Hindawi
Security and Communication Networks
Volume 2021, Article ID 6671648, 13 pages
https://doi.org/10.1155/2021/6671648

Research Article

A Blockchain System Based on Quantum-Resistant Digital Signature

Peijun Zhang,[1] **Lianhai Wang**,[1] **Wei Wang**,[1] **Kunlun Fu**,[1] **and Jinpeng Wang**[2]

[1] *Qilu University of Technology (Shandong Academy of Sciences), Shandong Provincial Key Laboratory of Computer Networks, Shandong Computer Science Center (National Supercomputer Center in Jinan), Jinan 250014, China*
[2] *Shandong Computer Science Center (National Supercomputer Center in Jinan), Jinan 250014, China*

Correspondence should be addressed to Lianhai Wang; wanglh@sdas.org

Received 17 December 2020; Revised 23 January 2021; Accepted 1 February 2021; Published 4 March 2021

Academic Editor: Debiao He

Blockchain, which has a distributed structure, has been widely used in many areas. Especially in the area of smart cities, blockchain technology shows great potential. The security issues of blockchain affect the construction of smart cities to varying degrees. With the rapid development of quantum computation, elliptic curves cryptosystems used in blockchain are not secure enough. This paper presents a blockchain system based on lattice cipher, which can resist the attack of quantum computation. The most challenge is that the size of public keys and signatures used by lattice cryptosystems is typically very large. As a result, each block in a blockchain can only accommodate a small number of transactions. It will affect the running speed and performance of the blockchain. For overcoming this problem, we proposed a way that we only put the hash values of public keys and signatures on the blockchain and store the complete content of them on an IPFS (interplanetary file system). In this way, the number of bytes occupied by each transaction is greatly reduced. We design a bitcoin exchange scheme to evaluate the performance of the proposed quantum-resistant blockchain system. The simulation platform is verified to be available and effective.

1. Introduction

Smart city [1] is the application of new technology to city management and service. Blockchain technology shows great potential in the field of smart cities. In terms of economic products, blockchain provides a unique identity of goods, which helps in real-time quality monitoring [2]. In terms of medicine, blockchain allows data to be stored safely. And it can be applied to the supervision and identification of drug supply chains. Blockchain is being paid attention to by more and more governments and is gradually being applied in smart cities.

In 2008, an author named Satoshi Nakamoto published a paper entitled “Bitcoin-A Peer-To-Peer Electronic Cash System”. Afterwards, more and more developers have invested in blockchain research. Eth [3] (Ethereum), EOS [4] (Enterprise Operation System), EPT [5] (Electronic Payment To-ken), and other blockchain technologies [6, 7] emerge one after another. These technologies are widely used in finance, Internet of Things, intellectual property, traceability, and other areas. Up to now, there are more than 3,000 kinds of digital currencies in the world, with a total market value of 150 billion US dollars.

Blockchain is essentially a distributed ledger that allows distrusted parties to trade directly without a third party. It has the characteristics of nontamper, nonforgery, traceable, transparent data especially safety like above, and so forth. These characteristics largely depend on the underlying public key cryptography used in the blockchain. The security strength of traditional public key cryptosystems was dependent on one of the two difficult problems [8, 9]: (1) factorization of large integers and (2) discrete logarithm problem. However, in 1997, Shor [10] and Grover et al. proposed quantum search algorithms, which make the decomposition of large integer factors no longer insoluble. And quantum search algorithms that break traditional public key cryptography are proposed continuously. As shown in Figure 1, with the development of quantum search

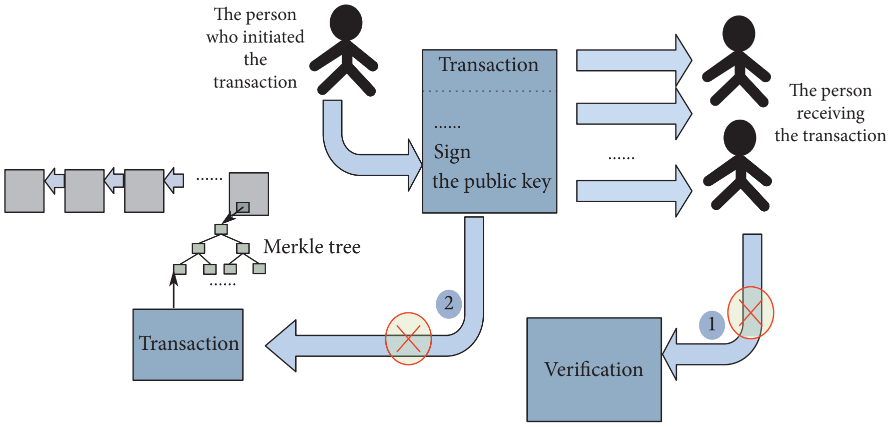


Figure 1: Middleman attacks blockchain.

algorithms, the security of blockchain based on traditional public key cryptosystems has aroused people's doubts.

The need for blockchain to resist the attack of quantum algorithms is urgent. Thankfully, through the continuous efforts of researchers, there have been a lot of public key cryptosystems that are quantum-resistant algorithms. Among them, the number of lattice-based public key cryptosystems is the most competitive one. Up to now, there is no quantum algorithm that can solve the difficult problem of lattice-based public key. Regev [11] described several public key cryptosystems signatures based on lattices. This quantum-resistant cryptography brings hope for blockchain to resist the attack of quantum search algorithms. But the size of public keys and signatures used by lattice cryptosystems is typically very large.

1.1. Our Contributions. In order to solve the problems faced by block chain, the following works are done in this paper:

> We propose an quantum-resistant blockchain scheme that the digital signature based on the elliptic curve is replaced by qTESLA digital signature based on lattice cipher to resist the attack of the quantum computer. We design a bitcoin exchange system to evaluate the performance of our system.
>
> The size of public keys and signatures used by qTESLA is very large. It will take up too much capacity of block. We store public keys and sign on IPFS and only put the hash values of them on the blockchain. Set the difficulty of POW (Proof of Work) to a suitable range; our system will be more efficient.
>
> We evaluated the strengths and weaknesses of the three systems. It provides effective experimental conclusions for future research.

1.2. The Paper Structure. The rest of the paper is organized as follows: in Section 2, we will look at related works on quantum computers and quantum-resistant-lattice cryptography. We will introduce the techniques used, including Fiat–Shamir and its transformation, qTESLA's key generation and signature, and the principle of verification in Section 3; in Section 4, we propose a new quantum-resistant blockchain system. The availability, stability, and efficiency are analyzed in Section 5 and Section 6 concludes this paper.

2. Related Work

2.1. Quantum Computers. As early as in the early 1980s, Benioff [12] proposed a two-order quantum system that could be used to simulate digital computation. Over the next few years, quantum computing gradually has taken on the basic form of mathematics. In 1997, Shor et al. proposed a polynomial time quantum algorithm for factorization of large integer and discrete logarithm problems, which seriously threatened the security of digital signature based on the elliptic curve. D-wave went from the first 16-bit quantum computer in 2007 to a 512-bit one, which provided the rapid development of quantum computers greatly. At the same time, IBM in the United States has found a key technology that can massively increase the quantum number of quantum computers. In 2016, IBM launched the world's first quantum computing cloud platform: IBMQ. Currently, the IBMQ processor has reached 17 qubits. In 2018, Google's Quantum Artificial Laboratory launched Britlecone. In 2020, Pan et al. at the University of Science and Technology of China have developed a dedicated quantum computer. The rapid development of quantum computer threatens the security of the traditional cryptographic public key system, and it is urgent to improve the blockchain technology used in the traditional cryptography.

