Review Article/Derleme Makale

GAZİ
JOURNAL OF ENGINEERING SCIENCES

The intersection of Blockchain and Malware: A Comprehensive Review and Analysis

Egemen Taşkın[*a], **İbrahim Alper Doğru**[b]

Submitted: 17.11.2023 Revised: 21.12.2023 Accepted: 23.12.2023 doi:10.30855/gmbd.0705S07

ABSTRACT

Blockchain, as a type of distributed ledger technology, emerged as a reliable and transparent mechanism. Its key features are immutability, cryptographic encryption, auditability, and traceability. Blockchain technology, which started with the leadership of the financial sector, has spread to different sectors such as health, supply chain, real estate, law, and information security. Blockchain, integrated with technologies such as Industry 4.0, Internet of Things, Machine Learning and Artificial Intelligence, has caused both progress and challenges in the field of cybersecurity. Malicious actors produce and distribute blockchain-based malware using Industry 4.0 tools. This research contributes to one main issue: Examining current and advanced malware for blockchain systems and detection. In conclusion, this research highlights the critical importance of understanding the interaction between blockchain and malware. Revealing the emerging risks and challenges in this field, this study aims to equip researchers and cybersecurity practitioners with valuable knowledge to strengthen blockchain networks and effectively combat malicious threats.

Keywords: Blockchain, Malware, Machine Learning

[a,*] Gazi University,
Technology Faculty,
Dept. of Information Security Engineering
06560 - Ankara, Türkiye
Orcid: 0000-0001-8241-2145
e mail: egementaskin@gmail.com

[b] Gazi University,
Technology Faculty,
Dept. of Computer Engineering
06560 - Ankara, Türkiye
Orcid: 0000-0002-5979-4197

*Corresponding author:
egementaskin@gmail.com

Blokzincir ve Kötü Amaçlı Yazılımların Kesişimi: Kapsamlı Bir İnceleme ve Analiz

ÖZ

Blokzincir, dağıtık defter teknolojisinin bir türü olarak, güvenilir ve şeffaf bir mekanizma olarak ortaya çıkmıştır. Temel özellikleri değişmezlik, kriptografik şifreleme, denetlenebilirlik ve izlenebilirliktir. Finans sektörünün öncülüğünde başlayan blokzincir teknolojisi, sağlık, tedarik zinciri, emlak, hukuk ve bilgi güvenliği gibi farklı sektörlere yayılmıştır. Endüstri 4.0, Nesnelerin İnterneti, Makine Öğrenmesi ve Yapay Zekâ gibi teknolojilerle entegre edilen blokzincir, siber güvenlik alanında hem ilerlemeye hem de zorluklara neden olmuştur. Kötü niyetli aktörler, Endüstri 4.0 araçlarını kullanarak blokzincir tabanlı kötücül yazılımlar üretmekte ve dağıtmaktadır. Bu araştırma, blokzincir sistemlerine yönelik güncel ve ileri düzeydeki kötücül yazılımların incelenmesi ve bunların nasıl tespit edildiğini ele almaktadır. Sonuç olarak, bu araştırma blokzincir ve kötücül yazılımlar arasındaki etkileşimi anlamanın kritik önemini vurgulamaktadır. Bu alanda ortaya çıkan riskleri ve zorlukları ortaya çıkaran bu çalışma, araştırmacıları ve siber güvenlik uygulayıcılarını blokzincir ağlarını güçlendirmek ve kötü niyetli tehditlerle etkili bir şekilde mücadele etmek için değerli bilgilerle donatmayı amaçlamaktadır.

Anahtar Kelimeler: Blokzincir, Kötücül Yazılım, Makine Öğrenmesi

To cite this article: E. Taskin and I.A. Dogru, "The intersection of Blockchain and Malware: A Comprehensive Review and Analysis" *Gazi Journal of Engineering Sciences,* vol.9, no.4, pp. 58-69, 2023. doi:10.30855/gmbd.0705S07

1. Giriş (Introduction)

Genel olarak dağıtılmış defter teknolojisi olarak tanımlanan blokzincir, birbirini tanımayan bireyler veya uygulamalar arasında şeffaf bir şekilde güven sağlar [1]. Bu güven değişmezliğe, kriptografik şifrelemeye, denetlenebilirliğe ve çoğunlukla izlenebilirliğe dayanmaktadır [2]. Böylece birbirini tanımayan kimlikler arasında güven tesis etmek makul bir düzeye geldi. Blokzincir kullanımı, özellikle kripto para birimlerinin [3] yaygınlaşmasıyla birlikte kendisine daha geniş bir alan açmıştır. Bu noktada ana itici gücün finans sektörü olduğu söylenebilir. Ancak son zamanlarda finans dışında sağlık, tedarik zinciri, gayrimenkul, hukuk, bilgi güvenliği gibi farklı sektörlerden birçok kurum/kuruluş da blokzincir teknolojisinin sunduğu fırsatlardan yararlanmaya başlamıştır. Blokzincir, izin verilen (özel), yetkisiz (kamuya açık) ve hibrit (konsorsiyum) gibi seçeneklerin yanı sıra verilerin zincir üzerinde mi yoksa zincir dışı mı tutulacağına karar veren varlıklar tarafından kullanılabilir [5]. Endüstri 4.0'ın hayatımıza girmesiyle birlikte Nesnelerin İnterneti, Makine Öğrenimi ve Yapay Zekâ ile blokzincir teknolojisindeki gelişmeler siber güvenliği bir adım öteye taşımakta ve saldırıların özelliklerinde de ciddi gelişmelere neden olmaktadır [6]. Endüstri 4.0 teknolojik araç ve yöntemlerinin yardımıyla kötü amaçlı yazılım yaratıcıları, farklı türde bir blok zinciri kullanmayı ve savunucular tarafından kaldırılamayan kontrol bilgilerini yaymak için esnek tasarım ilkesini kullanmayı amaçlıyor [7]. Bu sebeplerden dolayı blokzincir teknolojisi ve kötücül yazılımları birlikte düşünmek gerekli hale gelmiştir. Bu çalışmanın temel araştırma katkısı; blokzincirleri hedefleyen son teknoloji kötü amaçlı yazılımların bir incelemesini sunmaktır. Bu makalenin geri kalanı şu şekilde düzenlenmiştir. Bölüm 2, bu çalışmanın oluşturulmasında kullanılan yöntemi açıklar. Bölüm 3'te blokzincirleri hedefleyen ve ona karşı savunma tekniklerini hedefleyen kötü amaçlı yazılımlara ve tespitine yönelik bir inceleme sunar. Bölüm 4, sonuç açıklamalarını ve tartışmayı sunar.

2. Yöntem (Method)

Bu araştırma, Sistematik Literatür Taraması metodolojisi ile yapılandırılmıştır. Tarama protokolü; kaynak seçimi, arama yöntemleri, kalite kriterleri ve veri sentezi stratejilerini belirlemeyi amaçlayan herhangi bir Sistematik Literatür İncelemesinin (SLR) kritik bir unsurudur [8]. Araştırma konusunda temel arama terimleri türetilmiştir. Arama sorgusu aşağıdaki gibi oluşturulmuştur: ("blockchain" veya "malware"). Web of Science ve Scopus gibi iki tanınmış dijital kütüphane üzerinden birincil çalışmalar için çevrim içi bir arama gerçekleştirilmiştir. İlk arama sürecinde 216 makale bulunmuştur. Daha sonra birincil çalışmaları seçmek için aşağıdaki dört adım uygulanmıştır:
Adım 1: Araştırma odakları uymayan çalışmaları elemek için başlıkları incelenmiştir.
Adım 2: Geriye kalan çalışmaların özetleri ve anahtar kelimelerini incelenmiştir. Eğer özetler veya anahtar kelimeler gerekli bilgiyi içermiyorsa, çalışmanın ilgili olup olmadığını belirlemek için sonuçlar ve sonuç bölümlerini incelenmiştir.
Adım 3: Farklı kütüphanelerden elde edilen aynı makaleler tespit edilip tekilleştirilmiştir.
Adım 4: Geriye kalan çalışmalar, Tablo 1'de belirtilen dahil etme ve dışlama ölçütleri kapsamında filtrelenmiştir.

