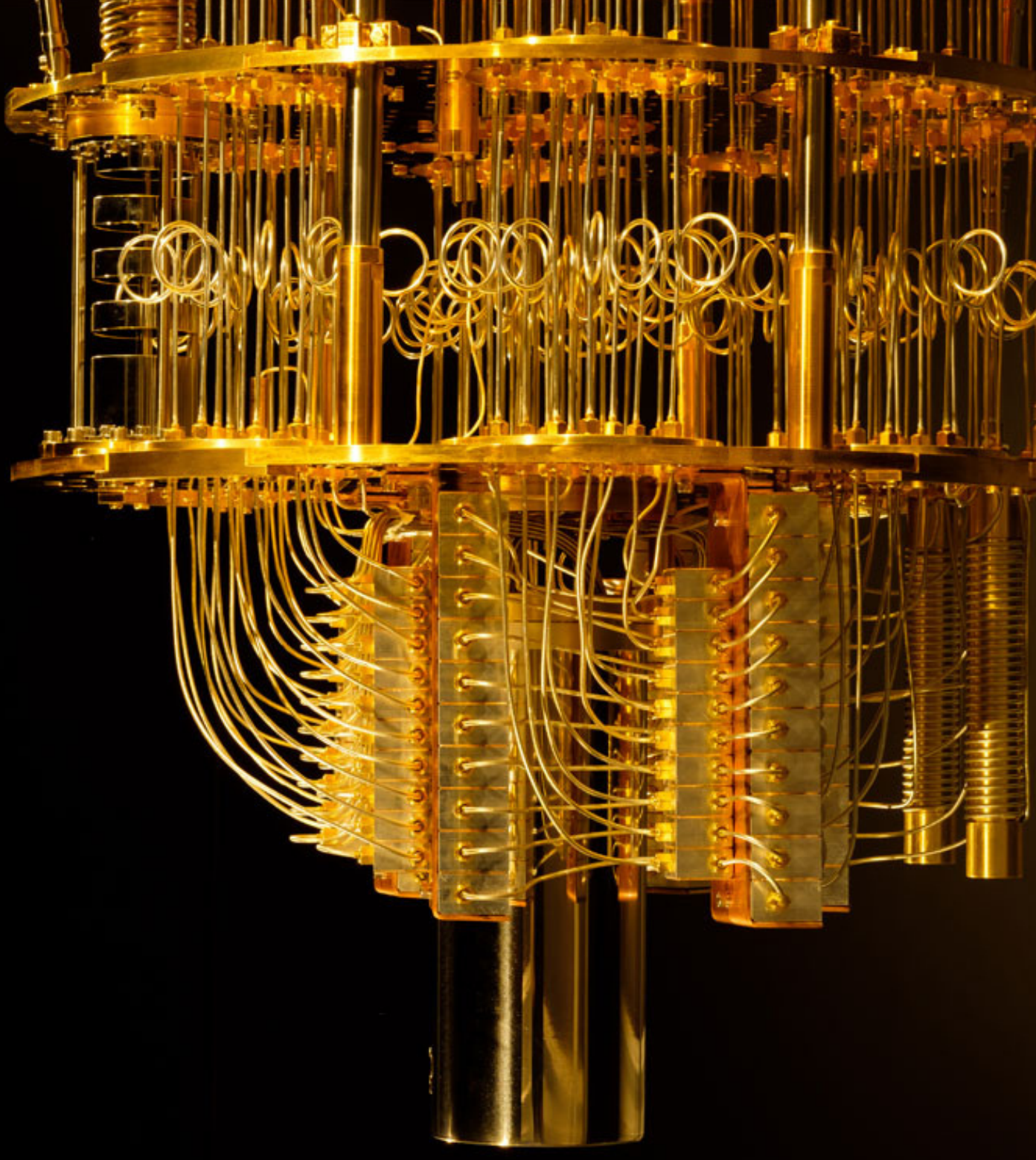


KT HACK-2020

BİLGİ KİTAPÇIĞI

Değerli katılımcımız, bu bilgi kitapçığını hazırlarkenki temel amacımız size her konuyla ilgili uzun uzadıya bilgi vermekten ziyade, bu alanlarla ilgili ufak bir literatür taraması sağlamaktır. Dolayısıyla her konu başlığının altında konu ile alakalı küçük bir tanıtım yapıldıktan sonra, alan ile alakalı daha derinlemesine nereden bilgi edinebileceğinizin ve daha önce Dünya'nın farklı yerlerinde düzenlenmiş hackatonlarda bu konularla ilgili ne gibi projeler yapıldığı bilgisine ulaşabilirsiniz.



İÇİNDEKİLER

• KUANTUM BİLGİSAYARLAR	4
• KUANTUM HESAPLAMA PARADİGMALARI	13
• KUANTUM SİMÜLASYON	18
• KUANTUM SENSÖRLER	22
• KUANTUM OYUNLAR	25
• KUANTUM MAKİNE ÖĞRENMESİ	30
• KUANTUM FİNANS UYGULAMALARI	37
• KUANTUM KRİPTOGRAFİ	43
• KUANTUM AĞLAR	47
• KUANTUM HATA DÜZELTME	50
• ÖNCEKİ HACKATHONLAR	52

KUANTUM BİLGİSAYARLAR

Kuantum bilgisayarlar klasik ikili (bir bitin 1 ya da 0 değerini alabildiği) sistemler yerine, kuantum fiziğinde süperpozisyon olarak bilinen kavramı kullanan kuantum bitler ile çalışmaktadır. Kübit olarak adlandırılan kuantum bitler aynı anda hem 0 hem de 1 olabilmektedir. Böylece kuantum bilgisayarlar, hesaplama kapasitesi olarak ciddi bir fark yaratmaktadır. Yıllarca kuantum bilgisayarların inşasına imkânsız gözüyle bakılmış olsa da günümüzde endüstriyel kapasitede kuantum bilgisayarların taslakları üzerinde çalışılmaktadır.

Kuantum bilgisayarlarda ana hedef yüksek sayıda kübit ile işlem yaparak hız elde etmektir. Ancak kübit sayısı arttıkça, daha zor öngörülebilir voltaj, sıcaklık ve diğer faktörler yüzünden, cihazı kontrol etmek ve sonuçlarda kesinlik sağlamak zorlaşıyor. Dolayısıyla yeni çalışmalar, çok sayıda kübiti bir arada barındırabilen ve dış faktörlerden olabildiğince az etkilenen makinaların tasarımı üzerinde yoğunlaşıyor. Bunun iyi bir örneği olan Sussex Üniversitesi'nde yapılan çalışma sonucu, milyonlarca kübiti bir arada tutan kuantum bilgisayarların inşa edilebileceği açıklanmıştır.



KUANTUM BİLGİSAYARLAR



Amerikalı teorik fizikçi David DiVincenzo'ya göre geniş ölçekli bir kuantum bilgisayar inşa edebilmek için olmazsa olmaz gereklilikler bulunmaktadır:

- Kübit sayısını artırmak için fiziksel olarak ölçeklenebilirlik
- Rastgele değerlere başlatılabilen kübitler oluşturabilmek
- Eşevresizlik (decoherence) zamanından daha hızlı olan kuantum kapıları tasarlamak
- Evrensel kuantum kapıları oluşturabilmek
- Kolayca okunabilen kübitler

Hesaplama noktasındaki farklılıklar ve bu gereklilikler hem teorik olarak hem de uygulama olarak farklı kuantum bilgisayarlar modellerinin ortaya çıkmasına sebebiyet vermiştir.

KUANTUM BİLGİSAYARLAR

Pratik önemi olan dört ana model şunlardır:

Kuantum kapı dizisi (Quantum gate array):

Birkaç kübit kuantum geçidi dizisine ayrılan hesaplama modelidir. Yaygın olarak kuantum devre (Quantum circuit model) modeli olarak tanınmaktadır.

Tek yönlü kuantum bilgisayar modeli (One-way quantum computer):

Yüksek derecede karışmış başlangıç durumuna veya küme durumuna uygulanan tek kübit ölçümleri dizisine ayrıştırılmış hesaplama modelidir. Ölçüm tabanlı kuantum bilgisayar (measurement based quantum computer) olarak da bilinmektedir.

Adyabatik kuantum bilgisayar modeli (Adiabatic quantum computation):

Kuantum tavlama (Quantum annealing) dayanan bir kuantum bilgisayar modelidir.

Topolojik kuantum bilgisayar modeli (Topological quantum computer):

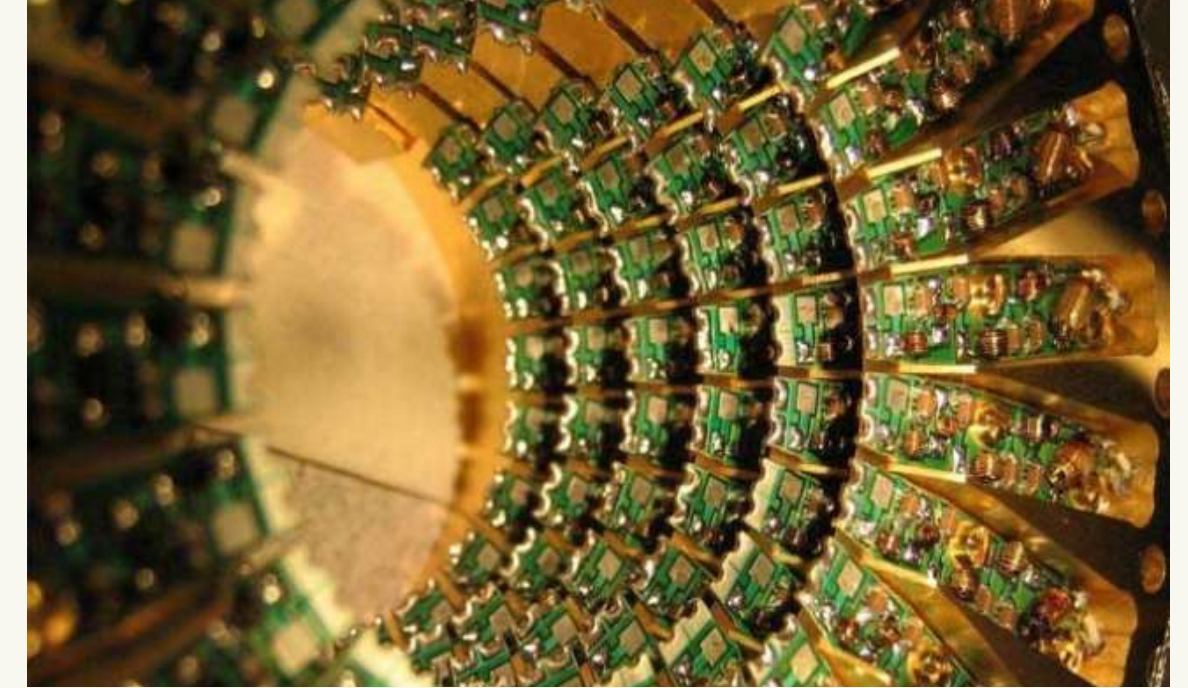
Üç boyutlu bir uzayda örgüler oluşturmak için birbirlerinden geçen iki boyutlu kuasiparçacıkları (quasiparticle) kullanan teorik bir kuantum bilgisayar modelidir.

KUANTUM BİLGİSAYARLAR

Teorik olarak mümkün olan ancak fiziksel anlamda uygulanması çok zor olan bir başka önemli model daha bulunmaktadır:

**Kuantum Turing makinesi (Quantum Turing machine)
veya (evrensel kuantum bilgisayar (universal
quantum computer):**

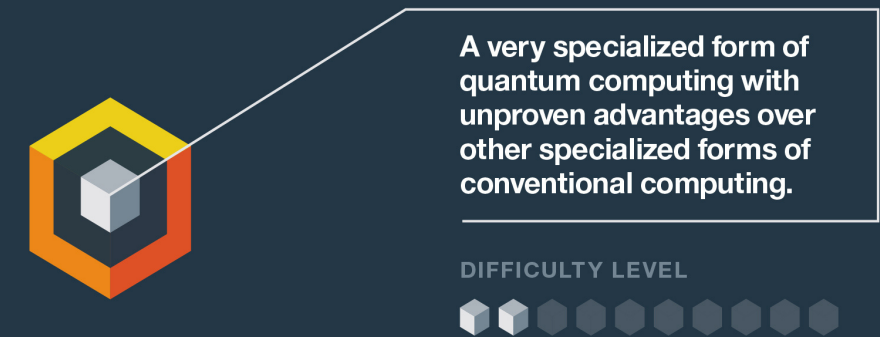
En güçlü, en genel ve gerçekleştirmesi en zor olan modeldir. Bir kuantum bilgisayarın etkilerini modellemek için kullanılan soyut bir makinedir. Kuantum hesaplamanın tüm gücünden faydalanmayı sağlayabilecek bir model sağlar. Kuantum Turing makineleri, geçiş matrislerine dayanan bir çerçevede klasik ve olasılıklı Turing makineleri ile ilişkilendirilebilirler.



İnfografik İncelemesi

IBM Research ekibinden bilim insanları ve mühendisler göre, bu ve benzeri bütün faktörler göz önüne alındığında ve modeller değerlendirildiğinde mümkün olduğu düşünülen üç tür kuantum bilgisayar ön plana çıkmaktadır.

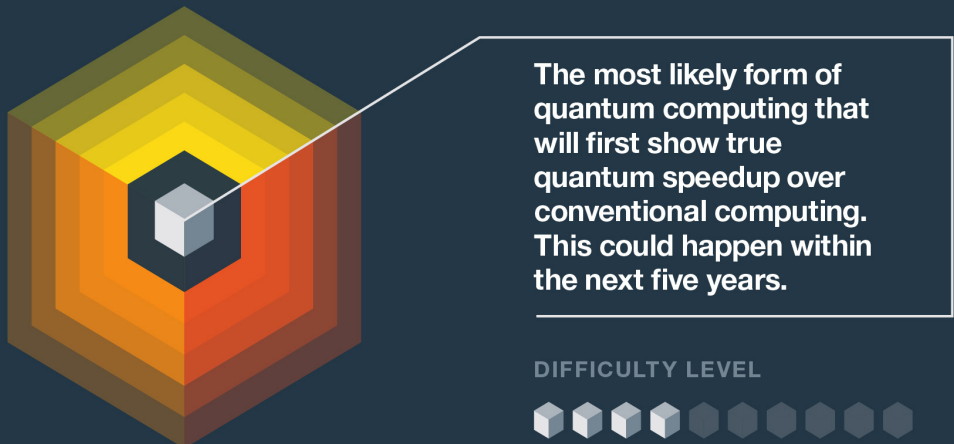
The three known types of quantum computing and their applications, generality, and computational power.