2.2. Quantum-Resistant-Lattice Cryptography

2.2.1. Public Key Cryptosystem Based on Lattice. There are four mainstream public key cryptosystems against quantum algorithms [13]: public key cryptosystems based on a hash function, public key cryptosystems based on error correction code, public key cryptosystems based on lattice, and multivariable public key cryptosystems.

In 1996, Ajtai [14] gave the specification of the general difficult case to the worst case on lattice for the first time in his paper, introduced the small integer solution problem and one-way function problem in the average case, and proved that solving the above problems was equal to the difficult case on lattice in the worst case. In 1997, Aharonov and Benor [15] presented a lattice-based public key encryption system with security proof under the worst-case complexity assumption. From 1997 to 1998, Hoffstein Pipher and Silverman designed using a polynomial ring UNRU encryption system. UNRU is fast in encryption and decryption and has a more compact key size but lacks formal security proofs and does not have any known difficult problems to regulate. In 1997, Goldreich, Goldwasser, and Halevi et al. directly applied the lattice difficulty problem to the lattice public key encryption and proposed the GGH cryptosystem. The GGH regime is easy to understand and intuitive, but there are no worst-case security guarantees, and the security assessment is in the heuristic proof phase. In 2002, Micciancio improved efficiency on polynomial rings. In 2003, Regev et al. introduced Gaussian distribution and harmony analysis in Ajtai-Dwork and transferred the security of cryptography schemes to the worst-case lattice problem at the bottom.

At present, a lattice-based cryptosystem [16, 17] is designed around two basic problems of small integer and learning error. In 2005, Regev [18] proposed the LWE problem to make the lattice-based cryptography system take into account provable security. In 2008, Ladner and Dwork [19] obtained the protiofate by using the single trap function on lattice (GPV) and constructed the public key encryption scheme and the signature scheme by using the protiofate sampling method.

2.2.2. Lattice Signature Scheme. At present, the digital signature based on lattice cipher can be divided into three types: lattice aggregation signature, proxy signature, and fuzzy identity signature. Yanhua et al. [20]. designed the converged signature of two lattice bases, which has no security proof, leading to the existence of serious security risks. Lattice ordered aggregate signatures can only be used in sequentially related systems, but not in a disordered user system such as blockchain. A proxy signature may designate an agent to continue the signature authentication operation in the absence of the signer. Fuzzy identity signature is more used in the identification of biological attributes.

All of the above signatures belong to two modes, Fiat–Shamir and Hash-And-Sign. Between the two modes, the signature in Fiat–Shamir mode has a higher implementation efficiency. qTESLA digital signature is a kind of digital signature in its mode.

2.2.3. Quantum-Resistant Blockchain System. The main technology used in the quantum-resistant computer blockchain system is to replace the original signature with a digital signature of the quantum-resistant algorithm. However, it only stays in theoretical research and lacks practical experience. The signed public key takes up a lot of block capacity. At present, the problem of the long public key has not been solved completely.

Some researchers are working on algorithms for digital signatures. Li et al. [21] proposed a digital signature algorithm using the Bonsai Trees technology. This algorithm can guarantee its security. However, it is inefficient. And its practicability needs to be verified. Gao et al. [22] proposed a double signature scheme that can be applied to the blockchain. However, the security of this scheme is only under the SIS assumption, which is not convincing. On the basis of Bonsai Tree, Yin et al. [23] extend a lattice space to multiple lattices. This scheme adds complexity to the signature. And the signatures produced by such schemes are enormous.

3. Background

As of now, there is no quantum algorithm which can solve the difficult problem based on lattice. The difficulty of lattice problem in the worst-case ensures its strong security. Moreover, the basic operations of lattices are parallel which will reduce the computation complexity. In this paper, qTESLA digital signature based on lattice cipher is used instead of the original digital signature based on the elliptic curve in bitcoin system to resist the attack of the quantum computer.

The qTESLA is a digital signature of Fiat–Shamir mode with high efficiency. Therefore, this section describes the Fiat–Shamir pattern in detail and gives its signature transformation and the basic principle of qTESLA.

3.1. Fiat–Shamir. Fiat–Shamir [24, 25] authentication protocol is an interactive zero-knowledge proof mode with high computational efficiency.

3.1.1. Identity Authentication Protocol Fiat–Shamir. The basic principle of Fiat–Shamir is as Figure 2: p and q; let $n = p \times q$. Alice generates her own private $s \in (1, n-1)$ and public keys $v = s^2 \bmod n$ using the key algorithm.

If Alice pretends to know the news s, she wants to perjure herself to prove it to Bob.

If Alice can predict in advance whether the c Bob is sending 0 or 1, then Alice can trick Bob.

If Alice cannot predict in advance the c that Bob sends, then the probability that Alice cheats Bob is $1/2^n$. After tests, the probability of Alice cheating Bob is almost zero.

In reality, Alice could not have foreseen Bob's challenge.

3.1.2. Fiat–Shamir Transformation. In Fiat–Shamir transformation, Alice uses hash function H instead of c to generate challenges in Figure 3. It can prove that Alice knows the message s without any interaction.

3.2. qTESLA. qTESLA's design is simple and easy to implement. It is compact, safe, and portable with better performance. The security of qTESLA is based on the hardness of the decision R-LWE problem and has strict security proof of the random oracle model.

Basic principles of qTESLA:

> *Preparatory Knowledge.* Some important parameter definitions are written in Figures 4–8. The integer polynomial y is called $B-short$ if each coefficient

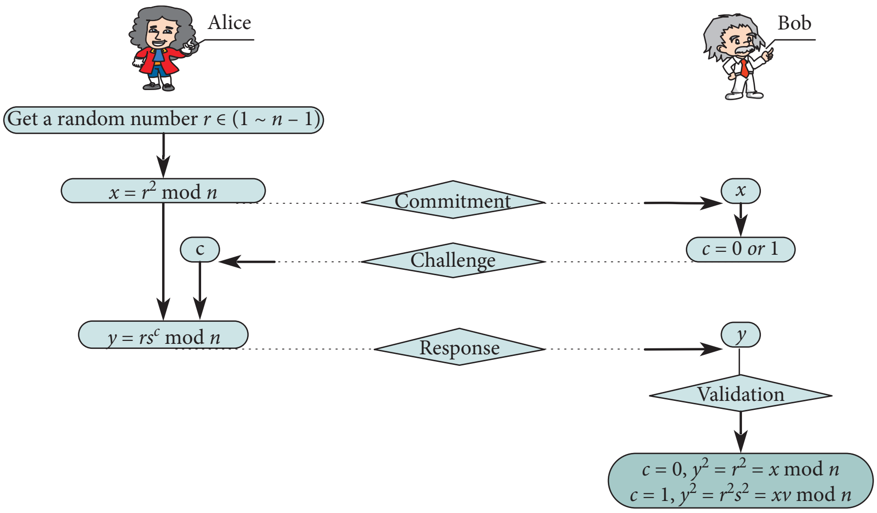

Alice
Bob
Get a random number $r \in (1 \sim n-1)$
$x = r^2 \bmod n$
Commitment
x
c
Challenge
$c = 0$ or 1
$y = rs^c \bmod n$
Response
y
Validation
$c = 0, y^2 = r^2 = x \bmod n$
$c = 1, y^2 = r^2s^2 = xv \bmod n$

Figure 2: The basic principle of Fiat–Shamir.

