

24.09-01.10



Суперкомпьютерные
дни в России

2022

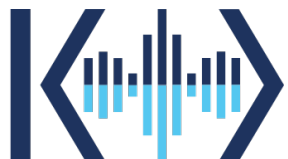
международный конгресс

Квантовые вычисления: прогнозы и препятствия

Сергей Кулик

Центр квантовых технологий

МГУ имени М.В.Ломоносова

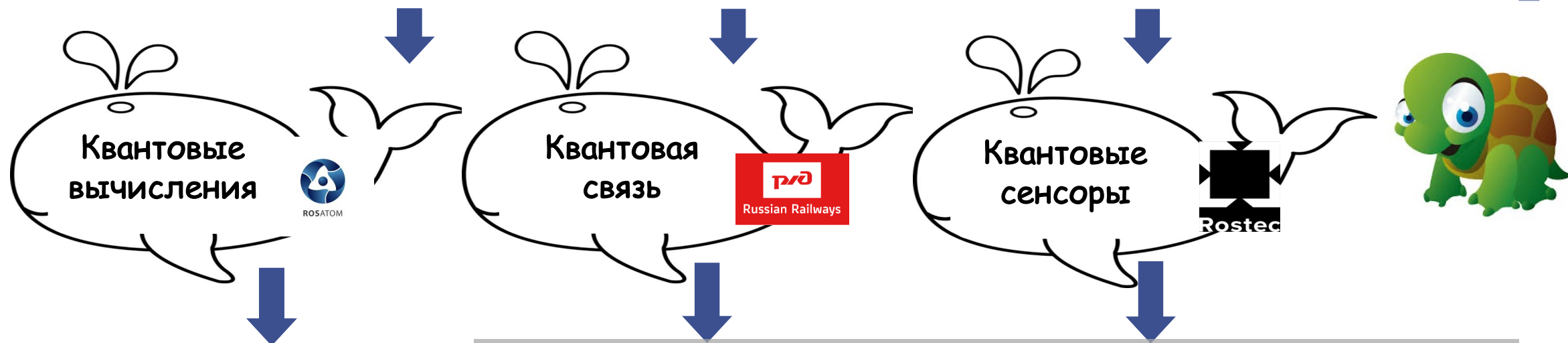


Центр
квантовых
технологий

Суперкомпьютерные дни в России
27 сентября 2022г.

Физический факультет
МГУ имени М.В.Ломоносова





Ионы и нейтральные атомы в ловушках

Линейно-оптические вычисления (фотонные чипы)

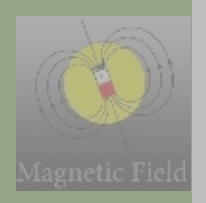
Сверхпроводниковые кубиты

Оптоволоконные каналы


Атмосферные/космические каналы: мобильные и стационарные

Квантовая память, квантовые интерфейсы...

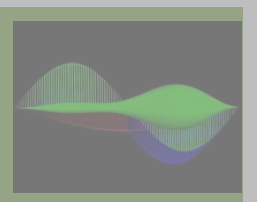
Сенсоры электрических и магнитных полей



Часы, гравиметры, гироскопы



Квантовая метрология



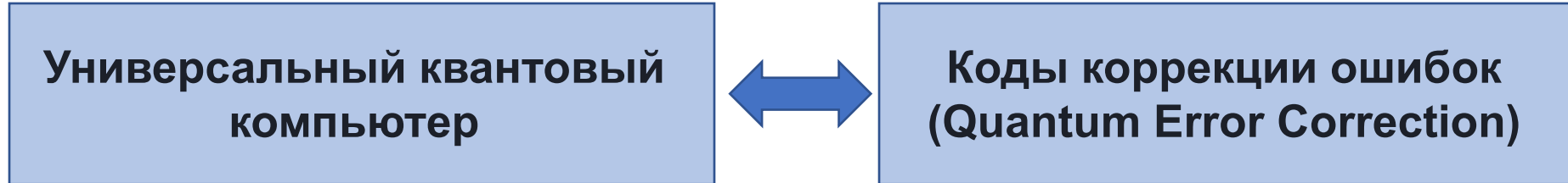
Что такое квантовый компьютер?

