Poznan University of Technology

Blockchain Technology And Quantum Computation Quantum Computing

Jakub Piotr Hamerliński

Blockchain Technology And Quantum Computation Quantum Computing

01. Introduction to quantum computing: quantum bits, quantum gates, quantum circuits
02. Theoretical foundations of quantum cryptography: BB84 protocol, E91 protocol
03. Limitations of classical cryptography and the need for quantum cryptography
04. Quantum algorithms, including Shor's algorithm and Grover's algorithm
05. Quantum attacks on blockchain technology

Introduction to quantum computing

Quantum Computing

Introduction to quantum computing

Quantum computing is an emerging field that utilizes principles from quantum mechanics to process and manipulate information. Unlike classical computers that use bits to represent and process data, quantum computers employ quantum bits, or qubits, as the fundamental units of information.

Quantum Computing

Introduction to quantum computing

01. Quantum Bits (Qubits): A qubit is the basic unit of quantum information. While a classical bit can be in one of two states, 0 or 1, a qubit can exist in a superposition of both states simultaneously. This means that a qubit can represent not just 0 or 1, but also any combination of both states. The state of a qubit is described by a mathematical object called a quantum state vector, which is a complex vector in a two-dimensional vector space.

Quantum Computing

Introduction to quantum computing

02. Quantum Gates: Quantum gates are analogous to classical logic gates and are used to manipulate qubits. They perform operations on qubits, transforming their quantum state. Quantum gates are represented by matrices, and their action on a qubit is described by matrix multiplication. These gates can be used to perform various operations, such as changing the probability amplitudes of a qubit, entangling multiple qubits, or performing quantum logic operations.

Quantum Computing

Introduction to quantum computing

03. Quantum Circuits: Quantum circuits are composed of quantum gates connected in a specific arrangement to perform quantum computations. They are analogous to classical electronic circuits that manipulate classical bits. In a quantum circuit, qubits are initialized to a known state, quantum gates are applied to manipulate the qubits, and the final state is measured to obtain the desired output. The sequence of gates and their connections in a quantum circuit determine the computation being performed.

Quantum Computing

Introduction to quantum computing

Quantum computing offers the potential to solve certain problems exponentially faster than classical computers. It has applications in fields like cryptography, optimization, simulation of quantum systems, and machine learning. However, quantum computing is still in its early stages, and building practical and scalable quantum computers poses significant technical challenges.

It's important to note that this introduction provides a high-level overview of quantum computing concepts. The field is vast and requires a deeper understanding of quantum mechanics, linear algebra, and other mathematical concepts to explore its complexity fully.

Theoretical foundations of quantum cryptography

Quantum Computing

Theoretical foundations of quantum cryptography

BB84 Protocol: The BB84 protocol, named after its inventors Charles Bennett and Gilles Brassard in 1984, is one of the earliest and most widely studied quantum cryptographic protocols. It enables two parties, traditionally referred to as Alice (the sender) and Bob (the receiver), to establish a secure shared key over an insecure communication channel.

Quantum Computing

Theoretical foundations of quantum cryptography

Here's a high-level overview of the BB84 protocol:

01. Alice prepares a string of randomly generated qubits, each representing one of four possible states: {$|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$ (basis states).
02. For each qubit, Alice randomly chooses one of two bases, either the standard basis ($|0\rangle$, $|1\rangle$) or the Hadamard basis ($|+\rangle$, $|-\rangle$), and measures the qubit in that basis.
03. Alice sends the prepared qubits to Bob over the insecure channel.
04. Bob randomly chooses a basis for each received qubit and measures them accordingly.
05. Alice and Bob publicly announce the bases they used for each qubit but not the measurement results.
06. They compare a subset of their measurement results to check for errors. If the error rate is below a certain threshold, they keep the corresponding bits as the shared key.

Quantum Computing

Theoretical foundations of quantum cryptography

The security of the BB84 protocol lies in the fact that any attempt to eavesdrop or intercept the qubits by an adversary, traditionally referred to as Eve, will introduce errors into the system. These errors will be detected during the error rate comparison, indicating the presence of an eavesdropper. If no eavesdropping is detected, Alice and Bob can use error correction and privacy amplification techniques to obtain a secure shared key.

