The Advance of Digital Signature with Quantum Computing

Zhanji Xu *

Department of International College of Chinese Studies, Fujian Normal University, Fuzhou, Fujian, 350000, China

* Corresponding author email: 154032020047@student.fjnu.edu.cn

Abstract. A digital transaction's sender or receiver's identity is verified using digital signature technology, a type of encryption. It allows users to prove their identity and the integrity of their message without relying on a third-party verification. Digital signatures are becoming increasingly important in the blockchain technology world. They enable users to verify the authenticity of digital assets, such as cryptocurrencies, and ensure that transactions remain secure. They also enable users to securely store their digital assets and prevent the unauthorized transfer of funds. Smart contracts, which are self-executing agreements that take effect when specific criteria are satisfied, also employ digital signatures. In addition, digital signatures are used to create digital signatures for digital documents, such as contracts, which allows users to securely sign documents without the need for a third-party verifier. This article presents the three primary digital signature algorithms presently utilized in blockchain technology: RSA, DSA, and ECDSA. It also discusses how quantum computers, which are currently being researched by some of the world's leading research companies, will affect traditional digital signature technology and what plans companies and countries have for this technology.

Keywords: Digital Signature; Cryptography; Blockchain; Digital Signature Algorithm; Quantum Computer.

1. Introduction

Blockchain technology is developing rapidly and has begun to be widely used in various fields [1]. Blockchain works in a decentralized environment that is enabled by comprising several core technologies, such as digital signatures, cryptographic hash, and distributed consensus algorithms [2]. The main advantage of blockchain technology is that it can guarantee the integrity and security of data, and blockchain technology also has the characteristics of decentralization. Blockchain technology to be still at an early stage of development. Most companies are still testing and working on prototypes [3]. With the advancement of technology, blockchain technology will continue to grow and develop, and it will profoundly impact many fields. In a word, blockchain is a decentralized accounting system that is built on top of technologies like as cryptographic algorithms, consensus procedures, point-to-point transmission, mathematics, and computer programming. Blockchains are used to record and verify transactions throughout a network. It can record transaction history and verify the legitimacy of transactions. Blockchain technology has a wide range of applications, and it can be used in finance, logistics, medical, legal, government, and other fields. The biggest advantage of blockchain technology lies in its decentralized nature, which makes it more effective in preventing cyberattacks and cyberfrauds.

Digital signature systems not requiring vital public cryptosystems are possible and can also be easier to certify [4]. Public-secret key pair encryption is the mechanism utilized by digital signatures in blockchain technology. Session keys, digital signatures, and data are typically encrypted using public keys that may be decoded with the accompanying secret key. This method can ensure that the key pair it produces is the only one in the world. If a piece of data is encrypted using one key while using this key pair, then it has to be decrypted using the second key in order to be readable.

To ensure that the public key is not tampered with during the digital signature process, it can be identified even if it has been tampered with. Digital certificate technology came into being. A digital certificate is a type of digital certification that is used to authenticate each participant involved in an Internet conversation by marking their identifying information. Digital identities are another name

for digital certificates. Digital certificates provide network users with the encryption or decryption necessary to communicate while maintaining the confidentiality and integrity of data and information.

In simple terms, a digital certificate is a digital signature of a public key. It prevents the sender from being hacked and tampered with when sending its public key to the receiver [5]. Both the public key and the secret key are examples of pairs of keys that may be produced by an algorithm. This particular sequence of digits provides not just considerable confirmation about the identity of the sender but also substantial proof regarding the legitimacy of the message. Public key, secret key, and a wallet are examples of digital signature tools in blockchain technology. It serves two purposes: proving that the message is truly signed and transmitted by the information sender, and determining the message's integrity. It has not been tampered with.

Due to the mature development and technical improvement of digital signature technology, and the unique identity authentication and security of blockchain technology, digital signature technology is widely used in blockchain technology for identity signature and verification.

Digital signature technology can effectively protect data access rights, and blockchain technology is conducive to storing and protecting various secret data due to its decentralization and other characteristics. Blockchain with digital signatures has become a key technology for many organizations as a security strategy to authenticate any object in the digital environment.

