Bitcoin e Computação Quântica. Ameaça ou mito?

A computação quântica é frequentemente apontada como uma tecnologia disruptiva, capaz de revolucionar áreas como criptografia, otimização e inteligência artificial. No entanto, também gera preocupações significativas, especialmente em sistemas que dependem de criptografia para segurança, tais como o Bitcoin.

A questão central é se computadores quânticos têm a capacidade de comprometer a rede Bitcoin, considerando a sua alta hashrate e a evolução da tecnologia de processamento quântico.

Computação Quântica: Entendendo o Contexto Atual

A computação quântica funciona de maneira fundamentalmente diferente dos computadores clássicos. Enquanto os computadores clássicos usam bits (0 ou 1), os qubits na computação quântica podem estar em estados de superposição, permitindo múltiplos cálculos simultaneamente.

A vantagem da computação quântica em certas tarefas é significativa, particularmente naquelas que envolvem a resolução de problemas complexos em escalas gigantescas.

Algoritmos Quânticos Relevantes

- **Algoritmo de Shor:** Resolve problemas de fatorização e logaritmo discreto de maneira, exponencialmente, mais eficiente e rápida do que os métodos clássicos. Esta é considerada a maior ameaça para a criptografia assimétrica, como ECDSA (Elliptic Curve Digital Signature Algorithm), usada no Bitcoin.
- **Algoritmo de Grover:** Acelera a pesquisa num espaço de chaves criptográficas, reduzindo o tempo de ataque de força bruta pela raiz quadrada, afetando algoritmos de hash como o SHA-256, contudo forma menos grave quanto o algoritmo de Shor impacta o ECDSA.

Estado Atual da Computação Quântica

Atualmente, os computadores quânticos possuem qubits em quantidades limitadas e são vulneráveis a erros. Sistemas como o Sycamore do Google (com 54 qubits) e computadores da IBM Quantum têm demonstrado capacidades impressionantes, mas estão longe de superar os limites práticos para realizar ataques complexos contra redes como o Bitcoin, considerando a necessidade de ambientes controlados de temperatura, por exemplo, para prevenir a decoerência, isto erros por perda de informação.

Para comprometer o Bitcoin, seria necessário um computador quântico com milhões de qubits corrigidos por erros, algo que pode levar décadas para ser alcançado, até porque atualmente o computador quântico com maior número de qubits – o Atom Computing, possui apenas 1180 qubits.

Bitcoin e o Papel do Hashrate na Defesa

A rede Bitcoin é protegida por dois elementos principais: o algoritmo SHA-256 e a sua hashrate (859.34 EH/s à data da escrita deste documento), que é a medida do poder computacional dedicado à mineração.

Hashrate Atual

Em 2024, o hashrate do Bitcoin atinge níveis recordes, superando 880 EH/s (exahashes por segundo). Isso significa que a rede é capaz de realizar 850 quintilhões de operações SHA-256 por segundo. Esse número representa uma barreira colossal contra qualquer tentativa de ataque, seja por computadores clássicos ou quânticos.

Impacto da Computação Quântica na Mineração

Um computador quântico hipotético capaz de resolver o SHA-256 mais rápido do que todos os mineradores combinados precisaria de ter desempenho incomparável com os sistemas atuais.

Usando o algoritmo de Grover, a procura quântica no SHA-256 seria cerca de 21282^{128} operações, o que ainda exigiria uma potência computacional além do alcance atual ou projetado da computação quântica.

Além disso, o ataque à mineração exige não apenas quebrar o SHA-256, mas também competir contra a hashrate em tempo real. A taxa de produção de blocos no Bitcoin (um bloco a cada 10 minutos) implica que o invasor precisaria, consistentemente, de superar os mineradores honestos para reorganizar blocos e, efetivamente controlar a rede.

ECDSA: O Elo Vulnerável

O ECDSA, que protege as assinaturas digitais no Bitcoin, apresenta maior probabilidade de risco de ataque através da computação quântica. Com o algoritmo de Shor, um computador quântico suficientemente poderoso poderia derivar a chave privada de uma transação que já expôs a chave pública, permitindo o controlo e roubo de fundos de endereços Bitcoin.

No entanto, a ameaça é limitada pelos seguintes fatores que mitigam o ataque:

Uso de Endereços Não Reutilizáveis: Enquanto a chave pública não for exposta, a computação quântica não consegue atacá-la, para isso deverá ser gerado um novo endereço para cada transação.

Tempo de Exposição: O invasor precisaria de quebrar a chave pública antes da transação ser incluída num bloco, o que exigiria não apenas um computador quântico avançado, mas também acesso rápido à rede.

Computação Quântica: Uma Ameaça Imediata?

Apesar das preocupações teóricas, a computação quântica não é uma ameaça imediata ao Bitcoin, por vários motivos:

- **Limitações de Escalabilidade**: Para comprometer o Bitcoin, um computador quântico precisaria de milhões de qubits estáveis. Os computadores quânticos atuais ainda se encontram em estágios experimentais e apresentam poucos qubits com altos níveis de erro.
- **Infraestrutura e Custo**: Desenvolver e operar um computador quântico capaz de ameaçar o Bitcoin exigiria recursos financeiros e tecnológicos colossais, acessíveis apenas a estados-nação ou grandes corporações.
- **Avanço em Criptografia Pós-Quântica**: Estudos e investigação em algoritmos resistentes à computação quântica já se encontram numa estágio avançado, onde o Bitcoin pode integrar essas soluções caso a ameaça se torne iminente.

Cenários Hipotéticos e Mitigação

Mesmo no cenário de avanço rápido da computação quântica, o Bitcoin possui opções para se adaptar:

- **Migração para Criptografia Pós-Quântica**: A transição para assinaturas digitais resistentes a ataques quânticos poderá ser implementada por meio de um hard fork, eliminando a vulnerabilidade do ECDSA.
- **Aumento da Segurança de Hash**: Caso a ameaça ao SHA-256 se torne relevante, algoritmos de hash mais robustos podem ser introduzidos, mantendo a segurança da mineração.
- **Acompanhamento Ativo**: A comunidade do Bitcoin está constantemente monitorizando o progresso da computação quântica, garantindo que mudanças sejam implementadas antes de qualquer impacto real.

Conclusão

Embora a computação quântica tenha o potencial de impactar sistemas criptográficos, o Bitcoin está protegido por sua alta hashrate e a, ainda elevada, robustez do SHA-256. A vulnerabilidade no ECDSA é real, mas mitigável por práticas atuais e futuras atualizações e adaptações da rede.

A computação quântica, apesar de ser um desafio a longo prazo, não representa uma ameaça imediata ao Protocolo Bitcoin que, através da sua comunidade ativa e adaptável, continua a evoluir para se proteger e adaptar, rapidamente, contra quaisquer avanços tecnológicos que possam surgir.

Assim, a narrativa de que a computação quântica "destruirá o Bitcoin" deve ser encarada com ceticismo e análise de informação técnica criteriosa.