1. Это физическое устройство, выполняющее логические операции над квантовыми состояниями путем унитарных преобразований (т.е. сохраняющих энергию), не нарушающих квантовые суперпозиции в процессе вычислений.
 2. Это физический компьютер, работа которого:
 - основана на уникальных свойствах квантовой физики;
 - принципиально отличается от практически всех существующих компьютеров (которые в совокупности называются классическими)



Критерии Ди Винченцо:

- масштабируемость;**
- надежная инициализация;**
- большие времена декогеренции (релаксации)
по сравнению с временем срабатывания
отдельных гейтов;**
- возможность манипуляций;**
- передача и считывание состояний кубитов**



Альтернативы

NISQ
(noisy intermediate-scale quantum)
компьютеры –
рядка сотни кубитов

Квантовый отжиг
(quantum annealing)

Сортировка бозонов
(boson sampling)

Квантовые симуляторы

СПЕЦИАЛИЗИРОВАННЫЙ КВАНТОВЫЙ СОПРОЦЕССОР



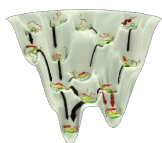
Квантовый отжиг



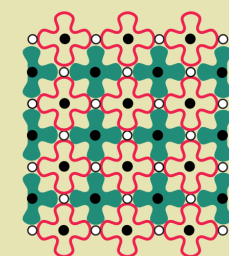
ПРИМЕНЕНИЕ
глобальная оптимизация

УНИВЕРСАЛЬНОСТЬ
ограниченная

ВЫЧИСЛИТЕЛЬНАЯ МОЩНОСТЬ
ограниченная



КЛАССИЧЕСКИЙ ВЫЧИСЛИТЕЛЬНЫЙ КЛАСТЕР



КВАНТОВЫЙ СОПРОЦЕССОР

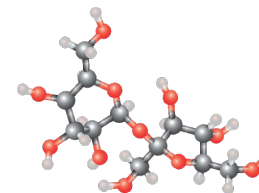
NISQ устройство

ПРИМЕНЕНИЕ
квантовая химия
наука о материалах
глобальная оптимизация
задачи сэмплинга
квантовая динамика



УНИВЕРСАЛЬНОСТЬ
частичная

ВЫЧИСЛИТЕЛЬНАЯ МОЩНОСТЬ
высокая?



Универсальный квантовый компьютер



ПРИМЕНЕНИЕ
защищенные вычисления
машинное обучение
криптография
квантовая химия
наука о материалах
глобальная оптимизация
задачи сэмплинга
квантовая динамика
задачи поиска

УНИВЕРСАЛЬНОСТЬ
полная, математически обоснованное
ускорение

ВЫЧИСЛИТЕЛЬНАЯ МОЩНОСТЬ
очень высокая



Сегодня обозначена возможность использования квантового компьютера для решения практически значимых задач

ФАЗЫ ЗРЕЛОСТИ КВАНТОВЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ

В БЛИЖНЕСРОЧНОЙ, СРЕДНЕСРОЧНОЙ И ДОЛГОСРОЧНОЙ ПЕРСПЕКТИВАХ



	«Эра» NISQ	Всеобщее квантовое превосходство	Полномасштабный помехоустойчивый квантовый компьютер
	3-5 лет	Более 10 лет	Более 20 лет
Технические достижения	Устранение ошибок	Исправление ошибок	Модульная архитектура
Пример влияния на бизнес	Симуляторы задач материаловедения	Оценки финансовых рисков в близком к реальному времени (например, для инвестиционных фондов)	Дизайн лекарств, содержащих большие биопрепараты, с минимальными побочными эффектами
Операционная прибыль	2-5 млрд. долларов	25-50 млрд. долларов	450-850 млрд. долларов



Задача	Полезно для...	Отраслевые приложения
Комбинаторная оптимизация	Минимизация или максимизация целевой функции, например, поиск наиболее эффективных ресурсов или поиск самого короткого расстояния между точками (задача странствующего коммивояжера)	<ul style="list-style-type: none"> • Оптимизация сети (например, для авиалиний, такси) • Оптимизация цепочек поставок и/или логистики • Оптимизация финансовых сервисов
Решение систем диф. уравнений	Моделирование поведения сложных систем, (например, уравнение Навье-Стокса в гидродинамике)	<ul style="list-style-type: none"> • Моделирование гидродинамики для дизайна - автомобильной и авиационной техники; • Моделирование медицинских приложений (например, анализ кровотока); • Молекулярное моделирование новых материалов и/или лекарств
Решение систем линейных уравнений	Задачи машинного обучения с использованием матрицы диагонализации (например в задаче кластеризации)	<ul style="list-style-type: none"> • Управление рисками в финансовой сфере • Классификация последовательностей ДНК • Маркетинг и сегментация клиентов
Задача факторизации	Криптография и компьютерная безопасность, (например, RSA)	<ul style="list-style-type: none"> • Дешифрование и/или взлом кода