Tablo 1. Yayın dahil etme ve dışlama ölçütleri

Dahil Etme Ölçütü	**Dışlama Ölçütü**
Sadece konferans bildirilerini ve bilimsel dergi makalelerini potansiyel çalışmalar olarak tut	Akademik olmayan makale ve bildirileri hariç tut
Sadece blokzincir ve kötücül yazılımları ele alan akademik yayınları tut	Yayınlanmamış çalışmaları, lisans üstü tezleri, teknik raporları, gazete makalelerini, posterleri ve kısa makaleleri hariç tut
Aynı araştırmanın ve aynı yazar(lar)ın en son versiyonunu tut	Aynı yazar(lar) tarafından yayımlanan akademik makalelerinin ön konferans bildirilerini hariç tut

3. Bulgular (Findings)

Günümüzde dijital tehditler, bilgisayar kullanıcılarını ve kurumları giderek daha karmaşık ve çeşitli biçimlerde hedef almaktadır. Taranan makalelerin incelenmesi neticesinde; blokzincir bağlamında bu tehditler arasında öne çıkan bazı önemli kategoriler; kötü amaçlı kripto madenciliği, fidye yazılımları ve oltalama saldırıları olduğu görülmüştür. Kötü Amaçlı Kripto Madenciliği, siber suçluların, kullanıcıların veya kurumların bilgisayar kaynaklarını izinsiz olarak kullanarak kripto para birimleri elde etmeye çalıştığı bir

yöntemdir. Fidye Yazılımları, dosyaları şifreleyerek erişimi engelleyen ve genellikle fidye talep eden kötü niyetli yazılımlardır. Oltalama ise sahte iletişim araçları veya web siteleri kullanılarak kişisel bilgilerin çalınmasını amaçlayan bir siber saldırı türüdür. Bu üç tehlikeli tehdidin detaylı bir şekilde incelenmesiyle, bu saldırılar blokzincir bağlamında detaylıca ele alınacak ve bunlara karşı hangi etkili önlemler geliştirildiği hakkında bilgi sağlanacaktır.

3.1. Kötü Amaçlı Kripto Madenciliği (Cryptojacking)

Kullanıcının rızası veya izni ile yapılan madencilik işlemine gönüllü madencilik(authedmine) denilirken; kullanıcının izni olmadan yapılan madencilik, kötü amaçlı kripto madenciliği [9] olarak adlandırılır. Kötü amaçlı kripto madenciliği temel olarak tarayıcı ve uygulama tabanlı olmak üzere iki kategoride incelenebilir. Tarayıcı tabanlı olanda, ziyaret edilen web sitesinden madencilik yapan JavaScript kodu veya web derlemesi indirilir ve tarayıcı aracılığıyla korumalı alanda(sandbox) çalıştırılır. Diğerinde ise madencilik gizli olarak arka planda kişisel bilgisayar uygulamaları veya mobil uygulamalar üzerinden yapılır. Blokzincir dünyasında birçok mutabakat protokolü olmasına rağmen en popüleri Bitcoin'de de kullanılan iş kanıtıdır (Proof of Work). En popüler olan Bitcoin, kimlikleri gizler ancak işlemleri izlenebilirdir. Ancak Monero tam bir anonimlik sağlar. Ayrıca Bitcoin madenciliği için ciddi kaynaklar (GPU, ASIC vb.) gerekli olsa da Monero isimli kripto para, CryptoNight iş kanıtı [10] mutabakat protokolünü kullanılarak düşük CPU kullanımı ile işlemleri gerçekleştirebilmektedir. Bu nedenle kötü amaçlı kripto madenciliği konusunda en çok tercih edilen kripto para birimlerinden biri Monero'dur.

3.1.1. Tarayıcı Temelli (Browser Based)

Günümüzde JavaScript kabiliyetleri açısından çok güçlü ve kullanımı popüler hale gelmiştir. JavaScript kullanılarak web uygulamalarının yanı sıra sunucu ve mobil uygulamalar dahi geliştirilebilmektedir. Bugün web tabanlı ön uç uygulamalarının neredeyse %98'i JavaScript [11] kullanmaktadır. Bu nedenle saldırganların hedefi haline gelmiştir. Kötü amaçlı kripto madenciliği dünyasındaki en bilinen komut dosyası, web sitesi sahiplerinin web sitelerine kripto madencisi koymasına izin veren bir hizmet olan CoinHive aracılığıyla yayınlanmıştır. Bu hizmet artık kullanılmasa da CoinHive betiği günde milyonlarca kez başka yöntemler aracılığıyla istemciler tarafından indirilmekte olup, bu da kötü amaçlı kripto madenciliğinin hala saldırganlar için hedef haline gelmesine neden olmaktadır [12]. Kötü amaçlı kripto madenciliğini tarayıcı aracılığıyla yaymanın başka bir yolu da içerik yönetim sistemleridir. Bu kripto madenciliği etkinleştirmek için hala bazı WordPress eklentileri bulunmaktadır [13]. Ayrıca saldırganlar, kripto madenciliği yapmaya imkân veren komut dosyasını yaymak için Google'ın DoubleClick reklam platformunu kullanmıştır [14]. Bunların yanı sıra, internet servis sağlayıcıları ve büyük kuruluşlar tarafından kullanılan MicroTik yönlendiricilerinin güvenlik açığı nedeniyle, Brezilya'da SSL kullanmayan web sayfalarına bazı kripto madencilik komut dosyaları eklenmiştir [15].

Tarayıcı temelli kötü amaçlı kripto madenciliğin tespiti NoCoin projesiyle başlamaktadır [16]. Bu proje, tarayıcı eklentisi ile DNS kara listeleri yayınlayarak web madenciliğini engellemeye amaçlamaktadır. Ancak zamanla birçok web sitesine kötü amaçlı kripto madenciliği sağlayan komut dosyalarının enjekte edilmesiyle, böyle bir kara liste tutmak mantıksız bulunmuştur. Kötü amaçlı kripto madenciliği Web Assembly yoluyla da yaygınlaştırılabilmektedir. Web Assembly (WASM); C, C++ gibi yüksek seviyeli programlama dilleri için taşınabilir program olarak hizmet eden bir ikili komut formatıdır. Web Assembly, web tarayıcılarında neredeyse yerel hızda kod çalıştıran düşük seviyeli bir sanal makine olacak şekilde tasarlanmıştır. Bu, geleneksel olarak yalnızca JavaScript gibi teknolojilerle zor olan yüksek performanslı uygulamaların web üzerinde gerçekleştirilmesini amaçlar. WASM programları manuel bir şekilde incelenerek Rüth ve ark. [17] web soketleri dinlenmiş ve WASM komutlarındaki diğer bazı ayırt edici özellikleri (XOR sayısı, kaydırma veya yükleme işlemleri) inceleyerek kötü amaçlı kripto madenciliği tespit edip sınıflandırmıştır. Sonuç olarak, 138 milyon domain üzerinde mevcuttan 5,7 kat daha fazla kötücül web sayfası tespit edilebilmiştir. Bunun yanında sözdizimsel özelliklere dayanan algılama yaklaşımları, saldırganlar tarafından kolaylıkla manipüle edilebilmektedir. Ancak, dinamik olarak elde edilen anlamsal kod özelliklerinin karıştırılması(obfuscating) daha zor olmakta ve bu nedenle madenci faaliyetlerinin tespitinde daha kullanışlı olduğu değerlendirilmektedir. SEISMIC [18], WASM komutlarındaki potansiyel kripto hırsızlığı saldırılarını semantik imza eşleştirmesi kullanarak tespit edebilmektedir. Destek Vektör Makineleri (SVM-Support Vector Machine) algoritmasını kullanan çalışma, %98 F1 değeri ile kötü amaçlı kripto madenciliği saldırılarını tespit edebilmekte ve bir tarayıcı eklentisi, vekil sunucu hizmeti veya güvenlik duvarı hizmeti olarak kolayca kullanılabilmektedir. Kripto hırsızlığını tespit etmek için kullanılacak bir diğer yöntem ise işlem kodu