Digital signature technology on the blockchain consists of two algorithms: signature and verification. Digital signatures may increase the security of information, and combining signatures with blockchain systems can increase security even more. The digital signature is used digital signature for signature verification when sending transactions in the blockchain. The digital signature of the blockchain is an anti-forgery string generated only by the transferor of the blockchain transfer. By verifying the number string, on the one hand, it is proved that the transferring party initiated the transaction. On the other hand, it is proved that the transaction information has not been changed during transmission.

Asymmetric encryption and a digital digest make up the digital signature. Using digital abstract technology, the transaction data is compressed into a fixed-length string, which is then encrypted using asymmetric encryption technology to establish a digital signature.

This paper mainly introduces the process of digital signature technology, the RSA encryption algorithm, the DSA and ECDSA elliptic curve digital signature algorithms, which are often used in encryption and digital signature technologies. Moreover, under the circumstances of the rapid development of quantum computers, this article discusses what impact it will have on the current mainstream encryption algorithms and digital signature technology algorithms and what defense plans various countries and companies have for the menacing quantum computer technology. Next, the effects of quantum computing on key distribution and factoring are explored [6].

2. Methods

2.1 Digital Signature Process

If it is important to Alice to send Bob as did sign text, she can generate a hash value (also known as a message digest) for the message, "encrypt" it with her secret key, and then append a "signature" to the message. Only her public key can decipher this communication. Using Alice's public key, Bob can "decrypt" the hash value once he gets the message (using the same method as described in the step before this one, "decrypting the message"). Comparing it to the text's hash value that he calculated. If the two messages are identical, Bob will be able to confirm that Alice's secret key was used to send the message and that the message did not undergo any changes while it was being sent from one person to another.

1) Make sure you have both a public and a secret key by creating a pair of them.

2) In order to produce signature information, hash value of the message should be encrypted using the secret key of the sender, and then that should be used.

3) Send the encrypted hash value and the information to be sent together with the recipient's shared key.

4) Using the public key of the sender, the recipient decrypts the encrypted hash value to recover the hash value.

5) Verify the signature information.

2.2 Realization of Digital Signature Technology

The RSA, DSA, and ECDSA algorithms are the ones that are used for digital signatures the most often nowadays.

2.2.1 RSA Digital Signature Algorithm

The three mathematicians by the names of Rivest, Shamir, and Adleman came up with a method for asymmetric encryption in the year 1977. The algorithm that would later be known as RSA was designed in their honor. The RSA algorithm has been the "asymmetric encryption algorithm" that has seen the most widespread use up to this point.

The most traditional computer encryption algorithm at the moment and the one that has generated the most digital signatures to date is RSA. It is not an exaggeration to assert that there will always be an RSA algorithm as long as there is a computer network. Both the RSA encryption algorithm and the RSA digital signature method use the same key implementation, and are thus abbreviated as RSA. The RSA algorithm is used to encrypt almost all digital certificates offered today, including SSL digital certificates, code signing certificates, document signatures, and email signatures. Key generation and conversion are the same for each of these types of certificates.

The Mathematical Principles of RSA Encryption.

1) Congruence theorem: If two numbers x and y are divided by n The resulting remainders are equal, then x and y are identical modulo n, recorded as $x \equiv y \pmod{n}$.

- Corollary 1: $\forall z, x + z = y + z \pmod{n}$.
- Corollary 2: $\forall z, xz \equiv yz \pmod{n}$.

2) Inverse element:

The complement of the positive integer as an element x relative to modulus m satisfies $ax = 1 \pmod{m}$, namely

$ax = km + 1$, k is any natural number. For example, $x = 3, m = 7, a = 5, 3 \times 5 = 15, 15\%7 = 1$, so 5 is the inverse of 3 modulo 7. If both m and x are relatively prime, then and only then does x have an inverse in relation to the modulo of m.

3) Euler function $\varphi(n)$:

This paper gives the number of numbers that are not higher than n and are prime to both n and itself.

$\varphi(n) = (p - 1) \times (q - 1)$, where n is equal to p multiplied by q, and both p and q are prime integers.

4) Euler-Fermat theorem:

If m and n are mutually prime numbers, then $m\varphi(n) = 1 \pmod{n}$. According to the Euler-Fermat theorem, if m and n are coprime, then it does not matter how many times m is repeated; it will still be coprime with n.

Part of the RSA encryption algorithm.

Original text (Message): M stands for the information that needs to be encrypted. This information can be numbers, text, video, audio, etc.

