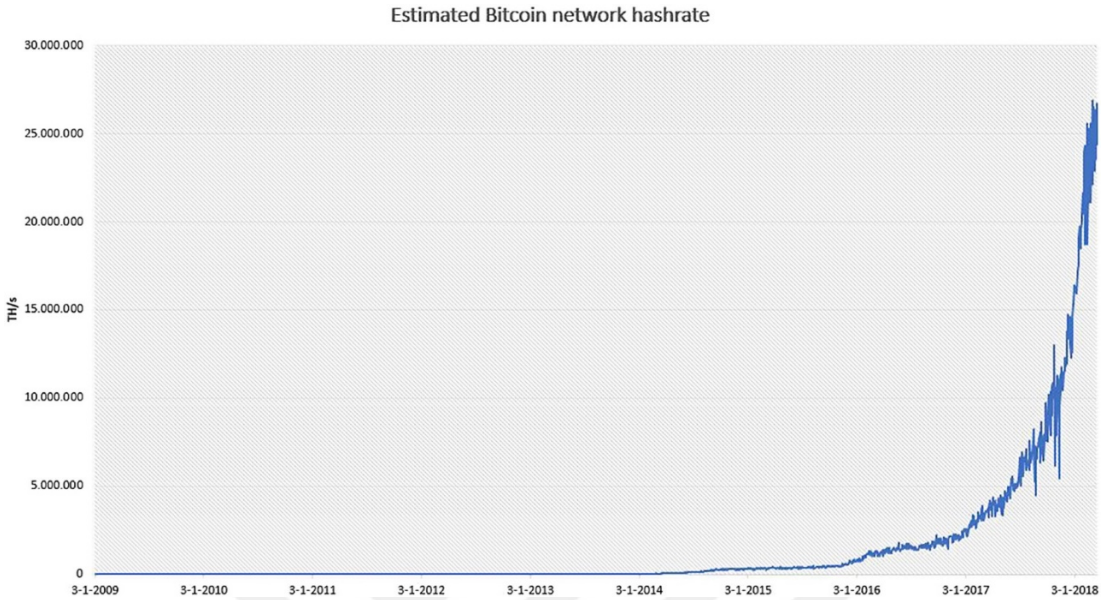
Bu özet değerini hesaplamak için işlem gücü (CPU) gerektirmektedir ve zorluk derecesi arttıkça gereken CPU gücüde artmaktadır. Bu durumda, kullanıcıları blok işlemeye teşvik etmek için sistem her işlenen blok için ödül vermektedir [3, 10]. Enflasyon oranını dengede tutmak için bu oran her 210.000 blokta yarıya inmektedir. Tezin yazıldığı zamanda ki ödül 12,5BTC'dir. Bu sonraki döngüde 6.5BTC'ye düşecektir [9]. Bu işlem, ödül 0BTC olana kadar devam edecektir. Bu durumda, sistem kullanıcıları madenciliğe teşvik etmek için blok transfer ücretinde ödül olarak vermektedir.

Çizelge 1.2: 2019 Bitcoin değerleri [9].

Parametre	Değer
Toplam Bitcoin	17.831.288
Toplam Üretilen Bitcoin	21.000.000
Toplam Üretilen Bitcoin Oranı	84.91%
Üretilebilecek Bitcoin	3.168.713
Bitcoin Değeri	$10.589,00
Günlük Üretilen Bitcoin Miktarı	1800
Bitcoin Enflasyon Oranı (Yıllık)	3.75%
Toplam Blok Sayısı	586.503
Ortalama Bir Blok Üretim Süresi	10dk
Ortalama Günlük Üretilen Blok Sayısı	144
Zorluk	9.064.159.826.491
Özet Oranı	75.20 Exahash/s

Fakat bu ödül mekanizmasına rağmen, Bitcoin uzun vadeli bir çözüm sunmamaktadır. Bu emek ispatı tabanlı tüm sistemler için geçerlidir. Bu tür sistemlerin güvenliği toplam işlem gücüne doğrudan bağlıdır [3,7,16]. Sürekli büyüyen bir sistemde, madenci sayasıda artacaktır. Dolayısıyla daha fazla enerji harcanacak, buna rağmen kazanılan ödülde bölüşülecektir. Bu durumdan dolayı daha az özet gücüne sahip madenciler ya donanımlarını güçlendirecek ya da daha büyük madenci havuzlarına dahil olmak isteyeceklerdir. Daha karlı olduğu için büyük havuzlara dahil olmak onlar için en güvenilir seçenek olacaktır. Bu büyük bir tehlike oluşturmaktadır. Madenci havuzlarının büyümesi, sistemin daha merkezi bir yapıya dönüşmesi, zincirin kontrolü bu havuzların kontrolünde olması demektir. Daha az özet gücüyle zincirin yapısı yapılan transferler değiştirilebilir [17]. 2014 yılında GHash adlı madenci havuzu 54%'lük özet gücünü elde etmişti, fakat zincirde herhangi bir değişim veya bozulma olmadı. Sistemdeki güven ortamını koruma adına Bitcoin madencileri de kendi işlem güçlerini başka havuzlara alarak bu duruma önlem aldılar [18]. Şekil 1.4'de görüldüğü üzere günümüze geldiğimizde yapılan özetleme işlemlerinin sayısı hızlı bir şekilde

artmaktadır. Bu artışla birlikte harcanan enerjide artmaktadır. Bitcoin sisteminin 2014 yılındaki enerji tüketim miktarı İrlanda Cumhuriyeti ile aynı miktardaydı [21].



Şekil 1.4: Bitcoin ağı tarafından yapılan saniyedeki tahmini terahash sayısı [8].

Kripto para sistemlerinde güvenlik-enerji tüketim durumunu ortadan kaldırmak için 2012 yılında yeni bir çözüm sunuldu. Bu çözüm Bitcoin forumlarında 2011 yılında tartışılmıştı. Emek ispatı protokolü yerine sunulan bu protokolün adı hisse ispatıdır (PoS). Sunny King ve Scott Nadal tarafından oluşturulmuştur ve adı Peercoin'dir [19]. Bu protokolde, sistem kullanıcıların zincirdeki hisselerine bağlıdır. Kullanıcı ne kadar çok hisseye sahipse o kadar çok blok işleme şansına sahiptir. Emek ispatı tabanlı sistemlerdeki gibi işlem gücüne sahip olmalarına gerek yoktur. Bu yüzden enerji tüketimi daha azdır.

1.1 Tezin Amacı

Enerji tüketiminden dolayı, emek ispatı tabanlı blokzincir sistemleri uzun süreli çözümler değildir. Bu problemi çözmek için hazırlanan yeni ispat algoritmalarından biri hisse ispatı protokolüdür. Bu protokol, kullanıcıların zincirdeki hisselerini esas alır. Fakat bu protokolünde kendine ait problemleri vardır. Tezin amacı; bu hisse ispatı uzlaşma protokolünü kullanan kriptopara uygulamalarına ait protokollerin detaylı bir teknik analizinin ve karşılaştırılmasının bu problemler üzerinden yapılmasıdır. Hedef, yapılan teknik analiz ve karşılaştırma sonucu hisse ispatı tabanlı sistemlerin önemli

bileşenleri ve karakteristiklerinin belirlenmesi ve bu sistemlerin ortak bir tasarım tanımının yapılmasıdır.

1.2 Yöntem

Karşılaştırma ve analiz, PeerCoin, Nxt ve Ethereum'un Casper protokolleri üzerinden olacaktır. Bu kriptoparaların seçilme nedeni, fikir birliği algoritmalarının temelde aynı prensipler üzerine kurulu olup, hisse ispatı protokolünü farklı işlemeleridir. Bu sistemlerin blok, zincir, ağ, sisteme katılım, madencilik, ceza sistemleri ve fikir birliği algoritmaları üzerinden detaylı teknik analizi yapılacaktır. Karşılaştırma, ortaya konan bir şey olmama problemi, tarih saldırısı, sahte hisse saldırısı, %51 problemi, DDoS saldırılarına karşı ürettikleri çözümler üzerinden olacaktır.
Teknik analiz genel bir terim. Öncelikle sistemler nicel özellikleri ortaya konacak ve bunları kaynak kodları, geliştirici dokümantasyonları ve yazılan makaleler ile pekiştirilecek. Daha sonrasında, bu sistemleri oluşturan parçalar ve aralarındaki ilişkiler çıkarılacak. Bulunan bu parçaların kritik noktaları, zayıf ve güçlü tarafları analiz edilip üst düzey bir genel model oluşturulacak.

1.3 Tezin İçeriği

Tezde ilk olarak literatür araştırmasında, araştırılan uygulamaların; Peercoin, Nxt ve Etherum'un Casper protokolleri anlatılmaktadır. Literatür araştırmasında önce bir blokzincir sisteminin önemli bileşenleri olan blok, zincir, ağ ve ağa katılım ve uzlaşma protokollerinden bahsedildi. Peercoin, Nxt ve Casper'ın araştırma için önemli görülen bileşenleri anlatıldı. Hisse ispatı sisteminin zayıf olduğu saldırılar ve problemler anlatıldı. Analiz ve karşılaştırma kısmında bu üç uygulamanın protokolleri karşılaştırıldı, ortak bir tasarım üretildi ve öneriler sunuldu. Sonuçlar kısmında yapılan çalışma özetlendi, kısıtlardan bahsedildi ve bulunan bulgular aktarıldı.

2. HİSSE İSPATI TABANLI SİSTEMLER

Bu bölümde literatür araştırmasına yer almaktadır. Bu kısımda hisse ispatının temel prensipleri anlatılacak, hisse ispatının farklı uygulamaları incelenecek ve hisse ispatının problemlerinden bahsedilecektir.

2.1 Sistem Bileşenleri

Sistemleri ve protokolü incelemeden önce sistemin temel yapılarının anlatılması gerekmektedir. Bir blokzincir sistemin temel parçaları; blok, zincir, protokol ve ağdır. 2.1.1, 2.1.2, 2.1.3 ve 2.1.4'de bu bileşenler anlatılmaktadır.

2.1.1 Blok

Transfer bilgilerinin tutulduğu kayıttır. İki parçadan oluşmaktadır; başlık ve ana kısım. Başlıkta önceki bloğa referans olan bir özet değeri ve bu değerin hesaplanması için gereken bilgileri bulunmaktadır. Eğer bir blok başka bir bloğa ait referans değeri taşımıyorsa, bu başlangıç bloğudur, zincirdeki ilk veridir.

2.1.1.1 Özet referans değeri

Bu referans değeri, bir özet değeri alınmış bir veriyi tutar. Verinin değişip, değişmediğini tekrar özet değeri alarak kontrol edebilmemiz için gereklidir [22]. Blokların tarihsel sırasının korunması için gereklidir.

2.1.2 Zincir

Blokların belli bir kurala göre sıraya göre dizilip oluşturduğu yapıdır. Bazı zamanlarda zincirin sırası bozulup, dallanmalara neden olabilir. Bu durumdan dolayı kullanıcıların para transferi yapıp blok işlemeye devam edebilmesi için bir zinciri seçmeleri gerekir. Bu genelde birbirini takip eden en uzun blok zinciri olur. Dağıtık sistemlerde bu yapının kurulması için mantıksal saate ihtiyaç vardır. Bu saat; dağıtık sistemlerde kronolojik ilişkinin kurulması için bir mekanizmadır.

2.1.2.1 Madencilik

Sürekli büyüyen bir zincire, düzenli olarak yeni blokların oluşturulup, belli bir sıraya göre eklenmesi işlemine madencilik denir. Katılımcılar bu blokların geçerliliğini belirlenen kurallara göre doğrulayabilir.

2.1.3 Ağ ve ağa katılım

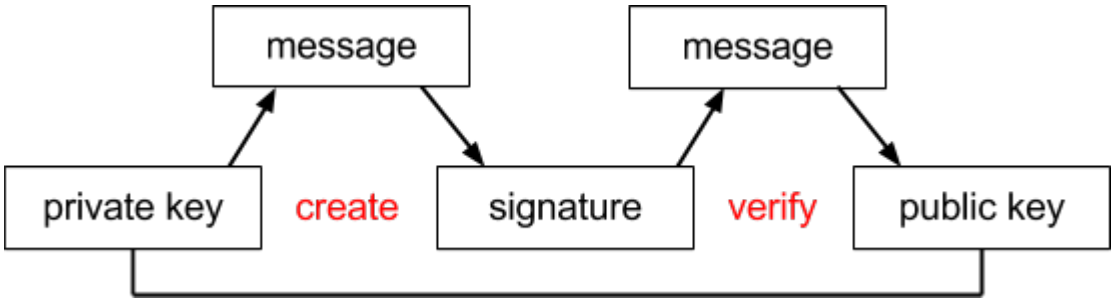
Kullanıcıları ayırt edebilmek, hangi veri kime ait anlayabilmemiz için her katılımcı açık ve gizli anahtarı ile işlem yapmalıdır. Sistem dijital imza yapısını kullanmaktadır. Verinin değişmemesi için sistem merkezi olmayan bir yapıya sahiptir. Yani veri tek bir otoritenin kontrolü altında değildir. Böyle bir sistem için eşler arası ağ yapısı en iyi çözümdür.

2.1.3.1 Eşler arası ağ

Bu dağıtık bir mimari yapıdır. Eşleri birbirleriyle tek bir amaç için bir araya gelirler ve belli verileri ortak bir şekilde kullanırlar. Bu sistemde otorite yoktur. Kurallar eşler tarafından belirlenir. Bir blokzincir sisteminde eşler zinciri ortak veri olarak kullanmaktadırlar. Zincire veriler belirlenmiş kurallara göre eklenir. Fakat eklenen verinin sonradan değişmediğini kanıtlayabilmemiz için her veri dijital imza ile imzalanır.

2.1.3.2 Dijital imza

Matematiksel bir dijital veri doğrulamasıdır. Geçerli bir dijital imza var olan bir veriden üretilir ve verinin sonradan değişmediğini ve oluşturulduğu andaki halini koruduğunu kanıtlamak için kullanılır. Şekil 2.1'de anlatıldığı üzere veri gizli anahtarla şifrelenir ve açık anahtarla doğrulanır.



Şekil 2.1: Dijital imza şeması [23].

2.1.4 Kurallar ve uzlaşma protokolü

Kullanıcılar eşler arası ağ yapısını kullanmaktadır ve sistemin güvenilir ve düzgün bir şekilde kullanılabilmesi için ortak kuralların önceden belirlenmiş olması gerekmektedir. Sistemin amacı herkeste ortak bir veri tabanı oluşturmaktır. Bu veri tabanına veri defteri denmektedir. Veri defterinin herkeste aynı sonuçları tutması için kullanıcıların, işlem yapabilmek için kullandığı uygulamanın aynı sonuçları üretmesi gerekmektedir. Kullanılan uygulama, kullanıcılar arasında veri paylaşımın yapılması ve uzlaşmayı sağlamaktadır. Eklenen verinin herkes veya belli kişiler tarafından onaylanması ve ana zincirde olması gerekmektedir. Bundan dolayı kullanıcılar arasında bir uzlaşma protokolü belirlenmiş olmalıdır.

2.1.4.1 Veri defteri

Veri defteri bir dosyadır ve tüm işlenmiş blok bilgilerini tutmaktadır. Blokzincir ise dijital ve dağıtık veri yapısını kullanan bir veri defteridir.

