به نام خدا

تأثیر کامپیوترهای کوانتومی بر پردازش داده ها

مولف :

عسل رضایی

انتشارات ارسطو

(سازمان چاپ و نشر ایران – ۱۴۰۳)

نسخه الکترونیکی این اثر در سایت سازمان چاپ و نشر ایران و اپلیکیشن کتاب رسان موجود می باشد

chaponashr.ir

سرشناسه : رضایی، عسل، ۱۳۸۰
عنوان و نام پدیدآور : تأثیر کامپیوترهای کوانتومی بر پردازش داده ها/ مولف عسل رضایی.
مشخصات نشر : انتشارات ارسطو (سازمان چاپ و نشر ایران)، ۱۴۰۳.
مشخصات ظاهری : ۱۴۴ ص.
شابک : ۶-۹۹۴-۴۰۸-۶۲۲-۹۷۸
وضعیت فهرست نویسی : فیپا
موضوع : کامپیوترهای کوانتومی - پردازش داده ها
رده بندی کنگره : Q۳۸۸
رده بندی دیویی : ۰۱۰/۹
شماره کتابشناسی ملی : ۹۷۲۷۸۰۸
اطلاعات رکورد کتابشناسی : فیپا

نام کتاب : تأثیر کامپیوترهای کوانتومی بر پردازش داده ها
مولف : عسل رضایی
ناشر : انتشارات ارسطو (سازمان چاپ و نشر ایران)
صفحه آرایی، تنظیم و طرح جلد: پروانه مهاجر
تیراژ : ۱۰۰۰ جلد
نوبت چاپ : اول – ۱۴۰۳
چاپ : زبرجد
قیمت : ۱۴۴۰۰۰ تومان
فروش نسخه الکترونیکی - کتاب‌رسان :
https://chaponashr.ir/ketabresan
شابک : ۶-۹۹۴-۴۰۸-۶۲۲-۹۷۸
تلفن مرکز پخش : ۰۹۱۲۰۲۳۹۲۵۵
www. chaponashr. ir