C stands for "ciphertext," which is the information that is left after encryption.

If $E(x)$ is an encryption algorithm, then the process of encrypting data may be viewed as

$$M^e = C \pmod{n} \quad (1)$$

$$C = M^e \,\%\, \varphi(n) \quad (2)$$

A ciphertext is produced when the method of encryption is applied to the text that was originally encrypted.

If the decryption algorithm is denoted by the letter $D(x)$, then the process of decryption may be characterized as

$$C^d = M \pmod n \tag{3}$$

$$M = C^d \,\%\, \varphi(n) \tag{4}$$

The plaintext may be reconstructed using the ciphertext and the technique for decryption in order to get the desired result.

RSA encryption public-secret key pair generation.

1) Choose p and q at random from the list of positive prime integers.

2) Perform the multiplication of p by q and record the result n

$$n = p \times q \tag{5}$$

3) Find the value of the Euler function $\varphi(n)$ for the given value of n. The Euler function illustrates that the equation is true if and only if both of the value's p and q are positive prime integers,

$$\varphi(n) = (p-1)(q-1) \tag{6}$$

4) Choose at random a positive integer e that meets two conditions: $\varphi(n)$ is a prime number that is pretty close to e, and $1 < e < \varphi(n)$

5) Get a value for d such that it satisfies the requirements, and then carry out the computation necessary to determine the modular inverse element d of e for $\varphi(n)$,

$$ed = 1 \bmod \varphi(n) \tag{7}$$

This formula is comparable to (or equivalent to)

$$e \times d - 1 = k \times \varphi(n) \tag{8}$$

In fact, for the equation

$$e \times d - k \times \varphi(n) = 1 \tag{9}$$

Find the integer solution to (d, k). Using the extended Euclidean technique, this equation may be resolved.

6) Last but not least, the value (e, n) is converted into a public key, while the value (d, n) is converted into a secret key.

2.2.2 DSA Digital Signature Algorithm

DSA is different from RSA, because it cannot be utilized for key exchange or encryption and decryption. It is substantially quicker than RSA because it is just utilized for signatures. Its security is comparable to that of RSA. The fact that the two prime numbers are public is a vital component of the DSA, since it allows you to verify the integrity of other people's p and q even if you don't have access to their secret keys. It cannot be done via the RSA algorithm.

Digital Signature Standard (DSS) NIST (National Institute of Standards and Technology) proposed DSA (Digital Signature Algorithm) also known as DSS (Digital Signature Standard) in 1991 and soon in 1993 [7].

However, the NIST release generated much criticism, more political than intellectual. Numerous significant software businesses that have licensed the RSA algorithm patent have come out against DSS. They have spent a substantial amount of money to develop the RSA algorithm, and they do not want for these monies to be wasted.

DSA signature algorithm process.

1) public key:

p: a positive prime integer comprising 512 to 1024 bits

q: 160 bits in length and a reasonably primary factor to $p-1$

g: $g = h^{(p-1)/q} \pmod p$, where h is smaller than p-1 and $h^{(p-1)/q} \pmod p > 1$ is greater than 1

y: This paper gets the value of y is $g^x \pmod p$

2) secret key x: $x < q$

3) Signature process (both r and s are sender signatures):

Choose a random number k, and $k < q$

$$r = \left(g^{k}(\text{mod } p)\right)(\text{mod } q) \tag{10}$$

$$s = \left(k^{-1} \times (H(m) + x \times r)\right)(\text{mod } q) \tag{11}$$

4) Verification process as shown Table 1:

Table 1. Verification Process

STEP	
(1)	$w = s^{-1} (\text{mod } q)$
(2)	$l_1 = (H(m) \times w)(\text{mod } q)$
(3)	$l_2 = (r \times w)(\text{mod } q)$
(4)	$v = \left(\left(g^{l_1} \times y^{l_2}\right)(\text{mod } p)\right)(\text{mod } q)$
(5)	If $v = r$, the signature is verified

DSA prime number generation.

The NIST, which has full name called National Institute of Standards and Technology recommends a method that may be used to generate the prime integers p and q, where q can be used to evenly divide p-1.

The number L bits, which may range from 512 to 1024 bits and is a multiple of 64, represents the prime integer p.

The amount of bits in the prime number q is 160.