(opcode) analizidir. Carlin ve ark. [19] kripto madenciliğinin dinamik işlem kodu analizini sunan ilk çalışmayı ortaya koymuştur. Bu çalışmada, CPU ile ilgili talimatları izlemek için OllyDbg etkinleştirilmiş ve ardından Intel x86/x64 mimarisindeki izlenen işlem kodları, makine öğrenmesinde kullanmak için CSV dosyasına aktarılmıştır. Çalışma, oluşturulmuş bir veri kümesi içindeki tarayıcı tabanlı kripto madenciliğinin Rastgele Orman (RF-Random Forest) algoritması ile %100'e varan doğrulukla tespit edilebileceğini ispat etmiştir. Outguard [20], büyük bir kripto madenciliği veri seti oluşturarak en iyi yedi özniteliği tespit etmiş, kötücül ve iyicil olanları sınıflandırmak için bir Destek Vektör Makinesi modeli kullanarak otomatik bir kripto hırsızlığı tespit sistemi ortaya koymuştur. Outguard; %97,9 doğru pozitif oranı ve %1,1 yanlış pozitif oranı elde etmiştir. Ayrıca Outguard, gereksiz kod blokları ekleme ve yeniden adlandırma gibi yöntemlerle yeniden oluşturulmuş kripto hırsızlığı ikili dosyalarıyla da test edilmiştir. %93 doğru pozitif oranı ve %1,2 yanlış pozitif oranı ulaşarak yanıltma (adversarial evasion) tekniklerine karşı toleranslı olduğu test edilmiştir. MineThrottle[21], tarayıcı içi kripto hırsızlığına karşı savunmanın başka bir yolunu sunmaktadır. Bu çalışma, blok düzeyinde program profili oluşturma adı verilen bir teknik kullanarak madencilikle ilgili kod bloklarını tanımlamakta ve WASM kodunu gerçek zamanlı olarak değiştirerek madencilik davranışını tespit etmektedir. MineThrottle daha sonra kullanıcı tarafından belirlenen politikalara göre madencilik davranışını yavaşlatabilmektedir. MineThrottle en popüler web sitelerinde değerlendirmiş ve tarayıcı içi kripto hırsızlığını tespit etme ve önlemede başarılı olduğunu ortaya koymuştur. Kötü amaçlı kripto madenciliği tespiti, klasik makine öğrenmesi algoritmaları ile yapılabildiği gibi derin öğrenme yöntem ve teknikleriyle de gerçekleştirilebilmektedir. MINOS [22], WASM teknolojisini kullanarak kripto korsanlık yapan kötü amaçlı yazılımları tespit etmek için derin öğrenmeyi kullanan bir tespit sistemidir. Sistem, iyicil web sayfaları ile yetkisiz madencilik için WASM kullananları ayırt etmek için mevcut kötü amaçlı ve iyicil WASM ikili dosyalarının veri kümesiyle eğitilmiş bir evrişimli sinir ağı (CNN-Convolutional Neural Networks) modelini kullanmaktadır. MINOS, WASM ikili dosyaları ve kötü amaçlı kripto madenciliğini içeren web sayfalarından oluşan iki veri kümesi kullanılarak değerlendirilmiştir. Sonuçlar, MINOS'un gerçek örneklerden oluşan derlenmiş bir veri kümesi üzerinde %98,97 doğrulukla WASM tabanlı kripto hırsızlığını tespit etmede son derece etkili olduğunu göstermiştir. Ek olarak MINOS hafif sıklet bir yapıya sahip olup hesaplama açısından ucuz ve platformdan bağımsızdır. Bununla birlikte, kripto korsanlığa yönelik kötü amaçlı yazılımların tespit edilmesi zordur. Çünkü iyi huylu web uygulamaları sıklıkla kripto korsanlığı yapan kötü amaçlı yazılımlarla aynı teknolojileri kullanmaktadır. Mevcut tespit yöntemlerinin, genellikle normal kullanıcılar tarafından erişilemeyen önemli düzeyde bilgisayar yönetimi uzmanlığı veya yürütme izinleri gerektirdiği gözlemlenmektedir. MinerAlert [23], kripto hırsızlığı faaliyetlerini gerçek zamanlı olarak tespit etmek için önerilmiştir. Kullanıcıların kullanımını kolaylaştırmak için bir tarayıcı uzantısı olarak tasarlanmıştır. Ancak MinerAlert'in tarayıcı dışındaki kripto hırsızlığı faaliyetlerini tespit edememesi, yanlış pozitif ve yanlış negatiflere ilişkin kapsamlı bir değerlendirmenin bulunmaması ve MinerAlert'in tarayıcı performansı ve kullanıcı deneyimi üzerindeki olası etkisi gibi bazı sınırlamaları bulunmaktadır. Hernandez-Suarez ve ark. [24] parmak izi tekniği, otomatik kodlama algoritması ve derin, yoğun bir sinir ağı kullanarak web tabanlı kripto hırsızlığını tespit etmek ve karakterize etmek için çok katmanlı bir yaklaşım önermektedir. Önerilen yöntem, normalleştirilmemiş ve normalleştirilmiş veri kümeleri üzerinde gerçekleştirilen deneysel testlerde %99'un üzerinde doğruluk oranıyla, web tabanlı kripto hırsızlığını tespit etme ve karakterize etmede yüksek başarım elde etmiştir. Ancak çalışmanın; yalnızca belirli bir veri kümesi üzerinde test edilmiş olması ve hesaplama maliyetinin ve diğer son teknoloji yöntemlerle karşılaştırmasının ele almadığı değerlendirilmiştir.

Sonuç olarak, web tabanlı ön uç uygulamalarda JavaScript'in popülaritesinin artmasıyla birlikte, kripto hırsızlığı saldırganlar için önemli bir hedef haline gelmiştir. CMS veya Google'ın DoubleClick reklam platformu gibi web sitelerine kripto hırsızlığı eklemenin çeşitli yolları olsa da kripto hırsızlığı faaliyetlerini tespit etmek ve önlemek için çeşitli tespit yöntemleri önerilmiştir. Tespit yöntemleri, sözdizimsel özellik tabanlı algılamadan anlamsal kod özelliği tabanlı algılamaya ve hatta CNN kullanan derin öğrenme tabanlı algılamaya kadar uzanmaktadır. Ancak, kripto hırsızlığı yapan kötü amaçlı yazılımları tespit etmek hala zordur ve mevcut algılama yöntemleri, önemli düzeyde bilgisayar yönetimi uzmanlığı veya yürütme izinleri gerektirir ve bunlara genellikle normal kullanıcılar erişemez. Bu nedenle, son kullanıcıları kripto hırsızlığı saldırılarının kurbanı olmaktan korumak için daha kullanıcı dostu ve erişilebilir tespit yöntemleri geliştirmeye yönelik araştırmaların sürdürülmesi önemlidir.

3.1.2. Ana Bilgisayar Temelli (Host Based)

Ana bilgisayar temelli kripto hırsızlığında, kötü amaçlı yazılım genellikle arka planda sessizce çalışır, önemli miktarda işlem gücü tüketir ve ısı üretir, bu da ana sistemi yavaşlatabilir ve potansiyel olarak donanım hasarına neden olabilir. Saldırgan, pahalı madencilik donanımına yatırım yapmak veya onu çalıştıracak

elektriğin bedelini ödemek zorunda kalmadan kripto para birimi kazanarak fayda sağlamaktadır. Ana bilgisayar tabanlı kripto hırsızlığı saldırıları genellikle hassas verilerin çalınmasını veya normal iş operasyonlarının kesintiye uğramasına sebep olmadığı için tespit edilmesi zor olabilmektedir. Ancak mağdur açısından artan enerji maliyetleri, azalan sistem performansı ve lisanssız yazılım çalıştırma nedeniyle potansiyel yasal sorumluluk gibi ciddi sonuçları doğurabilmektedir. Kripto hırsızlığı akıllı telefonları ve Nesnelerin İnterneti (IoT-Internet of Things) cihazlarını da hedef alabilmektedir. Android işletim sisteminde Google Play'e uğramadan uygulama dosyaları doğrudan internet üzerinden indirilip yüklenebilmektedir.

Alanyazında ana bilgisayar temelli kripto hırsızlığını tespit etmek için birçok sistem önerilmiştir. Önerilen sistemlerden ilki olan BotcoinTrap [25], ana bilgisayar tabanlı bir yaklaşım kullanarak Bitcoin madenciliği yapan zombi ağlarını(botnet) tespit etmeyi sağlamıştır. Tespit, uygulamaların en düşük yürütme düzeyinde çalıştırılarak dinamik analizi yoluyla sağlanmaktadır. Bu sistem, dinleyici bileşeninin yeni blokların özetlerini günlüğe kaydettiği ve dedektör bileşeninin kötü niyetli madencilik davranışını tanımlamak için bu günlükleri analiz ettiği asenkron mimariyi kullanmaktadır. BotcoinTrap yaklaşımı, mevcut ticari veya ticari olmayan Bitcoin madenci botnetlerin tespit yöntemleriyle karşılaştırılmamıştır. Ayrıca, değerlendirmesi simüle edilmiş Botcoin'lere dayanmakta olup gerçek madenci kötü amaçlı yazılımlarına karşı gerçek dünyadaki etkinliği belirsizdir. Ek olarak, BotcoinTrap'i gerçek zamanlı bir tespit sistemine uygulamada ölçeklenebilme ve performans konusunda bilgi verilmemiştir. Ayrıca, önerilen yaklaşımın sınırlamaları ve potansiyel yanlış pozitif/negatif oranları hakkındaki bilgiler yetersiz kalmaktadır. Başka bir çalışma [26], Android kötücül kripto madenciliği amaçlı uygulamaların tespiti ve tanınması için işlevsel ve istatistiksel özelliklerin bir kombinasyonunu kullanan makine öğrenmesi temelli hiyerarşik bir sınıflandırma yöntemi önermektedir. Çalışmada ayrıca, son dönemdeki kötü amaçlı yazılım tehdidi olan fidye yazılımına verilen özel önemden de bahsedilmekte; bu tehdidin yerini blokzincir üzerinde kripto para madenciliği aldığına da değinilmektedir. Her ne kadar makine öğrenmesi ile testlerin gerçekleşeceği ortam belirtilse de deneysel çalışmalar hakkında bilgi sunulmadığı için herhangi bir performans göstergesine rastlanmamıştır.

