IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 8, 2019, accepted August 29, 2019, date of publication September 12, 2019, date of current version October 4, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2941153

A Blockchain Smart Contract Based on Light-Weighted Quantum Blind Signature

ZHENGYING CAI, JING QU, PINGPING LIU, AND JIAO YU
College of Computer and Information Technology, China Three Gorges University, Yichang 443002, China

Corresponding author: Zhengying Cai (master_cai@163.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 71471102, in part by the Science and Technology Research Program of Hubei Provincial Department of Education in China under Grant D20101203, and in part by the Yichang University Applied Basic Research Project in China under Grant A17-302-a13.

ABSTRACT To improve the security performance of blockchain smart contracts against quantum attacks, a smart contract based on light-weighted quantum blind signature is proposed here. Firstly, a smart contract architecture is built after the discussion of related researches, and information processing and information transmitting for quantum blind signature are analyzed. Secondly, the life cycle and signature rules of quantum blind signature for smart contracts are presented. Thirdly, a quantum blind signature protocol for single signer in light-weighted smart contract is put forward, where its algorithm design and business flow are introduced in detail before the security performance of the proposed algorithm is analyzed. Fourthly, based on the former single-person signature algorithm, a more complex multi-person quantum blind signature algorithm is proposed, and its security is also analyzed. Fifthly, related references are compared to verify the proposed method. The proposed quantum signature schemes based on quantum entanglement features can be used in single signer case or more, and will improve the security of blockchain smart contracts against quantum attacks, but with light-weighted structure and no need of any trusted third party or arbitrary institute. Finally, some suggestions for engineering applications and the research results are summarized and the future research is prospected.

INDEX TERMS Blockchain, smart contract, blind signature, quantum signature.

I. INTRODUCTION

With the fast development and increasingly widespread application of blockchain technology, smart contracts have recently received great attention [1], [2]. In the blockchain system, all business parties can use a non-centralized distributed ledger to share data, and use smart contracts to set a predetermined time and condition to automatically complete the payment process [3], [4], greatly improving work efficiency, but also significantly reducing the problems caused by manual operations and other factors [5]. Therefore, secure smart contract technology plays an extremely important role in blockchain technology, which can safely program and digitize various business processes to reduce manual intervention [6]. To improve the security of blockchain smart contracts, relevant researches focus on main directions as follows.

(1) To setup a transaction verification mechanism for smart contracts. Smart contracts need to provide an automatic information verification mechanism for blockchain services, both to ensure that trading business are automatically verified according to smart contracts, and to ensure that blockchain business data is publicly available [1], [2]. Some scholars used an anti-counterfeiting technology [4] to establish a centrally-free account book on each block in the blockchain, which can automatically and intelligently record every fund flow generated in business operations. The smart contract can connect the distributed ledgers in different locations to verify the relevant data. Some scholars also tried to improve the security of the transaction verification mechanism [6], [7], in order to ensure that every account record is irretrievably adjusted under a secure smart contract. The role-based access mechanism [8] can also effectively guarantee the security and traceability of smart contracts.

(2) To build a privacy protection mechanism in smart contracts. In a general signature process of contracts, the signer needs to remember the signatures he has made, including the timestamp and the signature location, as well as the signed message and business object [4]. Robust control techniques were used in smart contracts [9] to improve the

The associate editor coordinating the review of this manuscript and approving it for publication was Chien-Ming Chen.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see http://creativecommons.org/licenses/by/4.0/

anti-jamming capabilities and privacy protection of payment systems. In blockchain business and smart contracts, anonymous technology [10] was adopted to protect privacy, so a blockchain or trader will not achieve the user's historical consumption records by tracing his signature. Reference [11] applied anti-counterfeiting technology to record the verification information on the blockchain, where on the one hand, the public can query the information but can not erase it, on the other hand, it also ensures that all cash is in the process of business flow and no one knows who are the previous users or the next one.

(3) To establish a data signature mechanism in smart contracts. For example, some scholars proposed a secure attribute-based signature scheme [12]. Once the signatures of the traders are checked and recorded in smart contracts, the signature operation of both parties can ensure the safe and orderly execution of the transaction process. Other researchers presented an ID-based signature scheme [13], where the non-repudiation, non-tampering and automatic execution of the transaction are technically guaranteed by the computer program through confirming the ID signature and the contract rules, so complete autonomy of the network can be realized by the smart contract. Some people proposed a smart contract with more complex multi-signatures [14], which is equivalent to a computer program and supporting equipment rather than an artificial intelligence or legal contract, and is limited to assisting multiple business parties to process transactions according to predefined conditions. Related researches, such as blockchain security detection model [15], and grid-based hidden attribute signature [16], were also put forward to improve the security of smart contracts to some extent.

However, security improving on smart contacts of researches above is based on the algorithm complexity, and the schemes with higher security will increase the burden in implementing smart contracts under the quantum attack environment. Here a light-weighted quantum blind signature scheme is proposed for smart contracts without a trusted arbitrator and is proved unconditionally secure independent of the algorithm complexity.

The structure of the full text is arranged as follows: Section II discusses the research background of this paper and related research progress, which leads to the research content of this paper. Section III introduces the basic architecture and mathematical model of smart contract based on quantum blind signature, and analyzes its information processing of quantum signature and quantum information transmission methods for smart contracts. Section IV presents the lifecycle of smart contracts and signature rules based on quantum blind signatures, paving the way for later chapters. Section V puts forward a single-person based quantum blind signature algorithm and security analysis. Section VI builds a more complex multi-person quantum blind signature algorithm based on the proposed single-person quantum blind signature algorithm, and analyzes its security. Section VII compares related algorithms in references and gives engineering application reference recommendations. The final section summarizes the full text and gives future research directions.

II. RELEVANT WORK

Although recent researches tried their best to improve the security of smart contracts, some shortcomings are still needed to be further solved.

(1) Security of blockchains and smart contracts in relevant work is mainly based on the complexity of algorithms and is vulnerable to quantum attacks [3], [4]. Fedorov *et al.* (2018) published a paper in *Nature* and concerned that blockchains and smart contracts may face security challenges from quantum technology [17]. Security of traditional smart contracts in the virtual world depends on the security technology of blockchain and the security mechanism of classical algorithms. Quantum attacks are taken as great threats to traditional encryption algorithms. Therefore, some scholars also tried to improve cryptographic algorithms against quantum attacks, mainly focusing on cryptographic techniques of hash functions [12], coding cryptography [14], [15], lattice cryptography [16] and cryptography by multivariate quadratic equations [18], etc. However, the security of these algorithms is still based on the algorithm's complexity, which is taken as relatively secure, that is, higher security means more complicated encryption and decryption processes. When these cryptographic techniques are applied to blockchains and smart contracts, it is very easy to cost more time for signature and verification, resulting in the reduced efficiency of blockchain transactions and smart contract execution.