Let $L - 1 = 160n + 6$

Table 2. DSA Process

STEP	
1)	S is an arbitrary sequence of at least 160 bits that must be selected. Let g represent the size of S in bits.
2)	$L = SHA(S) \oplus SHA((S + 1) (\text{mod } 2g))$, Secure Hash Algorithm (SHA).
3)	Form q by setting the highest and lowest bits of U to 1
4)	Verify whether q is a positive prime integer.
5)	Return to (1) if q is not a prime number.
6)	Let $C = 0, N = 2$
7)	For $k = 0,1,\cdots\cdots, n$, let $Vk = SHA((S + N + k) (\text{mod } 2g))$
8)	Let $W = V_0 + 2160V_1 + \cdots\cdots + 2160(n-1)V_{n-1} + 2160n\ (V_n \text{ mod } 2b)$, W is an integer, and $X = W + 2L - 1$. Note that X is a number whose length is L.
9)	$p = X - ((X \text{ mod } 2q) - 1)$. Observe that p is 1 congruent modulo 2q.
10)	Go to step (13), if $p < 2L - 1$
11)	Verify whether p is a positive prime integer.
12)	Go to step (15), if p is a positive prime number
13)	Let $C = C + 1, N = N + n + 1$
14)	If $C = 4096$, go to step (1); otherwise, proceed to step (7).
15)	Save the S and C values used to generate p and q

As shown DSA process (Table 2), S, C, and N are collectively referred to as "seed," "count," and "bias," respectively.

Utilizing a one-way hash function SHA can avoid behind-the-scenes interference.

This is more secure than RSA, where Prime numbers are not disclosed. Someone could manufacture false primes, or special forms of primes that factor easily, and you don't get that unless you get the secret key. Utilization of the one-way hashing algorithm SHA is able to prevent behind-the-scenes meddling.

DSA Security. A 512-bit DSA does not provide long-term security, but a 1024-bit DSA does. The value of k must be different for each signature and must be picked at random. In the DSA digital signature method, a reliable random number generator is crucial to the system's security.

2.2.3 ECDSA Elliptic Curve Digital Signature Algorithm

Using ECDSA creates digital signatures. It combines both ECC and DSA. The whole signing procedure resembles DSA. The distinction is that the final signed value is likewise separated into r and s, and the signature process is ECC. Elliptic curve cryptography, or ECC for short, is one type of elliptic curve encryption.

Since the signature process is similar to DSA, the signature process is not specifically introduced here, and the ECC algorithm is mainly introduced.

RSA's solution to decomposing integer issues demands an algorithm with sub-exponential time complexity, however, the most well-known strategies for resolving elliptic curve discrete logarithm problems (ECDLP) need an exponentially high amount of temporal complexity. This study may be able to give the same degree of security with a far shorter key in the elliptic curve system than can be achieved with RSA. This discovery may enable the same amount of security with a considerably shorter key in the elliptic curve system, which is a significant improvement over RSA. The use of a small key may speed up the encryption and decryption processes, save on energy costs, reduce bandwidth use, and cut down on the amount of storage space required.

Both Bitcoin and China's second-generation ID card use a 256-bit ECC algorithm.

Elliptic Curve Cryptography (ECC).

(1) elliptic curve

The word ellipse for elliptic curves comes from the integral formula of the perimeter of an ellipse.

The collection of all points on the projective plane that fulfill the Weierstrass equation constitutes an elliptic curve,

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \quad (12)$$

For the randomly selected point (x, y) on the ordinary plane, let $x = \frac{X}{Z}, y = \frac{Y}{Z}, Z \neq 0$, get the following equation

$$y^2Z^3 + a_1xyZ^3 + a_3yZ^3 = x^3 + a_2x^2Z^3 + a_4xZ^3 + a_6Z^3 \quad (13)$$

About to go to Z^3 can get

$$y^2 + a_1xy + a_3y = X^3 + a_2X^2 + a_4X^2 + a_6 \quad (14)$$

Simplified version of Weierstrass equation

$$E: y^2 = x^3 + ax + b \quad (15)$$

Simplify the equation properties:

- $\Delta = -16(4a3 + 27b) \neq 0$
- $a, b \in K$, K is the basic domain of E.
- point $O\infty$ is the only infinity point of the curve.