Quantum Annealer

The quantum annealer is least powerful and most restrictive form of quantum computers. It is the easiest to build, yet can only perform one specific function. The consensus of the scientific community is that a quantum annealer has no known advantages over conventional computing.

- APPLICATION**
Optimization Problems
- GENERABILITY**
Restrictive
- COMPUTATIONAL POWER**
Same as traditional computers



Analog Quantum

The analog quantum computer will be able to simulate complex quantum interactions that are intractable for any known conventional machine, or combinations of these machines. It is conjectured that the analog quantum computer will contain somewhere between 50 to 100 qubits.

- APPLICATIONS**
Quantum Chemistry
Material Science
Optimization Problems
Sampling
Quantum Dynamics
- GENERABILITY**
Partial
- COMPUTATIONAL POWER**
High



Universal Quantum

The universal quantum computer is the most powerful, the most general, and the hardest to build, posing a number of difficult technical challenges. Current estimates indicate that this machine will comprise more than 100,000 physical qubits.

- APPLICATIONS**
Secure computing
Machine Learning
Cryptography
Quantum Chemistry
Material Science
Optimization Problems
Sampling
Quantum Dynamics
Searching
- GENERABILITY**
Complete with known speed up
- COMPUTATIONAL POWER**
Very High

KUANTUM BİLGİSAYARLAR

Dilerseniz infografikte sunulan modellere bir göz atalım:

Kuantum Tavlayıcı

Bu model kuantum bilgisayar modellerinin en az güçlü, en kısıtlı ve oluşturması en kolay olanıdır. Yalnızca belirli bir işlevi gerçekleştirebilir. Bilimsel dünyasının bu model için ortak fikri; bu modelin, geleneksel bilgisayarlara göre bilinen bir avantajı olmadığıdır.

Uygulama Alanı: Optimizasyon problemleri

Genellik: Kısıtlı

Bilgisayım Gücü: Geleneksel bilgisayarlar ile aynı

Analog Kuantum Bilgisayar

Analog kuantum bilgisayarı, bilinen herhangi bir geleneksel makine veya bu makinelerin kombinasyonları için uygulanamaz karmaşık kuantum etkileşimlerini simüle edebilme kapasitesine sahiptir. Analog kuantum bilgisayarların 50 ile 100 kübit arasında bir yerde olacağı tahmin edilmektedir. 2019 yılında IBM, 53 kübitlik bir sistem tasarlamayı başarmıştır. Spesifik problemler için kuantum hesaplamanın farkının hissedilebileceği en olası kuantum hesaplama biçimi olma potansiyeli taşır. Infografiğe göre geliştirmelerinin zorluğu orta sınıftadır.

Uygulama Alanları: Kuantum kimyası
Malzeme bilimi
Optimizasyon problemleri
Örnekleme (Sampling)
Kuantum dinamikleri

Genellik: Kısmi

Bilgisayım Gücü: Yüksek

KUANTUM BİLGİSAYARLAR

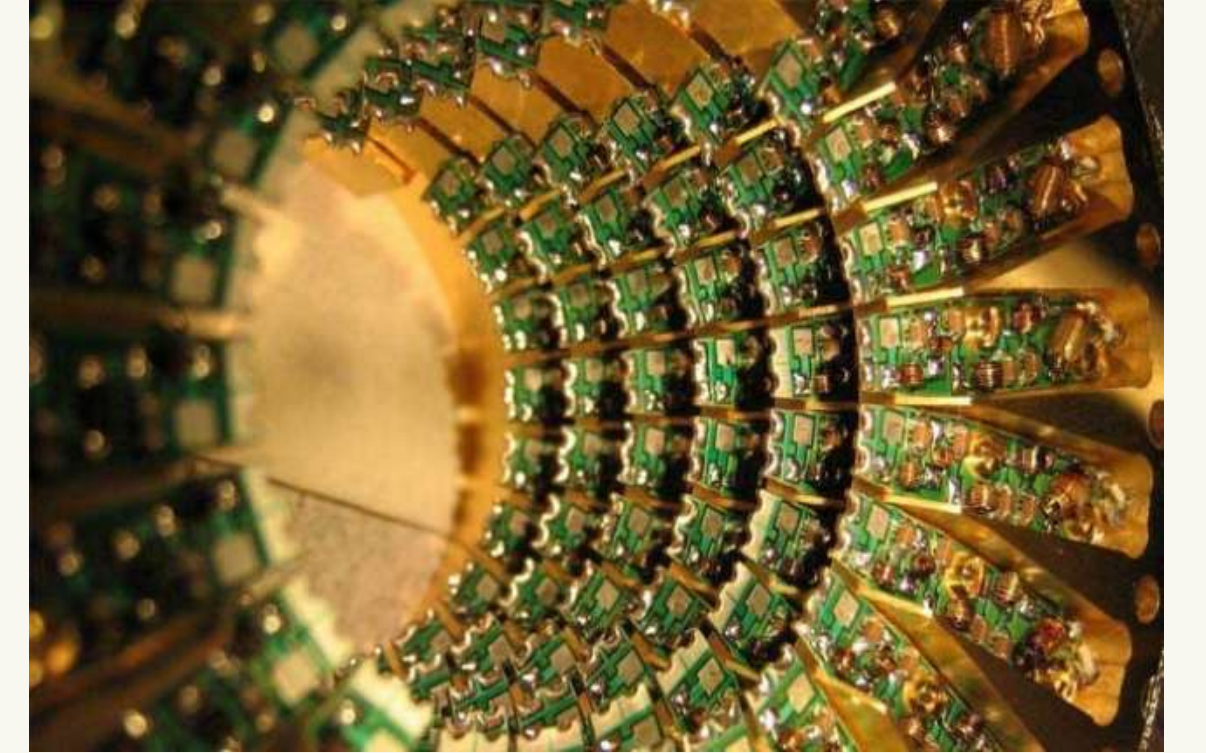
Evrensel Kuantum Bilgisayar

Evrensel kuantum bilgisayarı, en güçlü, en genel ve en zor olan kuantum bilgisayar modelidir. Geliştirilmesi şu an için teknik olarak mümkün görünmemektedir. Mevcut tahminler, bu makinenin 100.000'den fazla fiziksel kübit içereceğini göstermektedir. Evrensel kuantum bilgisayar, kuantum bitleri için kübit sayısı ile üstel olarak katlanarak ölçeklenen durumlar oluşturmak üzere süperpozisyon ve dolaşıklığın kuantum mekanik özelliklerinden yararlanır. Geleneksel bilgisayarların ötesinde üstel olarak çalışabilen çok daha hızlı bilgisayar modeline sahiptir. Geliştirilmesi bilim dünyası, teknoloji dünyası ve iş dünyasına birçok katkı sunabilir.

Uygulama Alanları: Güvenli bilgisayarım
Makine öğrenimi
Kriptografi
Kuantum kimyası
Optimizasyon problemleri
Örnekleme (Sampling)
Kuantum dinamikleri
Kuantum arama algoritmaları

Genellik: Genel

Bilgisayım Gücü: Çok yüksek



Genellikle herkes kuantum bilgisayarların kübit sayısına odaklanmaktadır. Ancak kuantum bilgisayarlar için en önemli faktör bu değildir. Hata oranı ve eşevresizlik süresi de önemli faktörlerdendir.

KUANTUM BİLGİSAYARLAR

Şirketler ve Çalıştıkları Modeller

Universal Gate Based Quantum Computers			Annealing
Superconducting Architecture			Quantum Annealing
			
Trapped Ions	Topological	Photonic	
			

Yukarıdaki görselde de görüldüğü üzere kuantum bilgisayar geliştirme üzerine çalışan şirketler farklı modelleri temel alıp, farklı mimarilerle çalışmaktadırlar.

KUANTUM BİLGİSAYARLAR

KUANTUM BİLGİSAYARLAR İLE İLGİLİ KAYNAKLAR

(kaynaklara erişmek için lütfen altı çizgili olan bağlantılara tıklayınız)

[Kuantum Bilgisayarların ABC'si](#)

[Kuantum Bilgisayarı Anlamak](#)

[What is a quantum computer?](#)

[MIT Explainer: What is a quantum computer?](#)

[How do quantum computers work?](#)

KUANTUM HESAPLAMA PARADİGMALARI

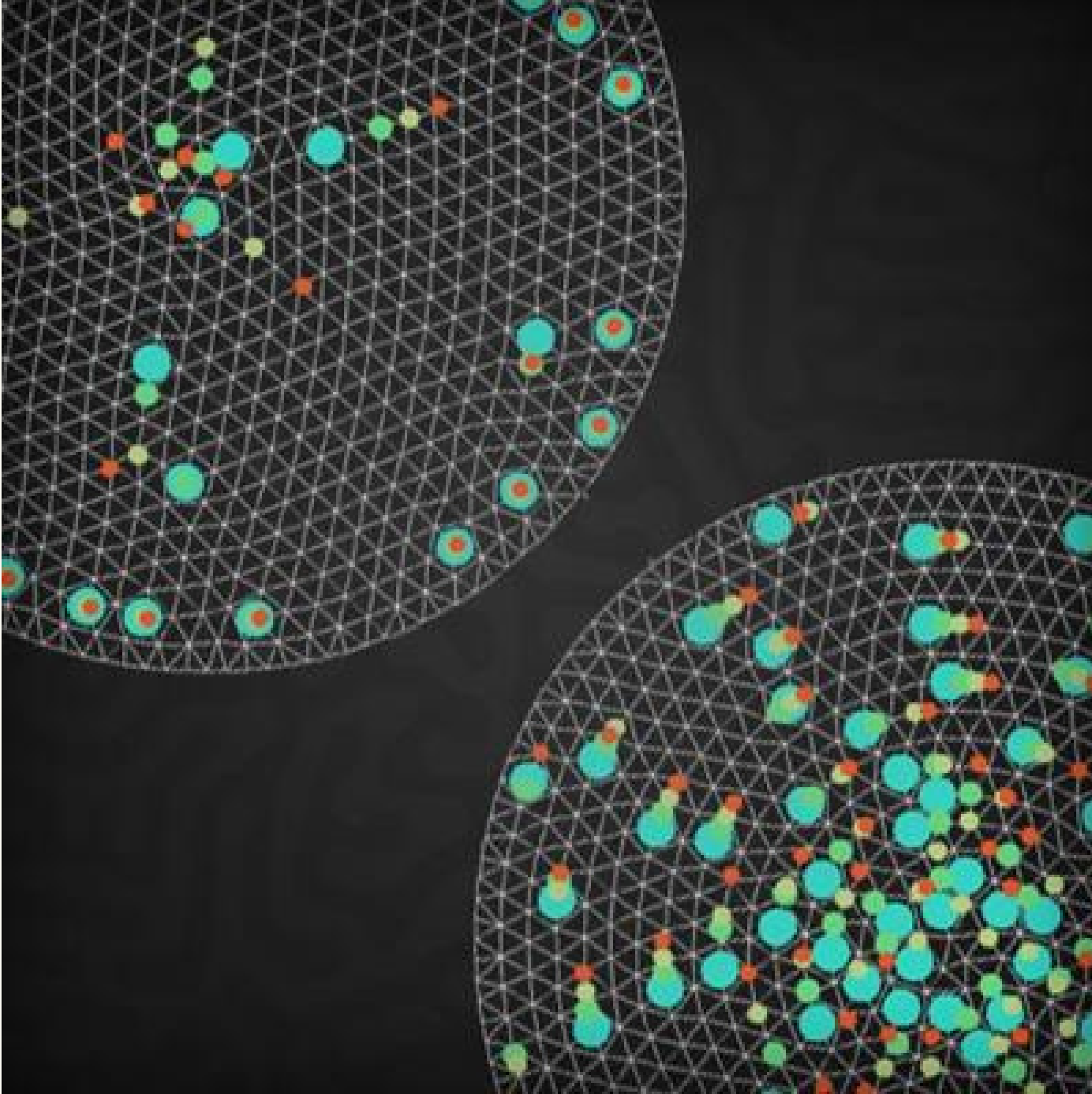
Klasik programlamada bilgisayarların ilk tasarımından beri öne sürülmüş ve kullanılmış farklı programlama dilleri mevcut. En popüler dillerden birisi olan Python, “object-oriented” ve “concurrent-programming” gibi paradigmaları destekliyor. Ancak bir programlama dili Python, C, Java gibi “for” döngülerinden, “class” tanımlamalarından oluşmak zorunda değil. Mesela Haskell tüm değişkenlerin fonksiyon olarak tanımlandığı, “for” döngüsü konsepti yerine “recursion” kullanan bir dildir. Ancak Church-Turing tezinden bildiğimiz üzere hepsinin hesaplama kapasitesi en nihayetinde aynıdır.

Benzer bir durum kuantum bilgisayarlar için de mevcut diyebiliriz. Kübitlerin fiziksel olarak nasıl yapıldığı, sizin onlar üzerinde nasıl operasyonlar yapabileceğinizi kısıtlıyor diyebiliriz.

Kitapçığımızın bu kısmında size bu farklı modellemelerden ve onları nasıl kullanabileceğinizden bahsetmek istiyoruz.



KUANTUM HESAPLAMA PARADİGMALARI



Gate-Based Quantum Computing

En popüler kuantum bilgisayar geliştirme yöntemlerinden birisi olan bu yöntem klasik bilgisayar tasarımından oldukça etkilenmiş durumda diyebiliriz. Kübitlerin üzerinde yapılacak işlemleri bir kuantum devresi oluşturup, operasyonları “gate” olarak tanımlamaya dayanıyor.

En büyük örnek ve ulaşım açısından kolaylık olarak IBM ve QuTech’in erişime açık kuantum bilgisayarları bu mantığa dayanıyor.

[IBM Quantum Experience](#)

[QuTech Quantum Inspire](#)

[Farklı Gate-based kuantum programlama dillerinin kıyaslandığı bir makale](#)

KUANTUM HESAPLAMA PARADİGMALARI

Adiabatic Quantum Computing

Devre tabanlı kuantum hesaplama yöntemi sunulduğundan beri bilgisayar bilimi camiası bir “NP-complete” problemini kuantum bilgisayar kullanarak polinom zamanda çözme üzerine araştırmalar yapıyor. Adyabatik kuantum hesaplama da bu amaçla öne sürülmüş bir yöntem.