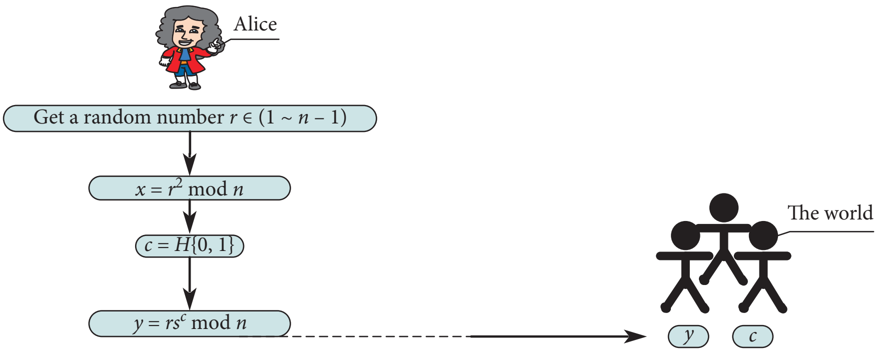


Figure 3: Fiat–Shamir transformation.

Ring:

q: In this paper, q stands for an odd prime, unless otherwise specified

$\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$: the quotient ring of the integers modulo q

R: represents ring $\mathbb{Z}[x]/<x^n + 1>$

R_q : represents ring $\mathbb{Z}_q[x]/<x^n + 1>$

Let $f = \sum_{i=0}^{n-1} f_i x^i \in R$, define f mod q: (f mod q) $= \sum_{i=0}^{n-1} (f_i \bmod q) x^i \in R_q$

Let $H_{n,h} = \{\sum_{i=0}^{n-1} f_i x^i \in R \mid f_i \in \{-1, 0, 1\}, \sum_{i=0}^{n-1} |f_i| = h\}$

Let $R_{[B]} = \{\sum_{i=0}^{n-1} f_i x^i \in R \mid f_i \in [-B, B]\}$

Figure 4: Some definitions of the ring.

satisfies $y^i \le B$. If w is $(q/2) - short$ and $[w]_L$ is $(2^{d-1} - E) - short$, w is $well - rounded$.

Signature and Verification. The principle of qTESLA is shown in Figures 9–11.

3.3. IPFS. The public key length based on the qTESLA digital signature is too long and will occupy most of the block memory. At present, the main solution of quantum-resistant computer blockchain system is to adjust the algorithm and reduce the length of the public key. Although this method improves the use of limited block capacity, it cannot fundamentally solve the problem of public key length. This article uses the IPFS protocol to solve this problem. After uploading the available file, we get a hash value. When we need the file, we just need to enter the corresponding hash value to get it.

The IPFS [26] protocol is a distributed file system that uses a combination of technologies [27] to ensure its unique advantages:

S/Kademlia DHT. The structure of S/Kademlia DHT is shown in Figure 12. After the node receives the information, it updates its k bucket, as shown in Figure 13. Next, the node needs an introducer to join the KAD network. The node inserts the introducer into its own k bucket and performs FINDNODE to updates its own k bucket until it completes the build of k bucket. Finally, it publishes its own information to other nodes' k buckets.

In the KAD network, the sender has to sign the sent message. After other nodes receive the message, they not only need to check the signature but also need to complete two difficult problems. It ensures that the

Rounding operator:

Let $d \in \mathbb{N}$, $c \in \mathbb{N}$, $-m/2 < c' \le m/2$ ($m \in \mathbb{Z}_{\ge 0}$), $c' = c\ mod^{\pm}\ m$ *as the unique element*

$[\cdot]_L: \mathbb{Z} \to \mathbb{Z},\ c \mapsto (c\ mod^{\pm}q)mod^{\pm}2^d$

$[\cdot]_M: \mathbb{Z} \to \mathbb{Z},\ c \mapsto (c\ mod^{\pm}q - [c]_L)/2^d$

thus, $c\ mod^{\pm}q = 2^d,\ [c]_M + [c]_L$ *represent* $c \in \mathbb{Z}$

polynomials:

for a given $f = \sum_{i=0}^{n-1} f_i x^i \in \mathrm{R}$

$[f]_L = \sum_{i=0}^{n-1} [f_i]_L x^i$

$[f]_M = \sum_{i=0}^{n-1} [f_i]_M x^i$

Figure 5: Some definitions of the rounding operator.

Infinity norm:

$max_k\ (f)$: *returns the k–th largest absolute coefficient of f*

for $c \in \mathbb{Z}_q$, $||c||_\infty = |c\ mod^{\pm}q|$

infinity norm of polynomial ($f \in R$): $||f||_\infty = \max_i ||f_i||_\infty$

Figure 6: Some definitions of the infinity norm.

information of the nodes joining the KAD network will not be attacked.

BitTorrent. BitTorrent is a content distribution protocol. The rationale is as follows: users forward portions of content they know to each other until each user gets all of it. This technique enables nodes in two peer-to-peer systems to send and receive files without having to trust each other.

SFS (Self-Certifying File System). SFS is a self-authenticating file system that can be shared globally. On the SFS network, various key management mechanisms can be built. This file system separates key revocation from cipher distribution and does not affect key recovery.

Git. A distributed version control system.

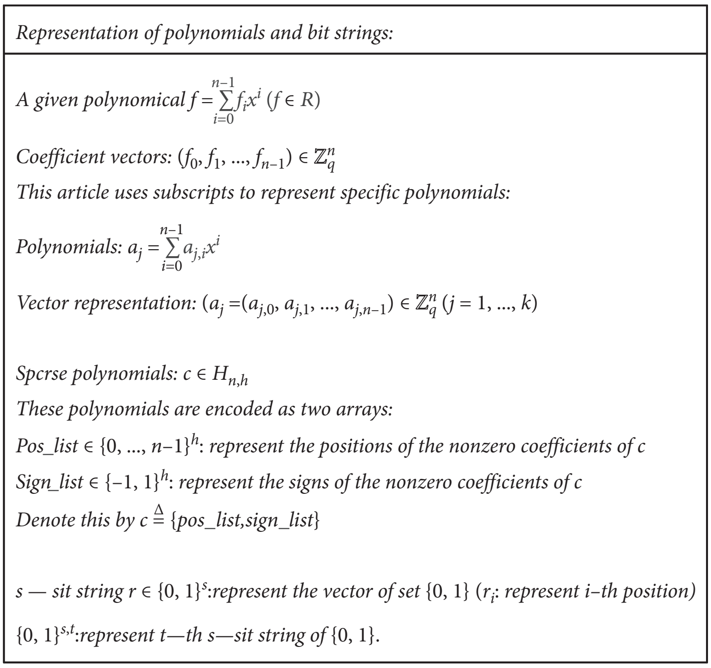
IPFS Technical Summary. Combining the advantages of the above four technologies, IPFS [28, 29] protocol constructs a globally distributed file system. IPFS does not immoderately distribute files in your local repository to other IPFS nodes. If no other IPFS nodes search your files, the files in your local repository will always exist locally. IPFS protocol has the characteristics of fast download, permanent storage of files, and natural resistance to DDOS attacks.

