



Bilişim Teknolojilerinde Blok Zincir ve Kuantum Hesaplamanın Ortak Geleceği: Kuantum Blok Zinciri

Sevdanur GENÇ^{1*}

¹Kastamonu Üniversitesi, Taşköprü Meslek Yüksekokulu, Bilgisayar Teknolojileri Bölümü, Kastamonu

Özet

Bitcoin, Ehtereum ve diğer kripto para birimleri blok zinciri teknolojisi üzerinde geliştirilmektedir. Bu teknoloji üzerinde veriler şifrelenerek parçalara bölünür ve bu şifreleme finansal işlemlerde kullanılır. Şifreleme algoritmalarının daha hızlı çalışması için kuantum hesaplama bir alternatif olarak sunulmaktadır. Bununla birlikte, kuantum hesaplamanın varlığı söz konusu olduğunda kuantum bilgisayarlara ve kuantum programlamaya daha fazla ilgi duyulmaktadır. Kuantum bilgisayarlar, günümüz klasik bilgisayarlara kıyasla algoritmaları daha güçlü ve hızlı bir şekilde çözümlenmektedir. Sorun şu ki, kuantum hesaplama gelecekte kripto para piyasasında kullanılırsa, blok zinciri üzerinde tüm işlemler hem hızlı bir şekilde sürdürülebilecek hem de güvenlik tehditlerine ve sahteciliklere karşı savunmasız kalacaktır.

Bu çalışmada, öncelikle blok zincir ve kuantum hesaplama hakkında bilgi verilmiştir. Kuantum bilgisayarların kripto para ve blok zinciri teknolojilerinin üzerindeki gelecek etkisi tartışılmış ve kuantum blok zinciri kavramından bahsedilmiştir. Aynı zamanda, kuantum hesaplamanın blok zincir üzerindeki olası olumlu - olumsuz etkilerinden söz edilmiştir. Son olarak yazılım endüstrisinin kriptografi alanı için tehdit olarak gördüğü kuantum hesaplama hakkındaki girişimlerinden bahsedilmiştir. Söz konusu çalışmanın Türkçe literatüre katkı sağlayacağı düşünülmektedir.

Anahtar Kelimeler: Blok Zinciri, Kripto Para, Kuantum Blok Zinciri, Kuantum Hesaplama, Kuantum Programlama.

Common Future of Blockchain and Quantum Computing in Information Technologies: Quantum Blockchain

Abstract

Bitcoin, Ethereum and other cryptocurrencies are developed on blockchain technology. On this technology, data is encrypted and divided into parts, and this encryption is used in financial transactions. Quantum computing is offered as an alternative for encryption algorithms to work faster. However, there is more interest in quantum computers and quantum programming when it comes to the existence of quantum computing. Quantum computers analyze algorithms more powerfully and faster than today's classical computers. The problem is that if quantum computing is used in the cryptocurrency market in the future, all transactions on the blockchain will both be able to resume quickly and be vulnerable to security threats and fraud.

Makale Bilgisi

Başvuru:

09/12/2022

Kabul:

19/12/2022

* İletişim e-posta: sgenc@kastamonu.edu.tr

In this study, first of all, information about blockchain and quantum computing is given. The future impact of quantum computers on crypto money and blockchain technologies is discussed and the concept of quantum blockchain is mentioned. At the same time, the possible positive and negative effects of quantum computing on the blockchain were mentioned. Finally, the software industry's attempts on quantum computing, which is seen as a threat to the field of cryptography, are mentioned. It is thought that this study will contribute to the Turkish literature.

Keywords: Blockchain, Cryptocurrency, Quantum Blockchain, Quantum Computing, Quantum Programming.

1 Giriş

Blok zinciri kullanan dağıtılmış defter teknolojileri, finans, hükümet, enerji ve ulaşım gibi alanlarda veri ve işlemlerin güvenliğini sağlamaya yardımcı olmaktadır. Kuantum hesaplama ise, yapay zeka ve blok zinciri ile aynı amaçlar doğrultusunda çakışmaktadır çünkü kuantum hesaplama, endüstri çözümleri için veri büyümesi ve birikimi arttıkça yeni hesaplama gücü ve verimlilik seviyeleri getirmeye yardımcı olacaktır.

Teknoloji üzerine araştırmalar yapan ve bu araştırmayı hem özel danışmanlık hem de yönetici programları ve konferanslar aracılığıyla paylaşan Gartner şirketinin öngörüsüne göre, 2024'ün sonlarında işletmelerin yaklaşık yüzde 75'i yapay zekayı operasyonel hale getirerek veri akışı ve analitik altyapılarında 5 kat artış sağlayacaktır. Ayrıca sağlık bilgi yönetim sistemleri ve hatta doğal dil işleme algoritmaları için hassas verilerin korunması gibi eğilimler aracılığıyla yapay zeka ve blok zincirinin müşteri deneyimini iyileştirmek için kullanılması küresel blok zinciri yapay zeka pazar büyüklüğünün 2027 yılına kadar 973,6 milyon ABD dolarına ulaşacağını tahmin edilmektedir [1].

Bu çalışma ile kuantum hesaplama ve blok zincirinin birbirinden oldukça farklı iki teknoloji olduğundan bahsedilmiş, aynı zaman da birbirleriyle nasıl etkileşime girecekleri ve her iki sektörde de sonsuza kadar nasıl değişkenlikler gösterecekleri tartışılmıştır. Ayrıca, kuantum blok zinciri terimi ile Türkçe literatüre katkı sağlanması hedeflenmiştir.

2 Literatür

Literatürde yer alan, son yıllarda yayınlanmış, kuantum hesaplama ve blok zinciri hakkında gerçekleştirilen farklı çalışmalardan başlıcaları incelenmiştir.

Rodenburg ve Pappas (2017) çalışmalarında, kuantum bilgisayarların geliştirilmesiyle ortaya çıkan blok zinciri teknolojisinin güvenlik açıklarını

incelemiş ve blok zincirinin bu tür teknolojik gelişmelere karşı nasıl daha dirençli hale getirilebileceğine dair genel öneriler sunmuşlardır [2].

Ikeda (2018) çalışmasında, Blockchain ve Kuantum Hesaplamanın Güvenliği ve Gizliliği hakkındaki bakış açısını sunmuştur. Kuantum teknolojisinin blok zinciri endüstrisine uygulanmasıyla ilgili ileri araştırmaların takip edilebilmesi için kuantum bilgi teorisine ve kuantum hesaplama pedagojik bir giriş yapmıştır [3].

Kiktenko vd. (2018) çalışmalarında, kuantum çağı blok zinciri sorununa olası bir çözüm önermişlerdir ve bilgi-teorik olarak güvenli kimlik doğrulama için bir kentsel fiber ağ üzerinden kuantum anahtar dağıtımını kullanan kuantum güvenli bir blok zinciri platformunun deneysel olarak gerçekleştirildiğini rapor etmişlerdir [4].