(2) Current privacy protection of smart contract in relevant works is also been threatened, especially with the advancing of quantum computing and attacks. On July 19, 2017, three of the largest Ethereum accounts were stolen by the multi-signature vulnerability in Parity Wallet's wallet ''multi-sig'' code because the creation process of wallet's multi-signature lacked protection letting the attacker be able to reset the ownership and arbitrary parameters of existing wallet [4]. If an attacker used quantum attack, the multi-signature and privacy protection of the smart contract will be faced with greater threats [17]. At present, public key systems and blind signature techniques were introduced into multi-signature [19]–[21] to improve the security and privacy protection of multi-signature technology. However, because classical privacy protection algorithms still rely on computational complexity, their application in blockchain smart contracts will reduce the transaction efficiency, and the fast development of quantum attacks will also pose a great threat to these programs.

(3) The complex time dependence in smart contracts raises inefficiency issues of greatly growing database [3], [4]. The smart contract records all the states and changes from its birth to current time point in the blockchain. There are strict time dependence and order dependencies between signers, and each node retains data backup in the blockchain. As the blockchain business grows, it will need greater data storage and make its security verification be more difficult.

Most smart contracts have to cut down security for weight reduction, and vice versa. Therefore, it is very difficult to find an effective way to balance the confliction between lightweight and security in classical secure technologies [4]. In the absence of a traditional monitoring mechanism, the human error being implied in smart contracts also puts higher demands on the dispute handling of blockchain transactions. If quantum attacks exploit this implicit human error and trading loopholes, it may easily lead to transaction failure.

Fortunately, quantum technology also brought us new improving opportunities while it challenged traditional smart contract technologies [17]. Quantum signature technology brings theoretical absolute security to data security because of its unique physical characteristics [18]. Related results in e-commerce fields are mainly divided into two categories, namely multi-person signature techniques [19]–[22] and blind signature techniques [21]–[24]. Based on the quantum blind signature technology [21], [22] appeared in recent years, this paper proposes a light-weighted quantum signature schemes suitable for smart contracts.

III. SMART CONTRACT ARCHITECTURE BASED ON QUANTUM BLIND SIGNATURE

A. BASIC ARCHITECTURE

To improve the security of light-weighted architecture against quantum attacks, our solution is to use a quantum key distribution(QKD) based on quantum entanglement for remote communication to carry out a single-person non-arbitrated signature protocol. In the signature process of smart contracts, the central institution or the arbitrator is not required, and the business information of smart contracts can be blindly signed for business guarantee. Therefore, privacy can be protected by both high security and high efficiency. According to references [1]–[4], [6]–[9] and [12]–[14], on blockchain smart contracts, and references [19]–[24] on quantum signature, the smart contract architecture based on quantum blind signature is built by five main levels: user layer, data layer, management layer, verification layer and execution layer, as shown in Figure 1.

The user layer includes user authority management, account management, security verification, user reputation management, and user's quantum blind signature. It provides the basic underlying software and hardware platforms for smart contract businesses, including networks, communication facilities, and signature agreements to process classic information and quantum information. The data layer includes data acquisition, data cleaning, data processing, data storage, and quantum information processing. It has classic data and quantum data on and out of the blockchain, offering various business data services for smart contracts. The management layer encapsulates the core business management modules such as contract management, protocol management, parameter management, business management, and quantum key management, and can process contract coding protocols, contract texts, contract standards, and quantum key distribution parameters used by contract parties.

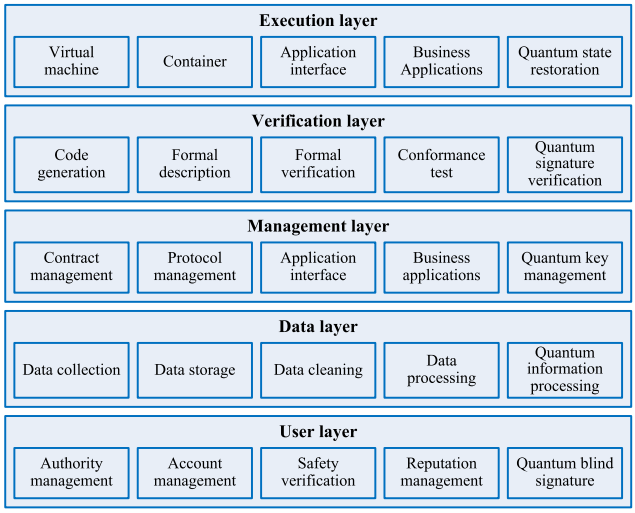

FIGURE 1. Architecture of blockchain smart contract based on quantum blind signature.

The verification layer mainly includes all kinds of verification methods such as code generation, formal description, formal verification, conformance testing, and quantum signature verification to ensure the consistency of contract code and contract text. The execution layer includes virtual machine, container (Docker), application interface, business application, quantum state restoration, and other related software or hardware platforms processing smart contracts. It provides necessary operating environment and services for blockchain smart contracts, and can transform quantum information into classical information for further application.

The smart contract architecture in Figure 1 defines a set of commitments in the form of classical and quantum information, where all participants of the contract will automatically execute the commitments in the contract business. Obviously, the proposed architecture based on quantum blind signature is in essence an automatic contract protocol to be able to process classic information and quantum information. On the one hand, it can meet various contract conditions including payment rights, mortgage, QKD, privacy and confidentiality. On the other hand, it can lower transaction costs, execution costs, and arbitration costs, transaction losses from quantum attacks and contract fraud. Same as all computer programs, the smart contract architecture based on quantum blind signature also requires corresponding support of software, hardware, and pre-set rules, so that all components in the architecture can collaboratively operate without any intermediary, and complete the decentralization contract businesses.

The predefined rules comprise:

(1) Digital assets. The smart contract architecture based on quantum blind signature shown in Figure 1 should digitize all products and services for production and life involved in the transaction process, as well as the product parts, tangible or intangible or non-monetary assets in the business process. They will be stored in a computer as electronic data. Digitized assets are indispensable parts of smart contracts

and can help us limit the rights and obligations of traders, such as product and service delivery, project cooperation and other subject matters. Digital assets should be distributed and shared in smart contracts through interconnected blockchain networks and quantum entanglement channels.

(2) One or more medium of exchange. The smart contract based on quantum blind signature shown in the architecture of Figure 1 must use an easy-to-operate media of exchange, which may be a banknote or coin legally issued by the country, or may be a non-circulating encrypted digital token or other exchangeable notes. Smart contracts often contain an entry for the medium of exchange to be input and output, or an interface for signing and verifying the transaction, and an entry for the quantum signature to implement a blockchain business.

