Blok Zinciri Teknolojisine Yapılan Saldırılar Üzerine bir İnceleme

Literatür Makalesi/Review Article

Oğuzhan TAŞ, Farzad KİANİ

Bilgisayar Mühendisliği, İstanbul Sabahattin Zaim Üniversitesi, Mühendislik ve Doğa Bilimleri Fakültesi, İstanbul, Türkiye.
oguzhan.tas@std.izu.edu.tr, farzad.kiyani@izu.edu.tr
(Geliş/Received:07.08.2018; Kabul/Accepted:10.10.2018)
DOI: 10.17671/gazibtd.451695

Özet— Son zamanlarda; blok zinciri tabanlı kripto para ödeme sistemleri(bitcoin, ethereum) oldukça popüler olmuştur. Merkezi olmayan eşler arası(P2P: Peer to Peer) ağ yapısına sahip olan bu sistemde tüm işlemler, sadece ekleme yapılabilen bir ana defterde(ledger) tutulmaktadır. Madenciler ise bu ağ yapısındaki düğümleri oluşturmaktadır, her madenci defterin yerel kopyasına sahiptir. Blok zincirinde, Çalışma İspatı(PoW: Proof of Work) uzlaşma algoritması işlemi onaylamakta ve zincire yeni blok eklenmesine izin vermektedir. Ödülü almak için, madenciler eşler arası ağda işlemi tamamlamak için birbirleriyle yarışırlar. Ödül sistemi, blok zinciri kullanan bitcoin'i popülerleştirmiş, fakat aynı zamanda saldırganların blok zincirine ilgisini artırmıştır. Saldırganlar tarafından blok zincirinin madenci havuzuna ve ağ yapısının güvenliğine farklı saldırılar yapılmıştır. Bu makalede, blok zinciri alt yapısına karşı mevcut saldırılar sunulmuştur. İlk bölümlerde, P2P mimarisine, uzlaşma protokolüne ve işlemlere yönelik saldırı tipleri araştırılmıştır. Bu bölümde, %51 saldırısı, Çift harcama, Finney, Vector76, Kaba Kuvvet(Brute Force), Sybil, Eclipse, Denge(Balance) gibi saldırılar açıklanmış ve çözümler önerilmiştir. Daha sonra, Bencil madencilik ve Blok Atma, Blok Tutma(BWH: Block Witholding Attack), Blok Tutma Sonrası Çatallanma(FAW:Fork after Witholding), Havuz sıçrama saldırısı, Cezalandırıcı Çatallanma ile Kara Listeye Alma, Köpük saldırısı ve Rüşvet Saldırısı gibi madencilik havuzuna karşı saldırılar incelenmiş ve savunma stratejileri sunulmuştur. Son bölümde de blok zinciri altyapısında kullanılan kriptografi'nin geleceği üzerinde tartışılmış ve Post Kuantum Kriptografi'nin etkilerinden bahsedilmiştir.

Anahtar Kelimeler— blok zinciri, güvenlik, bitcoin, ethereum

A Survey of Attacks on Blockchain Technology

Abstract— In recent times, popularity of blockchain based crypto currencies (bitcoin and ethereum) have been increased. Blockchain system has decentralized Peer to Peer (P2P) network, all transactions are recorded in a public ledger that can only be appended. The miners constitute the nodes of this network and every miner has local copy of ledger. In blockchain, PoW(Proof of Work) consensus algorithm is used to verify transaction and give permission to append new blocks to chain. To get reward, miners compete with each other to complete transactions on the P2P network. The reward system popularized Bitcoin, which uses block-chain, but at the same time attracted the atention of the attackers in the block chain. In this paper, current attacks against the block-chain are presented. In the first part, attack types to P2P architecture, consensus protocol and transaction are investigated. In this part, 51%, Double Spending, Finney, Vector76, Brute Force, Sybil, Eclipse and Balance attacks are explained and solutions are proposed. In addition, pool mining attacks such as Block Withholding Attack (BWH), Pool Hoping Attack, Blacklisting via Punitive Forking, Feather Forking and Bribery Attack are presented. In the last part, the future of cryptography used in blockchain infrastructure has been discussed and effects of Post Quantum Cryptography have been mentioned.

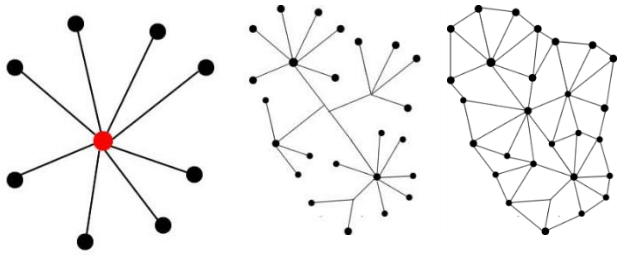
Keywords— blockchain, security, bitcoin, ethereum

1. GİRİŞ (INTRODUCTION)

İnternet üzerinden para transferi, günümüzde insanların işlerini büyük oranda rahatlatan teknolojik olanaklardan birdir. Özellikle e-ticaret popülerleşmesiyle ürün ve hizmetlerin internet üzerinden farklı ödeme seçenekleriyle temin edilebilmesi yeni bir ekonomi doğurmuştur. E-ticarette en çok tercih edilen ödeme tekniği olan kredi kartı hayatımızı büyük oranda rahatlatmıştır. Bankaya gidip sıra bekleme, mesai saatlerine göre hareket etme, ekstra masraflar ödeme derdinden müşterileri kurtardığı gibi, bankayı da aşırı iş yükünden, çalıştırılan fazla personel maaşından, kira vb. şube giderlerinden kurtarmıştır. 7/24 aktif olan internet bankacılığı, kısa sürede birçok işlemin kolaylıkla gerçekleştirilmesini sağlamıştır. Banka şubeleri, internet üzerinden henüz gerçekleştirilmeyen birçok işlem için gerekse de, internet bankacılığı şubelerin yükünü de hafifletmiştir.

Hayatımızın dijital hale gelmesinin getirdiği kolaylık, pratiklik ve hızlılık geniş kitleler tarafından kabul görünce, farklı ödeme teknikleri geliştirilmiştir. Özellikle uluslararası ticarette ödenen ekstra masraflar, işlemlerin yavaş ilerlemesi, pratik olmaması alternatif ödeme şekillerinin geliştirilmesine neden olmuştur[1]. Fakat bankalar gibi finansal birimler sistemin vazgeçilmez bir unsuru olmaya halen devam etmektedir. Alıcı ve satıcı birbirine güvenmemekte, bankaya güvenmektedir. Çünkü bankalar ticaret yapan taraflar arasındaki tüm işlemleri kayıt altına almaktadır, herhangi bir anlaşmazlıkta devreye girerek problemleri çözmektedir. Örneğin satıcı parayı alıp ürünü göndermeyebilir, alıcı ürünü aldığı halde «Almadım» diyebilir. Dürüst olmayan satıcıya ve alıcıya karşı farklı koruma mekanizmaları vardır. Sonuçta uluslararası ticarette izlenmesi gereken birçok zorunlu prosedür bulunmaktadır. Bankalar iki taraf arasında yer almanın karşılığında bir bedel talep etmektedir. Özellikle uluslararası para transferi yavaş olduğundan, vergisiz, hızlı ve düşük masraflı kripto para gündeme gelmiştir. Dijital para kavramı ilk defa 1982 yılında Chaum tarafından önerilmiştir[2].Şu an piyasada 1565 farklı kripto para[3] bulunmaktadır ve her geçen gün artmaktadır, 606 milyar dolar pazar hacmine sahiptir. Kripto paralardan en popülerlerinden birisi olan bitcoin'in toplam sermaye büyüklüğü 115 milyar dolardır[4].

Kripto paraların alt yapısında blok zinciri yapısı yer almaktadır. Blok zinciri, 2008 yılında Satoshi Nakamoto takma adlı bir kişi tarafından, merkezi sistemlerin sıkıntılarından dolayı önerilmiştir[5]. Eşler arası (P2P) ağı kullanan sistemde, bir merkez olmadan bir taraftan diğer tarafa elektronik ödeme yapılabilmekte ve işlem kayıtları her düğümde yer alan veri tabanlarında yerel kopya olarak tutulmaktadır. Bankalar gibi güvenilir bir finansal otorite yoktur. Sistemin güvenliği kriptografi kullanarak sağlanıp, hızlı şekilde alış veriş hedeflenmektedir. Şekil 1'de bankaların kullandığı yıldız ağ yapısına benzeyen merkezi yapı ve blok zinciri sisteminin kullandığı merkezi olmayan eşler arası ağ yapısı görülmektedir.



a) Merkezi yapı b)Merkezi olmayan yapı c)Dağıtık Yapı

Şekil 1. Merkezi, merkezi olmayan ve dağıtık ağlar.
(Centralized, decentralized and distributed networks)

Makalenin geri kalanı şöyle organize edilmiştir. Bölüm 2'de blok zinciri alt yapısını anlamak için kriptografi terimlerine değinilmiş, Bölüm 3'de blok zincirini oluşturan elementler üzerinde durulmuş, bölüm 4'de blok zincir uygulamalarına değinilmiş, bölüm 5'te bitcoin ve blok zincirine yapılan saldırılar detaylı şekilde anlatılmış, bölüm 6'da saldırılara karşı savunma önerileri sunulmuştur.

2. KRİPTOGRAFİ (CRYPTOGRAPHY)

Blok zinciri alt yapısını anlamak için mesaj özütü algoritmaları, tek anahtar şifreleme, çift anahtar şifreleme, sayısal imza kavramlarına kısaca değinilmiştir.

2.1 *Mesaj Özütü Algoritmaları (Hash Algorithms)*

Mesaj özütü algoritmaları, girdi metni ne kadar büyük olursa olsun, sabit uzunlukta bir çıktı üreten algoritmalardır. Mesaj özütü algoritmaları tek yönlü algoritmalardır. Yani üretilen bir çıktıdan tekrar orijinal metine dönmek imkânsızdır. Orijinal metin içerisinde yapılan en küçük değişiklik bile algoritma çıktısını etkilemektedir, sonuç değişmektedir.

Mesaj özütü algoritmaları sayısal imza altyapısında kimlik doğrulama için, iletilen mesajda bütünlük kontrolü için sıklıkla kullanılırlar. Birçok mesaj özütü algoritması geliştirilmiştir. Örneğin MD5 algoritması 128 bit, SHA-1 algoritması 160 bit, RIPEMD algoritması 160 bit, SHA-256(SHA-2) algoritması 256 bit büyüklüğünde bir çıktı üretmektedir. Son olarak, 2015 yılında NIST tarafından yapılan yarışmasında SHA-3 standardı olarak kabul edilen ve 3GPP ağlarda kullanılan KECCAK algoritması, 512 bit uzunlukta çıktı üretmektedir.

Özüt algoritmalarında en önemli ölçüt, çakışma olmamasıdır. İki farklı metin, mesaj özütü algoritmasından geçirildiğinde aynı sonuç elde ediliyorsa, çakışma oluşmuştur ve o algoritma artık kullanılmaz. SHA-1, MD5 gibi algoritmalarda çakışmalara rastlandığından artık kullanılmamaktadır. Bitcoin kripto para sisteminde kullanılan özüt algoritması SHA-256'dır, bitcoin adresi üretilirken ise SHA-256 ve RIPEMD 160 algoritmaları kullanılmaktadır. Diğer para birimleri Scrypt, Blake-256, CryptoNight, HEFTY1, Quark, SHA-3, scrypt-jane gibi algoritmaları kullanmaktadır. Mesaj m, h() özüt alma fonksiyonu, t ise

özüt sonucu olsun. Matematiksel olarak özüt işlemi t=h(m) ile gösterilir.