فهرست

فصلاول: مقدمه‌ای بر کامپیوترهای کوانتومی ۱۱

تاریخچه محاسبات و ظهور فناوری کوانتومی ۱۳

تفاوت محاسبات کلاسیک و کوانتومی ۱۵

مفاهیم اولیه مکانیک کوانتومی ۱۷

بیت کوانتومی (کیوبیت) و ویژگی‌های آن ۱۹

برهم‌نهی کوانتومی ۱۹

درهم‌تنیدگی کوانتومی ۱۹

اندازه‌گیری و فروپاشی تابع موج ۲۰

گیت‌های کوانتومی و عملیات روی کیوبیت‌ها ۲۰

درهم‌تنیدگی و برهم‌نهی در کامپیوترهای کوانتومی ۲۰

برهم‌نهی (Superposition) در کامپیوترهای کوانتومی ۲۱

کاربرد برهم‌نهی در پردازش داده‌ها ۲۱

درهم‌تنیدگی (Entanglement) در کامپیوترهای کوانتومی ۲۱

کاربرد درهم‌تنیدگی در پردازش کوانتومی ۲۲

چالش‌های استفاده از برهم‌نهی و درهم‌تنیدگی ۲۲

چشم‌انداز آینده محاسبات کوانتومی ۲۳

فصل دوم: مبانی نظری محاسبات کوانتومی ۲۷

مبانی نظری محاسبات کوانتومی ۲۷

اصول ریاضیاتی محاسبات کوانتومی ۳۰

دروازه‌های منطقی کوانتومی ۳۳

الگوریتم‌های پایه کوانتومی ۳۵

شبیه‌سازی پدیده‌های فیزیکی با کوانتوم ۳۷
زبان‌های برنامه‌نویسی کوانتومی ۳۹
مدل‌های محاسباتی در دنیای کوانتوم ۴۲
فصل سوم: سخت‌افزار کامپیوترهای کوانتومی ۴۷
فناوری‌های ساخت کیوبیت ۴۸
سیستم‌های ابررسانا و تله‌یونی ۵۰
معماری پردازنده‌های کوانتومی ۵۲
ویژگی‌های معماری پردازنده‌های کوانتومی خطی ۵۳
مزایای معماری پردازنده‌های کوانتومی خطی ۵۳
چالش‌ها و معایب ۵۴
چالش‌های فنی در سخت‌افزار کوانتومی ۵۴
محیط‌های نگهداری و کنترل کوانتومی ۵۷
پیشرفت‌های اخیر در سخت‌افزار کوانتومی ۶۰
فصل چهارم: الگوریتم‌های کوانتومی و پردازش داده‌ها ۶۳
الگوریتم شور و رمزگشایی سریع ۶۵
نحوه عملکرد الگوریتم شور ۶۵
مراحل کلیدی الگوریتم شور ۶۵
تهدید برای رمزنگاریRSA ۶۶
کاربردها و چشم‌اندازهای آینده ۶۶
الگوریتم گروور و جستجوی کوانتومی ۶۷
نحوه عملکرد الگوریتم گروور ۶۷
مراحل کلیدی الگوریتم گروور ۶۷

تهدید برای رمزنگاری ۶۹
چشم‌انداز آینده ۶۹
الگوریتم‌های یادگیری ماشین کوانتومی ۶۹
ویژگی‌های محاسبات کوانتومی و پردازش داده‌های کلان ۷۲
الگوریتم‌های کوانتومی و پردازش داده‌های کلان ۷۲
چالش‌ها و فرصت‌ها ۷۲
کاربردهای پردازش داده‌های کلان با محاسبات کوانتومی ۷۳
تفاوت الگوریتم‌های کوانتومی و کلاسیک ۷۴
بهینه‌سازی و حل مسائل پیچیده با کوانتوم ۷۶
فصل پنجم:تأثیر کامپیوترهای کوانتومی بر امنیت اطلاعات.....۸۱
تهدیدات امنیتی ناشی از کامپیوترهای کوانتومی ۸۱
تأثیرات در سیستم‌های رمزنگاری..... ۸۲
محاسبات کوانتومی و رمزنگاری مقاوم به کوانتوم ۸۲
توسعه استانداردهای رمزنگاری مقاوم به کوانتوم ۸۳
تهدیدات کوانتومی علیه رمزنگاری کلاسیک ۸۳
رمزنگاری پساکوانتومی و راهکارهای جدید..... ۸۶
چالش‌ها و ضرورت رمزنگاری پساکوانتومی ۸۷
راهکارهای جدید در رمزنگاری پساکوانتومی ۸۷
چالش‌ها و آینده رمزنگاری پساکوانتومی..... ۸۹
تبادل کلید کوانتومی و امنیت سایبری..... ۸۹
اصول تبادل کلید کوانتومی ۹۰
الگوریتم‌های معروف در تبادل کلید کوانتومی ۹۰

امنیت تبادل کلید کوانتومی ۹۰
تأثیر تبادل کلید کوانتومی بر امنیت سایبری ۹۱
چالش‌های تبادل کلید کوانتومی در امنیت سایبری..... ۹۱
آینده تبادل کلید کوانتومی و امنیت سایبری ۹۲
نقش هوش مصنوعی در امنیت کوانتومی ۹۲
هوش مصنوعی و تهدیدات امنیتی کوانتومی ۹۳
کشف الگوها و پیش‌بینی حملات کوانتومی با استفاده از هوش مصنوعی ۹۳
ایجاد الگوریتم‌های پساکوانتومی با هوش مصنوعی ۹۴
مدیریت داده‌های کوانتومی و امنیت آن با استفاده از هوش مصنوعی ۹۴
توسعه شبکه‌های کوانتومی امن با استفاده از AI ۹۴
آینده‌ی امنیت دیجیتال در عصر کوانتومی ۹۵
تهدیدات کوانتومی برای امنیت دیجیتال ۹۵
رمزنگاری پساکوانتومی ۹۶
تبادل کلید کوانتومی(QKD) ۹۶
هوش مصنوعی و امنیت کوانتومی ۹۶
چالش‌ها و فرصت‌ها ۹۷
چالش‌های قانونی و اخلاقی در امنیت کوانتومی ۹۷
چالش‌های قانونی..... ۹۷
چالش‌های اخلاقی ۹۸
چالش‌های اجتماعی و بین‌المللی ۹۹
فصل ششم: تأثیر کامپیوترهای کوانتومی بر کلان‌داده‌ها Big Data..... ۱۰۱
توانایی‌های پردازشی کامپیوترهای کوانتومی ۱۰۱