4. Quantum-Resistant Blockchain System Based on qTESLA

In this section, we describe the designed secure blockchain against quantum search algorithm and carried out experimental verification of the above theory. We simulate a bitcoin transaction simulation scenario and construct a blockchain system based on a quantum-resistant digital signature. In this system, we set up three time periods. Figure 14 shows our system architecture. Table 1 shows our experimental environment.

4.1. Phase A: Account Create. The wallet is used to create an account. And it contains several modules: a module to generate public-private key pairs, a module to generate account addresses, and a signature module.

In this phase, the node generates a pair of public and private keys from the signature algorithm of the wallet. *pk* generates the address of this account through a hash algorithm. *sk* is used to generate the signature. Then, we upload the public key to *IPFS* and get a hash sequence. In the future, the hash sequence will represent the public key. And it is much smaller than the original public key. So it is much better to write the $hash_{IPFS}$ into the transaction and store $hash_{IPFS}$ than to just manipulate the string of the public key.



Representation of polynomials and bit strings:

A given polynomical $f = \sum_{i=0}^{n-1} f_i x^i$ ($f \in R$)

Coefficient vectors: $(f_0, f_1, ..., f_{n-1}) \in \mathbb{Z}_q^n$

This article uses subscripts to represent specific polynomials:

Polynomials: $a_j = \sum_{i=0}^{n-1} a_{j,i} x^i$

Vector representation: $(a_j = (a_{j,0}, a_{j,1}, ..., a_{j,n-1}) \in \mathbb{Z}_q^n$ $(j = 1, ..., k)$

Spcrse polynomials: $c \in H_{n,h}$

These polynomials are encoded as two arrays:

Pos_list $\in \{0, ..., n-1\}^h$*: represent the positions of the nonzero coefficients of c*

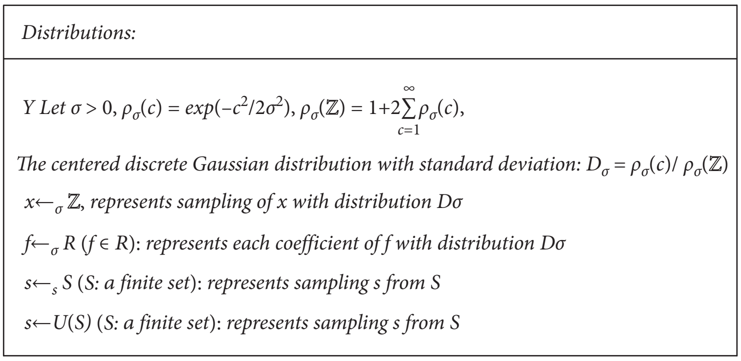
Sign_list $\in \{-1, 1\}^h$*: represent the signs of the nonzero coefficients of c*

Denote this by $c \overset{\Delta}{=} \{pos\_list, sign\_list\}$

s — sit string $r \in \{0, 1\}^s$*:represent the vector of set* $\{0, 1\}$ (r_i*: represent i–th position)*

$\{0, 1\}^{s,t}$*:represent t—th s—sit string of* $\{0, 1\}$.

Figure 7: Some definitions of representation of polynomials and bit strings.



Distributions:

Y Let $\sigma > 0$, $\rho_\sigma(c) = exp(-c^2/2\sigma^2)$, $\rho_\sigma(\mathbb{Z}) = 1+2\sum_{c=1}^{\infty} \rho_\sigma(c)$,

The centered discrete Gaussian distribution with standard deviation: $D_\sigma = \rho_\sigma(c)/\ \rho_\sigma(\mathbb{Z})$

$x \leftarrow_\sigma \mathbb{Z}$*, represents sampling of x with distribution Dσ*

$f \leftarrow_\sigma R$ ($f \in R$)*: represents each coefficient of f with distribution Dσ*

$s \leftarrow_s S$ (*S: a finite set*)*: represents sampling s from S*

$s \leftarrow U(S)$ (*S: a finite set*)*: represents sampling s from S*

Figure 8: Some definitions of distributions.

4.2. Phase B: Transactions Generates. We are working on the assumption that account A transferred 0.3 bitcoins to account B. In a blockchain, transaction information is written in UTXO. Our system divides UTXO into two parts, the input and the output. And we set up two scripts which are the signature script and the unlocking script. In Figure 15, 1 and 2 belong to the input script and 3 belongs to the unlocking script.

As shown in Figure 16, when A initiates a transaction, it is divided into two steps:

Step 1: we make a message of the transaction for the signature. This message contains the address of *A*, the id of the transaction, the number of transactions output, and the entire output.

Step 2: the transaction is signed by qTESLA. Then, we enter the signature information and the IPFS hash sequence of *A* in the signature script.

4.3. Phase C: Charge. As shown in Figure 17, the transaction is broadcast through the P2P network structure and waits for verification by *B* and other miner nodes. After receiving the transaction, the miner node verifies the transaction by getting *A*'s public key from the IPFS network through.

The mining node packages trades in the nearest time period into blocks (candidate blocks). The miner calculated a difficult hash value (POW consensus algorithm), which was verified through the whole network and then written into the blockchain.

5. Experiment and Analysis

The system uses quantum-resistant digital signatures, so its security is impeccable. In this section, we explore the performance and efficiency of the system.

Under the same simulation scenario, we tested three different blockchain systems: (1) quantum-resistant

