UNIVERSIDADE FEDERAL DE SANTA CATARINA

CFM - DEPARTAMENTO DE FÍSICA

Disciplina: FSC 7152 Computação Quântica 1

Professor: Prof. Dr. Eduardo Inacio Duzzioni

Semestre: 2022_2

Blockchains e a Ameaça Quântica

Equipe:

Victor do Valle Cunha (20104135)

Guilherme Corby Moreira (19150166)

Cristina Elisabeth Ricken (16150317)

Resumo

O desenvolvimento da computação quântica representa uma ameaça para muitos protocolos criptográficos utilizados em criptomoedas em operação na atualidade. Tecnologias Blockchain, por exemplo, dependem de protocolos criptográficos para muitas de suas sub-rotinas essenciais. Alguns destes protocolos estão suscetíveis a ataques quânticos. No presente artigo serão analisadas as principais criptomoedas baseada em Blockchain, como Bitcoin e Ethereum, assim como serão identificadas as principais fragilidades dentro de seu funcionamento e que tornaria o sistema vulnerável a ataques.

1. Introdução

A introdução dos computadores quânticos representa uma das muitas oportunidades para resolução de problemas que requerem processamento de dados em diversas áreas como na Física, Química, Biologia, Finanças e Inteligência Artificial e Criptografia.. Computadores quânticos operam baseados nas leis da Mecânica Quântica, tais como o Princípio da Superposição, entrelaçamento, Desigualdade de Bell, Funções de Bloch, dentre outras. Mais do que isso, o avanço científico e tecnológico desta nova classe de computadores possibilita o processamento de operações de forma mais eficiente do que por meio de máquinas clássicas. No entanto, este avanço vem acompanhado de preocupações em relação à criptografia moderna, com ataques em algoritmos de criptografia assimétrica e funções de hash que poderiam ser fortemente afetadas.

Assim, será abordado o contexto de utilização de computadores quânticos para quebrar esses protocolos criptográficos de Blockchain. Nesse sentido, após esta introdução, este documento foi dividido em três partes: (2) fundamentação teórica, na qual serão abordados os conceitos como blockchain, assinatura digital, algoritmo de Shor e Grover; (3) desenvolvimento, em que se discute como o funcionamento de determinadas criptomoedas impacta em como o algoritmos quânticos as afetam, assim como possíveis perspectivas para tais ameaças; (4) conclusão, em que retomamos os principais aspectos do artigo.

2. Fundamentação teórica

Blockchain

Blockchain é um sistema de registro de informações que se caracteriza por ter três características fundamentais: descentralização, consenso, imutabilidade. A grande revolução da blockchain para criptomoedas é a possibilidade de não utilizar uma entidade central que detém todo o controle da rede. Desse modo, todos os participantes mantêm uma cópia da cadeia de dados, se tornando dessa maneira uma tecnologia descentralizada e distribuída.

Em contrapartida, para que uma transação seja identificada como válida, é necessário que mais da metade dos computadores presentes na rede validem a transição. Caso contrário, a transação é negada. Essa lógica de validação, também conhecida como consenso, é o que garante a legitimidade das transações, até mesmo contra tentativas de realizar transações fraudulentas, e permite o bom funcionamento da cadeia de blocos.

Além disso, para garantir a imutabilidade das informações que serão mantidas na blockchain, o sistema é organizado em blocos que são interligados por referências a blocos anteriores. Assim, cada bloco é uma parte imutável da blockchain, uma vez que se alterado, bloco seguinte conteria referência a um bloco inexistente. Dessa maneira, uma vez que o bloco é inserido na cadeia, os dados são vistos como permanentes e não podem ser alterados.

Criptografia assimétrica

A criptografia surge como a necessidade básica de alguns povos antigos transmitirem mensagens com estratégias de guerra, sem que seus inimigos conseguissem decifrá-las, caso capturassem essas mensagens. Nesse sentido, o primeiro grande modelo de criptografia existente foi a cifra de César, que utilizava o esquema de substituição de algarismos para embaralhar a mensagem desejada. Com o avanço científico nesta área, dois esquemas de criptografia se firmaram: a criptografia simétrica e a assimétrica. A primeira funciona basicamente com um par de chaves iguais, que realizam tanto o papel de criptografar quanto de descriptografar a mensagem. Isso, no entanto, abriu espaço para o problema de compartilhamento das chaves.