Gao vd. (2018) çalışmalarında, kuantum sonrası blok zincirinin tanımını sunmuşlar ve kuantum hesaplama saldırılarına direnebilen kuantum sonrası blok zincirine dayalı güvenli bir kripto para birimi şeması önermişlerdir. Aynı zamanda, kripto para birimi şemasını daha güvenli ve verimli hale getirebilecek önerilerde bulunmuşlardır [5].

Chuntang vd. (2019) çalışmalarında, kuantum blok zinciri alanındaki gelişmeleri gözden geçirmişler ve klasik blok zincirine kıyasla avantajlarını kısaca analiz etmişlerdir. Kuantum blok zincirinin yapısı ve çerçevesi tanıtılmış ve ardından, genel blok zincirinin belirli bir bölümüne kuantum teknolojisi uygulama yöntemi incelenmiştir. Ayrıca kuantum blok zincirinin klasik blok zincirine göre avantajları ve geliştirme beklentileri de özetlenmiştir [6].

Fernández-Caramès ve Fraga-Lamas (2020) çalışmalarında, kuantum hesaplama saldırılarına dirençli blok zinciri kriptografisi üzerine bir inceleme yapmışlardır. Kuantum hesaplamanın hızlı ilerlemesi, yakın gelecekte Grover'in [7] ve Shor'un [8] algoritmalarına dayalı saldırılar gerçekleştirme olasılığından bahsetmişlerdir. Ayrıca, en alakalı post-kuantum blok zinciri

sistemleri ve bunların ana zorlukları incelenmiştir. Bununla birlikte, blok zincirler için en umut verici kuantum sonrası açık anahtar şifreleme ve dijital imza şemalarının özellikleri ve performansı hakkında kapsamlı karşılaştırmalar yapılmıştır [9]. Alghamdi ve Almuhammadi (2021) çalışmalarında, kuantum saldırıları altında günümüzün kripto para blokajlarının güvenliğini değerlendirmişlerdir. Ayrıca Kuantum Çağında blok zincirlerini korumak için önerilen çözümlerden bazılarını da gözden geçirmektedir. Ayrıca, kuantum güvenli blok zincirleri oluşturmak için kullanılan bir dizi kuantum sonrası dijital imza şeması sunmuşlardır [10].

Srivastava vd. (2022) çalışmalarında, arka planı, mimarisi ve özellikleri gibi blok zincir teknolojisi hakkında ayrıntılı bir genel bakış sunmuşlardır. Ayrıca, kullanımdaki farklı popüler blok zincirlerinin kuantum düzeyindeki güvenlik açıklarını ve blok zincirinde kullanılan farklı şifreleme kavramlarını açıklamışlar ve ardından blok zinciri teknolojisi ile birlikte kuantum hesaplama kavramını vurgulamışlardır. Sonunda, kuantum öncesi ve kuantum sonrası blok zinciri hakkında bir fikir vermişlerdir [11].

3 Blok Zincir

Blok zinciri (Blockchain), bir iş ağına maddi veya maddi olmayan işlemlerin kaydedilmesi ve bu varlıkların izlenmesi sürecini kolaylaştıran dağıtılmış değişmez bir hesap defteridir. Neredeyse değeri olan her şey bir blok zinciri ağına izlenebilir ve alınıp satılabilir. Bu durum riskleri azaltır ve ilgili herkes için maliyetleri düşürür. Blok zinciri yapısı itibarıyla veri tabanı veya elektronik tablo olarak da bilinmektedir. Bu yapıya yalnızca bilgi eklenebilir, önceki bilgiler silinemez veya herhangi bir şekilde değiştirilemez. Blok olarak adlandırılan her bir bilgi girişi son bilgi girişine kriptografik olarak bağlanmaktadır. Her yeni giriş, sonuncunun hash algoritmalarıyla bir tür dijital parmak izini içermektedir. Böylelikle blok zincir yapısı ortaya çıkmaktadır. Bu yapılar, değiştirilmemelidir. Eğer değiştirilmeye çalışılırsa parmak izi değiştirilmiş olur. Bu parmak izi bir sonraki bloğa dahil edilmek istenildiğinde, bir sonraki blokta etkilenecek ve değişecektir. Bu mekanizmaların başarılı bir şekilde çalışması konsensüs (fikir birliği) algoritmalarına bağlıdır. Proof of Work (PoW) [12] ve Proof of Stake (PoS) [13] gibi konsensüs algoritmalar [14], kripto para birimlerinin ve dağıtılmış defterlerin işleyişi için hayati bir öneme sahiptir.

Blok zinciri düğümler, bir dizi dağıtılmış bilgisayar tarafından doğrulanır ve sonrasında etkin bir şekilde değiştirilemeyen bir bilgi defteri haline getirilir. Bu defter, kriptografiyi kullanan bir dizi dağıtılmış defter teknolojisi olarak tanımlanmaktadır. Bu tanımlanma aşamasında, çeşitli konsensüs (fikir birliği) mekanizmaları kullanılır. Dağıtılmış bir düğüm ağı, bilgi bloklarını doğrularak blok zincirine eklenir [15]. Blok zincirleri tamamen klasik bilgi işlem alanındadır, yani blok zincirinin zamanda bir noktada yalnızca tek bir durumda olacağı anlamına gelmektedir.

Endüstride blok zincir teknolojisi, dijital para birimleri, lojistik ve kayıt tutma protokolleri ve çeşitli finansal ürünler dahil olmak üzere kendi kendini yürüten akıllı sözleşmeler yoluyla dağıtılmış uygulamalar oluşturmak için kullanılan bir araçtır. Bunlara borç verme, stake etme [16], verim çiftçiliği ve hatta dağıtılmış sigorta protokolleri de dahildir [1].

Bununla birlikte, ağ kısıtlamaları nedeniyle, blok zinciri, yüksek düzeyde hesaplamalı problem çözme yeteneği gerektiren problemleri çözmede iyi değildir. Aslında, yavaş işlem hızı, günümüzde blok zincirindeki en büyük sorunlardan biridir ve yeni blok zincirleri, daha yüksek miktarda işlem (TPS - Transactions per second) ile çalışabilen çözümler sunmak için çabalamaktadır. Buna karşılık, kuantum hesaplama, bilim ve teknolojinin sunduğu bazı büyük, karmaşık sorunları çözmek için büyük bir potansiyele sahiptir, ancak şu an için oldukça masraflı ve ulaşılması güç bir araçtır.