Berecz ve Czibula[27], kripto hırsızlığını tespit etmek için hem statik hem de dinamik olarak analiz eden bir sistem önermiştir. İyicil uygulamalar ile kripto korsanları arasında ayrım yapmak için seçilen özelliklere göre üç farklı denetimli öğrenme sınıflandırma modeli (SVM, RF, Çok Katmanlı Algılayıcılar (MLP-Multilayer Perceptron)) eğitilmiştir. Sistemin veri kümesi; Malshare, Ninite ve Filehippo dahil olmak üzere çeşitli kaynaklardan oluşturulmuştur. Modeller ortalama %92,46 doğruluk oranı elde etmiştir. Ancak çalışma, kullanılan veri kümesinin boyutu veya belirli özellikleri hakkında belirli ayrıntılar sağlamamakta ve seçilen özelliklerin sınırlamalarını veya eğitim verilerindeki potansiyel önyargıları ve kullanılan denetimli öğrenme sınıflandırma modellerinin veya herhangi birinin potansiyel sınırlamalarını tartışmamaktadır. Ayrıca, iyicil uygulamalar ile kötü amaçlı kripto madenciliği yapan uygulamalar arasında doğru bir şekilde ayrım yapılmasındaki olası zorluklar ve önerilen metodolojinin yeni veya gelişen kripto hırsızlığı türlerine ölçeklenebilirlik veya genelleştirilebilirlik açısından potansiyel sınırlamalar ele alınmamıştır.

Darabian ve ark.[28] kötü amaçlı kripto madenciliği yazılımlarının hem statik hem de dinamik analizi için derin öğrenme tekniklerini, özellikle Uzun Kısa Süreli Bellek(LSTM - Long Short-Term Memory), Dikkat Tabanlı LSTM (ATT(Attention)-LSTM) ve CNN kullanan bir sistem geliştirmiştir. Örnekleri sınıflandırmak ve kötü amaçlı kripto madenciliği yazılımlarını tespit etmek için bu yöntemleri işlem kodu dizilerine ve sistem çağrısı olaylarına uygulamıştır. Statik analiz için sistem, düşük hatalı pozitif oranıyla %95'lik bir doğruluk oranı elde etmiştir. Dinamik analiz için sistem, kötü amaçlı yazılımı çalıştırma ve sistem çağrı olaylarının sıralarını yakalamak için Cuckoo sanal makinesini kullanmıştır. Daha sonra, elde edilen veri setine derin öğrenme yaklaşımları uygulanarak %0,6'lık gibi düşük bir yanlış pozitif oranıyla, %99'luk bir doğruluk oranı elde edilmiştir. Çalışma, derin öğrenme tekniklerini kullanarak kötü amaçlı kripto madenciliği uygulamalarını tespit etmeye odaklanmakta olup karşılaştırma amacıyla diğer geleneksel veya derin öğrenme tabanlı olmayan öğrenme yaklaşımlarını sunmamaktadır. Ayrıca çalışma, pratik uygulamada potansiyel bir sınırlama olabilecek derin öğrenme modellerinin eğitimi ve dağıtımı için gerekli olan hesaplama kaynaklarının ayrıntılı bir analizini sağlamamaktadır. En önemlisi de kötü amaçlı yazılım geliştiricilerinin çalışmada önerilen tespit yöntemlerini atlamak için kullanabileceği kaçınma tekniklerine yönelik bir ifade de bulunmamaktadır.

Vesely ve Zadník[29], kripto para birimi madencilerini tespit etmek için madencilik modellerini belirlemek ve tespit edilen madencileri doğrulamak için ağ trafiğini analiz eden pasif/aktif trafik izleme ve büyük havuzlardan madencilik yazılımı ayrıntılarını toplayan ve bunları kolay erişim için sMaSheD adı verilen bir web uygulamasında saklayan bir madencilik sunucusu kataloğu yöntemini geliştirmiştir. Bu aracın

davranışını lisanslı madencilik yazılımlarıyla karşılaştırmış ve biri manuel olarak tasarlanmış, diğeri makine öğrenimine dayalı iki sınıflandırıcı ile değerlendirmiştir. İki aşamalı tespit şemasının tamamının makine öğrenmesi tabanlı sınıflandırıcıyla değerlendirilmesi neticesinde %100 gerçek pozitif ve gerçek negatif sonucu elde edilmiştir. Manuel sınıflandırıcı her sınıfın yaklaşık 10 örneğini doğru bir şekilde tanıyamamış olup; bu da yanlış pozitifler durumunda daha fazla sayıda proba yol açmıştır. Ancak, çalışma kapsamında üç büyük kuruluştan yalnızca üç alt ağa odaklanan deneylerin sınırlı ölçeği, tüm kurumsal ağların çeşitliliğini ve karmaşıklığını tam olarak temsil etmeyebileceği değerlendirilmiştir.

CCEC[30], çeşitli çevrimiçi veri kaynakların(Kaggle, UCI deposu, Buzzfeed, Socrata Açık Veri, Google Veri kümeleri, Wikipedia, Quandl, Quantopian ve Fixshare) kullanılarak kötü amaçlı kripto hırsızlığı yapan yazılımları tespit etmek için harcanan süreyi azaltmaya yönelik bir platform olarak kurgulanmıştır. Bu platform, verileri kümelemek ve küme sayısını tahmin etmek için hafif sıklet bir kümeleme topluluğu yöntemi olan Bayesci Konsensüs Kümelemeyi(Bayesian Consensus Clustering(BCC) kullanmaktadır. Ayrıca RF ve Uyarlanabilir Yükseltme(Adaboosting) dahil olmak üzere birden fazla algoritma, kötü amaçlı yazılımların tespiti için CCEC çerçevesinde temel sınıflandırıcılar olarak test edilmiştir. Yapılan deneysel çalışmalar neticesinde kripto hırsızlığını yapan uygulamaların tespitinde %99,87 doğruluk oranı ile başarım elde edilmiştir.

Başka bir çalışma [31], kripto hırsızlığı yapan kötü amaçlı yazılımlara yönelik, ağ kullanımı ve kriptografik kütüphanelere yapılan çağrılar gibi ek ölçümleri içeren, seçilen örneklere göre %93'lük bir doğruluk oranıyla sonuçlanan gelişmiş bir tespit programı önermektedir. Tespit işlemi, bir karar ağacı algoritması için parametreler olarak CPU kullanımı, CPU ve RAM kullanımı ve CPU kullanımının ikinci dereceden sapmasına dayanmaktadır. Çalışma, CPU tabanlı kripto hırsızlarına odaklanmakta ve GPU tabanlı kripto hırsızlarına yönelik bir deney bulunmaması nedeniyle önerilen tespit tekniğinin genelleştirilebilirliğini sınırlamaktadır. Ayrıca, deneylerin gerçek dünya senaryolarını doğru şekilde temsil etmeyebilecek bir sanal makine üzerinde gerçekleştirilmesi önemli bir sınırlılık oluşturmaktadır. Sonuçların güvenilirliğini ve genellenebilirliğini etkileyebilecek, test için kullanılan veri kümesinin boyutu ve çeşitliliği hakkında bilgi bulunmamaktadır. Diğer bir sınırlama ise, tespit programının etkinliği ve doğruluğu hakkında fikir verebilecek yanlış negatiflerin ve yanlış pozitiflerin ayrıntılı bir analizini sağlanmamasıdır.

Sonuç olarak, kötü amaçlı kripto hırsızlığının tespiti için farklı yöntemlerin önerildiği ancak her birinin avantajları ve sınırlamaları olduğu görülmektedir. Bu alandaki araştırmaların daha fazla çalışma ve genelleştirilebilirlik açısından daha fazla incelemeyi gerektirmektedir.