A criptografia assimétrica, ou também chamada de criptografia de chave pública, é um modelo de criptografia em que, diferentemente da criptografia simétrica, há duas chaves com papéis diferentes dentro da comunicação. A chave pública pode ser divulgada para todos os remetentes de uma mensagem. A chave privada, por sua vez, deve ser mantida em segredo pelo destinatário, pois somente ele deve ser capaz de decifrar a mensagem. Dessa forma, pode ser resolvido o problema de compartilhamento de chaves, já que a disponibilização da chave pública para todos os envolvidos na rede não enfraquece o sistema.

Existem, atualmente, diversos algoritmos de criptografia assimétrica. Dentre eles, o mais famoso é o RSA (Rivest-Shamir-Adleman), o qual utiliza esse tipo de criptografia para realizar transmissão de dados seguros. Nesse algoritmo, o poder de sua segurança é baseado no problema de fatoração, em que é muito difícil de decompor um número em dois fatores que são primos.

Além do RSA, também há os algoritmos que se baseiam em curvas elípticas para criptografar e descriptografar uma mensagem. Esses algoritmos, por sua vez, apresentam um grande diferencial com relação ao tamanho de suas chaves, o que reduz o espaço necessário para o seu armazenamento. Por exemplo, uma chave de apenas 256 bit utilizada pelo ECDSA tem o mesmo nível de segurança que a chave RSA de 3072 bits.

Assinatura digital

Uma assinatura digital é um esquema para verificar a autenticidade de mensagens, documentos digitais e legitimidade de transações financeiras. Ela recebeu esse nome porque faz analogia às assinaturas físicas feitas em documentos. A base de sua segurança está em seus esquemas de criptografia assimétrica, mencionados anteriormente. De maneira simples, assim como observado na Figura 1, esses esquemas apresentam duas etapas essenciais: uma de assinatura propriamente e uma de verificação. Na primeira etapa, uma função recebe como entrada a mensagem a ser assinada juntamente a chave privada, garantindo unicidade de que aquela chave é somente daquele remetente; na segunda etapa essa assinatura, juntamente com a chave pública, tornam-se entradas de uma nova função que responde de assinatura corresponde ao remetente da mensagem.