(2) Elliptic Curve Abelian Group

Some Mathematical Terms Group: An algebraic object consisting of a set on which is defined a binary operation with certain properties [8]. It is known that the set sum operation $(G, *)$ must meet the following requirements if it is a group.

(3) Ellipse geometric addition

Since elliptic curves are Abelian groups, the formulas $P + Q + R = 0$ and $P + Q = -R$ hold. On the elliptic curve, draw the points and link them using the line that goes through both points. A

comparison will be made between this line and the elliptic curve up to a third point, which will be designated as R. Obtain the inverse element $-R$ of R according to R, $P + Q = -R$.

(4) algebraic addition

To calculate the addition of points, this paper must turn the previous geometry discussion to the algebra discussion, considering non-zero, asymmetric points $P(x_1, y_1)$ and $Q(x_2, y_2)$, R (x_3, y_3) is the intersection point of P, Q and the curve, then:

$$x_3 = k^2 - x_1 - x_2 \tag{16}$$

$$y_3 = k(x_1 - x_3) - y_1 \tag{17}$$

If $P = Q$, then

$$k = \frac{3x_1^2 + a}{2y_1} \tag{18}$$

If $P \neq Q$, then

$$k = \frac{y_2 - y_1}{(x_2 - x_1)} \tag{19}$$

(5) scalar multiplication

Same-point addition, if there are k identical points P added, denoted as kP.

(6) Finite Field Elliptic Curves

This paper gives a finite field F_p

Table 3. Addition of Finite Field Elliptic Curves

STEP	
(1)	F_p has the following elements: 0, 1, 2,..., p-2, p-1 (p is a prime integer).
(2)	F_p is $a + b \equiv c \pmod p$
(3)	F_p is $a \times b \equiv c \pmod p$
(4)	The division of F_p is $a \div b \equiv c \pmod p$, that is, $a \times b^{-1} \equiv c \pmod p$, b^{-1} is also an integer between 0 and $p - 1$, but satisfies $b \times b^{-1} \equiv 1 \pmod p$
(5)	F_p has a unit element of 1 and a zero element of 0.
(6)	Operations in the F_p domain are compliant with the rules of commutation, association, and distribution.
(7)	Elliptic curve $E_p(a,b)$, p is a prime number, $x, y \in [0, p-1]$ $y^2 = x^3 + a \times x + b \pmod p$ $4 \times a^3 + 27 \times b^2 \neq 0 \pmod p$
(8)	The element at position O_∞ is zero, this paper has $O_\infty + O_\infty = O_\infty$ $O_\infty + P = P$
(9)	The unfavorable component of $P(x,y)$ is $(x, -y \pmod p) = (x, py)$ $P + (-P) = O_\infty$
(10)	$P(x_1, y_1)$, $Q(x_2, y_2)$ and $R(x_3, y_3)$ have something special between the three of them: $x_3 = k^2 - x_1 - x_2 \pmod p$ $y_3 = k \times (x_1 - x_2) - y_1 \pmod p$

As shown in Table 3

k equals $\left(\frac{3x_1^2+a}{2y1}\right) \pmod p$ if and only if P=Q.

If P is greater than Q or Q is greater than P, k will equal $\left(\frac{y2-y1}{x2-x1}\right) (mod\ p)$

After the step 10 as shown in Figure 2, the lowest positive integer n that can be found on a point P on an elliptic curve where the multiplied number by $nP = O_\infty$ is referred to as the order of P. P has an infinite order of if n is not actual.

(7) Elliptic Curve Cryptography

Take into mind the equation K=kG, in which both K and G are points on the elliptic curve $E_p(a, b)$, n is the order of G ($nG = O_\infty$), and k is an integer that is less than n. Given k and G, it is not difficult to find K based on the addition rule; yet, it is very challenging to determine k given k and G. Both of these statements are true. When you have k and G, computing K is a simple task. It is difficult to compute list each of the n potential solutions in the preceding table. since the ECC in practical usage causes p to be rather big in concept and n to be fairly huge as well.

This paper calls the Point G as baes point.

1. The sender chose an elliptic curve $E_p(a, b)$ at random, and on the curve a randomly selected point is called G as a base point.

