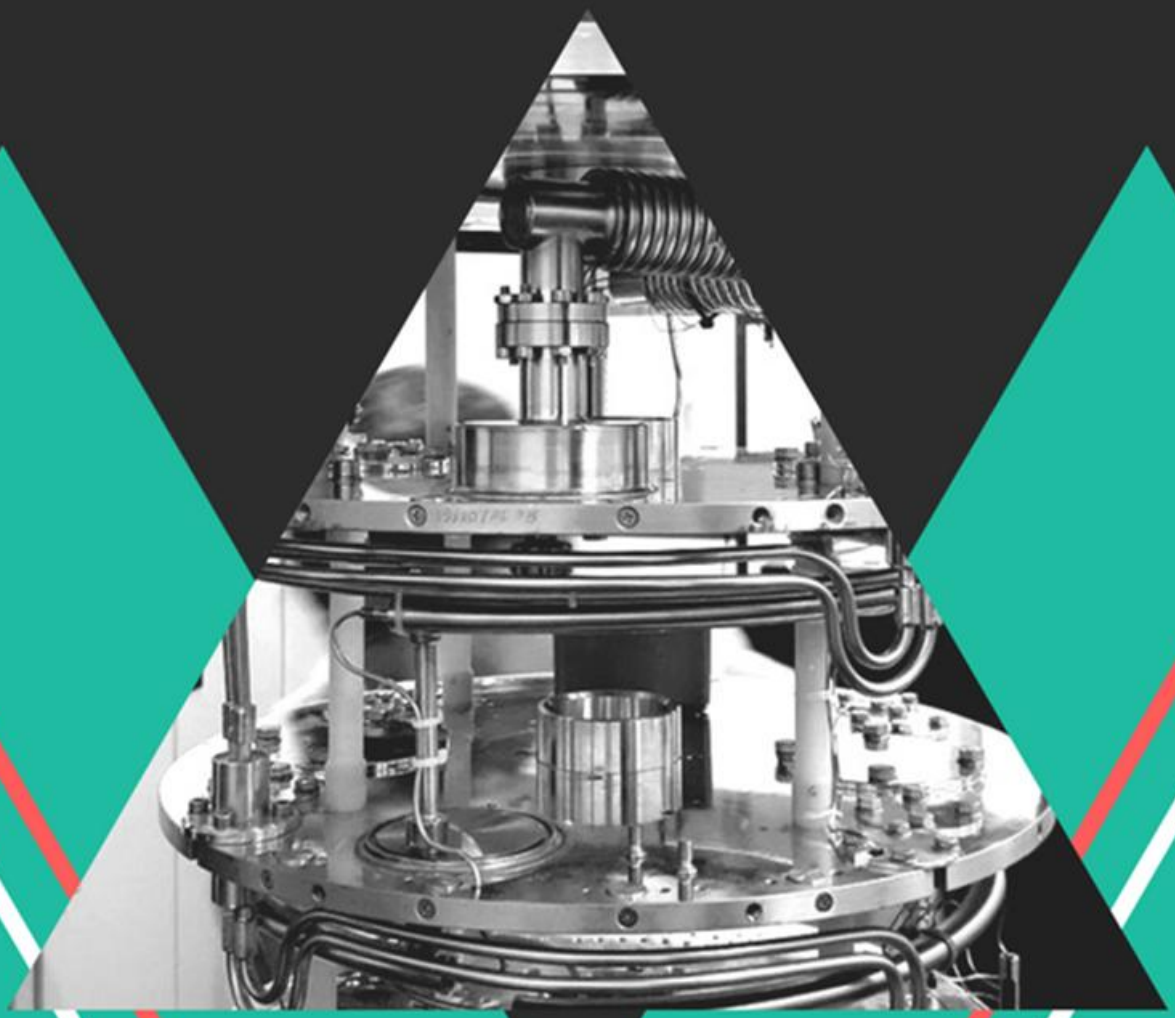
QILIMANJARO

A PRÓXIMA GERAÇÃO DA COMPUTAÇÃO



QILIMANJARO

Computação Quântica na ponta dos seus dedos

Maio 2018

Versão 1.5.

Resumo

A computação quântica não é mais um sonho distante. As realizações impressionantes no campo transformaram, nos últimos anos, uma busca acadêmica em uma realidade comercial iminente, onde os computadores clássicos serão superados em tarefas selecionadas, mas extremamente relevantes. Estamos testemunhando o nascimento de uma revolução tecnológica que irá remodelar nossa sociedade na qual a computação quântica é central. Atualmente, várias corporações gigantescas, incluindo Google, IBM, D-Wave, Rigetti e Microsoft, estão perseguindo ferozmente a construção de um computador quântico operacional.

O Qilimanjaro quer abrir o mundo da computação quântica para todas as empresas e indivíduos, sem a necessidade de comprar um computador quântico ou fazer parcerias dispendiosas com grandes participantes na corrida da computação quântica.

Nossa visão é construir uma plataforma de computação quântica disponível para a maioria dos usuários, incluindo indivíduos e corporações, e dessa maneira fornecer acesso a novos paradigmas da computação quântica com a mais transformadora de todas as tecnologias quânticas, a um custo acessível.

Conteúdo

1. Introdução

1.1. Tecnologias Quânticas em poucas palavras

A Ciência Quântica chegou ao ponto em que a manipulação de sistemas quânticos individuais, como átomos e fótons, é bem compreendida e está sob rígido controle. Conquistas recentes abrem a possibilidade de preparar, comunicar e processar informações em um nível fundamental seguindo as leis da mecânica quântica. Tal campo emergente atende pelo nome de Informação Quântica. A busca por implementações práticas da Informação Quântica levou, nos últimos anos, ao conceito de Tecnologias Quânticas.

A Comissão Européia propôs uma organização mais apurada das tecnologias quânticas em quatro áreas (veja o relatório final do comitê de alto nível de peritos [1]):

- Metrologia Quântica. Sensores quânticos para áreas de aplicação específicas, como imagens, saúde, geociências, etc.
- Comunicação Quântica. Desenvolvimento de dispositivos de rede, aplicações e sistemas de última geração para redes mesh de comunicação quântica.
- Simulação Quântica. Desenvolvimento de demonstradores operacionais, baseados em plataformas físicas existentes.
- Computação Quântica. Desenvolvimento de sistemas abertos e plataformas experimentais de computadores quânticos.

Abaixo, expomos essas quatro áreas em mais detalhes.

1.1.1. Metrologia Quântica

Novos sensores quânticos permitem realizar medições com uma incrível precisão, por exemplo: campos gravitacionais, acelerações ou campos magnéticos. Existem novas

empresas, como a Muquans na França, que oferecem dispositivos comerciais baseados em novas idéias em torno da detecção quântica.

Outros sensores quânticos concentram-se na área das ciências da vida para visualizar partes de nossos corpos com precisão sem precedentes. O exemplo prototípico é o centro de vazio do nitrogênio no diamante, com propriedades quânticas muito ricas que poderiam eventualmente substituir a atual tecnologia de ressonância magnética convencionalmente usada em hospitais.

1.1.2. Comunicação Quântica

A comunicação quântica visa tornar comprovadamente seguras todas as comunicações, explorando o fato de que os bisbilhoteiros inevitavelmente modificarão a mensagem que estão interceptando.

Na comunicação quântica, um dos aspectos mais intrigantes da mecânica quântica é empregado como recurso-chave: entrelaçamento quântico. Aqui, pares de fótons são gerados simultaneamente em um estado emaranhado, que é o único estado quântico que é compartilhado entre seus dois constituintes. Contra-intuitivamente, esta existência geminada continua, mesmo quando as partículas são separadas por grandes distâncias: uma modificação do estado quântico de uma parte afetará inevitavelmente a outra.

Em agosto de 2017, pesquisadores chineses verificaram uma "ação fantasmagórica à distância", como disse o próprio Einstein [3], no espaço com o lançamento do satélite Micius. A equipe liderada pelo Prof. Jian Wei Pan conseguiu distribuir pares de fótons emaranhados em dois pontos separados por 1.200 km. Um experimento de acompanhamento alcançou uma comunicação intercontinental codificada com criptografia quântica [4]. Tal feito tecnológico notável é um passo significativo em direção ao objetivo de criar uma Internet quântica inatingível. O experimento do satélite é a base para produzir uma nova forma de rede de comunicação, na qual a informação é codificada pelos estados quânticos dos pares de fótons emaranhados, ao invés de seqüências de 0s e

1s. A enorme vantagem na segurança resulta da impossibilidade de um intruso medir o estado dos fótons sem perturbá-los, revelando assim sua presença.

A criptografia quântica é, de longe, a tecnologia quântica mais próxima do uso comercial. Uma empresa proeminente que desenvolveu a distribuição comercial de chaves quânticas é a IdQuantique [5], de Genebra.

1.1.3. Simulação Quântica

A mecânica quântica é muito difícil de simular em um computador clássico. O desafio está em capturar todos os possíveis estados quânticos permitidos em um dado sistema que poderia ser preenchido de uma só vez. Em outras palavras, um sistema de 50 bits quânticos já requer 250 bits clássicos de informação para armazenar todos os estados quânticos possíveis que o sistema pode visitar em uma dada evolução dinâmica. Computar tal evolução já não é possível com o maior supercomputador da Terra. Aqui está um exemplo verdadeiro de quando a mecânica quântica começa a se tornar realmente útil.

Uma versão menor de um computador quântico já pode simular outros sistemas quânticos de relevância significativa. Um simulador quântico é adequado para explorar uma vasta gama de sistemas físicos como transições de fase exóticas na física da matéria condensada, novos materiais, fertilizantes, drogas etc. Por exemplo, experimentos de prova de conceito em redes óticas já mostraram que átomos frios simulam o comportamento de elétrons em um material real. Esses experimentos permitiram a exploração de propriedades críticas de matéria artificial. Muitos físicos quânticos sustentam a opinião de que a simulação quântica é a maneira de empurrar a tecnologia para explorar o poder computacional da mecânica quântica como a primeira aplicação verdadeira dos processadores quânticos.

1.1.4. Computação Quântica

A computação quântica se destaca como o objetivo mais importante das tecnologias quânticas, devido às suas implicações econômicas e políticas. De fato, a computação quântica superará os computadores clássicos em tarefas selecionadas, mas extremamente relevantes. O exemplo mais notável é a possibilidade de quebrar os protocolos criptográficos utilizados atualmente, o RSA. As consequências dramáticas para a geopolítica da criação de tal computador quântico foram enfatizadas por H. Clinton no final de 2015, alegando que um projeto semelhante a Manhattan deveria ser posto em prática para os EUA ganharem uma vantagem tecnológica quântica sobre o mundo [6].

Mas o poder da computação quântica é muito mais do que uma ameaça à atual segurança global da informação. Um algoritmo quântico mais eficiente baseado em pesquisa e um algoritmo para resolver sistemas lineares de equações foram descobertos ao longo dos anos desde o início da computação quântica. Algoritmos quânticos mais recentes, adaptados aos dispositivos quânticos reais já em uso como plataformas de nuvem, usam métodos variacionais para calcular propriedades, como a energia de ligação de um sistema molecular. Além disso, muitos problemas de otimização podem ser bem adaptados para que um computador quântico encontre soluções de maneira mais rápida do que suas contrapartes clássicas.

1.2. Computadores Quânticos

Uma máquina que é capaz de processar informações com elementos constituintes que obedecem às leis da mecânica quântica é chamada de computador quântico. A idéia foi proposta pela primeira vez pelo ganhador do Prêmio Nobel, Richard P. Feynman [7]. Ele viu que a mecânica quântica era particularmente difícil de se simular em um computador clássico. Em retrospectiva, essa idéia acabou sendo o gatilho para a revolução da tecnologia quântica que estamos presenciando nos dias de hoje. Como solução, ele propôs o primeiro modelo teórico de um computador quântico. Portanto, determina-se

que uma máquina quântica é adequada para simular a si mesma. Desta forma, existem problemas em que as leis da mecânica quântica produzem uma vantagem computacional sobre as leis clássicas.

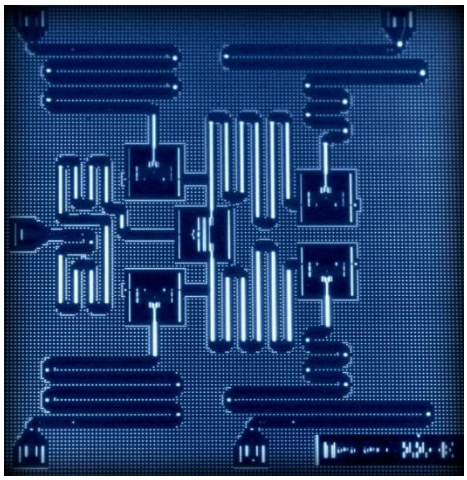
Dois tipos de computadores quânticos foram imaginados:

Computadores quânticos completos (universais): estes dispositivos são capazes de realizar portais quânticos arbitrários organizados em circuitos quânticos. Tais máquinas são conhecidas como computadores quânticos digitais.

Recozimentos quânticos: Esses dispositivos são capazes de encontrar uma boa solução para problemas de otimização. Tais máquinas são conhecidas como computadores quânticos analógicos.

O campo da computação quântica experimentou um progresso significativo nos últimos anos. Primeiro, o matemático Peter Shor produziu um algoritmo quântico para fatorar eficientemente grandes números [8]. A possibilidade de quebrar a criptografia atual foi, então, colocada na mesa. Mais tarde, I. Cirac e P. Zoller propuseram uma maneira explícita de implementar o CNOT de porta lógica em um sistema de armadilha de íons [9]. Esta proposta foi finalmente realizada pela equipe de R. Blatt, em Innsbruck [10]. A partir daí, uma explosão de propostas, provas de conceito e dispositivos reais que realizam computação quântica assumiram o campo da informação quântica.

O primeiro computador quântico em nuvem com 5 qubits foi lançado pela IBM no final de 2016. O sucesso dessa iniciativa é impressionante. Mais de 100.000 entusiastas quânticos registraram-se no site da experiência quântica da IBM e executaram seus próprios algoritmos quânticos [11]. Vários meses atrás, a IBM atualizou o computador quântico original para 16 qubits, o que aumentou o número de experimentos realizados por usuários remotos para 1,7 milhão. Esses números nos dão uma idéia aproximada da aceitação e abrangência que esse setor pode ter no futuro próximo.