پردازش سریع‌تر و دقیق‌تر داده‌ها ۱۰۱
بهینه‌سازی و جستجوی داده‌ها ۱۰۲
یادگیری ماشین کوانتومی و تحلیل داده‌ها ۱۰۲
چالش‌ها و محدودیت‌های فناوری کوانتومی ۱۰۲
پردازش سریع داده‌های حجیم با کوانتوم ۱۰۳
ویژگی‌های کوانتومی و تأثیر آن‌ها بر پردازش داده‌های حجیم ۱۰۳
پردازش داده‌های حجیم در پردازش موازی با کامپیوترهای کوانتومی ۱۰۳
الگوریتم‌های کوانتومی در پردازش داده‌های حجیم ۱۰۴
یادگیری ماشین و تحلیل داده‌های حجیم با کوانتوم ۱۰۴
چالش‌های پردازش داده‌های حجیم با کوانتوم ۱۰۴
یادگیری ماشین کوانتومی برای تحلیل داده‌ها ۱۰۵
مزایای یادگیری ماشین کوانتومی ۱۰۶
الگوریتم‌های کوانتومی در یادگیری ماشین ۱۰۶
ذخیره‌سازی و مدیریت داده‌ها در کامپیوترهای کوانتومی ۱۰۷
چالش‌های ذخیره‌سازی داده در کامپیوترهای کوانتومی ۱۰۸
مدیریت داده‌ها در سیستم‌های کوانتومی ۱۰۹
داده‌کاوی کوانتومی و کاربردهای آن ۱۰۹
ویژگی‌های داده‌کاوی کوانتومی ۱۱۰
مزایای داده‌کاوی کوانتومی ۱۱۰
کاربردهای داده‌کاوی کوانتومی ۱۱۱
چالش‌های داده‌کاوی کوانتومی ۱۱۲
شبکه‌های عصبی کوانتومی در تحلیل داده‌ها ۱۱۲

ویژگی‌های اصلی شبکه‌های عصبی کوانتومی ۱۱۳
کاربردهای شبکه‌های عصبی کوانتومی در تحلیل داده‌ها ۱۱۳
چالش‌ها و محدودیت‌ها..... ۱۱۴
آینده تحلیل داده‌ها با قدرت پردازشی کوانتومی..... ۱۱۵
ویژگی‌های منحصر به فرد پردازش کوانتومی در تحلیل داده‌ها..... ۱۱۶
کاربردهای پردازش داده‌ها با کامپیوترهای کوانتومی..... ۱۱۶
فصل هفتم : تأثیر کامپیوترهای کوانتومی بر صنایع مختلف ۱۱۹
صنعت داروسازی و سلامت ۱۱۹
صنعت مالی و بیمه..... ۱۲۰
صنعت خودروسازی و حمل و نقل ۱۲۰
صنعت تولید و ساخت ۱۲۱
امنیت سایبری و رمزنگاری ۱۲۱
صنعت کشاورزی و منابع طبیعی..... ۱۲۱
تأثیر بر اقتصاد و امور مالی..... ۱۲۲
تأثیر کامپیوترهای کوانتومی بر اقتصاد و امور مالی ۱۲۲
کاربرد در شیمی و داروسازی ۱۲۵
کاربرد کامپیوترهای کوانتومی در شیمی و داروسازی ۱۲۵
پیشرفت‌های پزشکی و تصویربرداری کوانتومی ۱۲۷
تأثیر بر مهندسی و طراحی مواد جدید..... ۱۲۹
تأثیر کامپیوترهای کوانتومی بر مهندسی و طراحی مواد جدید..... ۱۲۹
نقش کامپیوترهای کوانتومی در هوافضا..... ۱۳۱
آینده شبیه‌سازی‌های علمی با کوانتوم ۱۳۳