4 Kuantum Hesaplama ve Kuantum Bilgisayarlar

Genellikle klasik bilgisayarlar olarak adlandırılan mevcut bilgisayarlar, 0'lar veya 1'ler olan ancak her ikisi birden olmayan bitlerden oluşmaktadır. Kuantum bilgisayarlar da ise bitler yerine Kübit'ler (Qubit) bulunmaktadır. Kuantum süperpozisyon (Quantum Superposition) [17] adı verilen bir kavramla birlikte, bu bitler her iki durumda da aynı anda var olmaktadır. Geleneksel bitlerin aksine kübitler, tüm bilgi işlem sistemi için tek, büyük bir kuantum durumu oluşturan Kuantum Dolanıklığı (Quantum Entanglement) [18] adı verilen bir süreçte birbirlerini etkilemektedirler. Kübit sayısı arttıkça, bilgisayarın potansiyel durumlarının sayısı iki katına çıkmaktadır ve bu bilgisayarlar klasik bilgisayarlara kıyasla daha üstün hesaplama yetenekleri kazandırmaktadır.

Kuantum hesaplama, kuantum mekanik bitleri olarak bilinen kubitler nedeniyle geleneksel ve süper bilgisayarlar kıyasla problem çözme hızlandırma konusunda önemli bir potansiyele sahiptirler. Bu bilgisayarların yaygın olarak iş alanları tarafından benimsenmesine daha birkaç yıl bulunmaktadır, ancak IBM ve Google gibi bazı büyük ölçekli teknoloji şirketleri şu anda yatırım yapmaktadır. Kuruluşların, en son gelişmeleri takip ederek, verileri potansiyel bilgisayar korsanlarından nasıl daha iyi koruyabileceklerini araştırarak ve geleceğin teknolojiyle kesintiye uğrayabilecek iş ve endüstri yörüngelerini şekillendirerek kuantum bilişim [19] geleceğine hazırlanmaları gerekmektedir.

Kuantum hesaplama, büyük miktarda işlem gücü gerektiren veya normal süper bilgisayarların çözmesi neredeyse imkansız olan mantık problemlerini çözmek için benzersiz bir bilgi işlem türü olan kuantum durumlarını (quantum states) [20] kullanmaktadır. Bu bilgisayarlar, geleneksel bir süper bilgisayar gibi bir dizi sorunu tek tek analiz etmek yerine, büyük miktarda potansiyel sorunu ve yanıtı aynı anda analiz edebilmektedir. Aynı zamanda bu bilgisayarlar, olası yanlış cevapların miktarını büyük bir hızla en aza indirmek için kuantum fiziğinin güçlerini kullanır ve potansiyel olarak doğru cevapları yine büyük bir hızla geliştirebilir.

Kuantum hesaplama, karmaşık sorunları çözmenin yanı sıra şifreleme dünyasını da değiştirmek için karakteristik bir özelliğe sahiptir. Kuantum fiziğinin ve kuantum durumlarının doğası gereği, belirli bir bilgi parçasının durumu, gözlemlendiğinde değişkenlik gösterir. Bu nedenle, teorik olarak herhangi bir bilgi parçasının durumu amaçlanan taraf dışında herhangi bir insan veya makine tarafından görüntülendiğinde geri alınmaz bir şekilde değişmektedir. Bu sebepten ötürü, kuantum hesaplama tarafından oluşturulan güçlü kuantum şifreleme teknolojileri gerçekten çözülemez durumdadır. Aynı zamanda, potansiyel diğer kırılmaz şifreleme teknolojileri de kırılabilir ve bu da onu blok zincirlerin tüm amacı ile bir çatışmaya sokabilir [1].

IBM gibi büyük şirketler şu anda elektrikli arabalar için daha yüksek enerji yoğunluklu piller, daha az karbon emisyonu ile oluşturulabilecek yeni malzemeler geliştirmeye ve hatta evrenin kökenine ışık tutabilecek parçacıkları aramaya kadar çeşitli sorunları çözmek için kuantum bilgisayarları kullanmaktadır [1].

5 Kuantum Blok Zinciri - Quantum Blockchain

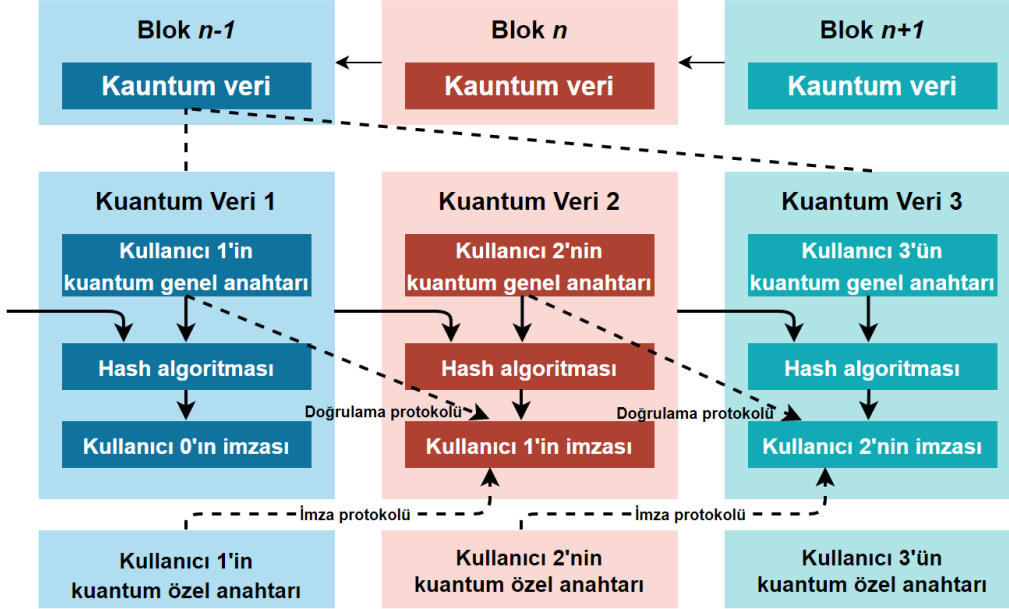
Kuantum şifrelemenin koşulsuz güvenliği göz önünde bulundurulduğunda, kuantum mekaniğinin ilkeleri blok zincirine de uyarlanmıştır. Genel olarak, kuantum mekaniğini blok zincir ile birleştiren kuantum blok zinciri çalışması, kuantum bilgisayar saldırılarından kaynaklanan tehditle başa çıkmada büyük önem taşımaktadır.

Kuantum blok zinciri temel olarak şu altı adımdan oluşur: anahtar oluşturma, şifreleme, yayınlama, şifre çözme, minting ve birleştirilme. Minting yeni bilgilerin doğrulanması sonucu, yeni blokların oluşturulması ve bu bilginin blok zincire kaydedilmesi sürecidir. Bu doğrultuda blokların nasıl oluşturulduğu ve verilerin bloğa nasıl eklendiğini belirleyen minting süreci mekanizması Proof of Stake (PoS) gibi konsensüs bir algoritmadır [21].

Kuantum kripto parası, kuantum kanalı tarafından iletilen bir kubit dizisidir (ör. n-kubit, bir kuantum kripto parayı belirtir). Bu paralar ilk kez iletildiklerinde, kuantum blok zinciri sistemi tarafından üretilmekte ve dağıtılmaktadırlar. Keyfi bir kuantum durumunu (kuantum kripto para) kopyalamak imkansızdır. Dolayısıyla kuantum mekaniği, bir kripto para birimi olarak kabul edilen kuantum durumu için bariz avantajlar sağlar ve yeni kripto para birimi türleri için çifte harcama saldırısını önleyebilir. Bu da, kuantum kripto paranın sahteciliğe karşı güvenli olduğunu gösterir.