3.2. Fidye Yazılımı (Ransomware)

Fidye yazılımı, bir bilgisayar sistemine veya dosyalara erişimi engellemek amacıyla tasarlanan kötü amaçlı bir yazılım türüdür. Bir sistem fidye yazılımına maruz kaldığında, dosyalar şifrelenir ve genellikle kullanıcı veya kuruluşa bir fidye notu sunularak şifrenin çözülmesi için ödeme talep edilir. Genellikle bir fidye karşılığında, genellikle kripto parada ödeme yapılana kadar dosyalar şifrenmiş bir biçimde bekler. Blokzincir teknolojisi doğrudan fidye yazılımı ile bağlantılı olmasa da genellikle kripto paraların kullanıldığı fidye saldırıları için tercih edilen ödeme yöntemleri arasında bir bağlantı bulunmaktadır. Kripto paralar; sınır ötesi işlem kolaylığı, merkezi olmama özelliği, anonimlik sağlaması ve ödemelerin geri alınamaması gibi sebeplerden dolayı tercih edilmektedir. Günümüzde en popüler kripto paralarından biri olan Bitcoin fidye amaçlı da kullanılabilmektedir. Ancak Bitcoin işlemleri, takip edilmesi zor olsa da tamamen anonim değildir ve finansal hareketler IP adresleri ve para akışları aracılığıyla takip edilebilir. Elliptic gibi blokzincir istihbarat şirketleri, Bitcoin ağını analiz etmek ve şüpheli davranış kalıplarını belirlemek için yapay zekayı kullanarak kara para aklamanın tespitini kolaylaştırmaktadır. Blokzincir teknolojisini kötü amaçla kullanan yapılar yeni nesil kripto para birimlerini kullanarak tespit edilme olasılığını daha da azaltabilmektedir [32]. Çoğu kuruluşun fidye yazılımı saldırılarıyla baş etme konusunda siber güvenlik uzmanlığı veya deneyimi bulunmamaktadır. ABD sağlık kurumlarının %85'inin temel siber güvenlik görevleri için nitelikli personelden yoksun olduğu öne sürülmektedir [33]. Dünya Ekonomik Forumu, kripto para daha yaygın olarak benimsendikçe fidye yazılımı saldırılarının artabileceği değerlendirilmekte olup 2027 yılına kadar küresel Gayri Safi Yurt İçi Hasıla (GSYİH)'nın %10'unun blokzincirlerde depolanması da dikkat çekici bir durumdur [34].

Bitcoin'i kötücül amaçla kullananların tespiti ve takibi için Bitcoin'in blok yapısı izlenerek bazı çalışmalar yapılmaya başlanmıştır. Huang ve ark.[35] fidye yazılımı ödemelerini, kurbanları ve operatörleri iki yıllık bir süre boyunca izlemek için kullanılan ve fidye yazılımı ikili dosyaları, fidye ödemeleri, kurban telemetrisi ve

Bitcoin adreslerinden oluşan bir veri tabanı gibi çeşitli veri kaynaklarını birleştiren bir ölçüm çerçevesi sunmaktadır. Finansal işlemlerin izlenmesi ve BTC-e'nin para çekmek için bir Bitcoin ve nakit değişim ofisi olarak kullanımının belirlenmesi de dahil olmak üzere, fidye yazılımı ekosistemi ve bununla ilişkili üçüncü taraf altyapısının ana hatlarını çizmektedir. Çalışma, artık kullanılmayan bir Bitcoin borsası olan BTC-e'yi, birçok fidye yazılımı operatörünün kazançlarını nakde çevirmek için kullandığı ortak bir platform olarak tanımlamaktadır. Bu çalışmada, aralarında CoinVault, CryptXXX, CryptoDefense, CryptoLocker, CryptoWall, Dharma, Spora ve WannaCry'ın da bulunduğu sekiz fidye yazılım ailesinden uygulamalar sayesinde gerçek kurbanlardan fidye adresleri toplanmıştır. Ayrıca Cerber ve Locky fidye yazılım ailelerinden de tohum fidye adresleri elde edilmiştir. Sonuç olarak 19.750 kurbandan fidye maksatlı 16 milyon dolardan fazla transfer olduğu tespit edilmiştir. Clouston ve ark.[36] 35 fidye yazılımı ile ilgili işlemleri izlemek ve analiz etmek için halka açık Bitcoin bloklarında bırakılan ayak izlerini analiz etmiştir. Bu yöntemi uygulayarak, her bir fidye yazılımı ailesinin alt sınırdaki doğrudan mali etkisini tahmin etmekte ve fidye yazılımı ödemeleri için yasa dışı pazarın büyüklüğüne ilişkin istatistikler sağlamaktadır. 2013'ten 2017 ortasına kadar 35 fidye yazılımı ailesinin alt sınır doğrudan mali etkisinin en az 12.768.536 dolar olduğu değerlendirilmiştir.

Mohatar ve ark.[37] otomasyon ve adil değişim için akıllı sözleşmeleri ve kriptografik temelleri kullanan blokzincir tabanlı fidye yazılımı şemalarının kullanılmasını önermiştir. Bu öneriler Ethereum Ropsten test ağında uygulanmış ve tam bir fidye yazılımı kampanyası yürütmenin kurban başına sadece 3 cent dolar ek maliyet getireceği tespit edilmiştir. Uygun politikalar ve karşı önlemler geliştirmek için bu programları tanımanın ve incelemenin çok önemli olduğunu vurgulanmıştır. Ancak deneyler ve analizlerin, Ethereum Ropsten test ağında gerçekleştirilmesi; bu, önerilen şemaların gerçek dünya senaryosunda performansını ve ölçeklenebilirliğini doğru şekilde yansıtmayabileceği değerlendirilmiştir.

Özer ve diğerleri [38], veri toplamak ve siber suçlulara karşı yeterli yöntemler geliştirmek için küresel bir fidye yazılımı merkezinin kurulmasını önermektedir. Siber suçlulara karşı etkili yöntemler geliştirmek ve bu saldırıların arkasındaki kişi veya grupları tespit etmek için hem gelişmiş tespit ve önleme sistemlerine hem de veri toplanmasına ihtiyaç duyulduğu vurgulanmaktadır. Ayrıca ilgili Bitcoin adreslerini ve karanlık web sitelerini birbirine bağlamak için grafik bağlantısı analizinin kullanıldığı ve kara listeye alınan Bitcoin adreslerinin anonimleştirilmesine yardımcı olduklarından da bahsedilmektedir. Ancak Bitcoin işlemlerini ortaya çıkarmak veya Bitcoin işlemlerinin anonimliğini azaltmak için önerilen tekniklerin herhangi bir ampirik değerlendirmesinden veya testinden bahsedilmemiştir. CryptoDrop[39] veya ShieldFS[40] gibi mevcut fidye yazılımı tespit ve önleme sistemlerinin başarı oranlarına veya sınırlamalarına ilişkin kapsamlı bir analiz sunulmamıştır.

Karapapas ve diğerleri [41], gelişmiş gizlilik, otomatik ödemeler, düşük maliyet ve düşük genel gider sunan Ethereum akıllı sözleşmelerini ve Gezegenler Arası Dosya Sistemini(IPFS- InterPlanetary File System) kullanarak Hizmet Olarak Fidye Yazılımı (RaaS) kavramını ortaya atmıştır. Daha fazla etkinlik, gizlilik ve güvenlik için sıfır bilgi kanıtları ve anonim ödemelerin dahil edilmesiyle sistemin daha da geliştirilebileceği belirtilmektedir. Ancak bir failin, önerilen fidye yazılımını, saldırgan güvenlik araştırmaları için etik sınırlara uygun olarak, bir hizmet planı olarak serbest bırakmasına izin verebilecek ayrıntılı teknik hususlar sunulmamıştır.

Fidye yazılımlarına karşı jenerik çözümler sunulsa da doğrudan ilgili alana dair ihtiyaçlara yönelik çözümler de önem arz etmektedir. Örneğin, sağlık sektöründe klinik verileri yönetme ve koruma alanına giderek endişe yaratan konulardan biri, fidye yazılımı saldırılarının artması ve hastanelere ve ulusal sağlık bilgi hizmetlerine küresel olarak önemli tehditler oluşturan hassas bilgi ihlallerinin endişe verici şekilde ortaya çıkmasıdır. Mendes ve ark.[42] tarafından önerilen blokzincir çözümü, fidye yazılımı saldırılarını önleyerek Akıllı Ortam Destekli SAAL(Smart Ambient Assisted Living) veri güvenliğini artırmaktadır. Akıllı telefon tabanlı SAAL, verilerin bütünlüğünü ve gizliliğini sağlayarak yetkili paydaşlara özel kimlik doğrulama yaparak verilere erişmesine ve bunları değiştirmesine olanak tanımaktadır. Temel olarak blokzincir çözümü, kontrollü veri erişimini kolaylaştırırken SAAL hasta verilerini korumaktadır.