2.2 *Tek Anahtar Şifreleme (Single Key Encryption)*

Tek anahtar şifrelemede, mesajları şifrelemede ve şifre çözme işleminde aynı anahtar kullanılır. Eğer bu anahtar ele geçirilirse tüm mesajlar çözülebilir. Bu şifreleme tarzı "Gizli Anahtar Şifreleme(Secret Key)" ya da "Simetrik anahtar(Symmetric Key)" şifreleme olarak da adlandırılır. Tek anahtar şifrelemede, fiziksel iletişimi olmayan iki taraf arasında anahtar dağıtımı problemdir. Bu tarzda çalışan algoritmalara örnek olarak AES, DES, 3DES, RC5 şifreleme algoritmaları örnek verilebilir. AES algoritması; sağlamlık, donanım ve yazılım üzerinde hızlı çalışma gibi birçok kriter baz alınarak, NIST tarafından yüzlerce algoritma içinden seçilen Rijndael algoritmasıdır. 128, 192 ve 256 bit anahtar uzunluklarında çalışabilir, anahtar uzunluğu ne kadar fazla ise sistemin güvenliği o oranda artar ama işlemler büyük anahtar boyutunda daha yavaş yapılır. Şifreleme ve şifre çözme işlemleri çift anahtarlı sisteme göre hızlıdır. Bu algoritmalar, blok tabanlı ve akış(stream) tabanlı olmak üzere iki kısma ayrılır. Akış algoritmaları, bit tabanlı çalışan, donanım üzerinde daha hızlı işlem yapmak için geliştirilmişlerdir. GSM/3G güvenliğinde A5/1 ve A5/2 kullanılmış, RC4 algoritması ise kablosuz şifreleme için modemlerde WEP, WPA standardı içinde, Bittorent şifreleme protokolünde, Microsoft Office XP içinde vb. birçok yerde kullanılmıştır, fakat artık güvenli değildir. Blok tabanlı algoritmalar ise sabit uzunluktaki bit grubu üzerinde işlem yaparlar, genelde yazılım üzerinde kullanılmakla birlikte gelişen donanım teknolojileri ile KASUMI, AES-128 gibi algoritmalar 3G ve 4G ağlarda kullanılmaktadır.

Şifrelenecek mesaj m, kullanılan anahtar k, şifreleme fonksiyonu e(), şifre çözme fonksiyonu d(), şifreli metin sonucu c ise; $c=e_k(m)$ ifadesi şifreleme işlemini, $m=d_k(c)$ işlemi de şifre çözme işlemini göstermektedir. Görüldüğü gibi iki fonksiyonda da aynı k anahtarı kullanılmıştır.

2.3. *Çift Anahtar Şifreleme (Double Key Encryption)*

Mesajları şifreleme için bir anahtar, şifreyi çözmek için başka anahtar kullanılır. "Asimetrik Anahtar" ya da "Genel Anahtar" şifreleme olarak da adlandırılır. Bu tarz şifrelemede, genel anahtar(public key) şifreleme ve sayısal imzayı doğrulamada, gizli anahtar(private key) ise şifre çözmede ve sayısal imzayı oluşturmada kullanılır. Farklı anahtarlar kullanıldığı için anahtar dağıtımı, simetrik tarza göre daha rahattır. Genel anahtar herkese açıktır, şifreleme için ve sayısal bir imzayı doğrulamak için kullanılır. Özel anahtar ise gizlidir, kimseye verilmez, şifre çözme ve imzalama için kullanılır. Bu algoritmalara RSA, Elgamal, Eliptik Eğri, McEliece örnek verilebilir. Merkle Hellman, Knapsack ise artık kullanılmamaktadır. RSA, en çok kullanılan ve bilinen çift anahtar şifreleme algoritmasıdır. Fakat RSA algoritması hantaldır, günümüzde Eliptik Eğri düşük anahtar boyutlarında güvenli şifreleme yaptığı için daha çok tercih edilmektedir. SSL, SSH, TLS, S/MIME, PGP ve GPG gibi internet standartlarının altında asimetrik anahtar şifrelemesi kullanılmaktadır.

Şifrelenecek mesaj m, şifrelemede kullanılan genel anahtar "genelk", şifre çözmede kullanılan özel anahtar "ozelk", şifreleme fonksiyonu e(), şifre çözme fonksiyonu d(), şifreli metin sonucu "c" ise; $c=e_{genelk}(m)$ ifadesi şifreleme işlemini, $m=d_{ozelk}(c)$ işlemi de şifre çözme işlemini göstermektedir. Görüldüğü gibi iki fonksiyonda farklı anahtarlar (genelk, ozelk) kullanılmıştır.

2.4. *Sayısal İmza (Digital Signature)*

Sayısal İmza işleminde, önce mesaj özüt algoritmasından geçirilerek, 256 bit gibi sabit uzunlukta bir mesaj özütü elde edilir. Sonra bu mesaj özütü, özel anahtar ile imzalanarak sayısal imza oluşturulur. Bundan sonra karşı tarafa orijinal mesaj ile iletilir. Şifrelenecek mesajı m, özüt fonksiyonu h(), özüt sonucu t, imzalama fonksiyonu s(), genel anahtar "genelk", özel anahtar "ozelk", sayısal imzayı y ile gösterelim. O zaman imza oluşturmada t=h(m), $y=s_{özelk}(t)$. Doğrulamada ise, önce $t=s_{genelk}(y)$ elde ederiz, sonra bu özüt sonucu ile imza gelen mesajın özütünü tekrar t'=h(m) ile elde edip, karşılaştırılır t=t' ise özütler aynıdır ve imza doğrulanmış olur, aksi takdirde mesaj veya imza değişmiştir. Şekil 2'de görüldüğü gibi gönderenin özel anahtarı, sayısal imza oluşturmakta kullanılmaktadır.

Şekil 2. İmzalama
(Signing)

Sayısal imza ve mesajı alan karşı taraf şu işlemleri yapar. (i) Alıcı taraf gelen mesajı mesaj özütü algoritmasından geçirerek mesaj özütünü elde eder. (ii) Aldığı sayısal imzayı gönderenin genel anahtarı ile çözer ve mesaj özütünü elde eder.

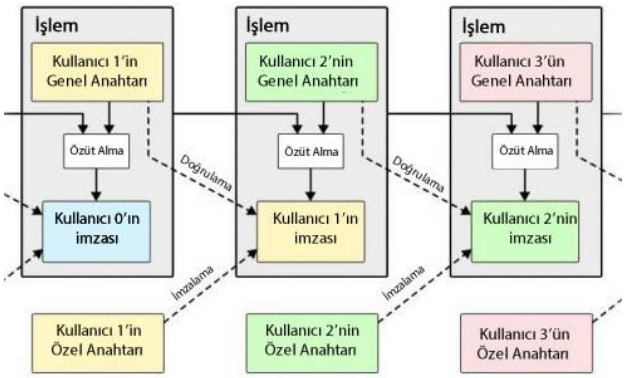
Şekil 3. Doğrulama
(Verification)

(iii) birinci ve ikinci adımda elde edilen mesaj özütlerini karşılaştırır, eğer sonuç aynı ise sayısal imza işlemi doğrudur. Kripto para işlemlerinde de alış veriş işlemi, müşteri tarafından imzalanmaktadır, karşı taraf yani satıcı ise imzayı müşterinin genel anahtarı ile doğrulamaktadır.

3. BLOK ZİNCİRİ (BLOCKCHAIN)

Blok zinciri, uzlaşma(consensus) algoritmalarıyla birçok site, ülke ve/veya enstitü arasında kopyalanmış,

paylaşılmış ve senkronize edilmiş bir veri yapısıdır. Ağda meydana gelen her olay, düğümlerde doğrulanmakta ve kaydedilmektedir. Blok zincirinde ilk başlangıç bloğuna "genesis blok" ismi verilir. Her blok, kendinden önceki bloğun özüt(hash) algoritmasından geçirilmiş içeriğine sahiptir. Böylece sistemdeki bir işlemi değiştirmek isteyen kişi, geriye doğru tüm işlemlerin özüt sonucunu hesaplamak zorundadır. Bu işlem pratik olarak mümkün değildir, çünkü hesaplanan sonuçların tüm madencilerde de aynı olması gerekmektedir.



Şekil 4. Basitleştirilmiş Bitcoin Blok Zinciri.
(Simplified Bitcoin Blockchain)

Blok içeriği aşağıdaki tabloda görüldüğü gibidir. Bir blok içerisinde birden fazla işlem olabilir[6].

Tablo 1. Blok içeriği
(Block Content)

Sihirli Sayı	Blok zincirini tanımlayan eşsiz sayı, sonraki tüm bloklar için sabit kalır.
Blok boyutu	Bloğun sonuna kadar takip eden bayt sayısı
Sürüm Numarası	Blok format biçimi.
Önceki blok bağlantısı	Önceki bloğun özütü
İşlem Özütü	Merkle ağacının kök düğümü, ağaçtaki tüm özüt çiftlerinin bir torunu. Kök düğüm, bloktaki tüm işlemlere bağlı 256 bit özüttür.
Zaman Damgası	Bloğun oluşturulduğu zaman
Kazma Güçlüğü	Yeni blok bulmanın bağıl zorluk ölçüsü. Zorluk, ağdaki madencilerin ne kadar özüt gücü harcadığının bir fonksiyonu olarak periyodik şekilde güncellenir.
bks(Nonce)	Bir defa kullanılan sayı(bks), PoW hesaplamasında kullanılır.
İşlem Sayısı	Bu bloktaki işlem sayısı
İşlemler	İşlemler listesi (boş olmaz)

Blok zinciri sisteminde her kullanıcı kendi bilgisayar kaynaklarını kullanır. Ağdaki her bir düğüm tüm defter kaydının tam kopyasına sahiptir.

3.1 Akıllı Sözleşmeler (Smart Contracts)

Blok zincirinde depolanan ve önceden belirlenmiş şartlar gerçekleştiğinde otomatik olarak çalıştırılan kod satırlarıdır. En basit ifadeyle, geliştirenler tarafından çalışmak üzere ayarlanmış programlardır. Akıllı sözleşmelerin faydası en çok iş anlaşmalarında görülmektedir, tarafların üzerinde mutabık kaldığı sözleşmelere herhangi bir noter vs. gibi üçüncü taraf olmadan uyma zorunluluğu getirmektedir[7,8].

Akıllı sözleşmeler sayesinde, günlük hayatta ev, araba alırken karşılaştığımız zor ve uzun işlem süreci kolaylaşacak ve hızlanacaktır[9]. Ayrıca aracı kurum ve kişilerin sayısı da azalacaktır, çünkü doğrulama işlemlerini yapacak kişilerin yerini kodlar alacaktır.