P.N. Lebedev
Physical Institute

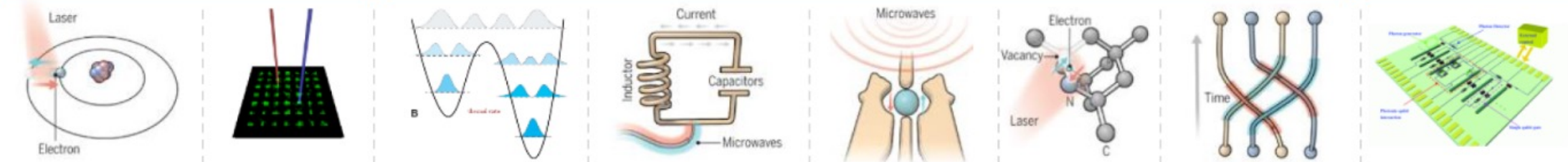
	Ионы	Нейтральные атомы	Сверхпроводники	Фотоны
Масштабируемость	Симуляторы - 53 кубита 1D-2D Вычислители - 11 кубит (попарно связанных) [1,2]	Симуляторы – 51 кубит 1D-3D [5]	Вычислители - 72 кубита 1D-2D [9]	100 кубитов
Время когерентности	До 10 мин [3]	До 7 с [6]	До 320 мкс [10]	«бесконечное»
Время срабатывания гейта	От 1 мкс	400 нс	10 нс	Менее 1 нс
Fidelity (достоверность)	99.996% один кубит [4] 99.9% два кубита [4]	99.6% один кубит [7] 97.4% два кубита [8]	99.92 % один кубит [11] 99.4% два кубита [11]	99,9 один кубит 99,9 два кубита*
R-фактор	До 10⁹	До 10⁷	До 10⁴	«бесконечное»

* Вероятностная модель – 10%

СВОДНАЯ ДИАГРАММА ОСНОВНЫХ РАЗРАБОТЧИКОВ И ПРОИЗВОДИТЕЛЕЙ КВАНТОВЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ



атомы	электроны <i>сверхпроводниковые контуры и управляемые спины</i>	фотоны
-------	---	--------



производители



лаборатории



ПРОГНОЗИРУЕМЫЕ СРОКИ СОЗДАНИЯ КВАНТОВЫХ КОМПЬЮТЕРОВ ОТ ЛИДИРУЮЩИХ КОМПАНИЙ



№	компания	Тип кубита	Срок создания КвК
1	IBM	сверхпроводники	Сегодня: 137 кубитов Начало 2022: 433 кубитов “Osprey”; Конец 2023 - 1121 кубитов “Condor”
3	Google	сверхпроводники	Квантовый компьютер с кодами коррекции ошибок, способный выполнять полезные вычисления, будет построен к 2029г.
4	IONQ	ионы	Прогнозируемый квантовый объем - 4 млн. 2023 год – демонстрация полномасштабного квантового превосходства. 2028 год – 1024 алгоритмических кубита
4	Honeywell	ионы	2021г. -квантовый объем 1024.
5	PsiQuantum	фотоны	2025г. - 1 млн. кубитов, 1000 логических кубитов
6	Xanadu	фотоны	1 млн. кубитов с исправлением ошибок (срок не указан)
7	Pascal	Нейтральные атомы (Rb)	1000 физических кубитов (без сроков)
8	QuERA	Нейтральные атомы	2021 г.- 256-512 физических кубитов; 2022 г. - полностью программируемый КвК с 64 кубитами 2024 – полностью программируемый КвК с 1024 кубитами.
9	D-Wave	Гибридная платформа: квантовый отжиг и сверхпроводниковые кубиты	2023-2024гг – 7000 кубитов