(3) Multiple distributed databases. Smart contracts based on quantum blind signatures also use distributed ledgers to complete transaction accounting for all geographically dispersed nodes, which can jointly monitor the performance of smart contracts and the legality of blockchain transactions. All distributed nodes are capable of manipulating classic information and quantum information, and recording distributed accounts with consensus mechanism by which all nodes can collaboratively demonstrate successful transactions.

According to the rules above, smart contracts based on quantum blind signatures can reduce the dependence on trusted third-party institutions and execute contract terms under specified conditions to avoid disputes, accidents or malicious incidents caused by quantum attacks [6], [7]. Therefore, the ''if-then'' statement similar to the computer language can also be used to implement the trading mechanism of the smart contract. The corresponding contract terms will be implemented once a smart contract is triggered by a predetermined condition, and the finished transaction process will realize the interacting between users and assets in real-world. If the above rules can be safely implemented in smart contracts based on quantum blind signature, the architecture shown in Figure 1 can automatically complete every business without human intervention under quantum attack environment.

B. INFORMATION PROCESSING FOR QUANTUM SIGNATURE

Different from the classical signature algorithms with only classic information, the proposed smart contracts with quantum blind signature use additional quantum information and are based on a quantum system, where the system state satisfies the superposition principle of quantum states. Apparently, the quantum blind signature is completely different from the classical signature methods. If a quantum blind signature state $|\psi\rangle$ may be $|\psi_1\rangle$ or $|\psi_2\rangle$, where in the case, the state $|\psi\rangle$ remains unbroken, then there will be no physical method to certificate whether the state $|\psi\rangle$ is $|\psi_1\rangle$ or $|_2\psi\rangle$. It is assumed that $|\rangle$ denotes a Dirac symbol of quantum state; α, β are two complex constants; $|\psi_1\rangle$, $|\psi_2\rangle$ are both uniform and are orthogonal to each other; the wave function $|\psi\rangle$ of quantum blind signature conforms to the normalization condition $|\alpha|^2 + |\beta|^2 = 1$. Now, the state $|\psi\rangle$ of the quantum blind signature system can be described as a superposition state of these two states $|\psi_1\rangle$ and $|\psi_2\rangle$:

$$|\psi\rangle = \alpha\,|\psi_1\rangle + \beta\,|\psi_2\rangle \tag{1}$$

Based on the superposition principle of quantum state, there is a physical basis for smart contracts to implement massively parallel computing of quantum blind signatures. In quantum signature, a quantum system with two linear independent states can be noted as a qubit, and the two linear independent states of a qubit can be given as $|0\rangle$, $|1\rangle$, respectively. The probabilities of $|0\rangle$, $|1\rangle$ are equal in this superposition state of quantum blind signature, where the state $|\psi\rangle$ contains not only the information of state $|0\rangle$, but also the information of state $|1\rangle$. Hence the signature qubit is the superposition state of $|0\rangle$ and $|1\rangle$, that is

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{2}$$

If these two qubits are employed to form a quantum signature system, then the formed system will be in the superposition state of four states $|0\rangle\,|0\rangle$, $|0\rangle\,|1\rangle$, $|1\rangle\,|0\rangle$, and $|1\rangle\,|1\rangle$. These four different superposition states can be denoted as $\{|0\rangle\,|0\rangle, |0\rangle\,|1\rangle, |1\rangle\,|0\rangle, |1\rangle\,|1\rangle\}$ and can simultaneously exist with a certain probability.

The process of quantum blind signature follows the third basic assumption of quantum mechanics and is a time evolution process of encoding quantum states. $\hat{H}$ is the Hamilton operator of the quantum signature system, which is isolated and determined only by the internal interactions in quantum signature system. The time evolution of a state vector ψ in an isolated quantum signature system can be given as a Schrödinger equation:

$$i\hbar\frac{\partial\psi}{\partial t} = \hat{H}\psi \tag{3}$$

The time evolution of quantum signature state can be denoted by a time evolution operator $\hat{U}$ of an isolated quantum system.

$$|\psi\rangle = \hat{U}(t, t_0)\,|\psi(t_0)\rangle \tag{4}$$

where the time evolution operator $\hat{U}(t, t_0)$ transforms the state $|\psi(t_0)\rangle$ at the moment t_0 to the state $|\psi(t)\rangle$ at time t in the quantum signature system. If the equation (4) is substituted into equation (3), the time evolution operator of quantum signature can be gotten as follow:

$$i\hbar\frac{\partial\hat{U}}{\partial t} = \hat{H}\hat{U} \tag{5}$$

Similar to a Hilbert space with 2^n dimensions and n qubits, the measurement basis of quantum signature can be described as $2^n\{|i\rangle\}$, where i is an n-bit binary string. The quantum blind signature system can prepare a general state of n qubits:

$$|\psi\rangle = \sum_{i=0}^{2^n-1} c_i\,|i\rangle \tag{6}$$

where $|\psi\rangle$ contains 2^n basic states to encode 2^n binary numbers for quantum blind signature.

C. QUANTUM INFORMATION TRANSMISSION

Quantum key distribution used by smart contracts does not adopt the classical blockchain network, but the entanglement channel for transmitting quantum information or quantum states, realizing the remote distribution and secure transmission of quantum signature keys with unconditional security. In 1984, American scientists Charles Henry Bennett and Gilles Brassard proposed the first quantum key distribution scheme, namely the BB84 protocol, which opened the era of quantum cryptography. The protocol is based on the quantum non-cloning principle and uses two sets of orthogonal quantum bases to implement key distribution. In 1992, Bennett proposed a simplified, halved efficiency scheme, the B92 protocol. These two schemes are also the basis for the safe implementation of the quantum blind signature scheme in this paper. Quantum information transmission in this paper is mainly used to establish and transmit quantum keys in smart contracts, instead of transmitting plaintext or ciphertext. According to the uncertainty principle of quantum mechanics and the quantum non-cloning principle, the quantum key communication in the proposed scheme can find any eavesdropper, ensuring the absolute security and user privacy of the signature information and blind transaction information transmitted in the classic channel.

Smart contracts based on quantum blind signature include noisy quantum information transmission and noiseless quantum information transmission. Assuming that channel noise is not considered, the BB84 quantum communication protocol used in this paper consists of two phases. The first stage uses the quantum channel for quantum key distribution and key communication of the traders or signers; the second stage is that the trader and the block creator use the classic channel for key negotiation to detect whether there is an eavesdropper or a quantum attacker, and the final signature key is determined based on the negotiation results. The BB84 protocol uses two different sets of orthogonal bases A0 and A1, which are the rotational polarization states $|45°\rangle$ and $|135°\rangle$ (the left-handed and right-handed states), and the linear polarization states $|90°\rangle$ and $|0°\rangle$ (vertical linear polarization state and horizontal linear polarization state). A0 and A1 form a Hilbert space, and each element represents the polarization state of a single particle (or photon). Through these two stages of quantum information transmission, it is possible to provide secure quantum signature and verification for this smart contract scheme when the noise is low.