Quantum Computing

Theoretical foundations of quantum cryptography

E91 Protocol: The E91 protocol, proposed by Artur Ekert in 1991, is a protocol for secure quantum key distribution that relies on the phenomenon of quantum entanglement. Unlike the BB84 protocol, which is based on the exchange of single qubits, the E91 protocol uses pairs of entangled qubits to establish a shared key between Alice and Bob.

Quantum Computing

Theoretical foundations of quantum cryptography

01. Here's a high-level overview of the E91 protocol:
02. Alice and Bob each generate a pair of entangled qubits, typically using a source of entangled photon pairs.
03. Alice and Bob randomly choose one of two measurement bases for each qubit, similar to the BB84 protocol.
04. They send their respective qubits to a central location, traditionally referred to as Charlie.
05. Charlie randomly chooses a subset of the received qubits and announces the measurement bases used for those qubits.
06. Alice and Bob publicly announce the remaining measurement bases for all their qubits.
07. Alice and Bob compare their measurement results for the qubits with matching bases to establish a subset of correlated bits.
08. They perform error correction and privacy amplification on the correlated bits to obtain a secure shared key.

Quantum Computing

Theoretical foundations of quantum cryptography

The E91 protocol relies on the non-local correlations between entangled qubits, known as quantum entanglement, to establish a secure key. Any attempt to intercept the entangled qubits would disrupt the correlations and be detectable during the comparison phase.

Both the BB84 and E91 protocols provide a means for secure key distribution, allowing two parties to establish a shared key without the need for a pre-existing shared secret. These protocols leverage the properties of quantum mechanics to ensure the security of the communication channel, making it difficult for an eavesdropper to gain information without detection.

Limitations of classical cryptography and the need for quantum cryptography

Quantum Computing

Limitations of classical cryptography and the need for quantum cryptography

Classical cryptography, which is based on mathematical algorithms and computational complexity, has been widely used to secure communication and protect sensitive data. However, classical cryptography faces certain limitations that make it vulnerable to attacks in the era of increasingly powerful computers and advancing technologies. Here are some key limitations of classical cryptography:

Quantum Computing

Limitations of classical cryptography and the need for quantum cryptography

01. Computational Power: Classical cryptographic algorithms are designed to rely on the computational difficulty of certain mathematical problems, such as factoring large numbers or solving discrete logarithm problems. However, the advent of powerful computers and the potential future development of quantum computers could render these problems solvable in significantly less time. This poses a threat to the security of classical cryptographic algorithms.

Quantum Computing

Limitations of classical cryptography and the need for quantum cryptography

02. Security Assumptions: Classical cryptography relies on the assumption that certain mathematical problems are difficult to solve, such as factoring large numbers or finding discrete logarithms. If new mathematical techniques or algorithms are discovered that can efficiently solve these problems, the security of classical cryptographic schemes can be compromised.

Quantum Computing

Limitations of classical cryptography and the need for quantum cryptography

03. Key Distribution: Secure key distribution is a fundamental requirement in cryptography. Classical key distribution methods often rely on secure channels or pre-shared keys, which can be challenging to establish and maintain securely, especially in large-scale communication networks. Quantum cryptography offers a unique advantage in terms of secure key distribution, as it can provide provable security based on the laws of quantum physics.

Quantum Computing

Limitations of classical cryptography and the need for quantum cryptography

04. Information Leakage: Classical cryptographic systems are vulnerable to various types of attacks, including eavesdropping, interception, and tampering. Adversaries can exploit vulnerabilities in the communication channels, compromise encryption keys, or use advanced cryptanalytic techniques to break the encryption. Quantum cryptography, on the other hand, provides mechanisms that detect eavesdropping attempts, ensuring the integrity and confidentiality of transmitted data.

Quantum Computing

Limitations of classical cryptography and the need for quantum cryptography

Quantum cryptography addresses these limitations by leveraging the principles of quantum mechanics to provide strong security guarantees. Quantum cryptography offers the following advantages:

01. Quantum Key Distribution (QKD): QKD protocols, such as the BB84 and E91 protocols, enable the secure distribution of encryption keys between two parties, even in the presence of an eavesdropper. The security of QKD is based on fundamental physical properties, such as the no-cloning theorem and the uncertainty principle, making it highly resistant to computational attacks.