O primeiro computador quântico na nuvem com 5 qubits. Os qubits podem ser identificados pelas áreas quadradas e mais escuras. As linhas wiggly são ressonadores usados para ler cada estado qubit individualmente, bem como fornecer interações qubit-qubit diretas, necessárias na implementação de portas quânticas de dois qubits.

Em uma linha de trabalho pronta para uso, os analisadores quânticos estão a caminho para resolver problemas de otimização. Recozimentos quânticos comerciais já estão sendo produzidos pela D-Wave Systems Inc [12]. O analisador quântico D-Wave tem sido empregado na solução do problema de coloração, analisando a otimização do fluxo de tráfego, computando pequenas moléculas e simulando materiais reais, entre vários outros problemas relevantes.

1.3. Computação Quântica

É fascinante pensar sobre o modo como a tecnologia evoluiu nos últimos anos. Hoje em dia, os smartphones têm o poder de computação de um computador militar de 50 anos atrás, que era do tamanho de uma sala inteira. John von Neumann, matemático e colaborador fundamental no desenvolvimento da computação, disse que mais de um computador em cada continente não seria necessário, enquanto hoje cerca de 2,3 bilhões de smartphones e 2 bilhões de computadores pessoais estão funcionando em todo o mundo. Vivemos em uma era da tecnologia, mas mesmo com os avanços fenomenais feitos com tecnologia e computadores clássicos desde o início da revolução do

computador, permanecem problemas que esses últimos simplesmente não conseguem resolver. Muitos acreditam que os computadores quânticos são o caminho a seguir.

1. 3. 1. Os limites dos computadores clássicos

O princípio que impulsionou a revolução da tecnologia da informação é a lei de Moore. Esta lei determina que a cada 18 a 24 meses, o número de transistores em um chip de microprocessador será dobrado para gerar o dobro de poder de processamento. Esse fato se traduz em transistores cada vez menores, a fim de continuar cumprindo a lei, tendência observada desde 1965, permitindo um rápido progresso tecnológico nas últimas quatro décadas.

Com um tamanho de chip menor e um número crescente de componentes, os dispositivos eletrônicos atualmente contêm milhões de transistores de até 7 nm (10 mil vezes mais finos que um fio de cabelo humano e apenas 20 vezes maior que alguns átomos). As dimensões do transistor podem continuar diminuindo com o tempo, no entanto, eles atingirão um limite físico onde os efeitos quânticos aparecerão e não haverá controle sobre o fluxo do sinal eletrônico.

Assim, a indústria de computadores é forçada a encontrar maneiras de melhorar a eficiência na computação, uma vez que já atingimos os limites da eficiência energética usando métodos clássicos. Os cientistas estão procurando novos métodos que exigem menos tempo e espaço para computar e armazenar dados. Veremos a indústria de dispositivos de varejo ainda melhorando ao longo do tempo, mas os campos corporativos, como o Big Data, encontraram um gargalo que é difícil de superar. Uma solução plausível para esse problema é a computação quântica.

Então, vamos deixar claro. Computação quântica não significa "abrir mais rápido um documento de texto do que um computador clássico". Estamos falando de habilidades diferentes. Problemas que exigem mais energia e tempo do que os supercomputadores

atuais podem acomodar. Problemas intratáveis. Esses são os problemas que os computadores quânticos estão previstos para atacar e resolver.

1. 3. 2. Os Princípios dos Computadores Quânticos

Os computadores convencionais operam com bits, que são limitados para obter um de dois valores, 0 ou 1. Eles representam dois estados e decisões sobre os dados que inserimos, seguindo um conjunto de instruções previamente combinado. Por contraste, os computadores quânticos operam com bits quânticos, ou qubits, que funcionam com a superposição de ambos os estados, ou seja, operam 0 e 1 simultaneamente. A superposição quântica torna a computação quântica um personagem especial com novas portas quânticas lógicas que, por sua vez, dão origem a novos algoritmos quânticos, contra-intuitivos e muito poderosos.

Pode parecer que os qubits são dotados de características mágicas, mas não são mágicos. Qubits seguem as leis físicas. Suas propriedades ocorrem "naturalmente", da mesma maneira que os pólos opostos de um ímã se atraem, ou a gravidade faz com que as massas caiam. A computação quântica se baseia em novas leis, novos fenômenos que podemos aproveitar.

Os Qubits exibem uma superposição quântica de opções clássicas. Como resultado dessa superposição, os computadores quânticos podem alcançar um enorme potencial de processamento em certas operações, sendo máquinas extremamente rápidas comparadas às suas contrapartes clássicas. Podemos pensar em um computador quântico como uma máquina massivamente paralelizada que é capaz de realizar muitas operações simultaneamente, tentando todas as soluções de um problema ao mesmo tempo. A beleza dos algoritmos quânticos verdadeiramente poderosos - que ao mesmo tempo é o que dificulta o encontra de novos - reside em poder se beneficiar desta computação paralela massiva para produzir o resultado desejado mais rapidamente do que o algoritmo existente mais conhecido.

Ao entrar neste reino quântico da computação, onde as leis clássicas da física não se aplicam mais, seremos capazes de criar computadores que empregam qubits, armazenando uma enorme quantidade de informação, sendo mais rápidos do que os computadores clássicos e consumindo menos energia.

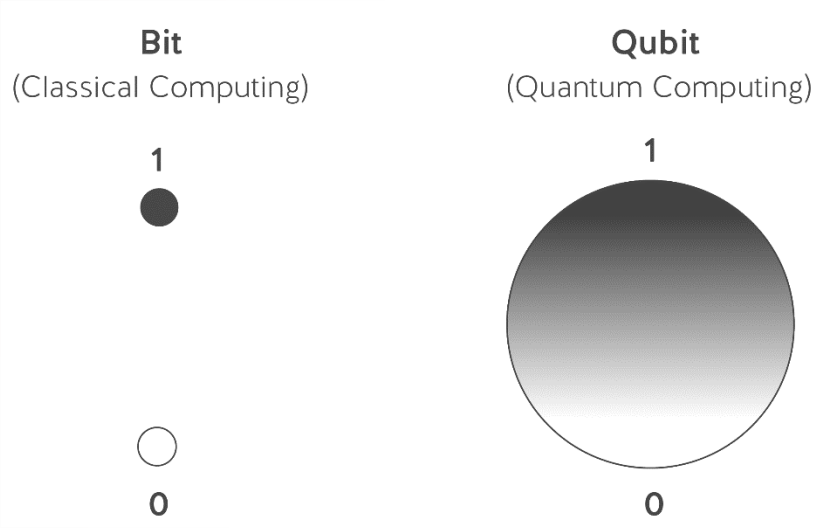


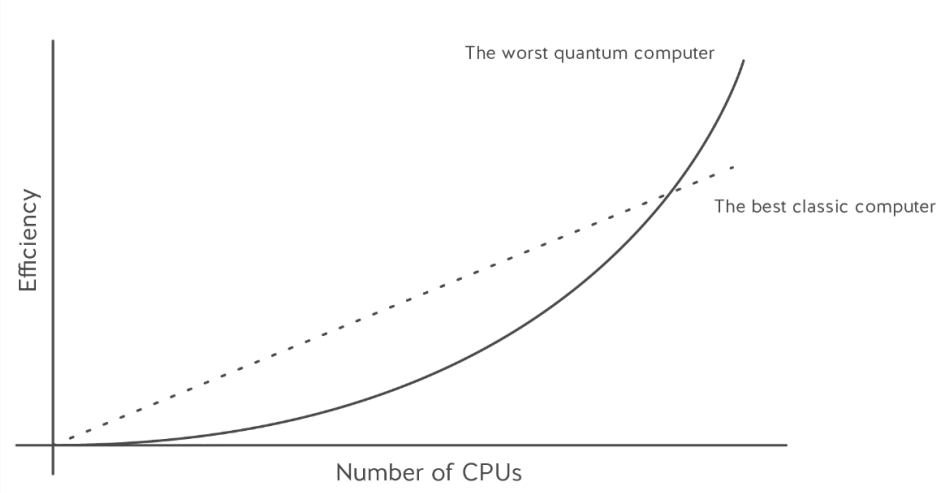
Ilustração da diferença entre bits e qubits. Imaginando uma esfera, um bit pode estar em qualquer um dos dois pólos da esfera, mas um qubit pode existir em qualquer ponto da superfície dela.

1. 3. 3. Poder da Computação Quântica

Usando bits clássicos, um registrador de três bits produziria oito possibilidades {000, 001, 010, 011, 100, 101, 110, 111}. Qualquer registro clássico só poderia ter um desses oito valores. Por outro lado, se tivermos um registrador de três qubits, o sistema carrega informações sobre os oito valores diferentes ao mesmo tempo, graças à superposição quântica. Assim, um registrador de três qubits permite operações em oito opções paralelamente. De fato, o número de operações realizadas é exponencial em relação ao número de qubits. Portanto, uma máquina quântica é mais ou menos poderosa dependendo do número de qubits. Com menos qubits, uma máquina quântica não poderia resolver problemas muito complexos, mas, com cada qubit adicional, duplicaria sua capacidade de processamento equivalente.

Vamos pegar alguns exemplos para tornar esse fato mais visual:

- Computador de 3 qubits: executa 8 opções em paralelo.
- Computador quântico de 5 ou 6 qubits: o computador executará 32 ou 64 opções em paralelo.
- Computador quântico de 30 qubits: executa tantas opções quanto as armazenadas em 134 MBytes.
- 50-qubit quantum computer: Here we are already talking about 300 TBytes of information. At this point, we are reaching the “quantum supremacy”. This concept has been proposed to represent the instant in which a quantum device is able to handle such an amount of registers that no single classical device on Earth can keep up with. A quantum computer with 50 qubits would be smaller, more powerful and more energy friendly than the best existing classical computer on Earth.
- Computador quântico de 50 qubits: Aqui já estamos falando de 300 TBytes de informação. Neste ponto, estamos atingindo a "supremacia quântica". Este conceito foi proposto para representar o instante em que um dispositivo quântico é capaz de lidar com uma quantidade tão grande de registros que nenhum dispositivo clássico na Terra pode acompanhar. Um computador quântico com 50 qubits seria menor, mais potente e mais ecológico do que o melhor computador clássico existente na Terra.



A linha sólida preta exponencial mostrada na figura mostra que os computadores quânticos podem duplicar sua capacidade de computação quântica com cada qubit adicional.

É provável que computadores quânticos se fundam com os computadores clássicos. Não precisamos usar um computador quântico para escrever um documento de texto ou executar uma planilha. Isso provavelmente seria bastante ineficiente. Computadores clássicos permanecerão em uso, da mesma forma que utilizamos lápis para escrever uma simples nota. Quando uma tarefa for muito pesada para um computador clássico, uma unidade de processamento quântico (QPU) assumirá o controle da CPU clássica. Esta é uma simbiose maravilhosa; Computadores clássicos e quânticos irão colaborar de forma transparente em uma plataforma híbrida para se tornar a mais poderosa máquina de computação já construída pela humanidade.

1. 3. 4. Consumo de Energia de Computadores Quânticos

Computadores quânticos oferecem uma vantagem computacional sobre os clássicos e, além disso, usam muito menos energia do que uma máquina clássica.

Vamos considerar o exemplo relevante de computadores quânticos baseados em circuitos supercondutores. Esses dispositivos precisam ficar em temperaturas muito baixas para ficarem operacionais, próximos a 0,01K (-273,14ºC). O procedimento de resfriamento requer um instrumento especial conhecido como refrigerador de diluição. Alcançar temperaturas tão baixas demanda uma certa quantidade de energia. Mas uma vez que a temperatura base é atingida, o computador quântico funciona perfeitamente, com um consumo de energia significativamente pequeno. A energia consumida para atingir as temperaturas mais baixas quase não dependerá do tamanho do computador quântico. Portanto, não há lei de escala verdadeira, ao contrário dos tradicionais processadores clássicos semicondutores.

É natural argumentar que computadores quânticos produzem duas vantagens: poder computacional e economia de energia. Este último não deve ser subestimado.

2. Economia da Tecnologia Quântica

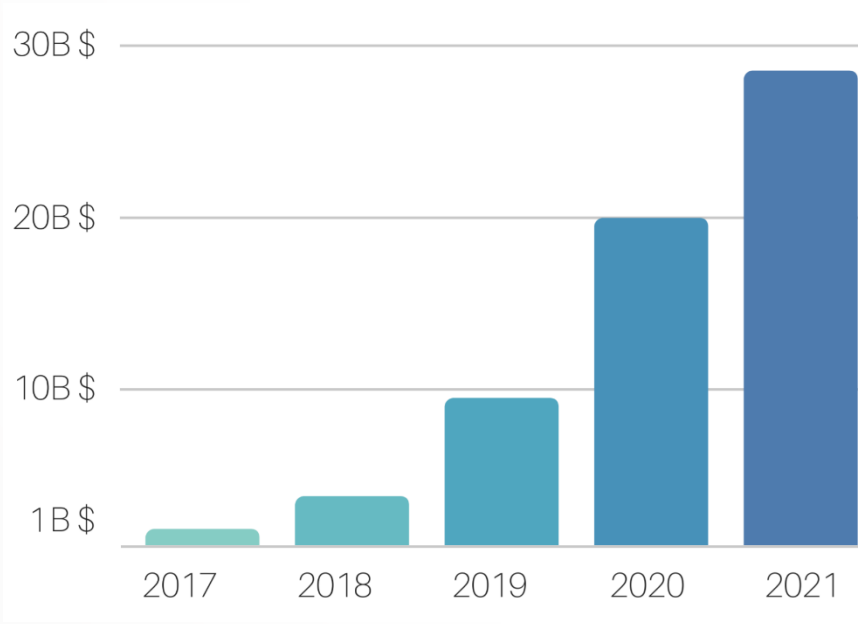
2.1. Oportunidade de Mercado

Grandes quantidades de recursos em todo o mundo (por outro lado, bilhões de dólares) são atualmente dedicados à informação quântica, provenientes principalmente do setor militar e empresas privadas nos EUA.

A União Europeia lançou recentemente uma nova iniciativa em tecnologias quânticas com o objetivo de investir 1 bilhão de euros nos próximos dez anos [13].