Şekil 1'de kuantum blok zincirinin yapısı verilmiştir. Bu yapıda, kuantum bloklarını birbirine bağlamak için zaman serisinde kuantum dolanıklığı kullanılmaktadır. Sırasıyla $n - 1$, n ve $n+1$ blokları kuantum bloklarıdır ve bu kuantum bloklarında doğrulama protokolleri tarafından doğrulanmış kuantum verileri depolanır. Bu protokoller yardımıyla kuantum hesaplama veri kimlik doğrulaması ile ilgili algoritmalarından yardım alınarak blok zinciri teknolojisine dahil edilmektedir. Kuantum mekaniğinin ve kuantum kriptografisinin temel özelliklerine dayanan bu dağıtılmış düğümler, kuantum ağı aracılığıyla kimliği doğrulanmış ve güvenli bir kuantum bilgi veri tabanını paylaşır. Her kullanıcı, kuantum ağlarında yayınlanan ve diğer düğümler tarafından doğrulanan kuantum imzaları aracılığıyla doğrulanabilir bir kuantum bilgisi üretebilmektedir. Ardından, diğer düğümler adil bir konsensüs algoritması yardımıyla yeni kuantum blokları için hazırda beklerler ve bu kuantum

bloklarını zaman içinde kuantum dolanıklığı ile birbirleriyle ilişkilendirilirler. Sonuç olarak, tüm düğümler yeni kuantum bloğunu kuantum kanalları aracılığıyla kendi kuantum blok zincirine ekler.



Şekil 1: Kuantum blok zincirinin organizasyon yapısı [22].



Şekil 2. Kuantum blok zincirinin iş akışı.

Şekil 2'de kuantum blok zincirine ait iş akışı verilmiştir. Buna göre, kuantum blok zinciri, tam olarak merkezi olmayan bir yapı ile oluşmaktadır. Dağıtılmış birbirine bağlantılı bir kuantum ağı üzerinde, her düğüm kuantum depolama alanına dahil olmaktadır ve kuantum hazırlığı, kuantum iletimi gibi kuantum yeteneklerine ait işlevler sırasıyla gerçekleşmektedir. Kuantum blok zincirindeki her düğüm, en az bir kuantum bit veri doğrulama protokolünde yer alan kuantum hesaplamasını gerçekleştirme yeteneğine sahiptir. Farklı düğümler arasındaki iletişim koşulsuz olarak güvenlidir. Aynı zamanda, tüm madenciler tarafından fikir birliğine varmak için kullanılabilir bir fikir birliği algoritması da bulunmaktadır [23]. Nihayetinde, ortak bir kuantum veri tabanı üzerinde açık ve şeffaf bir bilgi alışverişi yapılmaktadır.

Kauntum blok zinciri teknolojisi var olan blok zinciri teknolojisi ile karşılaştırıldığında [22],

- Kuantum klonlama ilkesine dayalı olarak, kuantum durumları kopyalanamamaktadır. Bu sebeple, kuantum blok zincirinde var olan bir finansal işleme ait kuantum kripto para taklit edilememekte ve kopyalanamamaktadır.
- Her kullanıcı, kuantum kanalı aracılığıyla iletişim için bilgileri kübit'ler ile taşımaktadır. Kuantum hızlı kodlama yeteneğiyle, kuantum ağlarında bilgi iletimi daha verimli olmaktadır.
- Kuantum blok zincirinde bir bilgiyi doğrulamak, var olan blok zinciri teknolojisinden çok daha hızlı olmaktadır.
- Kuantum kriptografisi ve kuantum ilkeleriyle birleşen kuantum blok zinciri, kuantum bilgisayar saldırılarına karşı direnebilen kullanıcılar için güvenlik her zaman ön planda olmaktadır.

6 Blok Zincir ve Kuantum Hesaplamanın Ortak Geleceği

Teknolojinin geleceği söz konusu olduğunda, blok zinciri ve kuantum hesaplama önemli ve tartışmalı teknolojilerden ikisidir. Blok zinciri, hem bireyler hem de işletmeler tarafından kullanılabilen kripto para birimi ve kriptografinin oluşturulması uygulamalar üzerinde çok daha gelişmiş bir alana sahip olsa da, kuantum hesaplama teknolojisi de hızla ilerlemektedir. Aslında, kuantum hesaplama, endüstrinin 2022'den 2027'ye kadar yılda %25 oranında büyümesi beklenmektedir ve endüstri büyüme oranlarında blok zincirinden sonra belki de ikinci sırada yerini alacaktır [24].

Kuantum bilgisayarlar en gelişmiş blok zincirlerinin bile şifrelemesini kırabilir. Alternatif olarak, kuantum bilgisayarlar, bazı kapasitelerde, verilerin geleceğini güvence altına almak için daha gelişmiş bir yöntem olarak blok zincirlerin yerini alabilir. Asıl soru, kuantum bilgisayarların blok zincirlerini kırmak için yeterince hızlı gelişip gelişmeyeceğidir. Cevap ise kriptografların kendilerini kuantum korsanlarından (Quantum Hackers) korumak için yeterince hızlı güvenlik çözümleri geliştirip geliştirmediklerine göre belirlenecektir [25].

Blok zincirinin en önemli özelliklerinden biri, neredeyse aşılmaz güvenliğe sahip olmalarıdır. Kripto yatırımcılar, kuantum bilişim alanındaki gelişmelere dikkat etmelidir. Kripto para birimlerinin bireysel olarak kuantum bilişimi dikkate alarak şifreleme yöntemlerine güncelleme yapmaları gerekebilir. Kripto para yatırımcılarının muhtemelen bir noktada varlıklarını daha güvenli cüzdanlara aktarmaları gerekecektir. Kripto varlıklar eğer bir kripto borsasında saklanırsa, dönüşüm işlemlerini halletmek büyük olasılıkla daha kolay olacaktır. Bununla birlikte, kripto varlıklar merkezi olmayan bir cüzdanda saklanırsa, ekstra dikkatli olmaları gerekecektir. Bunların yanı sıra diğer teknolojiler de tehlike yaratabilir. Örneğin, Bitcoin'in 12 yıl önce yaptığı gibi, blok zincirini geçersiz kılan teknolojiler ortaya çıkarabilir ve kriptografi protokollerini engelleyebilir [26].