3.2 Madencilik (Mining)

Blok zincirine bir blok içinde yeni bir işlem kaydı eklenmesi aktivitesine madencilik adı verilir. Bloktaki ilk işlem, para tabanı(coinbase) işlemi olarak adlandırılır. En son blok zincirine yeni eklenen blok, tüm düğümlere gönderilir, böylece sistemin kaydı tüm düğümlerce tutulmuş olur. Her blok üretiminde yeni bitcoin'ler yayınlanır ve bloku ekleyene ödül olarak verilir. Kullanıcı, kendi bilgisayar kaynaklarını kullanarak işlemleri doğrular ve ödemeleri kaydeder. Oluşturulan ödeme işleminin karşılığında ödül olarak bitcoin kazanır. Her 210.000 blokta bir ödül yarıya düşmektedir. İlk başta 50 BTC iken şimdi 6.25 BTC civarıdır.

Madenciler, hesaplama gücü için CPU, GPU, FPGA ve ASIC gibi donanımları kullanabilirler, ya da bulut hesaplama aracılığı ile madencilik yapabilirler[7]. CPU ve FPGA yavaş olduğundan, paralel işlem yapan GPU, ya da özüt için özel geliştirilmiş, daha hızlı ASIC donanımları kullanılmaktadır.

3.3. Uzlaşma protokolü (Consensus Protocols)

Merkezi bir birimde kararlar tek bir lider tarafından verilir. Merkezi olmayan eşler arası kullanan P2P gibi bir yapıda, lider olmadığından kritik kararların verilmesi için uzlaşma(consensus) protokolü kullanılmaktadır. Aslında uzlaşma, en basit ifadeyle bir gruptaki kullanıcıların çoğunluk oyları ile grubun faydasına olacak şekilde karar verilmesidir.

Uzlaşma protokolleri de güvenlik ihtiyacından doğmuştur. Çok sık karşılaşılan, ağ üzerinden giden mesajların değiştirilmesi söz konusu olabilir, örneğin 4 BTC göndermek isteyen bir kullanıcının mesajı ağda 40 BTC olarak değiştirilebilir. Bu durumu önlemek için Satoshi Nakamoto, PoW ismini verdiği protokolü önermiştir.

3.3.1. PoW Uzlaşma Protokolü (PoW Consensus Protocol)

Çalışma İspatı (PoW-Proof of Work) protokolü, Bitcoin'de blok zincirinin en önemli elementlerinden biridir. Bu protokolün çalışmasını adım adım şöyle açıklayabiliriz.

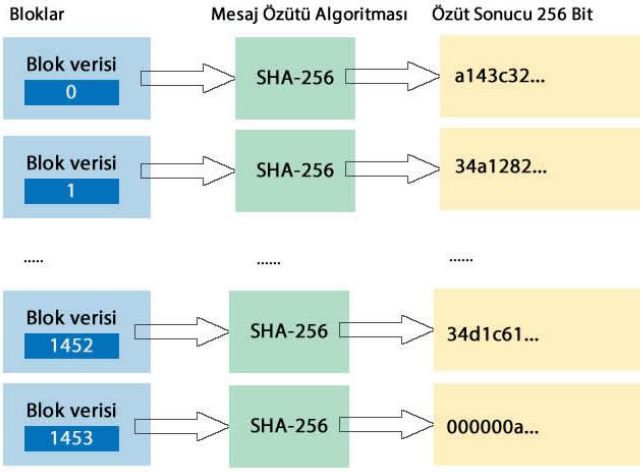
i. Onaltılık sistemde rastgele bir sayı seçilir, buna bir defa kullanılan sayı (bks) adı verilir. Aşağıdaki şekilde mavi blok içinde görülen 0 değeri, bks değerini ifade etmektedir. Blok başlangıcına bks eklenerek "hizmet reddi (DOS-

Denial of Service)" saldırılarına karşı sistem korunmuş olur.

ii. Daha sonra metin ile bks birleştirilir ve sonuca bakılır. Örneğin özüt sonucu, başta 6 tane sıfır ile başlayacak denebilir. Bitcoin, PoW algoritmasını HashCash[10] ismiyle kullanır.

iii. Ardından eğer 6 tane sıfırla başlayacak mesaj özütü elde edilmişse gönderilir, değilse sürekli bks sayısı değiştirilerek istenilen özüt elde edilene kadar uğraşılır, bu işlem büyük hesaplama gücü ve zaman gerektirir, PoW'da buna bulmaca (puzzle) çözme işlemi denir.

iv. Mesaj karşı tarafa iletilince kaç tane sıfırla başlayıp başlamadığına bakılır eğer ağda değiştirilmişse, özüt değişeceğinden içeriğin değiştiği anlaşılmış olur[11,12].



Şekil 5. PoW protokolünde bulmaca çözme ile yeni eklenecek bloğu bulma.
(Finding new block via solving puzzle in PoW protocol)

Bu algoritma yüksek grafik işlemci gücü gerektirdiğinden, fazla kaynak harcamaktadır. Ayrıca ödül problemi çözen tek kişiye verildiği için madenciler birbirleriyle yarışırlar ve çok fazla enerji tüketilmiş olur. PoW'ün en çok eleştirilen noktası da fazla tüketilen enerjidir. Diğer bir eleştirilen yanı da PoW'un yavaş olmasıdır, yeni eklenen bir blokun doğrulaması 10 dakika sürmektedir. Klasik kredi kartları hemen çekim yaparken, PoW için beklenilen bu süre eleştirilmektedir. Bu duruma göre yılda en fazla 365 x 24 x 6= 52.560 blok dâhil edilebilmektedir.

Doğrulama işlemini hızlandırmak için Sompolinsky ve arkadaşları tarafından GHOST[13,14] protokolü önerilmiştir. En iyi zinciri bulmak için düğümlerin yollarını değiştirerek, saniyedeki işlem sayısını(TPS) artırmak amaçlanmaktadır. GHOST protokolünü bir türevi de Ethereum projesine uygulanmıştır. Fakat, bu protokolün hızlı işlem yapması, ileride değinilecek olan çift harcama gibi saldırıların yapılmasını kolaylaştırmakta, güvenlik açıkları doğurmaktadır. Bu sorunu çözmek için daha sonra önerdikleri DAG(Yönlü Düz Ağaç) yaklaşımı[15] ile GHOST protokolünde hızlı işlem yapmadan dolayı yaşanan sorunlar çözülse de, "tersine işlem yapabilme" saldırganların düşük maliyette saldırı gerçekleştirmelerine neden olmuştur.

3.3.2. PoS Uzlaşma Protokolü (PoS Consensus Protocol)

PoW'u Bicoin kullanırken, Hisse İspatı (PoS-Proof of Stake) protokolünü Ethereum kripto para sistemi kullanır. PoW protokolü çok fazla enerji tüketip, sistem kaynaklarını boşa harcarken, PoS'un çok fazla enerji tüketmesine gerek yoktur. PoS blok zinciri ağında, katılımcıların ellerinde tuttukları oran kadar madencilik hakkı verir. Madenciler blokları kazmak için, belirlenen eşik değerinin üzerinde bir miktar kadar parayı ellerinde tuttuklarını göstermek zorundadır[7]. PoS protokolünde, büyük miktarda parayı elinde tutan kişinin saldırmak için parasını riske atması gerektiğinden, bu işlem de pahalıya geldiğinden, kötü niyetli saldırılara karşı koruma sağlanmış olur[8]. Ayrıca, elinde büyük miktarda hisse bulunan kişi, çift harcama gibi saldırılarla sisteme zarar vermeyecektir. Böyle saldırılar, zamanla kripto para değerini ve hisse değerini düşürecektir.

3.4. Madenci Havuzu (Mining Pool)

Hesaplama gücünü artırarak, blokların doğrulama zamanını etkilemek ve daha fazla ödül kapmak amacıyla madencilerin birleşerek oluşturdukları yapılardır. Madenci havuzları, çözülmemiş işlem birimlerini havuz üyelerine(madenciler) ileten, havuz yöneticisi tarafından kontrol edilir. Madenci yeni bir blok keşfettiği zaman, FPoW protokolü aracılığıyla havuz yöneticisine gönderir. Havuz yöneticisi, ödülü almak amacıyla bitcoin ağında yayınlar. Havuz Yöneticisi, ödülü katılan madenciler arasında paylaşım oranına göre dağıtır. Böylece, havuzdaki üyeler PPoW protokolüne göre ödüllendirilmiş olur, PPoW'un Bitcoin sistemde gerçek bir değeri yoktur[16].

3.5. GPU ve ASIC Donanımları (GPU and ASIC Hardware)

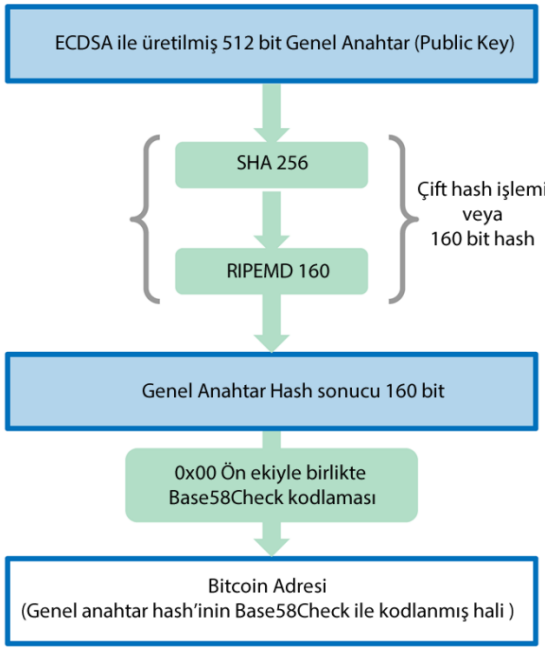
Bilgisayar kaynaklarının güçlülüğü ile kazanılan ödül arasında paralellik vardır, yani blok zincirine hesaplama gücü daha yüksek olan avantaja sahiptir. Madencilik işleminde bilgisayar merkezi işlem birimi(CPU) yerine ekran kartı grafik işlem birimi(GPU) kullanılır. GPU'lar yani grafik İşlemci birimleri, matematiksel problemleri çözmede, işlemcilere(CPU) göre daha verimlidir. Tek bir GPU çekirdeği, CPU çekirdeğinden daha yavaş çalışır. Fakat GPU'da çok fazla işlemci paralel olarak işlem yaptığından hız artar. 2013 yılından itibaren ise, mesaj özütü alma işlemini daha hızlı yapabilmek için ASIC adı verilen özel donanımlar tasarlanmıştır. ASIC, "uygulamaya yönelik tümleşik devre" anlamına gelmektedir.

ASIC, en iyi CPU'dan 100.000 kat daha hızlıdır. Mesaj özütü alma işlemine odaklı olduklarından aşırı ısınırlar ve soğutulmaları için fan gerektirir, bu da aşırı gürültü demektir. Ayrıca, bu donanımlar fazla güç çektiğinden elektriğin fazla tüketilmesine ve elektrik faturasının yüklü gelmesine neden olurlar.

3.6. Bitcoin

Kripto para birimleri içinde en popüler olanıdır, geliştirildiği 2009 yılından beri şirketlerin, devletlerin ilgisini çekmiştir. Üçüncü bir güvenilir otorite olmadan rahatlıkla çalışır. Sahibi bitcoin üzerinde tam yetkiye sahiptir, banka gibi herhangi bir birime sormadan istediği zaman istediği yere harcayabilir. Açık kaynak bir sistemdir ve kimsenin kontrolünde değildir. Bitcoin, diğer para birimleriyle değiştirilebilir, ürün ve hizmet satın alınması yapılabilir. Kullanıcılar gerçek isimlerini yayınlamayabilirler, tamamen anonim bir yapı hâkimdir, tüm hesap işlemleri isteyen herkes tarafından görülebilir.