A China também está estabelecendo uma grande iniciativa para desenvolver tecnologias quânticas em Hefei, investindo cerca de 10 bilhões de dólares [14].

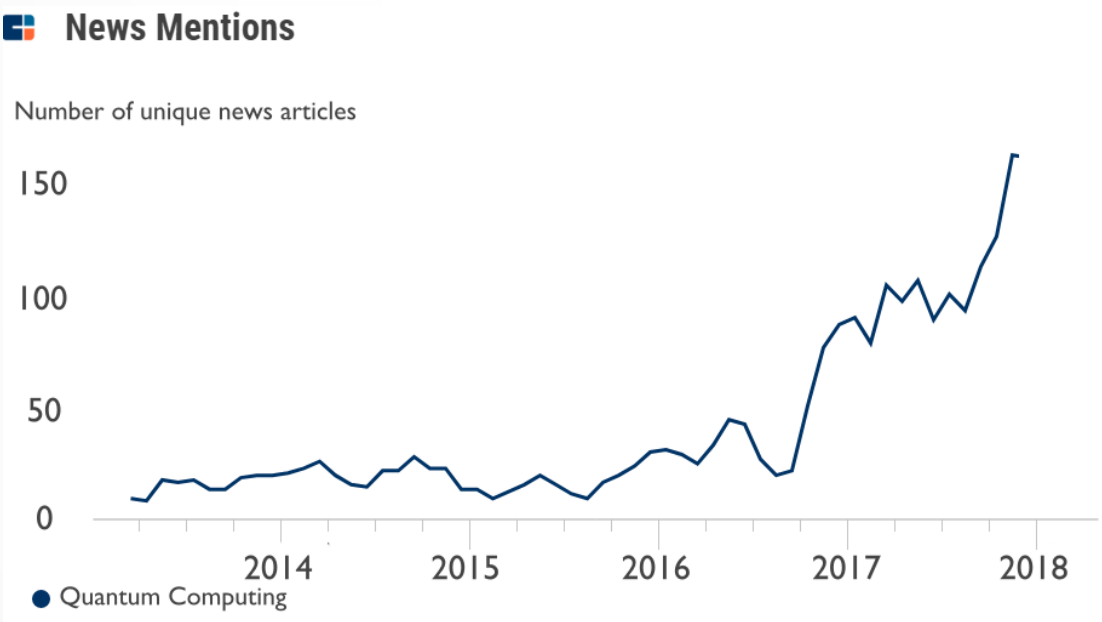
A Goldman Sachs projetou que a indústria de computação quântica poderia ser de US$ 29 bilhões até 2021 [15]. Considerando que esse campo pode atualmente ser avaliado em alguns bilhões de dólares, essa previsão estabelece um crescimento muito significativo e um alto ROI para seus primeiros investidores.



Análise do Goldman Sachs sobre o potencial da indústria da computação quântica.

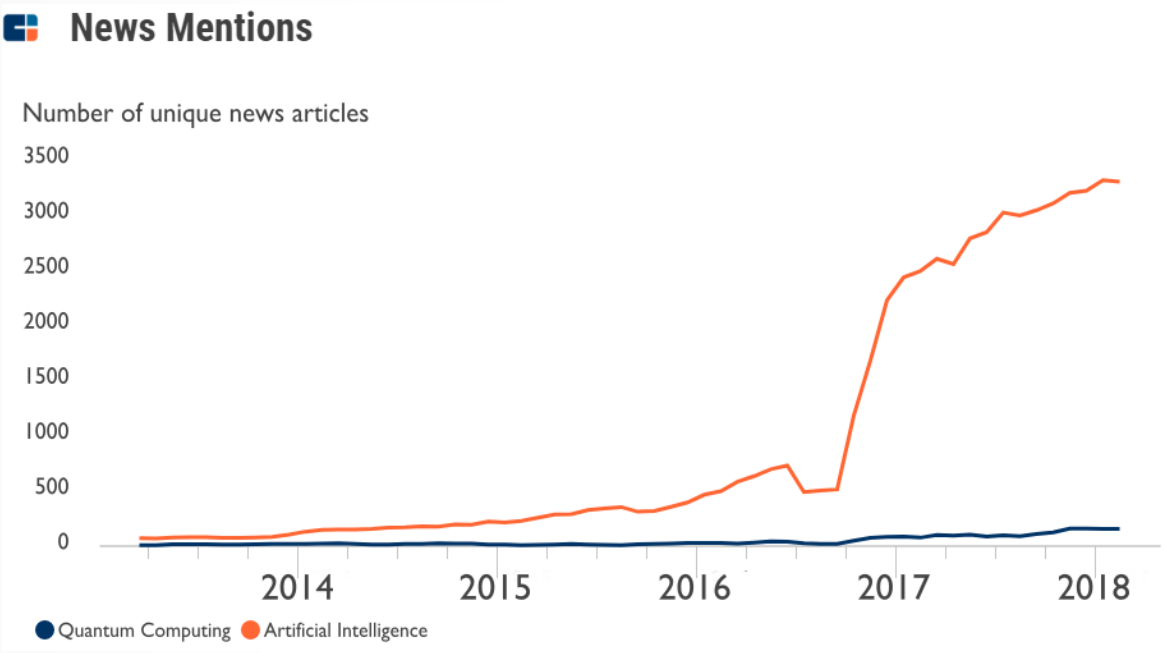
A computação quântica é uma área cada vez mais quente para pesquisa e investimento, com grandes corporações como IBM, Google ou Microsoft. Em conjunto com esses grandes investimentos empresariais, os governos da União Européia, EUA e China, entre outros, também estão apoiando projetos voltados à comercialização de computadores quânticos. Esses dados, juntamente com a análise de quanta atenção da mídia há na tecnologia quântica, podem nos dar uma idéia da atual oportunidade de mercado.

Assim, o Qilimanjaro realizou um estudo que quantifica a atenção da mídia para prever tendências tecnológicas quânticas. Esta análise é feita com a ferramenta New Mentions (Novas Menções) na plataforma CB Insights. É um software que analisa milhões de artigos de mídia para identificar e compreender programaticamente a taxa de adoção de tecnologias e inovações emergentes. A CB Insights New Mentions aplica o aprendizado de máquina a um corpus massivo de artigos de mídia para permitir um método em tempo real baseado em dados para descobrir, prever e plotar o arco de expectativas e entusiasmo pelas tecnologias emergentes.



O gráfico acima para o termo "computação quântica" destaca que a tecnologia é uma tendência cada vez mais comentada na mídia (a linha azul ascendente representa o

aumento no número de menções de mídia a partir de meados de 2015). No entanto, quando comparamos "Computação quântica" com uma tendência mais conhecida, por exemplo, "Inteligência artificial" (no segundo gráfico denotado pela linha laranja), é aparente que "computação quântica" é, na verdade, um jovem tendência tecnológica que ainda tem um longo caminho a percorrer.



Nosso estudo e os dados do CB Insights sugerem que o ecossistema geral que apóia o desenvolvimento dessas empresas ainda está surgindo. A aplicação comercial de computadores quânticos (tanto para hardware quanto para software) está nascendo neste momento. Isto implica que pode ser muito benéfico investir neste campo emergente nesta fase inicial.

Investigações científicas, processos de aprendizado de máquina, análise de dados, tudo isso requer lidar com grandes quantidades de informação. Um computador quântico com número suficiente de qubits, seria capaz de realizar tarefas de análise que são extremamente difíceis, se não impossíveis, com computadores comuns.

O potencial da computação quântica como uma nova tecnologia é grande e, no momento, estamos apenas testemunhando seus primeiros passos.

Nos próximos anos, os humanos estabelecerão as bases de uma nova era da tecnologia quântica com algoritmos que quebram os protocolos criptográficos atuais e minimizam o tempo necessário para resolver problemas difíceis de otimização. É um novo caminho na história da computação.

A Qilimanjaro quer fazer parte dessa revolução: ajudar a desenvolver a arquitetura desses sistemas, enriquecer o ecossistema e fornecer acesso ao grande potencial de um computador quântico.

2.2. Aplicações Quânticas para Negócios Reais

Como mencionado acima, os analisadores quânticos são um tipo particular de computadores quânticos analógicos especificamente projetados para encontrar o mínimo de uma determinada função de custo. Portanto, os analisadores quânticos são projetados e construídos para executar tarefas específicas. Um problema diferente pode ser resolvido por um projeto diferente de circuito de recozimento quântico. Por outro lado, os computadores quânticos universais digitais podem resolver qualquer tipo de problema. No entanto, a execução de computadores quânticos digitais requer uma correção quântica de erros, o que implica na adição de grandes quantidades de qubits auxiliares para executar operações redundantes. Ao todo, os computadores quânticos universais digitais precisam de milhões ou bilhões de qubits para operar com sucesso. Na prática, os analisadores quânticos podem resolver imediatamente os problemas que são de interesse prático e requerem números de qubit da ordem de 100. Desta forma, listamos alguns exemplos onde os computadores quânticos podem fornecer uma vantagem sobre os computadores clássicos:

- Química Quântica

Calcular a estrutura das moléculas é um problema computacionalmente difícil. Atualmente, a simulação clássica de química é limitada devido ao número exponencial de recursos computacionais necessários. Os computadores quânticos representam, então, uma

ferramenta nova e poderosa para lidar com problemas relacionados à compreensão de moléculas e ao design de novas drogas, fertilizantes, gases para capturar o carbono atmosférico, etc. [16].

- Problemas de otimização, como tráfego e agendamento

Uma das principais tarefas de um analisador quântico é poder otimizar qualquer tipo de problema de agendamento. Várias empresas já estão investigando os princípios do poder do recozimento quântico para resolver rotinas de otimização. A NASA desenvolveu um algoritmo quântico para lidar com problemas de programação (cheque NASA quantum initiative [17]). O problema de otimizar os fluxos de tráfego em Pequim [18] está sendo tratado pela Volkswagen junto com os sistemas D-Wave.

- Treinamento de redes neurais

A área de treinamento em redes neurais usando algoritmos clássicos já tem uma longa história em suas costas. Portanto, competir contra ela já requer processadores quânticos muito poderosos. O treinamento de redes neurais usando recozimento quântico só foi apresentado muito recentemente e, como tal, as idéias são apenas muito preliminares [19]. É concebível encontrar caminhos em problemas em particular, onde uma vantagem pode ser obtida usando um processador quântico no tempo necessário para treinar uma rede neural de um certo tamanho.

- Finança

O uso de recozimentos quânticos para resolver problemas em finanças pode permitir encontrar novas maneiras de realizar a modelagem de dados financeiros e, desse modo, isolar os fatores de risco. As implicações econômicas aqui são bastante importantes.

- Criptografia e segurança

Um computador quântico completo será capaz de realizar tarefas como a fatoração de grandes números. Isso coloca em risco todos os algoritmos criptográficos como RSA, DSA e EEC, uma vez que eles podem ser atacados usando uma eficiente Quantum Fourier Transform. Na verdade, a computação quântica é uma grande ameaça à política e

economia atuais, que fazem uso extensivo da criptografia baseada em RSA. Em um futuro não muito distante, a segurança será aprimorada pelo uso da criptografia quântica, que é robusta contra o ataque de um computador quântico.

A computação quântica é, portanto, capaz de acelerar o crescimento e o desenvolvimento de praticamente qualquer campo econômico que possa impactar.

2. 3. Cenário Atual de Computação Quântica

Atualmente, várias empresas estão buscando ferozmente a construção de um computador quântico completo.

O momento em que um dispositivo quântico puder realizar uma certa computação que não é reproduzível em um computador clássico foi denominado "Supremacia Quântica". Esse marco está previsto para meados de 2018, como afirma repetidamente John Martinis, líder da iniciativa de computação quântica do Google [20].

A lista dos principais competidores no campo da computação quântica inclui:

- IBM

A IBM lançou o primeiro computador em nuvem de 5 qubits que foi recentemente atualizado para 16 qubits. A IBM também anunciou um computador quântico de 20 qubits que não será mais aberto, nem gratuito. A IBM também divulgou seus esforços para operar um computador quântico de 50 qubits em meados de 2018.

- Google

O Google persegue várias estratégias de computação quântica em paralelo. Primeiro comprou uma máquina D-WAVE junto com a NASA. Mais tarde, financiou um grande grupo liderado por John Martinis, ex-professor da UCSB. O Google afirma que alcançará a supremacia quântica em 2018, com um processador quântico de alta qualidade e mais de 50 qubits. O Google está enfatizando a necessidade de qualidade dos portais quânticos,

ou seja, o desempenho de alta fidelidade para cada porta quântica. O Google também anunciou uma iniciativa para construir um analisador quântico próprio.

- Rigetti

Chad Rigetti, ex-funcionário da IBM, fundou uma empresa com sede no Vale do Silício, em homenagem a ele, que arrecadou 65 M $ de capital de risco. Esta startup apresenta-se como uma empresa full-stacked, fornecendo serviços em computação quântica e software quântico. A Rigetti Computing abriu recentemente um computador quântico de 19 qubits com acesso seletivo à nuvem.

- Microsoft

A Microsoft optou por um tipo diferente de qubits, os chamados quatros Majorana. A Microsoft anunciou uma solução de computação quântica full-stack.

A IBM, o Google e a Rigetti empregam qubits supercondutores em seus computadores quânticos. Esses qubits são idealmente projetados para oferecer tempos de coerência muito altos, nomeados de transbits qubits [21]. Todas essas máquinas têm dimensões de 20 a 50 qubits e receberam investimentos da ordem de 50-200 milhões de dólares. A IonQ [22] é outra startup de computação quântica baseada na tecnologia de ion traps. A empresa ainda não divulgou informações relevantes sobre seu progresso.

Uma série de analisadores quânticos foi construída pela empresa canadense D-Wave. Seu dispositivo mais avançado exibe um chip de 2048 qubits. O desempenho quântico deste dispositivo foi debatido devido aos tempos curtos e coerentes dos qubits usados. As máquinas D-Wave foram vendidas ou compartilhadas com fins de pesquisa para vários clientes que incluem a Lockheed Martin, a NASA, Los Alamos Laboratory, Oak Ridge, The Quantum Artificial Intelligence Lab, USC Information Sciences Institute, Temporal Defense Systems, Airbus e Volkswagen.