Quantum Computing

Limitations of classical cryptography and the need for quantum cryptography

02. Detection of Eavesdropping: Quantum cryptography provides a mechanism to detect any attempt to intercept or eavesdrop on the transmitted quantum information. Any eavesdropping activity will introduce detectable disturbances in the quantum states, alerting the communicating parties to potential security breaches.

Quantum Computing

Limitations of classical cryptography and the need for quantum cryptography

03. Information-Theoretic Security: Quantum cryptography offers information-theoretic security, which means that the security of the system is based on the fundamental laws of physics and not on computational assumptions. This provides a higher level of confidence in the security of the communication, even against attacks from future technologies.

Quantum algorithms, including Shor's algorithm and Grover's algorithm

Quantum Computing

Quantum algorithms, including Shor’s algorithm and Grover’s algorithm

Quantum algorithms are algorithms specifically designed to be executed on quantum computers, taking advantage of the principles of quantum mechanics to solve computational problems more efficiently than classical algorithms. Two prominent examples of quantum algorithms are Shor’s algorithm and Grover’s algorithm.

Quantum Computing

Quantum algorithms, including Shor's algorithm and Grover's algorithm

01. Shor's Algorithm: Shor's algorithm, developed by Peter Shor in 1994, is a quantum algorithm that efficiently solves the factorization problem. The factorization problem involves finding the prime factors of a composite number. In classical computing, factoring large numbers becomes exponentially more difficult as the size of the number increases, making it computationally infeasible for very large numbers.

Quantum Computing

Quantum algorithms, including Shor's algorithm and Grover's algorithm

Shor's algorithm, on the other hand, leverages the quantum properties of superposition and entanglement to perform efficient factorization. The algorithm can factorize large numbers in polynomial time, which has significant implications for breaking cryptographic systems that rely on the computational difficulty of factoring large numbers, such as RSA encryption. Shor's algorithm poses a potential threat to the security of widely deployed classical cryptographic systems.

Quantum Computing

Quantum algorithms, including Shor's algorithm and Grover's algorithm

02. Grover's Algorithm: Grover's algorithm, proposed by Lov Grover in 1996, is a quantum algorithm that provides a speedup for searching an unsorted database. In classical computing, searching an unsorted database requires, on average, a time complexity proportional to the number of items in the database.

Quantum Computing

Quantum algorithms, including Shor’s algorithm and Grover’s algorithm

Grover’s algorithm, however, offers a quadratic speedup compared to classical algorithms. It uses the principles of quantum superposition and interference to search an unsorted database with a time complexity of approximately the square root of the number of items. This algorithm is particularly useful for problems like database search, optimization, and finding solutions in an unstructured search space.

Quantum Computing

Quantum algorithms, including Shor’s algorithm and Grover’s algorithm

While Shor’s algorithm and Grover’s algorithm are significant advancements in quantum computing, it’s important to note that their practical implementation faces several challenges. These challenges include the need for error correction to mitigate the effects of noise and decoherence, as well as the requirement for large-scale, fault-tolerant quantum computers to execute these algorithms with sufficient precision and accuracy.

Quantum Computing

Quantum algorithms, including Shor's algorithm and Grover's algorithm

Despite these challenges, these quantum algorithms demonstrate the potential of quantum computing to solve specific problems more efficiently than classical counterparts, which has implications for cryptography, optimization, and other computational domains. Ongoing research and development in quantum computing aim to overcome these challenges and explore the broader applicability of quantum algorithms in various fields.