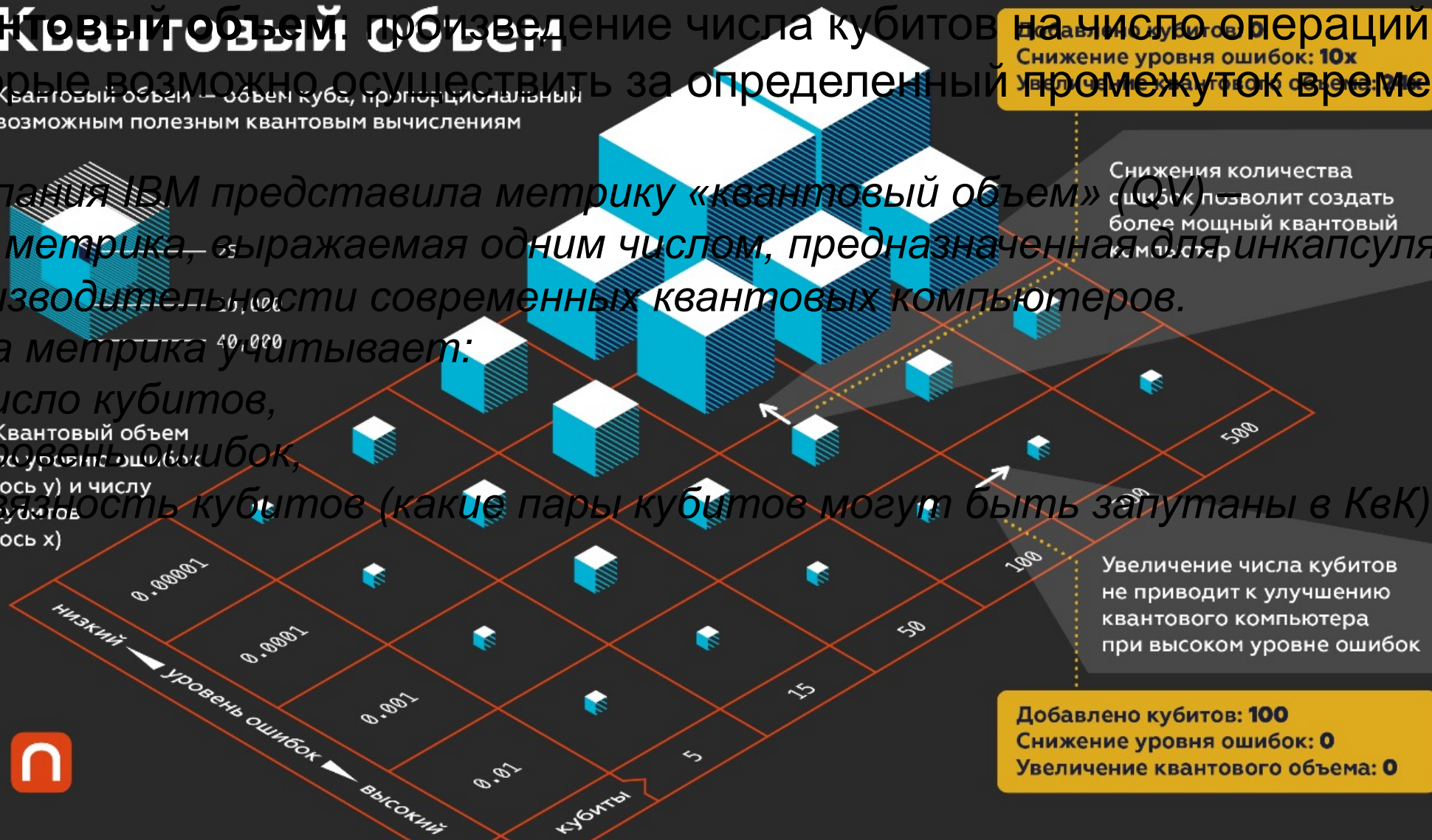
Квантовый объем — произведение числа кубитов, которые возможно осуществить за определенный промежуток времени, на число операций,

Квантовый объем — объем куба, пропорциональный возможным полезным квантовым вычислениям

Компания IBM представила метрику «квантовый объем» (QV) — это метрика, выражаемая одним числом, предназначенная для инкапсуляции производительности современных квантовых компьютеров.

Эта метрика учитывает:

- число кубитов,
- уровень ошибок (ось y) и число кубитов (ось x)
- связность кубитов (какие пары кубитов могут быть запутаны в КвК).