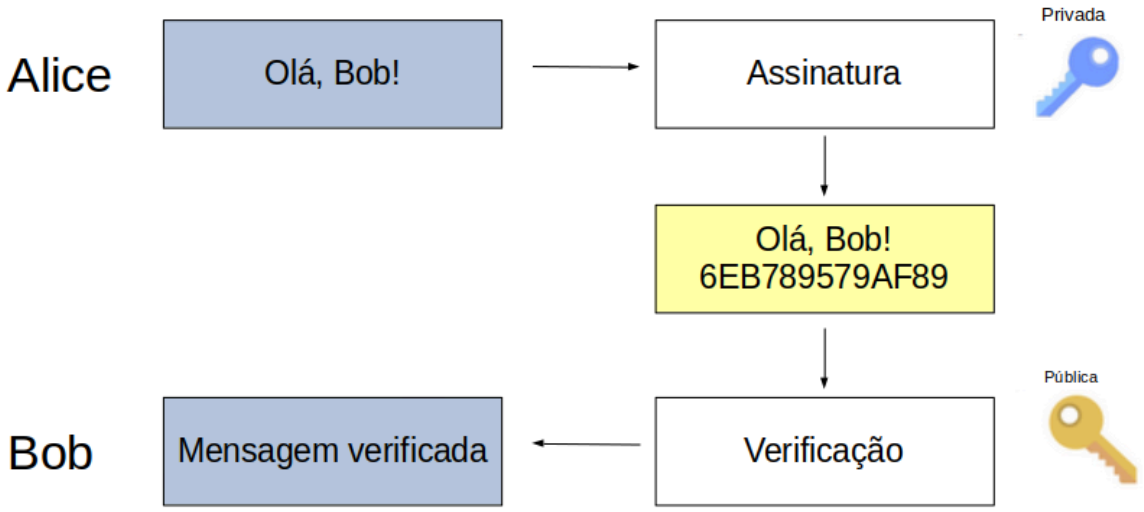

Figura 1: Assinatura digital

Algoritmo de Shor

O algoritmo de Shor, desenvolvido pelo matemático Peter Shor (SHOR, 1994; 1997) é um algoritmo quântico que permite encontrar fatores primos para um número N (composto inteiro e ímpar) em tempo polinomial (NIELSEN; CHUANG, 2010). Com as instruções deste algoritmo seria possível quebrar os programas de criptografia de chaves públicas, como o RSA, Campo Finito de Diffie-Hellman e a Curva Elíptica de Diffie-Hellman, dado um computador quântico suficientemente poderoso. O algoritmo de Shor é probabilístico, de modo que a probabilidade de erro de uma resposta pode ser decrementada por meio de repetições do algoritmo e, sendo a resposta verificável em tempo polinomial, pode ser obtida sem erros.

A parte clássica do algoritmo procura determinar os fatores primos de um número N ímpar e não primo a partir da escolha de um número randômico que é primo em relação a N, reduzindo o problema à determinação de ordem, processo passível de execução em um computador clássico. A parte quântica para encontrar o período r de a^x mod (N) é executada de modo eficiente em um computador quântico, por meio da Transformada de Fourier Quântica. (NIELSEN; CHUANG, 2010)

Síntese do Algoritmo de Shor

1. Escolher um número randômico $1 < a < N$
2. Computar máximo divisor comum MDC (a, N)
3. Se MDC (a, N) ≠ 1, então MDC é fator não trivial comum de N e um dos fatores foi encontrado. Atribua p = MDC(a,N), então q = N/p e a fatoração foi concluída
4. Senão, encontre o período r para $f(x) = a^x \bmod (N)$ (Inicia a parte quântica)
5. Se r for ímpar, vá para passo 1)
6. Se $a^{r/2} \equiv -1 \pmod N$, vá para passo 1)
7. Senão, r foi encontrado e os fatores são p = MDC ($a^{r/2} - 1$, N) e q= MDC ($a^{r/2} + 1$, N) e a fatoração foi concluída

Algoritmo de Grover

Algoritmo criado pelo cientista da computação Lov Grover, sendo empregado para buscar um dado elemento em uma lista não ordenada. Sua vantagem está no fato de se um computador clássico realiza essa tarefa em tempo N e o algoritmo de Grover a realiza em $\sqrt{N}$.

O alvo para ataque são aquelas blockchains que utilizam o Proof of Work (POW) como mecanismo de consenso. O POW funciona de forma que os nós (mineradores) tem que resolver um problema matemático gerando uma Hash com um determinado tamanho, neste caso, uma string que começa com uma certa quantidade de zeros.

Um minerador com um computador quântico é capaz de resolver o problema matemático muito mais rápido, numa velocidade quadrática. Mais do que isso, o minerador teria uma prova de trabalho da ordem de toda a rede, o que implicaria na capacidade de atacar qualquer bloco e alterá-lo.

3. Desenvolvimento

Bitcoin

Considerada a primeira moeda digital mundial descentralizada, Bitcoin surge com o propósito de realizar transações financeiras sem intermediários, evitando, também, que qualquer autoridade financeira manipule a emissão da moeda. Para isso, todas as transações são verificadas por todos usuários, que são gravadas, então, na blockchain.

O funcionamento da blockchain para a bitcoin é separado em dois atores: os usuários que realizam as transações e os mineradores que escutam essas transações para adicioná-las na cadeia de blocos. Para o usuário realizar uma transação é exigido, no mínimo, três chaves criptográficas. Uma chave pública do remetente (endereço do remetente); a chave privada do endereço remetente; o hash de uma chave pública (endereço do destinatário).