Quantum attacks on blockchain technology

Quantum Computing

Quantum attacks on blockchain technology

Quantum computing has the potential to pose a significant threat to certain aspects of blockchain technology, particularly in the context of cryptographic algorithms used to secure blockchains. While quantum computers are not yet powerful enough to break commonly used cryptographic algorithms, their development and progress could potentially undermine the security of blockchain systems in the future. Here are a few areas where quantum attacks could impact blockchain technology:

Quantum Computing

Quantum attacks on blockchain technology

01. Public Key Cryptography: Blockchain technology relies heavily on public key cryptography for secure transactions and digital signatures. Algorithms such as RSA and Elliptic Curve Cryptography (ECC) are widely used in blockchain systems. However, Shor's algorithm, a quantum algorithm discussed earlier, has the potential to efficiently factorize large numbers and solve the discrete logarithm problem, which are the foundation of the security for RSA and ECC respectively. If large-scale, fault-tolerant quantum computers become a reality, they could break the security of these cryptographic algorithms and compromise the integrity of blockchain systems.

Quantum Computing

Quantum attacks on blockchain technology

02. Quantum-resistant Cryptography: To mitigate the risks of quantum attacks, researchers have been developing quantum-resistant cryptographic algorithms, also known as post-quantum cryptography. These algorithms are designed to withstand attacks from both classical and quantum computers. Many post-quantum cryptographic schemes are currently being studied, including lattice-based cryptography, code-based cryptography, multivariate cryptography, and others. Integrating these quantum-resistant cryptographic algorithms into blockchain systems before quantum computers become a threat is crucial to maintaining the security of blockchain technology in the long term.

Quantum Computing

Quantum attacks on blockchain technology

03. Chain Reorganization Attacks: Quantum computers may also have implications for the consensus mechanisms employed by blockchains, such as proof-of-work (PoW) or proof-of-stake (PoS). With sufficient computational power, a quantum attacker could potentially perform chain reorganization attacks. These attacks involve attempting to replace blocks in the blockchain with an alternative branch, leading to double-spending or other disruptive actions. Quantum computers could potentially speed up the computational processes required for such attacks, making them more feasible.

Quantum Computing

Quantum attacks on blockchain technology

It's important to note that the timeline for the development of practical, large-scale quantum computers is uncertain, and there is ongoing research and development in both quantum computing and post-quantum cryptography. Efforts are being made to explore quantum-resistant cryptographic solutions that can be integrated into blockchain systems to ensure their long-term security.

Quantum Computing

Quantum attacks on blockchain technology

Blockchain developers and organizations are actively monitoring advancements in quantum computing and researching strategies to address potential quantum threats. The goal is to evolve blockchain technology to be resistant to quantum attacks by implementing quantum-resistant cryptographic algorithms and preparing for the quantum era.

Sources

Sources

Introduction to Quantum Computing:

01. "Quantum Computing for Computer Scientists" by Noson S. Yanofsky and Mirco A. Mannucci.
02. "Quantum Computing: A Gentle Introduction" by Eleanor G. Rieffel and Wolfgang H. Polak.
03. "Quantum Computing: An Overview" by Andris Ambainis.
04. "Quantum Computing: A Short Course from Theory to Experiment" by Joachim Stolze and Dieter Suter.

Sources

Theoretical Foundations of Quantum Cryptography:

01. "Quantum Cryptography: Public Key Distribution and Coin Tossing" by Gilles Brassard and Louis Salvail.
02. "Introduction to Quantum Information Science" by Vlatko Vedral.
03. "Quantum Information Theory and Quantum Statistics" by Masahito Hayashi.
04. "Quantum Cryptography and Secret-Key Distillation" by Stefano Pirandola.

Sources

Limitations of Classical Cryptography and the Need for Quantum Cryptography:

01. "Post-Quantum Cryptography" by Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen.
02. "Quantum-Safe Cryptography" by Mark P. Wilding and David J. Wales.
03. "Breaking RSA Encryption with a Quantum Computer" by Peter Shor.
04. "Quantum Cryptanalysis of Hash Functions and Symmetric Ciphers" by Willi Meier and Christof Paar.

Sources

Quantum Algorithms, including Shor’s Algorithm and Grover’s Algorithm:

01. "Quantum Computing: An Applied Approach" by Jack D. Hidary.
02. "Quantum Computing: From Linear Algebra to Physical Realizations" by Mikio Nakahara and Tetsuo Ohmi.
03. "Quantum Computation and Quantum Information" by Michael A. Nielsen and Isaac L. Chuang.

