Analysis on Quantum Mechanics and the Impact of Quantum Computing on Blockchain Security

Authors：Eric Fu, Jame Su, Guin Peng, Caroline Feng, Jill Chow

Translator: Yicheng Chen, Page Xu, Johnny Huang, Patrick Velleman

Abstract

Quantum Mechanics is not only the most significant component of modern physics, but it is also responsible for technological advances that influence our everyday lives. As one of the up and rising industries, blockchain is also under the impact of quantum mechanics. To be more specific, quantum computing can post threats to cryptography algorithms that blockchains are now using. This report will introduce some basic concepts of Quantum Mechanics and discuss how the applications of Quantum Mechanics can affect blockchain security with the example of Bitcoin. In the meantime, GateChain is also seeking its innovative approach to defend against Quantum Computing attacks.

Key Takeaways:

- In the late 19th century, as scientists discovered phenomena that could not be explained by classical mechanics, the idea of “quanta” was postulated. Theories such as Schrödinger’s wave mechanics and Heisenberg’s matrix mechanics were proven as the study of quantum physics gradually established

- Nowadays, quantum mechanics has been applied in many fields. The technology of Quantum Key Distribution (QKD), which involves particle polarization and uncertainty principle in quantum mechanics, is one of the most advanced cryptographic protocols.

- With the improvement of modern scientific research, the computational power of traditional computers can no longer meet the demand of simulations at the microscopic level. Therefore, the need for high-performance quantum computers designed based on quantum mechanics emerges. Many tech giants and governments have already entered the race of next-generation computing.

- Quantum computing has posed severe threats to blockchain cryptography, wherein hash algorithm and other private keys encryption algorithms are likely to be cracked. In particular, Grover’ s algorithm and Shor’ s algorithm are proven to be able to crack the elliptic curve cryptography and SHA256 algorithm efficiently.

- Currently, using quantum-proof algorithms is an effective way to resist quantum computing attacks, but it is likely to cause the problem of node centralization. In the meantime, GateChain will try to discover innovative approaches to defend itself against quantum computing attacks while maintaining network security and capacity.

Content

1 Classical Mechanics & Quantum Mechanics

1.1 Introduction to Classical Mechanics

Classical mechanics is the study of the motion of macroscopic objects and the forces that affect them. It is called Newtonian mechanics since it is built on Isaac Newton’s laws of motion.

In the late 19th century, as technology advanced, scientists were able to measure with greater precision and observed strange phenomena that classical mechanics failed to explain. Two of these failures led to the proposal of the Special Theory of Relativity and Quantum Hypothesis.

1.2 The Failure of Classical Mechanics

1.2.1 The Denial of Ether: Einstein’s Special Relativity

Ether Theories propose that “Ether,” a substance that exists throughout the entire space, is a transmission medium for the propagation of electromagnetic forces.

However, in 1905, based on the fact established by the Michelson-Morley experiment, Albert Einstein concluded that the velocity of light is constant regardless of motions of the earth; hence the laws of physics are the same for all systems that move uniformly relative to one another. He also stated that the transmission of light and electromagnetic waves does not need any medium, suggesting that Ether does not exist.

1.2.2 Blackbody Radiation Explained: The Proposal of Quantum Hypothesis

At the end of the 19thcentury, much more attention was given to the study of light. In the meantime, scientists had found more experimental phenomena that could not be adequately explained by classical physics. One of them was the disagreement between theory and experiment in the ultraviolet region of the blackbody spectrum.

Attempts to explain blackbody radiation include the famous but not completely successful Wien’ s Law and Rayleigh-Jeans law. For example, according to Rayleigh-Jeans law, the intensity at short wavelengths should go to infinity, but in reality, it drops to zero instead. This result was called the “ultraviolet catastrophe.”

In 1900, Max Planck discovered an equation that could describe the blackbody spectrum..

$$u(v,T)=\frac{4\pi}{c}I(v,T)=\frac{8\pi hv^3}{c^3}\frac{1}{e^{\frac{hv}{kT}}-1}$$

This equation describes the relationship between the rate and the frequency of electromagnetic radiation emitted by a blackbody under a temperature T . However, classical physics could not explain the results Planck found. Therefore, he came up with the constant h(now known as the “Planck’ s Constant”), and postulated that that energy does not flow evenly but instead is discharged in discrete packets – “quanta.” The postulate is quantized by the equation below.

$$\epsilon_{n=nhv} \ (n=1,2,3,\ldots)$$

This equation indicates that the energy of the radiating oscillators in the blackbody could take on only specific, quantized energy, which is an integer multiple of hv . This revolutionary theory of energy was considered the birth of quantum physics (or quantum mechanics) and paved the way for more discoveries.

2 Quantum Mechanics

As researches on quantum physics continued to advance, more applications of quantum physics are made possible in the real world. This chapter will introduce some of the fundamental theories in quantum mechanics and provide insights on how quantum mechanics is established.

2.1 Introduction to Quantum Mechanics

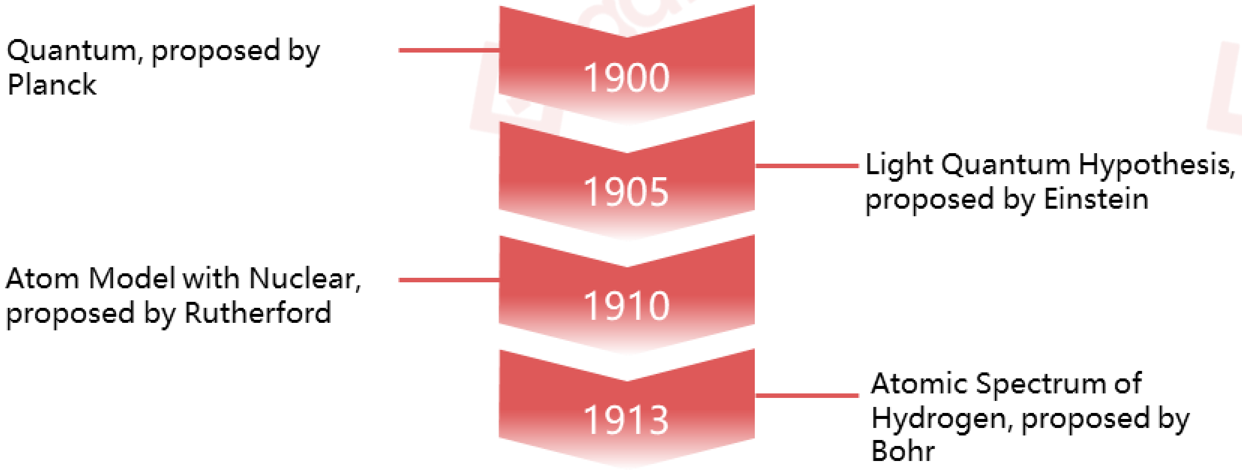
2.1.1 Definition

Quantum mechanics is the branch of physics that studies the motion and interaction of subatomic particles. It describes the structure, properties, and components of molecules, atoms and other particles on the atomic and subatomic level.

2.1.2 The Development of Quantum Mechanics

Planck’ s discovery had instigated more theories in the new field. The period from 1900 to 1925, before De Broglie proposed the theory of electron waves, is referred to as the pre-quantum mechanical period.