As empresas que atualmente trabalham com essa tecnologia fizeram grandes progressos nos últimos anos. Seus computadores quânticos provavelmente serão usados no mercado corporativo.

3. Qilimanjaro

3.1. Proposta de Valor

Atualmente, há grande entusiasmo em desenvolver computadores quânticos funcionais, com os esforços significativos feitos tanto na academia quanto na indústria. Grandes empresas da alta tecnologia, como IBM, Google, Intel e Microsoft, assim como várias empresas iniciantes (sendo a Rigetti uma das maiores), estão progredindo e lançando as bases da computação quântica experimental. As tecnologias de computação quântica representam uma indústria próspera e crescente, mas para muitos usuários em potencial, existe uma barreira de acessibilidade para sistemas centralizados. Atualmente existe uma competição para alcançar a Supremacia Quântica, para tornar os componentes e softwares proprietários, e patentear possíveis implementações de algoritmos quânticos.

O Qilimanjaro é um projeto que visa abrir o mundo da computação quântica para todas as empresas e indivíduos, sem a necessidade de adquirir um computador quântico caro, nem estar matriculado em uma determinada universidade ou programa, ou fazer parcerias dispendiosas com grandes players da indústria de computação quântica. Em particular, nosso projeto gira em torno dos seguintes pilares:

- Criar um computador quântico acessível
- Fornecer um serviço de software de tradução, adaptando problemas clássicos em algoritmos quânticos
- Prosseguir com o desenvolvimento de uma linguagem de computação quântica de código aberto universal (Qibo)

- Criar uma comunidade de usuários onde as contribuições são recompensadas, com o objetivo de capacitar o atual ecossistema de software quântico.

O Qilimanjaro é estruturado em duas equipes

- Serviços de Computação do Qilimanjaro(QCS).
- Serviços de Software Qilimanjaro(QSS).

Cada equipe tem objetivos diferentes para impulsionar o progresso e suprir uma necessidade no mercado atual. A tabela a seguir resume estes objetivos:

<table>
<tr><th></th><th>Objetivo</th><th>Produto/Serviço</th><th colspan="2">Especificações</th></tr>
<tr><td rowspan="5">Serviços de Computação do Qilimanjaro (QCS)</td><td rowspan="5">Construir Computadores Quânticos</td><td rowspan="4">Analisador Quântico Qilimanjaro</td><td>Estágio 1: 5 qubits</td><td rowspan="4">Serviço de computação quântica em nuvem, fornecendo acesso a usuários interessados em explorar o processamento de informações quânticas.</td></tr>
<tr><td>Estágio 2: 10 qubits</td></tr>
<tr><td>Estágio 3: 50 qubits</td></tr>
<tr><td>Estágio 4: >100 qubits</td></tr>
<tr><td>Pesquisa</td><td colspan="2">Desenvolvimento de tecnologia de recozimento quântico para computadores quânticos universais.</td></tr>
<tr><td rowspan="2">Serviços de Software Qilimanjaro(QSS).</td><td rowspan="2">Serviços de desenvolvimento e avaliação de software</td><td>Consultoria</td><td colspan="2">Ajudar os usuários a adaptar os problemas em uma arquitetura de computação quântica, escrever código para executar problemas na lógica quântica, executar o algoritmo no computador quântico do Qilimanjaro.</td></tr>
<tr><td>Qibo</td><td colspan="2">Linguagem quântica de código aberto universal, projetada para operar qualquer computador</td></tr>
</table>

			quântico on-line existente (por exemplo: IMB, D-Waves, IonQ ..).
		Comunidade	Fazer crrescer uma comunidade de código aberto quântica sólida. Aprimorar o desenvolvimento de bibliotecas Qibo. Acelerar a pesquisa sobre algoritmos quânticos utilizáveis.

3. 2. Serviço de Computação do Qilimanjaro (QCS)

Permitir o acesso remoto a computadores quânticos através de um serviço em nuvem é um fator crucial hoje em dia para ser competitivo. Uma comunidade mais ampla de usuários crescerá à medida que mais plataformas de computação quântica se tornarem disponíveis on-line.

A equipe de Serviços de Computação do Qilimanjaro (QSC) se concentrará na construção de um analisador quântico baseado em qubits coerentes para ser acessado por meio de uma plataforma baseada em nuvem, conforme detalhado na Seção 3.3. O analsador quântico permitirá que indivíduos e empresas explorem as possibilidades da computação quântica a um preço baixo.

A equipe do QCS desenvolverá uma interface simples e amigável, oferecendo aos usuários externos recursos de edição para criar programas personalizados. O editor on-line contará com um conjunto de ferramentas para compilar algoritmos quânticos a serem agrupados na plataforma de computadores quânticos on-line. Uma máquina virtual baseada no Qibo permitirá que os usuários testem seus programas em condições reais simuladas antes de testar o dispositivo real.

3. 2. 1. Localização do Laboratório e Infraestrutura

A equipe de cientistas do Qilimanjaro tem feito uma pesquisa pioneira em Informação Quântica por mais de dez anos, com um progresso constante tanto no desenvolvimento de algoritmos quânticos quanto na construção de dispositivos quânticos. Até agora, a equipe desenvolveu sua pesquisa no ambiente acadêmico. Ao longo de suas carreiras, os cientistas envolvidos com o Qilimanjaro trabalharam em diferentes universidades que incluem: Universitat de Barcelona (Espanha), MIT (EUA), Niels Bohr Institute (Dinamarca), CQT (Cingapura), Stony Brook (EUA), ICN2 (Espanha) e BSC (Espanha).

Embora uma parte da pesquisa científica básica ainda esteja relacionada a instituições públicas, o Qilimanjaro instalará seu laboratório em instalações de última geração na área de Barcelona, na Espanha.

As estreitas relações com a comunidade de pesquisa em todo o mundo permanecerão fundamentais para o progresso do Qilimanjaro.

3. 2. 2. Melhorias técnicas no Analisador Técnico do Qilimanjaro

O desafio de "industrializar" a tecnologia de computação quântica é produzir dispositivos quânticos confiáveis. Assim como na computação clássica, o projeto de computadores quânticos precisa garantir que o processador quântico siga as instruções que programamos nos algoritmos quânticos. Quando falamos de qubits, isso é particularmente difícil, já que seu estado quântico é propenso a erros causados por seu ambiente flutuante (campos magnéticos e elétricos, ruído de contradores eletrônicos, flutuações de temperatura, vibrações, interferência acústica, infravermelho, radiação de microondas, etc.). O modelo de computação quântica baseado em gate é muito sensível a esses erros, exigindo protocolos de correção de erro quântico (QEC) para funcionar da forma mais eficiente possível. Mas o QEC tem um alto custo: qubits auxiliares, o que implica que, para

operar um computador quântico baseado em gate, são necessários milhões de qubits para realizar operações de maneira confiável.

Por outro lado, os computadores quânticos analógicos são um pouco mais robustos do que os computadores quânticos baseados em gate. O modo de operação de um computador quântico analógico é permitir que o sistema evolua livremente sob seus próprios parâmetros. A desvantagem é a não-universalidade: um único computador quântico analógico não pode, a princípio, resolver todos os problemas possíveis que um computador quântico deve ser capaz de resolver. A robustez contra o ruído do qubit ainda é um forte ponto favorável para fazer dos computadores quânticos analógicos o candidato natural para se tornarem os primeiros computadores quânticos comerciais, como está provando a empresa canadense D-Wave. De fato, existe uma receita para transformar um computador quântico analógico em um computador quântico universal, e parte do roteiro do Qilimanjaro é apontar os desenvolvimentos para essa direção.

Analisadores quânticos são um tipo particular de computador quântico analógico. O projeto Qilimanjaro quer se distinguir de outras plataformas de recozimento quântico, particularmente a D-Wave, produzindo qubits que são bem protegidos de seu ambiente com ruídos. Tais qubits mostram coerência quântica, o que, em termos simples, significa que seu comportamento é governado pelas leis dos sistemas quânticos isolados, e não por seu ambiente ruidoso. O computador QCS pode, assim, ser referido como um analisador quântico coerente. Outro importante aspecto distintivo entre os analisadores quânticos é a rede de conectividade qubit. Quanto mais conectado um dado qubit ao resto dos qubits está, mais difícil é simular através de um computador clássico, o que significa que problemas mais difíceis podem ser implementados e resolvidos em um analisador quântico, que não seria executado em um dispositivo clássico.

É importante destacar as diferenças entre o Analisador Quântico Qilimanjaro (QQA) e os analisadores quânticos construídos pela D-Wave. A tabela a seguir apresenta detalhes específicos entre os dois sistemas.

	D-Wave	QCS
Tipo de qubits	Sendo um primeiro jogador no campo, o D-Wave usava um circuito tradicionalmente conhecido como rf-SQUID. Este tipo de qubits está entre a versão mais simples de um qubit. O que é realmente problemático é que eles exibem tempos coerentes muito curtos, particularmente com o processo industrial usado pelo D-Wave para fabricá-los. O baixo nível de coerência exibido pelos rf-SQUIDs é um ponto fraco para o D-Wave. Muitos cientistas debateram o poder real das máquinas D-Wave, enfatizando que qualquer vantagem computacional é difícil de provar [23]. O D-Wave merece reconhecimento por ser o primeiro dispositivo quântico usado para resolver problemas de relevância para os negócios.	O QCS irá trabalhar com um tipo diferente de qubits, chamado de qubits de fluxo de corrente persistente, ou simplesmente qubits de fluxo [24]. Esses tipos de qubits exibem longos tempos de coerência, mais longos do que o tempo normal para executar um determinado protocolo de computação. É importante entender que os longos tempos de coerência são críticos para um computador quântico exibir efeitos quânticos genuínos, ou seja, experimentando uma aceleração quântica e potencialmente muito mais poderosa do que suas contrapartes clássicas. A ausência de coerência transforma qualquer dispositivo efetivamente em um clássico, que é a principal falha que o Qilimanjaro quer evitar.
Connectivity architecture of the machine	Atualmente, o D-Wave usa a chamada arquitetura quimera, baseada em conjuntos altamente conectados de qubits que são, então, mal conectados a outros conjuntos. Tem sido defendido que a conectividade total não é possível com a tecnologia atual. Novas idéias relacionadas a arquiteturas 3D estão sendo consideradas.	O QCS irá optar por um nível misto de arquitetura, relaxando a conectividade local em favor do acoplamentos de longo alcance. Isso é necessário para enfrentar os desafios computacionais do mundo real.

3. 2. 3. Objetivos Técnicos do QCS

O QCS visa construir 4 computadores quânticos com diferentes objetivos específicos:

- *Analisador Quântico Qilimanjaro*: Este computador é o primeiro objetivo principal do Qilimanjaro. O computador hospedará nossa plataforma em nuvem, o OpenQ, a partir da qual os usuários remotos terão acesso ao poder computacional de um processador quântico.

- *Qilimanjaro Twins*: Dois processadores quânticos adicionais estarão focados na melhoria da tecnologia de recozimento quântico, na qualidade deo qubit, conectividade de rede do qubit e, mais importante, aprimoramento da complexidade do circuito quântico em direção à computação quântica universal. Assim, esses computadores são planejados como dispositivos de pesquisa para melhorar a tecnologia a ser fornecida no Analisador Quântico Qilimanjaro.

- *Qilimanjaro Threelean*: Os objetivos do quarto processador quântico são a exploração de idéias gerais de portais quânticos e circuitos quânticos. Um objetivo particular neste processador é o desenvolvimento de uma álgebra "Threelean" (uma evolução da tradicional Booleana) para projetar novas portas lógicas quânticas baseadas em qutrits.

O objetivo de longo prazo é atingir um nível de competitividade tanto em circuitos de recozimento quânticos quanto em circuitos quânticos baseados em gate, servindo principalmente a tecnologia de recozimento quântico para os usuários.

3. 3. Serviços de Software Qilimanjaro (QSS)

Os Serviços de Software Qilimanjaro (QSS) ajudará indivíduos e empresas a adaptar seus problemas a algoritmos quânticos que são executados em máquinas quânticas tradicionais. Como conseqüência, o QSS pretende construir um sistema operacional que funcionará no computador quântico do Qilimanjaro para fornecer um serviço completo aos clientes.

O QSS oferecerá serviços algorítmicos quânticos que oferecerão soluções para::

- Adaptar problemas do mundo real a algoritmos quânticos
- Otimização de algoritmos quânticos para qualquer hardware quântico existente, incluindo outras plataformas quânticas fora do Qilimanjaro
- Executando e analisando experimentos em nosso computador quântico

Um serviço adicional fornecido pela equipe do QSS consistirá no desenvolvimento de uma interface simples para programar o Analisador Quântico do Qilimanjaro.

3. 3. 1. Objetivos Técnicos do QSS

Traduzir um problema do mundo real para o mundo quântico não é fácil. A mecânica quântica vem com novos tipos de operações lógicas. No entanto, também traz algumas restrições fundamentais para outras tarefas, como copiar um determinado estado quântico. Em outras palavras, os algoritmos quânticos oferecem um novo paradigma computacional.

As empresas que gostariam de explorar o poder da computação quântica não podem simplesmente executar seu software em uma máquina quântica. Hoje, as implementações de cada algoritmo devem atender a cada dispositivo quântico em particular. Como conseqüência, muitos conhecimentos são necessários para desenvolver algoritmos quânticos adaptados a um processador quântico.

Os Serviços de Software Qilimanjaro oferecerão um serviço completo aos usuários dispostos a usar a Computadores Quânticos. Isso inclui ajudar indivíduos ou empresas a identificar os problemas que podem se beneficiar de um computador quântico, traduzindo seu problema para a linguagem da lógica quântica e, eventualmente, executando o algoritmo no dispositivo quântico.

A maioria dos problemas que serão executados no analisador quântico estão relacionados a otimizações. Este tipo de problemas requer encontrar um ponto ótimo, um mínimo de função de custo, que pode ser formulado como um QUBO (Quadratic Unconstrained Binary Optimization). Por sua vez, um QUBO deve ser mapeado em uma função de custo

(hamiltoniana), para ser minimizada na conectividade real de qubits. Hoje, essas etapas são realizadas de maneira não trivial e podem precisar da ajuda de especialistas quânticos.