نتیجه‌گیری و پیامدهای جهانی کامپیوترهای کوانتومی ۱۳۴
پیشنهادات: ۱۳۸
منابع انگلیسی: ۱۴۱
سایت‌های مرتبط با کامپیوترهای کوانتومی: ۱۴۴

فصل اول

مقدمه‌ای بر کامپیوترهای کوانتومی

کامپیوترهای کوانتومی یکی از نوآورانه‌ترین فناوری‌های قرن بیست و یکم هستند که می‌توانند تحولی عظیم در پردازش داده‌ها ایجاد کنند. برخلاف کامپیوترهای کلاسیک که مبتنی بر بیت‌های صفر و یک هستند، کامپیوترهای کوانتومی از کیوبیت‌ها استفاده می‌کنند که قادر به نگهداری و پردازش اطلاعات در وضعیت‌های مختلف به‌صورت همزمان هستند (Nielsen & Chuang, 2010). این ویژگی، که برهم‌نهی نام دارد، به کامپیوترهای کوانتومی امکان می‌دهد محاسبات پیچیده را با سرعتی بسیار بیشتر از کامپیوترهای سنتی انجام دهند (Preskill, ۲۰۱۸).

یکی از اصول اساسی کامپیوترهای کوانتومی، درهم‌تنیدگی کوانتومی است. این خاصیت به کیوبیت‌ها اجازه می‌دهد که به‌صورت غیرمحلی با یکدیگر ارتباط برقرار کنند، به‌گونه‌ای که تغییر وضعیت یکی از کیوبیت‌ها مستقیماً بر وضعیت دیگری تأثیر می‌گذارد، حتی اگر در فاصله‌ای زیاد از یکدیگر قرار داشته باشند (Einstein et al., 1935). این ویژگی کامپیوترهای کوانتومی را قادر می‌سازد تا در حوزه‌هایی مانند رمزنگاری، بهینه‌سازی و شبیه‌سازی‌های پیچیده عملکردی بی‌نظیر داشته باشند (Shor, 1994).

یکی از مهم‌ترین دستاوردهای این حوزه، الگوریتم شور است که امکان شکستن سیستم‌های رمزنگاری مبتنی بر فاکتورگیری اعداد اول را فراهم می‌کند. این الگوریتم نشان می‌دهد که با استفاده از کامپیوترهای کوانتومی، می‌توان مسائل ریاضی بسیار پیچیده را که برای کامپیوترهای کلاسیک غیرممکن یا زمان‌بر هستند، در زمانی کوتاه حل کرد (Shor, 1997). این موضوع نگرانی‌های بسیاری را در زمینه امنیت سایبری ایجاد کرده است و پژوهشگران در تلاش‌اند تا رمزنگاری‌های مقاوم در برابر حملات کوانتومی توسعه دهند (Bernstein et al., 2009).

پردازش کوانتومی همچنین در حوزه هوش مصنوعی و یادگیری ماشین تأثیر بسزایی دارد. به کمک الگوریتم‌های کوانتومی، می‌توان حجم وسیعی از داده‌ها را به‌طور همزمان پردازش کرد و الگوهای پنهان را سریع‌تر از روش‌های سنتی کشف نمود .(Biamonte et al., 2017) این قابلیت باعث می‌شود که مدل‌های یادگیری عمیق عملکرد بهتری داشته باشند و در کاربردهایی مانند بینایی ماشین، تشخیص گفتار و تحلیل داده‌های پزشکی به کار گرفته شوند (Harrow et al., 2009).