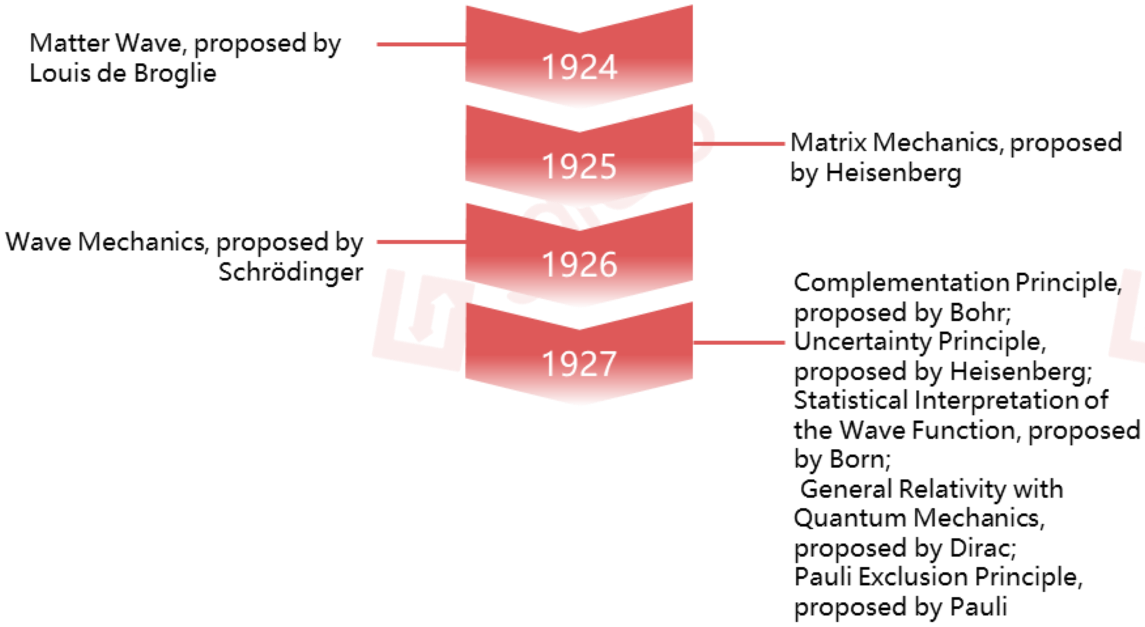
- Pre-Quantum Mechanical Theories


Quantum, proposed by Planck
1900
1905
Light Quantum Hypothesis, proposed by Einstein
Atom Model with Nuclear, proposed by Rutherford
1910
1913
Atomic Spectrum of Hydrogen, proposed by Bohr

The above chart shows the theories proposed during the pre-quantum mechanical period. These unconventional and innovative theories laid the foundation for the later establishment of quantum mechanics.

- The Establishment of Quantum Mechanics

Following the groundbreaking theory of electron wave proposed by De Broglie, the study of physical mechanics has gradually established itself. Many physicists have started to involve themselves in researches at the atomic and subatomic levels, while the theoretical structure of quantum mechanics is continuing to mature.

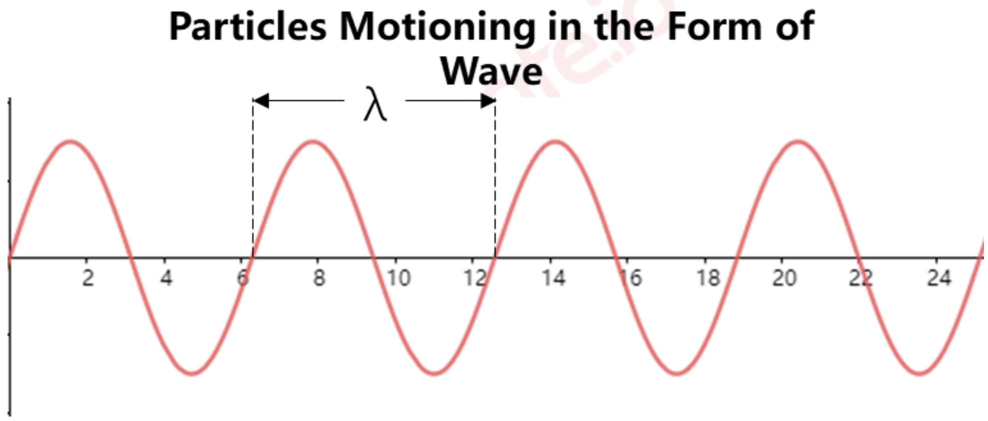

Matter Wave, proposed by Louis de Broglie
1924
1925
Matrix Mechanics, proposed by Heisenberg
Wave Mechanics, proposed by Schrödinger
1926
1927
Complementation Principle, proposed by Bohr;
Uncertainty Principle, proposed by Heisenberg;
Statistical Interpretation of the Wave Function, proposed by Born;
General Relativity with Quantum Mechanics, proposed by Dirac;
Pauli Exclusion Principle, proposed by Pauli

2.2 Fundamental Theories of Quantum Mechanics

Throughout the development of quantum mechanics, there have been many invaluable pieces of research and discoveries. Optical quantum hypothesis, Heisenberg military formation mechanics and the uncertainty principle, Schrödinger’ s wave mechanics and Copenhagen interpretations are the representatives amongst others. The following sessions will briefly introduce these fundamental theories in quantum mechanics.

2.2.1 Einstein and the Photoelectric Effect

Einstein was greatly inspired by Planck’ s postulation and proposed that similar to energy, light also travels in packets, and light is composed of particles called “Photon.” He also believed that light not only exhibits wave properties of interference, diffraction, and polarization, it also has particle properties of volume, density and mass.



Graph: Gate.io Research

As shown in the graph, the photons travels as waves.

2.2.2 Heisenberg’ s Matrix Mechanics and the Uncertainty Principle

After Einstein’ s quantum theory of light, Heisenberg proposed Matrix Mechanics and the Uncertainty Principle.

- Matrix Mechanics

  Matrix Mechanics is a formulation of quantum mechanics created by Werner Heisenberg, Max Born, and Pascual Jordan, published in a groundbreaking paper in 1925.

- Uncertainty principle

  Besides the uncertainty principle, Heisenberg also articulated another theory - the uncertainty principle. It states that the position and momentum of a participle cannot both be precisely determined simultaneously. The position of a particle is x, and the momentum P_x, then:

$$\Delta x \Delta P_x \geq \frac{h}{4\pi}$$

Δx is the position of the particle, ΔP_x is the momentum of the particle, h is Planck’ s constant. According to the equation, the more precise Δx is, the more uncertain ΔP_x will be, and vice versa. The same relation can be found between energy and time of a particle:

$$\Delta E \Delta t \geq \frac{h}{4\pi}$$

ΔE is the energy of the particle while Δt is the time. It appears that the uncertainty principle also applies in this case.

- The discovery of J/psi particle

The discovery of J/psi particle further proves the uncertainty of energy can be calculated. Discovered by team led by Samuel Ting at Brookhaven National Laboratory in 1974, the J/psi particle is a flavor-neutral meson with a mean lifetime of about thousand times longer than expected. The calculation of the lifetime of the particle is as follows:

$$\Delta t \geq \frac{h}{4\pi \Delta E} = \frac{6.63 \times 10^{-34}}{4\pi \times 6.3 \times 10^{4} \times 1.6 \times 10^{-19}} = 1.0 \times 10^{-20} s$$

According to the above formula, given ΔE, the lifetime of the particle Δt is greater than or equal to$1.0 \times 10^{-20} s$.

2.2.3 Schrödinger' s Wave Mechanics

Erwin Schrödinger originally developed wave mechanics in 1926. It is the fundamental equation of quantum mechanics that describes the wave function or state function of a quantum mechanical system. The forms of Schrödinger Equation include the time-dependent Schrödinger equation and the time-independent Schrödinger equation.