2.2 Hisse İspatı Protokolü

Bu protokolde uzlaşma kullanıcıların zincirdeki hisselerine bağlıdır. Bir kullanıcı, ne kadar para zincirde bulundurursa, blok işleme olasılığı o kadar artar. Emek ispatında ise bir madencinin özetleme gücü ne kadar fazla ise, onunda bir bloğu işleme olasılığı o kadar fazla olur. Yani blok işlemek için yapılan işi göstermek yerine hisseler ile kanıt sunulur.

Bu protokol ilk olarak BitcoinTalk forumunda "QuantumMechanic" adlı kullanıcı tarafından sunuldu [20]. Ana fikir zincirde en uzun süre tutulan ve en fazla miktarda olan hissenin sahibi olduğunu kanıtlamak. Eğer bu kanıtlandığı takdirde, bu kullanıcı yeni bloğu işleme hakkına sahip olacak ve Bitcoin'de olduğu gibi bunun karşılığında ödül alacak. Bu sistemin emek ispatı sistemlerinden en önemli farkı ise az enerji harcamasıdır. Bitcoin'de hedef değere ulaşmak için, zorluk derecesine bağlı birden fazla tane özetleme yapılırken, hisse ispatında bir kere yapılması. Fakat bu protokolde kendine has problemler içermektedir. Bunlardan en önemli olanı ise ortaya konan bir şey olamama (NaS) problemidir. Bu problemde sorun, blok işlemek isteyen kullanıcıların enerji harcamadan bu işi yapıyor olmalarıdır. Yani kullanıcılar her çıkan yeni transfer bloğunu işlemeye katılabilirler. Fakat emek ispatı sisteminde bunu

yapmak daha zordur, çünkü özetleme gücümüzü her blok için ayırmamız gerekmektedir.

Peercoin [19], BlackCoin [25], Nxt [24] ve BitShares [26] bu protokolü kullanan ilk uygulamalardandır. Her uygulama kendine özgü PoS protokolü geliştirmiştir. Bunlardan bazıları para yaşına dayalı, rassal ve temsilcilerin bulunduğu blok üretici seçimi olarak gruplayabiliriz.

2.2.1 Para yaşına dayalı seçim

Bu fikir, 2010'da ilk olarak Satoshi Nakamoto tarafından sunuldu. Bu metot para yaşını parametre olarak kullanmaktadır. Zincirdeki harcanmayan her paranın bir yaşı vardır ve üzerinden belli bir süre geçtikçe bu yaş değeri artar. Burada ispat para yaşı ve değeri üzerinden yapılmaktadır. PeerCoin bu seçim yöntemini kullanmaktadır.

2.2.2 Rassal Seçim

Buradaki fikir, para yaşının kullanıcıları paralarını harcamamaya teşvik etmesinden dolayı para yaşı parametresini kaldırmıştır. Burada ispat kullanıcıların zincirdeki para miktarı ile yapılmaktadır. Nxt ve BlackCoin bu seçim yöntemini kullanıyor.

2.2.3 Temsilcilerin Bulunduğu Seçim (DPoS)

Steemit, EOS ve BitShares bu yöntemi kullanmaktadır. Bu yöntemde, zincirde parası bulunanlar blok işleme hakkına değil, oy verme hakkına sahiptirler. Kullanıcılar oylarıyla, kendi aralarından bir delege seçerler ve bu delegeler blokları işleme işini yaparlar. Blok işleme sırası, delegeler arasında, belli aralıklarla değişir. Bu her delegeye blok işleme hakkı verir. Eğer bir delege blok işleme sırasını kaçırır ve geçerli olmayan blokları işlemeye çalışırsa, kullanıcılar bu kullanıcıdan delege haklarını alabilir ve onun yerine başka bir delege seçebilir.

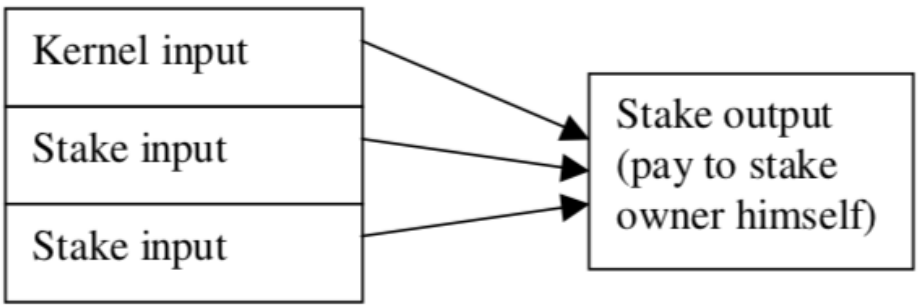
Bu sistemde, emek ispatındaki rekabet etmek yerine, delegeler birlikte çalışabilir. DPoS blok işleme hızı olarak çoğu uzlaşma protokolünden daha hızlıdır. EOS, 1 saniyenin altında blok işleyen ilk uygulamadır. Tabi bunun karşılığında sistem daha merkezi bir yapıya geçmiş olmaktadır.

2.3 Peercoin

PeerCoin Sunny King ve Scott Nadal tarafından 2012'de sunuldu [19]. Burada fikrin çıkış noktası; PoW tabanlı kripto para uygulamaları, enerji tüketimleri yüksek olması ve bu enerji tüketiminin direk sistemin güvenliği ve merkezileşmesi ile bağlantılı olmasıydı. Sunulan protokol ile bu bağlantının ortadan kaldırılması amaçlanmaktadır. PeerCoin emek ve hisse ispatının birlikte kullanıldığı bir çözümdür [19, 28]. Emek ispatı kısmı transfer bloklarını üretme işini yaparken, hisse ispatı kısmı ise kanıt bloğunu üretme işini yapar. PeerCoin'de kullanıcıların yaptıkları işin az olması nedeniyle, blok üretme işlemine "para basma" ismi verilmiştir [19]. Para birimi ise PPC'dir.

2.3.1 Blok

PeerCoin; PoW ve PoS protokollerinin birlikte kullandığından, ikisi için ayrı blok oluşturur. PoS için oluşturduğu bloğun ismi "coinstake"'dir. Bu blokta kullanıcının kendine ödediği bilgiler bulunmaktadır. Bundaki amaç kullanıcının kendisine ödeme yaparak para yaşını harcaması ve blok oluşturma hakkı kazanmasıdır. Coinstake oluşum diyagramını Ek 1'dedir.



Şekil 2.2: Coinstake blok yapısı [19].

Şekil 2.2'de görüldüğü üzere, bu bloğun ilk parametresinin ismi kernel'dir ve bu değer belli bir hedef özet değerine ulaşmak zorundadır. Fakat burada önemli olan, özetleme işleminin belli bir kısıtlama altında yapılıyor olması yani Bitcoin'deki gibi sınırsız bir alana sahip olmamasıdır. Burada kısıt bu işlemin saniyede bir yapılabiliyor olmasıdır [19]. Buradaki rassallığı sağlayan değer, tek seferlik sayı yerine zamandır.

Çizelge 2.1: PeerCoin PoW blok içeriği [28].

Bayt	Adı	Açıklama
4	Blok büyüklüğü	Bu bloğun bayt değerinde büyüklük değerini tutar.
4	Versiyon Numarası	1'e eşit olması bekleniyor. Bu bloktan bir tane oluşmuş olması lazım.
32	Önceki Bloğun Özet Değeri	Bir önceki bloğun özet değerini içerir.
32	Merkle Root Özet Değeri	Merkle root değeri, tüm transfer verilerinin özet değerinden oluşmaktadır (bu blok da dahil). Bu değer zincirin bütünlüğünü sağlar.
4	Zaman	Oluşturulma zamanını tutar.
4	nBits	Hedef zorluk derecesini tutar.
4	Tek Kullanımlık Sayı	Hedef özet değerine ulaşmamız için kullanılan tek kullanımlık sayı değeri.
1-9	Transfer Sayacı	Birden fazla transfer yapılabildiği için girdi-çıktı sayılarını tutar.
Transfer sayısı ile değişir	Transferler	Tüm transfer bilgilerini içerir.
1-9	* Blok İmza Büyüklüğü	txout[0] (giden transferin ilk sahibi) sahibi tarafından imzalanır.
Blok imza büyüklüğüne göre değişir	* Blok İmzası	Blok imzasını bayt kodu olarak içerir.

2.3.2 Protokol

Peercoin para yaşına dayalı seçimi kullanır. Bu yöntem Nakamoto tarafından biliniyordu. Bu yöntem aslında Bitcoin transferlerini öncelik sırası belirlemek için kullanılıyor fakat güvenlik açısından bir önem araz etmiyor. Bu model, basitçe, ne kadar çok para zincirde tutulursa, o kadar kullanıcının blok işleme şansı artıyor. Örnek olarak; bir A kullanıcısı 10PPC aldı ve bunu 10 gün boyunca harcamadı. B kullanıcısı da 10PPC aldı ve bunu 20 gün boyunca tuttu. Bu durumda, 10'ncu günün sonunda A kullanıcısının para yaşı 100 olurken, B kullanıcınsın para yaşı 200 olur ve B kullanıcısı blok onaylayıcısı olarak seçilmek isterse, bunun ihtimali A kullanıcısının olma ihtimalinin iki katıdır. Bu tutulan paralar harcanırsa veya blok işleme için kullanılırsa tüm biriktirilen para yaşı da harcanmış olur. Bir paranın maksimum yaşı 90 gün olabilir [19, 28].

$$
\begin{aligned}
& hash(nStakeModifier \\
& + txPrev.block.nTime \\
& + txPrev.offset \\
& + txPrev.nTime \\
& + txPrev.vout.n \\
& + nTime) \\
& < bnTarget \\
& * nCoinDayWeight
\end{aligned}
\tag{2.1}
$$

Formül 2.1'de hesaplanan özet değeri, para yaşı kanıtı için gereklidir [31]. Kernel alanındaki ilk değer, bu değere ulaşmalıdır. Önceki blok değerleri ile zaman (nTime) değerinin özet değeri alınır. Belirlenen zorluk derecesi (bnTarget) ve para yaşı çarpımından küçük olması gerekmektedir. Zaman değeri burada sürekli arttırılır ve her saniyede yeni bir özet değeri hesaplanır. Para yaşı ne kadar büyükse bu değere ulaşmak o kadar kolay olur.

Hisse sahibi biri, blok işlemek isterse bu 2.1'deki değeri içeren coinstake bloğunu oluşturmak zorundadır. Blok oluştuktan sonra, biriktirilen para yaşı sıfırlanır [19].

Bitcoin'de bu hedef özet değeri her blok için sabitken, Peercoin'de para yaşına bağlı olarak değiştiğini formül 2.1'den görebiliriz. Ne kadar para yaşı harcanırsa, blok işleme şansı o kadar artmaktadır. Örnek olarak, A kullanıcı 10PPC'yi iki gün bekletirse 20 para yaşına sahip olur, B kullanıcısı, aynı miktarı, 1 gün bekletirse 10 para yaşına

sahip olur. A kullanıcısı bir bloğu bir günde işleyebilme gücüne sahipken, B'nin 2dir [19].

Bu zincirde para bekletme durumu, kullanıcıları çeken bir durum değildir. Çünkü kullanıcı, para yaşı biriktirmesi için parasını harcamaması gerekmektedir. Bu maksimum 90 gündür [19]. Bu durumu daha cazip hale getirmek için Peercoin, kullanıcının biriktirdiği paranın 1%'ni yıllık olarak ödeme yapar. Peercoin transfer ücreti ödemesi yapmaz. 0.01 PPC/kB olarak protokolde belirlendi fakat kullanılmamaktadır. Bunu blok işleyen kişiye ulaşmadan yok eder. Ayrıca oluşturulan tüm para için bir limit belirlenmemiştir. Bu yok etme işlemi enflasyon düşürme için yapılmaktadır.

2.3.3 Mükerrer kayıt protokolü

Bu protokol DDoS saldırılarını durdurmak için oluşturulmuştur. Sistem oluşturup, sisteme dağıtılan blokların kernel girdilerini kontrol eder. Bir önceki gelen ile aynı girdiye sahip bir veri varsa yeni gelen blok eklenme işlemi gerçekleşene kadar reddedilir [19]. Bu yüzden her blok, kopyalanmaması için, oluşturan kişi tarafından imzalanmalıdır.

2.3.4 Ana Zincir Seçim Protokolü

Her transfer işlemi, harcanmış para yaşı içerir. Bu protokol ise kazanan zincir olarak en çok para yaşı harcanmış zinciri seçer. Bitcoin'de ise, en çok iş yapılan zincir seçilir [19, 28]. Bu durum 51% problemini gerçekleşme ihtimaliniz azaltmaktadır [19]. Burada zincirin gidişatını değiştirmek isteyen bir kullanıcı zincirdeki çok yüklü miktarda parasının olması gerekmektedir. Ayrıca her blok işleme durumunda para yaşı harcandığı için bu problemin olmasını zorlaştırır.

Fakat kaynak kodunu incelediğimizde biraz farklı bir durum söz konusudur. Kodu incelediğimizde en yeksek güvene sahip olan blokların bulunduğu zincir seçilmektedir. Kodu basitleştirdiğimizde formül 2.2 ve 2.3'deki durum söz konusudur.

$$PoS = \frac{2^{256}}{(bnTarget\ + 1)} \tag{2.2}$$

$$PoW = 1 \tag{2.3}$$

Zincir seçiminde aslında en çok güven (blockTrust) sahibi olan bloklar seçilir. Formül 2.2'de ki hedef değeri (bnTarget) önceden belirlenmiş zorluk değeridir. Bitcoin'deki nBits ile aynı işlevi görür.

2.3.5 Kontrol Noktaları

Para yaşı modeli bazı sorunları çözmesine rağmen, başka problemlerin olma ihtimalini de arttırmaktadır. Bu problemler zincirin bütünlüğünün bozulmasına neden olabilecek saldırılara karşı zayıflatır. Bitcoin bu duruma karşı güçlü olmasına rağmen, Satoshi Nakamoto, 2010 yılında, blokzincirin geçmişini sağlamlaştıracak kontrol noktası çözümünü sundu. Burada fikir, zincirin belli bir kontrol noktasından sonra geçmişinin değişmemesi üzerine.

Burada en büyük sorun çifte harcama problemidir. Kullanıcı belli bir para yaşı biriktirip, bunu her zincire eklenmek istenen bloklar için kullanabilir. Peercoin bunu çözmek için kontrol noktaları kullanmaktadır. Fakat bu kontrol noktalarını, günde birkaç kez olmak üzere, tek bir merkezden yayınlamaktadır. Bitcoin'deki alarm sistemine benzemektedir.

Bitcoin kullanıcıları en çok iş yapılan zinciri, ana zincir olarak kabul etmektedir. Peercoin'de ise en çok para yaşı harcanan zincir, ana zincir olarak seçilir. Kullanıcı aynı para yaşını her gelen yeni blok için harcasa bile, zincir günlük doğrulandığı için, oluşturduğu blok ana zincirde değilse ödülü alamayacaktır ve tüm biriktirdiği para yaşını kaybedecektir.