Adyabatik kuantum hesaplama metodu fiziksel bir sistemin en düşük enerji seviyesinde (ground-state) kalma isteğini kullanıyor. Temel mantık yapılacak hesaplama simüle edecek bir üniter transformasyonu fiziksel bir Hamiltonyan olarak tanımlayıp, sistemi yavaş bir şekilde bu Hamiltonyan’a göre geliştirmek.

Bu yöntemi kullanan en ünlü firma olan DWave’in bilgisayarlarına aylık toplamda 1 dakika kullanım süresi ile ücretsiz erişim mümkün. Aşağıdaki linkten nasıl erişebileceğinizi ve adyabatik kuantum hesaplama ile nasıl problem çözebileceğinizi öğrenebilirsiniz.

[D-wave](#)

[Adiabatic Quantum Computation: \(Part 1\)](#)

[Notes on Adiabatic Quantum Computers](#)

[Adiabatic Quantum Computation and Quantum Annealing: Theory and Practice](#)

[Adiabatic Quantum Computing: An Overview](#)

[An introduction to adiabatic quantum computation](#)

KUANTUM HESAPLAMA PARADİGMALARI

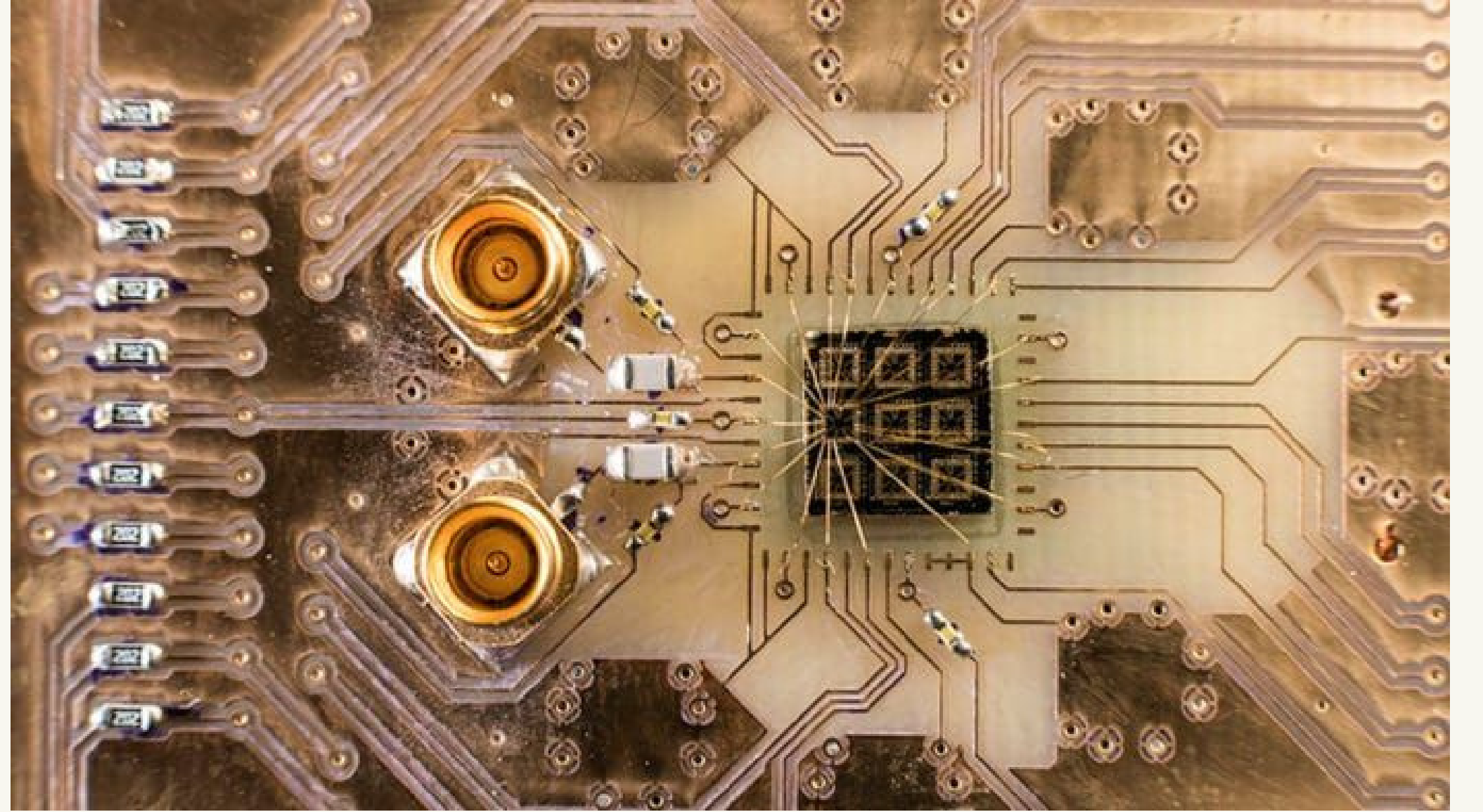
Measurement-Based Quantum Computing

Önceki paradigmlar kadar popüler olmasa da ölçüm tabanlı kuantum hesaplama da hala üzerine araştırma yapılan ve daha verimli olabileceği öne sürülen bir diğer hesaplama yöntemi.

Konu ile detaylı bir inceleme ve neler yapılabileceğine dair aşağıdaki linklerden kolayca bilgi edinebilirsiniz.

[An introduction to measurement based quantum computation](#)

[Measurement-based quantum computation with cluster states](#)



KUANTUM HESAPLAMA PARADİGMALARI

QAOA ve VQE

Quantum Approximate Optimization Algorithm (QAOA) ve Variational Quantum Eigensolver (VQE) kuantum hesaplama paradigmalarından ziyade kuantum algoritmalarıdır. Burada dahil etmek istememizin sebebi ise çok farklı alanlarda kullanılabilen bu iki algoritma gerçekten geliştireceğiniz proje için işinize yarayabilir.

Eğer projeniz bir optimizasyon problemi çözmeyi içeriyorsa ya da genel olarak bu iki algoritmaya dair bilgi edinmek isterseniz aşağıdaki linklere göz atmanızı tavsiye ederiz:

[Variational Quantum Eigensolver & QAOA](#)

[Gaurav Singh Medium Yazıları](#)

[Qiskit Textbook'un QAOA kısmı](#)

[Qiskit Textbook'un VQE kısmı](#)

[Peter Wittek'in QAOA Dersi](#)

[A Tutorial on Quantum Approximate Optimization Algorithm \(QAOA\): Fundamentals and Applications](#)

[Variational-Quantum-Eigensolver \(VQE\)](#)

[A brief overview of VQE](#)

[The Variational Quantum Eigensolver](#)

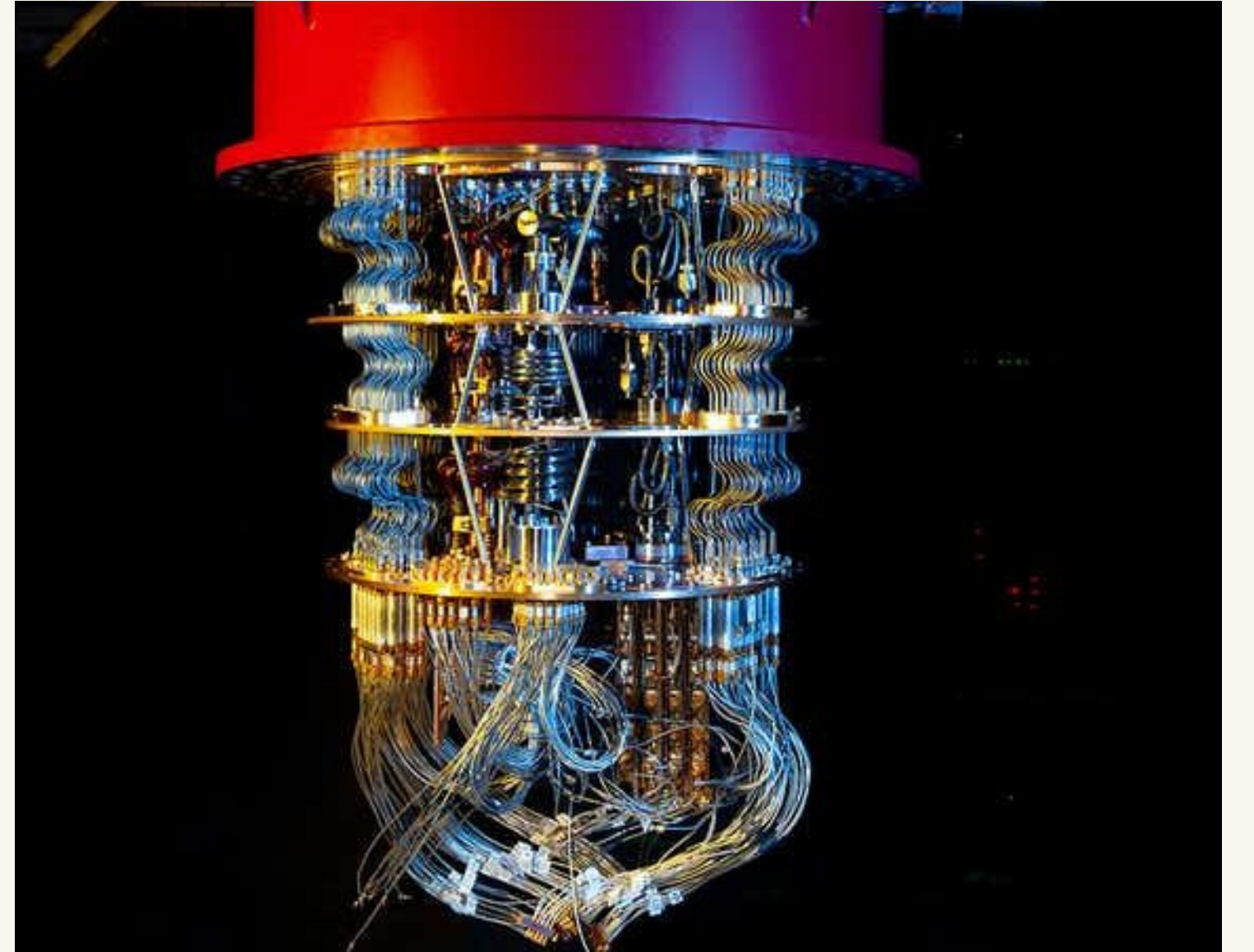
[Quantum Simulation for Chemistry using VQE](#)

KUANTUM SİMÜLASYON

Kitapçığımızın bu bölümünde kuantum simülasyon ile ilgili bir proje yapmak istemeniz halinde faydalanabileceğiniz kaynakları, örnek projeleri ve kuantum teknolojilerinde simülasyonun ne olduğuna dair kısa bir tanıtım sunacağız.

Tanıtım

Simülasyon veya benzetim, teknik anlamda bir sürecin veya sistemin işletilmesinin zaman üzerinden taklididir. Kuantum simülasyonu ise, bir kuantum sistemini simüle etmenin bir yolu olarak tanımlanır. "Kuantum Simülasyon" alanı, Richard Feynman tarafından 1980'lerde tanıtılmıştır. Sıradan bilgisayarlarda çözülmesi çok zor olan kuantum mekaniği sorunlarına yaklaşmak için yeni bir yöntem olarak önerilmiştir. Bu önerinin arkasındaki fikir, bilgisayarlara daha erişilebilir bir kuantum sistemi olarak kullanarak ilgilenilen karmaşık kuantum etkilerini taklidini elde etmektir.



KUANTUM SİMÜLASYON

Kuantum simülasyon, kuantum simülatörleri ile gerçekleştirilir. Bu simülatörler, belirli bir süreci simüle etmek için özel olarak tasarlanmış bir kuantum bilgisayar veya yazılımdır. Bu nedenle yalnızca sınırlı sayıda sorunu çözebilirler. Başka problemleri çözmek istiyorsanız, bu belirli problemleri çözmek için tasarlanmış yeni bir kuantum simülatörü oluşturmanız gerekir.

Bu zamana kadar oldukça basit birtakım kuantum simülasyon örnekleri halihazırda gösterilmiştir ancak henüz klasik bilgisayarları geçememiştir. Bununla birlikte hızlı bir ilerleme kaydediyor ve araştırmacılar, en güçlü klasik bilgisayarın bile ulaşamayacağı bir problemi çözme anlamına gelen kuantum üstünlüğünü göstermek için gereken seviyeye ölçeklendirmeye hazırlanıyorlar. Buna bağlı olarak kuantum simülasyonu için kullanılabilir uygulamalar beş yıl içinde beklenmektedir.

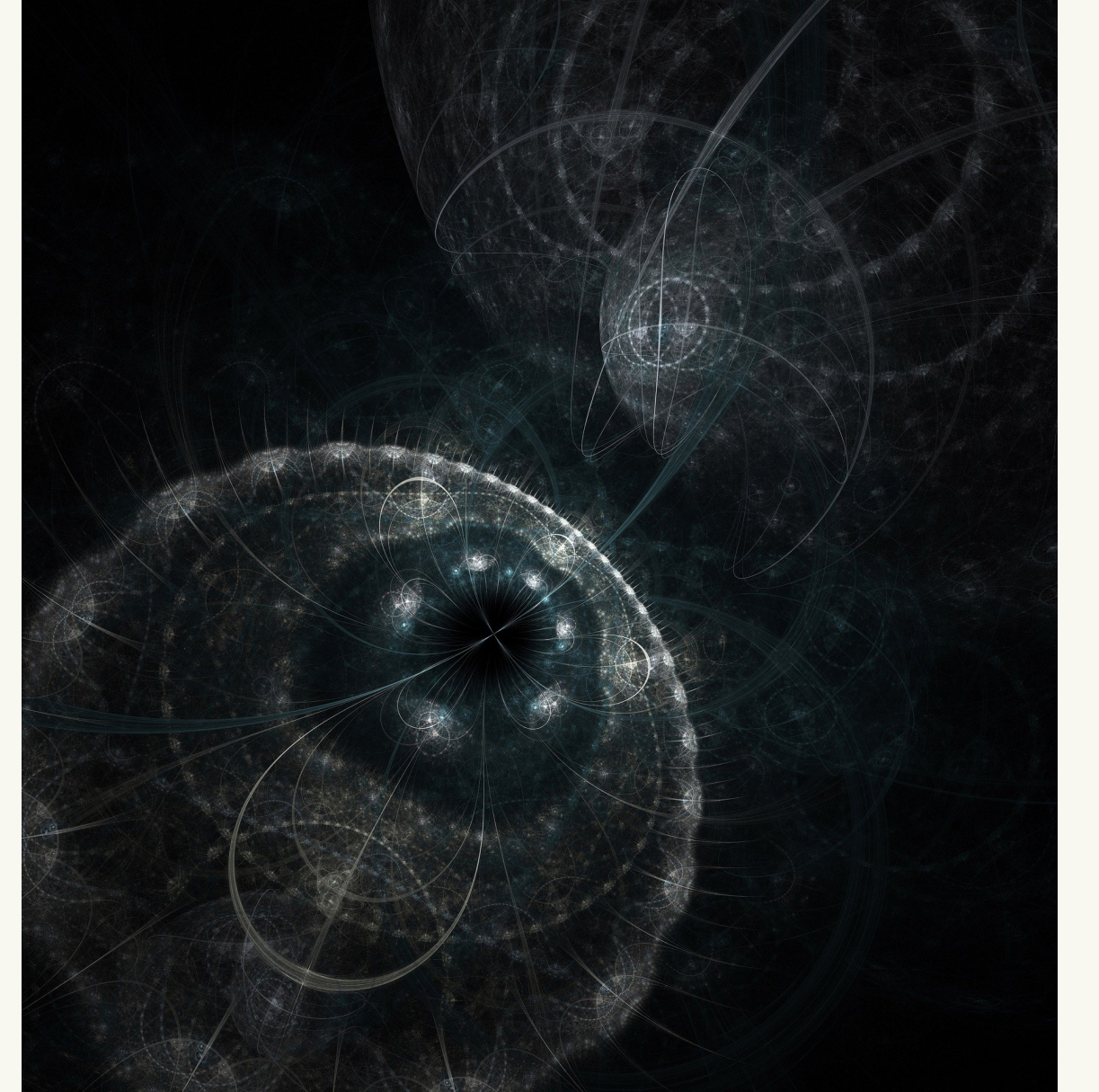
Başlıca üç tür kuantum simülasyon yolu bulunmaktadır:

- Dijital kuantum sistemlerinin klasik simülasyonu için kuantum simülasyonu
- Analog kuantum simülasyonu
- Kuantum bilgi temelli algoritmaların simülasyonu.