Time-dependent Schrödinger Equation:

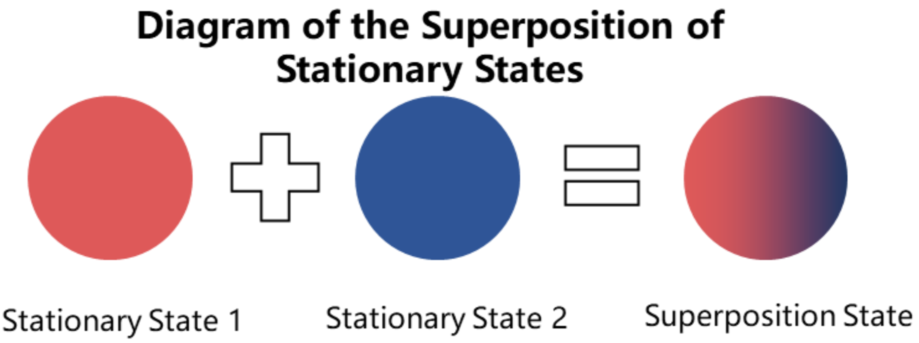
$$-\frac{\bar{h}^2}{2m}\nabla^2\psi(r,t) + V(r,t)\psi(r,t) = i\bar{h}\frac{\partial\psi(r,t)}{\partial t}$$

In the above equation, m is the mass of the particle, $\psi(r,t)$ is the wave function at position r and time t, and ∇^2 is the Laplace operator. It predict the future of a quantum system at $V(r,t)$. The time-dependent Schrödinger Equation is a partial differential equation, therefore when $V(r,t)$ is irrelevant to time, the time-independent Schrödinger Equation can be solved by separating the variables:

$$-\frac{\bar{h}^2}{2m}\nabla^2\psi(r) + V(r)\psi(r) = E\psi(r)$$

The time-independent Schrödinger Equation can also be written as $\hat{H}\psi = E\psi(r)$, where $\hat{H} = -\frac{\bar{h}^2}{2m}\nabla^2\psi(r) + V(r)$, an operator called the Hamiltonian. In this equation,

ψ is a time-independent wave function, E is energy, and the Hamiltonian operator corresponds to the sum of the kinetic energies plus the potential energies for all the particles in the system. The time-independent Schrödinger equation is also an Eigenvalue equation in which E is the eigenvalue.



Graph: Gate.io Research

The Schrödinger equation is also a linear equation. Mathematically speaking, any linear combination of solutions can also be a solution. Similarly, in quantum mechanics, any two or more quantum states can be added together and the result will be another valid quantum state. This is called Quantum Superposition.

2.2.4 The Copenhagen Interpretation

The Copenhagen Interpretation refers to the collection of quantum theories developed by Niels Bohr, Werner Heisenberg, and other scientists. Some of the central ideas of Copenhagen Interpretation include the statistical interpretation developed by Max Born, the Uncertainty Principle by Heisenberg, and the complementarity concept by Bohr. According to the Copenhagen Interpretation, physical systems generally do not have definite properties before being measured, and quantum mechanics can only predict the probability distribution of a given measurement's possible results. The act of measurement affects the system, causing the set of probabilities to reduce to only one of the possible values immediately after the measurement. This feature is known as wave function collapse.

2.3 Debates Emerged

Like much other scientific research, disputes about quantum mechanics emerges as it continues to develop. Two of the most important debates were the onde between Heisenberg and Schrödinger, and the Bohr-Einstein debate.

Matrix Mechanics by Heisenberg and Wave Mechanics by Schrödinger' s were proposed around the same period (in 1925 and 1926, respectively). The main difference between the two ideas is that Heisenberg was describing quantized particles and Schrödinger was describing quantized waves. Although the two theories were developed from different viewpoints and with different approaches, the two were proven to be equivalent. According to Dirac Notation, the general equation of quantum mechanics can be written as:

$$\widehat{H}|\psi\rangle = E|\psi\rangle$$

meaning that the $E|\psi\rangle$ in wave mechanics equals to Hermite $\widehat{H}|\psi\rangle$ in matrix mechanics.

In 1935, Albert Einstein, Boris Podolsky and Nathan Rosen published a paper that proposed a thought experiment named the Einstein-Podolsky-Rosen paradox as a challenge to the Copenhagen Interpretation. They indicated that the explanation of physical reality provided by quantum mechanics was incomplete, but John Bell' s Inequalities denied the paradox in 1964.

2.3.1 Erwin Schrödinger's Cat

Schrödinger' s cat is a thought experiment that illustrates what Schrödinger saw as the problem of the Copenhagen interpretation of quantum mechanics applied to everyday objects.

In this experiment, A cat is placed in a sealed box along with a container of cyanide and a small amount of radioactive particles. There is a chance where the radioactive material decays and emits radioactive particles; the particles will break open the cyanide container and kill the cat.

According to Copenhagen Interpretation, whether the cat is alive or dead can only be determined when the box is opened, which means that before opening the box, the cat will either be alive or dead. Schrödinger created this thought experiment to show how absurd the Copenhagen Interpretation was for macroscopic objects. However, as quantum mechanics continues to develop, Copenhagen Interpretation was recognized by many scientists nowadays.

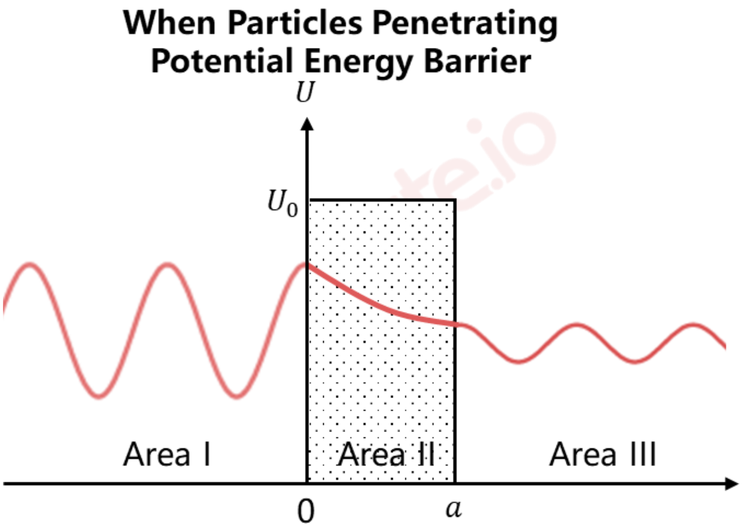
Another most recognized explanation of Schrödinger’ s cat is the Many-Worlds Interpretation. According to Many-Worlds Interpretation, the instance the box is opened, the world split into two universes – one where the cat is alive while the other one where the cat is dead, suggesting that each possible outcome can be realized in some “worlds” .

2.4 Quantum Mechanical Phenomena

During the quantum mechanical researches, phenomena such as quantum tunneling, potential well, and quantum entanglement were observed. The following session will introduce these three phenomena in detail and provide a better understanding of quantum mechanics.

2.4.1 Quantum Tunneling

The analogy of climbing a wall helps understand the phenomenon of quantum tunneling. In classical mechanics, the kinetic energy a person has must be greater than the potential energy of the wall to climb a wall. However, according to quantum mechanics, where particles travel in wave packets, the probability exists where one does not have to possess such a great amount of energy to surmount the wall but to penetrate it. This phenomenon is called quantum tunneling in the microscopic world..



Graph: Gate.io Research

From the graph above, when a particle encounters a potential barrier while it travels, the state of its motion can be categorized into three different regions – before the potential barrier (region i), within the potential barrier (region ii), and after the potential barrier (region iii). The amplitude of the quantum will decrease exponentially, but it continues to phase through the barrier.

The motion of the particle in different regions can be described using Schrödinger' s equation.

Region i:

$$-\frac{h^2}{2m}\frac{d^2\psi_1}{dx^2} = E\psi_1$$

Region ii:

$$-\frac{h^2}{2m}\frac{d^2\psi_2}{dx^2} + U_0\psi_2 = E\psi_2$$

Region iii:

$$-\frac{h^2}{2m}\frac{d^2\psi_3}{dx^2} = E\psi_3$$

According to the equation, the wave function in region i is ψ_1 while h is the Planck' s constant, the energy that the particle posseses is $E\psi_1$. In region i, the particle is moving forward in the sinusoidal waveform. When the particle travels through the potential barrier, its energy is $E\psi_2$, which is affected by the potential energy of the barrier. As the particle continues to experience the decay, it reaches region iii and moves freely again as wave function ψ_3, but with lower frequency and amplitude.