2. The sender chooses a private key to keep to themselves and then generates a public key using the algorithm. $K = kG$.

3. The sender directs K and G to the receiver while sending $E_p(a, b)$.

4. After receiving the data, the receiver will first generate a positive random number called r ($r < n$), and then it will encrypt the plaintext that will be delivered to a location called M on $E_p(a, b)$. There are several encoding techniques, which will not be covered in this article.

5. The receiver determines the points $C_1 = M + rK$ and $C_2 = rG$ by computing them.

6. The transmitter receives the values C_1 and C_2 from the receiver.

7. The sender, having received the data, then does the calculation $C_1 - kC_2$, and the value that is obtained is point M. At decoding point M, the plaintext will be revealed.

Elliptic Curve Digital Signature Algorithm (ECDSA).

(1) process

1. The elliptic curve and the base point on the curve are defined by the same global parameters for all communication people in the relationship in the digital signature.

2. To begin, the signer creates a set of public and secret keys. Select a random integer or pseudo-random number as the secret key, and then compute the public key using the random number and the base point.

3. Identify the message's hash value, then create a signature using the secret key, global parameters, and hash value.

4. Using the signer's public key, general settings, etc., the verifier validates.

(2) global parameters

1.q: a prime quantity

2.a, b: decimal digits on Z_p, define the elliptic curve by $y^2 = x^3 + a \times x + b$

3.G: Points that satisfy the elliptic curve equation, expressed as $G = (x_g, y_g)$

4.n: The lowest positive integer that meets the formula $nG = O$ is the order of point G, or n.

(3) Every sender is required to produce a public-secret pair of keys.

1. Choose an integer d at random, the value of d is larger than 1, but it is not greater than n-1.

2. To get a solution point on the curve $E_q(a, b)$, compute the equation $Q = dG$.

3. The public key of the sender is Q, while the sender's secret key is d.

Here is the elliptic curve defined on Z_p . The multiplication operation on the elliptic curve is the accumulation operation of multiple points, and the outcome remains a point on the elliptic curve.

(4) generate signature as shown Table 4

After having the public key, the sending party message m generates a 320-byte digital signature

Table 4. Generate Signature

STEP	
(1)	Randomly (or pseudo-randomly) choose an integer k, the value of k is larger than 1, but it is not greater than n-1.
(2)	Determine the point on the curve that represents the solution, $P = (x, y) = kG$ and $r = x \pmod n$. If $r = 0$, skip to step 1.
(3)	Calculate $t = k^{-1} \pmod n$.
(4)	Calculate $e = H(m)$, H is the 160-bit hash value produced by the SHA-1 hash algorithm.
(5)	Compute $s = k^{-1}(e + dr) \pmod n$. Skip to step 1, if $s = 0$.
(6)	The m-word serves as the message's signature (r ,s).

In the Table 4, Step 2 ensures that the final calculated public key (point on the elliptic curve) falls on the curve. In step 5, if it is point O, it is also inconsistent, so it must be regenerated.

(5) verify signature as shown Table 5

The recipient is able to validate the signature after they have obtained the sender's public key in addition to the global parameters.

Table 5. Verify Signature

STEP	
(1)	Make sure whether r and s are integers, the value of s is larger than 1, but it is not greater than n-1.
(2)	Calculate $e = H(m)$ by using the SHA-1 hash algorithm, where H is the 160-bit hash value obtained by the SHA-1 hash method.
(3)	Calculate $w = s^{-1} \pmod n$
(4)	Calculate $l_1 = e \times w$ and $l_2 = r \times w$
(5)	Calculate node $X = (x_1, y_1) = l_1 \times G + l_2 \times G$
(6)	If X is equal to O, then the signature cannot be accepted; else, compute $v = x_1 \pmod n$.
(7)	Accept the signature from the sender when and only when $v = r$

Advantages of ECC over RSA

- The security performance is better with the same key length. For instance, 1024-bit RSA and DSA are equivalent to 160-bit ECC.
- security strength.
- Little calculation is performed, and processing happens automatically. In the processing speed of the secret key (decryption and signature), ECDSA is much faster than RSA and DSA [9].
- DSA is much faster.
- Compared to other cryptosystems, the key length and system parameters of ECC are much smaller and its storage space is also much smaller [10].