6.1 Kuantum Hesaplamanın Blok Zinciri Üzerindeki Olası Etkileri

Kuantum hesaplama ve blok zinciri teknolojilerinin ortak gelecekleri konusu ele alındığında iki önemli konuya dikkat edilmesi gerekir;

- Şifreleme algoritmaları söz konusu olduğunda, kuantum hesaplama teknolojisinin kripto para birimlerine zarar verilebileceği
- Kuantum hesaplama teknolojisinin blok zincir teknolojisiyle aynı amaç için kullanılıp şifreleme algoritmalarını daha fazla güçlendirebileceği ve günümüzün protokollerinden katlanarak daha güvenli blok zincirleri oluşturabileceği

Kuantum hesaplama ve blok zinciri arasındaki ilişki mutlaka negatif yönde ilerlemeyebilir; aksine kuantum hesaplama ve blok zinciri teknolojisi birleştiğinde daha güçlü bir teknoloji ortaya çıkabilir. Bu teknoloji hem kriptografik hem de gerçek dünyadaki çeşitli sorunları çözmeye yardımcı olabilecek daha güvenli, daha hızlı ve potansiyel olarak devrim niteliğinde bilgi işlem çözümleri yaratabilir. Shor ve Grover algoritmaları bunlara örnek verilebilir.

Shor fonksiyonu [8] olarak adlandırılan iyi bilinen bir teorik bilgisayar algoritması, bir kuantum bilgisayar tarafından uygulandığında, eliptik eğri çarpımı [27] tarafından gizlenmiş olan asal faktörleri çözebilmektedir. Bu, tersine çevrilmesi neredeyse imkansız olan hash algoritması için kullanılan bir çarpma şekli olabilir [28]. Örneğin, araştırmacılar, eliptik eğri çarpmasını kullanan bir genel anahtarla ilişkili özel bir anahtarı belirlemek için klasik bir bilgisayar temel işlemlerini gerektireceğini hesapladılar. Teorik olarak, bu binlerce yıl sürebilir. Buna karşılık, aynı hesaplamalara göre, Shor'un fonksiyonunu kullanan bir kuantum bilgisayar, bir ortak anahtarla ilişkili özel anahtarı belirlemek için yalnızca bir temel işlem gerçekleştirecektir. Bu sadece birkaç saat sürebilir. Bununla birlikte, ana akım kuantum bilgisayarlar üzerinde Shor'un fonksiyonunu kullanma yeteneği geliştirilmektedir [29].

Grover'in algoritması [7], kuantum arama yeteneklerini kolaylaştırmaya yardımcı olarak, kullanıcıların milyarlarca yapılandırılmamış veri noktası arasında bir kerede değerleri hızla bulmasını sağlar. Shor'un algoritmasından farklı olarak, Grover'in algoritması, şifrelemeden ziyade kriptografik hash algoritmaları için bir tehdittir. Kriptografik hashler tehlikeye girdiğinde, hem blok zinciri bütünlüğü hem de blok madenciliği zarar görür. Grover'in algoritmasını kullanarak, bir kuantum korsanı varsayımsal olarak aynı hash değerini üreten iki girdi bulabilir. Bu, hash çarpışması olarak bilinir. Grover'in algoritmasını kullanarak biraz daha kolay bir saldırı, iş kanıtı madenciliğini içerir. Grover'in arama algoritmasını

kullanan bir kuantum madencisi, geleneksel bir madenciden çok daha hızlı bir şekilde madencilik yapabilir. Bir kuantum madencisi, bir nonce (Number Only Used Once - Yalnızca Bir Kez Kullanılan Sayı) tahminini kolaylaştırmak için Grover'ın arama algoritmasını da kullanabilir (Nonce, blok zincir madencilerinin kripto para almak için çözdüğü sayıdır). Bunun nedeni, Grover'ın algoritmasının klasik bir bilgisayar üzerinden ikinci dereceden bir hızlanma sağlamasıdır [30].

Her iki algoritmaya karşı koruma mekanizması geliştiren bir çözüm ise Kuantum Dirençli Defter (QRL - Quantum Resistant Ledger)'dir. QRL, klasik ve kuantum hesaplama saldırılarına dayanıklı, hash algoritma tabanlı dijital imzalar kullanan bir kripto para birimi defter tasarımıdır [31].

Tüm olasılıklar birlikte düşünüldüğünde, blok zincirler hem geleneksel bilgisayar korsanlarına hem de kuantum bilgisayar saldırılarına karşı oldukça dirençli olmak zorundadır. Asimetrik anahtar algoritmaları gibi geleneksel blok zinciri şifreleme yöntemlerinin ve eliptik eğri çarpmasını kullanan hash fonksiyonlarının kuantum anahtarlarla değiştirilebilme ihtimali bulunmaktadır. Kuantum anahtar dağılımı (QKD - Quantum Key Distribution) [32] olarak da bilinen kuantum anahtar kriptografisi (Quantum Key Cryptography), optik bir bağlantı boyunca fotonlar şeklinde ışığın kuantum parçacıklarını (Quantum Particles) [33] göndererek çalışır [34]. Bir dinleyicinin iletilen fotonları görüntülemeye yönelik herhangi bir girişimi, doğrulama işlemi etkin bir şekilde iptal edecektir. Pratik olarak etkili olmaları için, bu kuantum anahtarlarının, yalnızca bir kez kullanılacak anahtarlar üretecek olan Tek Kullanımlık Pad (OTP - One-Time Pad) şifrelemesi ile kullanılması gerekir [35].

Tüm bu sebeplerden dolayı, kuantum hesaplama ve blok zincirinin geleceği son derece belirsizdir ve bilgisayar biliminin geleceğinde belirleyici faktörlerden biri olabilir. Blok zinciri interneti demokratikleştirmeye, kripto para birimleri oluşturmaya yardımcı oldu ve Bitcoin ve Ethereum [36] gibi popüler blok zincirleri biçiminde dünyanın en büyük dağıtılmış bilgisayar ağlarını oluşturdu. Buna karşılık, henüz başlangıç aşamasında olan kuantum hesaplama, zamanımızın en etkili bilimsel ve teknolojik sorularının çoğunun çözülmesine yardımcı olma potansiyeline sahiptir ve teknolojiyi henüz öngörülemez şekillerde ilerletir. Kuantum hesaplama ve blok zinciri çatışır, epik

boyutlarda bir felaket olabilir. Bununla birlikte, kriptografi giderek kuantum dirençli şifreleme yöntemleri oluşturmak için ilerlemeye devam ederse veya kuantum şifrelemenin kendisi blok zincirlerine entegre edilirse, bu umut verici teknolojilerin birlikteliği, olumlu bir etki yaratma potansiyeli daha yüksek, daha güvenli, demokratik bir internet oluşturmaya yardımcı olabilir.

6.1.1 Olumsuz Etkileri

Kuantum bilgisayarların blok zincirler üzerindeki olası olumsuz etkilerinden bahsedilecek olursa;

Açık Anahtar Şifreleme : Kripto para birimleri, açık anahtarlı şifreleme (public-key cryptography) olarak bilinen bir teknikte güvence altına alınmaktadır. Bu teknoloji ile mesajlar şifrelenir ve tek hedeflenen alıcının onları görebilmesi için çevrimiçi işlemler güvence altına alınmaktadır. Bu sistem, herkesin görebileceği bir genel anahtar, yalnızca sahibinin görebileceği özel bir anahtarla birleştirmektedir [37].