If the environmental noisy of quantum blind signature is high enough to be considered, the trader and the block creator need to distinguish whether the detection error is caused by noise or by an eavesdropper or a quantum attacker, and the second phase of communication will be adjusted at this time. The transmission protocol of noisy quantum information still consists of two phases. The first phase is exactly the same as the communication in the quantum channel of noiseless protocol. The second phase is still performed on the common classical channel, but divided into four sub-phases. The first sub-phase is the same as the noise-free BB84 protocol, where the trader and the block creator generate the original keys and initially determine the original key. In the second sub-phase, the trader and the block creator test the original keys and complete the error estimation. In the third sub-phase, the trader and the block creator determine whether the error is caused by noise or caused by the eavesdropper according to the error threshold, and complete the renegotiation of the quantum sequence. In the fourth sub-phase, the trader and the block creator select a part of the detected quantum sequence to encode and generate the final signature key. In a noisy environment, the solution is still able to provide secure quantum signature and verification for this smart contract architecture.

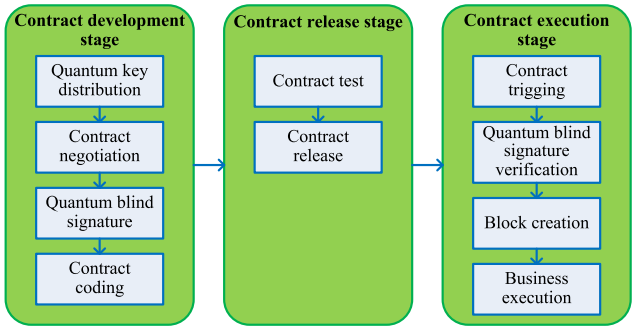

FIGURE 2. The life cycle of smart contracts.

IV. THE LIFE CYCLE OF SMART CONTRACT WITH QUANTUM BLIND SIGNATURE

A. THE LIFE CYCLE

Similar to the classic blockchain smart contracts, as shown in Figure 2, the life cycle of a smart contract based on quantum blind signature includes contract development stage, contract release stage, and contract execution stage. Different levels in the smart contract architecture in figure 1 based on quantum blind signature will cooperate with each other in different life stages. In the whole life cycle of smart contracts, there are not only classic channels and classical information, but also quantum channels and quantum information to be used.

In the contract development stage, it is mainly negotiated by multiple parties of the contract, including the distribution and negotiation of quantum keys, contract rules and terms, the quantum blind signature, and the completion of contract coding. After negotiation, the contract participants can determine the rights and obligations of different parties in a transaction, clarify the standard text of the contract, program the contract text, complete the negotiation of the original quantum key and quantum blind signature, and form a standard contract code. Contract negotiation and key agreement are performed on classic blockchain network, virtual machines and containers, using classic channels and classic information, which will be determined by experts in the relevant fields

and contract participants after repeated iterations. Quantum key distribution and quantum blind signature use quantum information and quantum channels, and are related to the core of contract security, providing an optional set of quantum key codes to ensure the validity, security, and privacy of the contracts.

In the contract release phase, it mainly includes contract test and contract release. The verified and coded contracts need to be tested in the blockchain environment. The tested contracts are sent to each node through the classic blockchain networks, and each node agrees with them according to the received contracts. Each node packs the received contracts into a contract set, completes its hash value calculation and assembles them into a block before broadcasting to other nodes. Then the node receiving the block compares its hash value with the hash value in its own contract set, and compares the quantum keys held by each hand. Then all nodes of the whole network can reach a final consensus on the released contracts after several comparisons. Now, the agreed contract set is broadcasted to each node in a block mode, and block information mainly includes a timestamp, the hash value of the current block, the hash value of the prior block, contract parameters, quantum key parameters, and other information.

In the contract execution stage, there is contract triggering, quantum blind signature verification, block creation, and business execution. This phase uses an event-based trigger mechanism and maintains a complete state machine that can accept and process various transaction services. The smart contract can set a timer to continuously traverse the triggering conditions and state machine of each contract. The contract meeting the triggering conditions will be pushed into a block to create a queue for verification of quantum blind signature. The contract verification is performed on the virtual machines and the container in the classic blockchain networks. The contract to be verified will be broadcasted to each node of the whole network. The block creator firstly performs the verification of quantum blind signature to determine whether the contract is valid and the verification is successful, before it creates a valid block and conducts a network-wide consensus. A successful contract can automatically execute the businesses; otherwise, the block creation will fail and the contract will not be executed. Each stage of the smart contract is automatically completed by the smart contract architecture shown in Figure 1 without manual intervention, and the contract is transparent and cannot be tampered with.

B. SIGNATURE RULE

While implementing quantum blind signature of smart contracts, it is often necessary for trading parties to execute quantum key distribution protocols, and run smart contracts without arbitration or traditional management organization. Each transaction process of each trader is pre-programmed according to the smart contracts, and coding rules can work by themselves. First, the quantum blind signature is used for the transaction message which is blinded by the block creator in the first place. Second, the blinded message finishes its quantum signature operation to be released by the trader. Thirdly, the signature is debunked and the trader's signature of the original text is obtained by the block creator. The quantum blind signature can prevent the signers and others from knowing the private content of the signed messages and let the block creator confirm the signature. Therefore, in addition to the usual digital signature rules, the quantum signature rules have the following characteristics:

(1) The quantum blind signature of a smart contract is decentralized. The quantum blind signature scheme does not rely on a centralized arbitration party or a trusted third party, but only the block creator and traders. Different traders' signatures are distributed and are automatically completed by the network nodes according to the protocol. Once the signature protocol is activated, it can operate on its own, complete multiple signatures and verifications in turn, and automatically execute the smart contract terms when the verification succeeds, without the intervention of other participants or arbitrators.

(2) The quantum blind signature of smart contracts can be self-sufficient. The achievement of all quantum blind signatures can guarantee the completion of the entire transaction business. Once the block creator verifies a signed transaction message, the smart contract will be executed immediately, the user can obtain the available products or services, and the merchant can get the full payment or the available fund.

(3) Blind. The signers in the smart contract can not know the specific content of the original message text while performing the quantum blind signature on a transaction message, that is, the signed message is not visible to the signers, and can protect the privacy of the signed transaction message. After the transaction message is signed and published, all nodes on the entire blockchain will be able to access the public information about the transaction, although the signers or others cannot track the private content and timestamp information by the signed message.

(4) Un-forgeable and non-repudiation. Due to the entanglement features of the quantum states, only the signer himself can generate his own effective quantum blind signature, and no one else or an attacker can forge others' signatures or complete a valid signature of smart contracts. Blindly signed messages are untraceable and unmodifiable, and transaction information and signed messages are also exposed by the entire blockchain. Each signer cannot deny his own signature on any successful transaction, because he cannot know which content it is on his signature.