KUANTUM SİMÜLASYON

Kuantum Simülasyonun Kimya Uygulamaları

Kuantum simülasyon, yoğunluklu olarak kuantum kimya çalışmalarında kullanılmaktadır. Kuantum simülasyonun kimya uygulamaları, yeni malzeme tasarımlarını, moleküler dinamikleri hesaplamayı ve kimyasal reaksiyon dinamiklerinin çözümünü mümkün kılmaktadır. Yakın gelecekte kuantum simülasyonunun klasik hesaplamalara göre kuantum kimyası için güçlü bir araç olacağı tahmin edilmektedir.



[Quantum chemistry simulation on quantum computers: theories and experiments](#)

KUANTUM SİMÜLASYON

Kullanabileceğiniz Kuantum Simülatörler

(lütfen linklere erişmek için altı çizgili alanlara tıklayınız)

- [Qiskit](#)
- [Q# QDK](#)
- [Intel Quantum Simulator](#)

Yukarıdaki simülatörlerin haricindeki kuantum simülatörlerin tam listesine de [buradan](#) ulaşabilirsiniz.

Ayrıca, aşağıdaki bağlantılar aracılığıyla alanı daha iyi tanıyabilirsiniz.

[Quantum Simulator](#)
[What is Quantum Simulator?](#)

Güncel Makaleler

Quantum information scrambling in a trapped-ion quantum simulator with tunable range interactions, [Phys. Rev. Lett. 124, 240505 \(2020\)](#).
Cross-Platform Verification of Intermediate Scale Quantum Devices, [Phys. Rev. Lett. 124, 10504 \(2020\)](#).
Self-verifying variational quantum simulation of lattice models, [Nature 569, 355 \(2019\)](#).
Probing Rényi entanglement entropy via randomized measurements, [Science 364, 260 \(2019\)](#).
Environment-assisted quantum transport in a 10-qubit network, [Phys. Rev. Lett. 122, 050501 \(2019\)](#).
Quantum chemistry calculations on a trapped-ion quantum simulator, [Phys. Rev. X, 8, 031022 \(2018\)](#).
Observation of Entangled States of a Fully Controlled 20-Qubit System, [Phys. Rev. X, 8, 021012 \(2018\)](#).
Efficient tomography of a quantum many-body system, [Nature Phys. 13, 1158 \(2017\)](#).
Direct observation of dynamical quantum phase transitions in an interacting many-body system, [Phys. Rev. Lett. 119, 080501 \(2017\)](#).

KUANTUM SENSÖRLER

Kuantum teknolojisi bilgi işlem, iletişim, görüntüleme ve sensörleri kapsar.

Kuantum sensörler, kuantum algılamalar ile fiziksel bir miktarın ölçümünü gerçekleştirmek için bir kuantum sistemin, kuantum özelliklerinin veya kuantum olaylarının kullanımını tanımlar. Frekans, elektromanyetik alan ve sıcaklık gibi fiziksel nicelikleri oldukça hassas şekilde ölçebilir. Ayrıca, kuantum sensörler değişik uygulamaları ile uydulardan uçaklara kadar farklı alanlarda kullanılabilir.

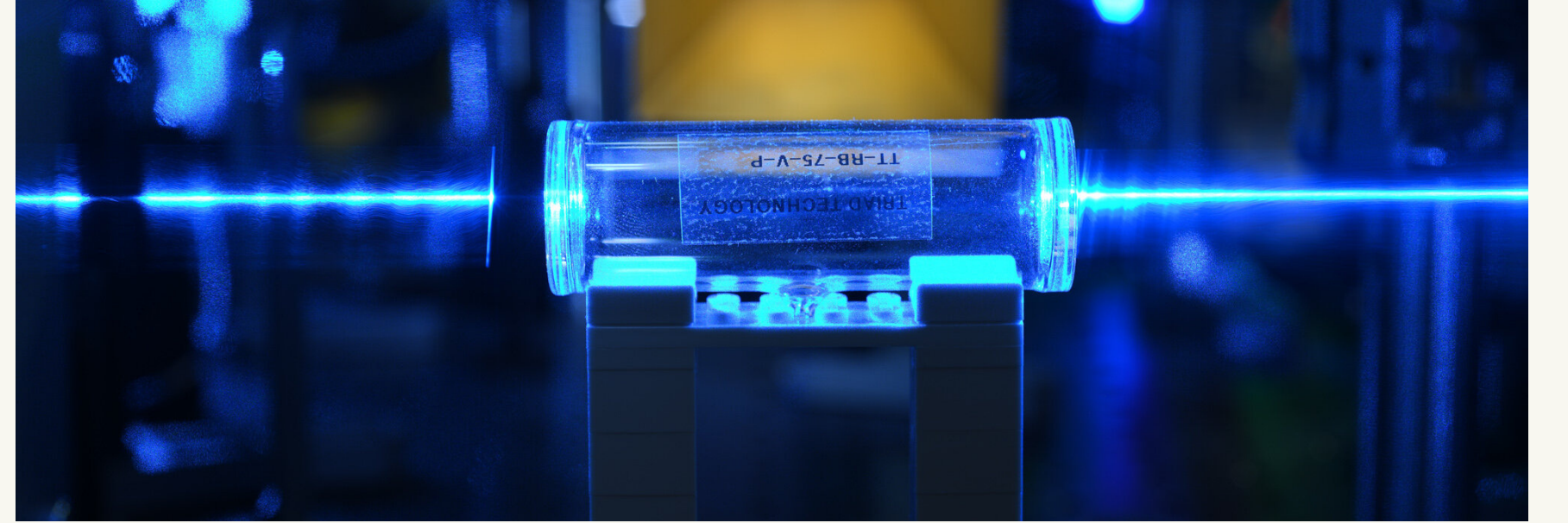
Kuantum sensörlerin tarihsel örnekleri, süperiletken kuantum girişim cihazlarına ve atomik buharlara veya atomik saatlere dayanan manyetometreleri içerir. Yakın zamanda ise kuantum algılama, kuantum bilimi ve teknolojisi alanlarında farklı ve hızla büyüyen bir araştırma dalı haline geldi. Bu, otonom, ulaşım, navigasyon ve beyin görüntülemeden nesnelerin internetine kadar her şeyde ilerlememize yardımcı olacak.



KUANTUM SENSÖRLER

Kuantum sensörlerin bazı amaçları:

- Süperiletkenlik dahil olmak üzere kuantum etkileri
- Termal gürültüyü azaltmak için düşük sıcaklıklar
- Görüntüleme ve litografi
- Gelişmiş sensörlerin geliştirilmesi
- Tek kuantum parçacık algılamayı etkinleştirmek



Bu amaçların özel olarak hizmet ettiği bazı faaliyetler:

- Malzeme analizi ve nükleer malzeme muhasebesini içeren uygulamalar için süperiletken x-ışını ve gama-ışını spektrometreleri
- Gizli silah tespiti ve erken evreni anlamayı içeren uygulamalar için süperiletken mikrobolometreler
- Kriyojenik sensörlerin yayılmasına yardımcı olmak için gelişmiş kriyojenikler
- X-ışını teknikleriyle malzeme analizini kolaylaştırmak için x-ışını temel parametrelerinin belirlenmesi
- Hassas atalet algılama gerçekleştirmeye ve özellikle atom interferometri yoluyla yerçekimi ve yerçekimi gradyanlarının ölçümü
- Yer altı dünyasının haritasını çıkarmak
- Tam çözünürlüklü beyin

KUANTUM SENSÖRLER

Faydalı olabilecek linkler

[Atom interferometrik kuantum sensörlerinin gerçek hayata uyarlanması](#)

[UK Quantum Technology Hub Sensors and Timing' in teknolojileri](#)

[Kuantum sensörler grubu ve yaptıkları için](#)

[Kuantum sensörlerinin keşfedilmemiş bölgeleri keşfetmesi](#)

[Elmas tabanlı kuantum sensörler](#)

[Tek kuantum parçacık algılamayı etkinleştirmek için kuantum sensörlerin geliştirilmesi](#)

<https://arxiv.org/abs/1611.02427>

<https://medium.com/swlh/quantum-sensors-are-already-here-9401bda60c25>

<https://medium.com/proceedings-of-the-national-academy-of-sciences/core-concept-quantum-sensors-probe-uncharted-territories-from-earths-crust-to-the-human-brain-5f2482cfc357>

<https://medium.com/quantum-tech/nathans-quantum-tech-newsletter-24-gravitational-quantum-sensors-a2ce0489e76c>

<https://www.bbc.com/news/business-47294704>

https://indico.cern.ch/event/870453/contributions/3671194/attachments/1960742/3258611/BRN_QuantumSensors.pdf

https://en.wikipedia.org/wiki/Quantum_sensor#:~:text=In%20solid%2Dstate%20physics%2C%20a,be%20done%20with%20classical%20sensors

<http://www.apogee-tr.com/manuals/SQ-214-224manual.pdf>

<https://www.birmingham.ac.uk/research/activity/gravity/quantum-sensors.aspx>

<https://medium.com/@steffen.eberle/scientists-create-quantum-sensor-that-covers-entire-radio-frequency-spectrum-6f217f7e928c>

<https://medium.com/@steffen.eberle/tiny-quantum-sensors-watch-materials-transform-under-pressure-393f79f48ac8>

https://www.youtube.com/watch?v=UF5_Uwpg3SA

KUANTUM OYUNLAR

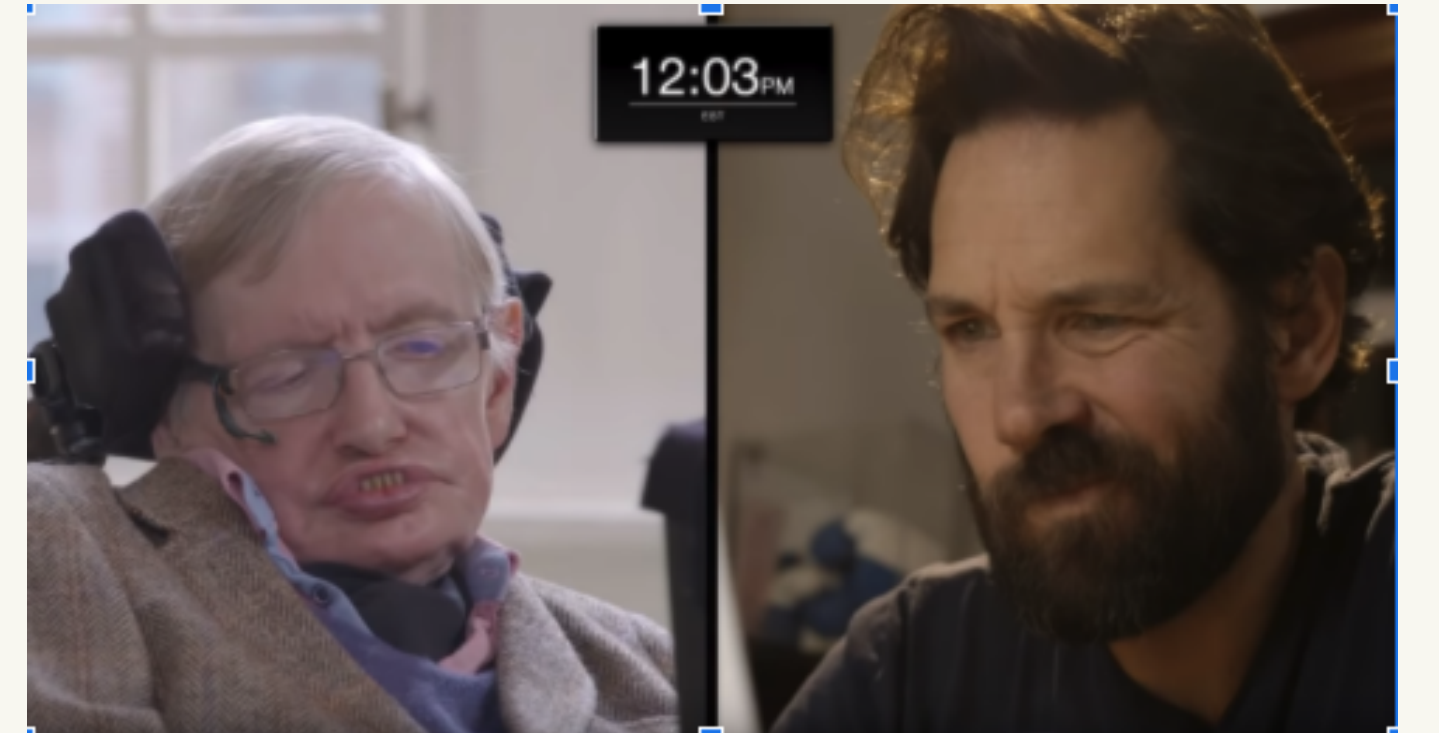
Tanıtım

Bilgi kitapçığımızın bu kısmında size kuantum oyunlar ile ilişkili proje yapmak isterseniz neler yapabileceğinize dair bilgi ve kaynak önerisi vereceğiz. Şimdiye kadar düzenlenmiş farklı hackathonlarda proje olarak yapılmış ya da herhangi bir hackathondan bağımsız olarak geliştirilmiş oyunlar iki kategoride düzenlenebilir. Birincisi kuantum mekaniğine veya kuantum programlamaya dair temel konseptleri öğretmek üzere tasarlanmış oyunlar, ikincisi ise kuantum mekaniğinin “garip”liklerini, süperpozisyon ve gerçek rastgelelik gibi, oyunun mekaniğine entegre ederek tasarlanmış oyunlardır. Örnekler üzerinden ilerleyelim.