یکی از چالش‌های اساسی در توسعه کامپیوترهای کوانتومی، پایداری کیوبیت‌ها و کاهش خطای محاسباتی است. به دلیل ماهیت حساس سیستم‌های کوانتومی، کیوبیت‌ها به‌شدت تحت تأثیر نویزهای محیطی قرار دارند و پایداری آن‌ها یکی از مشکلات اساسی برای توسعه سیستم‌های مقیاس‌پذیر است .(Devoret & Schoelkopf, 2013) ازاین‌رو، تصحیح خطای کوانتومی یکی از حوزه‌های کلیدی تحقیقاتی است که به بهبود عملکرد این سیستم‌ها کمک می‌کند (Gottesman, 1997).

در سال‌های اخیر، شرکت‌های بزرگی مانند گوگل، آی‌بی‌ام و مایکروسافت سرمایه‌گذاری‌های عظیمی در حوزه محاسبات کوانتومی انجام داده‌اند. گوگل در سال ۲۰۱۹ ادعا کرد که موفق به دستیابی به برتری کوانتومی شده است، مفهومی که نشان‌دهنده برتری کامپیوترهای کوانتومی بر کامپیوترهای کلاسیک در انجام یک وظیفه خاص است .(Arute et al., 2019) هرچند این ادعا همچنان موردبحث است، اما نشان‌دهنده پیشرفت‌های چشمگیر در این حوزه می‌باشد.

کاربردهای محاسبات کوانتومی فراتر از رمزنگاری و یادگیری ماشین است. در علوم زیستی، می‌توان از این فناوری برای شبیه‌سازی مولکول‌ها و کشف داروهای جدید استفاده کرد. به دلیل توانایی فوق‌العاده کامپیوترهای کوانتومی در مدل‌سازی سیستم‌های پیچیده، آن‌ها می‌توانند به کشف داروهای مؤثرتر و طراحی مواد جدید کمک کنند.(Aspuru-Guzik et al., 2005)

محاسبات کوانتومی همچنین می‌توانند نقش کلیدی در حل مسائل بهینه‌سازی ایفا کنند. بسیاری از مسائل مهندسی، مالی و صنعتی نیازمند یافتن بهترین راه‌حل از میان میلیاردها گزینه ممکن هستند. کامپیوترهای کوانتومی با بهره‌گیری از روش‌هایی مانند الگوریتم گروور می‌توانند این مشکلات را بسیار سریع‌تر از روش‌های کلاسیک حل کنند.(Grover, 1996)

بااین‌حال، مسیر توسعه کامپیوترهای کوانتومی همچنان چالش‌های زیادی پیش رو دارد. علاوه بر پایداری کیوبیت‌ها، توسعه نرم‌افزارهای کوانتومی نیز یکی از موانع مهم در این حوزه است. برنامه‌نویسی برای سیستم‌های کوانتومی نیازمند رویکردهای جدیدی است که با روش‌های سنتی بسیار متفاوت می‌باشند.(Selinger, 2004)

از منظر اقتصادی، ظهور کامپیوترهای کوانتومی می‌تواند تأثیرات گسترده‌ای بر صنایع مختلف داشته باشد. بانک‌ها و مؤسسات مالی می‌توانند از این فناوری برای بهینه‌سازی سبدهای سرمایه‌گذاری و تحلیل ریسک استفاده کنند، درحالی‌که صنایع تولیدی می‌توانند فرآیندهای پیچیده خود را بهینه‌سازی نمایند.(Orús et al., 2019)

در سطح سیاست‌گذاری، کشورهای مختلف به‌طور جدی در حال رقابت برای پیشرفت در این حوزه هستند. ایالات متحده، چین و اتحادیه اروپا سرمایه‌گذاری‌های کلانی برای توسعه فناوری کوانتومی انجام داده‌اند و انتظار می‌رود که این رقابت در آینده شدت بیشتری پیدا کند (National Academies of Sciences, 2019).