V. SMART CONTRACT USING SINGLE-PERSON QUANTUM BLIND SIGNATURE ALGORITHM

A. ALGORITHM DESIGN

As can be seen from the above analysis, the arbitrated signature is not suitable for the signature scheme in blockchain smart contracts. Because of the non-centrality of the blockchain, a third-party intervention is not required, otherwise the security risk will be increased and the efficiency of smart contracts will be reduced. How to ensure the security of

TABLE 1. Signature and recovery operation.

Trader's signature	Particle b_i	Recovery operation of block creator
$\left\|\varphi^{+}_{a_iR_i}\right\rangle$	$\alpha\|0\rangle-\beta\|1\rangle$	$\hat{\sigma}_3$
$\left\|\varphi^{-}_{a_iR_i}\right\rangle$	$\alpha\|0\rangle+\beta\|1\rangle$	I
$\left\|\varphi^{\rightarrow}_{a_iR_i}\right\rangle$	$\alpha\|1\rangle-\beta\|0\rangle$	$\hat{\sigma}_3\hat{\sigma}_1$
$\left\|\varphi^{\uparrow}_{a_iR_i}\right\rangle$	$\alpha\|1\rangle+\beta\|0\rangle$	$\hat{\sigma}_3$

blockchain business without relying on the central arbitration is the key to realize the quantum signature of smart contracts. Based on the architecture above, this section introduces a single-person signature scheme using quantum entanglement for remote communication without any arbitration. In the signature process of smart contracts, the central institution or the arbitrator is not involved, and business information of the smart contract can be blindly signed. So it has high security and efficiency while ensuring business privacy.

In smart contracts, the trader and the block creator perform the quantum key distribution via the quantum channel through the BB84 protocol (see Section III C). The trader sends the transaction message to the block creator via the classic channel where the transaction message is signed by negotiated quantum keys and then attached. The proposed methods will prevent the message from being tampered by the attackers, where the block creator verifies the authenticity of the message and determines whether the smart contract will be run by the verification results of signatures or not. The transaction message in this signature scheme is blinded, and the signer does not know the private content of a business message.

After the block creator receives the signature S sent from the business trader, the shared key K is used to decrypt the signature S to produce a signed business request R_i. Due to the measurement of entangled particles in the business trader, the quantum state of the entangled particles of the block creator will collapse into one of the following four states with equal probability: $\alpha\,|0\rangle\,-\,\beta\,|1\rangle$, $\alpha\,|0\rangle\,+\,\beta\,|1\rangle$, $\alpha\,|1\rangle+\beta\,|0\rangle$, $\alpha\,|1\rangle-\beta\,|0\rangle$. Therefore, the block creator needs to perform a corresponding unitary transformation on the signature particle b_i, and restore the initial quantum state of the transaction message on the b_i. The corresponding unitary transformation operations are shown in Table 1.

The block creator verifies the business signature by comparing whether R_i and b_i are equal. According to the transformation shown in Table 1, the quantum states of R_i and b_i are identical. Quantum exchange test circuits can be used for this kind of comparison, rather than directly measuring the quantum state of b_i to prevent its quantum state from collapsing instantaneously. When the results of the comparison indicate $|b_i\rangle = |R_i\rangle$, the signature of the trader will be accepted and the smart contract will be automatically executed. If the results of the comparison do not meet the predefined requirements, the business transaction will be terminated and the block creation will fail.

B. ALGORITHM FLOW

The smart contract with single-person quantum blind signature has three main steps, namely contract development, contract release, and contract execution.

Step 1: Contract will be developed. This step consists of four main sub-steps:

Sub-step 1-1, quantum key distribution.

The trader and the block creator perform quantum key distribution on the quantum channel and share a pair of quantum keys K, and the n pairs of entangled particles are prepared by the block creator.

$$|\phi_k\rangle = \frac{1}{\sqrt{2}}(|0\rangle_{ai}\,|1\rangle_{bi} + |1\rangle_{ai}\,|0\rangle_{bi}) \tag{7}$$

where, a_i and b_i represent the i-th pair of entangled particles, and each particle is prepared to be in the quantum superposition state shown in formula (1).

Sub-step 1-2, contract negotiation. Including negotiation of contract terms and negotiation of quantum key, the trader and the block creator determine whether the contract terms are reasonable and feasible, the quantum communication is not being eavesdropped and the key is safe.

Sub-step 1-3, single-person quantum blind signature.

Above all, the blinding factor r and the transaction summary information s are randomly selected to blindly process the business transaction request R_i'.

$$R_i = rsR_i'(\mathrm{mod}n) \tag{8}$$

Then the service request to be signed has been blindly transformed, and the blinded service data will be sent to the signer. The signer selects the negotiated particles that are safe according to the negotiation result of the quantum key, and each pair of particles for signature is a quantum state R_i.

$$|R_i(a)\rangle = |R_i(b)\rangle = \alpha_i\,|0\rangle + \beta_i\,|1\rangle \tag{9}$$

$$\|\alpha_i\|^2 + \|\beta_i\|^2 = 1; \quad i = 1, 2, 3, ..., n \tag{10}$$

where, α_i and β_i represent the gradient values of the i-th pair of entangled particles and are owned by the business trader.

Next, the business trader sends a part of the quantum state $R_i(b)$ in the quantum sequence of the blinded transaction request to the block creator, and retains a part of the quantum state $R_i(a)$ of the quantum sequence in its own hand. After receiving the request of the business trader $R_i(b)$, the block creator sends a series of the entangled particle pair to the trader and leaves the particle b of the entangled pair in its own hand to confirm the validity of the signed transaction request.

Thus, the particles a_i, b_i and R_i form a mixed quantum state:

$$\begin{aligned}&\left|\phi_{a_ib_iR_i}\right\rangle\\ &= \frac{1}{2}\Big[\left|\phi^{+}_{a_iR_i}\right\rangle(\alpha_i|0\rangle - \beta_i|1\rangle)_{b_i} + \left|\phi^{-}_{a_iR_i}\right\rangle(\alpha_i|0\rangle + \beta_i|1\rangle)_{b_i}\\ &\quad + \left|\phi^{\rightarrow}_{a_iR_i}\right\rangle(\alpha_i|1\rangle - \beta_i|0\rangle)_{b_i} + \left|\phi^{\uparrow}_{a_iR_i}\right\rangle(\alpha_i|1\rangle + \beta_i|0\rangle)_{b_i}\Big]\end{aligned} \tag{11}$$

where,

$$\left|\phi^{\pm}_{a_iR_i}\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{a_iR_i}$$
$$\left|\phi^{\rightarrow\uparrow}_{a_iR_i}\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{a_iR_i}$$

Again, after receiving the quantum states of the particles sent by the block creator, the business trader jointly measures the particles a_i and R_i, and the Bell measurement results are one of the four quantum states $\left|\phi^{+}\right\rangle$, $\left|\phi^{-}\right\rangle$, $|\phi^{\rightarrow}\rangle$, $\left|\phi^{\uparrow}\right\rangle$, where the measurement results are recorded and encoded into two-bit classic messages. $\left|\phi^{+}\right\rangle \rightarrow 00$, $\left|\phi^{-}\right\rangle \rightarrow 01$, $|\phi^{\rightarrow}\rangle \rightarrow 10$, $\left|\phi^{\uparrow}\right\rangle \rightarrow 11$. So far, the business trader's measurement results contain 2 bits of classic information.