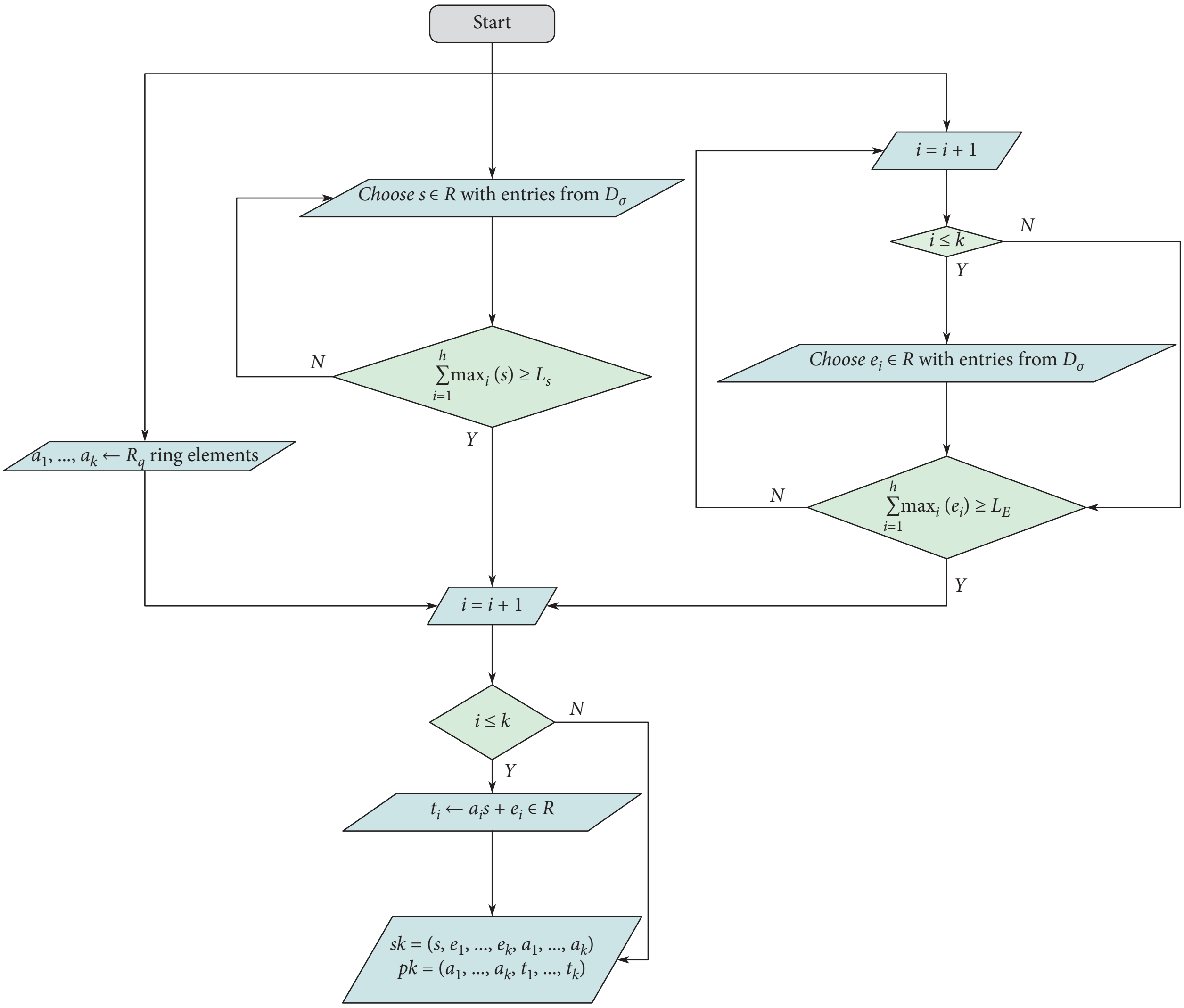

Start
Choose $s \in R$ with entries from D_σ
$\sum_{i=1}^{h} \max_i (s) \geq L_s$
N
Y
$a_1, \ldots, a_k \leftarrow R_q$ ring elements
$i = i + 1$
$i \leq k$
N
Y
Choose $e_i \in R$ with entries from D_σ
$\sum_{i=1}^{h} \max_i (e_i) \geq L_E$
N
Y
$i = i + 1$
$i \leq k$
N
Y
$t_i \leftarrow a_i s + e_i \in R$
$sk = (s, e_1, \ldots, e_k, a_1, \ldots, a_k)$
$pk = (a_1, \ldots, a_k, t_1, \ldots, t_k)$

Figure 9: Key generation.

blockchain system employs IPFS and qTESLA. (2) Quantum-resistant blockchain system employs qTESLA without IPFS. (3) And blockchain system based on elliptic curve cryptography cannot resist quantum attack.

5.1. Efficiency. In our simulation system, the transactions are sequential. A signature and a verification are generated while a transaction is created. Each system was tested 1,000 times to get the duration of the signature, the duration of verification, and the duration of the transaction.

Table 2 shows that the average time of blockchain based on the elliptic curve is the shortest in the three systems. But the blockchain based on the elliptic curve cryptography cannot guarantee security. In addition, POW (Proof of Work) can take up a lot of time when a block generates. The duration of the transaction is negligible. We have reached the conclusion that the average mining time (workforce) is 2 seconds when the difficulty is 5 (a hash value that the first five digits is 0).

5.2. Analysis. The standard deviations of the time taken for these three systems are shown in Table 3. The Table 3 shows that the qTESLA based blockchain system has the most stable performance. The time of qTESLA based blockchain with IPFS will be -instability due to the network. But the time is within acceptable limits.

As shown in Table 4, we processed the maximum and minimum values of the transactions' time in each system according to equation (1). The smaller the value, the better the stability. This result confirms our system is more stable:

$$\text{percentage} = \frac{\text{MAX} - \text{MIN}}{\text{MAX} + \text{MIN}}. \quad (1)$$

5.3. Blockchain System Analysis with or without IPFS. In this section, we evaluate the performance of blockchain used IPFS network. This system not only resists the attack of quantum algorithm but also relieves the stress of capacity. And it is more efficient than blockchain systems without IPFS, when the difficulty of PoW is appropriate.