Geliştiricilerin iddiasına göre bu önlem sadece büyüme aşaması için gerekliydi. Versiyon 0.2'den sonra bunun sistemin kritik bir parçası olmadığı iddia edildi. Geçmiş zincir bilgileri, önemli bir hata durumu için 2016 yılına kadar yoğun olarak tutulmuştur. Bu 0.6 versiyonundan sonra kullanıcıya seçenek olarak sunulmuştur [30].

2.4 Nxt

Nxt, bir emek ispatı protokolü kullanan, açık kaynaklı java projesidir. 2013 yılında, "BCNext" isimli, anonim bir yazılım geliştiricisi tarafından geliştirilmiştir. 2015'te Farla Webmedia "NXT Asset Exchange" projesini piyasaya sürmüştür. Peercoin'deki gibi kullanıcıların zincirdeki para miktarlarını kullanır. Para yaşı parametresini kullanmaz. Burada madencilik işine demircilik denir. Para birimi NXT'dir. Bir milyar NXT sisteme dağıtılmıştır. Curve25519 şifreleme ve SHA256 özetleme algoritmalarını kullanmaktadır. Ortalama her 60 saniyede bir blok oluşturmaktadır. Transfer ücreti blokları, bu ortalama süre hesabına dahil değildir. Her 10 blokta bir transfer blokları sabitlenmiş olur. Nxt, şu anki mimari yapısı ve blok büyüklüğü düşünüldüğünde günde toplam 367200 transfer yapabilme gücündedir.

2.4.1 Blok

Diğer kripto paralarda olduğu gibi Nxt'de bloklar bir zincire, belli bir sıra halinde eklenir. Her hesap bu zinciri kendisinde tutar. Buradaki transfer bilgileri kullanıcılar tarafından onaylanır. Bir kullanıcı blok işleyicisi olmak istiyorsa, kendisine yapılan bir transferin 1440 kere onaylanmış olması gerekmektedir [24]. Bu durum 2.4.2'de anlatılmaktadır. Bundan sonra bu kullanıcı aktif bir kullanıcı konumuna geçmiş olur.

Nxt'de her blok maksimum 255 transfere kadar bilgi tutabilmektedir. Blok başlığı 192 bayttır. Ayırt edici özelliklerini içerir. Transfer bilgilerinin tutulduğu kısım ise 160 bayttır ve bir bloğun maksimum boyutu 32KB olabilir [24].
Bir bloğun içeriği şu şekildedir;

- Blok versiyonu.
- Blok derecesi (zincirdeki sırası).
- Blok ID'si.
- Zaman (saniye bazında).
- Kullanıcının ID'si ve açık anahtarı
- Bir önceki bloğun ID'si
- Transfer sayısı.
- Toplam NXT miktarı.
- Tüm transferlerin bilgileri ve ID'leri
- Blok oluşturma imzası.

- Bütün bloğun özeti değeri.
- Temel hedef değeri.
- Kümülatif zorluk değeri.

Blok yapısı ek 2'de ayrıntılı olarak gösterilmiştir.

2.4.2 Protokol

Nxt'de Peercoin gibi ne kadar cok para zincirde tutulan para miktarına bağlı, blok işleme şansını arttıran bir sisteme sahiptir. Transfer sonunda yeni para üretilmez, transfer ücreti işleyen kişiye verilir. Bu yüzden Peercoin'deki gibi bu işlemin adına para basma (minting) yerine, "forging" denmiştir [24].

İşlenen bloklar yine başlangıç bloğuna kadar takip edilebilir. Diğer sistemlerde olduğu gibi Nxt bloklarında da bir önceki bloğu referans veren özet değerlerini taşımaktadır.

Blok işleme hakkı kazanmak için her kullanıcı, diğer sistemlerde olduğu gibi belli bir hedef değerinden daha küçük bir özet değeri üretmek zorundadır. Fakat bu değer Bitcoin'de olduğu gibi her blok için sabit değildir. Üç anahtar değer blok işleme için belirleyicidir. Bunlar temel hedef değeri, hedef değeri ve kümülatif zorluk değerleridir [24].

Blok işleme hakkı kazanmak için kullanıcılar bir özet değeri hesaplar ve bu özet değeri temel hedef değerinden düşük olmalıdır. Bu değer her blokta değişiklik gösterir. Bir önceki bloğun temel hedef değeri ve bloğu oluşturmak için gereken zamanın çarpımından elde edilir.

$$T = T_b * S * B_e \tag{2.4}$$

Formül 2.4'de görüldüğü üzere her kullanıcı kendi hedef değerini hesaplamalıdır. Bu formülde T; hesaplanacak hedef değeri, $T_{b;}$ bir önceki bloğa ait temel hedef değeri, S; bir önceki bloğun işlenmesinden sonra geçen süre (saniye olarak) ve B_e ise kullanıcının o anki kullanılabilir para miktarıdır. 2.3'den anlaşılacağı üzere hedef değeri her saniye geçtikçe artmaktadır. Kullanıcın para miktarı hariç, tüm değerler diğer kullanıcılar için eşittir.

Zincirdeki her blok, üretim imzasına sahiptir. Blok işlemek isteyen bir kullanıcı, EC-KCDSA [24,32,33] ile bir önceki bloğun üretim imzasını imzalar. Bu 64 baytlık bir imza oluşturur. Sonra SHA256 ile özeti oluşturulur. Sonra bu değerin ilk 8 baytı alınır ve kullanıcının hesapladığı hedef değeri ile karşılaştırılır. Bu 8 baytlık değer, bizim

bulduğumuz değerden küçük ise blok işlenir. Değilse, Peercoin'deki gibi her saniye için tekrar hesaplanır ve kontrol edilir.

Fakat burada şöyle bir sorun karşımıza çıkmaktadır. Bu durum ise bir kullanıcı, hesabındaki değeri, sürekli kendine ait başka hesaplara atıp transfer ücretini düzenli olarak alabilir. Çünkü bloğu kimin işleyebileceği tahmin edilebilir. Bundan dolayı Nxt'te, bir hesap, blok işlemeye sadece 1440 blok öncesine kadarki değeriyle katılabiliyor.

Peercoin'de olduğu gibi transferler tek bir blokta toplanabilir. Bir kullanıcı blok işleme hakkı kazandığı transferleri tek bir blok altında işleyebilir. Bu 255 tane transfer için yapılabilir [24, 32].

Aynı transfer bloğunun oluşma durumunda ise, ağ toplam zorluk derecesi en yüksek olan bloğu tercih edeceklerdir. Bu durum 2.4.4'te anlatılmaktadır.

2.4.3 Kontrol Noktaları

Peercoin'deki gibi bir kontrol noktası sistemine sahiptir. Fakat bu kontrol noktası yöntemi yayınlanmaz. Burada 720 blok öncesine kadar bloklarda değişiklik yapılabilir [24, 32, 33]. Bundan öncesi için yapılan ekleme ve değişiklikler ağ tarafından reddedilir. Bu Nxt'in tek kontrol noktasıdır.

Her blok, kendisinden sonraki 10ncu blok işlendiğinde sabitlenmiş olur ve transfer gerçekleşir.

2.4.4 Artan Zorluk

Aynı transfer bloğundan birden fazla oluşma durumunda ise kullanıcılar zorluk derecesi en yüksek olanı seçecektir. Aksi takdirde bu durum zincirde çatallaşmaya yol açabilir.

Formül 2.5'de kümülatif zorluk derecesi; D_{cb} değerinin hesabı yapılmıştır. Bu değeri hesaplamak için önceki bloğun zorluk derecesi değeri; D_{pb} ve bir önceki bloğun hedef değeri; T_b gerekmektedir.

$$D_{cb} = D_{pb} + \frac{2^{64}}{T_b} \tag{2.5}$$

2.4.5 Ekonomik Kümelenme

Bu özellik hala geliştirilme aşamasındadır. Burada olay, bir saldırgan, geçmişi değiştirmesine teşebbüs etmesini engellemektir. Sisteme yeni bir blok eklendiğinde bunun esas zincirde olması gerekmektedir. Bu zincir, sistemin esas ekonomik kümesidir. Bu kümenin dışında başka bir kümeye bir blok eklenmeye çalışıldığında kullanıcı buradan ödül alamaz [24]. Blok işleme hakkı bir süreliğine elinden alınır.

2.5 Casper

Casper, Ethereum'un yeni hisse ispatı tabanlı kripto para sistemidir. Bu sistemin Ethereum'un eski sisteminin yerine yapılması için tasarlanmıştır. Bizans hata toleransı (BFT) ile hisse ispatını protokollerini birlikte kullanan hibrit bir tasarımdır.

İki çeşit hisse ispatı tasarımı vardır; bunlardan biri emek ispatını mekaniklerini ve özelliklerini kullananlardır. Bunlar Peercoin, Nxt, Blackcoin gibi uygulamalardır. Diğeri ise BFT kullanan PoS tasarımlarıdır. Bunu ilk PoS için tasarlayan uygulama Tendermint'tir. Casper'da bu tasarımı kullanmaktadır. Bu tasarımda kullanıcıların 2/3'ü veya daha fazlası dürüst davrandığı sürece protokol doğru işleyecektir.

Casper ekstra olarak, BFT algoritmasının sağlamadığı özellikleri içermektedir. Bunlar;

- Mali sorumluluk; eğer bir onaylayıcı, belirlenen kuralları çiğnerse cezalandırılır.
- Dinamik onaylayıcılar; onaylayıcılar zaman içeresinde değişir.
- Koruma; onaylayıcıların 1/3'ü çevrim dışı ise, uzun menzil saldırılarına karşı koruma sağlar.
- Güncellenebilir olması; var olan PoW tabanlı uygulamalar için kolayca eklenebilir.

Normal şartlar altında, sistemde blokların bir sıralı liste oluşturması beklenmektedir. Bunun her üst bloğa bağlı tek bir alt bloğun oluşturulması gerekmektedir. Fakat birden fazla alt blok oluşmuş olabilir. Casper'ın işi ise zincir için doğru alt bloğu seçmektir.

Casper aslında iki ayrı projeden çıkmıştır. Bunlar; Casper the Friendly Finality Gadget (FFG) ve Casper the Friendly GHOST: Correct-by-Construction (CBC) projeleridir.

FFG projesi Ethereum'un PoS protokolüne geçiş için hazırlanmış PoS-PoW tabanlı bir projedir. Bu Vitalik Buterin tarafından geliştirilmiştir. CBC ise oluşabilecek

problemlere çözümleri formüle etmiştir. Bu proje Vlad Zamfir tarafından geliştirilmiştir. Casper projesinin son hali iki çalışmanın ortak bir ürünü olacaktır.

2.5.1 Protokol

Casper protokolü şu an için emek ispatı ile birlikte kullanılacak şekilde tasarlanmıştır. İleride bu değiştirilmesi düşünülmektedir. Bu versiyon her bloğun düzenli bir şekilde, oluşturulması sırasına göre sıralı bir liste halinde olması beklenmektedir. Olası bir gecikme, ağa bağlama sorunu veya saldırılar sonucu bir üst blok için birden fazla alt blok oluşabilir. Casper protokolünün işi doğru bloğu zincire eklemektir.

Verimli olmak adına, Casper tüm zincirle uğraşmak yerine sadece zincirin belli bir kısmıyla ilgilenir. Bunu kontrol noktaları sayesinde yapar. Kontrol noktaları 2.5.2'de anlatılmaktadır.

Bir blok işlemek için, blok işleyicilerin 2/3'ünden fazlasının onayına ihtiyaç vardır. Blok işleyicisi olmak için, kullanıcının zincirdeki hissesinin tamamını veya bir kısmını depozit olarak vermesi gerekir, Kullanıcı katıldıktan sonra bu depozito değeri cezalara veya ödüllere bağlı olarak artıp azalabilir. Burada 2/3 ile belirlenen pay ise kullanıcıların depozito değerleridir. Kullanıcıların depozito değerlerinin toplamının, tüm onaylayıcıların depozito değerlerinin toplamının 2/3'ü etmesi gerekmektedir.

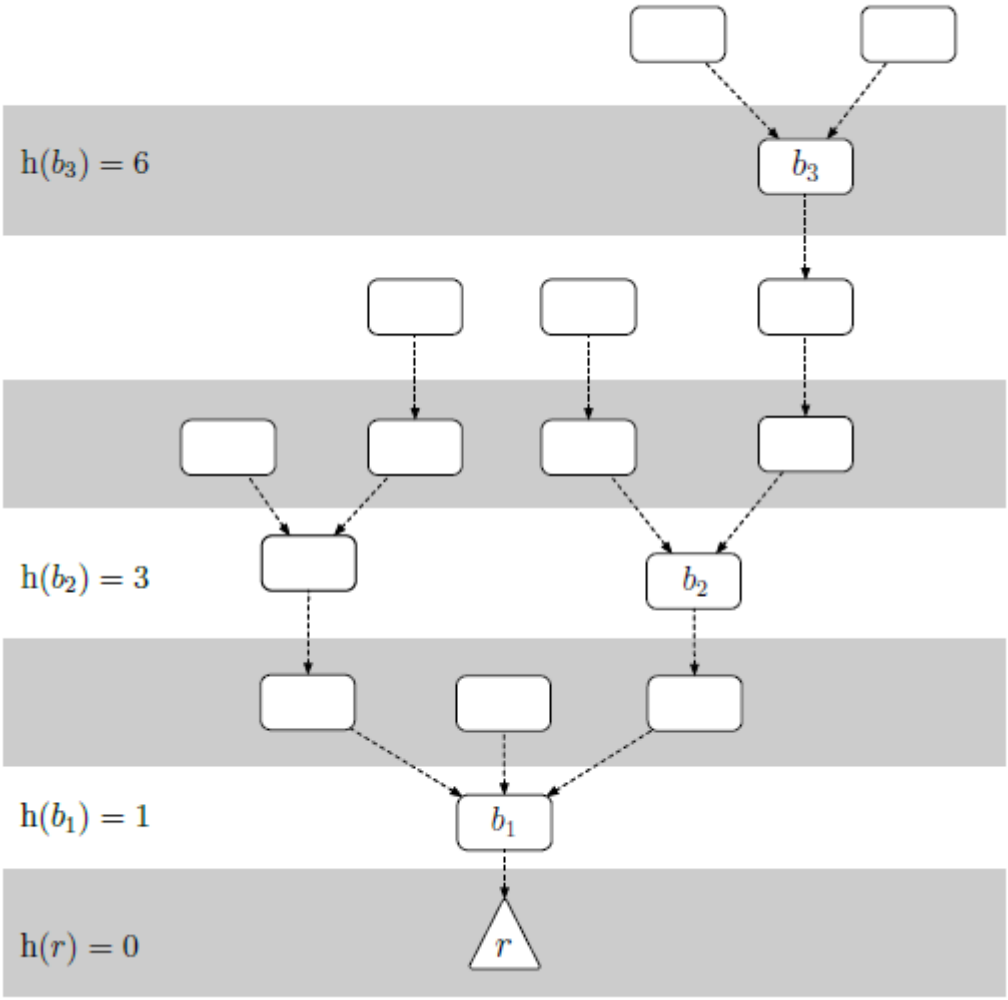
Kullanıcı onaylayıcı olduğu zaman açık anahtarı, onaylayıcı grubunda yayınlanır. Onay mesajı yollayan bir kullanıcının burada açık anahtarı bulunmuyorsa mesaj reddedilir.