At this time, the business trader uses the Bell measurement of the quantum states of all the particle groups to produce an effective quantum key for signature, and obtains the encrypted measurement results as the signature S. Additionally, signature encryption process can also use controlled unitary transformations, such as controlled non-gate *Cnot*.

$$S = E_K(R_i) \tag{12}$$

Sub-step 1-4, contract coding. The business trader can encode the signed contract in a prescribed format for transmission and send it to other blocks through the classic channel for consensus testing.

Step 2: The contract will be released. This step consists of two main sub-steps.

Sub-step 2-1, contract test. The coded contract needs to be tested using a consensus mechanism, by which all blocks will reach a consensus on the newly released contract only if all tests are successful.

Sub-step 2-2, the contract is released. The contracts that have been agreed upon by all blocks after testing will be spread to different nodes on the whole network in a block manner.

Step 3: Contract will be executed. This step consists of four main sub-steps:

Sub-step 3-1, contract trigging. If the preset triggering condition of a smart contract is met, the contract will be triggered and be further determined whether it will be executed.

Sub-step 3-2, verification of single-person quantum blind signature. The block creator uses the shared quantum key to decrypt and verify the signature. If the signature verification is successful, the subsequent steps of the smart contract will be automatically executed, and the blind removal transformation will be performed to obtain transaction message R'_i, namely:

$$R'_i = r^{-1}R_i(\text{mod } n) \tag{13}$$

Sub-step 3-3, block creation. The block will be successfully created at this sub-step, and the message of successful transaction will be broadcasted on the entire blockchain through the classic networks before distributed common accounting was completed by all blocks. Or else, the transaction is automatically rejected and stopped by the smart contract.

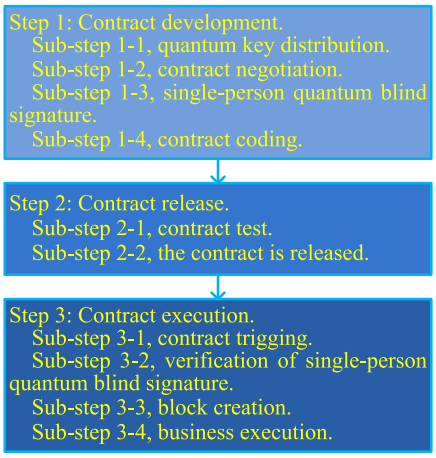

FIGURE 3. Single-person quantum blind signature algorithm for smart contracts.

Sub-step 3-4, business execution. Complete business transactions will be finished following the contract terms to fit the business request of the trader.

The flow chart of this agreement is shown in Figure 3.

C. SECURITY ANALYSIS

In the proposed smart contract scheme, the quantum signature is different from the classical encryption algorithm. Using the BB84 protocol, which has been proved to be unconditionally secure, it can guarantee the correctness and performance of smart contracts. Assuming that in the business execution, there may be three main kinds of security threats, and the security will still be guaranteed.

(1) The trader cannot deny his signature.

In the usual payment system and the arbitrated signature system, since an arbitrator or trusted center is used to confirm the transaction signer and the transaction recipient, it can effectively prevent the transaction signer from refusing his signature, and can prevent the transaction verifier from rejecting the transaction signature. However, our blockchain smart contracts are light-weighted, and there is no arbitrator or trusted center. The trade applicant and the block creator need to automatically complete the determination of the transaction signature under the framework of smart contracts.

Since the scheme is a blinded quantum signature in our scheme, the transaction applicant cannot know which transaction message is signed, and he cannot deny which transaction he signed. Once the business trader finishes his signature, the block creator can confirm the signer according to the received timestamp and transaction signature, where the quantum key shared by the trader and the block creator is included in the transaction signature. The block creator can then instruct the trader to sign the message. After the block creator broadcasts the signed transaction messages to all blocks on the entire blockchain and performs distributed accounting, the transaction applicant will not be able to deny his quantum signature on the business transaction.

Similarly, the block creator cannot deny the completed transaction and the received signature. In the transaction

verification, the trader and the block creator both measure quantum states shared by their hands, perform the corresponding positive transformation operation on the quantum signature and restore the original information of the business transaction. When the message recovery is completed, the block creator cannot claim that the signed message has not been received or the business information has not been recovered. When the quantum state measurement is used to verify the trader signature, it has been proved that the block creator has received the trader's signature. After the block creator broadcasts the transaction and the signed message to all blocks on the entire blockchain and performs distributed accounting, the block creator cannot lie to have not received the quantum signature of the trader.

(2) The attackers cannot impersonate the trader to sign the message.

Assuming that the attacker wants to impersonate the trader to sign the smart contract, it must know the quantum key shared by the trader and the block creator in the initial stage of the smart contract, and use the quantum key to complete the encryption and signature of the smart contract. Since quantum key distribution uses several coded qubits in an entangled state, which has non-cloning characteristic and unconditional security, an attacker cannot obtain the key to impersonate the trader by employing entanglement, cloning, copying, and measurement. Therefore, it is impossible for the attackers to impersonate the trader to sign the smart contract.

(3) The attacker cannot falsify the signature information of the smart contract.

To falsify the signature information includes the trader's signature and the trading message of the smart contract. It is known in the previous sections that the trader's signature cannot be falsified because the attacker cannot obtain the shared quantum key of trader by any method.

If the attacker needs to falsify the business transaction message R_i sent by the trader, all quantum states need to be intercepted, and a new business transaction message R_i' and signature should be prepared to replace the true transaction message and signature belonging to the trader. The attacker sends the falsified business transaction message to the block creator, and the tamper-generated quantum state will result in a collapse after the block creator makes a specified base measurement. However, the real quantum key is always in the hands of the trading parties. Only the real trading parties can measure the signature to produce the real quantum signatures. The measurement results are not exactly the same as the attacker's measurement results, because the quantum state measurements of trader and attacker are random and independent. So the block creator will erroneously transform the received forged message, failing to correctly restore the quantum state of the trader's signature on the business message. At this point, an excessive error rate between the trader and the block creator will result in the forged business transaction messages being detected.

Further, the blind signature of the message content can prevent an attacker from accessing the private content of the business message.