Kuantum Satranç

Link: https://www.youtube.com/watch?v=Hi0BzqV_b44&t=600s

Açıklama: Bir çoğumuzun Ant-man filminden tanıdığı Paul Rudd’un, Stephen Hawking ile olan efsanevi kuantum satranç oyununu görmüşsünüzdür. Görmeyenler için özet geçmek gerekirse, “Kuantum mekaniğinde sık sık karşılaştığımız süperpozisyon ilkesini satranç oyununa entegre edersek nasıl olur?” sorusunu eğlenceli bir şekilde işlemişler diyebiliriz.

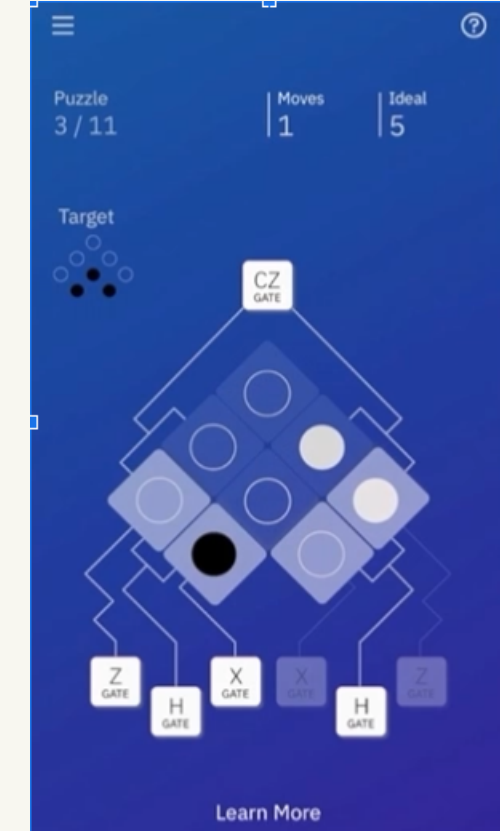


KUANTUM OYUNLAR

Hello Quantum

Link: <https://helloquantum.mybluemix.net>

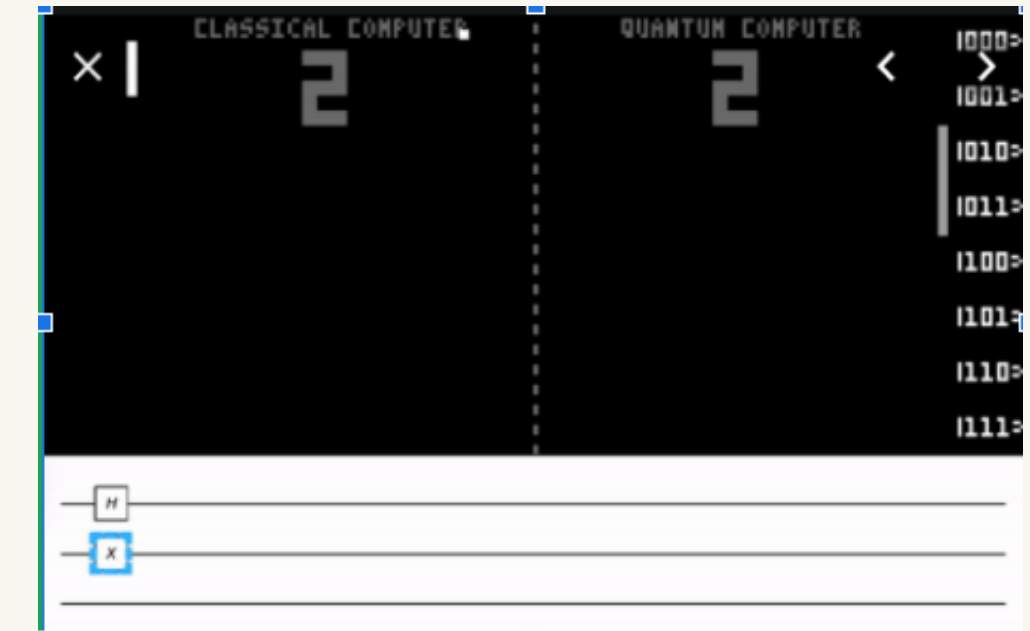
Açıklama: IBM'in yaptığı bir bulmaca oyunu olan Hello Quantum, oyuncudan verilen kuantum kapılarını kullanarak başlangıç durumundaki kübitleri istenilen son duruma götürmesini istiyor. Bulmacaların tek bir çözümü olmamasına rağmen her zaman minimum hareket kullanarak elde edilebilen bir optimal çözümü bulunuyor ve oyuncu ne kadar az hareket yaparsa o kadar yüksek puan alıyor.



QPong

Link: <https://www.youtube.com/watch?v=a1NZC5rqQD8&feature=youtu.be>
<https://github.com/HuangJunye/QPong>

Açıklama: QPong da kuantum programlama konseptlerini öğretmek için geliştirilmiş bir başka oyun. Oyuncunun hareketleri doğru kuantum devresini üreterek karşıdan gelen topu karşılamaya çalışmaya yönelik ve oyunun zorluk seviyesine göre başlangıçtaki kübit sayısı artıyor.



KUANTUM OYUNLAR

Quantum Go

Link: <https://physicsworld.com/a/quantum-go-machine-plays-ancient-board-game-using-entangled-photons/>

Açıklama: 2016'da DeepMind tarafından yapay zeka ile geliştirilmiş AlphaGo, dünya şampiyonu Lee Sedol'ü mağlup etmişti. Yukarıda verilen linkte ise aynı işin kuantum bilgisayar kullanarak yapılabileceğinden bahsediliyor.



QLogic

Link: <https://thequantumdaily.com/2020/09/18/gaming-your-way-into-quantum-computing/>

Açıklama: Bu küçük yazıyla tanıtımı yapılan QLogic de kuantum programlamanın temellerini oyun bazlı anlatmaya çalışan bir başka oyun. Yukarıda verilen linkte oyunu geliştirirken yaşadıkları bazı zorluklardan da bahsediyorlar. Dolayısıyla benzer bir proje yapmak isterseniz önceden bu yazıyı okumak yardımcı olabilir.



KUANTUM OYUNLAR



James Wootton Yazıları

Link: <https://medium.com/@decodoku>

Açıklama: Dr. James Wootton, Google'a "Quantum Games" yazdığınızda hemen karşınıza çıkacak isimlerden birisidir. Kendi Medium sayfasında, bizim de bu yazıları yazarken faydalandığımız, yazılarını yayınlıyor. Mesela "[My Ideas for a quantum hackathon](#)" isimli yazısı tam da size hitap eden bir yazı, eğer projenizi bu alanda yapmak isterseniz tabii. Mesela "[How to program a quantum computer](#)", eğer kuantum programlama ile alakalı hiçbir fikriniz yoksa okuyabileceğiniz, konuya küçük bir giriş yapan, daha sonrasında ise küçük bir Battleship oyununun nasıl yapılabileceğini anlatan bir yazısıdır.

KUANTUM OYUNLAR

Hackathon Projeleri

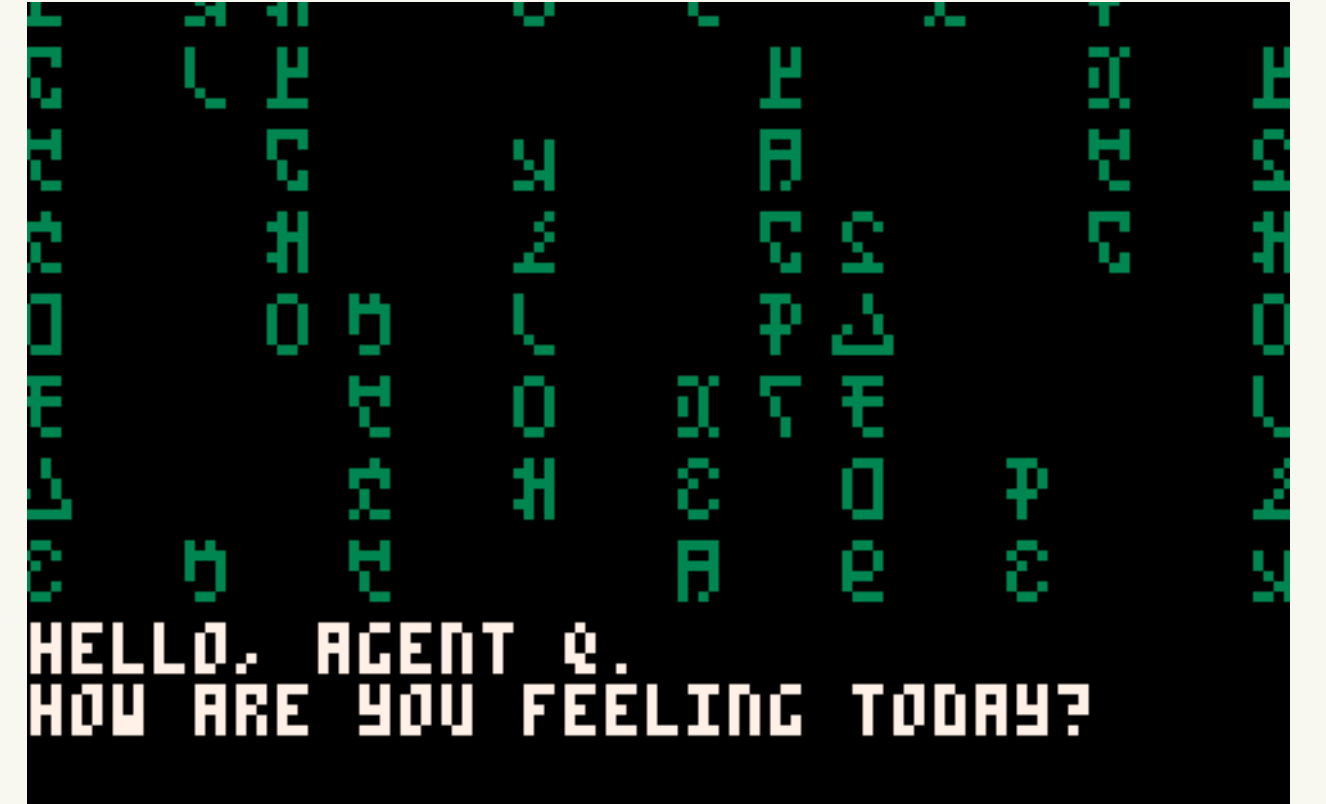
Link: [Qiskit Asya Hackathon](#), [Qiskit Singapur Hackathon](#)

Açıklama: Qiskit'in 2019 Asya kampında ve Singapur hackathonunda öne sürülen projeler içerisinde, kuantum oyunlar başlığı altına alabileceğimiz bir sürü örnek proje vardır. Mesela öne sürülen projelerden bir tanesi Grover'ın arama algoritmasını kullanarak sudoku çözmek üzerinedir. Bir diğeri ise iki oyuncuya aynı başlangıç kübitlerini verip aynı final hallerini isteyip daha hızlı yapanın kazandığı çekişmeli bir oyundur. Kesinlikle bu iki linki uzun uzadıya incelemenizi tavsiye ediyoruz.

Quantum Game Jam

Link: [IndiQ Quantum Game Jam #1](#)
[IndiQ Quantum Game Jam #2](#)

Açıklama: Kuantum Programlama Hackathon'ları başlığı altında geliştirilen oyunlar dışında, direkt kuantum oyunlar üzerine yapılmış farklı yarışmalar da vardır. Yukarıda verilen linklerden bu yıl içerisinde düzenlenmiş olan iki tanesine erişebilirsiniz.



KUANTUM MAKİNE ÖĞRENMESİ

Kuantum makine öğrenmesi literatürde çok farklı yöntemler için kullanılan, kuantum mekaniği ve makine öğrenmesi alanlarının bir kesişimidir. Son yıllarda kuantum bilgisayarların piyasa sürülmesiyle çok geniş bir alana hitap eden bu kavram, biraz daha net çizgilere oturmaya başlasa da başlığında “Kuantum Makine Öğrenmesi” gördüğünüz her makale bir başka alanda çalışma sunuyor olabilir. Bu sebeple bu alandaki çalışmaların detayına girmeden, bu alanın kapsadığı alt başlıklara küçük bir bakış atmanın faydası var.