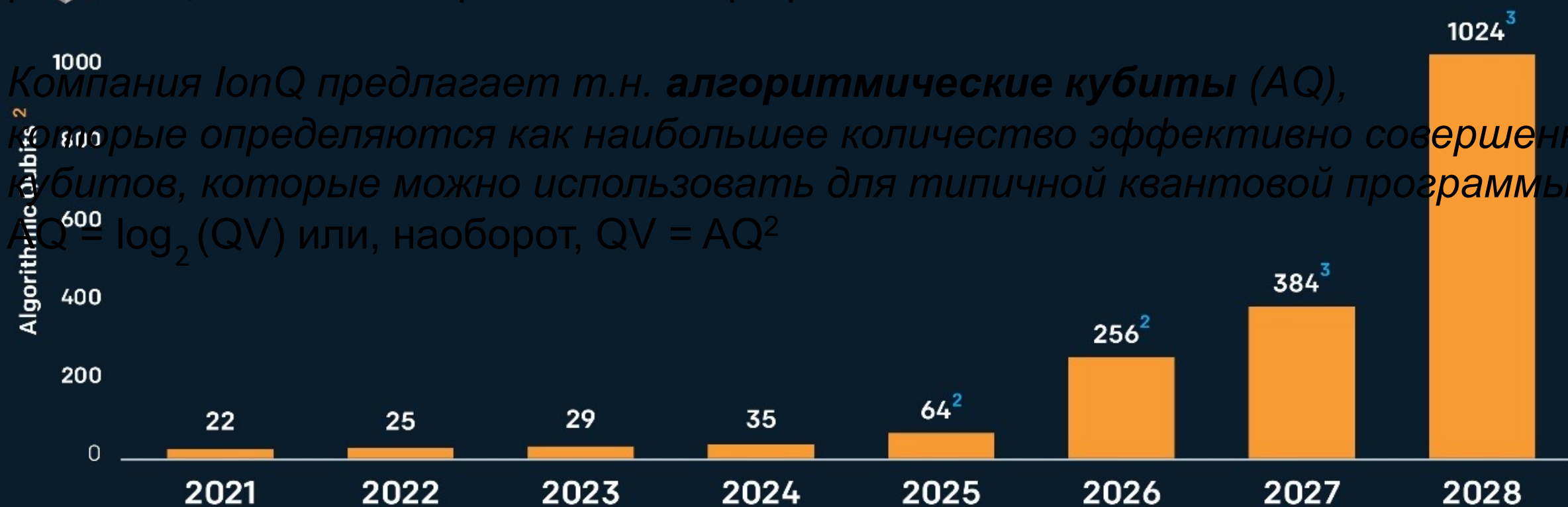




Платформа на основе ионов в ловушках Пауля - более высокая точность реализации гатов. Метрика QV быстро растет!

Компания IonQ предлагает т.н. **алгоритмические кубиты (AQ)**, которые определяются как наибольшее количество эффективно совершенных кубитов, которые можно использовать для типичной квантовой программы:

$$AQ = \log_2(QV) \text{ или, наоборот, } QV = AQ^2$$



¹ Algorithmic qubits defined as the effective number of qubits for typical algorithms, limited by the 2Q fidelity

² Employs 16:1 error-correction encoding

³ Employs 32:1 error-correction encoding

ОЦЕНКИ НЕОБХОДИМЫХ РЕСУРСОВ

(ЧИСЛА ЛОГИЧЕСКИХ КУБИТОВ, ЭЛЕМЕНТАРНЫХ КВАНТОВЫХ ВЕНТИЛЕЙ)

ДЛЯ ПОЛНОГО ПОИСКА КЛЮЧА ШИФРОВАНИЯ

ДЛЯ АЛГОРИТМА ШИФРОВАНИЯ AES С РАЗНОЙ ДЛИНОЙ КЛЮЧА*

*Для идеальных квантовых вентилей

длина ключа k	вентили		глубина схемы		число логических кубитов
	T	Клиффорд	T	всего	
128	$1.19 \cdot 2^{86}$	$1.55 \cdot 2^{86}$	$1.06 \cdot 2^{80}$	$1.16 \cdot 2^{81}$	2953
192	$1.81 \cdot 2^{118}$	$1.17 \cdot 2^{119}$	$1.21 \cdot 2^{112}$	$1.33 \cdot 2^{113}$	4449
256	$1.41 \cdot 2^{151}$	$1.83 \cdot 2^{151}$	$1.44 \cdot 2^{144}$	$1.57 \cdot 2^{145}$	6681

$$T\text{-gate} = \begin{pmatrix} 1 & 0 \\ 0 & \exp(i\pi/4) \end{pmatrix}$$

Клиффорд:

$$H = 1/\sqrt{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}; \quad S = \begin{pmatrix} 1 & 0 \\ 0 & \exp(i\pi/2) \end{pmatrix}; \quad CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \quad Y = \begin{pmatrix} 0 & -i \\ 1 & 0 \end{pmatrix}; \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Число логических кубитов, необходимых для взлома AES, составляет около 3000-7000