Fidye yazılımlarının tespiti istatiksel yöntemler ve makine öğrenmesi yoluyla da yapılabilmektedir. Akcora ve ark[43] fidye yazılımlarını tespit etmek için topolojik veri analizi yöntemini kullanmış ve mevcut sezgisel tabanlı yaklaşımlarla(RF, Ekstrem Gradyan Arttırma(XGBT-Extreme Gradient Boosting), Yoğunluk Tabanlı Uygulamaların Gürültülü Mekânsal Kümelenmesi(DBSCAN-Density-Based Spatial Clustering of Applications with Noise), K-Means) karşılaştırıldığında daha yüksek oranda doğrulukla tespite ulaşılmıştır. Ancak, topolojik veri analizi yaklaşımının sınırlamalarından açıkça bahsedilmemektedir. Ayrıca önerilen

metodolojinin ölçeklenebilirliği veya daha büyük veri kümeleri üzerindeki performansı hakkında herhangi bir bilgi sağlanmamıştır. Ek olarak, fidye yazılımı tespitinin etkinliğini etkileyebilecek yaklaşımlarının potansiyel yanlış pozitif veya yanlış negatif oranları tartışılmamıştır.

Turner ve diğerleri [44], kripto para işlem ağlarındaki fidye yazılımı saldırılarıyla ilişkili çekirdek düğümleri tanımlamak için ağ analizinin kullanımını önermektedir. Ağlardaki düğümlerin konumunu değerlendirmek ve kripto para birimi işlem ağlarındaki fidye yazılımı saldırılarıyla ilişkili riskli düğümleri belirlemek için denetimsiz makine öğrenmesi grafik algoritması olan DeepWalk kullanılmıştır. Ancak analiz sistemi, halen geliştirilme aşamasında olan ve grafik veri bilimi için Neo4j üretim kütüphanesinde yayınlanmayan DeepWalk algoritması tarafından üretilen grafik yerleştirmelerin kalitesine oldukça bağımlı olduğu değerlendirilmiştir.

Sonuç olarak, Bitcoin işlemleri izlenebilir olmasına rağmen fidye yazılımı saldırıları ve hassas bilgi ihlalleri, küresel olarak ciddi bir tehdit haline gelmiştir. Blokzincir ve diğer teknolojiler, bu tür saldırıları önlemek ve siber suçluları tespit etmek için potansiyel çözümler sunmaktadır. Ancak bu çözümlerin gerçek dünya senaryolarında ne kadar etkili olduğu, ölçeklenebilirlikleri ve sınırlamaları hakkında daha fazla araştırma ve test gerekmektedir. Ayrıca, siber güvenlik uzmanlarının eğitimi ve bilinçlenmesi ile bu tür saldırılara karşı daha etkili bir savunma sağlanabileceği değerlendirilmektedir. Fidye yazılımı saldırılarına karşı mücadelede çoklu ve entegre bir yaklaşımın benimsenmesi de önemli ve temel bir yaklaşımdır.

3.3. Oltalama (Phishing)

Oltalama, kişisel bilgileri sahte iletişimler veya web siteleri aracılığıyla çalmayı amaçlayan kötü niyetli siber saldırıların bir türüdür. Öte yandan, blokzincir teknolojisi verilerin güvenli ve merkezi olmayan bir şekilde kaydedilmesini sağlayan bir teknoloji olarak bilinmektedir. Oltalama veri güvenliğini tehlikeye atarken, blokzincir teknolojisi ise bu tür tehditlere karşı koruma sağlamaktadır. Bu iki kavram, siber güvenlik alanında önemli bir rol oynamaktadır. Her ne kadar birbirinin zıttı kavramlar gibi görünse de oltalama yoluyla Bitcoin veya diğer kripto varlıkların ele geçirilmesine veya cüzdan kimliklerine yönelik girişimler olmaktadır.

Xia ve ekibi [45], COVID-19 temalı kripto para birimi dolandırıcılıklarını araştırmak için hibrit bir yaklaşım kullanmıştır. Bu yaklaşım iki ana adımı içermektedir: 1) rapor edilen dolandırıcılıkların toplanması ve 2) alanlar ve tweet'ler gibi şüpheli varlıklardan toplanan bilgilere dayanarak açıklanmayan dolandırıcılıkların tespit edilmesi. Çalışmada toplam 195 doğrulanmış COVID-19 kripto para dolandırıcılığı ve bu dolandırıcılıklarla ilişkili 200'den fazla blokzincir adresi belirlenmiştir.

Holub ve Connor[45], kimlik avı kampanyalarını tespit etmek için hafif, ölçeklenebilir ve küresel olarak dağıtılmış bir doğal dil işleme temelli bir sistem kullanmıştır. Potansiyel kimlik avı alanlarını belirlemek için özellikle Cisco Umbrella çözümleyicileri tarafından yakalanan küresel DNS verilerinin analiz edilmesine odaklanmaktadır. Araştırmacılar ayrıca "Coinhoarder" kampanyası adı verilen bir Bitcoin kimlik avı operasyonunu takip etmek için Ukrayna Siber Polisi ile iş birliği yapmıştır. Bu, kanıt ve öngörü toplamak amacıyla kimlik avı halkasının faaliyetlerinin izlenmesini ve araştırılmasını içermektedir. Genel olarak çalışma, kripto para kimlik avının yükselişi ve bununla mücadele çabaları hakkında değerli bilgiler sunsa da teknik ayrıntılar, etkililik değerlendirmesi ve daha geniş kapsamlı sonuçlar açısından sınırlamalara sahiptir.

Guri[47], saldırganların hava boşluklu cüzdanlara sızmak için kullandıkları çeşitli yöntemleri tartışmakta; bunlara, cüzdan kurulumu sırasında kötü amaçlı yazılımın önceden yüklenmesi veya gönderilmesi veya çıkarılabilir medya yoluyla sisteme bulaştırılması da dahil etmektedir. Hava boşluklu cüzdanlardan özel anahtarların nasıl çalınabileceğini göstermek için fiziksel, elektromanyetik, elektrik, manyetik, akustik, optik ve termal yöntemler gibi farklı sızma tekniklerini değerlendirmiştir. Bazı gizli kanalları tespit etmek ve engellemek için davranış analizi, makine öğrenimi ve anormallik tespit teknikleri de önerilmiştir, ancak bunlar yüksek yanlış pozitif oranları durumu tartışmalı hale getirmiştir.

Sonuç olarak araştırmalar, blokzincir ile oltalama arasındaki ilişkiyi inceleyerek, bu alandaki zorlukları ortaya koymuştur. Örneğin, COVID-19 dolandırıcılıklarını araştıran bir çalışma, blokzincir ile ilişkilendirilen dolandırıcılıkları incelemiştir. Başka bir çalışma, kimlik avı kampanyalarını tespit etmek için blokzincir teknolojisini kullanmıştır. Ayrıca, cüzdan güvenliği üzerine yapılan araştırmalar, sızma teknikleri ve koruma yöntemleri hakkında bilgi sunmuştur. Bu çalışmalar, blokzincir ve oltalama arasındaki karmaşıklığı anlamamıza yardımcı olurken, daha fazla araştırma ve geliştirme gerekliliğini de vurgulamaktadır.