Bitcoin kullanıcıları, işlemler oluşturarak bitcoin'i kullanıcılar arasında transfer ederler. Hedef adres ya da Bitcoin adresi olarak adlandırılan adres, kullanıcını genel anahtarı ile tersine dönülemez özüt fonksiyonları(SHA 256 ve RIPEMD 160) vasıtasıyla gerçekleştirilir. Şekil 6'da bitcoin adresi oluşturma adımları görülmektedir.



Şekil 6. Bitcoin'de adres oluşturma adımları.
(Step by step creation of bitcoin address)

3.7. Cüzdanlar(Wallets)

Bitcoin'de en küçük para birimi Satoshi'dir. Bir bitcoin'in yüz milyonda biridir. 1 satoshi=0.00000001 BTC'dir. Başka bir deyişle 1 BTC = 100.000.000 Satoshi'dir.

Bitcoin'de bir kullanıcının birden fazla genel anahtar ile üretilmiş birden fazla adresi olabilir, bu adresler bir veya daha fazla cüzdanda saklanabilir. Bitcoin'i harcayabilmek için kullanıcı kendi özel anahtarı ile işlemi imzalamalıdır. Eliptik Eğri Sayısal İmzalama Algoritması (ECDSA) ile imzalama işlemi gerçekleştirilmektedir. Eliptik Eğri (ECC) algoritmasının kullanılma nedeni, RSA algoritmasına göre küçük anahtar boyutunda daha fazla güvenlik sağlamasıdır.

4. BLOK ZİNCİRİ UYGULAMA ALANLARI (APPLICATIONS OF BLOCKCHAIN)

Devletler, üniversiteler, şirketler, hastaneler arasındaki tüm işlemler blok zincirinde tutulabilir. Blok zincirinin evrimsel gelişim sürecini kaynaklar üç kısma ayırmaktadır.

- Blok Zinciri 1.0 – Para transferi, havale ve dijital ödeme
- Blok Zinciri 2.0 – Akıllı Sözleşmelerin gelişmesiyle birlikte, hisse senetleri, tahviller, vadeli işlemler, krediler, ipotek gibi piyasalarda ve finansal işlemlerde
- Blok Zinciri 3.0 – Para ve maliye piyasalarının haricindeki hükümet, sağlık, bilim, kültür sanat alanlarda kullanılmaktadır[17].

Blok zincirinin getirdiği avantajlardan dolayı birçok uygulama alanı bulmuştur. Kriptografi teknikleriyle belgeleri, sözleşmeleri vb. değerleri koruması nedeniyle blok zinciri sağlık, emlak, otomotiv gibi alanlarda sıklıkla kullanılmaya başlamıştır. Herkese açık, şeffaf yapısından dolayı, tarafların birbirilerinin işlemlerinden haberdar olması ve bu sayede dolandırıcılık faaliyetlerinin azaltılması hedeflenmektedir. Blok zincirine yapılabilecek eklemeler ile sürekli genişleyebilir, kalıcı bir yapı oluşturabilme sağlanmıştır. Şirketler ve devletler için ucuz hizmet sağlama, verimliliği ve kullanışlılığı artırma, yeniliklere açık esnek bir sistem oluşturma gibi pozitif faktörlerden dolayı farklı sektörlerde sorunlara çözüm önerisi olarak sunulmaktadır[18].

Akıllı şebekeler, nesnelerin İnterneti(IoT), akıllı şehirler, taşıtlar arası ağlar, sağlıkta veri yönetimi uygulamaları gibi gelecek nesil teknolojiler, blok zinciri ve uzlaşma protokolü ile gelişecektir.

5. BLOK ZİNİCİRİ VE BITCOIN GÜVENLİĞİ (BLOCKCHAIN AND BITCOIN SECURITY)

Bazı özel durumlar ve saldırılar hariç, çoğu durumda blok zincir altyapısı, iç mekanizmalarıyla kendi güvenliğini sağlar. Bütün sistemi tek bir merkezde toplayıp o merkezin güvenliğini sağlamak daha zordur. Örneğin hizmet reddi (DDOS) saldırısı tek bir merkeze çok kolay yapılabilir, fakat merkezi olmayan, her düğümde tüm kayıtların bulunduğu bir sisteme DDOS saldırısı yapmanın anlamı olmayacaktır.

Saldırıların dışında bir ülke blok zincirini kendi denetimi altına almak isteyebilir, örneğin bir devlet, *X* kişisi tarafından yapılan işlemleri engellemek istesin. Ağın %100 sahibi olmadıkça, bu mümkün değildir, blok zincirinde elbet bir madenci, *X* kişisinin işlemini blok zincirine dâhil edecektir. Sadece belli bir süre gecikme ve rahatsızlık yaşanacaktır, fakat sonuç değişmeyecektir. Diğer taraftan, bitcoin gibi kripto para sistemleri aşağıda değineceğimiz bazı saldırılara ve potansiyel risklere karşı açıktır.

5.1. Goldfinger veya %51 Saldırısı (Godfinger and 51% Attack)

Bir organizasyonun veya kişinin bitcoin ağ madenciliğinin büyük çoğunluğunu kontrol etmesidir. Bitcoin'in güvenliği, madencilik işiyle uğraşanlar tarafından çoğunluk olarak doğrulanmış bir kayıt olan blok zinciri tarafından sağlanır. Bitcoin düğümleri geçerli blok zinciri üzerinde birbirlerini doğrularlar. Eğer madencilerin çoğu tek bir varlık(kişi veya kurum) tarafından kontrol edilirse, hangi işlemin onaylanıp onaylanmayacağına bu varlık karar verebilir[19]. Örneğin Ocak 2014'de Ghash isimli bitcoin madenci havuzu %42-%47 arası bir orana ulaşmıştır.

Bir kişi veya gurup, zincirin %51'ini ele geçirdiğinde hileli işlemler yapabilir, örneğin diğer işlemleri onaylamayıp, sadece kendi bitcoin'lerini birçok defa onaylayarak çift harcama yapabilir, başkalarının varlıklarını çalabilir. %51 saldırısı, teorik olarak mümkün olan, fakat çok düşük olasılıkla gerçekleşebilecek bir saldırı türüdür[17,18].

Normalde bir kişinin kazanabileceği bir değere saldırması mantıklı değildir. İyi tarafta olup, blok doğrulamak daha faydalı bir iştir. Türev ve vadeli işlemler piyasası ile blok zincirine saldırarak kazanma pozisyon alınabilir. James Bond'un Goldfinger filmindeki olaylara benzetilerek, bu saldırı şekli Goldfinger Saldırısı olarak da anılmaya başlanmıştır, Ayrıca, ağın %50'den fazlasına rüşvet vererek vb. yollarla sahip olunabilir, rüşvet saldırısı ayrı başlık altında incelenmiştir.

Bu saldırıya karşı savunma mekanizması olarak;

(i) her bir işlem tam olarak tamamlanmadan yapılacak doğrulama sayısı artırılabilir. Örneğin, %51 saldırısına karşı, Feathercoin doğrulamayı 6'dan 100'e çıkarmış, Reddcoin satıcıları ise doğrulamayı 6'dan 60'a çıkarmıştır.

(ii) Saldırı yapan varlık boykot edilebilir, özüt oranı %51 altına düşürülebilir.

(iii) Blok içerisinde tutulan işlemler arasında da blok zinciri benzeri bağlantı kuran 2P-PoW[22] kullanılabilir. Bu protokolde ile her işlem bir önceki işlemin özütünü tutar ve saldırı meydana geldiğinde sorun anlaşılır.

(iv) Teorik bir çözüm olarak, büyük havuzların DDOS ile saldırı yapan varlığı yavaşlatılarak, özüt oranı düşürmesi sayılabilir[23].

5.2. Çift Harcama Saldırısı (Double Spending Attack)

Bitcoin ağında iki farklı parasal işlemde aynı bitcoin harcaması eş zamanlı olarak gerçekleşirse, çift harcama(double spending) meydana gelebilir. Örneğin, art arda gönderilen iki farklı işlem çakışabilir.

X kötü niyetli bir müşteri olsun, *U* üreticisinden ürün almak istesin, bu kişinin oluşturduğu alış işlemi için A_U^X gibi bir işlem oluşturarak, *z* zamanında B_c bitcoin kümesini kullanmak isteyebilir. *X*, bitcoin ağında A_U^X 'i yayımlar, ***z'*** zamanda (*z'* yaklaşık *z*), *X* aynı bitcoinleri(B_c) kullanarak diğer bir işlem A_X^X işlemi başlatabilir. Bu senaryoda *X* tarafından çift harcama gerçekleşecektir.

Dağıtık zaman damgalı ve PoW tabanlı protokol, blok zincirinde eskiden yapılan işlemleri depolanmasında kullanılır. Böylece bir madenci gelen A_U^X ve A_X^X işlemlerine bakar, bir tanesini işletir, diğerini reddeder.

Madenci veya madencilerin bir bloğu kazma oranı, ilgili PoW uzlaşma protokolünün çözülmesine bağlı olduğundan, bu kişilerin bilgisayar gücü ne kadar fazlaysa, o kadar hızlı PoW'u çözerler ve tehlike yaratabilirler. Bilgisayar kaynağı dışında, çift harcama saldırısının gerçekleşmesi; ağ yayılma gecikmesi, bitcoin değiş-tokuş servislerinin bağlantısı, bitcoin ağındaki pozisyonları ve dürüst madencilerin sayısı gibi başka faktörlere de bağlıdır.

Savunma olarak, yalnızca harcanmayan bitcoinlerin, önceki işlem çıkışını takip eden işlemde kullanıldığından emin olarak, tüm işlemleri madenci ağı doğrular ve işletir. Bu kural, çift harcamalara karşı çalışma zamanında dinamik olarak işlettirilir[24].

5.3. Finney Saldırısı (Finney Attack)

Bir çift harcama saldırı biçimidir. Düşman A_X^X işlemini içeren bir bloku önceden kazar ve sonra A_U^X satın alma işlemini için aynı bitcoin'i *U* üreticisi için oluşturur. Madencilikle elde edilen blok ile ilgili ağ bilgilendirilmez ve *X* düşmanı A_U^X işlemi, *U* üreticisi tarafından kabul edilene kadar bekler. Diğer taraftan *U* üreticisi, sadece madencilerden A_U^X'nin doğru olduğuna dair doğrulama alınca ve blok zincirine eklendiği bildirilince sadece A_U^X işlemini kabul eder.

Bir defa *X* düşmanı *U* üreticisinden ürün alınca, saldırgan önceden kazdığı bloğu ağda serbest bırakır, böylece var olan çatallanma ($B_{çatallanma}$) ile aynı uzunlukta blok zinciri çatallanmasını ($B'_{çatallanma}$) oluşturur. Bundan sonra gelecek kazılan blok, $B_{çatallanma}$ yerine $B'_{çatallanma}$ olacaktır. Sonra bitcoin ağındaki kurallara göre tüm madenciler $B'_{çatallanma}$ üzerine zinciri inşa edeceklerdir. $B'_{çatallanma}$ ağdaki en uzun zincir olunca, tüm madenciler $B_{çatallanma}$'u yok sayacaktır ve bu nedenle $B_{çatallanma}$'taki A_U^X içeren üst blok geçersiz olacaktır. Sonuçta, A_U^X geçersiz olunca, müşteri A_X^X işlemi ile parasını geri alacak fakat *U* üreticisi ürünü kaybedecektir.