Onaylayıcılar, yani blok işleyen kullanıcılar bir onay mesajı yayınlar. Bu çizelge 2.2.'deki ilk dört bilgiden oluşur. Eğer iki kontrol noktası arasında yayınlanmış birden fazla onay mesajı varsa veya aynı yükseklikte başka bir onay mesajı oluşturmuş ise protokol kullanıcıyı cezalandırır. Bu cezalandırma protokolüne "slasher" ismi verilmiştir.

Çizelge 2.2: Casper blok onaylama mesaj içeriği.

Değer	Açıklama
s	Kontrol noktası olan bir bloğun özet değeri.
t	s bloğundan sonra gelen bir kontrol noktası bloğunun özet değeri.
h(s)	s bloğunun zincirdeki yükseklik değeri.
h(t)	t bloğunun zincirdeki yükseklik değeri.
S	Onaylayıcının gizli anahtarı ile imzalanmış ⟨s; t; h(s); h(t)⟩ bilgileri.
V	Kullanıcının gizli anahtarı.

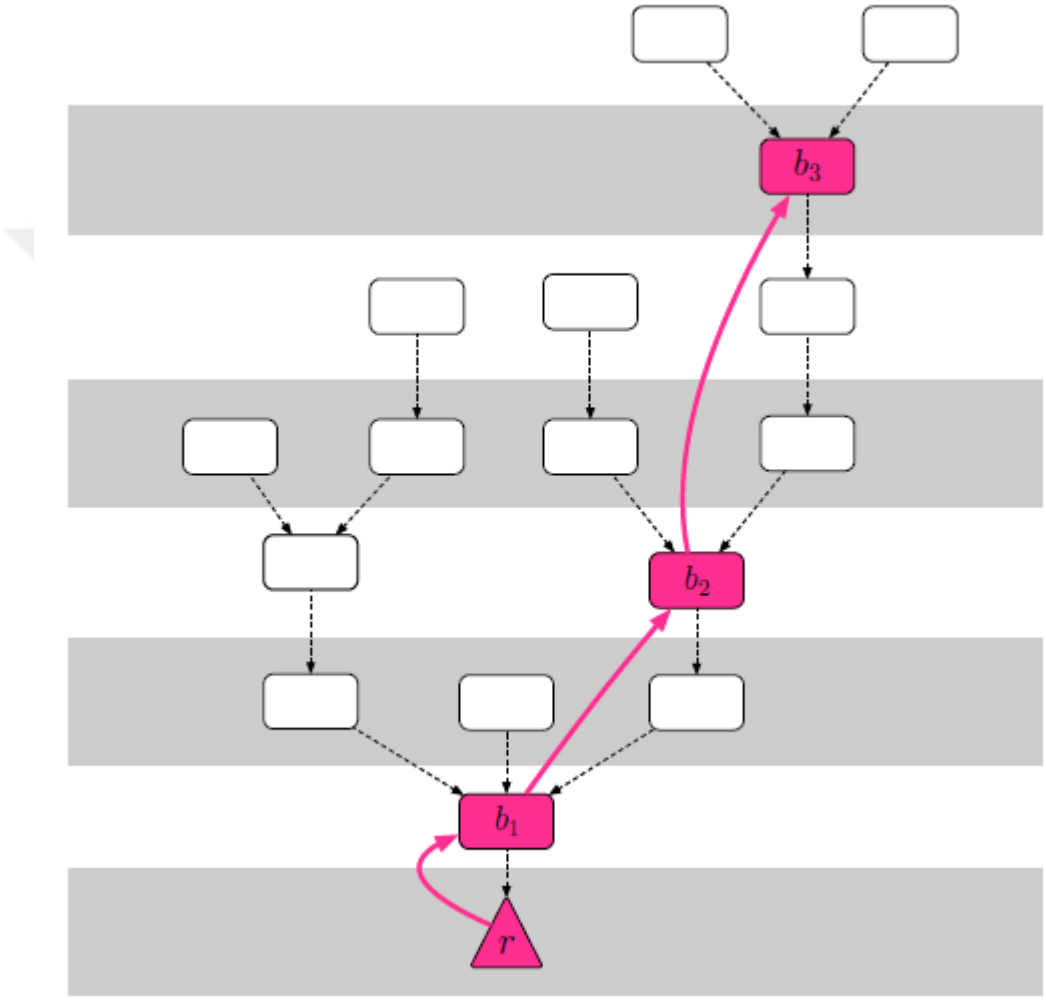
Blok yüksekliği hesaplaması şekil 2.3'de gösterilmiştir. Oluşturulacak bloğun yüksekliği 0 kabul edilir. Ondan önce gelen blok 1'den başlayarak geriye doğru gider.



Şekil 2.3: Blok yükseklik hesaplaması [35].

Bir kullanıcı Şekil 2.4'teki gibi r bloğunun eklenmesi için onay mesajı gönderebilir. Fakat zincirde çatallaşmaya neden olabilecek başka bir blok için aynı anda mesaj gönderemez. Bu durumlar aşağıda açıklanmıştır.

Onay veren kullanıcı, ⟨v; s1; t1; h(s1); h(t1)⟩ ve ⟨v; s2; t2; h(s2); h(t2)⟩ mesajlarını yayınlayabilir. Fakat aşağıda verilen koşullarda şu iki ayrı onay mesajını yayınlamamalıdır.



Şekil 2.4: Kontrol noktaları kontrolüne uygun eklenen blok örneği [35].

Formül 2.6'daki gibi yayınlarsa, aynı yükseklikte iki farklı mesaj yayınlamış olur. Bu protokol kurallarına aykırıdır. Kullanıcı cezalandırılır.

$$h(t_1) = h(t_2) \tag{2.6}$$

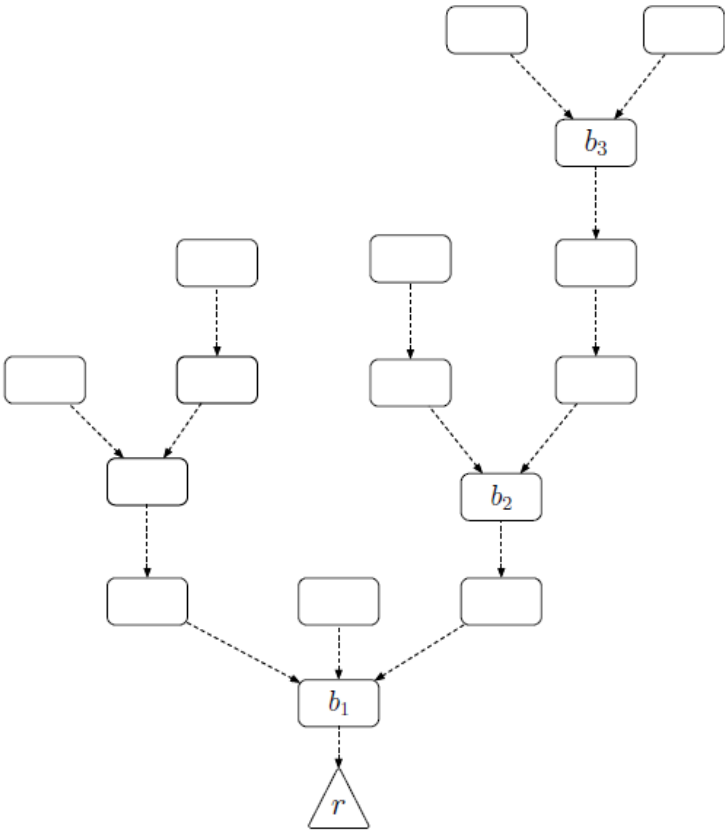
Formül 2.7'deki gibi yayınlarsa, aynı aralıkta ikinci bir onay mesajı yayınlamaya çalışmakta olduğu anlaşılır ve kullanıcı cezalandırılır.

$$h(s_1) < h(s_2) < h(t_2) < h(t_1) \tag{2.7}$$

İki durumda da depozito toplamları 2/3'e ulaşan kullanıcılar bu mesaja onay verse bile, kanıt olarak zincirde duracaktır. Kullanıcıların raporlamasıyla bu blok sonradan kaldırılabilir. Doğru raporlama yapan kullanıcılar ödüllendirilmektedir.

2.5.2 Kontrol Noktaları

Casper protokolü Peercoin ve Nxt'de olduğu gibi kontrol noktası sistemine sahiptir. Bu kontrol noktası sisteminde her 100'ün katı olan blok kontrol noktası olarak seçilmektedir.

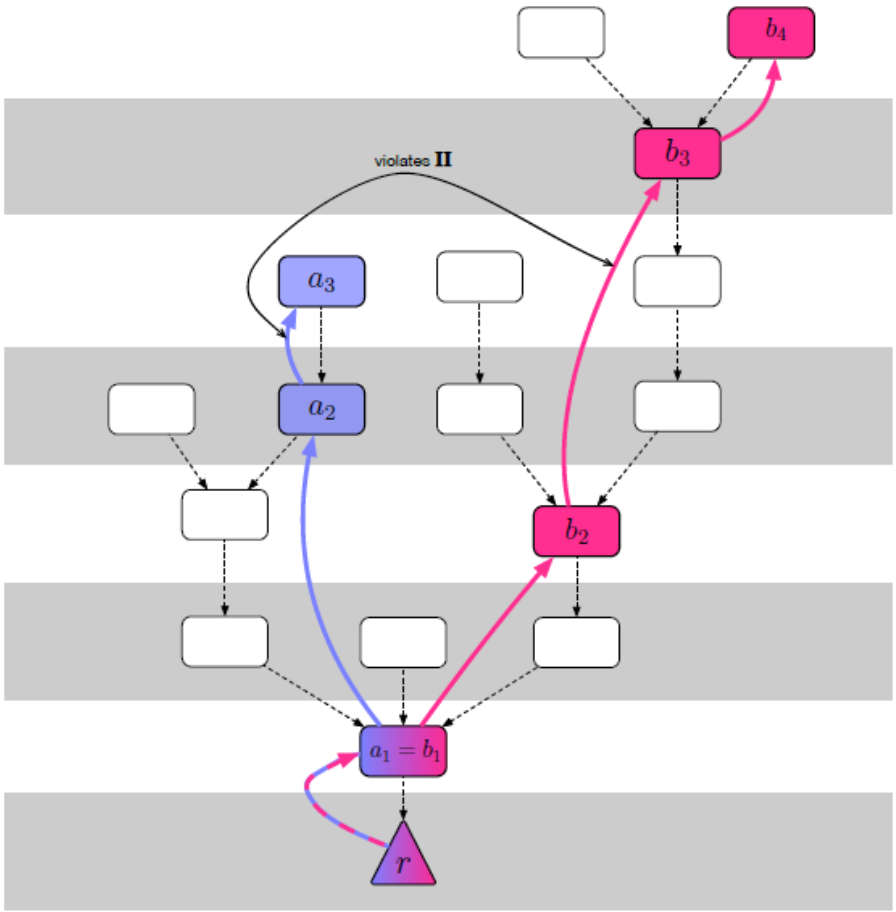


Şekil 2.5: Kontrol noktaları örneği [35].

Şekil 2.5'te kontrol noktaları örneklendirilmiştir. Noktalı olarak gösterilen çizgiler 100 bloğu temsil etmektedir.

Bir noktanın kontrol noktası olarak belirlenmesi yine onaylayıcıların görevidir. Bu sefer onay mesajı yerine hazırlık mesajı gönderirler. Yine depozito toplamı 2/3'e tekabül eden onaylayıcıların oyu belirleyici olmaktadır. Onaylayıcılar, aynı blok için kontrol noktası mesajı yolladıktan sonra, işleme mesajı gönderirler. Yine 2/3'ün oyundan sonra nokta kontrol noktası olarak belirlenir. Bu belirlemede, blok işleme kuralları geçerlidir. Yani yanlış oylarda slasher protokolü devreye girer.

Casper'ın iki önemli özelliği vardır. Bunları iki ayrı teorem olarak tanımlanabilir. Teorem 1, iki kesişen kontrol noktası varsa, ikisi de tanımlamaz. Şekil 2.6'da görüldüğü üzere iki kontrol noktası arasında sadece bir tane kontrol noktası olabilir. Şekildeki örnekte ise a3 veya a2 kontrol noktası olarak seçilemez, çünkü b2-b3 arasında sadece bir kontrol noktası olabilir.



Şekil 2.6: İki kontrol nokta arasında oluşan kontrol noktaları [35].

Eğer teorem 1'deki durum gerçekleşirse slasher protokolü devreye girer. Hatalı kontrol noktasını oylayan kullanıcılar cezalandırılır.

İkinci teorem ise başka bir çatalda daha yüksek bir kontrol noktasının tanımlanabilir olmasıdır. A bloğu en yüksek tanımlanmış kontrol noktasıdır. B ise belirlenmiş daha yüksek bir kontrol noktasıdır fakat tanımlanmamıştır. A' ve B' bu noktaların alt noktalarıdır. Eğer 2.8'deki denklem sağlanabiliyorsa, B noktası tanımlanabilir.

$$h(A') = h(B') + 1 \tag{2.8}$$

2.5.3 Ana Zincir Seçim Protokolü

Emek ispatı tabanlı sistemler her zaman en fazla iş yapılan zinciri ana zincir olarak seçmektedirler ve bunun için tüm kullanıcıların onayı gerekmemektedir. Casper için durum böyle değildir. Tüm onaylayıcıların ve kullanıcıların en uzun zincir için kurallara uyması gerekmektedir. Bu kurallardan en önemlisi en uzun zincir üzerine blok işlenmesidir. Buda kontrol noktaları aracılığıyla belirlenir. En yüksek kontrol noktasının olduğu zincir en uzun zincir kabul edilir. Bu kontrol noktasının tanımlanmış olması gerekmektedir. Fakat teorem 2'den hatırlanacağı üzerine bu nokta değişebilir.

2.5.4 Onaylayıcı Değişimi

Blok onaylayıcılarının belli aralıklarla değişmeleri gerekmektedir. Yeni onaylayıcılar katılmalı ve ayrılabilmelidirler. Bunu yapabilmek için blok soyu tanımlanmıştır. Bir bloğun blok soyu, o bloğa kadar tanımlanmış ve onaylanmış kontrol noktalarının sayısı kadardır. Onaylayıcı olmak isteyen bir kullanıcı, depozit olarak bir para ortaya koyması gerekmektedir. Bu depozit için oluşan bloktan, sonra tanımlanmış iki kontrol noktası sonrasında bu kullanıcı onaylayıcı grubuna dahil olur. Buna başlangıç soyu denir.

$$DS(v) = d + 2 \tag{2.9}$$

Formül 2.9'da v onaylayıcıdır, d; bloğun soyudur. DS(v) ise onaylayıcı olacak kullanıcın başlangıç soyudur.

$$DE(v) = d + 2 \tag{2.10}$$

Formül 2.10'da, 2.9 ile aynıdır. Bu sefer bu mesaj, onaylayıcı rolünden ayrılmak için oluşturulur. DE(v), kullanıcının onaylayıcı olmaktan ayrılacağı soy bilgisidir. Bir kullanıcı onaylayıcı olmaktan ayırılırsa, onaylayıcı grubundan açık anahtarı çıkarılır ve bir daha bu guruba dâhil olamaz.

$$\begin{aligned} \mathcal{V}_{\mathrm{f}}(d) &\equiv \{\nu : \mathrm{DS}(\nu) \leq d < \mathrm{DE}(\nu)\} \\ \mathcal{V}_{\mathrm{r}}(d) &\equiv \{\nu : \mathrm{DS}(\nu) < d \leq \mathrm{DE}(\nu)\} \end{aligned} \tag{2.11}$$

Formül 2.11'de iki onaylayıcı türü için küme oluşturulmuştur. İlk küme ileri (forward) onaylayıcılar, ikinci küme yakın (rear) onaylayıcılardır. Bu iki onaylayıcı kümesi sürekli yer değiştirerek, onaylayıcı kümesinin düzenli olarak değişmesini sağlar.