Hash Algoritmaları : Blok zincirleri, kuantum bilgisayarın bozabileceği bir tür dijital parmak izi olan hash algoritmalarına sahiptir. Kuantum bilişim, kullanıcıların dijital varlıklarını takip etmek için kullandıkları kripto para cüzdanlarına karşı savunmasız olabilir. Bu cüzdanlar, bireylerin blok zinciri varlıklarına erişmek için özel anahtarlarını tutar. Kuantum korsanları tarafından planlanan başarılı bir saldırı, bir cüzdanın geçersiz kılınmasına neden olabilir.

Kuantum Bilişim : Kuantum bilgisayarlar, kubitlerde depolanan verileri manipüle etmektedir. Örneğin, bu bilgisayarlar şifrelemeyi kırmak için günümüzün cihazlarından önemli ölçüde daha fazla binlerce kubit gerektirecektir. Bu makineler ayrıca şu anda mümkün olandan çok daha fazla uzun süreler boyunca hesaplamaları yürütmelerine izin verecek kalıcı kubitler gerektirmektedir. Mevcut kuantum bilgisayarların gelişimi devam ederse, kuantum bilişim kripto endüstrisi için ciddi bir tehdit oluşturarak açık anahtar şifrelemesini kıracaktır. Sadece kripto para ticaretini değil, aynı zamanda para birimlerini de etkileyecektir [26].

Kuantum Korsanları - Kripto Hack : Kuantum korsanları, kuantum bilgisayarları kullanarak blok zinciri şifrelemesini aşabilir ve bilinen şekliyle güvenli kripto para biriminin sona ermesine yol açabilir. Kuantum şifreleme, blok zinciri kriptografisini yenebilirse, büyük kripto para hırsızlığına ve tüm kripto endüstrisi için çökmeye bile büyük hasarlara yol açabilir. Örneğin; Deloitte

tarafından yapılan bir araştırma, Bitcoin'in %25'inin tek bir saldırıda çalınabileceğini gösterdi. Ocak 2022 itibarıyla, bu yaklaşık 300 milyar dolar olacak ve kripto para piyasası büyümeye devam ettikçe, kuantum bilgisayar tabanlı bir kripto hack, trilyonlarca doların çalınmasıyla sonuçlanabilir, potansiyel olarak küresel ekonomiyi kaosa sürükleyebilir ve bu süreçte tüm blok zincirlerini yok edebilir [1].

Kripto Para Madenciliği : Kuantum bilgisayarların kripto para madenciliği içinde büyük bir tehdittir. Bu bilgisayarlar, teoride olduğu gibi, ASIC'ler gibi geleneksel madencilik ekipmanlarından katlanarak daha hızlı madencilik yapabiliyorsa, istikrarsız varlık fiyatlarına, %51 saldırılarına ve madencilik gücünün aşırı merkezleşmesine yol açabilir.

Maliyet : Kuantum anahtar oluşturma dahil olmak üzere kuantum hesaplama işlevlerinin düğüm operatörleri aracılığıyla nasıl dağıtılacağıdır. Şu anda, çoğu kuantum bilgisayarı hem oldukça deneysel hem de son derece pahalıdır; bu, gerçekten merkezi olmayan bir blok zinciri için gereken çok sayıda düğüm operatörüne ulaşmanın zor olabileceği anlamına gelir. Ancak bu değişebilir; Çin'deki bir şirket, şu anda tam bir Ethereum düğümünü çalıştırmak için gerekenden çok daha az olan, yalnızca 5.000 dolara mal olan küçük bir kuantum bilgisayarı tanıttı.

6.1.2 Olumlu Etkileri

İşlem Süresi : Olumsuz etkilerde bahsedilen maddelerden çoğu yeni kuantum blok zincirlerinin yaratılmasına atıfta bulunurken, kuantum teknolojisinin mevcut blok zincirlerine uygulanabilmesi de mümkündür; bu, hem merkezleşmeyi artıracak hem de Bitcoin, Ethereum ve Solana gibi büyük blok zincirleri için işlem sürelerini potansiyel olarak azaltabilecektir.

Kauntum Direnci : Kuantum bilgisayarlarının gelişim sürecinin tahmin edilememesi sonucu geleneksel kriptografinin kırılmayacağı düşünülebilir. Örneğin, Bitcoin'de kullanılan SHA-256 [38] şifrelemesinin kuantuma dayanıklı olabileceğine inanılıyor [39]. Kuantum bilgisayarlar mevcut blok zinciri şifreleme yöntemlerini kırabilecek olsa bile, bu 10-20 yıl alabilir ve blok zinciri kriptografilerine yeni ve daha güçlü şifreleme yöntemleri geliştirmek için güçlü bir başlangıç sağlar [40]. Ek olarak, eliptik eğri kriptografisine en yaygın alternatif olan RSA şifrelemesi [41] de bir

miktar kuantum dirençli olabilir. Geleneksel şifre çözme söz konusu olduğunda eliptik eğri şifrelemesi RSA şifrelemesinden daha güvenli kabul edilirken, kuantum şifre çözme söz konusu olduğunda bunun tersinin doğru olabileceğini öne sürüyorlar [42]. Ayrıca, RSA kuantum hacklenebilir [43] hale gelse bile sürekli değişen cüzdan adresleri, kuantum bilgisayarların blok zincirlerini kırma veya kripto para birimi çalma konusundaki pratik yeteneğinin çoğunu hafifletebilir [1].

7 Sonuç ve Tartışma

Kuantum hesaplama, kubitler sayesinde geleneksel ve süper bilgisayarlara kıyasla problem çözmeyi hızlandırma konusunda önemli bir yeteneğe sahiptir. Bu bilgisayarların yaygın olarak farklı sektörler tarafından benimsenmesine daha birkaç yıl var, ancak Google, IBM ve Ledger gibi bazı büyük ölçekli teknoloji şirketleri şu anda yatırım yapmaktadır.

Kuruluşların, en son gelişmeleri takip ederek, verileri potansiyel bilgisayar korsanlarından nasıl daha iyi koruyabileceklerini öğrenmeleri önerilir. Aynı zamanda, kuruluşların geleceğin teknolojisiyle kesintiye uğramaması için iş ve endüstri yörüngelerini şekillendirerek kuantum bilişim geleceğine hazırlanmaları gerekir.