The Schrödinger equation can be solved as the following:

$$\psi_1(x) = Ae^{ik_1x} + A^{'}e^{-ik_1x} \qquad -\infty < x < 0$$

$$\psi_2(x) = Be^{k_2x} + B^{'}e^{-k_2x} \qquad 0 \le x \le a$$

$$\psi_3(x) = Ce^{ik_1x} \qquad a < x < \infty$$

According to the above solution, the particle movement in region i can be described as $\psi_1(x) = Ae^{ik_1x} + A^{'}e^{-ik_1x}$, region ii as $\psi_2(x) = Be^{k_2x} + B^{'}e^{-k_2x}$, and region iii as $\psi_3(x) = Ce^{ik_1x}$, while a is the width of the potential barrier.

2.4.2 Potential Well

In quantum mechanics, the potential well describes a situation where a particle is trapped in a space surrounded by impenetrable barriers. The participle can only move within that space.

The situation can be described with Schrödinger equation (stationary state):

$$-\frac{h^2}{2m}\frac{d^2\psi_2}{dx^2}+(E-U)\psi_2=0$$

The Eigenstate and Eigenvalue of the equation can be solved as follows:

$$\text{Eigenstate: } \psi_n(x)=\begin{cases}\sqrt{2/a}\,sin\frac{n\pi x}{a}e^{-\frac{i}{h}E_n t} & 0<x<a\\ 0 & \text{Others}\end{cases}$$

$$\text{Eigenvalue: } E_n=n^2\frac{\pi^2 h^2}{2ma^2}$$

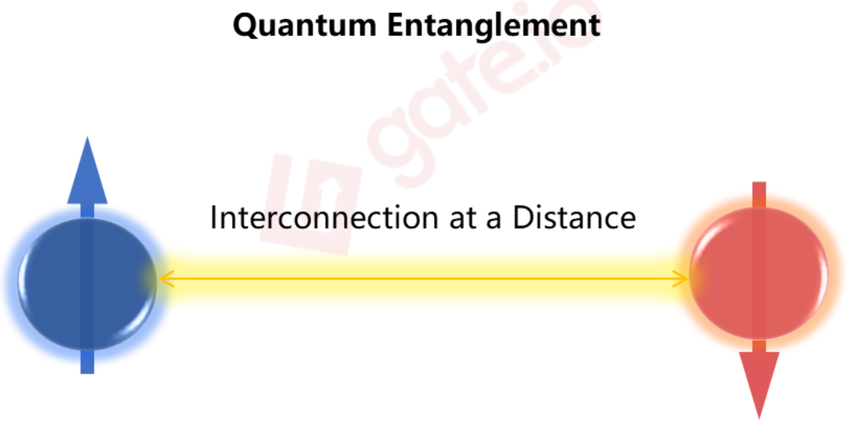
The eigenstate $\psi_n(x)$ describes how the particle move in the potential well, while the eigennvalue E_n is the value of participles in different positions. To better understand the equation, we can square the eigenstate:

$$|\psi_n(x)|^2=\frac{2}{a}sin^2\frac{n\pi x}{a}$$

In the above formula, $|\psi_n(x)|^2$ is the probability of a particle showing up in different positions, while the biggest probability where the particle can be found in certain position represent the peak of the sine wave.

2.4.3 Quantum Entanglement

Quantum entanglement is a phenomenon that two or multiple particles are linked together in a way such that the quantum states of the particle should be described with reference to each other .



Graph: Gate.io Research

As shown in the graph above, even when the two particles are spatially separated, when the state of one of the particles changes, the state of the other linked particle will change instantly.

3 Applications of Quantum Mechanics

The emergence of quantum mechanics has a cross-generational significance to modern science and technology. Two applications of quantum mechanics will be concretely introduced as follows.

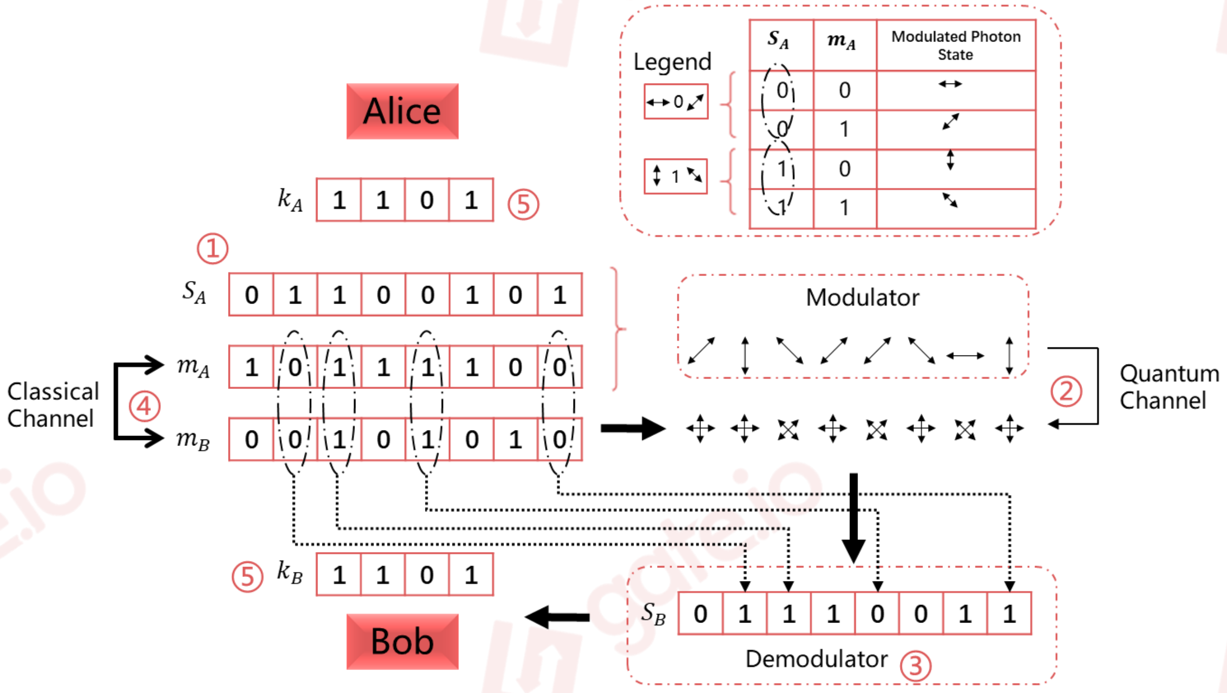
3.1 Quantum Key Distribution

Quantum key distribution is widely used for its high security. Generally, two parties will each hold an encrypted private key that cannot be decoded during communication; however, it is hard to know whether the information of the private key will be intercepted by a third party resulting in the information leak.

Quantum key distribution is to solve the above problem under the theory from quantum mechanics, which states that the change of one party’ s quantum condition will cause an instant change of another’ s on account of quantum entanglement. By observing the change of quantum condition, interception can be discovered during the sending process so that countermeasures can be made immediately.

BB84 is a well-known quantum key distribution scheme developed in 1984, which states that two parties communicating with each other can uninterruptedly emit photons and monitor the photon condition. As is shown below:

The Encryption and Transfer of Information



S_A	m_A	Modulated Photon State
0	0	↔
0	1	⤢
1	0	↕
1	1	⤡

Graph: Gate.io Research

① Firstly, Alice randomly chose two basic sequences,（S_A) and （m_A） respectively, and transformed them into quantum information through the prepared quantum state. Finally, the information was sent over the quantum channel to Bob.

② Meanwhile, Bob randomly chose a basic sequence（m_B） and prepared a quantum state to detect the information sent by Alice.

③ Bob transformed the sequences sent by Alice into a self-defined quantum state and produced a new sequence（S_B） through detecting. Then Bob sent sequence（m_B） over the classical channel to Alice.

④ In the meantime, Alice contrasted her sequence (m_A) and sequence (m_B) sent by Bob.

⑤ Alice recorded the detected sequences as K_A and K_B, and informed Bob of the same locations of two sequences. Eventually, by comparing, whether the private key had been intercepted could be told from the accurate rate of the detected sequences.