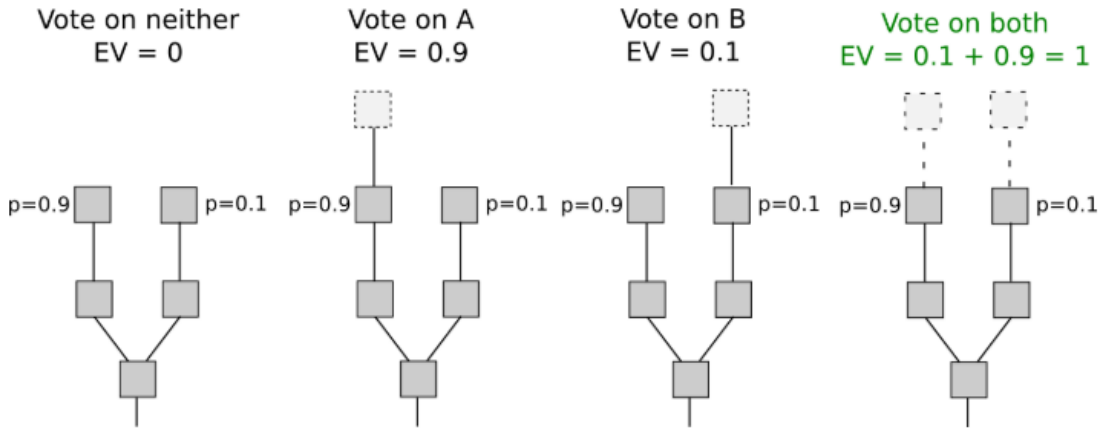
2.6 Problemler

Diğer kripto para uygulamalarında olduğu gibi hisse ispatı tabanlı sistemlerde de bazı problemlerin ve potansiyel saldırıların, teorik de olsa oluşmasına imkân vardır.
Bu problemlerin hisse ispatına özel olanı ise ortaya konan bir şey olmama (nothing at stake) problemidir. Bitcoin'de ve diğer kripto paralarda olan bir önemli problemde %51 problemidir ve bu problem hisse tabanlı sistemler için de geçerlidir.
Bu sistemlere yapılabilecek olası saldırılar da mevcuttur. DDoS, geçmiş saldırısı, uzun menzil saldırısıdır.

2.6.1 Ortaya Konan Bir Şey Olmama Problemi (NaS)

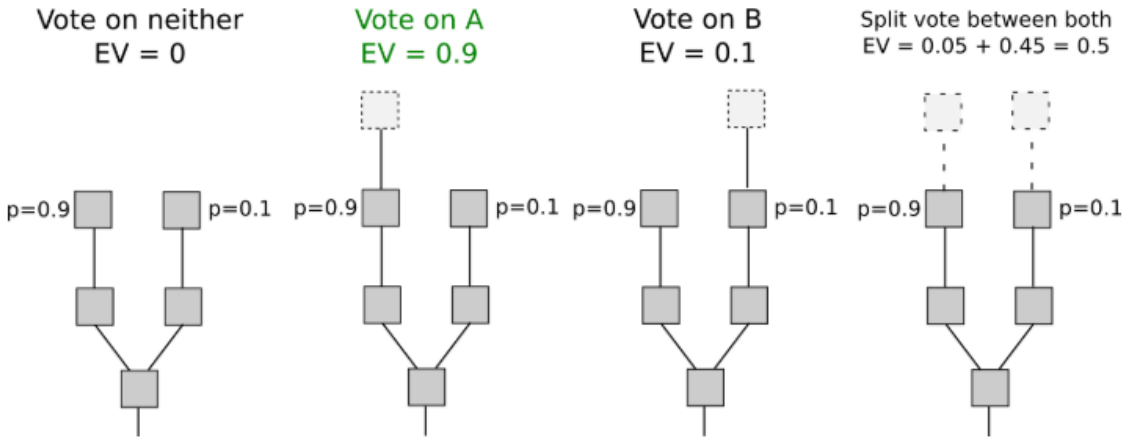
Bitcoin sistemimde tüm transferler açık olarak veri defterinde tutulmaktadır. Madenciler bu deftere veri eklemek için büyük bir enerji ve zaman harcamaktadırlar. Blok onayı madencilerin yaptıkları iş ile gerçekleşir. Zincirin çatallanması sonucu oluşan yeni zincire yeni blokların eklemek kullanıcılar için enerjilerini boşa harcamak olacaktır, çünkü sistem en çok iş yapılan zinciri seçeceği için kullanıcının çatala eklediği bloklardan ödül alamayacaktır ve yaptıkları iş boşa gidecektir. Fakat aynı durum hisse ispatı sistemleri için geçerli değildir. Onaylayıcıların harcadığı enerji, emek ispatı tabanlı sistemlere göre daha az olduğu için bunu her yeni transfer için yapabilirler çünkü kullanıcın ortaya koyduğu ve kaybedeceği bir şey yoktur. Bu

problem çifte harcama problemini tetiklemektedir. Aynı transfer, aynı hisse miktarı ile başka çatallara eklenebilir.



Şekil 2.7: PoS tabanlı sistemler için NaS problemi [36].

Şekil 2.7'da görüldüğü üzere PoS tabanlı sistemler için iki ayrı çataldaki blok için kullanıcı hissesini iki farklı blok için ayırabilir ve iki ayrı çatalda blok oluşturabilir ve ana zincir seçimi yapılmadan bu parayı iki zincirde de harcayabilir.



Şekil 2.8: PoW tabanlı sistemler için NaS problemi [36].

Emek ispatı sistemlerinde kullanıcı iki farklı bloğu işlemek istediğinde özet gücünü ikiye ayırması gerekmektedir. Buda blok işleme şansını azaltmaktadır.

2.6.2 51% Problemi

Emek ispatı tabanlı sistemlerde, tüm ağın özet gücünün %50'sinden fazlasına sahip belli bir grup kullanıcı, ana zinciri kendi oluşturdukları bir zincirle değiştirme gücüne de sahiptirler.

Gizli bir şekilde zincirin bir noktasından başlayarak blok işleyerek, kendilerine ait bir zincir oluşturabilirler. Ana zincirle olan yarışın sonunda %50'den daha fazla güce sahip oldukları için belli bir noktada esas zinciri geçeceklerdir. Bu zincir yayımlandığında, kullanıcılar en çok emek harcanan zinciri seçecekler ve bu zincir gizli olarak oluşturulan zincir olacaktır. Bu sırada esas zincirde kendi paralarını harcayabilecekler ve zincir değiştiğinde harcanan paralar esas zincirde kalacak. Yeni ana zincirde paraları harcanmamış olarak duracaktır.
Bu durum hisse ispatı sistemi içinde aynıdır. Burada özet gücü yerine, sistemdeki toplam hissenin %50'den fazlasının elde edilmesi gerekmektedir.

$$z_{i+1} = \begin{cases} z_i + 1 \text{ with probability p} \\ z_i - 1 \text{ with probability q} \end{cases} \tag{2.11}$$

Dürüst kullanıcıların blok oluşturma oranını p olduğunu varsayarsak, saldırganların blok oluşturma olasılığı q=1-p'dir. İki zincir arasındaki farka z diyelim. Eğer dürüst bir kullanıcı blok oluşturmak isterse z'yi 1 arttıracaktır. Saldırgan kullanıcı ise oluşturduğunda ise z 1 azalacaktır. Eğer q>p durumu oluşursa, saldırganın çoğunluğu ele geçirmiş demektir. Bu durumda z değeri azalarak sonsuza doğru gidecektir [38].

2.7 Olası Saldırılar

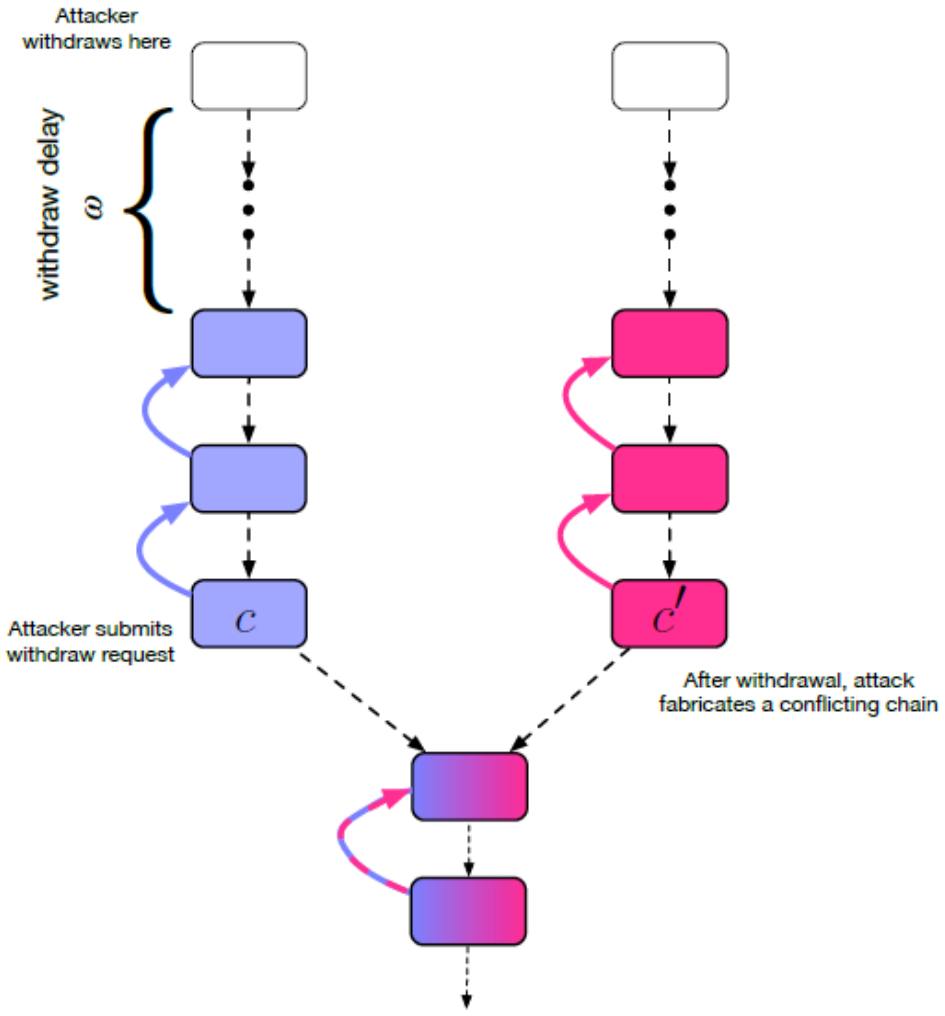
Bir PoS sistemine yapılabilecek saldırılardan bazıları DDoS, tarih saldırısı (history attack), uzun menzil saldırılarıdır (long range attack).

2.7.1 Geçmiş Saldırısı

Geçmiş saldırısında, kullanıcılardan biri, fazla miktarda para biriktirip, bunu transfer eder. Bunu sattığı sırada zincirde çatal oluşturmaya neden olacak başka bir blok oluşturmaya çalışır. Eğer başarılı bir şekilde zincirin çatallaşmasına sebep olup ve bu oluşan çatal ana zincir seçilip devam ederse, transfer ettiği paralar kendisine geri gelir. Eğer başarılı olamazsa ise parası karşılığında bir şey satın almış olur.

2.7.2 Uzun Menzil Saldırısı

Basit bir şekilde yazılmış hisse ispatı tabanlı uygulamada, ilk blok oluşumundan sonra sistemdeki tüm paranın %1'lik kısmına sahip olursa kendi zincirini işlemeye başlayabilir. %1'lik blok işleme olasılığı olsa da saldırgan, diğer kullanıcılardan 100 kat daha fazla blok işleyebilir ve en uzun zinciri oluşturabilir.



Şekil 2.9: Uzun menzil saldırısı. [36].

Bitcoin %51 probleminde, bir hesaba konulan 100BTC'yi transfer edip, onaylanmasını (6 blok sonra onaylanır) bekleriz. Bu bekleme sırasında başka bir hesaba, yine aynı parayı gönderebilir (çevrim dışı olarak). Tüm özet gücümüzü (>%51 bizde) bu bloğun olduğu zincire harcarsak. 2.6.2'de anlatıldığı gibi en uzun zinciri oluşturabiliriz ve ilk gönderdiğimiz paradan aldığımız değerlerde bizde kalır. Şekil 2.7'de görüldüğü üzere,

uzun menzil saldırılarında, onay sayısı öncesinden değil de daha geriden başlatabiliriz. Bu PoS sistemleri için kolay bir saldırı olabilir fakat Bitcoin için uzun zinciri yakalamak daha zordur. Kısacası bu bir %51 saldırısıdır, fakat daha geriden başlatılıp, yapılanıdır.

2.7.3 DDoS Saldırısı

Her web üzerinde olan ve dışarıdan istek alan uygulamalar gibi, kripto para uygulamaları da DDoS saldırılarına karşı açıktır. Blokzincir sistemlerinde, sistem tek bir noktadan kontrol edilmediği için, tek bir noktaya saldırı yapılamaz. Bu blokzincir sistemlerinin bu saldırıya karşı en büyük avantajıdır. Yani sistemin kullanılamaz hale getirme konusu imkânsıza yakındır.

IP adreslerine yapılabilecek saldırılar etkili olabilir. IP adresi bilinen bir kullanıcıyı ağdan düşürmek mümkündür. Blok işleyen bir kullanıcı ise blok işleyebilir fakat bunu ağa duyuramaz ve blok işleme hakkını kaybedebilir ve ödülü alamaz.

Blokzincir sistemine yapılabilecek diğer bir DDoS saldırısı ise, sürekli ağa bir veri aktarmaktır. Sürekli bir blok mesajı üretilip, ağa duyurulabilir. Bu mesajlar düğer kullanıcılar tarafından reddedilmelidir.

2.8 Ortak Model

Bir PoS tabanlı sistemin olması gereken önemli bileşenlerini, bu üç uygulamayı incelenerek belirlendi. Çizelge 3.1'de görüleceği üzere bir hisse ispatı tabanlı uygulama da olması gereken bileşenler çıkartılmıştır. Özetleme algoritması, blokları birbirine bağlaması için gereklidir. Eklenen blokların oluşturduğu zincirin bozulması durumunda ana zincir seçimini yapacak bir protokol önceden belirlenmiş olması gerekmektedir. Bu zincirdeki blok verilerinin tüm kullanıcılarda bulunması gerekmektedir ve bu veriler düzenli olarak güncellenmelidir. Blokları eklerken, hatalı blokların eklenmemesi için bir fikir birliği protokolü belirlenmelidir. Her blok birden fazla transfer bilgisini içerebilmelidir. Bu tutulan verilerin boyutunu azaltacaktır ve transferlerin onaylanmasını hızlandıracaktır. Bu blok işleme protokolü güncellenebilmelidir. Bu güncelleme, eski veri yapısını bozmamalıdır. Eski veriler yeni protokolde de kullanılabilmelidir. Dijital imza kullanılmalıdır. Hangi transfer, hangi kullanıcıya ait belirlenebilmelidir. Kullanıcılar protokol ihlallerinde cezalandırılmalıdırlar. Bu ceza sistemi, kullanıcıları daha dürüst olmaya zorlayacaktır.