Çözüm olarak, Finney saldırısından kaçınmak için, ürünü müşteriye göndermeden önce üretici, çoklu doğrulamayı beklemelidir[25]. Çoklu doğrulamayı beklemek sadece saldırgan için çift harcama saldırısını zorlaştıracaktır, fakat çift harcama saldırısının gerçekleşme olasılığı yine mümkündür.

5.4. Vector76 Saldırısı (Vector76 Attack)

Çift harcama saldırısının farklı bir biçimidir. Dijital pazar yeri ismi verilen bitcoin satın alma, satma veya diğer

değerlerle bitcoin'i takas etme işlemine "Bitcoin değiş-tokuşu(exchange)" denmektedir.

Bu tip saldırıda saldırgan (*X*), mevduat(depozito) uygulanan işlemi içeren kazılan bloğu alıkoyarak bekletir. Ardından gelecek blok duyurusunu bekler ve zaman geldiğinde değiş-tokuş için son kazılan blokla birlikte önceden kazılmış bloğu direkt olarak veya yakınındaki eş düğüm aracılığıyla Bitcoin piyasasına gönderir. Bu durumda, bazı yakın eşler de önceden kazılmış bloğu ($B'_{çatallanma}$) içeren zinciri, ana zincir gibi düşünürler.

Saldırgan, önceki işlemde depozit olarak verilen aynı paraların değiş-tokuşunun iptal edilmesini içeren diğer bir işlemi hızlıca gönderir. Eğer aynı zamanda, saldırgan tarafından kullanılan işlemi içermeyen bir çatallanma ($B_{çatallanma}$) paraların kaybolmaması için depolanırsa, depozito geçersiz olacaktır fakat saldırgan tarafından iptal işlemi zaten gerçekleştirilmiş olacaktır. Böylece değiş tokuş işleminde kripto paralar kaybedilecektir[26]. Bu saldırıya karşı çözüm olarak yine çoklu doğrulama kullanılabilir.

5.5. Kaba Kuvvet Saldırısı (Brute Force Attack)

Finney saldırısının geliştirilmiş halidir. Daha yetenekli olan saldırgan bu saldırıda, ağdaki n düğümü kontrol altına alır. Bu düğümler beraberce, çift harcama saldırısını gerçekleştirmek amacıyla özel bir madencilik şeması üzerine çalışırlar. Önceki durumda olduğu gibi saldırgan, özel blok zincirini ($B'_{çatallanma}$) genişletmek üzere çalışır. Üreticinin işlem kabul etmeden önce *x* tane onay beklediğini farz edelim, sonra da *x* onaydan sonra ürünü göndersin. Daha sonra *x* tane bloğu kazarak ağa bıraksın. $B_{çatallanma}$'dan daha uzun olduğu için $B'_{çatallanma}$ ağdaki diğer madenciler tarafından kabul edilecek ve genişletilecektir[27]. Bu durum sonucunda Finney saldırısı ile aynı etkiyi yapacak ve çift harcama saldırısı gerçekleşmiş olacaktır. Dolayısıyla bu saldırı, çift harcama saldırısının meydana gelmesini kolaylaştırmaktadır.

5.6. Denge Saldırısı (Balance Attack)

Blok zincirinde, PoW tabanlı uzlaşma mekanizmasına yapılan saldırı şeklidir. Bu saldırı, dengelenmiş madencilik gücüne sahip birçok madenci alt grubu arasındaki ağ iletişimini geciktirmekten ibarettir.

Natoli ve arkadaşları[28] tarafından, dünya çapındaki 70 finansal kurum tarafından oluşturulan R3 konsorsiyumuna ait özel blok zinciri üzerinde teorik analiz yapılmıştır. Bu çalışmada, ağ haberleşmesindeki gecikme ile Ethereum'a çift harcama saldırısı yapmak için ihtiyaç duyulan madencilik gücü arasında denge olduğu belirtilmiştir. Dolayısıyla, bu saldırı şekli Ethereum ve özel blok zincirlerde de geçerlidir. Ethereum'un kullandığı GHOST[13,14] uzlaşma protokolü üzerinde de etkilidir.

5.7. Sybil Saldırısı (Sybil Attack)

Kablosuz algılayıcı ağlar gibi birçok ağ sistemine yapılan eski saldırı tiplerinden birisidir. Sybil saldırısı ile madenci, birçok sahte sanal düğüm oluşturur. Bu düğümler yanlış bilgi göndererek, hem ağı gereksiz olarak meşgul edip yavaşlatır hem de yanlış bilgi araya karıştırarak sistemi çökertmeye çalışırlar[29]. Örneğin, oylama sonucu negatif iken pozitif gösterebilirler. PoW uzlaşma protokolü ile madenciler, matematiksel hesaplama işlemleri yaparak doğrulama gerçekleştirirler ve sanal düğümlerin gerçek düğüm olmadıkları anlaşılır.

Önceki bölümde de anlatılan PoW protokolünün işleyişine bakıldığında, bir defa kullanılan sayı(bks) değerinden başlanarak sürekli özüt algoritmasından geçirilip istenen sonuç el edilene kadar hesaplamalar yapılır. İstenilen sonuca ulaşınca bulmaca(puzzle) çözülmüş olur ve bulmacayı çözen bloku zincire ekler. Bu işlemi sanal düğümler yapamaz çünkü doğrulama işlemi için ağdaki düğümlerin yoğun hesaplama yapılması gerekir, sadece kimlik belirterek ağda aktif olarak yer almak mümkün değildir.

Sonuç olarak sanal düğümlerin yoğun hesaplama yapamayacağı ön görüsünden yola çıkılarak, Sybil saldırısının yapılamayacağı düşünülmektedir.

5.8. Netsplit ve Eclipse Saldırısı (Netsplit and Eclipse Attack)

Eclipse ve Netsplit saldırısında, blok zinciri ağ yapısına yapılan saldırıdır, bu saldırıda düşman eşler arası ağın(P2P) kontrolünü elinde tutmaya çalışır. Eşler arası ağda kurban, düşman tarafından kuşatılıp ağın geri kalanından izole edilir. Bu saldırı şekli %51, Çift harcama ve bencil madencilik saldırısının gerçekleşmesi için zemin oluşturmaktadır.

Marcus ve arkadaşları tarafından yayınlanan bir çalışmada[30], komşu düğüm keşfi amacıyla eşler arası ağa yapılan Eclipse Saldırısı ile ağ kaynakları sömürülmüştür. Sadece tek IP adresine sahip iki düğüm ile saldırı başlatılmış, daha sonra kurbanın gelen ve giden tüm bağlantılarını kontrol altına alarak ağın geri kalanından ayrıştırılmıştır. İlgili çalışmada, Ethereum ağının zayıflığı üzerinde durulmuştur.

Bu saldırıya karşı önlem olarak iki çözüm önerilmiştir. (i)Gelen bağlantıları pasif yapmak, (ii) belirli giden mesajları seçerek, bilinen(beyaz liste vb. listede yer alan) veya iyi bağlantı yapılmış eş düğümlere gönderme[31] sayılabilir.

5.9. Madenci Havuzuna Saldırılar (Mining Pool Attacks)

Madenci havuzuna yapılan saldırılar iç saldırılar ve dış saldırılar olmak üzere iki kısma ayrılır. İç Saldırılarda, madenciler ödülün dağılımından daha fazla bir miktarı havuzdan kötü niyetli bir şekilde toplar veya havuzun işleyişini bozarlar. Dış Saldırılarda ise madenciler yüksek özüt gücünü kullanarak çift harcama gibi saldırıları gerçekleştirirler. Eğer düşman, havuzun %30 özüt oranına(HR=hash rate) sahip ise, her kazılan blok için ödül paylaşımından 0.3 bitcoin ödül alacaktır. Ödüllerden elde ettiği bu miktar ile daha fazla madencilik için yatırım yapacak ve hissesini daha da artıracaktır. Mevcut HR'nin %1'i kadar zenginleşecektir. Standart madencilik

stratejisinde %1 eklenen HR için ancak 0.0069 bitcoin ek gelir kazanacaktır.

Havuzdan parça alma stratejisini gerçekleştirerek, saldırgan kendi havuzundan ödül alırken, diğer havuzlardan da %1 HR'sini paylaşarak ek ödüller alabilecektir. Bu kötü niyetli davranış, çok büyük miktarda işlemler yapılmadığı sürecek dikkat çekmeyecek ve tespit edilemeyecektir.

5.9.1. Blok Tutma Saldırısı (Block Witholding Attack)

Blok tutma saldırısında (BWH), bencil madenciliğe benzer şekilde düşmanlar blokları ellerinde tutarlar fakat asla paylaşmazlar. Böylece havuz gelirini engellemiş olurlar[32].

Havuz gelirini engellemek için, PPoW'den oluşan kazılmış blokları gönderirken FPoW'leri göndermezler. Aslında kaynaklarda[33], sabotaj ve pusuya yatma olmak üzere iki tip blok tutma saldırısından bahsedilir. Sabotaj saldırısında, düşman bir bitcoin kazanmaz, fakat diğer havuz üyeleri bitcoin kaybeder. Pusuya Yatma saldırısında ise düşman, bencil madencilik saldırısına benzer şekilde k tane blok gizleme gerçekleştirir.

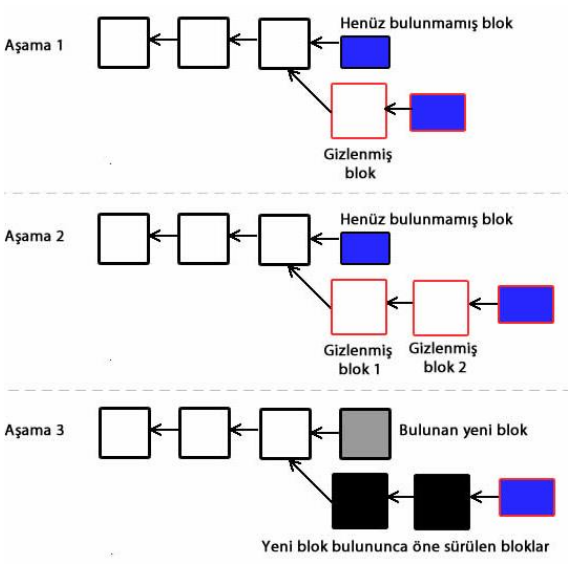
Bag ve arkadaşları[32], herhangi bir madenci havuzunda gerçekleşebilecek blok tutma saldırısına karşı iki öneride bulunmuşlardır. İlk olarak, yeni bir dâhil olma şeması geliştirmiş, ikinci olarak blok yapısı içeriğine yeni ekledikleri özüt işlemleri ile düzenbaz madencilere ve havuz yöneticilerine karşı bir önlem olarak sunmuşlardır.

5.9.2. Bencil Madencilik veya Blok Atma Saldırısı (Self Mining or Block Discarding Attack)

Bencil Madencilik ya da diğer popüler adıyla bilinen Blok Atma saldırısında, saldırganlar kazdıkları bloğu tutarak bilgi gizlemenin yanı sıra, bazı yollarla da sisteme zarar verirler. Örneğin, harcadıkları hesaplama gücünden daha büyük bir ödülü, adil dağıtım kurallarına ters bir şekilde elde edebilirler. Ayrıca diğer madencileri aldatarak, kaynaklarını yanlış yönde harcamaları için yönlendirebilirler[34, 35].