Finans, siber güvenlik, kimya ve ilaç gibi pek çok sektöre ait şirketlerin potansiyel bilgisayar korsanlarından veri güvenliğinin nasıl daha iyi sağlanabileceği öğrenilerek kuantum hesaplama faydalanabilirler. Örneğin; kimyasal deneylerin test edilmesi pahalı bir süreçtir ve araştırmacılar çok daha fazla yöntemi bir arada hızla test edebilir. Kuantum hesaplamaların var olduğu kuantum bilgisayarlarda testler için gerekli olan simülasyonlar kimya ve fizik problemlerini çözebilir. Ar-Ge ve üretim verimliliklerini geliştirerek daha iyi çözüm hedeflerine yol gösterebilir. Yenilenebilir enerji için pillerin maliyetini, boyutunu ve şarj hızını iyileştirmek için geliştirilen yeni algoritmalar bu bilgisayarlarda test edilebilir. Tüketim ürünleri, hayvancılık ve ulaşım gibi sektörlerde malzeme tasarımları oluşturmak ve test etmek, yeni olasılıkları daha hızlı oluşturabilir ve aynı zamanda maliyetleri azaltabilecek çözümler üretebilir.

Öte yandan, yapay zeka ürün ve hizmet özelliklerini optimize etmek, yetenek yönetimini geliştirmek, tedarik zinciri operasyonlarında kestirimci bakım, müşteri hizmetleri analizi, lojistik ağ operasyonları

ve çok daha fazlası için kullanılmaktadır. İşletmeler, pazarlama ve satış, üretim, insan kaynakları, strateji ve finans ve tedarik zinciri yönetimi gibi iş fonksiyonlarının yarısında yapay zekadan elde edilen gelir artışlarını rapor etmektedir. En çok başarıyı gören şirketler, başarılarını yapay zeka ile açıklamaktadırlar. İşletmeler aynı zamanda, genel ve özel ağlar arasında paylaşılan dağıtılmış bir defter olan blok zincirine büyük yatırımlar yapmaktadır. Bilgisayar ağındaki her düğüm, zincire eklenmeden önce her yeni bloğun onaylandığı şifrelenmiş bilgileri tutar. Blok zinciri, bu teknolojinin faydalarından yararlanmak için bir aracıya ihtiyaç duymaktadır ve maliyetleri düşürmeye yardımcı olduğu için kuruluşlara stratejik değer getirmektedir. Belirli koşullar karşılandığında tetiklenecek şekilde otomatikleştirilen akıllı sözleşmelerde yaygın olarak kullanılır. İşletmeler çeşitli olanaklar için blok zinciri teknolojilerini araştırmaktadırlar. QR kod tarama ile ürünlerin orijinallikini doğrularken veya işçilik ve çevreye uygunluk için malzeme işleme tabi tutulurken şeffaflık ve izlenebilirlik tedarik zinciri operasyonları için önemlidir. Güvenli kimlikler ve araç bilgileri gibi kimlik doğrulama yoluyla insanların ulaşım hizmetlerini kullanma ve ödeme şeklini iyileştirme bir diğer örnek olarak verilebilir [44].

Blok zincir tarafında anahtarların güvenliği için yükseltilmesini sağlayabilmek için kuantum hesaplama teknolojisine ihtiyaç duyulacaktır. Ancak bu teknoloji aynı zamanda tehdit olarak da görülmektedir. Bu noktada, yazılım endüstrisi kriptografi teknolojileri için tehdit olan kuantum hesaplama sorununun üstesinden gelebilmek için girişimlerde bulunmaktadır. Amerika Birleşik Devletleri Ulusal Standartlar ve Teknoloji Enstitüsü (NIST), kuantum kanıtlı kriptografi algoritmaları oluşturmak için birkaç yıldır dünyanın her yerinden uzmanlarla işbirliği yapıyor. Örneğin, Bitcoin sonrasında ikinci en büyük kripto para birimi olan Ethereum projesi, post-kuantum projesini hazırlamaya başladı. 2019'da StarkWare konferansında, Justin Drake, Ethereum 3.0'daki kuantum direnci kavramları hakkında sunum yapmıştı. Bir diğer örnek, Cambridge Quantum Computing ve Honeywell, herhangi bir blok zinciri ağına dağıtılabilen kuantum güvenlik teknolojisi üzerine çalışmaktadırlar [35]. Kuantum hesaplama çağı için, birkaç firma kripto para birimleri ve blok zincir teknolojisi geliştiriyor. Örneğin, Hyperledger

[45], Quantum Resistant Ledger [46] ve Bitcoin Post Quantum [47].

Bu çalışmada, kuantum hesaplama ve blok zinciri teknolojilerinin farklı yapılarla sahip olmasından bahsedilmiştir. Aynı zamanda, gelecekte her iki teknoloji birlikte kullanıldığında aynı amaç için mi yoksa farklı amaçlar için mi kullanılacağı tartışılmıştır. Birbirinden farklı olan bu iki teknoloji, gelecekte birbirleriyle etkileşime girdiklerinde sonsuza kadar değişkenlik gösterecek bir ortaklığa sahip olabileceklerinden bahsedilmiştir.

Kaynaklar

- [1] Quantum Computing and Blockchain: What You Need to Know <https://supraoracles.com/academy/quantum-computing-and-blockchain-what-you-need-to-know/> (11.03.2022).
- [2] Rodenburg, Brandon, And Stephen P. Pappas. Blockchain And Quantum Computing. The Mitre Corporation, 2017.
- [3] Ikeda, Kazuki. "Security And Privacy Of Blockchain And Quantum Computation." Advances In Computers. Vol. 111. Elsevier, 2018. 199-228.
- [4] Kiktenko, Evgeniy O., Et Al. "Quantum-Secured Blockchain." Quantum Science And Technology 3.3 (2018): 035004.
- [5] Gao, Yu-Long, Et Al. "A Secure Cryptocurrency Scheme Based On Post-Quantum Blockchain." Ieee Access 6 (2018): 27205-27213.
- [6] Li, Chuntang, Et Al. "Quantum Blockchain: A Decentralized, Encrypted And Distributed Database Based On Quantum Mechanics." Journal Of Quantum Computing 1.2 (2019): 49.
- [7] Grassl, Markus, Et Al. "Applying Grover's Algorithm To Aes: Quantum Resource Estimates." Post-Quantum Cryptography. Springer, Cham, 2016.
- [8] Yimsiriwattana, Anocha, And Samuel J. Lomonaco Jr. "Distributed Quantum Computing: A Distributed Shor Algorithm." Quantum Information And Computation II. Vol. 5436. Spie, 2004.
- [9] Fernandez-Carames, Tiago M., And Paula Fraga-Lamas. "Towards Post-Quantum Blockchain: A Review On Blockchain Cryptography Resistant To Quantum Computing Attacks." Ieee Access 8 (2020): 21091-21116.
- [10] Alghamdi, Sarah, And Sultan Almuhammadi. "The Future Of Cryptocurrency Blockchains In The Quantum Era." 2021 Ieee International Conference On Blockchain (Blockchain). Ieee, 2021.
- [11] Srivastava, Tanya, Et Al. "Integration Of Quantum Computing And Blockchain Technology: A Cryptographic Perspective." Multimedia Technologies In The Internet Of Things Environment, Volume 3. Springer, Singapore, 2022. 197-228.