KUANTUM MAKİNE ÖĞRENMESİ

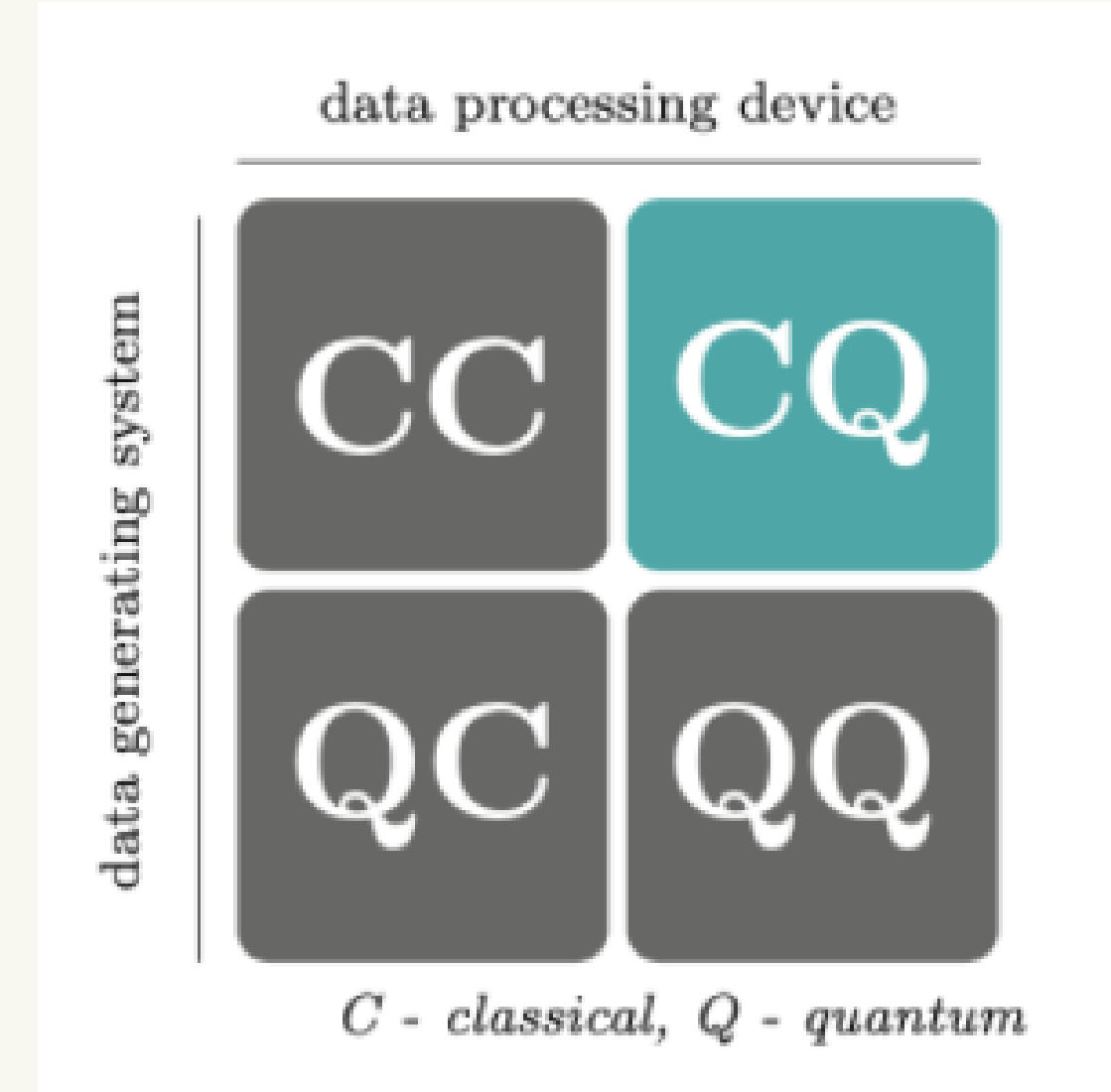
Şekil 1’de de görülebileceği üzere yöntemimizin adını verilere ve veri işleme cihazına göre 4 alt başlığa ayırabiliriz. Satırlar veri üreten sistemin kuantum veya klasik olduğunu belirlerken, sütunlar ise bu verinin hangi cihaz türü ile işlendiğini belirlemektedir. Bunlara kısaca örnek verecek olursak;

CC: Son 10 yılın hava durumu verilerine göre haftalık hava durumu tahmini algoritması.

QC: H₂O molekülünün enerji seviyelerinin deney verileri ve simülasyonlar yardımıyla belirlenmesi.

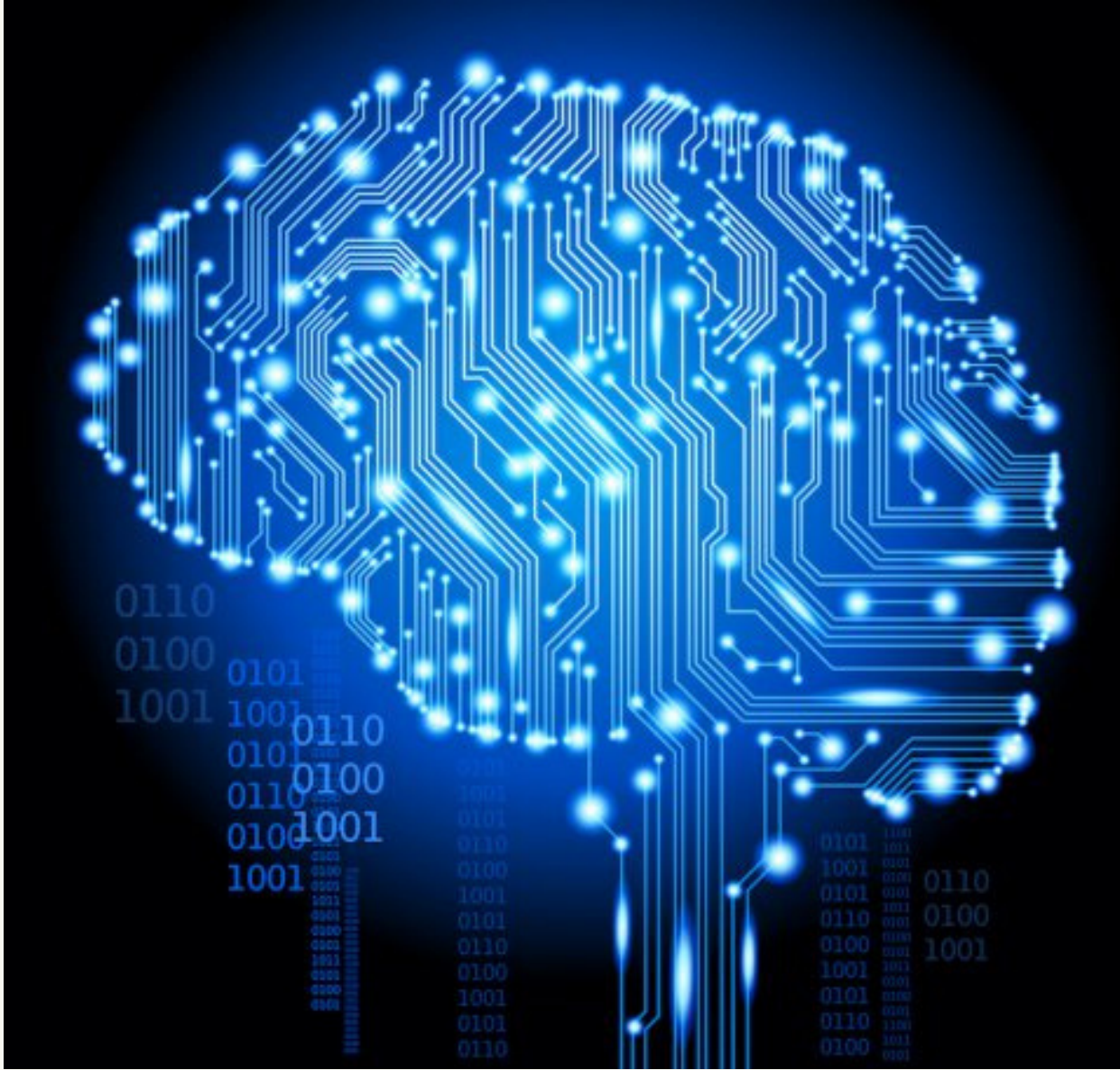
CQ: İki asal sayının çarpımından oluşan büyük bir sayının asal çarpanlarının bir kuantum bilgisayar kullanarak bulunması.

QQ: H₂O molekülünün kuantum bilgisayar ile modellenerek enerji seviyelerinin bulunması.



Şekil 1: Kuantum ve klasik veri işleme yöntemlerinin alt grupları.
Schuld, Petruccione, "Supervised Learning with Quantum Computers"
2017, Springer.

KUANTUM MAKİNE ÖĞRENMESİ



Yukarıda verilen bu 4 ana başlıktan içerisinde en az bir tane “Q” bulunması ve içerisinde herhangi bir makine öğrenmesi algoritması kullanılması durumuna literatürde “Kuantum Makine Öğrenmesi (KMÖ)” denmektedir. Son yıllarda kuantum bilgisayarların popülerleşmesi ile KMÖ daha çok veri işlenen cihazın bir kuantum bilgisayar olması durumunda kullanılan başlık olmuştur. Dolayısıyla yazının bu kısmından sonra KMÖ’den bahsettiğimizde bir kuantum bilgisayarın kullanılacağını anlamalıyız. Buraya küçük bir parantez açarak bu algoritmaların klasik bilgisayarlarda simüle edilebileceğini ve akademik çalışmaların çoğunda da bu yöntemin seçildiğini belirtmekte fayda var.

KUANTUM MAKİNE ÖĞRENMESİ

Kuantum Makine Öğrenmesi Çeşitleri

Tıpkı klasik Makine Öğrenmesi algoritmaları gibi KMÖ de bize pek çok çeşit sunmaktadır. Fakat, KMÖ’de bu çeşitlilik veri işleme türü de değişebildiği için daha da çeşitli bir hale gelerek bu algoritmaların sayısını bir hayli artırıyor. Bu algoritmaların hepsine burada yer vermemiz çok zor olduğu için bunlara ulaşılacak kaynakların bir listesini sunmak istedik.

KMÖ’de kullanılan başlıca Kuantum veri işleme yöntemlerini şu şekilde sıralayabiliriz;

Kuantum tavlama (Annealing):

Kuantum tavlama türü bilgisayarların kullanıldığı bu yöntemde kübitlere tek tek bir işlem uygulamak yerine kübitlerin arasındaki etkileşimler kontrol edilir.

Kuantum tavlama tipi bilgisayarların öncülerini geliştiren, D-Wave şirketinin Ocean kütüphanesine [buradan](#) ulaşabilirsiniz.

Bu alanda internet üzerinde bulunabilecek en kapsamlı ders serilerinden birisine [bu linkten](#) ulaşabilirsiniz.

KUANTUM MAKİNE ÖĞRENMESİ

Kapı tipi:

Kapı tipi kuantum bilgisayarlar da kubitlerin her birisine özelleşmiş işlemler uygulamanın yanı sıra kubitler arasında da işlemler yapabilir.

Bu tip kuantum bilgisayarlar için IBM'in açık kaynak olarak geliştirdiği Qiskit yazılımına [buradan](#) ulaşabilirsiniz.

Qiskit'in optimizasyon modülüne giriş için [bu yazıya](#) danışabilirsiniz.

Kapı tipi kuantum hesaplama için geliştirilen çokça Python kütüphanesi mevcut. Fakat bunların neredeyse hepsini aynı kodu kullanarak kullanma imkanı veren, hatta bu kütüphanelerle standartlaşmış Tensorflow ve PyTorch gibi klasik kütüphaneler arasında bir köprü görevi gören, Xanadu tarafından açık kaynak olarak geliştirilen PennyLane kütüphanesi belki de en önemli kütüphanelerden birisidir.

PennyLane dokümantasyonuna [buradan](#) erişebilirsiniz.

PennyLane'nin öğretici örneklerinin ve KMÖ'ye giriş için çok değerli kaynakların bulunduğu [websitesi](#).

KUANTUM MAKİNE ÖĞRENMESİ

Bu kütüphanelerin dışında daha pek çok kaynak ile KMÖ üzerine modeller geliştirmek ve kuantum bilgisayarlarda test etmek mümkün. Yukarıdaki kaynaklar giriş seviyesi için fazlasıyla yeterli olsa da bir adım ileriye gitmek veya bütün alternatiflere göz atmak isteyenler aşağıda sunacağımız linklere de bakabilir.

Kütüphaneler:

- [Ocean](#)
- [Qiskit](#)
- [PennyLane](#)
- [Tensorflow Quantum](#)
- [Microsoft Quantum SDK](#)
- [Yao](#)
- [Qucumber](#)
- [QML](#)

Faydalı olabilecek GitHub kaynak derlemeleri:

[Awesome Quantum Machine Learning](#)

[Awesome Quantum ML](#)

Video dersler ve seriler:

[Maria Schuld - Machine Learning With Quantum Computers \[IndabaX South Africa 2019\]](#)

[Quantum Machine Learning - Peter Wittek](#)

KUANTUM MAKİNE ÖĞRENMESİ

Faydalı olabilecek diğer yazılar:

[Machine Learning in the Quantum Era](#)

Diğer bir giriş yazısı ise biraz kuantum makine öğrenmesi tarihçesinden bahsettikten sonra donanım türlerinin bu konuyla etkisini ve gelecekte yapılabileceklerden bahsediyor. Detaylı okuma için kaynakçası faydalı olabilir.

Başka hackathonlarda yapılan projeler:

[QHACK](#)

[Kazanan proje](#)

[Qiskit Camp Asia](#)

Bu yazıda geçen sene düzenlediğimiz “Kuantum Programlama Hackathonu” kitapçığında ve Doğukan Tuna’nın [Kuantum Makine Öğrenmesi](#) yazısından faydalanılmıştır.

KUANTUM FİNANS UYGULAMALARI



Kuantum Bilgisayarlar ve Finans

Kuantum bilgisayarların en çok ve en yakın zamanda avantaj sağlayacağı alanlardan birinin de finans sektörü olacağı öngörülmektedir. Bu alanda özellikle portfolyo optimizasyonlarında, nakit akış tahmininde ve risk yönetiminde varlıkların dağılımı gibi her yeni parametreyle birlikte kombinasyonların üstel olarak arttığı problemlerde piyasaya gerçek zamanlı tepki vermeyi sağlayacağı öngörülmüyor.

KUANTUM FİNANS UYGULAMALARI

Günümüzde finans sektörünün özellikle akademik araştırmalarda karşılaştığı sorunlar konusunda, New York Cornell Üniversitesi profesörü Marcos López de Prado'nun güzel bir benzetmesi vardır. Örneğin bir fizikçi veya bir kimyager gerçek bir laboratuvarı belli koşulları oluşturup deney yapabiliyor. Finans konusunda araştırma yapan akademisyenlerin ise laboratuvarları piyasalar. Ancak finansal piyasalar çok karmaşık sistemler olduğu için bir araştırmacı piyasanın belli bir zamandaki halini birebir tekrar oluşturup deney yapamıyor. Yani bu bir fizikçinin Büyük Hadron Çarpıştırıcısı'na erişimi olmasına benziyor. Bu sebeple, bu tür durumlarda hangi senaryolara nasıl cevaplar verilmesi gerektiğini sınırlı veriyle modelleyebiliyorlar fakat gerçek ortamı oluşturup test edemiyorlar. Bu da araştırmaların sadece teoride kalmasına sebep oluyor. Fakat öngörülen kuantum bilgisayarların hesaplama gücü bunu karşılayabilecek nitelikte.