Bu saldırıda, genel zincirde dürüst madenciler yeni blok eklemeleri yaparak devam ederlerken ($B_{çatallanma}$), düşman özel zincire ekleme yapıp farklı bir çatal oluşturulmaktadır($B'_{çatallanma}$). Eğer bencil madenci $B'_{çatallanma}$ çatallanmasında uzun süre liderlik yaparsa, daha fazla ödül elde etme şansı artarken, dürüst madencilerin de para kaybetme oranı o miktarda artmaktadır.

Bencil madenciler kaybetme olasılığından kaçınmak için, $B_{çatallanma}$ ile $B'_{çatallanma}$ çatallanmaları aynı uzunluğa erişince daha önce kazdıkları blokları öne sürerler. Bundan sonra blok zincirindeki en uzun kuralı esas alındığından tüm madenciler, $B_{çatallanma}$ haline gelen $B'_{çatallanma}$ çatallanmasını kabul etmek durumunda kalırlar. Dürüst madenciler, daha önce blok zincirine blok olarak eklenen ödüllerini de bu durumda kaybederler[36].



Şekil 7. Bencil madencilik saldırısı.
(Self mining attack)

Analizler göstermiştir ki, bilgisayar kaynaklarının ve ödüllerin(dürüst madencilere ait) bencil madenci havuzunda boşa gitmesinin yanında, bencil madencilerin oluşturduğu havuz %50'yi aşarsa, blok zinciri sistemi için felaket olacaktır. Bencil madencilik her zaman kazançlı değildir, saldırgan kolayca tespit edilebilir ve pratik olmayan bir saldırı şeklidir[37, 38, 39].

Bu saldırıya karşı önlem olarak önerilen ZeroBlock tekniği[40] önerilmiştir. Bu savunma tekniği zaman damgası kullanmamaktadır. Eğer bencil bir düğüm, dürüst düğüm tarafından belirlenen zamandan daha fazla bir süre tutmak isterse, bloğun vadesi dolacak ve dürüst düğüm tarafından reddedilecektir. Bu çözümle, dürüst düğümler, blok tutma ile doldurulan zincirleri asla kabul etmeyeceklerdir. Artı olarak, dinamik bir ağda eğer dürüst bir düğüm ağa katılırsa, blok tutma ile bozulmuş zincirleri doğru şekilde teşhis edebilecektir.

Heilman[41] tarafından önerilen savunma mekanizmasında, işlenemez zaman damgaları kullanılmıştır. Bu çalışmada, bencil madencilik yapılabilmesi için saldırganın işi zorlaştırılmış, sahip olması gereken madenci gücü %25'den %32'ye çıkmıştır.

Diğer bir savunma önerisi de DECOR+[15,42,43] protokolüdür. İki veya daha fazla madenci eşit uzunlukta blokları çözerse, bencil madencilik için çıkar çatışması olacaktır. Rakip madencilerin her biri, kendi bloğunun ağdaki diğer madenciler tarafından en iyi zincir olarak seçilmesini istemektedir. Ağdaki tüm dürüst madenciler de herkesin ortak olarak bir zincirde karar kılmasını ister, böylece "geri dönme olasılığı" azalacaktır. İdeal çözüm, çakışan madencileri aynı dala(ağaç yapısında üst katmana) yönlendirmektir.
DECOR+ protokolü, madenciler arasında fazla etkileşim gerektirmeden, en doğru seçim için ekonomik teşvik ücretini belirler. DECOR+ ödül paylaşım stratejisidir, çatışmayı ekonomik olarak şöyle çözer; (i) Tüm tarafları aynı blok zinciri durum bilgisine eriştiği zaman, çatışma

deterministik olarak çözülür. (ii) Seçilen çözüm tüm madencilerin(çalışan iki madenci ve geri kalanın) gelirini maksimize eder. (iii)Çatışmanın çözülmesi ihmal edilebilecek, önemsiz bir zamanda gerçekleşir.

5.9.3. Blok Tutma Sonrası Çatallanma Saldırısı (Fork After Withholding Attack)

Blok tutma sonrası çatallanma(FAW) saldırısında, saldırgan BWH saldırısına eşit veya daha fazla ödül alabilir ve madenci havuzlarında BWH saldırısından dört kat daha sık rastlanan saldırı türüdür. BWH saldırısı gibi, saldırganın hesaplama gücü ve internet bağlantı durumuna bakılmaksızın kazanç elde edilebilir.

Tek havuz FAW saldırısında, BWH saldırısında olduğu gibi saldırgan hedef havuza dâhil olur ve FAW saldırısını havuza karşı başlatır. Düğüm FPoW'leri bir blok oluşturarak havuz yöneticisine gönderir, eğer havuz yöneticisi gönderilen FPoW'u kabul ederse, yayınlar ve çatallanma üretilmiş olur. Bundan sonra, tüm bitcoin ağı katılımcıları bir dal seçmelidir. Eğer saldırganın bloğu seçilirse, hedef havuz ödülü alır ve saldırgan havuzdan da ödül almış olur. Tek havuza saldırıldığında, FAW saldırganı, her durumda ekstra ödül kazanabilir. Yapılan hesaplamalara göre, tüm bitcoin ağının %20'sini temsil eden büyük bir havuzda FAW saldırganı, BWH saldırganına göre bir ile dört katı daha fazla ekstra ödül kazanır.

Çoklu havuz FAW saldırısında, saldırgan ödül miktarını artırmak için n tane havuza eş zamanlı FAW saldırısı düzenler. Örneğin saldırgan 4 havuza karşı saldırı gerçekleştirirse, BWH saldırısından %56 daha fazla ekstra ödül kazanacaktır.

FAW Saldırısını oyun teorisine göre, iki havuzun birbirine yaptığı bir saldırı üzerinde inceleyelim, oyunda Nash Dengesi vardır. Ancak BWH saldırısından farklı olarak daha büyük havuzun her zaman kazanacağı koşulu vardır. Bu durumda madencinin ikilemi olmayabilir. Bu nedenle, iki havuzun saldırıya karar verip vermediği FAW saldırı oyununun dengesi bir Pareto optimal(seksene yirmi kuralı) olabilir[44].

5.9.4. Havuz Sıçrama Saldırısı (Pool Hoping Attack)

Bu saldırıda, bencil madenciliği gerçekleştirmek amacıyla havuzdaki hisse sayısı hakkındaki bilgiyi kullanır. Düşman yeni bir blok keşfetmek için, madenci arkadaşlarının hangi sayıda hisse gönderdiğini sürekli analiz etmektedir.

Bu saldırıdaki ana fikir, eğer büyük miktarda hisse zaten gönderilmişse ve o zamana kadar yeni blok bulunamamışsa, düşman ödülden küçük bir hisse alabilecektir. Çünkü gönderilen hisseye bağlı olarak ödül dağıtılmaktadır. Böylece, düşman için diğer havuza geçmek veya bağımsız olarak madencilik yapmak daha kazançlı olabilecektir[45,46].

Bu saldırıya savunma tekniği olarak; havuz içinde hisse paylaşım yöntemlerinden PPLNS[33,47] yani "N hisse başına ödeme" yöntemi seçilirse önlenmiş olur. Havuzdaki i. bloğu bulma ile (i+1). bloğun bulunmasına kadar geçen zamana "tur" denir, tur ne kadar uzun sürerse, her bir paylaşımın kazancı düşer. Bundan dolayı, havuza hissesini kısa turda paylaşan biri, uzun turda paylaşan birinden daha avantajlı olur. Böylece daha kısa sürede turu tamamlamak ve ödül almak için havuzda kalacaktır.

5.9.5. Rüşvet Saldırısı (Bribery Attack)

Saldırgan, rüşvet ile bilgisayar kaynaklarının büyük bölümüne kısa bir süre için sahip olur. Üç yolla ağda gerçekleşebilir. Bant dışı ödeme, Negatif ücretli madenci havuzu ve çatallanma ile bant içi ödeme.

Bant dışı ödemede, düşman direkt olarak bilgisayar kaynaklarının sahibine ödeme yapar, o da karşılığında düşman tarafından kendisine atanan blokları kazar.

Negatif Ücret Madenci Havuzunda ise saldırgan daha yüksek ödeme yaparak havuzun istenilen şekilde biçimlendirilmesini yapar.

Çatallanma aracılığıyla bant içi ödemede ise saldırgan herhangi bir madenci tarafından serbest şekilde alınabilecek rüşvet ücretinin olduğu bir çatallanma oluşturarak, rüşvet vermeye kalkışır. Saldırganın yüksek özüt gücüne sahip olmasıyla birlikte, DDOS ve çift harcama gibi saldırıları gerçekleştirebilir[46]. Rüşveti alan madenciler kısa bir süre için fayda elde etseler de, daha sonra DDOS, Golfinger saldırılarıyla veya değiş-tokuş oranı ile uzun bir süre sonra kendileri için zarara dönüşecektir.

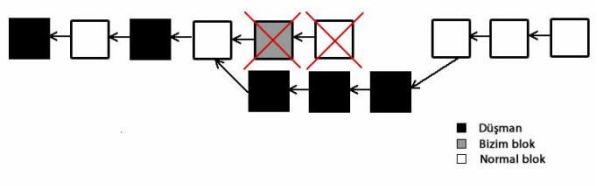
5.9.6. Cezalandırıcı Çatallanma ile Kara Listeye Alma (Blacklisting via Punitive Forking)

%50'den fazla özüt oranına sahip bir düşman, cezalandırıcı çatallanma ile kara listeye aldırabilir. Cezalandırıcı çatallanmanın amacı, belli kişilerin Bitcoin adreslerini engellemektir. Kara listeye alma üç şekilde gerçekleşebilir.

(i) Düşman, bizim bitcoin adresinden yapılan harcama işlemlerini içeren blok zincirinin genişlemeyeceğini duyurur. Eğer diğer madenciler blokta bizden gelen işlemleri kendilerine dâhil ederlerse, düşman hemen daha uzun başka bir blok zinciri çatallanması oluşturacaktır. Sonuçta, tarafımızdan oluşturulan işlemi içeren blok geçersiz kalmış ve asla yayınlanmamış olur, bizim işlemin arkasına blok ekleyen madenciler de ödüllerini kaybederler.

Aşağıdaki gibi Cezalandırıcı Çatallanma yapılabilmesi için, saldırganın özüt oranının %50'den büyük olması gerekmektedir. Şekilde görüldüğü gibi saldırgan, gri renkte gösterilen bizim işlemin zincirini devre dışı bırakarak başka bir çatal oluşturmuştur. Bu işlemde bizim blok engellenirken, arkamızdaki blok ya da bloklar da işlem dışı bırakılmış olur. Sonuç olarak, arkamızdaki

bloklar ödüllerini kaybetmiş olurlar ve asla yayınlanmazlar.



Şekil 8. Cezalandırıcı çatallanma ile ara listeye alma.
(Blacklisting via Punitive Forking)

5.9.7 Köpük Saldırısı (Feather Attack)

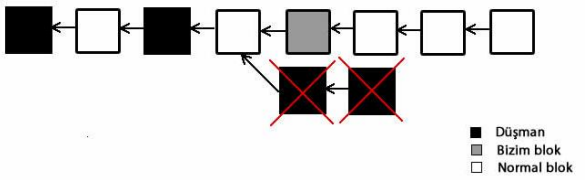
Köpük saldırısı, şartlar göz önüne alındığında Cezalandırıcı Çatallanma Saldırısı'na göre gerçekleştirilmesi daha kolay bir saldırıdır[48] çünkü cezalandırıcı çatallanma, en az %51 özüt gücüne(hashpower) sahip olunmasını gerektirir. Köpük saldırısında, saldırgan kötü niyetli madencilik yaparak, blok zincirinde bizim işlemi içeren bloğu görürse çatallanma girişiminde bulunacağını duyurur, fakat belli bir süre sonra vazgeçer.