A fundamental principle of **BB84** is shown above, while the specific content is far more complicated.

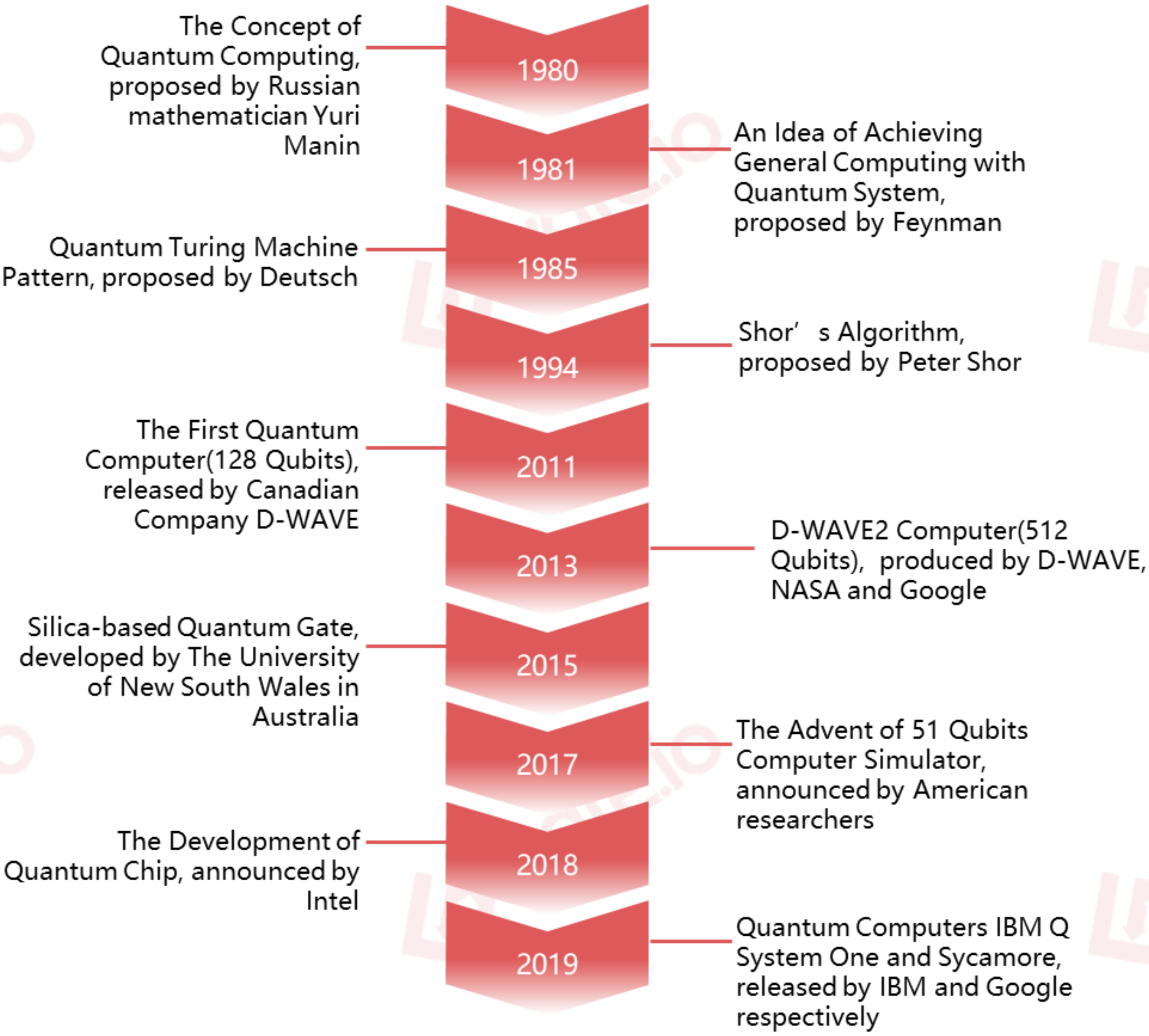
3.2 Quantum Computer

Quantum computers emerged in the research of quantum mechanics. Unlike the traditional computer, the quantum computer is a physical device that allows high-speed calculation of math and logic, stores, and processes quantum information complying with the rules of quantum mechanics. Any device that can process and calculate quantum information by quantum computing is a quantum computer whose concept generated from the study of reversible computers aiming to solve energy consumption during computing.

Simulating is the best way of learning for humans. The more we effectively simulate nature, the more we know about the laws of nature. The traditional computers can also simulate the movement of light and particle, the transfer of quantum and other micro-movements, but only at the expense of significant limitation, small computing scale, and low efficiency. The two basic operating principles between classical computers and quantum computers are different. For example, a well-decorated candle can never be compared to the lightbulb because they work in different ways. Seeing the value of quantum computers, many high-tech enterprises are now joining in the research and development.

3.2.1 Timeline of Quantum Computer

As the following graph depicts, many scientists have proposed various ideas towards quantum computers at different times. Up till now, the development of the quantum computers has been at its preliminary stage.


1980
The Concept of Quantum Computing, proposed by Russian mathematician Yuri Manin
1981
An Idea of Achieving General Computing with Quantum System, proposed by Feynman
1985
Quantum Turing Machine Pattern, proposed by Deutsch
1994
Shor' s Algorithm, proposed by Peter Shor
2011
The First Quantum Computer(128 Qubits), released by Canadian Company D-WAVE
2013
D-WAVE2 Computer(512 Qubits), produced by D-WAVE, NASA and Google
2015
Silica-based Quantum Gate, developed by The University of New South Wales in Australia
2017
The Advent of 51 Qubits Computer Simulator, announced by American researchers
2018
The Development of Quantum Chip, announced by Intel
2019
Quantum Computers IBM Q System One and Sycamore, released by IBM and Google respectively

3.2.2 Traditional Computers vs. Quantum Computers

As the proposal and development of quantum computers have been discussed above, the following content will cover the way that quantum computers work by comparing the differences between it and traditional computers.

- Traditional Computers

In traditional computers, a bit is a basic unit of information, and each bit represents either ‘0’ or ‘1’, regarded as two different properties and states. Therefore, the bit number is enormous in traditional computers (1 byte representing 8 bits), and the hard disk capacity of regular computers can reach 2TB.

An example will be used to describe the way that traditional computers work:

If a man is exploring a complex maze, the only way to exit is through constant tries. That is the same way as the way that traditional computer works, which keeps trying until the right way is found. Despite a relatively high speed, the keep-trying way of data processing has its upper limit. As a result, the movement in quantum theory comes to people’ s attention.

- Quantum Computers

The quantum computer is made up of bits which can represent ‘0’, ‘1’, or some combination, the basic unit of which is ‘qubit’ that is different from the traditional ‘bit’ representing either ‘0’ or ‘1’. They exist as two linear combinations of the ground state according to the theory of quantum mechanics:

$$|0\rangle = \binom{1}{0} \; and \; |1\rangle = \binom{0}{1}$$

As is shown in the above equation, a superposition state can exist between ‘0’ and ‘1’ in quantum computer so that this qubit can be either ‘0’ or ‘1’, which is more flexible. Qubit needs to be detected whether it is in the state of ‘0’ or ‘1’, during which the quantum state will collapse to a certain state. The result of the state has a probability distribution, which is directly proportional to the square of wave functions.

Due to its uncertainty of position, the quantum can exist in any position before it is detected. Once it is found, all circuits are collapsed at the same time, significantly reducing time consumption. That is how quantum computers work.

Currently, there are lots of physical ways to produce qubits. For example, electron spin-flipping can prepare qubits in states of topspin and backspin; photon’s polarization, including up-and-down polarization, left-and-right polarization, and elliptical polarization, can also make qubits. The quantum key distribution mentioned above was developed based on photon’s polarization.

3.2.3 Components of a Quantum Computer

In the working principle of quantum computers, we learn that one quantum, only representing ‘0’ and ‘1’, cannot process large numbers of calculations. In a quantum computer, there are lots of different qubits altogether processing the calculations, the collection of which is called the quantum register.