Já os mineradores, que são computadores especializados, são responsáveis por inserir uma sequência de transações dentro de um bloco que será adicionado na blockchain. Para isso, eles realizam cálculos matemáticos complexos para descobrir hashes criptográficos com propriedades específicas que garantem que o bloco adicionado na blockchain não foi adulterado. Uma das propriedades específicas é encontrar hash com um determinado número de zeros, por exemplo, 30 zeros no início do hash. Esse processo, que também é chamado de prova de trabalho, funciona da seguinte maneira: o minerador gera um número aleatório e o concatena com aquele bloco que deseja adicionar na blockchain. Caso o hash dessa concatenação contenha o número de zeros desejado, esse bloco é adicionado na blockchain, caso contrário, o minerador continua gerando novos números aleatórios.

Diante desta estrutura de funcionamento, a principal forma de ataque identificado é contra transações declaradas na rede que ainda não foram incorporadas a um bloco. Isso porque, enquanto uma transação nova não for colocada em um novo bloco da blockchain, a chave dessa conta está vulnerável a um atacante quântico. Assim, a partir desse momento, o atacante irá pegar a chave pública do remetente da transação e irá a derivar para encontrar a respectiva chave privada. Com essa chave em mãos, o atacante inicia uma transação concorrente para seu próprio endereço. Além disso, ele pode obter prioridade sobre a transação original, oferecendo uma taxa de mineração - uma taxa concedida aos mineradores

para obter prioridade na inclusão da sua transação dentro do bloco a ser adicionado - mais alta.

Ethereum

A segunda maior moeda digital, líder em número de desenvolvedores e projetos, surge, principalmente, como alternativa ao bitcoin. Como outras moedas digitais, ela é distribuída, permitindo realizar transferência entre indivíduos, sem a necessidade de uma terceira parte – como um banco ou uma empresa de remessa internacional.

Similarmente ao funcionamento das transações com moedas bitcoins, as transações com a moeda Ethereum utilizam carteiras associadas a um endereço específico (hash de uma chave pública). Nesse sentido, para realizar uma transação, os usuários precisam de suas credenciais (uma chave privada) para assinar digitalmente a transação e publicá-la na rede. Para verificar uma transação assinada, por sua vez, a chave pública associada é necessária. Com isso, a chave pública é transmitida juntamente com a transação. Com todos os dados necessários disponíveis, qualquer pessoa pode verificar se o legítimo proprietário dos fundos é quem criou a transação, sem expor a chave privada.

No entanto, há duas diferenças drásticas que afetam como os ataques quânticos vão impactar nos protocolos da criptomoeda. A primeira, é o uso de Proof of Stake (PoS) como forma de consenso ao invés de utilizar a prova de trabalho utilizada na bitcoin. Esse novo mecanismo seleciona aleatoriamente um dos computadores participantes do consenso para construir o bloco a ser adicionado na blockchain, e esse nó selecionado é chamado de verificador. Para que os verificadores selecionados atuem honestamente é necessário que "apostem" uma determinada quantia, assim, caso tentem agir de forma a prejudicar os outros participantes, essa quantia será debitada de sua carteira.

Outra diferença é que, enquanto o sistema da bitcoin recomenda fortemente gerar um par de chaves para cada transação, nas transações com Ethereum o par de chaves é o mesmo. Isso impacta ainda mais no ataque de transação descrito para bitcoin - ataque que se baseia no fato de que usuários que realizam uma transação precisam publicar a chave pública associada

ao endereço do remetente e, a partir disso, derivar rapidamente a chave privada para enviar uma transação concorrente dos mesmos fundos para o endereço do invasor.

Entretanto, no blockchain da criptomoeda Ethereum, o tempo médio para criação de um novo bloco é de cerca de 10 a 20 segundos. Isso é um tempo muito mais restrito do que o esperado para os computadores quânticos derivarem chaves privadas. Para isso, os invasores teriam que usar outros métodos de ataque adicionais para impedir que as transações sejam processadas rapidamente, ganhando tempo para realizar seu ataque quântico. Além disso, durante o período de pico de atividade, a rede pode ficar congestionada e as transações podem levar horas ou até dias para serem processadas. Isso ajuda os invasores a realizarem tal ataque e obter sua transação processada mais rapidamente, oferecendo uma taxa mais alta para os nós de processamento do que a transação original.