3. 3. 2. Acesso ao Computador Quântico na Nuvem

A execução de um algoritmo quântico, adequadamente projetado, deve ser fácil. Alguém gostaria de simplesmente escrever o código em uma interface simples e enviá-lo para execução em um dispositivo quântico. O QSS do Qilimanjaro visa essa meta, fornecendo diretamente um conjunto de ferramentas para facilitar o acesso e o uso de computadores quânticos.

A simplicidade desse procedimento abrirá as portas para os indivíduos que explorarem novas técnicas para resolver problemas em aberto. O dispositivo quântico atua como um dispositivo computacional cego que é alugado com base em execuções individuais, que por sua vez estão associadas ao token QBIT.

3. 4. Qibo: Ling. Quântica de Código Aberto Universal

O Qibo é uma metalinguagem para software quântico, configurando uma interface de programação acima dos detalhes específicos dos computadores quânticos, onde os programas serão executados. O Qibo já está em desenvolvimento pela equipe Qilimanjaro. A linguagem irá interagir com diferentes compiladores para cada dispositivo que seurge no mercado. Além disso, o Qibo foi projetado tendo em mente alcançar a maior comunidade de programadores interessados em programação quântica. A motivação é desenvolver as primeiras bibliotecas fundamentais quânticas e contribuir para o atual ecossistema da programação quântica, enquanto compensamos os esforços que promovem um sistema de recompensas, com base em nosso token QBIT do tipo ERC-20, conforme explicado na Seção 4.1.

3. 5. OpenQ

Todos os dias, mais universidades, grandes corporações e pequenas empresas estão interessadas em como a computação quântica pode mudar ou acelerar sua análise de dados. Somente as empresas mais ricas podem se dar ao luxo de dedicar grandes somas e recursos a essa causa, testar máquinas já desenvolvidas ou adquirir aplicativos de algoritmos para os seus próprios negócios.

Nós miramos um crescimento potencial por trás do uso da computação quântica, caso mais empresas e usuários acessem essa tecnologia, beneficiada por um custo acessível. Com o constante desenvolvimento dessa tecnologia, podemos prever uma adoção exponencial no mundo corporativo/de varejo para fornecer soluções rápidas e escalonáveis para os problemas pesados/intratáveis de hoje.

Devido à ampla variedade de aplicações de um computador quântico, os serviços que o Qilimanjaro oferecerá precisam abranger diferentes tipos de público, como governos, laboratórios de pesquisa, universidades, grandes e pequenas empresas e o usuário individual. O Qilimanjaro fornecerá serviço a qualquer usuário/setor que queira se beneficiar do potencial de computação quântica.

Nosso objetivo é criar um ecossistema para computação quântica descentralizada. Um mercado mundial de poder computacional onde os usuários podem se beneficiar das capacidades dos processadores quânticos, podendo executar algoritmos apropriados adequadamente implementados, adaptados às suas necessidades.

Desta maneira, queremos formar uma comunidade de código aberto para explorar totalmente o poder da computação quântica e alavancar ao máximo suas capacidades. Trabalhando com uma linguagem quântica adequadamente projetada, esta comunidade continuará a projetar e melhorar soluções quânticas. Criar novos algoritmos e fazer contribuições para uma aceleração ainda maior no desenvolvimento dessa tecnologia é essencial. Uma forte comunidade de código aberto é uma peça essencial no futuro das tecnologias de computação quântica, já que outras tecnologias se beneficiaram no passado ao abrir seu desenvolvimento para um público maior.

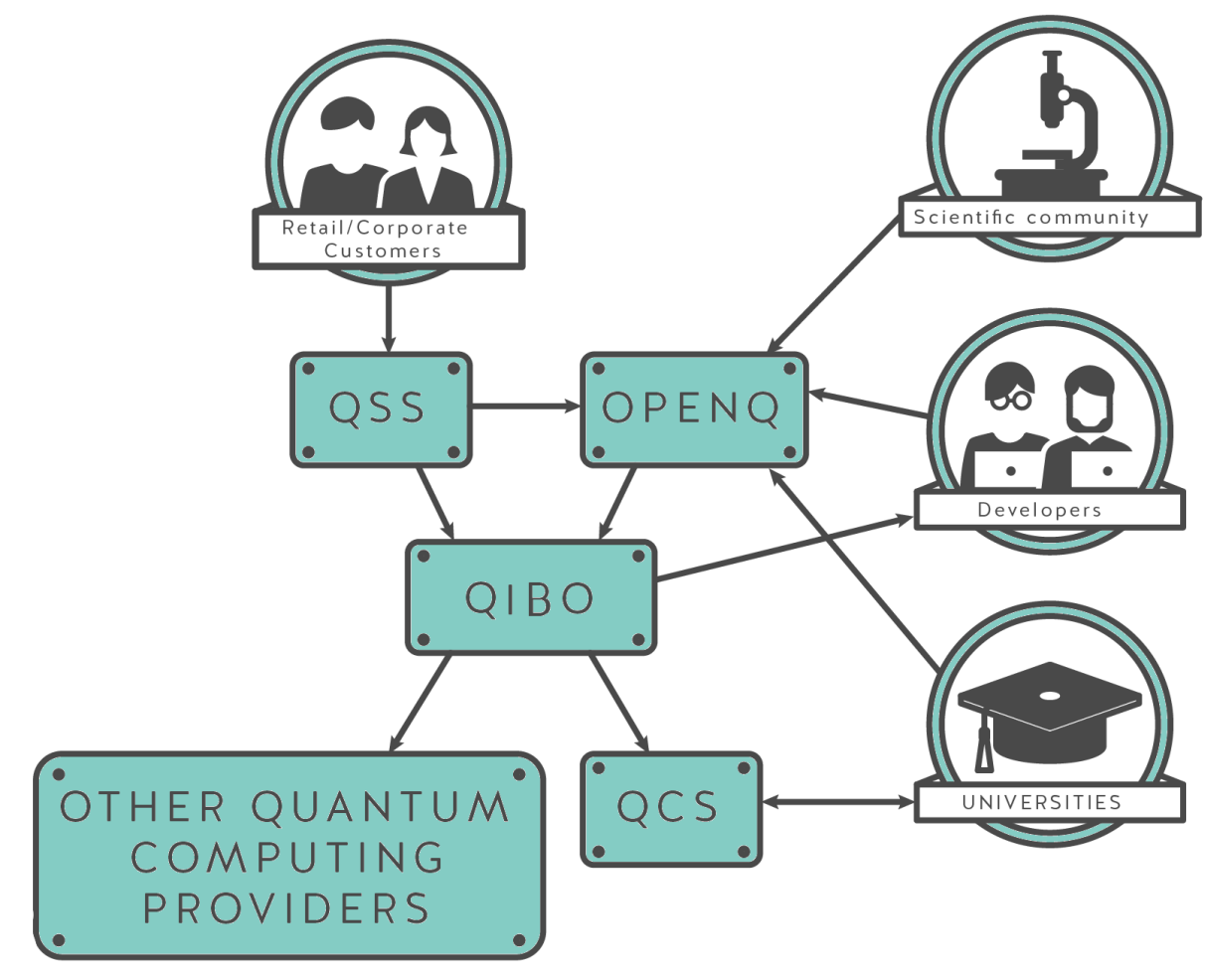
Portanto, o Qilimanjaro pretende gerenciar o OpenQ como uma ferramenta para a comunidade e uma rede de código aberto cuja capacidade de processamento é descentralizada.

Nossos clientes poderão escolher entre diferentes algoritmos pré-construídos ou solicitar soluções algorítmicas específicas que possam atender aos requisitos do problema a ser tratado, resultando em novos algoritmos a serem adicionados ao catálogo do Qilimanjaro.

A implementação e a discussão sobre o algoritmo serão tratadas dentro do OpenQ, onde qualquer cientista ou projetista de algoritmos será capaz de pesquisar algoritmos quânticos existentes e propor os seus próprios.

O OpenQ será o ponto de encontro entre a comunidade científica e os desenvolvedores, onde ambos serão recompensados pelo seu trabalho. Enquanto um especialista em algoritmo será capaz de colaborar com os outros e ser compensado fazendo propostas de algoritmos, desenvolvedores talentosos irão propor implementações concretas e serão recompensados de acordo com a importância de suas contribuições. Desta maneira, diferentes comunidades serão reunidas, resultando em aplicações reais, construindo soluções concretas para o mundo quântico.

Todo o conteúdo apresentado será submetido a uma revisão técnica pela equipe de cientistas do Qilimanjaro para garantir que ele cumpra os padrões do setor e esteja totalmente funcional antes de ser lançado no OpenQ.



A maioria dos projetos de computação quântica são privados e muito focados no lado corporativo das coisas. Nossa estrutura integra setores eficientes e críticos para pesquisa e desenvolvimento, ao mesmo tempo em que traz recompensas e abertura para a comunidade. Oferecemos o serviço mais completo em todas as camadas.

4. Função do Token

4. 1. Uso e Mecanismo do Token QBIT

QBITs (pronunciados como [kiúbits]) são tokens compatíveis com o ERC20 que autorizam seus proprietários a:

- Receber assistência para traduzir problemas do mundo real para a lógica de um determinado algoritmo quântico
- Executar algoritmos em uma máquina de recozimento quântico coerente
- Incentivar desenvolvedores de algoritmos quânticos que desejam adicionar seu algoritmo à nossa plataforma. Estes algoritmos serão primeiro verificados pela nossa equipe para verificar sua eficácia.

Os tokens permitirão que empresas e indivíduos explorem a computação quântica e resolvam problemas complexos da vida real, tanto no nível de software quântico quanto em dispositivos quânticos. Por sua vez, os tokens retornarão ao mercado de modo a manter o nosso cronômetro quântico na fronteira do desenvolvimento tecnológico.

4. 2. Pós-quântico: Criptografia quântica resistente para o QBIT

A criptografia usada atualmnte na tecnologia blockchain se tornará eventualmente insegura por computadores quânticos. O Qilimanjaro atualizará seus tokens para uma criptografia quântica resistente a computadores quânticos assim que a NSA produzir uma recomendação.

A NSA (Agência de Segurança Nacional) lançou uma competição através do NIST (Instituto Nacional de Padrões e Tecnologia) para propor novos algoritmos criptográficos que são resistentes a computadores quânticos. A idéia básica é substituir algoritmos atuais, como aqueles relacionados a curvas elípticas por novos que são, no presente, seguros contra um ataque de computadores quânticos. A escolha final para um novo padrão criptográfico provavelmente levará alguns anos.

Os QBITs serão introduzidos pela primeira vez usando criptografia tradicional e serão compatíveis com ERC20. À medida que a NSA emite uma recomendação final de mudança para um novo esquema de resistência quântica, os QBITs serão atualizados para usar esse protocolo criptográfico de resistência quântica.

5. Objetivos

5.1. Objetivos Gerais

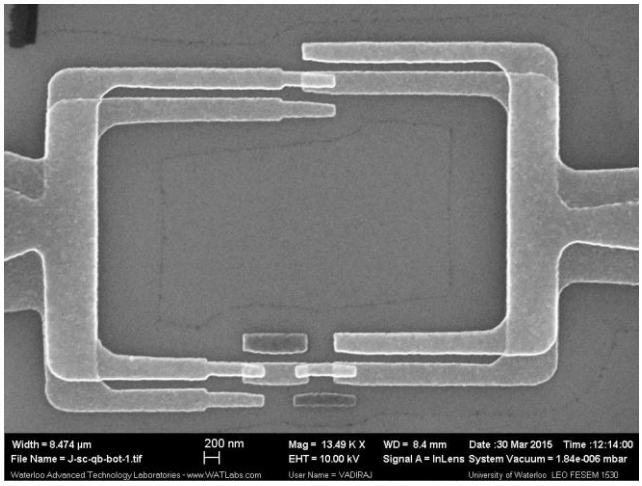
Os objetivos gerais do Qilimanjaro são:

- Contribuir com avanços científicos que agreguem valor aos fundamentos da computação quântica.
- Desenvolver plataformas e infraestruturas facilmente acessíveis a um público global.
- Integrar o desenvolvimento de padrões quânticos que facilitem o diálogo entre as diferentes empresas que desenvolvem esta tecnologia.
- Promover a colaboração com outras empresas e infraestruturas existentes para acelerar o desenvolvimento e a padronização de tecnologias quânticas.
- Promover a colaboração por meio de uma comunidade de código aberto. Estimular a criação de redes de pessoas, incentivando a mobilidade e o intercâmbio de conhecimentos.
- Promover a tecnologia de recozimento quântico e circuitos quânticos na Europa, onde nenhum investimento significativo foi feito nesta direção.

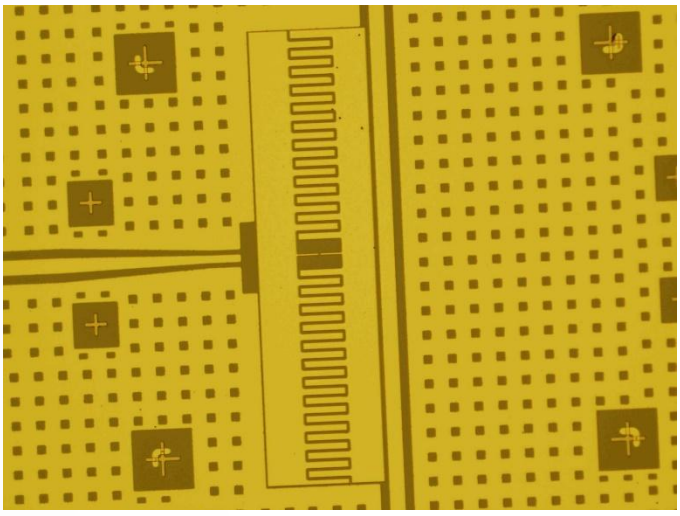
5.2. Objetivos de Curto Prazo

5.2.1. Fluxo de Qubits

Atualmente, já desenvolvemos o primeiro conjunto de qubits transmon e trans supercondutores. O primeiro é mais fácil de controlar, enquanto o segundo é mais difícil de produzir, mas permite um conjunto mais complexo de manipulações. As imagens mostradas abaixo correspondem aos dispositivos de qubit reais. Dispositivos semelhantes aos mostrados nas imagens serão usados para a primeira geração de experimentos para calibrar nossos circuitos de controle e instrumentação, em preparação para os sistemas de larga escala.