VI. EXTEND SINGLE-PERSON QUANTUM BLIND SIGNATURE TO MULTI-PERSON SCHEME

A. ALGORITHM EXTENSION

The previous section provides us a light-weighted quantum blind signature to be effectively used in a single signer case. But in multi-person smart contracts, the single-person algorithm can also be applied by necessary extension.

One simple scheme is to take a multi-person smart contract as a series of single-person smart contracts, where every singer implements a single-person quantum blind signature in turn. Take two traders for example, the two signatures S_A and S_B of the smart contracts use the quantum key K_{AC} shared by trader A and the block creator C, and the quantum key K_{BC} shared by trader B and the block creator C, respectively, abiding by the quantum mechanism. The whole process is similar to the scheme in section V. When all single-person quantum blind signatures are finished and a series of signatures are verified by the block creator, the smart contract can be effectively implemented before it is broadcasted on the whole blockchain. There are often not many signers in multi-person smart contracts, so the single-person quantum blind signature can be easily implemented by multi traders in turn with unconditionally security and lightweight. In this case, an error in the previous single-person quantum blind signature will stop the transaction at any time, and the after signatures will not be implemented any longer.

Another improved scheme considers that all traders make their own signatures in turn, and then the block creator checks all the signatures in the end before the smart contract implementation. Take two traders for example, the trader A and the trader B sign the same transaction service in turn, and the block creator C verifies the signatures of the traders A and B at a time. Because the particles A, B, C are in the hands of the traders A, B and the block creator C, respectively, after the first trader A signs S_A, the blinded transaction message will be sent to the trader B and the block creator C in turn. Then the trader B performs a specified unitary transformation on the particle B to make his signature S_B. In the end, the block creator C also performs a recovery operation on the signatures S_A and S_B to obtain the initial state of the transaction request R_i. After the verification is successful, the smart contract will be executed and the transaction process will be completed. In this case, an error in the previous single-person quantum blind signature will not be easily be found to stop the transaction, and the after signatures will also be implemented with the previous error until the block creator finds it in the end.

Both extended schemes have unconditional security of quantum states, and they do not depend on the complexity of the algorithm and the size of the blockchain. The situation with more traders can also be deduced by analogy in both cases. In most smart contracts with not too many traders, they

both can improve the security of the entire life cycle of smart contracts with balancing portability.

B. SECURITY ANALYSIS

Multi-person quantum blind signature of smart contracts is extended from single-person quantum blind signature, where all signers are unable to deny their signatures, and any signer or attacker cannot falsify a legal signature of other trader. In the multi- person quantum signature of smart contracts, the quantum signature scheme of the proposed protocol can also be proved to be unconditionally secure.

(1) Multiple signers can't deny their signature.

In a multi- person quantum signature scheme, the embed single-person quantum blind signature has been verified in the previous section to be able to ensure that all signers cannot deny their signatures, and the signature recipients or attackers cannot forge legal signatures. In the extended multi- person smart contracts, the validity of multiple signatures and the legitimacy of smart contracts can be mutually checked by multiple nodes.

Take two traders for example, because of the cloning feature, it is impossible for the trader A and the trader B to deny their signatures on a smart contract, and the block creator C can verify the validity of the signatures through the sharing quantum keys by the trader A and the trader B. Successfully verified signatures will automatically trigger the smart contract and the finished transaction will be released to all blocks on the whole blockchain. Then the transaction cannot be denied by anyone on the entire network.

Because the multi-person quantum signature is extended from the previous single-person method in section V, the trader A or B cannot deny the transaction message after they send the message in turn to the block creator C. Similarly, the block creator C can also verify the signatures S_A and S_B by the shared quantum key, and can not deny the signatures of the trader A and the trader B. Therefore, the trader A, B, and the block creator C cannot deny the received signatures.

(2) The attacker and other traders cannot impersonate legal traders to sign the message.

In the proposed smart contract, a business party or an attacker attempts to falsify the signature of another party, this is not possible.

For example, it is assumed that the trader A tries to forge the signature of the trader B. But the trader A does not get the key K_{BC} shared between the trader B and the block creator C, hence it is impossible for the trader A to forge the encrypted transaction request $R_i(a)$ and α. Any forged signature of trader B by trader A will not follow the entanglement feature of the quantum key shared by the trader B and the block creator C, so, the trader A cannot forge the signature S_B of the trader B to cheat the block creator C. Because of the absolute security of the quantum key, through operations such as cloning, entanglement, copying, and measurement, it is impossible for the trader A to get the K_{BC} to falsify a new signature encrypted by legal keys. That is, this falsified signature will be detected by the block creator C and the smart contracts cannot be successfully performed.

Similarly, it is impossible for an attacker to achieve legal keys by cloning, entanglement, copying, measuring, etc., and to forge a transaction message with a legitimate signature of the traders. In this smart contract with multi-person signature, the blind business request R_i and the signature S_A of the trader A will be encrypted by K_{AC}, and then the blind transaction requests R_i and the signature S_B of the trader B will be further encrypted by K_{BC}, so the attackers will not forge any signature or transaction through QKD because of the unconditional security of quantum keys K_{AC} and K_{BC}.

VII. ALGORITHM COMPARISON AND APPLICATION SUGGESTION

A. ALGORITHM COMPARISON AND ANALYSIS

This section compares different signature algorithms. The comparison indicators include the number of signatures, security, privacy, and dispute arbitration. Security includes classic security and anti-quantum attack security. Classical security depends on the complexity of the algorithm and is relatively secure, but the quantum security is independent of algorithm complexity and is absolutely secure. Privacy protection includes identity information, transaction information, timestamp, private message and more. Dispute arbitration includes transaction authenticity after the dispute arises, the rejection of the signature and the forgery. The compared algorithms include security attribute signatures [12], ID-based signatures [13], multiple signatures [14], lattice attribute signatures [16], optical signatures [18], quantum multiple signatures [19], and quantum blind signatures [21], [22], the model in Section V and the model in Section VI of this paper. The comparison analysis results of different signature algorithms are shown in Table 2.

Based on the above comparison results, we can see that:

(1) The model in Section V and the model in Section VI proposed in this paper can be used for single-person signatures and multi-person signatures, respectively, to meet the need for blockchain services and smart contracts that require different signatures. The lightweight of the proposed algorithm also increases the security of smart contracts throughout its lifecycle and is easy to be extended.

(2) The model of Section V and the model of Section VI proposed in this paper use the quantum signature scheme to resist both classical attacks and quantum attacks. The quantum attack problem in the literature [17] can be effectively solved with unconditional security and without increasing the algorithm complexity.

(3) The model in Section V and the model in Section VI proposed in this paper, as well as the quantum blind signature [21], [22] all use the blind processing of the signed message, can protect the private information in the blockchain business execution. For user privacy information, neither can the trader know the specific message content by his signature, nor can he deny his signed message.

TABLE 2. Comparative analysis of signature algorithms.