3. Sonuçlar ve Tartışma (Results and Discussion)

Siber güvenlik, günümüz dijital çağında bilgi teknolojilerinin yaygın kullanımıyla birlikte önemli bir konu haline gelmiştir. Bu bağlamda, kötü niyetli siber saldırılar giderek karmaşıklaşmakta ve çeşitlenmektedir. Kripto madenciliği, fidye yazılımları ve oltalama gibi saldırı türleri, siber güvenlik uzmanlarının karşı karşıya kaldığı ciddi tehditler arasında yer almaktadır. Bu makale, bu siber saldırı türleri ile blokzincir teknolojisi arasındaki ilişkileri derinlemesine inceleyerek, blokzincir teknolojisinin siber güvenlikteki potansiyel rolünü ele almaktadır. Kripto madenciliği, dijital varlıkların üretilmesi sürecini ifade eder ve genellikle siber suçlular tarafından kötü amaçlı bir şekilde kullanılır. Blokzincir, kripto paraların temel altyapısını oluşturan ve dağıtık bir yapıya sahip olan teknoloji olarak öne çıkar. Ancak, kripto madenciliğiyle ilgili sorunlar, blokzincirin güvenliğini zorlayabilir. Blokzincir ağlarındaki madencilik faaliyetlerini kontrol etmek ve istenmeyen madencilik girişimlerini tespit etmek için geliştirilen çeşitli yöntemlerle bu sorunlar ele alınabilir. Özellikle, blokzincir tabanlı güvenlik protokollerinin geliştirilmesi, kripto madenciliği tehditlerine karşı daha etkili bir savunma mekanizması sağlayabilir. Fidye yazılımları, bilgisayar sistemlerine sızarak dosyaları şifreleyen ve genellikle fidye ödenmeden önce dosyaların kilidini açmayı vaat eden kötü niyetli yazılımlardır. Blokzincir, merkezi olmayan ve güvenli veri depolama yetenekleri sağlaması açısından fidye yazılımlarıyla mücadelede önemli bir rol oynayabilir. Blokzincir teknolojisi, dosyaların şeffaf ve güvenli bir şekilde depolanmasını sağlar, bu da fidye yazılımlarının etkilerini azaltabilir. Ancak, blokzincir teknolojisinin ölçeklenebilirlik zorlukları ve fidye yazılımlarının evrimi, sürekli bir mücadeleyi gerektirir. Oltalama, kişisel bilgileri ele geçirmek amacıyla yapılan kötü niyetli siber saldırıların bir türüdür. Blokzincir, bu tür saldırılara karşı ek bir güvenlik katmanı sağlayabilir. Özellikle, merkezi olmayan kimlik doğrulama sistemleri ve şeffaf iletişim protokolleri, oltalama saldırılarına karşı etkili bir savunma mekanizması oluşturabilir. Blokzincir tabanlı kimlik doğrulama çözümleri, kullanıcıların dijital kimliklerini güvenli bir şekilde yönetmelerine olanak tanır. Ancak, blokzincirin siber güvenlikteki rolüne odaklanırken, karşılaşılan zorluklar da göz ardı edilmemelidir. Özellikle enerji tüketimi ve ölçeklenebilirlik konuları, blokzincirin geniş ölçekte benimsenmesini sınırlayan faktörler arasındadır. Gelecekte, blokzincir teknolojisinin bu zorlukları aşarak siber güvenlik alanında daha etkin bir şekilde kullanılabilmesi için daha fazla araştırma ve geliştirme çalışması gerekmektedir. Kötü amaçlı kripto madenciliği, fidye yazılımları ve oltalama gibi siber saldırı türleri, günümüzdeki dijital tehdit ortamının önemli birer unsuru haline gelmiştir. Blokzincir teknolojisi, bu tehditlere karşı potansiyel bir savunma veya izleme aracı olarak öne çıkmaktadır. Ancak, bu potansiyelin gerçekleştirilebilmesi için daha fazla araştırma ve geliştirme yapılması, blokzincirin siber güvenlikteki rolünü tam anlamıyla ortaya koymak için önemlidir. Blokzincir ve siber güvenlik arasındaki kompleks ilişki, siber güvenlik uzmanlarının sürekli olarak bu alanda çalışmalarını sürdürmelerini gerektirmektedir.

Teşekkür (Acknowledgment)

Çalışma 7373 hibe numarası ile Gazi Üniversitesi tarafından desteklenmiştir. Destekleri için Gazi Üniversitesine teşekkür ederiz.

Çıkar Çatışması Beyanı (Conflict of Interest Statement)

Yazarlar tarafından herhangi bir çıkar çatışması bildirilmemiştir.

Kaynaklar (References)

[1] S. Meunier, Transforming Climate Finance and Green Investment with Blockchains: *Chapter 3 – Blockchain 101: What is Blockchain and How Does This Revolutionary Technology Work?*, A. Marke: Ed. Academic Press, 2018, pp. 23–34.

[2] S. Li, T. Qin and G. Min, "Blockchain-Based Digital Forensics Investigation Framework in the Internet of Things and Social Systems" *IEEE Transactions on Computational Social Systems*, vol. 6, no. 6, pp. 1433-1441, December 2019. doi:10.1109/TCSS.2019.2927431.

[3] M. A. Zook and J. Blankenship, "New spaces of disruption? The failures of Bitcoin and the rhetorical power of algorithmic governance", *Geoforum*, vol. 96, pp. 248–255, November 2018. doi:10.1016/j.geoforum.2018.08.023

[4] S. Fosso Wamba, J. R. Kala Kamdjoug, R. Epie Bawack and J. G. Keogh, "Bitcoin, Blockchain and Fintech: a systematic review and case studies in the supply chain", *Production Planning & Control*, vol. 31, no. 2–3, pp. 115–142, December 2020. doi:10.1080/09537287.2019.1631460

[5] A. A. Sadawi, B. Madani, S. Saboor, M. Ndiaye, and G. Abu-Lebdeh, "A comprehensive hierarchical blockchain system for carbon

emission trading utilizing blockchain of things and smart contract", *Technological Forecasting and Social Change*, vol. 173, p. 121124, December 2021. doi:10.1016/j.techfore.2021.121124

[6] M. Javaid, A. Haleem, R. Pratap Singh, S. Khan, and R. Suman, "Blockchain technology applications for Industry 4.0: A literature-based review", *Blockchain: Research and Applications*, vol. 2, no. 4, pp. 100027, December 2021. doi:10.1016/j.bcra.2021.100027

[7] S. B. ElMamy, H. Mrabet, H. Gharbi, A. Jemai, and D. Trentesaux, "A Survey on the Usage of Blockchain Technology for Cyber-Threats in the Context of Industry 4.0", *Sustainability*, vol. 12, no. 21, November 2020. doi:10.3390/su12219179

[8] B. A. Kitchenham, "Procedures for Performing Systematic Reviews" *www.inf.ufsc.br*, 2004. [Online]. Available: https://www.inf.ufsc.br/~aldo.vw/kitchenham.pdf. [Accessed: Dec. 25, 2023].

[9] J. Rüth, T. Zimmermann, K. Wolsing, and O. Hohlfeld, "Digging into Browser-Based Crypto Mining", in *Proceedings of the Internet Measurement Conference 2018*, Boston, MA, USA, 2018, pp. 70–76. doi:10.1145/3278532.3278539

[10] E. Le Jamtel, "Swimming in the Monero pools" 2018 11th International Conference on IT Security Incident Management & IT Forensics (IMF), Hamburg, Germany, 2018, pp. 110-114, doi:10.1109/IMF.2018.00016.

[11] "Usage statistics of client-side programming languages for websites" *W3Techs*, [Online]. Available: https://w3techs.com/technologies/overview/client_side_language. [Accessed: 25-Dec-2023].

[12] "I now own the COINHIVE domain. here's how I'm Fighting Cryptojacking and doing good things with content security policies." *Troy Hunt*, 02-Apr-2021. [Online]. Available: https://www.troyhunt.com/i-now-own-the-coinhive-domain-heres-how-im-fighting-cryptojacking-and-doing-good-things-with-content-security-policies/. [Accessed: 25-Dec-2023].

[13] "Plugins categorized as mining" *WordPress*, [Online]. Available: https://wordpress.org/plugins/tags/mining/ [Accessed: 25-Dec-2023].

[14] D. Goodin, "Now even YouTube serves ads with CPU-draining cryptocurrency miners" *Ars Technica*, Jan. 26, 2018. [Online]. Available: https://arstechnica.com/information-technology/2018/01/now-even-youtube-serves-ads-with-cpu-draining-cryptocurrency-miners/ [Accessed: 25-Dec-2023].

[15] C. Osborne, "MikroTik routers enslaved in massive Coinhive cryptojacking campaign" *ZDNET*, [Online]. Available: https://www.zdnet.com/article/mikrotik-routers-enslaved-in-massive-coinhive-cryptojacking-campaign/ [Accessed: 25-Dec-2023].

[16] "No coin is a tiny browser extension aiming to block coin miners such as coinhive" *Github*, [Online]. Available: https://github.com/keraf/NoCoin [Accessed: 25-Dec-2023].

[17] J. Rüth, T. Zimmermann, K. Wolsing, and O. Hohlfeld, "Digging into Browser-Based Crypto Mining", in *Proceedings of the Internet Measurement Conference 2018*, Boston, MA, USA, 2018, pp. 70–76. doi:10.1145/3278532.3278539.

[18] W. Wang, B. Ferrell, X. Xu, K. W. Hamlen, and S. Hao, "SEISMIC: SEcure In-Lined Script Monitors for Interrupting Cryptojacks", in *Computer Security: 23rd European Symposium on Research in Computer Security, ESORICS 2018, Barcelona, Spain*, September 3-7, 2018, Proceedings, Part II, Barcelona, Spain, 2018, pp. 122–142. doi:10.1145/3278532.3278539.

[19] D. Carlin, P. O'Kane, S. Sezer and J. Burgess, "Detecting Cryptomining Using Dynamic Analysis" 2018 *16th Annual Conference on Privacy, Security and Trust (PST)*, Belfast, Ireland, 2018, pp. 1-6. doi:10.1109/PST.2018.8514167.