- Quantum Register

Quantum register is a system comprising multiple qubits, which could represent different exponentially rising states. If there are n qubits, not considering the quantum entanglement, the states can be conveyed as 2n numbers. The calculation is as follows:

$$\left(a_1 \Big|0\rangle \ + b_1 \Big| 1\rangle \ \right) \otimes \left(a_2 \Big|0\rangle \ + b_2 \Big| 1\rangle \ \right) \ldots \otimes (a_n|0\rangle \ + b_n|1\rangle \ )$$

Given the quantum entanglement, the states can be conveyed as 2n figures. For example, 5 qubits can store 32 figures; 128 qubits can store approximately $(3.4*10)^{38}$ figures, which could save many more figures than the traditional computer does.

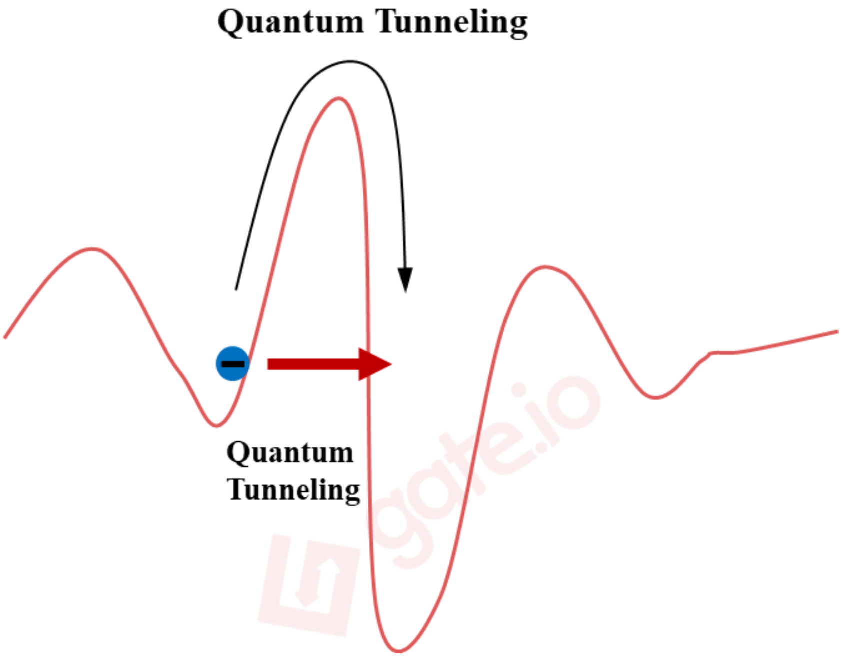
- Quantum Gate

Like traditional computer which can store and process data such as CPU (Central Processing Unit), quantum computers also have similar functions as a CPU. A quantum logic gate (or simply quantum gate) is a basic quantum circuit operating on a small number of qubits. They are the building blocks of quantum circuits like classical logic gates are for conventional digital circuits. Different from many classical logic gates, quantum gates are reversible. Through Unitary Matrix, quantum gates can keep transforming the quantum states, or change the probability distribution of qubits for quantum computing.

3.2.4 Quantum Algorithms

Quantum computers must operate with specific algorithms and comply with the motion law of quantum. Unlike classical algorithms, quantum algorithms work on the basis of the characteristics of quantum mechanics such as quantum superposition, quantum entanglement, quantum parallelism, and so on. Classical algorithms can’t effectively calculate many complicated problems, which, however, can be solved with quantum algorithms by processing substantial data at high speed. In contrast, classical algorithms consume more time to calculate as the number of data increases.

The primitively used quantum condensation algorithm aims to optimize the quantum computers. For example, cell phones will be at its best condition by reducing the heat to a minimum. There are many optimization problems in daily life, like medicines whose production processes need optimization to remain uniform. Nevertheless, the simulation of medicine development has limitations if manipulated by classical computers, which can hardly simulate the relevant particle structures. Instead, quantum computers can easily solve this problem.



Graph: Gate.io Research

As is shown above, generally, the classical condensation algorithm, a phenomenon observed from nature, will be used to optimize the extremum in search of the lowest point. For example, during steelmaking, impurity is subsided when the steels are transferred into cold water from high heat, meaning that the particles' structures become more and more compact.

Similarly, to know the lowest point of the particles, they should be heated to become dynamic enough in the system. As the blue particle in the above picture, traditionally, the particle needs enough energy to cross the hill and reach the lowest point. If it is operated in the quantum computer, the particle can save energy by quantum tunneling. The particle can detect its lowest potential energy, which tremendously improves efficiency.

Up till now, the valid quantum algorithms have been listed on Quantum Algorithm Zoo (a website), which had added over 60 algorithms and more than 400 academic papers by 2019. With an increasing amount of researches, quantum algorithms will definitely become the main study stream in the future.

4 The Impact of Quantum Computing on Blockchain Technology

As mentioned above, there are many theories and applications of quantum mechanics. Essentially, the difference between quantum mechanics and blockchain is huge. On the one hand, the former is about how humans perceive laws of nature. On the other hand, the latter is formed by rules set up by human. In science, quantum mechanics are being widely studied and applied. It starts attracting attention in the field of blockchain. The main reason for that is the threat to the security of blockchain, imposed by quantum computers. The following paragraphs will present how quantum computers threaten blockchain in detail.

4.1 Types of Encryption Methods

Generally speaking, its encryption process is to send information encoded by an encryption algorithm to a receiver. Then, the receiver can read the information by decoding it. According to the fact that whether the keys to decode and encode are the same, there are three algorithms: symmetrical Encryption, Asymmetric Encryption and the combination of both. As for blockchain, its encryption process is more sophisticated, such as the encryption process of Bitcoin. During this process, block headers should be hashed, which will generate a numerical value. Next, the numerical value will be signed. These two steps will be described in details as follows.

4.1.1 Hashing

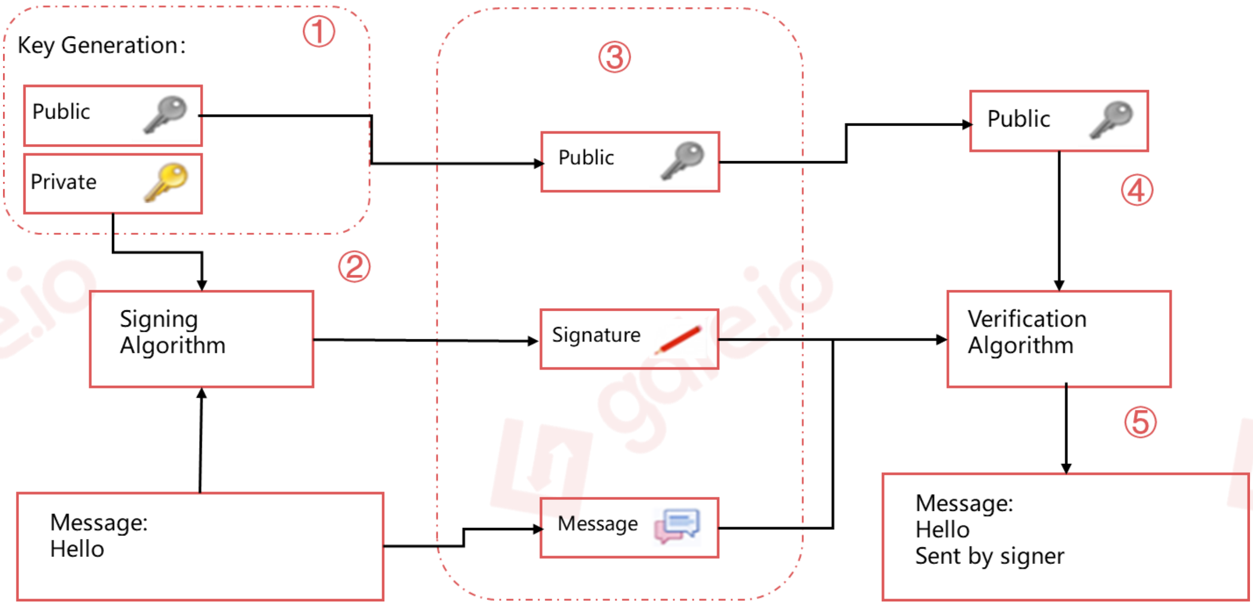
In PoW, the security of blockchain is based on computing power. Block headers should be hashed by SHA256 for example. For electronic computers, they have to calculate a 64-digit number called the "hash". The first one which can calculate the correct hash will be rewarded with bitcoins, and its block will be validated in the bitcoin network.