However, due to the large circuit depth of unrolling the entire Grover iteration, it seems challenging to implement this algorithm on an actual physical quantum computer, even if the gates are not error corrected!

Однако из-за большой глубины схемы развертывания всей итерации Гровера, представляется сложным реализовать этот алгоритм на реальном физическом квантовом компьютере, даже при использовании идеальных вентилях (без коррекции ошибок)!

ДАННЫЕ АНАЛИЗА ДЛЯ ОПТИМИЗИРОВАННЫХ КВАНТОВЫХ АЛГОРИТМОВ ПОЛНОГО ПЕРЕБОРА КЛЮЧЕЙ ДЛЯ АЛГОРИТМА ШИФРОВАНИЯ AES С РАЗНОЙ ДЛИНОЙ КЛЮЧА ПРИ РАЗЛИЧНЫХ ВЕЛИЧИНАХ ВЕРОЯТНОСТИ ОШИБКИ НА ВЕНТИЛЬ

AES-128				оценки 2020			оценки 2021		
p_g	s_q	n_ℓ	n_p	s_q	n_ℓ	n_p	s_q	n_ℓ	n_p
10^{-3}	101.66	15265	7.17×10^8	98.95	10924	4.04×10^9	98.95	10924	4.04×10^9
10^{-5}	97.19	2545	1.77×10^6	94.2	7564	1.74×10^7	94.2	7564	1.74×10^7

AES-192				оценки 2020			оценки 2021		
p_g	s_q	n_ℓ	n_p	s_q	n_ℓ	n_p	s_q	n_ℓ	n_p
10^{-3}	137.39	163793	2.93×10^9	135.29	62156	1.12×10^{10}	135.29	62156	1.12×10^{10}
10^{-5}	132.81	23393	7.81×10^6	130.67	11756	6.53×10^7	130.67	11756	6.53×10^7

AES-256				оценки 2020			оценки 2021		
p_g	s_q	n_ℓ	n_p	s_q	n_ℓ	n_p	s_q	n_ℓ	n_p
10^{-3}	170.49	218465	6.56×10^9	167.67	63884	2.24×10^{10}	167.67	63884	2.24×10^{10}
10^{-5}	166.0	34865	1.61×10^7	163.82	13484	1.15×10^8	163.82	13484	1.15×10^8

Параметры: p_g вероятность ошибки на вентиль

n_ℓ число логических кубитов

n_p число физических кубитов

s_q параметр секретности 2^{s_q}

Научный Совет РАН «Квантовые технологии» (председатель академик Г.Я.Красников)

1. Фундаментальные проблемы квантовых коммуникаций (19 ноября 2020);
2. Квантовые вычисления (18 февраля 2021);
3. Квантовые сенсоры – 1 (1 апреля 2021);
4. Квантовые сенсоры -2 (29 апреля 2021);
5. Математические модели и методы в квантовых технологиях (30 июня 2022);
6. Экспертное обсуждение отчета о реализации дорожной карты «Квантовые вычисления» в 2020 г. (4 августа 2021);
7. Анализ состояния фундаментальных исследований в Российской Федерации в области разработки материалов для квантовых технологий (17 ноября 2021);
9. Методы создания запутанных состояний (23 декабря 2021);
10. Экспертное обсуждение отчета о реализации дорожной карты «Квантовые вычисления» в 2021 г. (12 мая 2022);
11. Квантовые материалы -1 (23 июня 2022).

ФПИ

1. «Гамак» (МГУ имени М.В.Ломоносова) 2014-2017;
2. «Лиман» (ВНИИА имени В.Л.Духова), 2017-2020;
3. «Фотон» (ФТИ имени А.Ф.Иоффе) 2018-2020;
4. «Прибой» (МГУ имени М.В.Ломоносова) 2018-2022.