3. The Impact of Quantum Computer Technology on Digital Signatures

3.1 The Negative Impact of Quantum Computer Technology on Digital Signatures

Quantum computer technology has the potential to have a negative impact on digital signatures. By being able to break the encryption used in digital signatures, the security of cryptographic keys is compromised, resulting in a loss of trust in digital signatures. Furthermore, quantum computing can be used to decipher digital signatures, leading to potential data breaches. Companies may have to invest in more secure digital signature technologies to counter the potential threats of quantum

computing, which can be an expensive endeavor. Therefore, it is important to understand the potential implications of quantum computing and take steps to protect digital signatures.

3.2 The Positive Impact of Quantum Computer Technology on Digital Signatures

Quantum computer technology has the potential to significantly improve the security, efficiency, and scalability of digital signatures. By increasing the security of digital signatures, quantum computers can strengthen authentication methods and reduce the potential for data breaches. Additionally, quantum computing technology can expedite digital signature processing times and provide more efficient data processing for digital signatures. Lastly, quantum computing technology can facilitate the scalability of digital signature systems, allowing for more users and transactions to be processed simultaneously. The introduction of quantum computing technology has the potential to revolutionize digital signature systems and provide increased security, faster transactions, enhanced efficiency, and improved scalability.

4. Conclusion

In conclusion, quantum computers have the potential to impact digital signature technology significantly. By providing increased levels of encryption, complex digital signatures that are virtually impossible to break, and faster processing times, digital signature technology can be further secured and improved. This can lead to enhanced trust between parties, more secure transactions, and faster processing times. With the increasing development of quantum computing technology, digital signature technology can continue to be improved and strengthened. However, digital signature technologies widely used worldwide are recognized, for example, digital signature technology based on the RSA encryption algorithm, DSA digital signature technology, and ECDSA digital signature technology. These algorithms are based on some difficult mathematical puzzles. But for quantum computers, solving these mathematical puzzles is straightforward. So, before the more advanced digital signature technology is effectively developed and applied, each company or national government should strictly regulate the use of quantum computers and make timely plans for the popularization of quantum technology to prevent Information destruction on a massive scale. Therefore, the development of quantum computers promotes the successful development of new and more difficult-to-crack digital signature technology. But at the same time, the rapid development of quantum computer technology will also bring a devastating blow to traditional digital signature technology. These are the two sides of the development of science and technology, which is also a question worthy of more scientific researchers' deep thinking.

References

[1] Cheng Qiyun, Sun Caixin, Zhang Xiaoxing, et al. Short-Term load forecasting model and method for power system based on complementation of neural network and fuzzy logic. Transactions of China Electrotechnical Society, 2004, 19(10): 53-58.

[2] Monrat, A. A., Schelén, O., & Andersson, K. (2019). A survey of blockchain from the perspectives of applications, challenges, and opportunities. IEEE Access, 7, 117134-117151.

[3] Härting, R. C., Sprengel, A., Wottle, K., & Rettenmaier, J. (2020). Potentials of blockchain technologies in supply chain management-A conceptual model. Procedia Computer Science, 176, 1950-1959.

[4] Merkle, R. C. (1989, August). A certified digital signature. In Conference on the Theory and Application of Cryptology (pp. 218-238). Springer, New York, NY.

[5] Wang, C., Hao, Z. X., & Wang, Q. (2010). The Design of Digital Signature System Based on PKI. In Applied Mechanics and Materials (Vol. 20, pp. 1323-1327). Trans Tech Publications Ltd.

[6] Wright, M. A. (2000). The impact of quantum computing on cryptography. Network Security, 2000(9), 13-15.

[7] Kittur, A. S., & Pais, A. R. (2017). Batch verification of digital signatures: approaches and challenges. Journal of information security and applications, 37, 15-27.

[8] Chick, H. (1998). Cognition in the formal modes: Research mathematics and the SOLO taxonomy. Mathematics Education Research Journal, 10(2), 4-26.

[9] Fang, W., Chen, W., Zhang, W., Pei, J., Gao, W., & Wang, G. (2020). Digital signature scheme for information non-repudiation in blockchain: a state of the art review. EURASIP Journal on Wireless Communications and Networking, 2020(1), 1-15.

[10] Zhou, M. R., Jiang, Z. T., & Yang, C. (2014). Research on an Anonymous Authentication Scheme based on ECC for Electronic Report Systems. In Applied Mechanics and Materials (Vol. 574, pp. 737-742). Trans Tech Publications Ltd.