- [12] Kiayias, Aggelos, and Dionysis Zindros. "Proof-of-work sidechains." International Conference on Financial Cryptography and Data Security. Springer, Cham, 2019.
- [13] Gaži, Peter, Aggelos Kiayias, and Dionysis Zindros. "Proof-of-stake sidechains." 2019 IEEE Symposium on Security and Privacy (SP). IEEE, 2019.
- [14] Sriman, B., S. Ganesh Kumar, And P. Shamili. "Blockchain Technology: Consensus Protocol Proof Of Work And Proof Of Stake." Intelligent Computing And Applications. Springer, Singapore, 2021. 395-406.
- [15] Şafak, Emre, Et Al. "Dağıtık Defter Teknolojileri Ve Uygulama Alanları Üzerine Bir İnceleme." Avrupa Bilim Ve Teknoloji Dergisi 29 (2021): 36-45
- [16] Meraklı, Serkan. "Merkeziyetsiz Finans (Defi) Faaliyetlerinin İzinsiz Bankacılık Faaliyetinde Bulunma Suçu Bakımından Değerlendirilmesi." Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi 27.2 (2021): 1156-1190.
- [17] Friedman, Jonathan R., Et Al. "Quantum Superposition Of Distinct Macroscopic States." Nature 406.6791 (2000): 43-46.
- [18] Horodecki, Ryszard, Et Al. "Quantum Entanglement." Reviews Of Modern Physics 81.2 (2009): 865.
- [19] Steane, Andrew. "Quantum Computing." Reports On Progress In Physics 61.2 (1998): 117.
- [20] Chapman, Shira, And Giuseppe Policastro. "Quantum Computational Complexity From Quantum Information To Black Holes And Back." The European Physical Journal C 82.2 (2022): 1-40.
- [21] Kripto Minting (Basma) vs. Mining (Madencilik): Fark nedir? <https://phemex.com/tr/blogs/kripto-minting-vs-mining-fark-nedir> (22.06.2022)
- [22] Gao, Yu-Long, et al. "A novel quantum blockchain scheme base on quantum entanglement and DPOs." Quantum Information Processing 19.12 (2020): 1-15.
- [23] Sun, Xin, Piotr Kulicki, and Mirek Sopek. "Lottery and auction on quantum blockchain." Entropy 22.12 (2020): 1377.
- [24] Forecast size of the quantum computing market worldwide in 2020 and 2027 <https://www.statista.com/statistics/1067216/global-quantum-computing-revenues/> (03.02.2022)
- [25] Castelvechi, Davide. "The Race To Save The Internet From Quantum Hackers." (2022): 198-201.
- [26] Blockchain Vs. Quantum Computing: Is Quantum Computing The Biggest Threat To Crypto? <https://www.blockchain-council.org/blockchain/blockchain-vs-quantum-computing-is-quantum-computing-the-biggest-threat-to-crypto/> (08.12.2021)
- [27] YÜCELEN, Aziz Mahmut, Abdullah BAYKAL, and Cengiz COŞKUN. "Kriptolojide eliptik eğri algoritmasının uygulanması." Dicle Üniversitesi Mühendislik Fakültesi Mühendislik Dergisi 8.3 (2017): 503-513.
- [28] Proos, John, And Christof Zalka. "Shor's Discrete Logarithm Quantum Algorithm For Elliptic Curves." Arxiv Preprint Quant-Ph/0301141 (2003)
- [29] Cheung, Donny, Et Al. "On The Design And Optimization Of A Quantum Polynomial-Time Attack On Elliptic Curve Cryptography." Workshop On Quantum Computation, Communication, And Cryptography. Springer, Berlin, Heidelberg, 2008.
- [30] Is Bitcoin Safe from Shor's Algorithm or Grover's Algorithm? <https://www.insidequantumtechnology.com/news-archive/is-bitcoin-safe-from-shors-algorithm-or-grovers-algorithm/> (29.07.2021)
- [31] P. Waterland, "Quantum Resistant Ledger (Qrl)," Qrl Tech. Rep. 1 Oct. 2016. [Online]. Available: https://github.com/theqrl/whitepaper/blob/master/Qrl_Whitepaper.pdf
- [32] Scarani, Valerio, et al. "The security of practical quantum key distribution." Reviews of modern physics 81.3 (2009): 1301.
- [33] Jayaraman, Ramkumar, And Manoj Kumar. "Quantum Cryptography And Quantum Key Distribution." Holistic Approach To Quantum Cryptography In Cyber Security. Crc Press 179-192.
- [34] Ahn, Jongmin, Et Al. "Toward Quantum Secured Distributed Energy Resources: Adoption Of Post-Quantum Cryptography (Pqc) And Quantum Key Distribution (Qkd)." Energies 15.3 (2022): 714.
- [35] Upadhyay, Gaurav, And Manisha J. Nene. "One Time Pad Generation Using Quantum Superposition States." 2016 Ieee International Conference On Recent Trends In Electronics, Information & Communication Technology (Rteict). Ieee, 2016.
- [36] Vujičić, Dejan, Dijana Jagodić, And Siniša Randić. "Blockchain Technology, Bitcoin, And Ethereum: A Brief Overview." 2018 17th International Symposium Infoteh-Jahorina (Infoteh). Ieee, 2018.
- [37] Bos, Joppe W., Et Al. "Elliptic Curve Cryptography In Practice." International Conference On Financial Cryptography And Data Security. Springer, Berlin, Heidelberg, 2014.
- [38] Yoshida, Hirotaka, and Alex Biryukov. "Analysis of a SHA-256 variant." International Workshop on Selected Areas in Cryptography. Springer, Berlin, Heidelberg, 2005.
- [39] Alghamdi, Sarah, And Sultan Almuhammadi. "The Future Of Cryptocurrency Blockchains In The Quantum Era." 2021 Ieee International Conference On Blockchain (Blockchain). Ieee, 2021.
- [40] Seo, William Yunsoo. "Comparing Rsa Ecc And Post Quantum Cryptography." J. Math. Anal. Appl. 10 (2018): 19-33.
- [41] Milanov, Evgeny. "The RSA algorithm." RSA laboratories (2009): 1-11.

- [42] Elliptic-Curve Cryptography. Grayblock. <https://medium.com/coinmonks/elliptic-curve-cryptography-6de8fc748b8b>. (2018, Haziran)
- [43] Zhao, Yi, et al. "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems." *Physical Review A* 78.4 (2008): 042333.
- [44] Quantum Computing With AI and Blockchain In 2022: The Future of IT - <https://www.simplilearn.com/ai-and-blockchain-with-quantum-computing-article> (07.07.2022)
- [45] Cachin, Christian. "Architecture of the hyperledger blockchain fabric." *Workshop on distributed cryptocurrencies and consensus ledgers*. Vol. 310. No. 4. 2016.
- [46] Quantum Resistant Ledger - <https://coinmarketcap.com/currencies/quantum-resistant-ledger/> (2022, Aralık)
- [47] Anhao, Noah. "Bitcoin post-quantum." (2018).