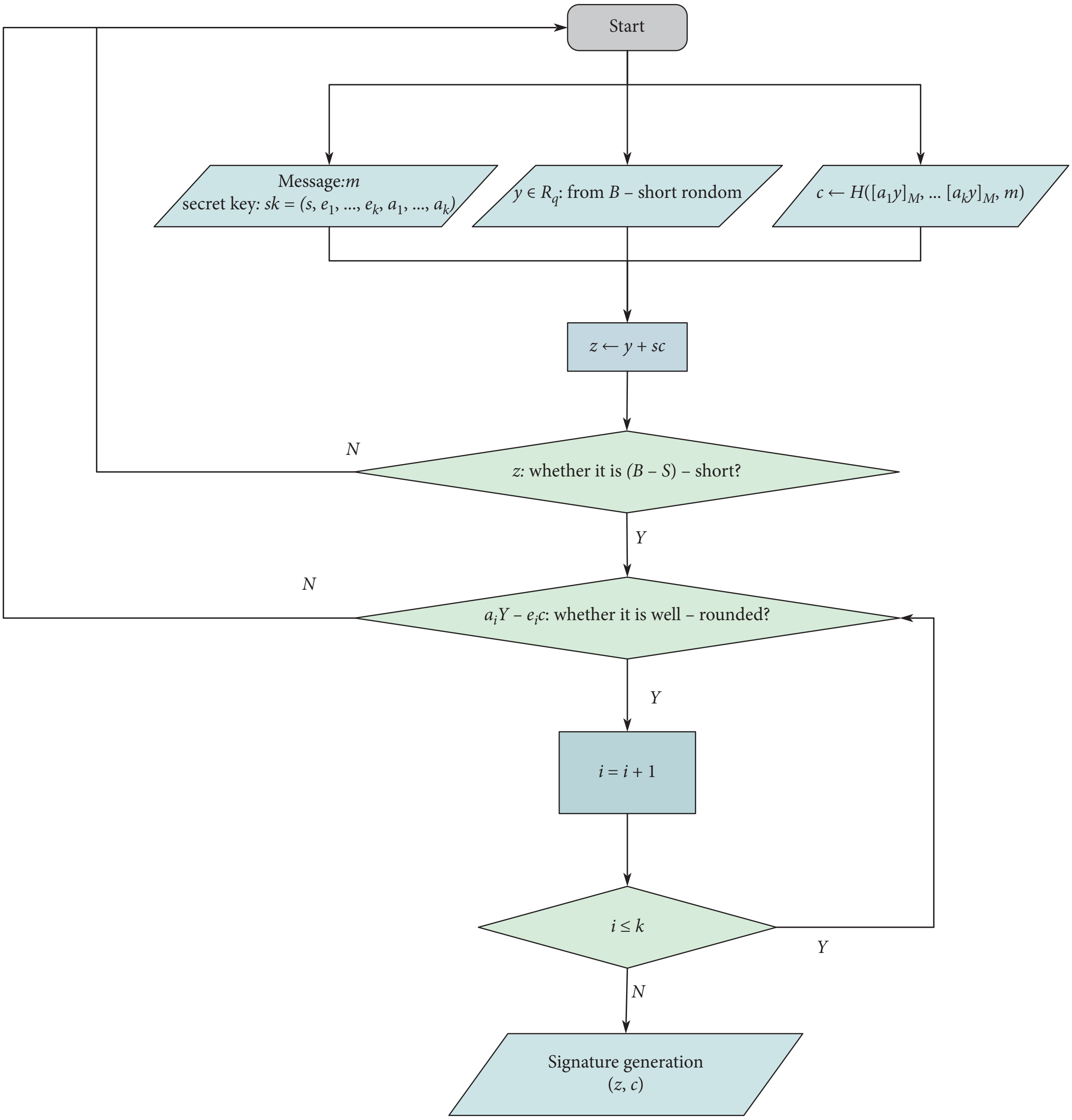

Start
Message:m
secret key: $sk = (s, e_1, ..., e_k, a_1, ..., a_k)$
$y \in R_q$: from B – short rondom
$c \leftarrow H([a_1 y]_M, ... [a_k y]_M, m)$
$z \leftarrow y + sc$
N
z: whether it is $(B - S)$ – short?
Y
N
$a_i Y - e_i c$: whether it is well – rounded?
Y
$i = i + 1$
$i \leq k$
Y
N
Signature generation
(z, c)

Figure 10: Signature.

As shown in Table 5, we measured some parameters about the size of each part of the UTXO (unspent transaction outputs) which is written into the block. Obviously, the number of bytes occupied by each transaction is greatly reduced. Through the test, we get the duration of each part of the transaction in Table 6. The duration of mining and the size of block together determine how long it takes to create a block. According to the data in Tables 5 and 6, we analyzed and concluded the blockchain system with IPFS is more efficient than the blockchain system without IPFS under suitable mining time in different block sizes. Table 7 lists the specific analysis values. The minimum mining time increases linearly as the size of the blockchain changes.

We set the size of block to 0.125 M and set the difficulty of PoW to 5. After each block has been packaged up, the miner can verify the transactions. And transactions are sequential. In the IPFS based blockchain, each block can be written to 88 transactions approximately and we set up two blocks which are put into 88 transactions. The block contains 3.58 transactions at most in the blockchain without IPFS and we set 3 transactions per block. There are 30 blocks. The experimental results show that the blockchain system with

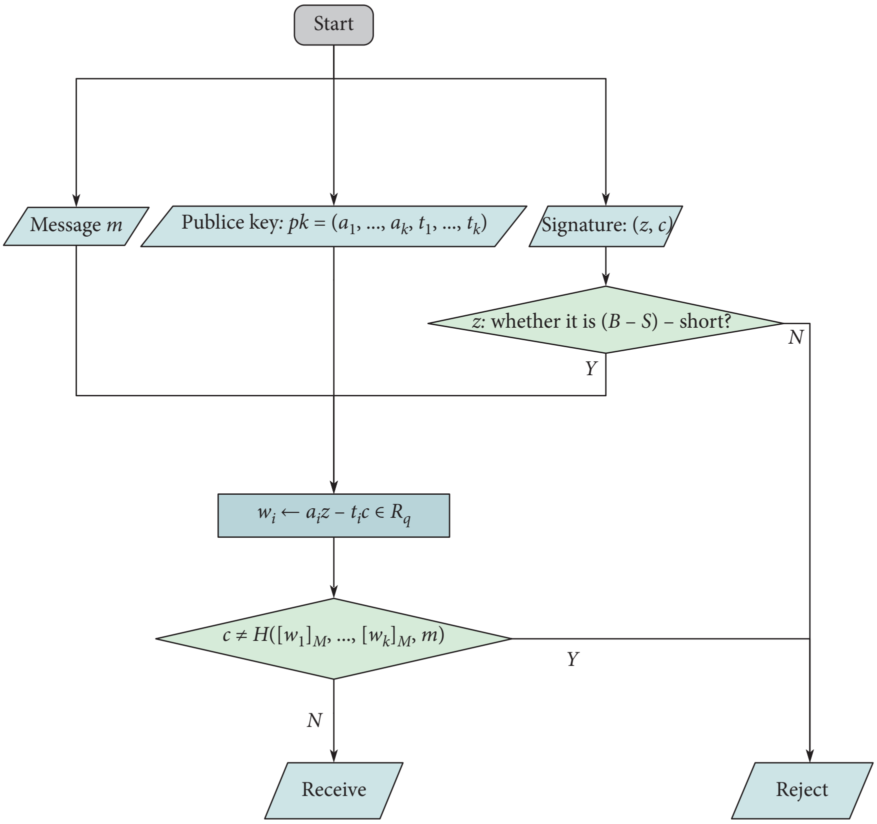

Start
Message m
Publice key: $pk = (a_1, ..., a_k, t_1, ..., t_k)$
Signature: (z, c)
z: whether it is $(B - S)$ – short?
N
Y
$w_i \leftarrow a_i z - t_i c \in R_q$
$c \neq H([w_1]_M, ..., [w_k]_M, m)$
Y
N
Receive
Reject

FIGURE 11: Verification.

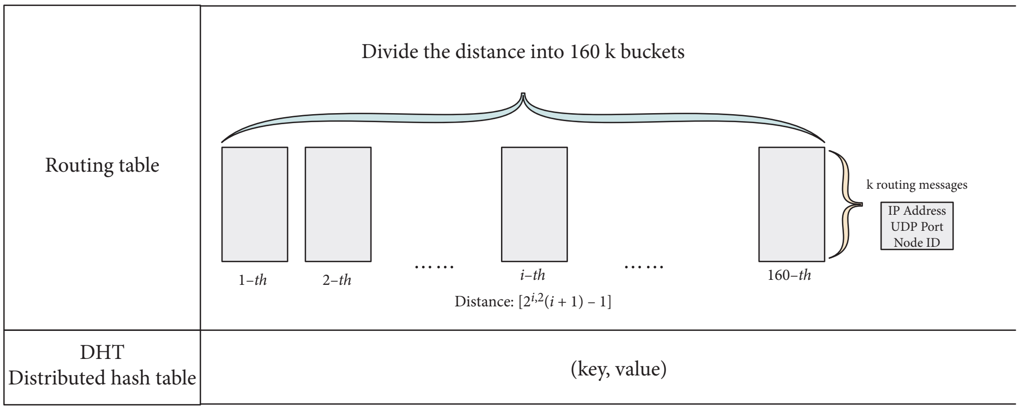


FIGURE 12: The structure of S/Kademlie.