Örneğin, herhangi bir portfolyo için değişen fiyatlara bağlı olarak meydana gelecek kârın veya zararın analiz edilmesi için milyonlarca fiyat olasılığı simüle ediliyor. Bu tür simülasyonların çalışma süreleri günler alabiliyor. Ancak kuantum bilgisayarların getireceği avantajla birlikte bu simülasyonlar saatler seviyesine indirgenebilecek hatta gerçek zamanlı yapılabilecek. Dolayısıyla bu, finansal bir kuruluşun rakiplerine karşı daha üstün olmasını sağlayacak. Bunun yanı sıra, piyasaların belli zamandaki durumu çok daha kolay simüle edilip daha doğru araştırma sonuçları elde edilebilecektir.

Diğer yandan kuantum bilgisayarlar, süperpozisyon özellikleri sayesinde, klasik bir bilgisayardan farklı olarak portfolyo dağılımlarını bir bütün olarak değerlendiriyor. Programlama açısından klasik bilgisayarlar gibi olmadıklarından, iş dünyasının bu avantajdan faydalanması için, araştırmacıların simülasyonları kuantum bilgisayarlara uyarlaması yani klasik algoritmaların kuantum karşılıklarını bulması gerekiyor. Bu konuda, son dönemde Chicago Quantum firmasının portfolyo optimizasyonu konusunda yaptığı çalışmalar incelenebilir. Makalenin detaylı anlatımına buradan ulaşabilirsiniz.

KUANTUM FİNANS UYGULAMALARI

Bir bankanın aldığı riskler ve yatırım stratejileri aslında tamamen o bankanın ne kadar iyi karar alabildiğiyle ilgilidir. Milyonlarca olasılık içinden tüm değişkenlerin kombinasyonlarının sonuçlarını analiz etmek aylar hatta yıllar alabiliyor. Bu sebeple finansal kuruluşlar, sahip oldukları bilgilerle ellerinden gelen en iyi kararı vermelidirler. Kuantum bilgisayarlar sadece kuantum mekaniğine özgü karakteristikleri ile tüm bu milyonlarca seçeneğe aynı anda bakabilmeyi sağlayacak ve bilgileri çok daha hızlandırılmış bir şekilde, gerçek zamanlı sunacak. Bu konuda Japonya ve Tokyo merkezli teknoloji firması Fujitsu'nun D-Wave benzeri kuantum tavlayıcı (annealer) ile yaptığı çalışmalar incelenebilir.

En iyi kararları verebilmek için risk analizinde sıklıkla kullanılan Monte Carlo simülasyonu da kuantum bilgisayarların çığır açacağı alanlardan biri olarak görülüyor. Finansın yanı sıra sigorta, enerji, petrol, ulaşım ve daha birçok endüstride de kullanılan Monte Carlo metodu, rastgele setler kullanarak alınacak kararların ve böylece oluşacak risklerin olasılık dağılımının hesaplanmasına yardımcı oluyor ve belirsizlik ortamında daha doğru kararlar alınmasını sağlıyor.

Bu konuda özellikle IBM Quantum araştırmaları ekibinde görev alan ve Monte Carlo simülasyonları konusunda çalışmaları olan Stefan Woerner'ın birçok yayını mevcut. Monte Carlo yöntemine alternatif bir çalışmaya buradan, kredi risk analizi ile ilgili başka bir makaleye de buradan erişilebilir.

Dünyanın önde gelen finansal kuruluşlarından JPMorgan Chase, Barclays, Goldman Sachs, Citigroup ve daha birçok kuruluş, bu konuda araştırmalarına birkaç yıl önce başladı. Bu kurumların bazıları kendi içlerinde quantum konusunda birkaç uzmanı da barındıran ekiplerle günümüzde var olan “Noisy Intermediate-Scale Quantum (NISQ)” bilgisayarlar üzerinde denemeler yapıyorlar. Goldman Sachs'ın, opsiyon fiyatlamalarında kuantum bilgisayarların kullanılması konusunda IBM ile birlikte yayınladığı makaleler mevcut.

KUANTUM FİNANS UYGULAMALARI

Finansal kuruluşlardan bazıları da kuantum konusunda danışmanlık veren yazılım firmalarıyla birlikte çalışıyorlar ve bu teknolojideki gelişmeleri yakından takip ediyorlar. Bunlardan Citigroup'un da yatırımcıları arasında bulunduğu Kaliforniya merkezli QC Ware'in, Goldman Sachs'dan başka Airbus ve BMW Group ile ortaklığı bulunuyor. Kanada, Vancouver'da bulunan 1QBit ise, University of British Columbia ve University of Waterloo gibi üniversitelerden danışmanlık alıyor ve yine finansal bir kuruluş olan Royal Bank of Scotland' la ortaklığı bulunuyor. Yine Kanada, Toronto merkezli Xanadu ise Bank of Montreal ve ScotiaBank'in de aralarında bulunduğu beş finansal kuruluşla çalışıyor.

Finansal kullanım alanlarının en çok üzerinde duran ve bilgisayar üretimi yanı sıra yazılım desteği de vermeyi hedefleyen Kaliforniya merkezli Rigetti, yakın zamanda bu amaçla Commonwealth Bank of Australia ile çalışan QxBranch'i satın aldı. Rigetti ayrıca, Aralık 2019'da Amazon'un kuantum platformu Braket üzerinden kullanıcıların denemeler yapması için bilgisayarlarını genel kullanıma açtı.

Firmaların kimi için temel amaç, şirketlerin hem üst düzey yönetimini hem de teknik kadrosunu kuantum konusunda bilinçlendirmek, çalışma grupları kurarak kuantum avantajının kullanılabileceği problemleri tespit etmek, kimisi için ise kurumların bünyesindeki uzmanlarla birlikte çalışıp bu konu üzerinde akademik yayınlar yapmaktır.

Firmaların denemeler yaptığı kullanım alanları; finans alanında başta portfolyo optimizasyonları olmak üzere, türev fiyatlandırması, risk analizinde veya dolandırıcılık tespitinde kuantum makine öğrenmesi, sigorta, perakende veya pazarlama önerileri ve Monte Carlo metodları gibi maliyetli hesaplamaları içeriyor.

KUANTUM FİNANS UYGULAMALARI

Bu aşamada kuantum bilgisayar teknolojisine yapılan yatırımın getirisinden söz etmek mümkün değil. Bu konuya şimdiden yüz binlerce dolar yatırım yapan firmalar, bir yandan mevcut teknolojileri takip ederken bir yandan da rakiplerine karşı benzersiz avantajlar sağlayacak geleceğin teknolojilerini keşfetmek istiyorlar.

Sonuç olarak, klasik bilgisayarlar gibi tüketiciye yönelik büyük ölçekli verilerle veya banka verileriyle hesaplama yapabilecek kuantum bilgisayarlar henüz üretilmedi. Ancak firmaların öngörüsü, yakın zamanda önemli gelişmelerin olacağı yönünde. Hatta hükümetlerin son dönemde yaptığı yatırımlar da bunu gösteriyor. Bu nedenle, öngörülen zamana kadar kendi problemlerini kuantum bilgisayarlar üzerinde çözmeye çalışan kurumlar, kuantum avantajına önceden sahip olacaklardır.



KUANTUM FİNANS UYGULAMALARI

Ek Kaynaklar:

Beyond optimization to Always Optimal: <https://www.fujitsu.com/global/solutions/industry/financial-services/quantum-inspired/index.html>
The Quantum Threat to Financial Services: <https://www.youtube.com/watch?v=kW-lr61RwSE>
The Quantum Computing Revolution in FinTech: <https://www.youtube.com/watch?v=vAu0CAktgQ>
Using quantum computers in financial risk analysis: https://www.youtube.com/watch?v=2lPrz-WH_Wo
New York Cornell Üniversitesi profesörü Marcos Lopez de Prado'nun finans araştırmalarında yaşanan zorluklar üzerine yaptığı konuşma: <https://www.youtube.com/watch?v=kU7vk9jmQC8>
Chicago Quantum firmasının portfolyo optimizasyonu konusundaki makalesi: <https://arxiv.org/abs/2008.08669>

Bu konu üzerine yazılmış bazı yazılar:

<https://medium.com/@cohen.sourcing/our-latest-financial-portfolio-optimization-success-a-custom-simulated-annealer-77c3c6468cab>

<https://medium.com/@cohen.sourcing/what-happened-when-we-tried-to-run-72-stocks-on-the-quantum-annealer-d93bfdd6c94c>

Çalışmanın özeti:

<https://www.swissquantumhub.com/portfolio-optimization-of-60-stocks-using-quantum-algorithms/>

Makalenin gözden geçirmesi: <https://www.youtube.com/watch?v=yX44xy6jG58>

Fujitsu'nun finansta kuantum bilgisayarların kullanımı ile ilgili kısa bir videosu: <https://www.youtube.com/watch?v=cMK5knQBvd8>

Fujitsu'nun yaptığı çalışmalarla ilgili doküman: <https://www.fujitsu.com/global/digitalannealer/pdf/wp-da-financialsector-ww-en.pdf>

IBM Kuantum araştırmaları ekip üyesi Stefan Woerner'in Monte Carlo simülasyonlarına alternatif kuantum algoritmalar konusundaki yayını:

<https://www.nature.com/articles/s41534-019-0130-6>

Stefan Woerner'in kredi risk analizi konusundaki makalesi: <https://arxiv.org/abs/1907.03044>

Opsiyon fiyatlama modelleri ile ilgili Goldman Sachs'ın IBM'le yaptığı çalışmalar sonucu yayınladığı makale: <https://arxiv.org/abs/1905.02666>

IBM'in Portfolyo optimizasyonunda varyasyonel kuantum optimizasyonu kullanımı ile ilgili makalesi: <https://arxiv.org/abs/1907.04769>

KUANTUM KRİPTOGRAFI

Kuantum-sonrası kriptografi iki başlık altında toplanabilir. Birincisi kuantum bilgisayarlara dayanıklı kriptografi sistemi geliştirilmesi; ikincisi ise kuantum sistemlerin özelliklerinin kriptografide kullanılmasıdır. Heisenberg'in Belirsizlik ilkesi ve foton polarizasyon & dolanıklık ilkelerinden yola çıkılarak oluşturulan kuantum kriptografi sistemi, bahsi geçen ikinci kategoriye dahildir diyebiliriz. Birçok farklı anahtar dağıtım (Key Distribution) protokollerine sahip olan sistem, her bir dağıtım protokolü için yukarıda bahsedilmiş olan fiziksel teoremlerin farklı yönlerini ya da çeşitli kombinasyonlarını kullanır. Ayrıntılı bilgi için aşağıdaki makaleleri incelemeniz tavsiye olunur.

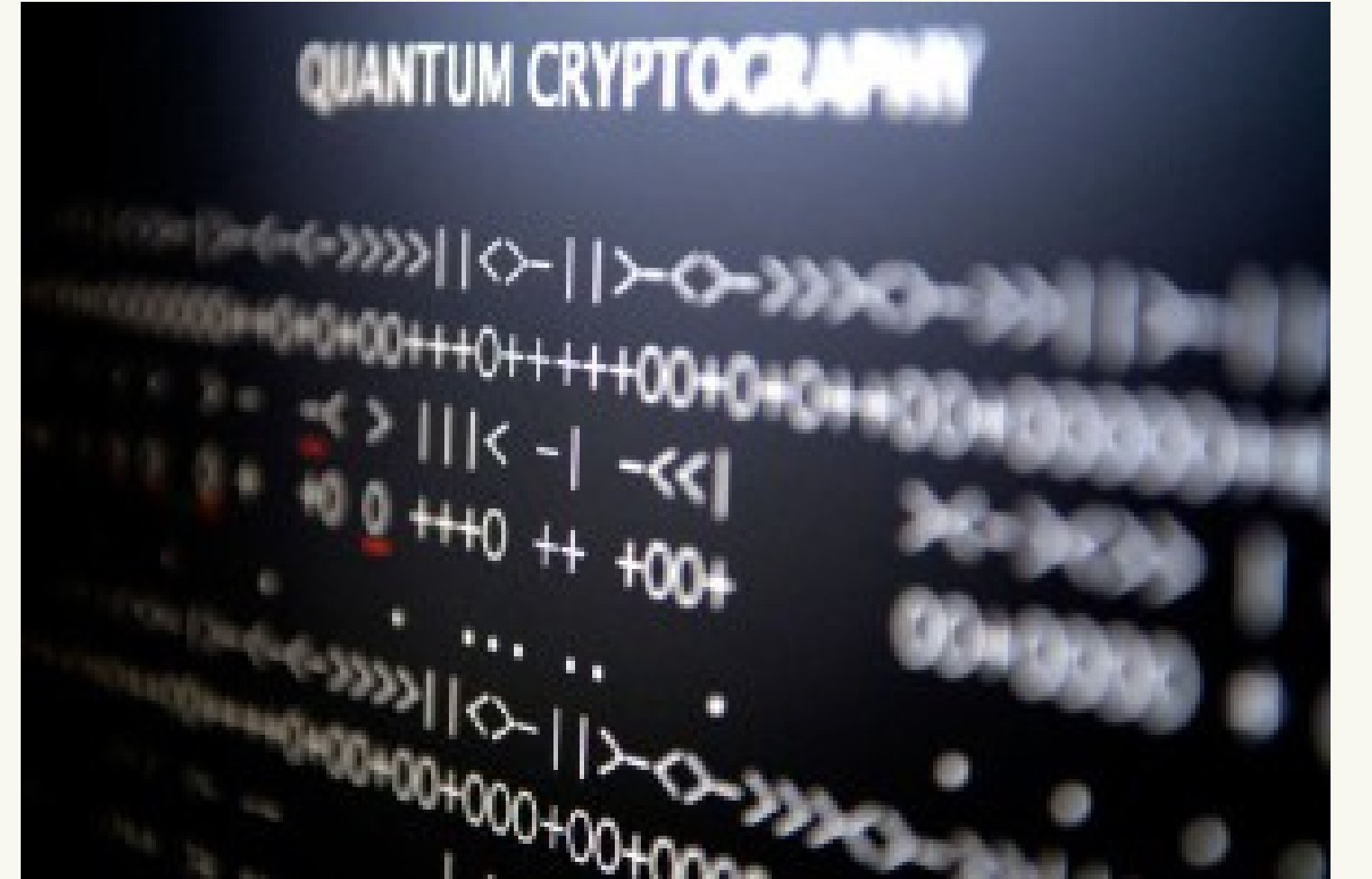
1. H. Singh, D.L.Gupta, A.K.Singh, "Quantum Key Distribution Protocols: A Review", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727 Volume 16, Issue 2, Ver. XI (Mar-Apr. 2014), PP 01-09 www.iosrjournals.org
2. A.K.Bishwas, A.Mani and V.Palade, "Quantum Supervised Clustering Algorithm for Big Data", 2018, 3rd International Conference for Convergence in Technology (I2CT) The Gateway Hotel, XION Complex, Wakad Road, Pune, India. Apr 06-08, 2018