به‌رغم تمام این چالش‌ها، آینده کامپیوترهای کوانتومی بسیار امیدوارکننده است. با پیشرفت در زمینه‌های سخت‌افزار، نرم‌افزار و الگوریتم‌های کوانتومی، می‌توان انتظار داشت که این فناوری در دهه‌های آینده به یکی از ارکان اصلی دنیای دیجیتال تبدیل شود.(Montanaro, 2016)

نتیجه‌گیری کلی این است که محاسبات کوانتومی نه‌تنها می‌توانند محاسبات پیچیده را سرعت بخشند، بلکه می‌توانند مسائل علمی و صنعتی حل‌نشده را با رویکردی کاملاً جدید موردبررسی قرار دهند. پیشرفت‌های آتی در این زمینه می‌توانند به تغییرات گسترده‌ای در نحوه پردازش اطلاعات و بهره‌گیری از فناوری منجر شوند، به‌طوری‌که بسیاری از چالش‌های امروزی در محاسبات کلاسیک برطرف گردند.(Ladd et al., 2010)

تاریخچه محاسبات و ظهور فناوری کوانتومی

محاسبات از دیرباز بخشی جدایی‌ناپذیر از پیشرفت علمی و فنی بشر بوده است. از چرتکه‌های باستانی تا رایانه‌های امروزی، مسیر پیشرفت محاسبات با تحولات چشمگیری همراه بوده است. در قرن هفدهم، ریاضیدانانی مانند بلیز پاسکال و گوتفرید ویلهلم لایبنیتس ماشین‌های محاسباتی

مکانیکی اولیه را توسعه دادند که می‌توانستند عملیات جمع و تفریق را انجام دهند. اما جهش واقعی در محاسبات با معرفی رایانه‌های الکترونیکی در قرن بیستم رخ داد.

در دهه ۱۹۴۰، جان فون نویمان با معرفی معماری ذخیره برنامه، بنیان رایانه‌های مدرن را بنا نهاد. این معماری، که همچنان در رایانه‌های امروزی استفاده می‌شود، شامل واحد پردازش مرکزی(CPU) ، حافظه و واحد ورودی/خروجی است. در سال‌های بعد، توسعه ترانزیستورها در دهه ۱۹۵۰ و مدارهای مجتمع در دهه ۱۹۶۰، به افزایش سرعت و کاهش اندازه رایانه‌ها منجر شد. در دهه ۱۹۷۰ و ۱۹۸۰، ظهور ریزپردازنده‌ها و رایانه‌های شخصی، محاسبات را به سطح جدیدی رساند و امکان استفاده گسترده از رایانه‌ها را فراهم کرد.

اما با افزایش تقاضا برای پردازش داده‌های پیچیده‌تر، محدودیت‌های رایانه‌های کلاسیک آشکار شد. بر اساس قانون مور، توان پردازشی تراشه‌ها تقریباً هر دو سال دو برابر می‌شد، اما این روند با نزدیک شدن به محدودیت‌های فیزیکی ترانزیستورها، کندتر شد. در این میان، دانشمندان به دنبال روش‌های جدیدی برای افزایش توان پردازشی بودند که یکی از آن‌ها، محاسبات کوانتومی بود.

فناوری کوانتومی ریشه در اصول مکانیک کوانتومی دارد، شاخه‌ای از فیزیک که رفتار ذرات در مقیاس بسیار کوچک را توصیف می‌کند. در دهه ۱۹۸۰، ریچارد فاینمن و یوری مانین پیشنهاد کردند که رایانه‌هایی که بر اساس قوانین کوانتومی کار می‌کنند، می‌توانند برخی از محاسبات را بسیار سریع‌تر از رایانه‌های کلاسیک انجام دهند. فاینمن معتقد بود که برای شبیه‌سازی سیستم‌های کوانتومی، باید از پردازنده‌هایی با ماهیت کوانتومی استفاده شود.