Perspectivas sobre a Criptografia Quântica e Pós-Quântica

Quantum key distribution (QKD), ou chave de segurança privada, é um protocolo cuja segurança pode ser provada e, por meio do qual, chaves privadas podem ser criadas entre duas partes para comunicação em um canal público. Os bits da chave podem ser usados para implementar um sistema de criptografia de chave privada clássico, possibilitando que as partes estabeleçam uma comunicação segura. O requisito para QKD é o de que qubits sejam comunicados através do canal público com uma taxa de erro inferior a um determinado limiar.

A segurança da chave resultante é garantida pelas propriedades da informação quântica. A ideia básica é a de que, considerando Alice e Bob como as partes comunicantes, a parte intrusa (no caso, Eva) não consegue obter qualquer informação dos qubits transmitidos entre Alice e Bob sem perturbar o estado destes. A partir do teorema de não clonagem, Eva não pode clonar os qubits de Alice e, dado que o ganho de informação implica em perturbação, qualquer tentativa de distinguir entre estados quânticos não ortogonais, o ganho de informação só é possível com introdução da perturbação no sinal (NIELSEN, M. A.; CHUANG, 2010)

O QKD consiste em uma tecnologia de criptografia quântica que difere das chaves de criptografia convencionais que são baseadas em métodos matemáticos complexos. A segurança de QKD é baseada no preceito da mecânica quântica de que o processo de medição

de um sistema quântico, em geral, gera perturbações neste. Ainda que o QKD não seja utilizado para transmitir mensagens em si, este pode ser usado juntamente com qualquer algoritmo de criptografia para encriptar a mensagem que pode, então, ser considerada provavelmente segura (CUI et al, 2020).

Funciona através de transmissão de fótons por cabos de fibra óptica entre os comunicadores. Cada fóton está em um estado quântico aleatório e, juntos, estes formam uma sequência de uns e zeros, os qubits. No final do percurso, os fótons passam por uma fenda e pegam uma abertura aleatória. Aqueles que foram conduzidos ao detector formam uma sequência única de bits que podem ser usados como uma chave para criptografar dados.

Alguns desafios para este método são a sua integração à infraestrutura local e a distância que os fótons possam percorrer. O QKD é, em teoria, totalmente seguro, mas uma falha ou aberração nos detectores de fótons podem expor o sistema a vulnerabilidades, além disso, na fibra óptica atual, os fios são capazes de de transportarem fótons por pouco mais de 100 km.

A Figura 2 apresenta alguns exemplos de Criptografia Quântica

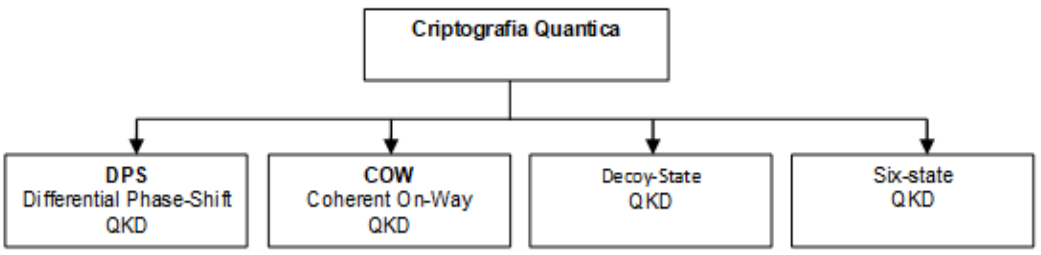

Figura 2: Criptografia Quântica

A criptografia Pós-Quântica é voltada para resistir aos ataques de criptoanálise que poderiam ser realizados por meio de computadores quânticos suficientemente poderosos (BERNSTEIN; 2009). Atualmente, seu desenvolvimento é baseado no tratamento de problemas matemáticos como fatoração de inteiros, logaritmos discretos e logaritmos discretos de curva elíptica. Estes métodos precisam garantir integridade dos dados e

confidencialidade, enquanto resistem ou previnem ataques. A Figura 3 apresenta alguns dos exemplos desenvolvidos para Criptografia Pós-Quantica.