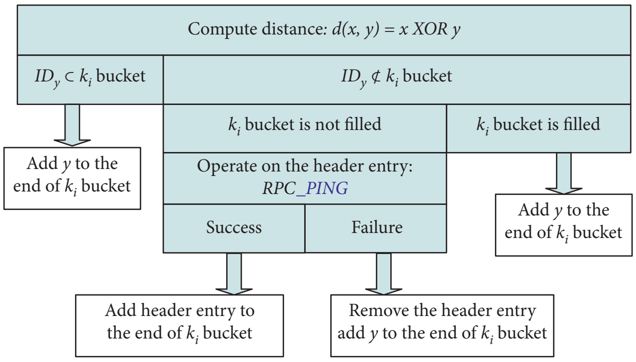

Compute distance: $d(x, y) = x$ XOR y
$ID_y \subset k_i$ bucket
$ID_y \not\subset k_i$ bucket
k_i bucket is not filled
k_i bucket is filled
Add y to the end of k_i bucket
Operate on the header entry: RPC_PING
Success
Failure
Add y to the end of k_i bucket
Add header entry to the end of k_i bucket
Remove the header entry add y to the end of k_i bucket

FIGURE 13: Add information.

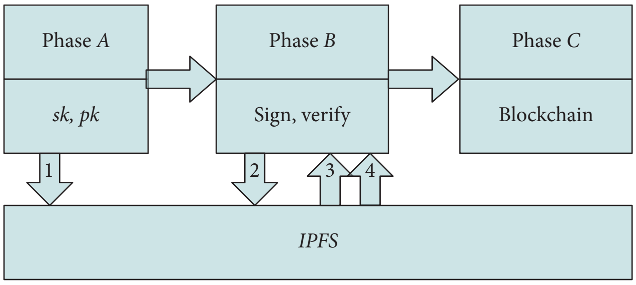
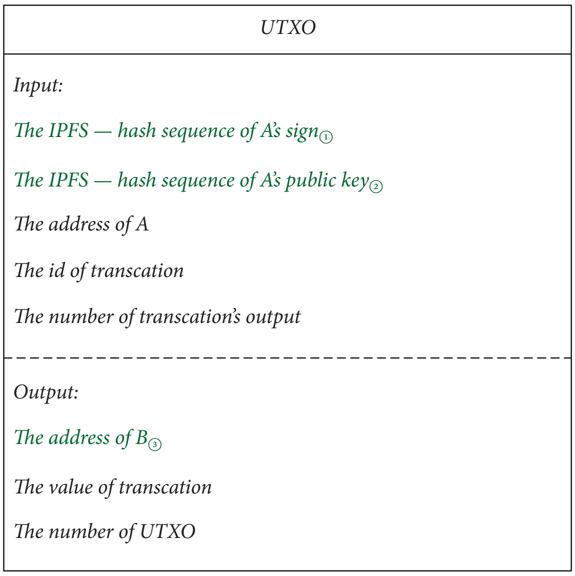


Figure 14: System architecture. sk represents the private key. pk stands for the public key. 1 and 2 are the upload process. 3 and 4 are the download process.

Table 1: Experimental environment.

Language	C(qTESLA) + Python (bitcoin exchange simulation scenario)
CPU	IntelRCoreTM i5-4570 CPU@3.20 GHz*4
System	Ubuntu



UTXO

Input:

*The IPFS — hash sequence of A's sign*①

*The IPFS — hash sequence of A's public key*②

The address of A

The id of transcation

The number of transcation's output

Output:

*The address of B*③

The value of transcation

The number of UTXO

Figure 15: The structure of the UTXO.

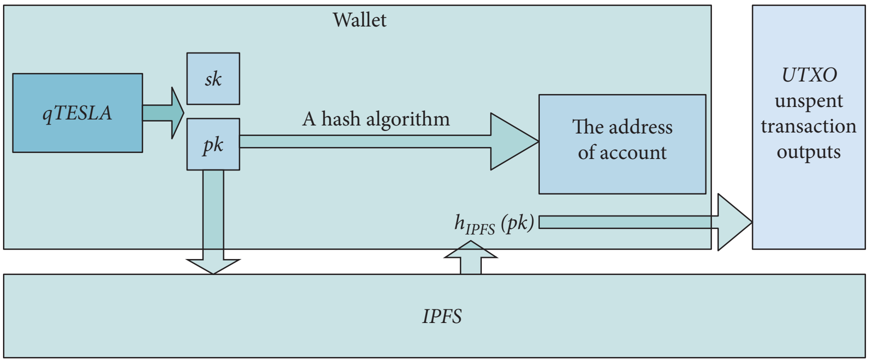


Figure 16: The public key is uploaded to the IPFS network.

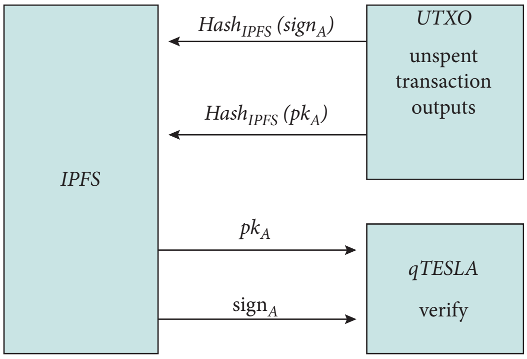


Figure 17: Miners get signatures and public keys from the IPFS.

Table 2: The average time of the signatures, verifications, and transactions.

System	ecdsa (s)	qTESLA (s)	qTESLA + IPFS (s)
Sign	0.0000195181217838204	0.0346034601243446	0.0705189092395684
Verify	0.0163973578420132	0.179651395134396	0.413346856886305
Transaction	0.0153545810636715	0.21463521849722	0.478353481311409

Table 3: The standard deviations for time of the signatures, verifications, and transactions.

System	ecdsa (s)	qTESLA (s)	qTESLA + IPFS (s)
Sign	0.000015735742425981	0.00369555959639125	0.0083706810517413
Verify	0.00651873643683476	0.0040036475046505	0.0100564873479481
Transaction	0.00217918300595782	0.0051345665106179	0.0160881929765899

Table 4: The maximum and minimum transaction times of the three systems are added and subtracted.

System	ecdsa	qTESLA	qTESLA + IPFS
Percentage	56.636%	13.721%	19.878%

It is the ratio of the latter to the former.

Table 5: The contents of the transaction and its size.

System	Public key (B)	Sign (B)	Other (B)
qTESLA	29760	5450	1390+
qTESLA + IPFS	47	47	1390+

Table 6: The average of blockchain's signature, verification, and transaction.

System	Transaction (s)	Sign (s)	Verification (s)
qTESLA	0.0337992995951315	0.03337018944616243	0.179651395134396
qTESLA + IPFS	0.105081087620143	0.105003335806339	0.413346856886305

IPFS is more efficient than the blockchain system without IPFS under suitable mining time in different block sizes.

Table 7: Suitable mining time in different block sizes guarantees that the blockchain system with IPFS is more efficient than the blockchain system without IPFS.