Belli bloklar, kontrol noktası olarak belirlenmelidir. Hata durumunda, sistemin yanlış işlemeye zorlanması durumunda uygulamanın bu noktaya geri dönüp, buradan işlemlerine devam etmesi sağlanmalıdır.

Çizelge 2.3: Peercoin, Nxt ve Casper uygulamalarının bileşenleri.

Bileşen	**Açıklama**
Özetleme	Blok başlıkları ile yeni gelen blokları zincire bağlamak için gereklidir. Transfer yapılan blokların sırasını korur.
Zincir Seçimi Protokolü	Çatallaşma durumunda ana zincir seçimin yapılması gerekmektedir. Çifte harcamayı engellemek için zincir seçimi çok önemlidir.
Verilerin Dağıtık Olarak Tutulması	Verilerin dağıtık bir yapıda, tüm kullanıcılarda aynı şekilde tutulması çok önemlidir. Verilerin senkronizasyonu çevrim içi kullanıcılar için düzenli bir şekilde sağlanmalıdır.
Konsensüs Protokolü	Bir blok oluşumu için sistemin bir fikir birliğine varması gerekmektedir. Bu oluşan konsensüsün dürüst ve dürüst olmayan kullanıcılar tarafından birlikte doğru sonuca ulaştırmalıdır.
Özet Ağaçları	Bunlar birden fazla transfer bilgisini tek bir transfer bloğunda tutması için gereklidir. Daha az blok ile daha fazla transfer bilgisi tutulması önemlidir.
Protokol Güncelleme Mekanizması	Sistemi güncellemek istediğimizde uygulamanın üzerinde çalıştığı protokolü, eski verileri etkilemeden doğru bir şekilde yapılabilmesi önemlidir.
Dijital İmza	Hangi transferin kime ait olduğunu tespit edebilmemiz için dijital imza gereklidir.
Cezalandırma Protokolü	Hatalı davranan kullanıcıların, sistem içerisinde cezalandırılması ve uzaklaştırılması sistemin kullanıcılarını dürüst olmaya zorlayacaktır.
Kontrol Noktaları	Belli bloklar uygulama içerisinde kontrol noktası olarak belirlenmelidir. Herhangi bir hata durumunda uygulama bu noktadan tekrar devam edebilmelidir.

2.8.1 Sınıflandırma

Şekil 3.2'de analizi yapılan uygulamaların bir sınıflandırılması yapılmıştır. Bu sınıflandırma şu değerlere göre olmuştur;

- Özet algoritması; iki blok başlığını birbirine bağlayan algoritma.
- Transfer sistemi, uygulama bir para transfer sistemi midir?
- Para durumu; para miktarı uygulama içinde sürekli artmakta mıdır veya azalmakta mıdır ya da başlangıçtan itibaren sabit midir?
- Konsensüs algoritması; uygulamanın blok işlemek için kullanıcıların aralarında belirlediği protokol.
- Meta-data yapısı; Blokların zincirdeki bütünlüğünü sağlayan yapıdır.
- Ağa katılım; uygulamaya katılım izin gerektirmekte midir ya da herkese açık mıdır?
- P2P ağ modeli; P2P yapısı multilayer mı yoksa unilayer mıdır?
- Kaynak kod durumu; kaynak kodu gizli mi yoksa herkese açık mıdır?
- Kod dili; uzlaşma yapısını oluşturan dil hangisidir?
- Dijital imza; ECDSA mı yoksa RSA tabanlı mıdır?
- Token sahiplik modeli; hesap tabanlı mı yoksa transfer tabanlı mıdır?
- Para birimi; uygulamaların kullandığı para birimi nedir?

Bu sorular yanıtlanmıştır. Casper protokolü kullanan bir uygulama olmadığı için yanıtlanan bazı sorular Ethereum üzerinden cevaplanmıştır.

Çizelge 2.4 : Peercoin, Nxt ve Casper uygulamalarının sınıflandırılması.

Değer	**Peercoin**	**Nxt**	**Casper**
Özet Algoritması	SHA-256	SHA-256	Ethash
Para Transfer Sistemi	Evet		
Para Durumu	Artan	Sabit	Artan-Azalan
Konsensüs Algoritması	PoW-PoS	PoS	BFT-PoS
Meta-data yapısı	Merkle-Hash-Tree	Merkle-Hash-Tree	Merkle-Patricia-Tree
Ağ Katılım	Herkese açık, izin gerektirmiyor		
P2P Ağ Modeli	Unilayer		
Kaynak Kod Durumu	Herkese Açık		
Kod Dili	C++	Java	Solidity
Dijital İmza	ECDSA tabanlı		
Token Sahiplik Modeli	Hesap tabanlı	Hesap tabanlı	Hesap tabanlı
Para Birimi	PPC	NXT	ETH

3. ANALİZ VE KARŞIL"AŞTIRMA

3.1 Hisse Kullanımı

Üç protokolde, blok oluşturma için hisse ile ispat sistemini kullanmaktadır. Fakat hisseyi kullanım yöntemleri farklıdır. Peercoin para yaşına dayalı bir seçim sistemi kullanmaktadır. Bu sistemde para yaşı parametresi vardır. Bu değer kullanıcının parası zincirde durdukça artmaktadır. Para yaşı ve miktarını kullanarak, kullanıcılar kanıt bloğu oluştururlar. Bu blok kullanıcının hisse miktarı ve para yaşı bilgisinin kanıtıdır. Bu kanıt ile oluşan hedef değerinden daha düşük bir özet değeri bulmak zorundandır. Bu özet değerini bir önceki bloğun bilgilerini kullanarak bulunur. Her saniye için, koşul sağlanana kadar, bu hesap yapılır.

Nxt ise para yaşını parametre olarak kullanmaz. Kullanıcının geçerli para miktarına bağlıdır. Bu miktar, bir önceki bloğun hedef değeri ile bir önceki bloğun oluşma süresinden geçen süre (saniye bazında) ile bir özet hesaplanır.

Casper ise BFT tabanlı bir sistemdir. Casper'da Nxt gibi sadece hisse miktarını kullanır. Kullanıcı, blok onaylayıcısı olmak istiyorsa belli bir miktar, depozito olarak gösterir. Bu depozito kullanıcın, blok işlemek için kullanacağı hissesidir. Sistem, depozito miktarı ile hesaplanan özet değeri ile önceden belirlenen kontrol noktaları ile karşılaştırma yapar.

Üç protokolde hisse miktarını, blok işleme için kullanmaktadır. Hisse miktarının yüksek olması, kullanıcının bir sonraki bloğu işleme ihtimalini arttırmaktadır.

3.2 Kontrol Noktaları Kullanımı

Üç uygulamanın protokolü de kontrol noktası kullanmaktadır. Peercoin, günlük zinciri dondurup, buradan kontrol noktaları oluşturup, ağa duyurur. Bu duyuru tek bir

merkezden yapılmaktadır. Bunu yeni versiyonlarında, kullanıcılarına seçenek olarak sunmuştur.

Nxt'de kontrol noktası sistemini kullanmaktadır. Bu bilgi yayınlanmaz, bu belirlenmiş bir kuraldır. Her 721nci blok bir kontrol noktası sayılır. Herhangi bir hata durumunda, bu noktaya geri gelinebilir.

Casper'da kontrol noktaları, protokolün önemli bir parçasıdır. Diğerlerinde olduğu gibi aynı zincirin bütünlüğünü sağlamak için kullanılır. Fakat bu noktaların diğer bir önemli amacı, herhangi bir ihlal durumunda, ihlali yapan kullanıcıyı cezalandırma içindir.

Bu üç uygulama kontrol noktası kullanmaktadır. Casper'da kullanılan kontrol noktaları protokolün önemli bir kısmını oluşturmaktadır. Peercoin ise başlangıçta kullanılmıştır, sonrası için bunu kullanmaya gerek görülmemiştir. Nxt'de ise bir kullanıcın hissesini belirlemek için kullanılır. Nxt'de belli bir yüksekliği geçtikten sonra o nokta kontrol noktası sayılır ve o yükseklikten daha sonrasında olan bloklar işlenmiş sayılır.

3.3 Geçmiş ve Uzun Menzil Saldırıları

Geçmiş saldırısında, kullanıcılardan biri, fazla miktarda para biriktirip, bunu transfer eder. Bunu sattığı sırada zincirde çatal oluşturmaya neden olacak başka bir blok oluşturmaya çalışır. Eğer başarılı bir şekilde zincirin çatallaşmasına sebep olup ve bu oluşan çatal ana zincir seçilip devam ederse, transfer ettiği paralar kendisine geri gelir. Eğer başarılı olamazsa ise parası karşılığında bir şey satın almış olur. Uzun menzil saldırısı ise bunun daha geriden yapılanıdır.

Bu üç protokol bu problemleri kontrol noktaları sayesinde çözmektedir. Nxt'de hisseler, blok işlemek için, 1440 blok sonrasında kullanılabilir. Çok büyük bir hisseye sahip bir kullanıcı için bu bir sorun olmayabilir. Bu yüzden Nxt'de bir blok 720 blok sonrasında işlenmiş kabul edilir.

Casper'da kontrol noktalarını kullanmaktadır. Bu protokolünün önemli bir parçasıdır. Yüksekliği 100'ün katı olan her blok bir kontrol noktasıdır. Slasher protokolü zincirin

bütünlüğünü kontrol eder. Eğer iki kontrol noktası arasında, bir kullanıcı iki farklı zincirde blok oluşturmaya çalışırsa, kullanıcıyı cezalandırır.

Peercoin'de bu sorunu aynı şekilde çözmektedir. Günlük olarak kontrol noktalarını paylaşmaktadır. Fakat bu kontrol noktası kontrolü, şu an için kullanıcının tercihine bırakılmıştır ve daha sonrası için terk edilecektir.

Aslında bu problem, hisse tabanlı bir sistemin, ilk kullanıma açıldığı zaman için geçerlidir. İlk kullanıcıların, sistemde belli bir paraya (%1) sahip olarak, diğerlerinden daha fazla oranda bir hisse miktarına sahip olabilirler. Bu da zincirin bütünlüğünü etkileyecek saldırılara neden olabilir. Zincirde çatallaşmaya neden olup, çifte harcama yapabilirler. Fakat sistem olgunlaştığında, hisseler belli bir oranda kullanıcılara dağıldığında böyle bir sorunun oluşma ihtimali oldukça düşüktür.

3.4 Ortaya Konan Bir Şey Olamama Sorunu

Üç uygulamada bu sorunu kullanıcıyı cezalandırarak çözmektedir. Kullanıcının herhangi bir kural ihlalinde sistem dışına itilmesi veya maddi olarak cezalandırılır. Fakat bu problem, bu protokollerin işleyiş biçimlerinden dolayı olası bir problemdir ve protokoller temel olarak bu soruna çözüm olarak çıkmışlardır. Yani bu problem aslında teknik ve ekonomik nedenlerle gerçekleşme olasılığı çok düşüktür.

Bu problemin ortaya çıkabilmesi için bazı koşulların sağlanması gerekmektedir;

- Blok işleyicisinin, her blok işleme fırsatını değerlendirmesi gerekmektedir. Yani blok işleyen kişi bundan kazanç sağlamalı.
- Hiçbir blok işleyicisinin tek bir zincir üzerinde çalışmaması gerekmektedir.
- Ana zincir seçimi yapan protokolün doğru çalışmaması gerekmektedir.

Bu üç şart sağlanırsa bu problemin oluşma ihtimali yüksektir.

Bu problemin gerçekleşmesi için blok işleyicilerinin her çatallaşmada oluşan blokları işlememesi için herhangi bir engel olmamasıdır. Bundan dolayı, hiçbir zaman fikir

birliğine varılamaması ve birden fazla geçerli olabilecek zincirlerin oluşmasına neden olacaktır.

Hisse ispatı tabanlı sistemlerin en önemli problemlerinden biri ortaya konan hiçbir şey olamam problemidir. Bu problemde saldırgan her gelen transferi, hissesi ile onaylamaya çalışır. Bunu yapmakla kullanıcı hiçbir şey kaybetmez. Bu teorik problemi engellenmesi için üç protokolde kural ihlali yapan kullanıcıyı cezalandırır.

Bu üç cezalandırma yöntemi birbirinden farklıdır. Peercoin para yaşı modelini kullanmaktadır. Bu modelde aynı hisse ile başka blokları onaylamaya çalışan kullanıcı para yaşını kaybeder. Eğer onaylanan blok, ana zincirde değilse ödülü de alamaz.

Nxt kullanıcıları da bu kural ihlalinde ödül alamaz. Nxt'in geliştirmekte olduğu ekonomik kümelenme modelinde, kullanıcı kural ihlalinde kümeden çıkarılır. Bunu kullanıcının onay yetkisini alarak yapmayı planlıyorlar.

Casper ise kullanıcılarını, kural ihlalinde para cezası ile cezalandırır. Kullanıcı onaylayıcı olmak için depozito olarak verdiği paraların hepsini kaybeder.

Üç protokolde de olan ve bu probleme karşı bir diğer koruma da bunun için belli bir hisseye sahip olunmasıdır. Burada kullanıcı hissesini bu saldırı için biriktirmek ve bunu saldırı için kullanmak zorundadır. Üç protokolde, burada kullanıcıyı bu süre içeresinde hissesine erişemez durumda bırakır. Aynı bilgilere transfer bloklarının, üç sistemde de sonradan gelenler, sistem tarafından reddedilir

Bir diğer versiyonu ise kullanıcıların, blokları oluşan her zincir üzerinde işlemesidir, çünkü bunu yaparken hiçbir şey kaybedilmeyeceği düşünülmemektedir. Bu aslında doğru değildir. Burada tüm kullanıcıların kaybedeceği bir durum vardır. Bu yüzden, kullanıcılar, hisselerinin ana zincirden ayrılmamasını isteyecektir. Başka bir zincir, ana zincir olarak kabul edildiğinde kullanıcıların burada yaptıkları transferler kaybolacaktır. Yani aslında kaybedecek bir şey vardır.

Başka bir versiyon ise aynı blokların sürekli işlenmesidir. Bu başka bir kaotik duruma yol açacaktır. Bu durum sisteme olan güvenin kaybolmasına neden olacaktır. Bu durum büyük bir değer kaybına yol açacaktır. Bu blokları işleyerek kazanılan ödülü değersiz yapacaktır.

Hisse olarak kullanılan paralar, belli bir süre harcanamaz. Bundan dolayı paranın değişim oranındaki düşüş, hisse sahipleri için büyük zarara yol açacaktır. Yani yüksek hisselere sahip kullanıcıların, bu problemi kullanarak kar etmeyi tercih etme ihtimalleri düşüktür. Sonuç olarak bu problemin gerçekleşme ihtimali hisse ispatı tabanlı sistemler için düşüktür.