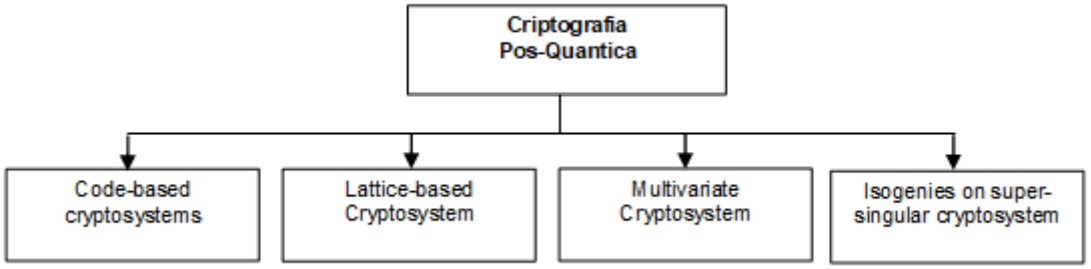

Figura 3: Criptografia pós-quântica

4. Conclusão

As maiores empresas globais estão investindo fortemente em modelos de computação quântica. Dentre elas, IBM, Google e Microsoft são os maiores exemplos do investimento em computadores quânticos, capazes de realizar cálculos e simulações que seriam impossíveis ou computacionalmente desgastantes de serem efetuadas em um tempo razoável por computadores clássicos. No entanto, a maioria dos computadores quânticos existentes exigem muito espaço precisa ser resfriado em baixas temperaturas.

Desse modo, uma das áreas que mais tem se dedicado parte do estudo científico é a de algoritmos quânticos. O algoritmo Shor, - que resolve a fatoração de números primos- e o algoritmo de Grover - que realiza a busca em um banco de dados desordenado - são os algoritmos mais famosos existentes hoje em dia.

Métodos pós Criptografia Quântica têm sido desenvolvidos diante das vulnerabilidades às máquinas quânticas, porém ainda se encontra em estágio inicial e há também a dificuldade prática de implementá-los conforme a teoria.

Este trabalho buscou trazer os principais ataques existentes com esses algoritmos dentro do contexto das criptomoedas que utilizam o esquema de blockchain para seu funcionamento. Para isso, foram revisados os principais conceitos necessários para a compreensão do funcionamento de uma blockchain, como o que são criptografia de chave pública, assinaturas digitais, funções de hash e prova de trabalho.

5. Referências

BERNSTEIN, D. J. Introduction to post-quantum cryptography. In **Post-Quantum Cryptography**. BERNSTEIN, D. J.; BUCHMAN,· J.; DAHMEN, E. , Editors. Springer, 2009.

CUI, Wei; Tong Dou e Shilu Yan, Threats and opportunities: Blockchain meets Quantum Computation. In 39th Chinese Control Conference (CCC), 2020, Shenyang, China. **Proceedings …** pp. 5822-5824, 2020.

GILLIS, Alexander. Quantum key distribution (QKD). TechTarget. 2022. Disponível em: https://www.techtarget.com/searchsecurity/definition/quantum-key-distribution-QKD. Acesso em: 18 de Dezembro de 2022.

KEARNEY, Joseph J.; Carlos A. Pereze-Delgado, Vulnerability of Blockchain Technologies to Quantum Attacks, 2021.

KIKTENKO, E.O.; POZHAR N.O.; ANUFRIEV, M.N. A.S., TRUSHECHKIN, R.R YUSUNOV, Y.V. KUROCHKIN, A.I LVOVSKY E A.K. FEDOROV, Quantum-secured Blockchain, 2018.

NIELSEN, M. A.; CHUANG, I. L. **Quantum Computation and Quantum Information**: 10th Anniversary Edition, 10th ed, Cambridge University Press, 2010.

SHOR, P. W. Algorithm for Quantum Computation: Discrete Logarithms and Factoring".In: **Symposium on Foundations of Computer Science**, 1994.

SHOR, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. **SIAM J. Comput**. V. 26, p 1484–1509, 1997.

SHOR, P. W. ; PRESKILL, J. Simple proof of security of the BB84 quantum key distribution protocol, **Phys. Rev. Letters**., 85: 441-444, 2000.