KUANTUM KRİPTOGRAFİ

Kuantum Kriptografi hakkında kısa genel bilgiler aşağıdaki gibidir

Kuantum İletişim:

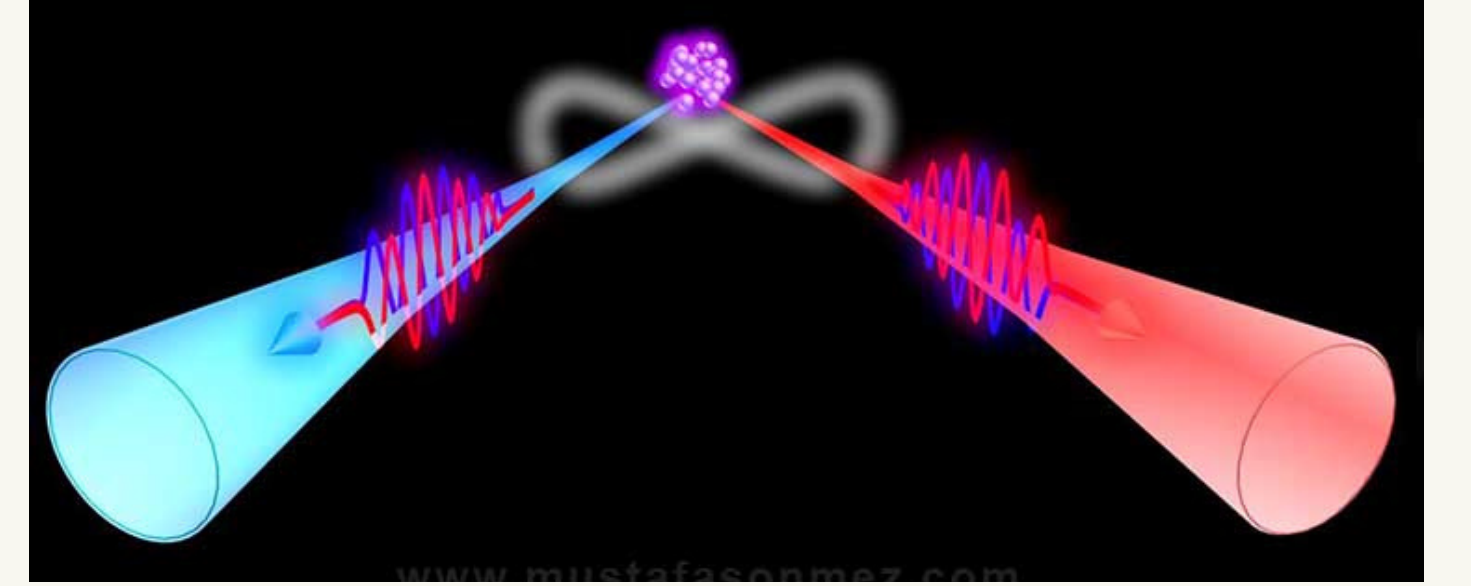
Kuantum İletişim birçok otorite tarafından günümüzde en güvenli yöntemlerden biri olarak kabul edilmektedir. Bu durumun sebebi ise tekli quantum sistemleri 0 ve 1'in süperpozisyon (süperpozisyon bir parçacığın kuantum durumunun hem 0 hem 1 olması anlamına gelir) olarak bulunabilir ve ikili sistemlerde mesela iki foton dolanık (entangled) hale gelebilir. Dolayısıyla qubit üzerinde bir ölçüm yapılırsa ya da araya giren birisi olursa, durum süperpozisyon özelliğini kaybedip rastgele 0 veya 1 durumlarından birine çöker.



KUANTUM KRİPTOGRAFİ

Kuantum Dolanıklık:

Dolanık haldeki parçacıkların kuantum durumlarının tek tek ifade edilmemesi ama tüm parçacıkların bir bütün olarak ifade edilebiliyor olması durumudur. Örneğin iki fotona sahip olduğunuzu düşünün. Bu fotonları A ve B olarak adlandıralım. Kuantum Dolanıklık ilkesinden dolayı bu A & B fotonlarını klasik fiziğin açıklayamadığı bir şekilde birbirlerinden ayrı tarif etmek mümkün değildir. Fotonlar arasındaki mesafe arttırılırsa bile durum değişmez ve fotonlar üzerinde ölçüm yapıldığı anda sistem çöker.



Bell Test:

Parçacıkların dolanık olup olmadığı ve dolanıklığın ne kadar güçlü olduğunu ölçmek için kullanılan bir testtir. -

https://en.wikipedia.org/wiki/Bell_test_experiments

KUANTUM KRİPTOGRAFİ

Kuantum Teleportasyon (Uzaktarım/Telenakil):

Kubitlerin kopyalanamaması prensibine dayanır. Kuantum bilgide klasik bilgide olduğu gibi kopyala-yapıştır yapılamaz (Non-Cloning thm). Çünkü kopyalamak aslında içeriğin görüntülendiği anlamına gelir.

Kuantum kriptografi ve anahtar dağıtımıyla ilgili daha detaylı bilgiye ulaşmak için: <https://www.idquantique.com/resource-library/quantum-key-distribution/>

TÜBİTAK BİLGEM'in bu alanda sahip olduğu fiziksel bir altyapı ürünü ve rassal sayı üreteçleri üzerine daha detaylı bilgi için: <https://arxiv.org/abs/1604.03304> ve <https://bilgem.tubitak.gov.tr/tr/urunler/kuantum-rsu-kuantum-tabanli-rasgele-sayi-ureteci>

Cambridge quantum computing grubunun rassal sayı üreteçleri hakkında yazdığı bir makale: <https://cambridgequantum.com/wp-content/uploads/2020/09/CQC-IBM-statement.pdf>

KUANTUM AĞLAR



Kuantum ağlar gelecekteki kuantum teknolojileri ekosisteminin belki de belkemiğini oluşturacak, oldukça önemli bir teknolojidir. Şu anda kullanılan klasik bilgisayar ağları gibi, kuantum ağların da birden çok işlevde kullanılması bekleniyor [1]. Atom saatlerinin senkronizasyonu, kuantum hesaplamaların dağıtık sistemlerde yapılması veya asimetrik kriptografinin en önemli kısımlarından olan açık anahtar dağıtımında kuantum ağların önemli olacağı düşünülüyor. Kuantum ağların potansiyel kullanım alanları hakkında Panagiotis Spentzouris'in sunumunu [2] da inceleyebilirsiniz.

Kuantum ağlar, diğer birçok modern kuantum teknoloji gibi kuantum mekaniğinin dolanıklık ilkesi sayesinde klasik ağlar ile elde edilemeyecek yeteneklere sahip oluyor. Dolanıklık aracılığıyla yapılan kuantum ışınlama, kübitlerin ölçülmeden aktarılabilmesini sağlıyor. Kuantum iletişimin temel ilkelerinden olan "no-cloning" teoremi [3] [4] sayesinde iletişimin güvenliği kılıyor.

KUANTUM AĞLAR

Kuantum anahtar dağıtım algoritmaları bu sebepten ötürü klasik algoritmalara üstünlük sağlıyor. Bu algoritmalar hakkında bilgi sahibi olmak isteyenler BB84 [5] ve E91 [6] algoritmalarını araştırabilirler.

Kuantum ağlar ile ilgili proje yapmak isteyenlerin 2018'deki Quantum Internet hackathonu ve 2019'daki Pan-European Quantum Internet hackathonunda yapılmış projeleri incelemeleri faydalı olacaktır. Buradaki projelerin büyük bir kısmı henüz genel kullanıma açık bir kuantum ağ bulunmadığı için kuantum ağ simülatörleri aracılığıyla gerçekleştirilmiştir. Endüstride ve akademik çalışmalarda QuTech tarafından geliştirilen SimulaQron ve NetSquid yazılımları yaygın bir şekilde kullanılmaktadır. Bunlar haricinde daha ufak gruplar tarafından geliştirilmiş olan simülatörler de mevcuttur.

Kuantum ağ teknolojisinin “state-of-the-art” sınırlarındaki akademik çalışmaları öğrenmek, çalışan gruplar hakkında bilgi sahibi olmak isteyenler, Quantum Internet Alliance'nin internet sayfasını inceleyebilir.

Quantum Internet Alliance:
<https://quantum-internet.team/>

Hackathonlar:
<https://quantum-internet.team/event/simulaqron-hackathon-2018/>
<https://github.com/PEQI19>
<https://github.com/gate42qc/quantum-futures-hackathon-2019>

Simülatörler:
SimulaQron - <http://www.simulaqron.org/>
NetSquid - <https://netsquid.org/>
SQUANCH - <https://pypi.org/project/SQUANCH/>
QuNetSim - https://aqua.sfc.wide.ad.jp/quisp_website/

- [1]Wang, C., Rahman, A. and R. Li (February, 2020). "Applications and Use Cases for the Quantum Internet", IETF Internet-Draft. <https://tools.ietf.org/id/draft-wang-qirg-quantum-internet-use-cases-02.html>
- [2]Spentzouris, P. (February 2020). "Potential Quantum Networking Applications", Quantum Internet Blueprint Workshop. https://www.orau.gov/qib-workshop/presentations/03-QInternet_Applications-2-P_Spentzouris.pdf
- [3]Wootters, William; Zurek, Wojciech (1982). "A Single Quantum Cannot be Cloned". Nature. 299 (5886): 802–803. doi:10.1038/299802a0.
- [4]Dieks, Dennis (1982). "Communication by EPR devices". Physics Letters A. 92 (6): 271–272. doi:10.1016/0375-9601(82)90084-6.
- [5]C. H. Bennett and G. Brassard. "Quantum cryptography: Public key distribution and coin tossing". In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, volume 175, page 8. New York, 1984. <http://researcher.watson.ibm.com/researcher/files/us-bennetc/BB84highest.pdf>
- [6]Ekert, Artur K. (5 August 1991). "Quantum cryptography based on Bell's theorem". Physical Review Letters. 67 (6): 661–663. doi:10.1103/PhysRevLett.67.661.

KUANTUM HATA DÜZELTME

Kuantum bilgisayarlar yeni gelişmekte olan bir teknoloji oldukları için hesaplama sırasında ideal bir kuantum bilgisayarın bulacağından farklı sonuçlar üretebilmektedirler. Kübitlerin decoherence ve diğer birtakım kuantum gürültüler sebebiyle istenen halde bulunamamaları bu hatalara sebep olmaktadır. Kullanılan farklı kuantum bilgisayarların çalışma prensipleri ve geometrik özellikleri olan topolojileri sebebiyle her bilgisayar farklı hata profillerine sahiptir. Kuantum algoritmalarından doğru sonuçlar almak adına bu hatalar düzeltilmelidir.

Bu noktada kuantum bilgisayarlarının olasılıksal doğasından kaynaklanan hatalı sonuçların kuantum hata düzeltme kapsamına girmediğini belirtmek gerekir. Bu tarz hataların düzeltilmesi için kullanılan algoritmalarda geliştirmeler yapmak gerekmektedir.



001111010010101010
010010101010010101
100010101001010101
01010 **ERROR** 0101010
101001010101001010
011000101001010101
010010101010010101

KUANTUM HATA DÜZELTME

Kuantum bilgisayarlarda hata düzeltmek için kullanılan tekniklerden birisi, aynı klasik bilgisayarlarda olduğu gibi hata düzeltme kodları kullanmaktır. Bu konuya giriş yapmak amacıyla [Qiskit Textbook \[1\]](#)'da yer alan ilgili bölüm kullanılabilir. Daha ayrıntılı bilgi için [Steane'in ilgili dökümanı \[2\]](#) okunabilir.

Hata düzeltme kodları kullanmak için fazladan kübitler kullanmak ve operasyonlar gerçekleştirmek gerekebilmektedir. Oysa günümüz bilgisayarlarında kübit sayıları azdır ve her operasyonla birlikte sisteme daha fazla gürültü eklenmektedir. Bunun alternatifi kuantum hata azaltma teknikleri kullanmaktır. Ölçümler sonrası elde edilen veriyi klasik bilgisayarlara incelemeyi içeren bu tekniğe giriş için yine [Qiskit Textbook \[1\]](#) kullanılabilir. Daha ayrıntılı bilgi için [Tannu ve Qureshi'nin \[3\]](#) veya Endo, Benjamin, Li'nin yazıları [\[4\]](#) okunabilir.

Hata düzeltme ve azaltma teknikleri günümüzde hali hazırda yaygın olarak kullanılmaktadır. [Qiskit Ignis \[5\]](#), Qiskit ile oluşturulmuş devreler için bu teknikleri kullanabilmektedir. Ayrıca platformdan bağımsız olarak çalışabilen Mitiq kütüphanesi [\[6\]](#) [\[7\]](#) de farklı bilgisayarlar için bu operasyonları gerçekleştirebilmektedir

ÖNCEKİ HACKATHONLAR

Kuantum teknolojileri ile ilgili düzenlenmiş bir sürü hackathon mevcut ve çoğu hackathon, bizim de yapmak istediğimiz gibi, projeleri bir Github hesabında topluyor ve erişime açıyor.

Projenize dair fikir almak, özgünlüğünü kontrol etmek istersiniz diye önceden düzenlenmiş hackathonların Github linklerini sizinle paylaşmak istedik.

[QTurkey Hackathon Aralık 2019](#)

[Quantum Internet Hackathon 2019](#)

[Qiskit Presentations](#)

[Qiskit Hackathon Taiwan 2020](#)

[IBM May 4 Quantum Challenge](#)

[Qiskit Camp Africa 19](#)

[Qiskit Hackathon Bilbao 19](#)

[Qiskit Camp Asia 19](#)

[Qiskit Hackathon Singapore 19](#)

[Qiskit Camp Europe 19](#)

[3rd Quantum Collective Knowledge Hackathon, Paris, 27 January 2019](#)

[4th Quantum Collective Knowledge Hackathon, Oxford, 15 March 2019](#)

[CDL Quantum Hackathon 2020](#)

[iQuHack2020](#)

EMEĐİ GEÇENLER

Bu kitapçık ařaĐıda adı geen QTurkey üyeleri tarafından hazırlanmıřtır.

Berat Yenilen

Caner Ercan

Cenk Tüysüz

Eda Altuntař

Ekin Aykut

Jale İpekoĐlu

Kübra Cin

Ufkum Deniz Altunkapak

Zeki Seskir