3.5 Gelir Dağılımı

Nxt'de 1,000,000,000 para 73 kullanıcıya dağıtılmıştır. Enflasyon değerini sabit tutmak için sadece transfer ücreti ile blok oluşturma işlemi desteklenir. Blok oluşturma ödülü 2 NXT'tir. Yani para başlangıçta belli kullanıcılara dağıtılmış, sonrasında takas ile para satımı yapılmıştır. Şekil 3.1'de görüldüğü üzere en büyük oran, %32,56 ile NXT-MT4P-AHG4-A4NA-CCMM2 hesabına aittir. Bu oran çok yüksektir ve bu istenen bir durum değildir.

Nxt uygulama monitörü izlendiğinde görülecektir, blok onaylayıcıları genellikle bu kullanıcılar arasında olmaktadır. Hisse büyüklükleri çok fazla oldukları için bu durumu değiştirmek baya zordur. Buradaki yaklaşım, rassal bir seçim modeline sahip olmasından kaynaklanmaktadır. Burada bir onaylayıcının, bir bloğu onaylayacağı kesin değildir [45]. Blok işleme protokolü 2.4.2'de anlatılmaktadır.

Next Block Generators

	Account	Stake (NXT)	% of 10k blocks
1	NXT-8MVA-XCVR-3JC9-2C7C3	50'008'927	30.71
2	NXT-MT4P-AHG4-A4NA-CCMM2	46'000'999	32.56
3	NXT-QA7E-SZJK-CUY7-97FUF	2'084'385	1.18
4	NXT-4RU9-TNCT-F3MU-8952K	30'331'875	19.32
5	NXT-URPK-4YBK-FCTH-2SFDW	1'001'076	0.64
6	NXT-RH5T-CKRV-LLPZ-C4ENV	500'592	8.43
7	NXT-VEKZ-64ZB-L2SX-DXYYD	500'482	0.27
8	NXT-ZCLD-5TVW-HHAN-FVEJC	850'294	0.35
9	NXT-6EGF-8342-45S6-2LAW4	1'709'574	0.30
10	NXT-M98B-95WS-F4AX-FL7ES	1'001'008	0.46

Şekil 3.1: Nxt blok işleyicileri [42].

Fakat durum Peercoin'de daha iyidir. Şekil 3.2'de görüldüğü üzere en büyük hesap hisselerin %7'sine sahiptir. Nxt'e göre daha dengeli bir dağılım söz konusudur. Bunun nedeni ise kullanılan protokolden kaynaklanmaktadır. Peercoin para yaşını kullandığı için bu tablo oluşmuştur. 2.3.2'de anlatılan protokolde, kullanıcı bir blok işlediğinde, biriktirdiği tüm para yaşını kaybeder, bu yüzden blok işleyicileri arasındaki dağılım daha düzenli olmaktadır. Bu yüzden bu tablonun oluştuğunu söyleyebiliriz.

Richest Addresses

Top 1000

Rank	Address	Amount	Percent of coins	Last Change
1	PN9ZrKwP...	1,789,938.08 PPC	7.01 %	2 days 19 hours
2	PR5KAV1a...	1,786,301.07 PPC	6.99 %	1 year 19 days
3	PR7KHMEK... BITTREX	964,794.00 PPC	3.78 %	9 days 6 hours
4	PMz8MpKF...	568,166.66 PPC	2.22 %	148 days 21 hours
5	P8tx5ggf...	553,009.76 PPC	2.16 %	3 years 349 days
6	P94Tjs2P...	515,648.00 PPC	2.02 %	49 days 22 hours
7	PLYhzmRJ...	456,000.00 PPC	1.78 %	6 days 1 hour
8	PJsyc7dW...	365,479.97 PPC	1.43 %	3 hours 16 minutes
9	PMQjBNMd...	312,682.29 PPC	1.22 %	1 year 223 days
10	P9WAwyxZ...	307,606.85 PPC	1.20 %	345 days 3 minutes

Şekil 3.2: En fazla hissye sahip olan 10 Peercoin hesabı [43].

Şekil 3.3'te görüldüğü üzere, Ethereum için durum daha da iyidir. Çünkü hisseler daha dengeli dağıtılmıştır. Fakat Ethereum'un şu anki versiyonu Casper protokolünü kullanmadığı hisse ispatı için bir analiz yapılamamaktadır. Fakat Casper'ı kullanmaya başlarsa onaylayıcı seçimi daha dengeli olacaktır.

Rank	Address	Name Tag	Balance	Percentage	Txn Count
1	0x742d35cc6634c0532925a3b844bc454e4438f44e	Bitfinex 5	1,731,125.76522553 Ether	1.61510034%	5,046
2	0xc02aaa39b223fe8d0a0e5c4f27ead9083c756cc2	Wrapped Ether	1,684,036.47236218 Ether	1.57116712%	416,661
3	0xbe0eb53f46cd790cd13851d5eff43d12404d33e8	Binance 7	1,656,546.76254243 Ether	1.54551985%	42
4	0x53d284357ec70ce289d6d64134dfac8e511c8a3d	Kraken 6	1,378,754.14306818 Ether	1.28634576%	14,995
5	0x66f820a414680b5bcda5eeca5dea238543f42054	Bittrex 3	1,300,001.58257192 Ether	1.21287144%	38
6	0xab7c74abc0c4d48d1bdad5dcb26153fc8780f83e		999,999.01246312 Ether	0.93297597%	459
7	0xdc76cd25977e0a5ae17155770273ad58648900d3	Huobi 6	850,860.64196888 Ether	0.79383332%	140
8	0x61edcdf5bb737adffe5043706e7c5bb1f1a56eea	Gemini 3	820,999.00001 Ether	0.76597310%	157
9	0xe853c56864a2ebe4576a807d26fdc4a0ada51919	Kraken 3	801,052.79995972 Ether	0.74736375%	151
10	0xfca70e67b3f93f679992cd36323eeb5a5370c8e4		791,999.89069608 Ether	0.73891760%	56

Şekil 3.3: En fazla hissye sahip olan 10 Ethereum hesabı [44].

Hisse ispatı tabanlı sistemlerde olası başka bir problem ise zenginin daha da zengin olmasıdır. Daha az parayla başlayan bir kullanıcı, daha fazla paraya sahip kullanıcılara karşı blok işleme konusunda dezavantajlı durumdadır. Fakat bu durum tam anlamıyla doğru değildir. Sistemler bu duruma karşı önlemini almışlardır. Peercoin para yaşını kullanarak bu sorunu çözmüştür. Nxt bu durumu tam olarak çözülememiştir. Rassal onaylayıcı seçiminde, hisse miktarı, belli kullanıcılarda arttıkça, rassallık tam olarak sağlanamamıştır. Casper için ise onaylayıcı protokolü 2.5.4'te anlatılmıştır. Fakat protokol uygulanmadığı için şu an için, veriler üzerinden bir analiz yapılamamaktadır.

3.6 Hibrit Yapı

Casper ve Peercoin, hibrit bir yapıda çalışmaktadır. Fakat Nxt'in blok işleme protokolünde herhangi bir yardımcı protokol içermemektedir. Üç protokolde hisse ispatını kullanmaktadır. Üç uygulamanın bu protokolü kullanma nedeni aynıdır. Daha az enerji tüketimi ve fikir birliğinin hızlı sağlanmasındandır.

Peercoin emek ispatı kullanmaktadır. Hisse ispatı ile kanıt bloğunu oluşturur. Bu blok üzerinden transfer bloklarını işlemeye çalışır. Bu yüzden blok işleme hızı, bir emek ispatı algoritması için yavaştır. Bir bloğun ortalama oluşma süresi 7-8 dakika arasıdır [46]. Peercoin, yeni versiyonu için emek ispatı yapısını kaldırmayı düşünmektedir.

Bunu kaldırmak doğru bir seçimdir, çünkü hisse ispatının kullanılmasının amacı emek ispatındaki enerji tüketimi ortadan kaldırmaktı.

Emek ispatının uygulamada kullanılma nedeni ise o zaman, blok işleme ve para üretme için en geçerli çözümün emek ispatı olmasıydı. Fakat şu an için bunun bir kazancı yoktur ve para basımı için donanım kullanmak, kullanıcıyı teşvik etmemektedir.

Casper ise Bizans hata toleransı kullanarak fikir birliği oluşturmaktadır. Bu sistemde kullanıcıların bir kısmının (2/3'ünden fazlasının) aynı kararı vermesi gerekmektedir. Doğru bir fikir birliğine varılabilmesi için kullanıcıların 2/3'ünün dürüst davranması gerekmektedir. Ethereum bu sistemi, kendi emek ispatı tabanlı sistemlerinin üzerine entegre olacak şekilde tasarlamaktadır, henüz uygulamaya geçmemiştir. Casper zaten kullanılan ve kullanıcı sayısı yüksek olan bir sisteme entegre edilecektir. Fakat Casper protokolü için, yeni bir uygulamaya entegre ettiğimizde büyük sorunlara yol açabilir. İlk kullanıcıların sayısı az olduğu için 2/3 daha kolay sağlanabilir. Bu da zincirin bütünlüğünü ve sistemin işleyişini değiştirmek için yeterlidir. Casper bunun için bir çözüm sunmamıştır. Nxt ise %100 bir hisse ispatı tabanlı sistemdir.

3.7 Onaylayıcıların Değişimi

Onaylayıcı ve blok işleyicilerinin değişimi sistemin merkezi olmayan yapısını koruması için önemlidir. Üç uygulamada bu probleme çözüm sunmaktadır.

Peercoin'de kullanıcılar bir blok işlediklerinde, para yaşını harcamış olurlar. Bu kullanıcın tekrar para yaşı biriktirmesi gerekmektedir. Bundan dolayı, para yaşını biriktirmiş başka kullanıcılarda blok işleme şansı bulurlar.

Casper'da onaylayıcı değişimi için bir protokol tanımlanmıştır. Çünkü Casper'da onaylayıcı seçiminde bu olay Nxt ve Peercoin'deki gibi para miktarına bağlı olarak değişmez. Bir kullanıcı onaylayıcı olmak istiyorsa bunu depozito olarak gösterdiği para ile bildirir ve bir sonraki onaylayıcı grubuna dahil olur. Sonrasında tekrar bir depozito bildirerek, sonraki guruba dahil olabilir. Bu protokol 2.5.4'te açıklanmıştır.

Nxt'de ise durum biraz kötüdür. Onaylayıcı grubu para miktarına bağlı olarak değişir. Şekil 3.2'de görüleceği üzere Nxt'de bazı kullanıcılar, para miktarının büyük bir kısmını ele geçirmiştir. Bu grup çok fazla değişmemektedir. Bunun için bu

kullanıcıların paralarını harcamaları gerekmektedir. Burada rassal seçim yöntemi yeterli değildir.

5. SONUÇ

Emek ispatı tabanlı sistemler, çok fazla enerji harcadıklarından dolayı uzun ömürlü sistemler değildirler, çünkü bu enerji tüketimi, sistemin güvenliği ile doğrudan bağlantılıdır. Kripto para sistemlerinde güvenlik-enerji tüketim durumunu ortadan kaldırmak için 2012 yılında yeni bir çözüm sunuldu. Bu çözüm Bitcoin forumlarında 2011 yılında tartışılmıştı. Emek ispatı protokolü yerine sunulan bu protokolün adı hisse ispatıdır (PoS). Sunny King ve Scott Nadal tarafından oluşturulmuştur ve adı Peercoin'dir. Bu protokolde, sistem kullanıcıların zincirdeki hisselerine bağlıdır. Kullanıcı ne kadar çok paraya sahipse o kadar çok blok işleme şansına sahiptir. Emek ispatı tabanlı sistemlerdeki gibi işlem gücüne sahip olmalarına gerek yoktur. Bu yüzden enerji tüketimi daha azdır. Bu tezde hisse ispatına ait

Karşılaştırma ve analiz, Peercoin, Nxt ve Ethereum'un Casper protokolleri üzerinden yapıldı. Bu kripto paraların seçilme nedeni, fikir birliği algoritmalarının temelde aynı prensipler üzerine kurulu olup, hisse ispatı protokolünü farklı işlemeleriydi. Bu sistemlerin blok, zincir, ağ, sisteme katılım, madencilik, ceza sistemleri ve fikir birliği algoritmaları üzerinden detaylı teknik analizi yapıldı. Sistemler nicel özellikleri ortaya konuldu ve bunları kaynak kodları, geliştirici dokümantasyonları ve yazılan makaleler ile pekiştirildi. Daha sonrasında, bu sistemleri oluşturan parçalar ve aralarındaki ilişkiler çıkarıldı. Bulunan bu parçaların kritik noktaları, zayıf ve güçlü tarafları analiz edilip tartışıldı.

Bir PoS tabanlı sistemin olması gereken önemli bileşenlerini, bu üç uygulamayı incelenerek belirlendi. Bir hisse ispatı tabanlı uygulama da olması gereken bileşenler çıkartılmıştır. Özetleme algoritması, blokları birbirine bağlaması için gereklidir. Eklenen blokların oluşturduğu zincirin bozulması durumunda ana zincir seçimini yapacak bir protokol önceden belirlenmiş olması gerekmektedir. Bu zincirdeki blok verilerinin tüm kullanıcılarda bulunması gerekmektedir ve bu veriler düzenli olarak güncellenmelidir. Blokları eklerken, hatalı blokların eklenmemesi için bir fikir birliği protokolü belirlenmelidir.

Her blok birden fazla transfer bilgisini içerebilmelidir. Bu tutulan verilerin boyutunu azaltacaktır ve transferlerin onaylanmasını hızlandıracaktır. Bu blok işleme protokolü güncellenebilmelidir.

Bu güncelleme, eski veri yapısını bozmamalıdır. Eski veriler yeni protokolde de kullanılabilmelidir. Dijital imza kullanılmalıdır. Hangi transfer, hangi kullanıcıya ait belirlenebilmelidir. Kullanıcılar protokol ihlallerinde cezalandırılmalıdırlar. Bu ceza sistemi, kullanıcıları daha dürüst olmaya zorlayacaktır. Belli bloklar, kontrol noktası olarak belirlenmelidir. Hata durumunda, sistemin yanlış işlemeye zorlanması durumunda uygulamanın bu noktaya geri dönüp, buradan işlemlerine devam etmesi sağlanmalıdır.

Üç uygulamayı incelediğimizde, üç uygulamanın da kendine has hisse ispatı çözümleri olduğunu görmekteyiz. Peercoin hisse ispatını emek ispatı protokolü ile birlikte kullanmaktadır. Casper BFT ile birllikte kullanırken, Nxt ikinci bir protokol kullanmaz. Üç protokolde hisse miktarını, blok işleme için kullanmaktadır. Hisse miktarının yüksek olması, kullanıcının bir sonraki bloğu işleme ihtimalini arttırmaktadır.

Bu üç uygulama kontrol noktası kullanmaktadır. Casper'da kullanılan kontrol noktaları protokolün önemli bir kısmını oluşturmaktadır. Peercoin ise başlangıçta kullanılmıştır, sonrası için bunu kullanmaya gerek görülmemiştir. Nxt'de ise bir kullanıcın hissesini belirlemek için kullanılır. Nxt'de belli bir yüksekliği geçtikten sonra o nokta kontrol noktası sayılır ve o yükseklikten daha sonrasında olan bloklar işlenmiş sayılır.