Micrografia Eletrônica de Varredura (SEM) de um qubit de fluxo supercondutor. As áreas mais claras são as junções Josephson, o elemento-chave para a tecnologia qubit supercondutora.



Uma visão macro de um circuito contendo um transmon qubit, visto no centro da tela. Imagem tirada por um microscópio convencional

5.2.2. Outros Objetivos

O plano de ação de curto prazo proposto inclui os seguintes itens:

- Configurar o primeiro analisador quântico com alguns qubits de fluxo (<5 qubits)
- Primeiros testes reais de algoritmos quânticos com alguns qubits.
- Oferecer consultoria em algoritmos quânticos. Os Serviços de Software Qilimanjaro ajudarão os usuários a adaptar seus problemas em um algoritmo quântico utilizável.
- Contribuir para o desenvolvimento do Qibo.
- Construir o OpenQ.

5.3. Objetivos de Longo Prazo

Nossos objetivos de longo prazo consistem em::

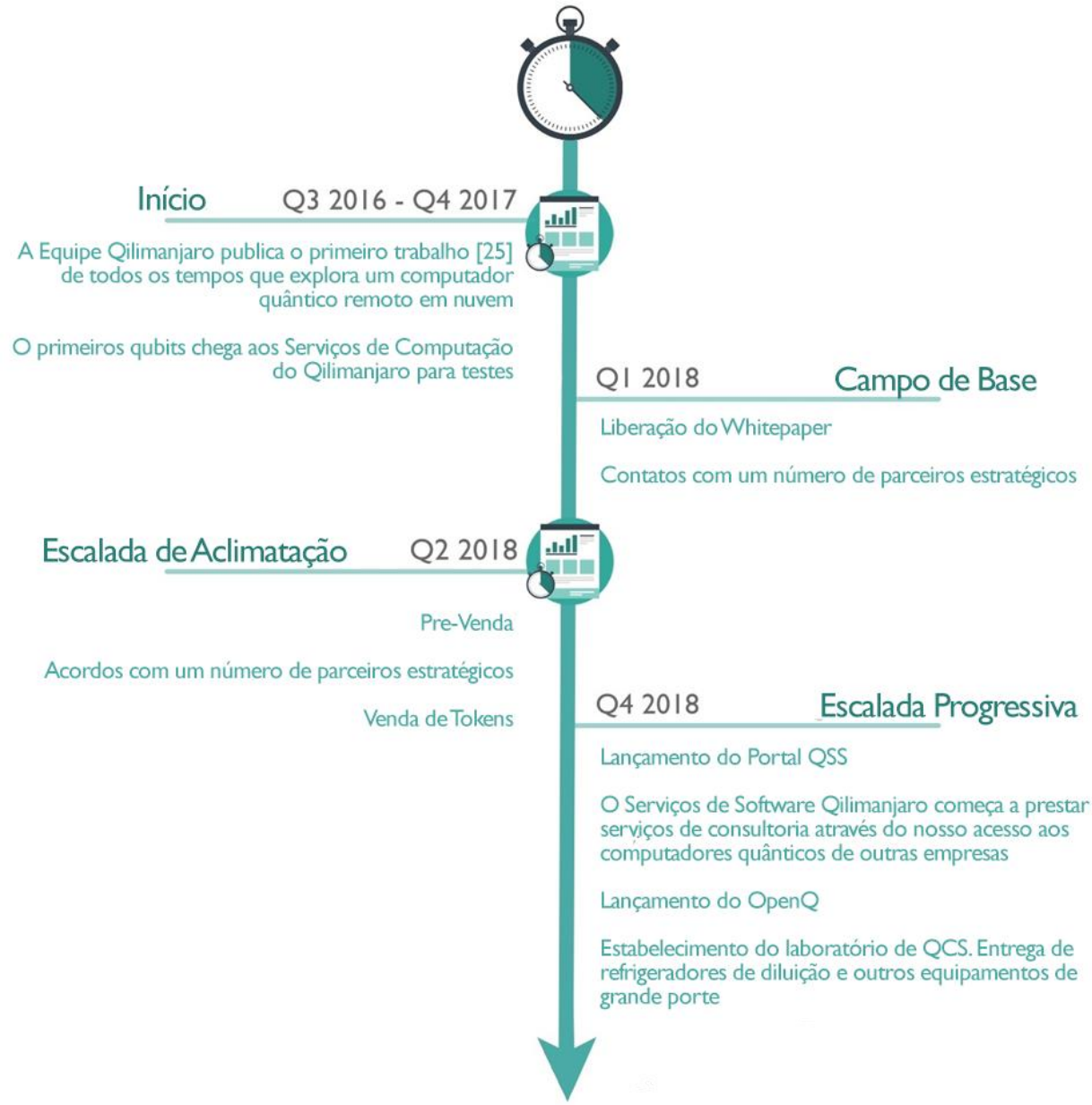
- Completar a construção de um analisador quântico coerente em tamanho real, alcançando a supremacia quântica (100 qubits). Sistemas de dimensões ainda maiores são previstos além do Qilimanjaro.
- Desenvolver uma linguagem quântica aberta amplamente usada
- Estimular pesquisas sobre algoritmos quânticos
- Melhorar o ecossistema da computação quântica
- Tornar computadores quânticos acessíveis
- Criar um token resistente a computadores quânticos

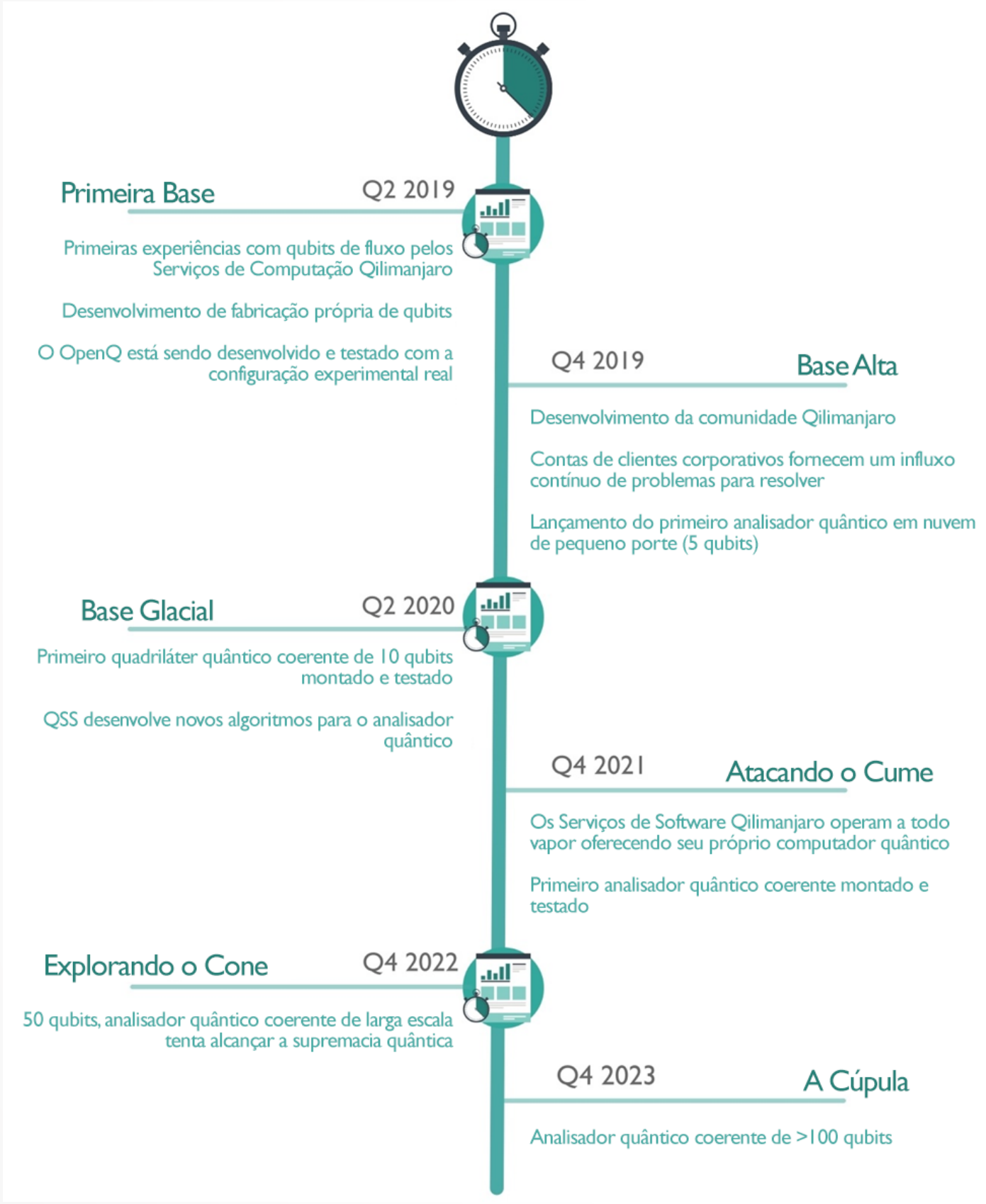
Um outro projeto de longo prazo é complementar o analisador quântico coerente do Qilimanjaro com um computador quântico de pleno direito. Dada a tecnologia dos qubits de fluxo empregada no dispositivo proposto pelo Qilimanjaro, a transição para um computador quântico completo seria muito mais suave.

6. Roadmap

Nosso projeto se baseará na experiência de pesquisas anteriores sobre analisadores quânticos pelo uso de qubits de alta qualidade. Existe um trade-off entre os grandes mas imperfeitos analisadores quânticos (D-Wave) e o proposto aqui, que é de melhor qualidade mas menor tamanho. O escalonamento do analisador quântico do Qilimanjaro virá naturalmente com o tempo.

Um roteiro mais detalhado é apresentado esquematicamente.




Primeira Base
Q2 2019
Primeiras experiências com qubits de fluxo pelos Serviços de Computação Qilimanjaro
Desenvolvimento de fabricação própria de qubits
O OpenQ está sendo desenvolvido e testado com a configuração experimental real
Q4 2019
Base Alta
Desenvolvimento da comunidade Qilimanjaro
Contas de clientes corporativos fornecem um influxo contínuo de problemas para resolver
Lançamento do primeiro analisador quântico em nuvem de pequeno porte (5 qubits)
Base Glacial
Q2 2020
Primeiro quadriláter quântico coerente de 10 qubits montado e testado
QSS desenvolve novos algoritmos para o analisador quântico
Q4 2021
Atacando o Cume
Os Serviços de Software Qilimanjaro operam a todo vapor oferecendo seu próprio computador quântico
Primeiro analisador quântico coerente montado e testado
Explorando o Cone
Q4 2022
50 qubits, analisador quântico coerente de larga escala tenta alcançar a supremacia quântica
Q4 2023
A Cúpula
Analisador quântico coerente de >100 qubits

7. Crowdfunding

A Crowdsale do Qilimanjaro e o processo de criação de tokens correspondentes serão organizados em torno de contratos inteligentes executados na rede do Ethereum.

Os participantes dispostos a apoiar o desenvolvimento do Projeto Qilimanjaro podem fazê-lo enviando a moeda Ether para o endereço designado. Ao fazer isso, eles estarão comprando Tokens QBITs (QBITs) que serão enviados instantaneamente para sua carteira.

- A moeda aceita durante a ICO é o Ether.
- Se a campanha de venda de tokens não atingir sua meta de capital mínimo de 8.000.000 de euros, todos os fundos serão devolvidos automaticamente aos detentores do QBIT pelo contrato inteligente da rede do Ethereum.
- A criação de token tem um hard cap: ao atingir esse limite, ela será interrompida e nenhuma outra contribuição será aceita.
- Tokens que não forem vendidos durante a Crowdsale serão queimados automaticamente pelo contrato inteligente. A queima de tokens pode potencialmente aumentar a valorização dos tokens QBIT restantes à medida que a oferta total em circulação for reduzida.

O token QBIT será um token de valor baseado na rede do Ethereum. O token é um ativo digital, tendo valor por si baseado em seus ativos subjacentes, propriedades e/ou direitos associados.

Os tokens baseados na rede do Ethereum contam com sua infraestrutura bem estabelecida, beneficiando-se de várias vantagens:

- Segurança e previsibilidade (em oposição a, por exemplo, ter que executar uma rede blockchain independente).
- Uso de clientes robustos e bem suportados (os tokens baseados no Ethereum podem ser gerenciados com clientes oficiais de sua rede).
- Alta liquidez, facilitando a listagem exchanges com uma infraestrutura já existente.

Nosso contrato de token baseado na rede do Ethereum está em conformidade com o padrão ERC20. Informações mais detalhadas sobre o padrão ERC20 podem ser obtidas em: https://github.com/ethereum/EIPs/issues/20.