Sources

Quantum Attacks on Blockchain Technology:

01. "Quantum Attacks on Bitcoin, and How to Protect Against Them" by Divesh Aggarwal, Gavin K. Brennen, Troy Lee, Miklos Santha, and Marco Tomamichel.
02. "Quantum Attacks on Public-Key Cryptosystems" by Tanja Lange and Daniel J. Bernstein.
03. "Quantum Attacks on Public-Key Cryptosystems" by Daniel J. Bernstein.
04. "Post-Quantum Bitcoin" by Aggelos Kiayias, Nikos Leonardos, and Dionysis Zindros.

Task

Task

Quantum Cryptography Challenge

This exercise is divided into three main parts:

01. Quantum Circuit Design: You will design and implement a simple quantum circuit using Q.js. Use your knowledge of quantum bits, gates, and circuits to accomplish this.
02. Encryption and Decryption: You will use the BB84 protocol to encrypt a short message and then decrypt it, using your designed quantum circuit. You will need to understand the theoretical foundations of the BB84 protocol to do this correctly.

Task

Quantum Cryptography Challenge

03. Quantum Attacks: The last part of the exercise involves trying to crack a message that another group has encrypted using their quantum circuit. Use your knowledge of quantum algorithms, like Shor's and Grover's, to attempt to break the encryption. You will also need to understand the limitations of classical cryptography and why quantum cryptography is needed.
04. Quantum Attacks on Blockchain: For an extra challenge, discuss potential vulnerabilities that quantum attacks could exploit in blockchain technology. You could either discuss this theoretically or, if feasible, demonstrate a simple example using your quantum circuit.

Task

Quantum Cryptography Challenge

Guidelines:

01. You can work in pairs, groups of 3, or 4.
02. The exercise should take approximately 30 minutes to complete.
03. You will need access to a computer with internet access to use the Q.js quantum circuit simulator.

Task

Quantum Cryptography Challenge

Deliverables:

01. A Q.js file of your designed quantum circuit.
02. A short report explaining your circuit design, how the encryption and decryption process works, your strategy for attempting to crack the encryption, and your discussion on quantum attacks on blockchain technology.

Task

Quantum Cryptography Challenge

Example Solution:

Here's how you could accomplish each part of the exercise using Q.js, based on an example from dev.to:

01. Quantum Circuit Design: Download the build folder from the Q.js library repo on GitHub. Next, create a new JavaScript file in the same folder. Inside this JavaScript file, create a circuit object in text format, and then append this circuit to the webpage's body using the toDom() method. As a simple example, you might create a Bell state circuit. A Bell state is a specific quantum state of two qubits that are in maximum entanglement. This circuit is designed using a Hadamard gate (H) and a Controlled-Not gate (CX).

Task

Quantum Cryptography Challenge

02. Encryption and Decryption: Once the quantum circuit has been implemented, you can simulate the circuit and display the results on your webpage using the report$() method. This method returns the results as a string, which represents the probability of getting a particular combination as the output. To encrypt a message, use the BB84 protocol with the Bell state circuit you've created. You can represent each bit of the message with a specific state of the qubits. For decryption, measure the state of the qubits, convert the state back into bits, and then convert the bits back into the original message.

Task

Quantum Cryptography Challenge

03. Quantum Attacks: To "attack" the encrypted message, you can attempt to measure the state of the qubits in different bases. If you measure in the correct basis, you will get the same state that was used for encryption, and you can then decrypt the message. If you measure in the wrong basis, you will get a random result, due to the no-cloning theorem in quantum mechanics.
04. Quantum Attacks on Blockchain: In this part of the exercise, discuss or demonstrate how a quantum computer might attack a blockchain. One example is using Shor's algorithm to find the factors of a large number,which is a key part of the encryption in most blockchains. Discuss how this would be done theoretically, or if feasible, demonstrate it using the Q.js library. This is just a simple example, and the actual implementation could be more complex depending on your knowledge and the level of complexity you want for the exercise. Note that working with quantum circuits, encryption, and attacks can be quite complex, so make sure that you have a solid understanding of the underlying concepts before attempting this exercise.

Thank you

Feel free to reach me via LinkedIn

Fin