Therefore, the security of blockchain hinges on the ability to calculate the correct hash.

4.1.2 Signature Algorithm

Signature Algorithm is another encryption algorithm to maintain the security of the blockchain. Its encryption process is shown in the flow chart below.

The Encryption and Transfer of Information

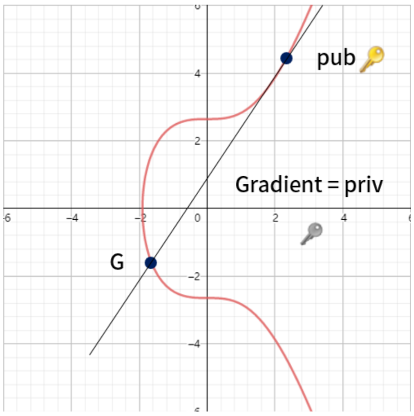


Graph: Gate.io Research

In the system of bitcoin, information has to be hashed (Secp256k1 and RIPEMD160) twice before sending out. A numerical value (160bytes) will be generated after hashing. Then, BTC will encode the numerical value due to its length, after which the bitcoin address will be formed.

To send out the information, the system will randomly generate a pair consisting of a private key and a public key. First, the bitcoin address will be encrypted by the private key, generating a signature. The information recipient will receive the encrypted message, the signature and a public key. With the public key, the recipient can determine that the signature was originally produced from the hash and the private key.

At present, there are two Signature Algorithms applied in blockchain: Elliptic Curve Digital Signature Algorithm and Edwards-curve Digital Signature Algorithm. The pros and cons of these two algorithms are presented as follows.



- Elliptic Curve Digital Signature Algorithm

Elliptic Curve Digital Signature Algorithm, known as “ECDSA” , is adopted in bitcoin. Being the most popular algorithm, it is also applied in BTC, ETH, EOS, TRON and ONT. What makes the algorithm so trendy is that it is an irreversible process, which means others cannot figure out the private key even with the public key. However, this established algorithm also comes with frequently repeated computing, lengthy signature and low efficiency.

This is the equation of the algorithm:

$$y^2 = x^3 + ax + b$$

Based on the equation, ‘a’ and ‘b’ are the parameters of the curve function. This means that for any ‘a’ and ‘b’ , different curves will be formed.

For ECDSA, ‘G’ is needed to represents a ‘reference point’ or a point of origin. The reference point could be any point on the curve. To create a signature, a private key is required, which equals to the Gradient of the line going through the reference point. A public key is a point on the curve generated from the point multiplication of G with the private key. We set ‘dA’ as the private key (random number) and ‘Qa’ as the public key (a point), so we have: Qa=dA*G (where G is the point of reference in the curve parameters).

This is the equation of Secp256k1:

$$\text{Secp256k1}：y^2 = x^3 + 7$$

According to the equation, there is only one fixed parameter, while other parameters are indefinite. In addition, only with a point of origin and a private key, can a public key be calculated.

- Edwards-curve Digital Signature Algorithm

Edwards-curve Digital Signature Algorithm (EdDSA) is mainly applied into ADA, Stella, Lisk, NEM, XMR and Tezos. With higher efficiency, the algorithm can be run on computers with lower performance. Nevertheless, this algorithm has flaws. For instance, double-spending issue may emerge, following the application of the algorithm into XMR. In some cases, by running this algorithm eight times, eight different numerical values can be generated. Thanks to the popularity of the algorithm, these flaws are mendable.

4.2 Threats Posed to Blockchain Encryptions

The security of the encryption mechanism of blockchain is weakening, as the development of quantum computer is gaining momentum. With that, the relationship between them is analyzed from two perspectives.

4.2.1 Quantum Computing Attacks

The security of bitcoin is based on computing power. For electronic computers, it is difficult to launch 51% attack as cracking down the encryption mechanism of bitcoin needs enormous computation. In such a case, it is very unlikely to manipulate more than 51% of the entire computing power. However, when running some algorithms, quantum computers can be hundreds of millions of times faster than electronic ones. Therefore, when computing SHA256, the bitcoin network will be highly vulnerable to a 51% attack, with squared even cubed running speed.

4.2.2 Cracking Private Keys

Quantum computers are able to decrypt private keys, which is another threat to blockchain. Compared to a 51% attack, this threat is more severe. Malicious intent can play a role in 51% attack. However, cracking private keys is equal to stealing money, meaning that our assets in wallet are accessible to others

4.3 Brute-Force Attacks: An Example of Quantum Computing Application

For quantum computers, through quantum algorithm, they can simulate quantum mechanical motion to reach high computing power. To crack the encryption mechanism, it is a must to decrypt a private key, a public key, a hash and a code. As mentioned above, the encryption mechanism is irreversible. So, for electronic computers, it is impossible to get access to private keys through brute-force attack due to immense computation and a time-consuming process. Moreover, keys of BTC are 256 bytes. But regarding quantum computers, brute-force attack is available if some algorithm could be implemented.

In conclusion, brute-force attack is a way to break the encryption mechanism of keys. Theoretically, after the public keys are updated, it will not be disclosed until its used, therefore it cannot be obtained by brute-force attack. However, there is still chances that the address can be cracked.

Meanwhile, it is not a popular choice to change an address frequently, as a result of inconvenience. The following paragraph will introduce how two algorithm threatens the security of blockchain.

4.3.1 Grover’ s Algorithm

Grover’ s algorithm is a quantum algorithm for searching the target number from an unordered set of numbers. In the set, it is very challenging to locate the target number. This can be solved through Grover’ s algorithm, which can achieve a square root speed up. For instance, it only needs 10 times to find the answer of $\sqrt{}10$. Although Grover’ s algorithm can increase efficiency, electronic computers can reach the same goal.

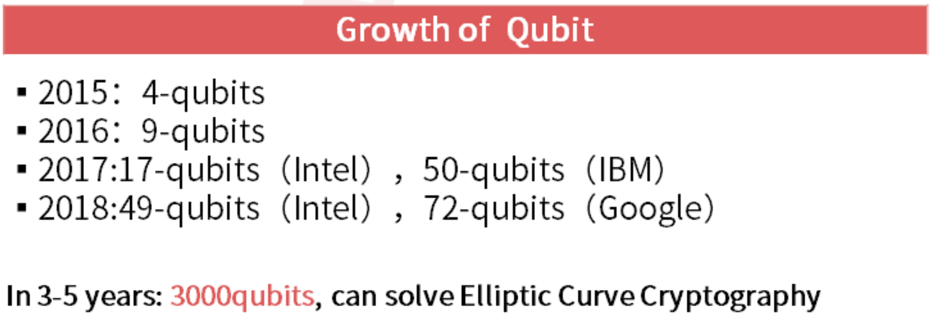
The threat imposed by Grover’ s algorithm is the collusion of keys and hash. In the bitcoin system, key algorithms and Hash are widely applied. Grover’ s algorithm can shorten the process of the collision, thus imposing a huge threat to the security of the system. Symmetric cryptography, such as AES, DES, used in the banking system is also under its threat, in addition to Hash, including SHA256, SHA-3 and RIPEMD-160. SHA256 and RIPEMD-160 are applied in bitcoin. With the implementation of Grover’ s algorithm, quantum computers can fasten the decryption of key algorithms and Hash. To prevent this problem, the length of keys should be multiplied in order to enhance security.