Dados Gerais		
Qualificação Legal	Moeda de Utilidade, não é uma security	
% de tokens a venda	45%	40% Pré-Venda
		60% Crowdsale
Softcap (inc. Pré-ICO)	8.000.000 € / 9.900.000 $	
Hardcap	20.300.000 € / 25.000.000 $	
Supply em Circulação	135.000.000 QBIT	
Supply Máximo	300.000.000 QBIT	
Moedas Aceitas	ETH	
Raíses Restritos	EUA (apenas investidores credenciados podem participar) / China	
Whitelist	Sim	
KYC	Sim	

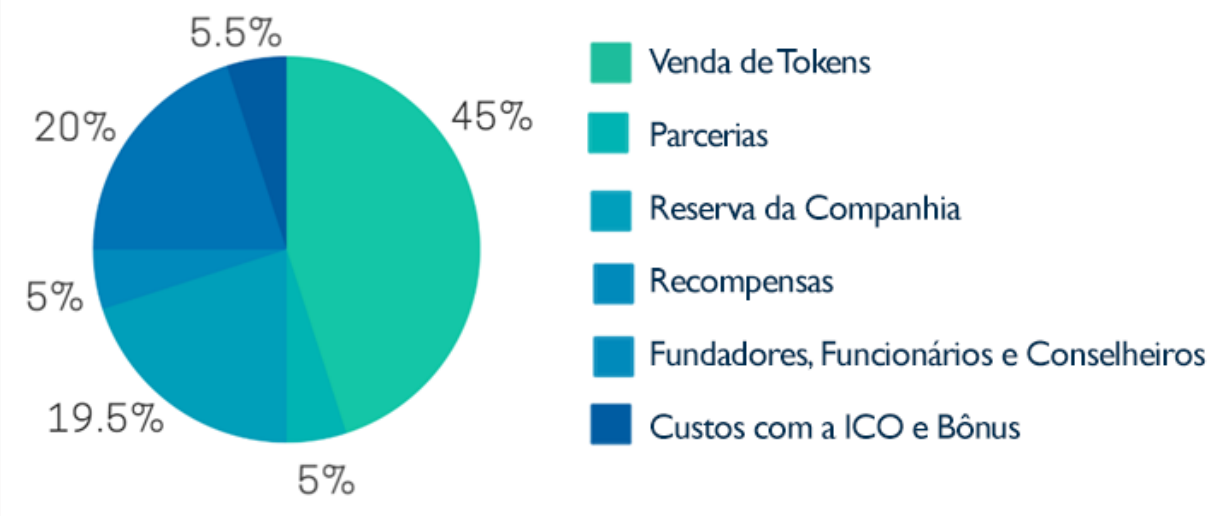
Fase 1 #1: Pré-Venda Privada		
Data de Início		Em Progresso
Total de tokens vendidos neste estágio	%	15% do total de token à venda
	Tokens	20.250.000 QBIT
Preço		0,15 € / 0,185 $ (+25% bonus no máximo)
Detalhes da Pré-Venda Privada		Para mais detalhes sobre a pré-venda privada, entre em contato com investments@qilimanjaro.io

Fase #2: Pré-Venda Pública		
Data de Início		A ser anunciada em breve
Total de tokens vendidos neste estágio	%	25% do total de tokens à venda
	Tokens	33.750.000 QBIT
Preço		0,15 € / 0,185 $ (Mesmo preço da ICO)
Contribuição Máxima		20.000 $
Bônus (Min – Máx)		0 % → De 20.000 $ a 50.000 $ +5% → De 50.000 $ a 125.000 $ +10% → De 125.000 $ a 250.000 $ +15% → De 250.000 $ a 500.000 $
Periodo de bloqueio de tokens de bônus		Sem bloqueio
Distribuição de Tokens		Entre 2-4 semanas
Bloqueados?		Sim
Data de Desbloqueio		Os tokens serão desbloqueados 15 dias após o fim da Crowdsale

Fase #3: Crowdsale		
Date start		A ser anunciada em breve
Total de tokens vendidos neste estágio	%	60% do total de tokens à venda
	Tokens	81.000.000 QBIT
Preço		0,15 € / 0,185 $
Bônus		Sem bônus
Contribuição Mínima		50 $
Contribuição Máxima		A ser definido
Distribuição de Tokens		Imediamtamente
Bloqueadp?		Sim
Data de Desbloqueio		Os tokens serão desbloqueados 15 dias após o fim da Crowdsale

7.1. Uso de fundos

Alocação de Tokens



Reserva da Companhia

Este orçamento será utilizado quando surgirem novas necessidades orçamentais ou quando uma das outras estimativas orçamentais for subestimada e ficar sem financiamento.

Recompensas

Uma parte do nosso orçamento será reservada para abastecer a comunidade Qilimanjaro e para um sistema de recompensas. Os especialistas em algoritmo e desenvolvedores talentosos serão recompensados de acordo com a importância de sua contribuição.

Fundadores, Funcionários e Conselheiros

Os membros da equipe principal terão um cronograma de aquisição de 2 anos para os tokens do QBIT, onde os consultores e parceiros estratégicos terão um cronograma de 6 meses para aquisição. A equipe receberá ¼ de sua alocação 6 meses após o término da

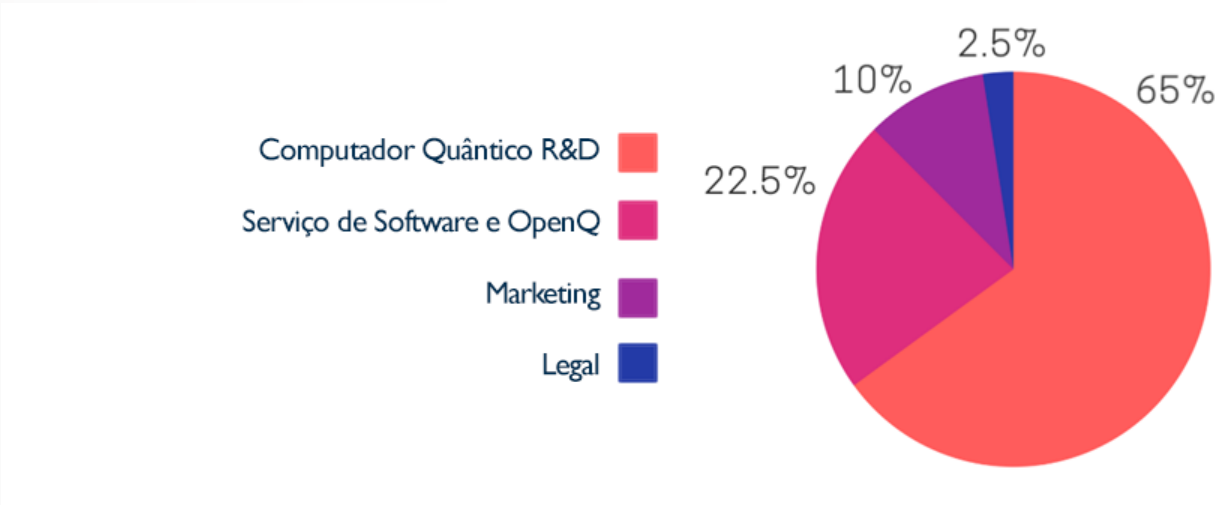
Venda Pública. Todos os meses a partir de então, a equipe receberá a proporção de sua alocação até que o cronograma de aquisição de direitos seja concluído.

Custos da ICO

Esta parte cobre os custos do evento de venda de tokens, como comunicação, auditoria de contrato inteligente, KYC, listagens em exchanges, etc.

Gerenciamento de Fundos

Os fundos recebidos na Venda de Tokens Qilimanjaro serão mantidos em uma carteira segura multi-assinada e serão alocados para os seguintes desenvolvimentos:



O financiamento será alocado para múltiplos aspectos do projeto. A maior parte servirá para desenvolver os Serviços de Computação Quântica e os Serviços de Software Quântico, mas também precisamos de um orçamento para apoiar atividades, como marketing.

Computador Quântico R&D

A maior parte dos recursos será destinada à pesquisa e desenvolvimento de analisadores quânticos, envolvendo a aquisição de materiais, como geladeiras de diluição, contratações de pelo menos 2 pós-doutores, 3 estudantes de doutorado e um técnico por computador.

Isso equivale, no mínimo, a mais 24 pessoas, além das que já integram o projeto. Os custos de funcionamento também são uma parte muito importante da manutenção de um computador quântico e não devem ser esquecidos.

Serviço de Software Quântico e OpenQ

Uma porção significativa dos fundos será reservada para desenvolver o QSS e o OpenQ. Como o desenvolvimento de software requer principalmente o trabalho de funcionários qualificados, essa parte do nosso orçamento será usada para pagar nossos desenvolvedores de software e programadores quânticos. Além disso, os Fundos serão utilizados para a operação e gerenciamento deste ambiente e para garantir a entrega de software com a máxima qualidade e em tempo hábil.

Marketing

O OpenQ será construído sob um forte senso de comunidade. Para este efeito, temos que garantir que fundos suficientes sejam alocados para o alcance de uma comunidade internacional. O orçamento de marketing será usado para criar conscientização e engajamento das possibilidades da nossa plataforma.

Legal

Essa alocação garante que a Qilimanjaro tenha os contratos legais certos em uma base contínua.

8. Equipe

8.1. Membros-chave da Equipe

José Ignacio LATORRE LinkedIn

UB, MIT, Niels Bohr Institute, University Singapore, Entanglement Partners

Informação Quântica, Física de Partículas, Inteligência Artificial

JIL obteve seu PhD em Física de Partículas na Univ. Barcelona. Ele era um Fullbright Fellow no MIT (EUA) e um pós-doutorado no Niels Bohr Institute em Copenhague. Ele então se tornou professor associado na Universitat de Barcelona e, posteriormente, professor titular em Física Teórica. Ele também desfruta de uma posição de visitante de longo prazo no Center for Quantum Technologies (Cingapura). Ele escreveu mais de 100 artigos sobre Partículas Físicas e Informação Quântica e dirigiu 12 teses de doutorado. Ele foi um dos fundadores do Centro de Ciências de Benasque Pedro Pascual. Ele produziu dois documentários, um deles sobre o último cientista vivo do Projeto Manhattan. Ele trabalhou como consultor em Inteligência Artificial para o setor privado. Ele foi um dos fundadores da colaboração NNPDF [26] que serve distribuições parton baseadas em redes neurais para o CERN. Ele é sócio e diretor científico da Entanglement Partners SL. Também investigador principal da equipe QUANTIC no Barcelona Supercomputing Center.

Pol FORN-DÍAZ

LinkedIn

DELFT, MIT, CALTECH, IQC Waterloo, Entanglement Partners, BSC

Pol lidera a equipe experimental da QUANTIC no Barcelona Supercomputing Center. Ele tem experiência em dispositivos quânticos supercondutores para aplicações de informação quântica e óptica quântica. Ele obteve seu PhD na TU Delft em 2010, com um estudo de qubits de fluxo supercondutores e os limites da força de interação para um ressonador supercondutor. Depois de seu PhD, ele foi um acadêmico visitante no laboratório do Prof. W. D. Oliver no MIT para um curto projeto. Ele era então um pesquisador de pós-doutorado no laboratório Kimble no California Institute of Technology, trabalhando na interface de átomos frios e guias de ondas fotônicos. Mais tarde ele foi um pós-doutorado no Instituto de Quantum Computing at the University of Waterloo, trabalhando em qubits supercondutores interagindo com campos de microondas de propagação. Ele é sócio da Entanglement Partners SL.

Artur GARCÍA-SÁEZ

Web

ICFO, UB, Stony Brook, BSC

Informação Quântica, Aprendizado de máquina, Programação Avançada

Artur García-Sáez obteve seu Ph.D. no The Institute of Photonic Sciences (ICFO) trabalhando em correlações clássicas e quânticas. Desde então, ele trabalhou na Universitat de Barcelona e no C.N. Yang Institute for Theoretical Physics em Stony Brook. Atualmente, ele trabalha no Barcelona Supercomputing Center em problemas de otimização e aplicativos de aprendizado de máquina. Ele é o chefe da equipe do algoritmo QUANTIC.

Jordi Blasco

LinkedIn

ARS CORPORATE

Especialista em fusões, aquisiçõese e finanças corporativas, além de conselheiro no Conselho de Administração. Jordi Blasco é advogado (Universitat Autònoma de Barcelona, ou UAB). Ele tem um diploma fiscal (EADA Business School), um mestrado em auditoria (UAB e o Catalan Chartered Accountants Institute), um MBA executivo (EADA Business School) e uma pós-graduação em administração de empresas (IESE Business School). Ele fundou várias empresas e firmas, entre elas uma firma de advocacia (BLASCO SELLARES legal + fiscal) e um banco de investimento boutique, o ARS Corporate. Membro de vários Conselhos de Administração em diferentes setores, incluindo mídia, infra-estrutura, consultoria, tecnologia ou educação. Atualmente é palestrante em estudos de Fusões, Aquisições e Fianancas Corporativas na EADA Business School e na Catalan Economists Bar Association.

8.2. Conselheiros

Víctor Canivell

LinkedIn

Diretor Geral na Quantum World Association

Victor Canivell é um executivo experiente com um histórico de sucesso como diretor europeu de multinacionais de TI (HP, 3Com, Silicon Graphics, PerkinElmer) e CEO/Melhor do Conselho de várias startups de software, principalmente no setor de segurança. Estrategista independente e consultor operacional para startups de alta tecnologia, para as PME de alta tecnologia da Comissão Européia no instrumento Horizon 2020 e para Consultores Alfa Beta. Seus interesses atuais residem na computação quântica, segurança e inteligência artificial. Victor é PhD em Física pela UB, possui um MBA pela ESADE e uma extensa experiência internacional em negócios.

Miklos Santha

Web

Diretor Sênior de Pesquisa no Center for Quantum

Miklos Santha recebeu seu PhD em Matemática pela Université Paris-Diderot. Ele é Diretor Sênior de Pesquisa no Centre National de la Recherche Scientifique desde 1988. Ele também é Pesquisador Principal e Professor Pesquisador Visitante do Centre for Quantum Technologies na National University of Singapore desde 2008. Ele é um especialista em algoritmos clássicos e quânticos e complexidade.

Gavin Brennen

Web

Diretor de Comunidade, Qubit Protocol.

A Qubit Protocol é uma plataforma de governança para o financiamento de startups de tecnologia quântica. Gavin Brennen é também professor associado da University of Macquarie e diretor da QSciTech and CI no ARC Centre of Excellence EQuS.

9. Aviso Legal

Este white paper (o "Whitepaper") oferece uma visão geral de certos aspectos do projeto Qilimanjaro Quantum Hub (projeto Qilimanjaro, abreviadamente) e o uso pretendido de seu token QBIT. Este Whitepaper e as informações aqui contidas não são juridicamente vinculativas.

A Venda de Tokens é feita apenas com base em um documento separado, o Documento de Oferta de Token, que será publicado logo após este Whitepaper.

Este Whitepaper não constitui uma oferta para investir ou comprar QBITs nem um convite para uma oferta de troca de qualquer quantidade de Ether por QBITs, ou de qualquer formar uma solicitação de qualquer tipo de suporte financeiro para o projeto Qilimanjaro.

Se você decidir participar da venda de Tokens QBIT como uma forma de investimento e/ou apoio financeiro ao projeto Qilimanjaro, a Qilimanjaro, seus fundadores e sua equipe expressamente avisam que um investimento ou qualquer tipo de suporte financeiro para Qilimanjaro e/ou QBITs carrega um risco de alto grau. Nenhum resultado para o projeto Qilimanjaro pode ser considerado certo, seguro ou garantido a qualquer momento.