در دهه ۱۹۹۰، پیتر شور الگوریتمی را معرفی کرد که نشان داد یک رایانه کوانتومی می‌تواند فاکتورگیری اعداد اول را با سرعتی بسیار بیشتر از رایانه‌های کلاسیک انجام دهد. این کشف نشان داد که فناوری کوانتومی می‌تواند تهدیدی جدی برای سیستم‌های رمزنگاری مبتنی بر اعداد اول باشد و از آن زمان، تحقیقات در این زمینه شدت گرفت.

در سال‌های اخیر، شرکت‌هایی مانند گوگل، آی‌بی‌ام و مایکروسافت سرمایه‌گذاری‌های گسترده‌ای در توسعه سخت‌افزارهای کوانتومی انجام داده‌اند. در سال ۲۰۱۹، گوگل اعلام کرد که به برتری کوانتومی دست یافته است، یعنی حل مسئله‌ای که برای رایانه‌های کلاسیک غیرعملی است. این

پیشرفت نشان داد که محاسبات کوانتومی دیگر یک تئوری صرف نیست، بلکه در حال تبدیل شدن به یک فناوری کاربردی است.

ظهور فناوری کوانتومی نه‌تنها محاسبات را متحول خواهد کرد، بلکه تأثیرات گسترده‌ای بر حوزه‌هایی مانند هوش مصنوعی، شیمی، فیزیک مواد و بهینه‌سازی خواهد داشت. با پیشرفت در توسعه کیوبیت‌های پایدارتر و الگوریتم‌های کوانتومی، انتظار می‌رود که در آینده‌ای نه‌چندان دور، محاسبات کوانتومی نقش کلیدی در پردازش داده‌ها ایفا کند.

تفاوت محاسبات کلاسیک و کوانتومی

محاسبات کلاسیک و کوانتومی دو رویکرد کاملاً متفاوت برای پردازش اطلاعات دارند. محاسبات کلاسیک بر پایه اصول فیزیک نیوتنی و منطق دودویی عمل می‌کند، درحالی‌که محاسبات کوانتومی از قوانین مکانیک کوانتومی پیروی می‌کند. این تفاوت‌های بنیادی باعث شده است که رایانه‌های کوانتومی، پتانسیل انجام محاسباتی را داشته باشند که برای رایانه‌های کلاسیک غیرعملی یا بسیار زمان‌بر هستند. در ادامه، برخی از تفاوت‌های کلیدی این دو نوع محاسبات بررسی می‌شود.

۱ .واحد پردازش اطلاعات: بیت در برابر کیوبیت

در محاسبات کلاسیک، اطلاعات توسط بیت (bit) نمایش داده می‌شود که می‌تواند مقدار ۰ یا ۱ داشته باشد. پردازش داده‌ها از طریق عملیات منطقی روی این بیت‌ها انجام می‌شود. در مقابل، رایانه‌های کوانتومی از کیوبیت (qubit) استفاده می‌کنند. کیوبیت برخلاف بیت کلاسیک می‌تواند در ترکیبی از ۰ و ۱ به‌صورت همزمان باشد، وضعیتی که به آن برهم‌نهی (superposition)می‌گویند. این ویژگی باعث می‌شود که رایانه‌های کوانتومی توانایی پردازش چندین مقدار را به‌طور همزمان داشته باشند.(Nielsen & Chuang, 2010)

۲ .برهم‌نهی کوانتومی و پردازش همزمان داده‌ها

در یک رایانه کلاسیک، اگر یک سیستم-n بیتی داشته باشیم، فقط یکی از ۲ n^حالت ممکن را در هر لحظه می‌توان ذخیره کرد و پردازش نمود. اما در محاسبات کوانتومی، به دلیل خاصیت برهم‌نهی، یک کیوبیت می‌تواند در ترکیبی از هر دو مقدار ۰ و ۱ باشد، و یک سیستم-n کیوبیتی می‌تواند به‌طور همزمان تمام ۲ n^حالت را پردازش کند. این ویژگی امکان انجام محاسبات موازی