Bloklarda doğrulama için genelde varsayılan olarak 1 verilir, bu değer güvenlik için yeterlidir, çoğu kişi de doğrulama için 3 değerini seçer, böylece işlemin geri dönmemesi garantilenmiş olur. Örneğin bizim bloğumuzda saldırgan, tx işleminde r tane doğrulama yaptıktan sonra bırakabilir.

Sahip olduğumuz madencilik gücü oransal olarak q değerinde olsun ($0<q<1$). Sadece 1 onaydan sonra vazgeçeceğimizi düşünelim r=1 olsun. Bizim bloğun yetim kalma(zincirden ayrı kalma) oranı q^2 olacaktır. Eğer q=0.2 olursa, yetim kalma olasılığı %4 olacaktır, bu da iyi bir oran değildir. Bu örnekte, q yani ağ özüt oranı %20 olarak kabul edilmiş, bu bilgiden türetilen "saldırganın işlemleri engelleme olasılığı" %4 olmuştur. Bu bilgiden yola çıkarak diğer madenciler bizim işlemi dâhil ederlerse, düşük bir ihtimal kendi blokları yetim kalacaktır[49]. Oyun teorisine göre madencilerin ikilemi; "işlemi dâhil etmeli mi yoksa etmemeli mi?", şeklinde olacaktır. Aşağıdaki formülle ikilemin ağırlığı daha iyi anlaşılabilir. Beklenen değer(BD), Blok Ödülü (B), İşlem ücreti (U) olmak üzere;

BD(Bizim blok dâhil edilirse) = $(1-q^2)$ *B + U
BD(Bizim blok dâhil edilmezse) = B

Bu sonuca göre, diğer madencilerin bizim işlemi kabul etmesi v e teşvik edici olarak kalması için blok ödülünün $(1-q^2)$ katı kadar daha fazla ödemeliyiz. Bu saldırıya karşı savunma olarak doğrulama sayısını çok yüksek değerlere çıkarmak, saldırganın daha fazla vakit harcamasına neden olacaktır. Fakat yine tam bir çözüm olamaz.



Şekil 9. Köpük saldırısı
(Feather Attack)

6. SALDIRILARA KARŞI SAVUNMA (DEFENSE AGAINST ATTACKS)

Tüm saldırı tipleri incelendiğinde, blok zinciri sisteminde güçler dengesinin önemli olduğu görülmektedir. Eğer bir madenci(veya madenci havuzu) ağın geri kalanından daha hızlı madencilik yapabiliyorsa, belli bir süre sonra %51 özüt oranının üzerine çıkacaktır. Daha hızlı işlem yapmak için geliştirilen özel donanımlar ve madenci havuzlarının yüzde olarak büyümesi saldırı risklerini artırmaktadır. Düşman, %51 oranına da rüşvet vb. yollarla da rahatlıkla çıkabilir, devletler veya büyük şirketler %51'i geçen madenci havuzları kurup, sistemi kontrol altına almak isteyebilir. Kripto para sistemlerine ilginin artması ve farklı yelpazede kullanıcıların olması yani sistemin tek bir varlığın kontrolünde olmaması, sistemin ayakta kalması için gereklidir. Eğer %51 aşılırsa, Çift Harcama, Eclipse, Goldfinger ve Cezalandırıcı Çatallanma gibi birçok saldırının gerçekleşmesi kolaylaşacaktır.

PoW protokolünün yavaşlığına çözüm bulmak için geliştirilen GHOST gibi protokoller, hızlı olmasına ve TPS'i artırmasına rağmen yeterince doğrulama yapılmadığından başka saldırıların önünü açmıştır. Sisteme gerçekleştirilen saldırıların büyük çoğunluğu doğrulama sayısı artırılarak saldırganın işi zorlaştırılabilir ya da atlatılabilir. %51, Finney, Vector76 ve Köpük gibi saldırılar için önleyici bir unsurdur. Doğrulama sayısını artırmak, işlemlerin beklenenden daha uzun sürmesine neden olur. "Yüksek güvenlik mi, yoksa işlem hızlılığı mı?" sorusu süregelen bir tartışma konusudur, bu seçin kullanıcıya bırakılmıştır. Yeni geliştirilen para birimleri de varsayılan doğrulama sayısını yüksek değerlerde tutmaktadır.

Tablo 2. Saldırılar
(Attacks)

Saldırı	Karşı Önlem
%51 veya Goldfinger	Doğrulama sayısını artırmak, saldırganı tüm madencilerin boykot etmesi ve özüt oranın %51 altına düşürülmesi, 2P-PoW protokolü[22] ile blok zincirinde olduğu gibi işlemleri birbirine bağlama. DDOS ile büyük özüt oranına sahip havuzlara karşı saldırı yapması[23]
Çift Harcama	Doğrulama sayısını artırmak, ağ içerisine gözlemciler yerleştirerek satıcıyı tehlike anında uyarma.
Finney	Doğrulama sayısını artırma.
Vector76	Doğrulama sayısını artırma.
Kaba Kuvvet	Ağ içerisine gözlemciler yerleştirerek satıcıyı tehlike anında uyarma.
Denge	PoW protokolü kullanılması
Sybil	PoW Protokolü kullanılması
Netsplit ve Eclipse	Gelen bağlantıları pasif yapmak, belirli giden mesajları seçerek, bilinen madencilere(beyaz

Saldırı	Karşı Önlem
	liste vb. listede yer alan) veya daha bağlantı yapılmış eş düğümlere gönderme[31]
Blok Tutma	Kriptografik taahhüt şemaları[32] Sadece güvenilen ve bilinen madencileri havuza alma, beklenilenin altında gelir elde edildiğinde havuzu dağıtma veya kapatma[34].
Bencil Madencilik veya Blok Atma	ZeroBlock tekniği[40], Heilman Savunma Önerisi[41],DECOR+ Protokolü[42]
Blok Tutma Sonrası Çatallanma	Çözüm önerilememiştir, tartışmalar devam etmektedir.
Havuz Sıçrama	Havuzların PPLNS(Son N hisse başına ödeme) modeline geçmesi[33,47].
Rüşvet	Madencilere verilen ödül ve işlem ücretinin artırılması.
Cezalandırıcı Çatallanma ile Kara Listeye Alma	özüt oranın %51'in altına düşürülmesi, %51 saldırısı için alınan tüm önlemlerin uygulanması
Köpük	Doğrulama sayısını artırmak caydırıcı olabilir, böylece saldırgan daha uzun zaman harcayacaktır.

7. BLOK ZİNCİRİ ALTYAPISINDA KULLANILAN KRİPTOGRAFİ'NİN GELECEĞİ (THE FUTURE OF CRYPTOGRAPHY USED IN BLOCKCHAIN INFRASTRUCTURE)

Bu bölümde, blok zinciri yapısında güvenlik için kullanılan kriptografi tekniklerinin geleceğini inceleyeceğiz. Özüt algoritmalarında çakışma meydana gelebilir. Matematiksel olarak ifade edecek olursak; m ve m' farklı mesajlar, h() özüt fonksiyonu olsun h(m)=h(m') ise çakışma meydana gelmiştir. Bu durumda özüt fonksiyonu artık kullanılamaz. Çünkü ne olursa olsun, özüt fonksiyonu iki farklı giriş verisinden aynı çıkışı üretmemelidir [50]. Ayrıca "ön görüntü (pre-image)" saldırısı[51,52] özüt algoritmaları için gerçekleşebilir, bu saldırı belirli özüt değerinin bilinen bir mesaj için bulunmasıdır.

Şifreleme algoritmalarının güvenliği, aşağıdaki üç zor matematiksel yönteme bağlıdır.

a) Tam sayı faktörizasyon problemi
b) Ayrık Logaritma Problemi
c) Eliptik Eğri Ayrık Logaritma Problemi

Post Kuantum Kriptografi, kuantum bilgisayarının saldırılarına karşı güvenli kriptografik algoritmaları(genelde asimetrik anahtar algoritmalarını) ifade eder. Fakat 2018 itibariyle çoğu asimetrik algoritma, güçlü kuramsal kuantum bilgisayarları ile kırılabilir. Belirtilen matematiksel yöntemlerin hepsi güçlü kuantum bilgisayarı ile Shor'un algoritması kullanılarak belli bir süre sonra çözülebilecektir[53,54].

Simetrik algoritmalar ve özüt fonksiyonları halen kuantum bilgisayarlara karşı dayanıklıdır[55]. Grover'in algoritması simetrik şifrelemeye karşı saldırıları hızlandırmasına rağmen, anahtar uzunluğu iki kat artırılarak güvenli hale getirilebilmektedir.

8. SONUÇ VE GELECEK ÇALIŞMALAR (CONCLUSION AND FUTURE WORKS)

Bu çalışmada, Bitcoin ve Bitcoin'in kullandığı blok zinciri alt yapısına karşı farklı saldırılar incelenmiştir. Saldırı tekniklerinin büyük çoğunluğu son birkaç yılda ortaya çıkmıştır. İlk bölümde %51, Çift Harcama, Finney Saldırısı, Vektör 76, Kaba Kuvvet, Sybil ve Netsplit, Eclipse ve Denge gibi saldırı tiplerine değinilmiştir. Daha sonra madenci havuzlarına karşı saldırılar incelenmiştir. Bencil madencilik veya blok Atma, Blok Tutma(BWH), Blok Tutma sonrası çatallanma(FAW), Havuz Sıçrama saldırısı, Cezalandırıcı Çatallanma ile Kara Listeye Alma, Köpük Saldırısı ve Rüşvet Saldırısı incelenmiştir.

Son bölümde de Blok Zinciri altyapısında kullanılan Kriptografi'nin geleceği üzerinde durulmuş, Post Kuantum Kriptografi'ye değinilmiştir. Gelecekte birçok uygulama alanı bulacak olan bu teknolojinin güvenliğinin sağlanması, önem arz etmektedir. Mevcut saldırı teknikleri bu çalışmada detaylı incelenmiştir, fakat bazı saldırılara tam çözüm bulunamamıştır, gelecek çalışmalarda bu saldırıları önlemek ve farklı çözüm önerileri geliştirilmek amaçlanmaktadır. Ayrıca, yeniden tasarlanan kriptografi algoritmaları incelenerek, blok zinciri sistemin güvenli kalması için kuantum bilgisayarlara dayanıklı kriptografi algoritmalarının ortaya konması gerekmektedir.