Block size (M)	Mining time (s)
0.125	1.3
0.25	2.23
0.5	4.5
1	9.06

6. Conclusions

With the rapid development of quantum computer, quantum-resistant blockchain system research is extremely urgent. In this paper, we draw a blockchain resisting quantum attacks. The qTESLA digital signature based on lattice cipher, which cannot be broken by quantum algorithm, is applied to the blockchain, and its public keys and signs are stored on the IPFS network. Thus, this way not only solves the problem of quantum attack but also solves the problem of block capacity. We have tested and analyzed our system. We have verified the feasibility and stability of our system and given some data reference. In the future, we can make a practical application based on our blockchain system.

The realization of our system increases confidence for future research on quantum-resistant blockchain. And we provide a new idea to deal with the problem of public keys' length. The experimental results show that our experiment is feasible. And with the suitable difficulty of POW, our system will be better. With the rapid development of 5G, IPFS networks will become faster and faster so that our systems will become more efficient. In the construction of smart cities, the blockchain technology has been applied more widely and deeply, such as government affairs, people's livelihood, and urban governance. Our solution uses quantum-resistant signatures to enhance the security of the blockchain and provide security for the construction of smart cities.

Our experiment has some limitations that parallel transactions are not allowed, in the experiment. However, we can ignore the limitations. Because, in the real network, there are many uncertain factors in the transaction. We only test the individual deals.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Key Research and Development Program of China (2018YFB0804104 and 2018YFC0830102), National Natural Science Foundation of China (61702309), Shandong Provincial Key Research and Development Program (2018CXGC0701, 2019JZZY020127, 2019JZZY020129, 2019JZZY020715, 2019JZZY010134, and 2019GGX105003), the Key Research and Development Program of Shandong Academy of Science, and the Science, Education, and Industry Integration Innovation Program of Qilu University of Technology (Shandong Academy of Science) (2020KJC-GH11 and 2020KJC-ZD02).

References

[1] K. Su, J. Li, and H. Fu, "Smart city and the applications," in *Proceedings of the 2011 International Conference on Electronics, Communications and Control (ICECC)*, pp. 1028–1031, Ningbo, China, September 2011.

[2] M. Lou, X. Dong, Z. Cao, and J. Shen, "SESCF: a secure and efficient supply chain framework via blockchain-based smart contracts," *Security and Communication Networks*, vol. 2021, Article ID 8884478, 18 pages, 2021.

[3] E. Sixt, Ethereum, 2017.

[4] C. Yang, L. Tan, N. Shi et al., "AuthPrivacyChain: a blockchain-based access control framework with privacy protection in cloud," *IEEE Access*, vol. 8, 2020.

[5] A. Murray, "Electronic payments and cryptocurrency," *Information Technology Law*, ResearchGate, Berlin, Germany, 2019.

[6] M. Mettler, "Blockchain technology in healthcare: the revolution starts here," in *Proceedings of the 2016 IEEE 18th International Conference on E-Health Networking, Applications and Services (Healthcom)*, IEEE, Munich, Germany, September 2016.

[7] Y. Zhang and J. Wen, "The IoT electric business model: using blockchain technology for the internet of things," *Peer-to-Peer Networking and Applications*, vol. 10, no. 4, pp. 983–994, 2017.

[8] P. Mohit and G. P. Biswas, "Modification of traditional RSA into symmetric-RSA cryptosystems," *International Journal of Business Data Communications and Networking*, vol. 13, no. 1, pp. 66–73, 2017.

[9] K. Okeya and K. Sakurai, "Efficient elliptic curve cryptosystems from a scalar multiplication algorithm with recovery of the y-coordinate on a montgomery-form elliptic curve," *Cryptographic Hardware and Embedded Systems*, vol. 2162, pp. 126–141, 2001.

[10] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *Siam Review*, vol. 41, no. 2, pp. 303–332, 1999.

[11] O. Regev, "New lattice-based cryptographic constructions," *Journal of the ACM*, vol. 51, no. 6, pp. 899–942, 2004.

[12] P. Benioff, "Quantum mechanical Hamiltonian models of turing machines," *Journal of Statistical Physics*, vol. 29, no. 3, pp. 515–546, 1982.

[13] M. Poornima, H. Ingrid, R. Clemens et al., "Altered surfactant homeostasis and alveolar epithelial cell stress in amiodarone-induced lung fibrosis," *Toxicological Sciences*, vol. 142, no. 1, pp. 285–297, 2014.

[14] G. L. Ajtai, "Twenty-eighth ACM sym-posium on theory of computing," in *Proceedings Of The Twenty-Eighth Annual ACM Symposium On Theory Of Computing*, Philadelphia, PA, USA, May 1996.

[15] D. Aharonov and M. Benor, "Quantum computation of Fourier transforms over symmetric groups," in *Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing*, El Paso, TX, USA, May 1997.

[16] P. C. Kuo and C. M. Cheng, "Lattice-based cryptanalysis-how to estimate the security parameter of lattice-based cryptosystem," in *Proceedings of the IEEE International Conference on Consumer Electronics*, IEEE, Taipei, Taiwan, May 2014.

[17] Y. Pan, Y. Deng, Y. Jiang, and Z. Tu, "A new lattice-based public-key cryptosystem mixed with a knapsack," *Cryptology and Network Security*, vol. 7092, pp. 126–137, 2011.

[18] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *Proceedings of the Annual ACM Symposium on Theory of Computing*, vol. 56, no. 6, 2009.

[19] R. Ladner and C. Dwork, "Symposium on theory of computing," in *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*, Columbia, SC, USA, May 2008.

[20] Z. Yanhua, H. Yupu, J. Mingming et al., *Lattice-Based Sequential Aggregate Signatures With Lazy Verification*, The Journal of China Universities of Posts and Telecommunications, Beijing, China, 2015.

[21] C. Y. Li, X. B. Chen, Y. L. Chen et al., "A new lattice-based signature scheme in post-quantum blockchain network," *IEEE Access*, vol. 7, 2019.

[22] Y. Gao, X. Chen, Y. Sun et al., "A secure cryptocurrency scheme based on post-quantum blockchain," *IEEE Access*, vol. 6, 2018.

[23] W. Yin, Q. Wen, W. Li et al., "An anti-quantum transaction authentication approach in blockchain," *IEEE Access*, vol. 6, 2018.

[24] G. Yao, G. Wang, and Y. Wang, "An improved identification scheme," *Coding, Cryptography and Combinatorics*, Springer, Berlin, Germany, 2004.

[25] A. Shamir, "Variants of the fiat-shamir identification and signature scheme," *Advances in Cryptology*, Springer, Berlin, Germany, 1990.

[26] J. Benet, *Ipfs-Content Addressed, Versioned, p2p File System*, Eprint Arxiv, Ithaca, NY, USA, 2014.

[27] X. Delord, S. Perret, and A. Duda, "Efficient mobile access to the WWW over GSM," in *Proceedings of the 8th ACM SIGOPS European Workshop on Support for Composing Distributed Applications*, Dresden, Germany, June 1998.

[28] M. S. Ali, K. Dolui, and F. Antonelli, "IOT data privacy via blockchains and IPFS," in *Proceedings of the Seventh International Conference on the Internet of Things*, pp. 1–7, Linz, Austria, October 2017.

[29] Y. Chen, H. Li, K. Li, and J. Zhang, "An improved p2p file system scheme based on IPFS and blockchain," in *Proceedings of the 2017 IEEE International Conference on Big Data (Big Data)*, Boston, MA, USA, December 2017.