Hisse ispatının temel problemlerinden biri olan NaS'a yaklaşımı üç protokolünde farklı da olsa temelde kullanıcıyı cezalandırmaya yöneliktir. Üç protokolde de olan ve bu probleme karşı bir diğer koruma da bunun için belli bir hisseye sahip olunmasıdır. Burada kullanıcı hissesini bu saldırı için biriktirmek ve bunu saldırı için kullanmak zorundadır. Üç protokolde, burada kullanıcıyı bu süre içeresinde hissesine erişemez durumda bırakır. Aynı bilgilere transfer bloklarının, üç sistemde de sonradan gelenler, sistem tarafından reddedilir

Sistemler geçmiş ve uzun menzil saldırılarına açıktır. Aslında bu problem, hisse tabanlı bir sistemin, ilk kullanıma açıldığı zaman için geçerlidir. İlk kullanıcıların, sistemde belli bir paraya (%1) sahip olarak, diğerlerinden daha fazla oranda bir hisse miktarına sahip olabilirler.

Bu da zincirin bütünlüğünü etkileyecek saldırılara neden olabilir. Zincirde çatallaşmaya neden olup, çifte harcama yapabilirler. Fakat sistem olgunlaştığında, hisseler belli bir oranda kullanıcılara dağıldığında böyle bir sorunun oluşma ihtimali oldukça düşüktür. Bu iç sistem içinde böyledir.

Hisse ispatı tabanlı sistemlerin emek ispatından kurtulmaları istenilen sistemdir. Ethereum Casper ile bu sisteme geçip, daha sonradan emek ispatından kurtulmak istemektedir. Nxt bunu başarmıştır. Peercoin'de bu şu an için yapılabilir durumdadır.

KAYNAKLAR

[1] **Mankiw, N G.** Principles of macroeconomics. Mason, OH: South-Western Cengage Learning, 2012. Print.

[2] **Szabo, N.**, (2001) Trusted Third Parties Are Security Holes, Retrieved June 10, 2019, https://nakamotoinstitute.org/trusted-third-parties

[3] **Nakamoto, S.**, (2008) Bitcoin: A peer-to-peer electronic cash system, Retrieved in May 21, 2019, https://bitcoin.org/bitcoin.pdf

[4] **O. Karame, E. Androulaki, and S. Capkun**, Double-spending fast payments in bitcoin, (2012) ACM conference on Computer and communications security - CCS '12, 2012.

[5] **W. Dai**, (1998) b-money, http://www.weidai.com/bmoney.txt

[6] **Nakamoto, S.**, (2002) Bitcoin: A peer-to-peer electronic cash system, Retrieved in May 21, 2019, http://www.hashcash.org/hashcash.pdf

[7] **H. Nicolas**, (2014) The Economics of Bitcoin Transaction Fees, SSRN Electronic Journal, 2014.

[8] **A. de Vries**, (2018) Bitcoin's Growing Energy Problem, Joule, vol. 2, no. 5, pp. 801–805, May 2018.

[9] Bitcoin Block Reward Halving Countdown, Retrieved in July 21, 2019, https://www.bitcoinblockhalf.com/

[10] **M. Carlsten, H. Kalodner, S. M. Weinberg, and A. Narayanan,** On the Instability of Bitcoin Without the Block Reward, (2016) ACM SIGSAC Conference on Computer and Communications Security - CCS'16, 2016.

[11] **Okupski, K**., (2014) Bitcoin Developer Reference, Retrieved in July 20, 2019, https://bitcoin.org/en/developer-reference,

[13] **Merkle, R. C.**, (1987) A digital signature based on a conventional encryption function, In: Advances in Cryptology—CRYPTO'87. Springer Berlin Heidelberg, 369-378. 1987.

[14] **Merkle, R. C.**, (1982) Method of providing digital signatures U.S. Patent No.4,309,569, 5 Jan. 1982.

[15] Bitcoin Hash Rate vs Difficulty, Retrieved in July 24, 2019, https://bitcoinwisdom.com/bitcoin/difficulty

[16] **U. Mukhopadhyay, A. Skjellum, O. Hambolu, J. Oakley, L. Yu, and R. Brooks**, (2016) A brief survey of Cryptocurrency systems,14th Annual Conference on Privacy, Security and Trust (PST), 2016.

[17] **I. Eyal and E. G. Sirer**, (2018) Majority is not enough, Communications of the ACM, vol. 61, no. 7, pp. 95–102, Jun. 2018.

[18] **Bastiaan, Martijn**, (2015) Preventing the 51%-attack: a stochastic analysis of two phase proof of work in bitcoin Retrieved in July 24, 2019, http://fmttools.ewi.utwente.nl/files/sprojects/268.pdf . 2015.

[19] **King, S., & Nadal, S.**, (2012) Ppcoin: Peer-to-peer crypto-currency with proof-of stake, self-published paper, 19 August 2012.

[20] Bitcointalk, Proof of stake instead of proof of work, Retrieved in July 24, 2019, https://bitcointalk.org/index.php?topic=27787.0

[21] **K.J. O'Dwyer, D. Malone.** (2014) Bitcoin Mining and its Energy Footprint. China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014), 2014, p. 280-285.

[22**] Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder**, **S.** (2016) Bitcoin and CryptocurrencyTechnologies.

[23] **Driscoll, S.,** (2013) How Bitcoin Works Under the Hood. Retrieved in 21 July, 2019, http://www.imponderablethings.com/2013/07/how-bitcoin-works- under-hood.html

[24] Whitepaper:Nxt. Retrieved June, 1, 2019, https://nxtwiki.org/wiki/Whitepaper:Nxt

[25] **Pavel Vasin**, (2013) BlackCoin, blackcoin.co, 2013.

[26] **Aggelos Kiayia, Ioannis Konstantinou, Alexander Russell, Bernardo David, Roman Oliynykov**, (2016). A Provably Secure Proof-of-Stake Blockchain Protocol. IACR Cryptology. 2016.

[27] BitShare, (2015) The BitShares Blockchain, Retrieved in 21 July 2019, https://www.bitshares.foundation/papers/BitSharesBlockchain.pdf

[28] PeerCoinTalk,(2015) PeerCoin Wiki,Retrieved in July 21, 2019, http://wiki.peercointalk.org

[29] **M. A. Al Ahmad, A. Al-Saleh, and F. A. Al Masoud**, (2018) Comparison between PoW and PoS Systems Of Cryptocurrency, Indonesian Journal of Electrical Engineering and Computer Science, vol. 10, no. 3, p. 1251

[30] PeerCoin Docs, Retrieved in 21 July, 2019, https://docs.peercoin.net

[31] Peercoin Official Development Repo, Retrieved in 21 July, 2019, https://github.com/peercoin/peercoin

[32] Nxt Forum, Retrieved in July 21, 2019, https://nxtforum.org/

[33] Nxt Source Code, Retrieved in July 21, 2019, https://bitbucket.org/JeanLucPicard/nxt/src/master/

[34] **Vitalik Buterin**, (2014), Slasher Ghost, and Other Developments in Proof of Stake, Retrieved in 21 July, 2019, https://blog.ethereum.org/2014/10/03/slasher-ghost-developments-proof-stake/

[35] **Vitalik Buterin**, Virgil Griffith (2017) Casper the Friendly Finality Gadget. Retrieved in June, 1, 2019, https://vitalik.ca/files/casper_note.html

[36] **Vitalik Buterin**. (2017) Incentives in Casper the Friendly Finality Gadget, Ethereum Foundation

[37] **Castro, M., Liskov, B**., (1999) Practical byzantine fault tolerance. In Leach, P. J. & Seltzer, M. (eds.) Proceedings of the Third Symposium on Operating Systems Design and Implementation, vol. 99, 173–186.

[38] **Tschorsch, F., & Scheuermann, B**., (2015) Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies, IACR Cryptology ePrint Archive2015.

[39] **Jimi S**., (2018), Retrieved in July 21, 2018 https://medium.com/coinmonks/what-is-a-51-attack-or-double-spend-attack-aa108db63474

[40] **S. Shanaev, A. Shuraeva, M. Vasenin, and M. Kuznetsov**, (2018) Cryptocurrency Value and 51% Attacks: Evidence from Event Studies," SSRN Electronic Journal.

[41] **Vitalik B.,** (2015) Retrieved in July 21,2019 https://blog.ethereum.org/2014/05/15/long-range-attacks-the-serious-problem-with-adaptive-proof-of-work/

[42] Nxt Portal Monitor, Retrieved in August 04, 2019, https://nxtportal.org/monitor/

[43] Peercoin Blockchain Explorer Retrieved in August 04, 2019, https://chainz.cryptoid.info/ppc/#!rich

[44] Etherscan, Retrieved in August 04, 2019, https://etherscan.io/accounts

[45] **Vitalik B**., Validator Ordering and Randomness in PoS Retrieved in August 04, 2019, https://vitalik.ca/files/randomness.html

[46] Peercoin Charts, Retrieved in August 04, 2019, https://bitinfocharts.com/peercoin/

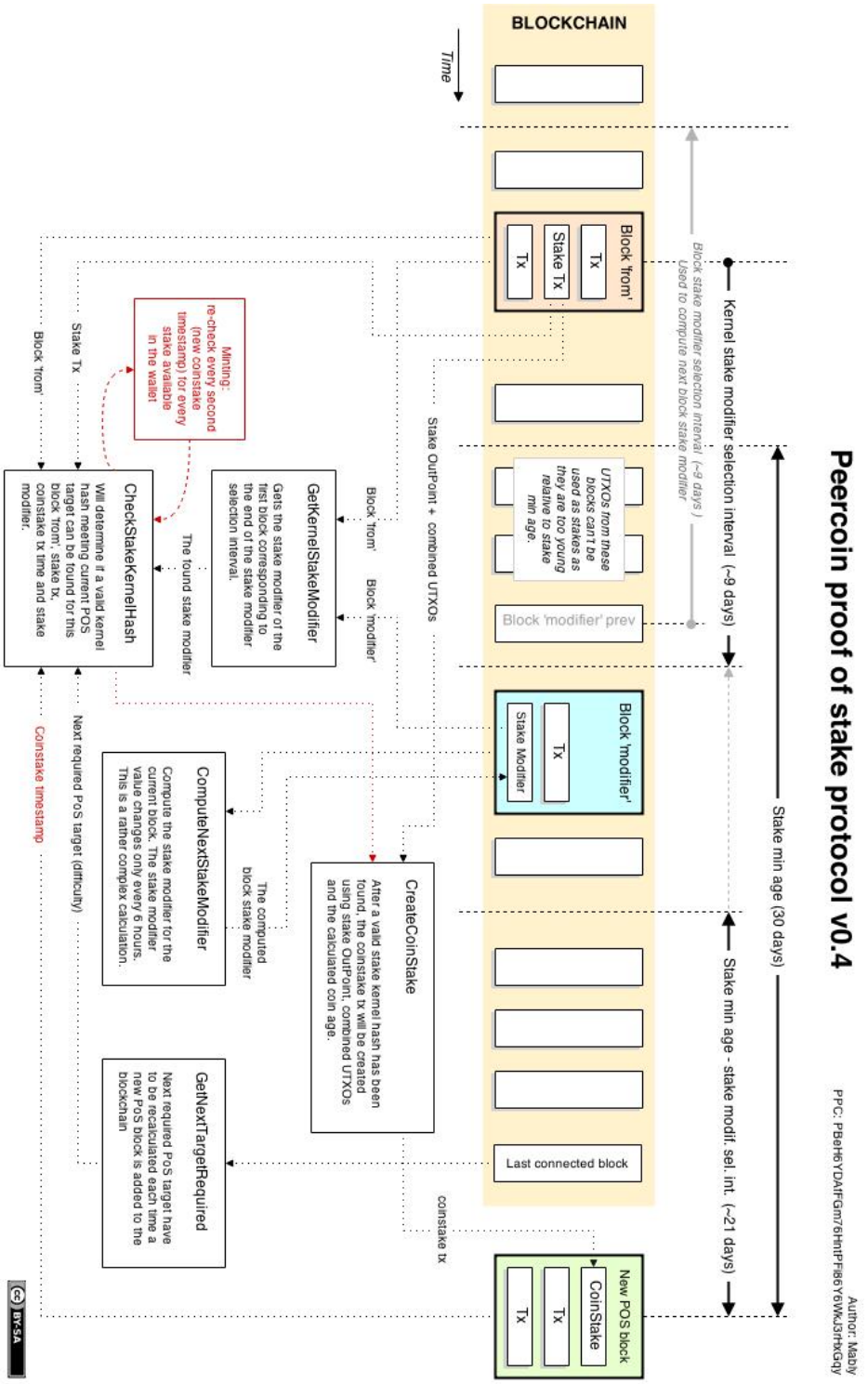
EKLER

EK 1: Peercoin PoS blok oluşum diagramı.

EK 2: Nxt blok yapısı.

EK 1

Şekil Ek 1.1: Peercoin PoS blok oluşum diagramı.



EK 2

Şekil Ek 1.2: Nxt blok yapısı.

Field Name	Data Type	NOT NULL
DB_ID	BIGINT(19)	yes
ID	BIGINT(19)	yes
VERSION	INTEGER(10)	yes
TIMESTAMP	INTEGER(10)	yes
PREVIOUS_BLOCK_ID	BIGINT(19)	no
TOTAL_AMOUNT	BIGINT(19)	yes
TOTAL_FEE	BIGINT(19)	yes
PAYLOAD_LENGTH	INTEGER(10)	yes
GENERATOR_PUBLIC_KEY	VARBINARY(32)	yes
PREVIOUS_BLOCK_HASH	VARBINARY(32)	no
CUMULATIVE_DIFFICULTY	VARBINARY(2147483647)	yes
BASE_TARGET	BIGINT(19)	yes
NEXT_BLOCK_ID	BIGINT(19)	no
HEIGHT	INTEGER(10)	yes
GENERATION_SIGNATURE	VARBINARY(64)	yes
BLOCK_SIGNATURE	VARBINARY(64)	yes
PAYLOAD_HASH	VARBINARY(32)	yes
GENERATOR_ID	BIGINT(19)	yes

ÖZGEÇMİŞ

Ad-Soyad : Yunus Çağrı YURDAKUL

Uyruğu : T.C.

Doğum Tarihi ve Yeri : 20.11.1990 Ankara

E-posta : ycagriyurdakul@gmail.com

ÖĞRENİM DURUMU:

- **Lisans** : 2015, Bilkent Üniversitesi,
  Mühendislik Fakültesi, Bilgisayar Mühendisliği
- **Yükseklisans** : 2019, TOBB Ekonomi ve Teknoloji Üniversitesi,
  Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı

MESLEKİ DENEYİM VE ÖDÜLLER:

Yıl	Yer	Görev
2016 – Halen	Türkiye Cumhuriyet Merkez Bankası	Bilgisayar Mühendisi
2015 – 2016	Verisan	Bilgisayar Mühendisi

YABANCI DİL: İngilizce

TEZDEN TÜRETİLEN YAYINLAR, SUNUMLAR VE PATENTLER

- **Yurdakul, Y. Ç.**, 2019. A Technical Analysis of Proof of Stake Based Blockchain Systems: Nothing at Stake Problem, International Conference on Theoretical Applied Computer Science and Engineering, (ICTACSE 2019), Oct. 11-12, İstanbul, Turkey.