РФФИ

РНФ

**Мин.науки и
ВО РФ**

**ГК Росатом
Дорожная карта по квантовым
вычислениям**

СП «КВАНТ»

ООО «МЦКТ»

ЦКТ (МГУ имени М.В.Ломоносова),
ФИАН имени П.Н.Лебедева,
ФТИ имени А.Ф.Иоффе, МИСиС,
ИФМ РАН, СКОЛТЕХ, МФТИ, МПГУ, ВШЭ



- 1. В области квантовых вычислений**, речь идет о создании в ближайшие 5 лет среднemasштабных вычислителей, способных продемонстрировать «квантовое преимущество» перед классическими суперкомпьютерами в ряде задач. Практическая ценность этих задач - под вопросом.
- 2. В настоящее время идет интенсивная борьба с декогерентизацией – параллельно с наращиванием числа физических кубитов – в парадигме эры NISQ (без кодов коррекции ошибок).**
- 3. Выход за пределы «эры» NISQ** прогнозируется к 2030 году – на основе сверхпроводников, фотонов, ионов и фотонных чипов*.
- 4. Работы ведутся примерно в десятке организаций (университеты, РАН) при определяющем финансировании со стороны ГК Росатом.**

* Эти сроки постоянно сдвигались из-за непредвиденных технических препятствий

ВМЕСТО ПОСЛЕСЛОВИЯ: меньше хайпа*!

«Два года назад, подключаясь к деятельности в области квантовых вычислений, мы говорили о том, что отстаем на семь-десять лет от стран, вступивших в квантовую гонку раньше нас. Сейчас уже можно сказать, что по некоторым направлениям мы входим в тройку лидеров».
Екатерина Солнцева, саммит деловых кругов «Сильная Россия – 2022»:

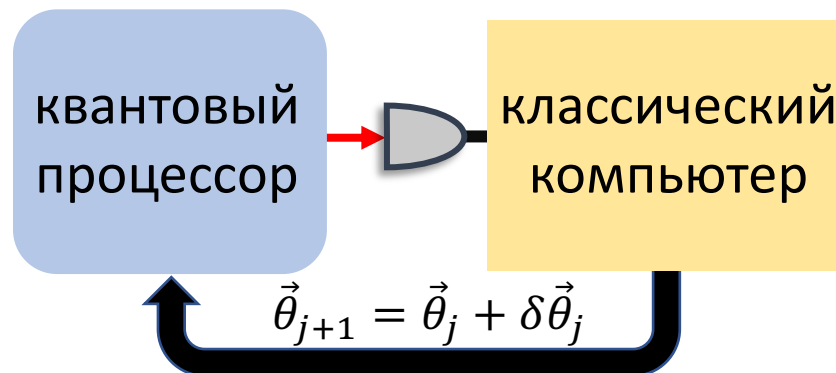
«Фактически «Росатом» сконцентрировал всю активность по квантовым вычислениям в нашей стране, за редким исключением. Отдельные исследования и разработки ведутся, но шансов на их успешное завершение, прямо скажем, немного, так как работы по теме квантовых вычислений требуют огромных по меркам ученых ресурсов, во всех смыслах этого слова»

Руслан Юнусов, клуб экспертов, Будет ли российский квантовый компьютер?
<https://www.bytemag.ru/articles/detail.php?ID=46170>. 04.08.2022

Хайп (от англ. *hype* — «шумиха») — агрессивная и навязчивая реклама, целью которой является формирование предпочтений потребителя. Название её происходит от слова, означающего надувательство, обман или трюк для привлечения внимания.

СПАСИБО ЗА ВНИМАНИЕ!

Квантовое химическое моделирование



Гамильтониан молекулы:

$$\hat{H} = \sum_{pq} h_{pq} \hat{a}_p^+ \hat{a}_q + \frac{1}{2} \sum_{pqrs} h_{pqrs} \hat{a}_p^+ \hat{a}_q^+ \hat{a}_r \hat{a}_s = \sum_{\alpha} g_{\alpha} \hat{H}_{\alpha}$$

h_{pq}, h_{pqrs} легко рассчитываются на классическом компьютере

$\langle \hat{a}_p^+ \hat{a}_q \rangle, \langle \hat{a}_p^+ \hat{a}_q^+ \hat{a}_r \hat{a}_s \rangle$ рассчитывают на квантовом процессоре