[20] A. Kharraz, Z. Ma, P. Murley, C. Lever, J. Mason, A. Miller, N. Borisov, M. Antonakakis, M. Bailey, "Outguard: Detecting in-browser covert cryptocurrency mining in the wild" in: *The World Wide Web Conference, WWW '19, Association for Computing Machinery*, New York, NY, USA, 2019, p. 840–852. doi:10.1145/3308558.3313665. doi:10.1145/3308558.3313665.

[21] W. Bian, W. Meng, M. Zhang, "MineThrottle: Defending against Wasm In-Browser Cryptojacking", *Association for Computing Machinery*, New York, NY, USA, 2020, p. 3112–3118. doi:10.1145/3366423.3380085

[22] F. Naseem, A. Aris, L. Babun, E. Tekiner, S. Uluagac, "Minos: A lightweight real-time cryptojacking detection system" in: *28th Annual Network and Distributed System Security Symposium*, NDSS, 2021. doi:10.14722/ndss.2021.24444

[23] F. Tommasi, C. Catalano, U. Corvaglia, I. Taurino, "Mineralert: an hybrid approach for web mining detection", *Journal of Computer Virology and Hacking Techniques,* March 2021. doi:10.1007/s11416-022-00420-7.

[24] A. Hernandez-Suarez, G. Sanchez-Perez, L.K. Toscano-Medina, J. Olivares-Mercado, J. Portillo-Portilo, J. Avalos and L.J. García Villalba, "Detecting Cryptojacking Web Threats: An Approach with Autoencoders and Deep Dense Neural Networks", *Applied Sciences*, vol. 12, no. 7, 2022. doi:10.3390/app12073234

[25] A. Zareh and H. R. Shahriari, "Botcointrap: Detection of bitcoin miner botnet using host based approach", in: *2018 15th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC)*, 2018, pp. 1–6. doi:10.1109/ISCISC.2018.8546867.

[26] S. Soviany, A. Scheianu, G. Suciu, A. Vulpe, O. Fratu and C. Istrate, "Android malware detection and crypto-mining recognition methodology with machine learning", in: *2018 IEEE 16th International Conference on Embedded and Ubiquitous Computing (EUC)*, 2018, pp. 14–21. doi:10.1109/EUC.2018.00010

[27] G. Berecz. and I. Czibula., "Hunting traits for cryptojackers", in: *Proceedings of the 16th International Joint Conference on e-Business and Telecommunications – SECRYPT*, 2019, pp. 386–393. doi:10.5220/0007837403860393

[28] H. Darabian, S. Hashemi, S. Homayounoot, A. Dehghantanha, H. Karimipour, R. M. Parizi and K. R. Choo, "Detecting Cryptomining Malware: a Deep Learning Approach for Static and Dynamic Analysis", *Journal of Grid Computing*, vol. 18, no. 2, pp. 293–303, Jun. 2020. doi:10.1007/s10723-020-09510-6

[29] V. Veselý and M. Žádník, "How to detect cryptocurrency miners? By traffic forensics!", *Digital Investigation*, vol. 31, p. 100884, 2019. doi: 10.1016/j.diin.2019.08.002

[30] S. Balamurugan and M. Thangaraj, "Cryptojacking Malware Detection using the Bayesian Consensus Clustering with Large Iterative Multi-Tier Ensemble in the Cryptocurrency in the Cloud" *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, no. 3. Blue Eyes Intelligence Engineering and Sciences Engineering and Sciences Publication - BEIESP, pp. 4256–4264, Sep. 30, 2019. doi:10.35940/ijrte.c5159.098319.

[31] D. Tanana and G. Tanana, "Advanced Behavior-Based Technique for Cryptojacking Malware Detection" 2020 *14th International Conference on Signal Processing and Communication Systems (ICSPCS)*, Adelaide, SA, Australia, 2020, pp. 1-4, doi:10.1109/ICSPCS50536.2020.9310048.

[32] "Bitcoin Tracker: Wannacry Doesn't Pay. " *Pymnts.Com*, May 19, 2017. [Online]. Available: www.pymnts.com/news/bitcoin-tracker/2017/bitcoin-tracker-wannacry-doesnt-pay/ [Accessed: 25-Dec-2023].

[33] M.Kan "Old Windows Pcs Can Stop WannaCry Ransomware with New Microsoft Patch." *Computerworld.com*, May 13, 2017. [Online]. Available: www.computerworld.com/article/3196693/old-windows-pcs-can-stop-wannacry-ransomware-with-new-microsoft-patch.html. [Accessed: 25-Dec-2023].

[34] "Deep Shift: Technology Tipping Points and Societal Impact", *weforum.org*, Sept. 9, 2023. [Online]. Available: https://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf. [Accessed: 25-Dec-2023].

[35] D. Y. Huang, M. M. Aliapoulios, V. G. Li, L. Invernizzi, E. Bursztein, K. McRoberts, J. Levin, K. Levchenko, A. C. Snoeren and D. McCoy, "Tracking ransomware end-to-end" in: *2018 IEEE Symposium on Security and Privacy (SP)*, 2018, pp. 618–631. doi:10.1109/SP.2018.00047.

[36] M. Paquet-Clouston, B. Haslhofer and B. Dupont, "Ransomware payments in the bitcoin ecosystem", *Journal of Cybersecurity*. vol. 5, no. 1. doi:10.1093/cybsec/tyz003.

[37] O. Delgado Mohatar, J. Sierra-C´amara and E. Anguiano, "Blockchain-based semi-autonomous ransomware", *Future Generation Computer Systems*, vol. 112, pp. 589-603, 2020. doi:10.1016/j.future.2020.02.037

[38] M. Ozer, S. Varlioglu, B. Gonen and M. Bastug, "A prevention and a traction system for ransomware attacks", in: *2019 International Conference on Computational Science and Computational Intelligence (CSCI)*, 2019, pp. 150–154. doi:10.1109/CSCI49370.2019.00032.

[39] N. Scaife, H. Carter, P. Traynor and K. R. B. Butler, "CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data," *2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS)*, Nara, Japan, 2016, pp. 303-312. doi:10.1109/ICDCS.2016.46.

[40] A. Continella, A. Guagnelli, G. Zingaro, G. Pasquale, A. Barenghi, S. Zanero and F. Maggi, "ShieldFS: A Self-Healing, Ransomware-Aware Filesystem", in *Proceedings of the 32nd Annual Conference on Computer Security Applications*, Los Angeles, California, USA, 2016, pp. 336–347. doi:10.1145/2991079.2991110

[41] D. Mendes, I. Rodrigues, C. Fonseca, M. Lopes, J. M. García-Alonso and J. Berrocal, "Anonymized Distributed PHR Using Blockchain for Openness and Non-repudiation Guarantee", in *Digital Libraries for Open Knowledge*, 2018, pp. 381–385. doi:10.1007/978-3-030-00066-0_45

[42] C. Karapapas, I. Pittaras, N. Fotiou and G. C. Polyzos, "Ransomware as a service using smart contracts and ipfs", in: *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2020, pp. 1–5. doi:10.1109/ICBC48266.2020.9169451

[43] C. G. Akcora, Y. Li, Y. R. Gel, and M. Kantarcioglu, 'BitcoinHeist: Topological Data Analysis for Ransomware Prediction on the Bitcoin Blockchain', in *Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence, IJCAI-20*, 7 2020, pp. 4439–4445. doi:10.24963/ijcai.2020/612

[44] A. Turner, S. Mccombie and A. Uhlmann, "Follow the money: Revealing risky nodes in a ransomware-bitcoin network" *Machine Learning and Predictive Analytics in Accounting, Finance, and Management*, January 2021. doi:10.24251/HICSS.2021.189.

[45] P. Xia, H. Wang, H. Wang, X. Luo, L. Wu, Y. Zhou, G. Bai, G. Xu, G. Huang and X. Liu, "Don't Fish in Troubled Waters! Characterizing Coronavirus-themed Cryptocurrency Scams", *APWG Symposium on Electronic Crime Research (eCrime)*, Boston, MA, USA, 2020, pp. 1-14, doi: 10.1109/eCrime51433.2020.9493255.

[46] A. Holub and J. O'Connor, "COINHOARDER: Tracking a ukrainian bitcoin phishing ring DNS style," *APWG Symposium on Electronic Crime Research (eCrime),* San Diego, CA, USA, 2018, pp. 1-5, doi: 10.1109/ECRIME.2018.8376207.

[47] M. Guri, "BeatCoin: Leaking Private Keys from Air-Gapped Cryptocurrency Wallets," *IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing*

(CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 2018, pp. 1308-1316, doi: 10.1109/Cybermatics_2018.2018.00227.

** This paper was presented at the 5th International Conference on Artificial Intelligence and Applied Mathematics in Engineering (ICAIAME 2023) and the abstract was published as an e-book.*