4.3.2 Shor’ s Algorithm

At present, Shor’ s algorithm is another huge threat. It is a quantum computer algorithm for efficient integer factorization. The ECDSA is designed to be irreversible when generating keys, which indicates that only through the collusion of a private key, a public key can be generated.

The reason why the ECDSA can’ t be reversed is based on the fact that the computing power of electronic computers is not able to break it, a discrete logarithm algorithm with high security. However, the algorithm is reversible theoretically as a discrete equation can be solved through Shor’ s algorithm, which allows the factorization of big integer and of a discrete logarithm. As a result, an asymmetric-key algorithm can be cracked efficiently, leading to a serious problem for bitcoin.

The chart below presents the growth of qubit:



Growth of Qubit

- 2015：4-qubits
- 2016：9-qubits
- 2017:17-qubits（Intel），50-qubits（IBM）
- 2018:49-qubits（Intel），72-qubits（Google）

In 3-5 years: 3000qubits, can solve Elliptic Curve Cryptography

According to the chart, breaking the ECDSA will be effortless once quantum computers reach 3000 qubits. Fortunately, these computers, developed by some large institutions for specific purposes, are exclusive. Even if 3000 qubits could be reached within 3 to 5 years, these computers will still have errors and bottlenecks. Therefore, the encryption mechanism applied in the system of bitcoin remains secure.

4.4 Anti-Quantum Algorithm – A Solution to Quantum Attacks

Generally speaking, when it comes to an anti-quantum algorithm, key size, computational efficiency, ciphertext or signature size, and other factors should be taken into consideration.

In the chart below, all algorithms are anti-quantum except for the last two of them. In terms of the anti-quantum algorithm, the sizes of a public key, a private key, and a signature are huge. This is a problem as the size of every block of the bitcoin will increase with a large amount of data on a transaction. In other words, to prevent the decryption by quantum computers, huge size blocks are needed, leading to the rapid growth of data. However, node centralization will occur due to the limited storage capacity of electronic computers. Therefore, the solution to the problem does not depend on an anti-quantum algorithm, which has its drawbacks.

Algorithm	Type	Public Key	Private Key	Signature
NTRU Encrypt	Lattice	6130B	6743B	
Streamlined NTRU Prime	Lattice	1232B		
Rainbow	Multivariate	124KB	95KB	
SPHINCS Large amount of data	Hash Signature	1KB	1KB	41KB
SPHINCS+	Hash Signature	32B	64B	8KB
BLISS-II	Lattice	7KB	2KB	5KB
GLP-Variant GLYPH Signature	Ring-LWE	2KB	0.4KB	1.8KB
New Hope	Ring-LWE	2KB	2KB	
Goppa-based McEiece	Code-based	1MB	11.5KB	
Random Linear Code based encryption	RLCE	115KB	3KB	
Quasi-cyclic MDPC-based McEliece	Code-based	1232B	2464B	
SIDH	Isogeny	751B	48B	
SIDH(compressed keys)	Isogeny	564B	48B	

3072-bit Discrete Log	Not PQC	384B	32B	96B
Non-quantum proof algorithm 256-bit Elliptic Curve	Not PQC	32B	32B	65B

Source: wiki ——Post Quantum Cryptography

4.5 The Impact of Quantum Computing on Bitcoin

With quantum computers advancing, SHA256 is one of the biggest problems of bitcoin. As for these computers, they can reach a square or cubic root speed up, reducing their time to break the algorithm at the same speed. For example, during mining, if the computing power of electronic computers is 10, then the same power of quantum computers will be 100. This means that 90% of the entire computing power is accessible to an attacker of the bitcoin network, which will put the network at huge risk.

In regard to encryption security, another problem is the ECDSA, which can be solved through SHA256. It will be very easy to crack down a private key given the fact that quantum computers can reach 3000 qubits within 3 to 5 years. As is known to all, the public address is a hashed version of a public key. Despite that, these computers can shorten the decryption process by achieving square or cubic speed up. As a result, the algorithm will be much more insecure, leading to a daunting problem.

So far, when transferring bitcoin, an address should be used once or for deposit exclusively without sending out, to maintain security. However, it is insecure if bitcoins are deposited in an address sent, according to theories.

5 Conclusion

The study of quantum mechanics were first established at the beginning of last century. It helps human beings discover the world at a microscopic level and now it is still one of the most researched fields.

As the theories of quantum mechanics continue to advance, there are an increasing number of cases of its real-life applications, including the most renowned quantum key distribution and quantum computers. Quantum key distribution is an important contribution to modern cryptography while quantum computes also mark a breakthrough in technology. A quantum computer can solve a function 10 million times faster than a traditional computer does, thus enabling solutions to many problems that used to be impossible to calculate.

However, the development of quantum computing poses severe threats to blockchain security. The encryption algorithm that blockchain currently uses can hardly protect its data against quantum computing. To defend against quantum computing attacks, some have proposed quantum-proof algorithms, which might be a solution to quantum attacks in the future.

Similar to other public blockchains, GateChain is also facing the challenge of quantum attacks. Whether to upgrade the encryption algorithm of GateChain to the quantum-proof level still needs to be discussed, as it might burden the network capacity and the storage of the blockchain. GateChain will try to discover innovative approaches to overcome the challenges imposed by quantum computing.

6 Reference

1. 一休.(2019). GateChain 量子力学讲座
2. Einstein, A.(1905). *Zur Elektrodynamik bewegter Körper; On the Electrodynamics of Moving Bodies* Annalen der Physik. 17:891-921.
3. 张孔辉. (1996). 海森堡矩阵力学体系的形成. 哈尔滨师范大学自然科学学报(02), 38-42.
4. 程民治, & 朱爱国. . 薛定谔创立波动力学的激励机制是“数学美”. 合肥工业大学学报(社会科学版)(1), 170-174.
5. 李宏芳. (2005). “薛定谔猫佯谬”的哲学研究. 科学技术哲学研究, 22(2), 35-38.
6. 钱国新. (1976). 必须重视对量子力学的哥本哈根解释的批判. 物理.
7. 王大洲. (2001). 论技术知识的难言性. 科学技术哲学研究(1).
8. 牛顿. (1997). 自然哲学的数学原理.
9. 曾谨言. (2007). 量子力学.卷 4. 科学出版社.
10. An Min MAO, An Ran LI. Multiplicity of Solutions for a Non-periodic Schrödinger Equation and a Superlinear Schrödinger-Maxwell Equation[J]. Acta Mathematica

Sinica, Chinese Series, 2012,55(3): 425-436

11. 第一个量子密钥分发协议--BB84 协议. (2018). Retrieved from https://baijiahao.baidu.com/s?id=1594512062830295717&wfr=spider&for=pc

12. 经典量子密钥分发（QKD）协议介绍（1) -- BB84 协议. (2018). Retrieved from https://www.qtumist.com/post/2178

13. 章岩扉. . 量子计算机的原理、发展及应用. 内燃机与配件, No.259(7), 230-231.

14. 量子力学目前最大的应用，量子计算机的计算能力有多强？超乎想象. (2019). Retrieved from https://baijiahao.baidu.com/s?id=1625193194791038557&wfr=spider&for=pc

15. Richard P. Feynman. (1986). Quantum mechanical computers. Foundations of Physics, 16(6), 507-531.

16. 区块链加密算法简述. (2018). Retrieved from https://blog.csdn.net/insistlee/article/details/80817760

17. Nakahara, Mikio, & Ohmi, Tetsuo. . Quantum computing (from linear algebra to physical realizations) || quantum computing with neutral atoms. , 10.1201/9781420012293, 311-328.

18. Quantum Algorithm Zoo. Retrieved from http://quantumalgorithmzoo.org/

19. Mavroeidis, V. , Vishi, K. , Zych, M. D. , & Audun Jøsang. (2018). The impact of quantum computing on present cryptography. International Journal of Advanced Computer Science and Applications, 9(3).