Nenhum direito de propriedade de qualquer espécie é adquirido se você decidir participar da Venda de Tokens QBIT, pois você não estaria investindo em qualquer parte de uma empresa ou entidade de qualquer natureza. Os portadores de tokens não terão direitos de voto no projeto Qilimanjaro ou em qualquer entidade associada a ele ou usados como fornecedores ou contratados para os propósitos do desenvolvimento do projeto Qilimanjaro. Os portadores do Token não serão considerados como credores do projeto Qilimanjaro. Os detentores do QBIT terão apenas os direitos definidos neste Whitepaper, relacionados ao uso do poder computacional, capacidades que o projeto Qilimanjaro desenvolverá e os serviços de consultoria associados a ele.

Declarações Prospectivas

Este Whitepaper contém certas declarações prospectivas, algumas baseadas em desenvolvimentos científicos, previsões e análises, algumas outras baseadas no que é esperado da computação quântica e seus efeitos na sociedade e fenômenos sociais de qualquer tipo.

Uma declaração prospectiva é uma declaração que não se relaciona a fatos e eventos históricos. As declarações prospectivas são baseadas em análises ou previsões de resultados futuros e estimativas de capacidades, qualidades ou valores ainda não determináveis ou previsíveis.

Tais afirmações sobre o futuro são identificadas pelo uso de termos e frases como "antecipar", "acreditar", "poderia", "estimar", "esperar", "pretender", "planejar", "prever", "projetar" ”,” Irá “e termos semelhantes, incluindo referências e suposições. Isso se aplica, em particular, a quaisquer declarações contidas neste Whitepaper contendo informações sobre desenvolvimentos futuros do Qilimanjaro, planos e expectativas sobre os QBITs, seus usos e aceitação social do Qilimanjaro e de suas atividades, ou até mesmo seu crescimento de valor.

As declarações prospectivas são baseadas nas estimativas e suposições atuais que os promotores do projeto Qilimanjaro fazem com o melhor de seu conhecimento atual. Tais declarações prospectivas estão sujeitas a riscos, incertezas e outros fatores que podem causar desenvolvimentos reais diferentes materialmente e piores do que o esperado ou presumidos ou descritos sob estas declarações prospectivas.

Consequentemente, quaisquer pessoas ou entidades interessadas em participar da Venda de Tokens ou dar qualquer tipo de apoio financeiro ou qualquer outro tipo de apoio ao projeto Qilimanjaro são fortemente aconselhados a considerar todos os riscos que possam ter impacto sobre ele.

Devido a riscos, incertezas e suposições, os eventos futuros descritos neste Whitepaper podem não ocorrer ou podem ocorrer muito depois do esperado.

Apêndice: Exemplos Práticos de Casos de Uso

- Finança

Suponha que você seja um grande gerente de ativos. Toda vez que você reequilibra seu portfólio, seus investidores perdem dinheiro, por causa dos custos de transação e impacto de preço (atrasos). Em um ambiente no qual a maioria dos fundos luta para obter retornos, perder uma porcentagem dos lucros em custos de rebalanceamento é uma sentença de morte por mil cortes.

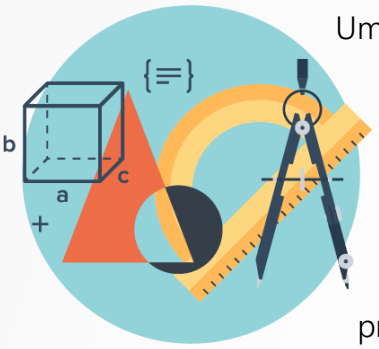
Um computador quântico pode encontrar um portfólio que seja ideal em vários horizontes de investimento, reduzindo significativamente a necessidade de reequilíbrios e suas perdas associadas. A computação convencional simplesmente não pode resolvê-lo.

- Pesquisa em Banco de Dados

Imagine que você só tem cinco minutos para encontrar um X escrito em uma página de um livro entre os 50 milhões de livros de uma grande biblioteca. Nesse cenário, você seria um computador comum e nunca encontraria o X. Mas, se tivesse 50 milhões de realidades paralelas e pudesse ver um livro diferente em cada uma dessas realidades (como um computador quântico), você encontraria o X. Por assim dizer, um computador quântico pode dividi-lo em 50 milhões de versões de si mesmo para tornar o trabalho rápido e fácil.

Em um mundo com tantos dados (mais dados foram gerados nos últimos dois anos do que em toda a história humana), os computadores quânticos, através do algoritmo Grover, oferecem uma solução para pesquisar eficientemente essas informações.

- Problemas de Otimização

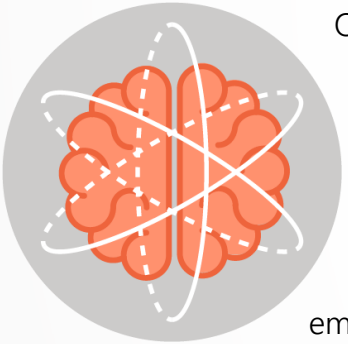


Um dos problemas mais difíceis em matemática é conhecido como o problema do vendedor ambulante, que pede para encontrar o caminho mais curto entre uma lista de endereços. Parece bastante simples, mas damos um exemplo.

Suponha que um entregador deva cobrir um colega doente e precise fazer quatro entregas em vez de três. Trabalhar com a rota mais eficiente é administrável. No entanto, esse problema aumenta rapidamente conforme você adiciona mais entregas. Por exemplo, fazer 10 entregas tem mais de 180.000 combinações. Imagine as combinações possíveis para a organização de uma frota inteira ou se surgir um problema inesperado!

Em termos de computação, é enorme e a aceleração que a computação quântica promete poderia proporcionar a mais alta redução de custos e melhorar suas habilidades.

- Treinamento de Redes Neurais

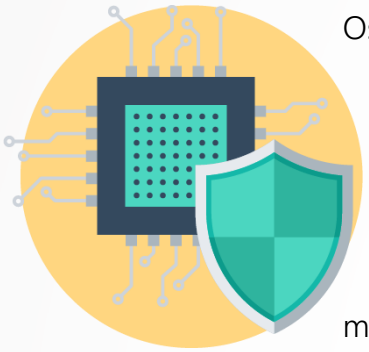


O principal trabalho de uma rede neural é reconhecer padrões. Inspirado pelo cérebro humano, é uma grade de unidades básicas de computação, os "neurônios".

Normalmente, os neurônios são organizados em camadas e a fiação entre eles não é fixada antecipadamente, mas se adapta em um processo de tentativa e erro. A rede pode ser alimentada com imagens rotuladas como “gatinho” ou “filhote”. Para cada imagem, ele atribui um rótulo, verifica se estava correto e ajusta as conexões neuronais, caso não esteja. Suas suposições são aleatórias no começo, mas melhoram; depois de talvez 10.000 exemplares, reconhece seus animais de estimação. Uma rede neural séria pode ter um bilhão de interconexões, todas as quais precisam ser sintonizadas.

Todas estas interconexões são representadas por uma matriz gigantesca e nada faz matrizes como um computador quântico, sendo sua resolução exponencialmente mais rápida que com um computador clássico.

- Criptografia e Segurança



Os dados financeiros codificados com criptografia quântica são de longe mais seguros do que a segurança digital atual.

Os atuais hackers podem copiar ou editar dados confidenciais, mas não em um mundo com segurança quântica. É graças às propriedades peculiares da mecânica quântica que: se uma mensagem é interceptada, quando alguém tenta observá-la, a mensagem não pode ser lida porque, irrevogavelmente, ela mudará seu estado quântico. Isto é baseado no princípio da incerteza de Heisenberg.

Para o mundo da segurança, a melhor solução está na combinação da computação quântica com a tecnologia blockchain.

- Química Quântica e Saúde

Exemplo 1: Levou 13 anos para mapear os 20.000 genes no genoma humano e mastrar que poderíamos projetar tratamentos adequados a uma composição genética específica. Mapear cada mutação nos 50 tipos de câncer mais comuns seria 10.000 vezes mais complexo. Os computadores convencionais não são poderosos o suficiente para executar bem essas tarefas, mas os computadores quânticos têm o poder de simular exatamente as moléculas grandes. Isso exigirá grandes computadores quânticos e ainda há um longo caminho a se percorrer.

Exemplo 2: A criação de fertilizantes sintetizadores é um processo que consome muita energia, responsável por cerca de 2% de todas as emissões globais de CO2. No entanto, a Terra faz isso naturalmente, usando bactérias vegetais e uma molécula - nitrogenase.

Analisar essa molécula é impossível para os computadores mais poderosos da atualidade. No entanto, é algo que está bem dentro das capacidades de um computador quântico.

Referências

[1] Quantum Technologies Flagship Final Report, High-Level Steering Committee 28 de Junho de 2017
URL: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=46979

[2] Daniel Greif, Maxwell F. Parsons, Anton Mazurenko, Christie S. Chiu, Sebastian Blatt, Florian Huber, Geoffrey Ji, Markus Greiner, Site-resolved imaging of a fermionic Mott insulator
URL: http://science.sciencemag.org/content/351/6276/953?ijkey=7lDwIMnxRJA5M&keytype=ref&siteid=scij/

[3] Juan Yin, Yuan Cao, Yu-Huai Li, Sheng-Kai Liao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Bo Li, Hui Dai, Guang-Bing Li, Qi-Ming Lu, Yun-Hong Gong, Yu Xu, Shuang-Lin Li, Feng-Zhi Li, Ya-Yun Yin, Zi-Qing Jiang, Ming Li, Jian-Jun Jia, Ge Ren, Dong He, Yi-Lin Zhou, Xiao-Xiang Zhang, Na Wang, Xiang Chang, Zhen-Cai Zhu, Nai-Le Liu, Yu-Ao Chen, Chao-Yang Lu, Rong Shu, Cheng-Zhi Peng, Jian-Yu Wang, Jian-Wei Pan,
Satellite-based entanglement distribution over 1200 kilometers
URL: http://science.sciencemag.org/content/356/6343/1140

[4] Focus: Intercontinental, Quantum-Encrypted Messaging and Video, APS Physics, 2018
URL: https://physics.aps.org/articles/v11/7

[5] Web Idquantique
URL: https://www.idquantique.com/

[6] Daniel Castro and Alan McQuinn, Information Technology & Innovation Foundation, Unlocking Encryption: Information Security and the Rule of Law
URL: http://www2.itif.org/2016-unlocking-encryption.pdf

[7] Richard P. Feynman, Simulating Physics with Computers, International Journal of Theoretical Physics, VoL 21, Nos. 6/7, 1982
URL: https://people.eecs.berkeley.edu/~christos/classics/Feynman.pdf

[8] Peter W. Shor (AT&T Research), Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer
URL: https://arxiv.org/abs/quant-ph/9508027v2

[9] J. I. Cirac and P. Zoller, Quantum Computations with Cold Trapped Ions
URL: https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.74.4091

[10] Ferdinand Schmidt-Kaler, Hartmut Häffner, Mark Riebe, Stephan Gulde, Gavin P. T. Lancaster, Thomas Deuschle, Christoph Becher, Christian F. Roos, Jürgen Eschner & Rainer Blatt, Realization of the Cirac–Zoller controlled-NOT quantum gate
URL: https://www.nature.com/articles/nature01494

[11] Web IBM Q
URL: https://www.research.ibm.com/ibm-q/

[12] Web DWave
URL: https://www.dwavesys.com/

[13] FET Flagship on Quantum Technologies, RIA Research and Innovation action, CSA Coordination and support action, FETFLAG-03-2018

URL: http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/fetflag-03-2018.html

[14] News in Web Popular Science
URL: https://www.popsci.com/chinas-launches-new-quantum-research-supercenter

[15] Video in section Our Thinking, Quantum computers: Solving Problems in Minutes, not millennia, Web Goldman Sachs
URL: http://www.goldmansachs.com/our-thinking/pages/toshiya-hari-quantum-computing.html

[16] Katherine Bourzac, Chemistry is quantum computing's killer app, Chemical and Engineering News, Volume 95 Issue 43 | pp. 27-31 October 30, 2017
URL: https://cen.acs.org/articles/95/i43/Chemistry-quantum-computings-killer-app.html

[17] First NASA Quantum Future Technologies Conference: QFT 1.0, NASA Quantum Artificial Intelligence Laboratory (QuAIL)
URL: https://ti.arc.nasa.gov/tech/dash/groups/physics/quail/

[18] Florian Neukart, Gabriele Compostella, Christian Seidel, David von Dollen, Sheir Yarkoni, Bob Parney, Traffic flow optimization using a quantum annealer
URL: https://arxiv.org/abs/1708.01625

[19] Alejandro Perdomo-Ortiz, Marcello Benedetti, John Realpe-Gómez and Rupak Biswas, Opportunities and challenges for quantum-assisted machine learning in near-term quantum computers
URL: https://arxiv.org/pdf/1708.09757.pdf

[20] Sergio Boixo, Sergei Isakov, Vadim Smelyanskiy, Ryan Babbush, Nan Ding, Zhang Jiang, Michael J. Bremner, John Martinis, Hartmut Neven, Characterizing Quantum Supremacy in Near-Term Devices
URL: https://research.google.com/pubs/pub46227.html

[21] R. Barends, J. Kelly, A. Megrant, D. Sank, E. Jeffrey, Y. Chen, Y. Yin, B. Chiaro, J. Mutus, C. Neill, P. O'Malley, P. Roushan, J. Wenner, T. C. White, A. N. Cleland, John M. Martinis, Coherent Josephson qubit suitable for scalable quantum integrated circuits
URL: https://arxiv.org/abs/1304.2322

[22] Web Ionq
URL: https://ionq.co/

[23] Scott Aaronson, Google, D-Wave, and the case of the factor-10^8 speedup for WHAT?, Critical Report
URL: https://www.scottaaronson.com/blog/?p=2555

[24] Fei Yan, Simon Gustavsson, Archana Kamal, Jeffrey Birenbaum, Adam P Sears, David Hover, Ted J. Gudmundsen, Danna Rosenberg, Gabriel Samach, S Weber, Jonilyn L. Yoder, Terry P. Orlando, John Clarke, Andrew J. Kerman & William D. Oliver, The flux qubit revisited to enhance coherence and reproducibility
URL: https://www.nature.com/articles/ncomms12964

[25] Daniel Alsina, José Ignacio Latorre, Experimental test of Mermin inequalities on a 5-qubit quantum computer

URL: https://arxiv.org/abs/1605.04220

[26] Web NNPDF
URL: http://nnpdf.mi.infn.it/