KISALTMALAR (ABBREVIATIONS)

AES	Advanced Encryption Standard (Gelişmiş Şifreleme Standardı)
ASIC	Application Specific Integrated Circuit (Uygulamaya Yönelik Tümleşik Devre)
BWH	Block Withholding Attack (Blok tutma saldırısı)
CPU	Central Processing Unit (Merkezi İşlem Birimi)
DAG	Direct Acyclic Graph (Yönlü Çevrim Yapmayan Çizge ya da Yönlü Düz Ağaç)
DECOR	DEterministic COnflict Resolution (Deterministik Çatışma Çözümü)
DES	Data Encryption Standard (Veri Şifreleme Standardı)
DOS	Denial of Service Attack (Hizmet Reddi saldırısı)
DDOS	Distributed Denial of Service Attack (Dağıtık Hizmet Reddi Saldırısı)
ECC	Elliptic Curve Cryptography (Eliptik Eğri Şifreleme)
ECDSA	Elliptic Curve Digital Signature Algorithm (Eliptik Eğri Dijital İmzalama Algoritması)
FAW	Fork After Withholding (Blok tutma sonrası çatallanma)
FPGA	Field Programmable Gate Array (Alanı programlanabilir geçit dizileri)
FPoW	Full Proof of Work(Havuz yöneticisinin genel bitcoin ağında kullandığı protokol)
GPU	Graphics Processing Unit (Grafik İşlem Birimi)
HR	Hash Rate (Özüt Oranı)
IoT	Internet of Things(Nesnelerin İnterneti)
P2P	Peer to Peer Network (Eşler arası ağ)
PoS	Proof of Stake (Hisse İspatı)
PoW	Proof of Work (Çalışma İspatı)
PPLNS	Pay Per Last N Share (Son N hisse başına ödeme)
PPoW	Partial Proof of Work (Madenci havuzunda kullanılan, genel bitcoin sistemi için anlamı olmayan protokol)
RSA	Rivest, Shamir ve Addleman'ın geliştirdiği Asimetrik şifreleme algoritması
TPS	Transaction per second (Saniyedeki işlem sayısı)

KAYNAKLAR (REFERENCES)

[1] İnternet: D. Furlonger, J. Lopez, What CIOs Should Tell the Board of Directors About Blockchain, Gartner Research, https://www.gartner.com/doc/3606027/cios-tell-board-directors-blockchain, 01.08.2018.

[2] D. Chaum, "Blind signatures for Untraceable payments", *Advances in Cryptology: Proceedings of Crypto* 82, 199-203, Springer, 1983.

[3] İnternet: Coin Market Cap, List of cryptocurrencies, https://coinmarketcap.com/all/views/all/, 15.07.2018.

[4] İnternet: Bitcoin Bitcoin (BTC) price stats and information, https://bitinfocharts.com/bitcoin/, 15.07.2018.

[5] İnternet: S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, https://bitcoin.org/bitcoin.pdf, 06.07.2018.

[6] A. Zohar, "Bitcoin under the Hood", *Communication of the ACM*, 58(9), 104-113, 2015.

[7] W. Stallings, "A Blockchain Tutorial", *Internet Protocol Journal*, 20(3), 2-24, 2017.

[8] I. Lin, T. Liao, "A Survey of Blockchain Security Issues and Challenges", *International Journal of Network Security*, 19(5), 653-659, 2017.

[9] İnternet: N. Gopie, What are smart contracts on blockchain?, https://www.ibm.com/blogs/blockchain/2018/07/what-are-smart-contracts-on-blockchain,17.07.2018.

[10] İnternet: G. Jenkinson, GPUs And ASICs - A Never Ending Battle For Mining Supremacy, https://cointelegraph.com/news/blockshow-announces-blockshow-americas-2018-conference-in-las-vegas-august-20-21, 24.07.2018.

[11] A. Back, **Hashcash - A Denial of Service Counter-Measure**, CyperSpace, 2002.

[12] İnternet: Basic primer, Blockchain Consensus Protocol, https://blockgeeks.com/guides/blockchain-consensus/,18.07.2018.

[13] A. Narayanan, J. Bonneau, E. Felten, A. Miller, S. Goldfeder, **Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction**, Princeton University Press, 2016.

[14] Y. Sompolinsky, A. Zohar, "Secure high-rate transaction processing in bitcoin", **International Conference on Financial Cryptography and Data Security**, 507–527, 2015.

[15] Y. Lewenberg, Y. Sompolinsky, A. Zohar, "Inclusive block chain protocols", **International Conference on Financial Cryptography and Data Security**, Springer, 2015

[16] M. Conti, S. Kumar E, C. Lal, S. Ruj, "A Survey on Security and Privacy Issues of Bitcoin", *IEEE Communications Surveys & Tutorials*, ArXiv preprint, arXiv:1706.00916**,** 2018.

[17] M. Swan, **Blockchain blueprint for a new economy**, O'Reilly Media, Inc., 2015.

[18] İnternet: A. Rosic, 5 Blockchain Applications That Are Shaping Your Future, HuffPost, https://www.huffingtonpost.com/ameer-rosic-/5-blockchain-applications_b_13279010.html/,13.07.2018.

[19] J. J. Xu, "Are blockchains immune to all malicious attacks?", *Financial Innovation*, 2016.

[20] İnternet: M. Crosby, P. Nachiappan Pattanayak, S. Verma, V. Kalyanarama, Blockchain technology: Beyond bitcoin, http://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf, 2016.

[21] Internet: J. Sinnige, Blockchain: how a 51% attack works (double spend attack), https://medium.com/coinmonks/what-is-a-51-attack-or-double-spend-attack-aa108db63474 , 6.08.2018.

[22] İnternet: I. Eyal, E. G. Sirer, How to disincentivize large bitcoin mining pools, http://hackingdistributed.com/2014/06/18/how-to-disincentivize-large-bitcoin-mining-pools/, 31.07.2018.

[23] İnternet: A. Quenston, 4 Lines of Defence Against a 51% Attack, https://www.ccn.com/4-lines-defence-51-attack/, 31.07.2018.

[24] G. O. Karame, E. Androulaki, and S. Capkun, "Two Bitcoins at the Price of One? Double-spending attacks on fast payments in bitcoin,", **ACM Conference on Computer and Communications Security (CCS'12)**, 2012.

[25] İnternet: Y. Sompolinsky, A. Zohar, Bitcoin's Security Model Revisited, Cryptography and Security, ArXiv preprint, arxiv:1605.09193, 2016.

[26] İnternet: Fake bitcoins?, 2011, https://bitcointalk.org/index.php?topic=36788.msg463391#msg463391, 20.06.2018

[27] İnternet: J. Heusser, Sat solvingan alternative to brute force bitcoin mining, https://jheusser.github.io/2013/02/03/satcoin.html, 20.06.2018.

[28] C. Natoli, V. Gramoli, "The Balance Attack Against Proof-Of-Work Blockchains: The R3 Testbed as an Example", *CoRR*, 2016.

[29] J.R.Douceur, "The Sybil Attack", *Peer-to-Peer Systems Lecture Notes in Computer Science***,** 2429, 251–60, 2002.

[30] İnternet: Y. Marcus, E. Heilman, S. Goldberg, Low-Resource Eclipse Attacks on Ethereum's Peer-to-Peer Network, ePrint (Cryptology) Report 2018 / 236, https://eprint.iacr.org/2018/236.pdf, 27.07.2018.

[31] E. Heilman, A. Kendler, A. Zohar, S. Goldberg. "Eclipse attacks on bitcoin's peer-to-peer network", **USENIX Security**, Washington D.C., ABD, 129-144, 12-14 Ağustos, 2015.

[32] S. Bag, S.Ruj, K. Sakurai, "Bitcoin Block Withholding Attack: Analysis and Mitigation", *IEEE Transactions on Information Forensics and Security*, 12(8), 1967-1978, 2017.

[33] M. Rosenfeld, "Analysis of bitcoin pooled mining reward systems", *Distributed, Parallel, and Cluster Computing*, ArXiv preprint, arxiv:1112.4980, 2011.

[34] İnternet: N. T. Courtois and L. Bahack, On Subversive Miner Strategies and Block Withholding Attack in Bitcoin Digital Currency, Cryptography and Security, ArXiv preprint, arxiv:1402.1718, 2014.

[35] İnternet: L. Bahack, Theoretical Bitcoin Attacks with Less than Half of the Computational Power, Cryptography and Security, ArXiv preprint, arxiv:1312.7013, 2013.

[36] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable", **Financial Cryptography and Data Security: 18th International Conference**, Springer Berlin Heidelberg, 2014.

[37] J.Bonneau, A.Miller, J.Clark, A.Narayanan, J.A.Kroll, E Felten, "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies", **2015 IEEE Symposium on Security and Privacy**, 2015.

[38] İnternet: V. Buterin, Selfish Mining: A 25% Attack Against the Bitcoin Network, https://bitcoinmagazine.com/articles/selfish-mining-a-25-attack-against-the-bitcoin-network-1383578440/ , 29.07.2018.

[39] G. Karame, E. Androulaki, S.Capkun, "Double-spending Fast Payments in Bitcoin", **In Proceedings of the ACM Conference on Computer and Communications Security (CCS)**, ACM, 2012.

[40] S.Solat, M.Potop-Butucaru, **ZeroBlock: Preventing Selfish Mining in Bitcoin**, Sorbonne Universites, UPMC University of Paris, 2016.

[41] E.Heilman, "One weird trick to stop selfish miners: Fresh bitcoins, a solution for the honest miner",**International Conference on Financial Cryptography and Data Security**, 2014.

[42] İnternet: S. D. Lerner, DECOR+ Protocol, https://bitslog.wordpress.com/2014/05/02/decor/, 07.08.2018.

[43] İnternet: S.D. Lerner, Bitcoin Powered Smart Contracts, RootStock Platform Whitepaper,

https://bravenewcoin.com/assets/Whitepapers/RootstockWhitePaperv9-Overview.pdf, 03.08.2018.

[44] Y. Kwon, D. Kim, Y. Son, E. Vasserman, Y. Kim, "Be selfish and avoid dilemmas: Fork after withholding (faw) attacks on bitcoin", **ACM SIGSAC Conference on Computer and Communications Security**, ACM, 2017.

[45] J. Bonneau, "Why buy when you can rent?", **International Conference on Financial Cryptography and Data Security**, Springer, 2016.

[46] M. Rosenfeld, "Mining pools reward methods", **Presentation at Bitcoin 2013 Conference**, 2013.

[47] Y. Zolotavkin, J. Garcia, C. Rudolph, "Incentive Compatibility of Pay Per Last N Shares in Bitcoin Mining Pools", **International Conference on Decision and Game Theory for Security**, 2017

[48] İnternet: A. Miller, Feather-forks: enforcing a blacklist with sub-50% hash power, https://bitcointalk.org/index.php?topic=312668.0, 07.08.2018.

[49] İnternet: M. Fang, P. Hayes, Game Theory and Network Attacks: How to Destroy Bitcoin, https://www.bitcoin.org.hk/media/2017/05/How_to_Destroy_Bitcoin.pdf, 04.08.2018.

[50] P. Rogaway, T. Shrimpton, "Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance". **Fast Software Encryption**, Springer-Verlag, 2004.

[51] K. Aoki, J. Guo, K. Matusiewicz, Y. Sasaki, L. Wang, "Preimages for step-reduced SHA-2", **International Conference on the Theory and Application of Cryptology and Information Security**, Advances in Cryptology–ASIACRYPT 2009.

[52] İnternet: D. Khovratovich, C. Rechberger & A. Savelieva, Bicliques for Preimages: Attacks on Skein-512 and the SHA-2 family, **International Workshop on Fast Software Encryption**, 2011.

[53] P.Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", *SIAM Journal on Computing*, 26(5), 1484-1509, 1995.

[54] D. J. Bernstein, J. Buchmann, **Post-Quantum Cryptography**, Springer, 2009.

[55] D.J. Bernstein,"Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete?", **Proceedings 4th Workshop on Special-purpose Hardware for Attacking Cryptograhic Systems**, 2009.