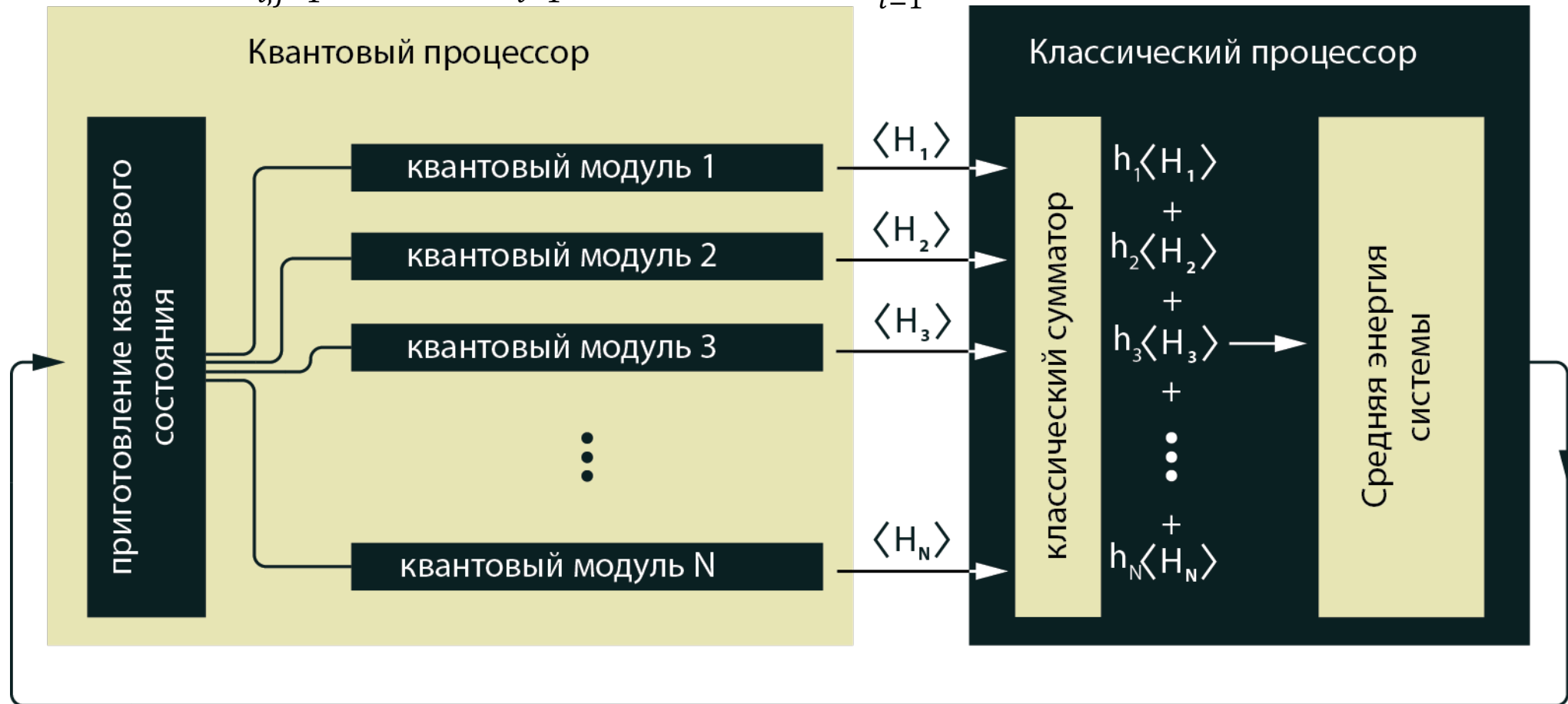
Приготавливаем анзац: $|\psi(\vec{\theta})\rangle$, находим минимум: $E(\vec{\theta}) = \sum_j h_j \langle \psi(\vec{\theta}) | \prod_i \hat{Z}_i^j | \psi(\vec{\theta}) \rangle$

Реализация вариационного алгоритма вычисления собственной энергии

H – гамильтониан исследуемой системы (H_2 и HeH^+)

$$H = \sum_{i,j=1}^4 h_{ij} \sigma_i \otimes \sigma_j = \sum_{i=1}^9 H_i$$

$$\langle H \rangle = \sum_{i=1}^9 \langle H_i \rangle - \text{оптимизируемая функция}$$



Классическая оптимизация параметров входного состояния