Model	Number of signatures	Security	Privacy	Dispute arbitration	Algorithm complexity
Security attribute signature [12]	Single	Relatively safe	No privacy protection	Decentralization	Security depends on algorithm complexity
ID-based signature [13]	Single	Relatively safe	No privacy protection	Decentralization	Security depends on algorithm complexity
Multi-signature [14]	More than two	Relatively safe	No privacy protection	Decentralization	Security depends on algorithm complexity
Lattice attribute signatures[16]	Single	Relatively safe	No privacy protection	Need arbitration	Security depends on algorithm complexity
Optical signature [18]	Single	Absolutely safe	No privacy protection	Need arbitration	Security depends on algorithm complexity
Quantum multi-signature [19]	More than two	Absolutely safe	No privacy protection	Need arbitration	Security is independent of algorithm complexity
Quantum blind signature [21],[22]	More than two	Absolutely safe	Blind message	Need arbitration	Security is independent of algorithm complexity
Proposed model in Section V	Single	Absolutely safe	Blind message	Decentralization	Light-weighted, security is independent of algorithm complexity
Proposed model in Section VI	More than two	Absolutely safe	Blind message	Decentralization	Light-weighted, security is independent of algorithm complexity

(4) In the smart contract disputes, the model of Section V and the model of Section VI proposed in this paper, as well as the signature of security attributes [12], ID-based signatures [13], and multiple signatures [14], do not require additional arbitration institution or certification center. But our article does not need to improve the complexity of the algorithm to improve security. The proposed methods are so light-weighted that it is suitable to be applied into the decentralization architecture of blockchain smart contracts.

B. ENGINEERING APPLICATION SUGGESTIONS

This paper introduces two blind signature schemes based on quantum entanglement features, which are characterized by the fact that they do not need a trusted arbitration party and are suitable for light-weighted blockchain smart contracts. In engineering applications, the two solutions described in this paper can use shared quantum keys to significantly improve the security of smart contracts and achieve theoretical absolute security.

(1) The scheme in Section V enables transaction information to be signed by a trader and verified by the block creator. The single-person quantum blind signature uses blinded transaction messages, and the trader cannot know what the specific transaction message is signed by mean of his signature. This scheme is very suitable for most applications in smart contracts that only need one trader for signature. Because the algorithm's function is simple, safe and reliable, the signature method and verification method are relatively easy to be implemented. In practice, the execution speed of proposed smart contracts will be very fast and suitable for mass transactions of high performance with a single signature, at the same time, it can also be easily extended in situations where multiple signers are required for the same transaction.

(2) The solution in Section VI enables transaction information to be signed by more traders and verified by a block creator. In reality, most smart contracts are required to use blinded transaction messages, where multiple traders cannot know which specific transaction messages are signed and cannot deny their signatures. Multiple traders and block creator check on the coherence of shared quantum states by the physical properties of quantum entanglement during signature and verification. The shared quantum keys used by multiparty signatures will produce an absolutely secure quantum key distribution protocol. The multi-person signature scheme is more complex than the single-person signature scheme, and the implementation difficulty is also increased. The signature process and the verification process of the multi-person signature scheme take more time, but it is more suitable for smart contract applications that require more than two parties to sign the same transaction.

(3) The single-person signature scheme and multi-person signature scheme described in this paper are blinded cryptographic schemes based on quantum entanglement features. In actual engineering applications, one trader or multiple traders can be selected to sign the transaction message as needed, before the block creator verifies all signatures and automatically executes the smart contract. In engineering applications, both of the smart contracts in this paper have unconditional security and are fully achievable under the current technology.

(4) In the blockchain application, the data transmission of different blocks has a certain time sequence, and the quantum ordered multi-signature protocol can also be used to complete the transmission, signature and verification of transaction messages utilizing quantum entanglement tunnels. A distributed ledger of multiple blocks is used for accounting to ensure the security of every transaction. In engineering applications, the quantum blind signature protocol can also hide the block number, hash value and the timestamp of the transaction, and realize distributed accounting and message hiding of private information. Additionally, the number of blocks is not limited to proposed schemes, and the transaction information can also be sequentially signed by users with different authorizations.

VIII. CONCLUSION

This paper tries to improve the security of blockchain smart contracts under quantum attack environment, and proposes a smart contract technology based on quantum blind signature. Different from the classical signature scheme with security dependent on algorithm complexity, the proposed smart contract architecture with quantum blind signature is unconditionally secure and independent of the algorithm complexity, and does not need any trusted arbitrator. Therefore, it is more suitable for decentralized distributed business applications such as blockchain smart contracts. The two schemes proposed in this paper, one for single-person quantum signature and verification, and the other for multiple-person quantum signature and verification, use quantum entanglement to achieve quantum signature on transactional messages. Although the latter only lists a transaction example with two traders to participate in the signature, it also can be applied to smart contracts with more than two signers, simply by preparing more particles with multi-quantum states to complete multi-party signatures.

Although the research results of this paper can be helpful to improve the security of blockchain smart contracts against quantum attacks, some minor factors are omitted in the analysis. Future research will further verify quantum signatures on multiple blocks, survey the impact of measurement error of quantum signatures on smart contracts, apply asymmetric quantum keys in smart contracts, and study the quantum denial of service attacks or quantum man-in-the-middle attacks on blockchain smart contracts.

ACKNOWLEDGMENT

Author thanks the hard work of all anonymous reviewers to improve the quality of this submission.

REFERENCES

[1] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
[2] P. Bailis, A. Narayanan, A. Miller, and S. Han, "Research for practice: Cryptocurrencies, blockchains, and smart contracts; hardware for deep learning," *Commun. ACM*, vol. 60, no. 5, pp. 48–51, 2017.
[3] P. Tsankov, A. Dan, D. Drachsler-Cohen, A. Gervais, F. Buenzli, and M. Vechev, "Securify: Practical security analysis of smart contracts," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, vol. 10, 2018, pp. 67–82.
[4] S. Rouhani and R. Deters, "Security, performance, and applications of smart contracts: A systematic survey," *IEEE Access.*, vol. 7, pp. 50759–50779, 2019.
[5] S.-C. Oh and A. J. Hildreth, "Decisions on energy demand response option contracts in smart grids based on activity-based costing and stochastic programming," *Energies*, vol. 6, no. 1, pp. 425–443, 2013.
[6] K. O'Hara, "Smart contracts—Dumb idea," *IEEE Internet Comput.*, vol. 21, no. 2, pp. 97–101, Mar./Apr. 2017.
[7] D. Magazzeni, P. McBurney, and W. Nash, "Validation and verification of smart contracts: A research agenda," *Computer*, vol. 50, no. 9, pp. 50–57, 2017.
[8] J. P. Cruz, Y. Kaji, and N. Yanai, "RBAC-SC: Role-based access control using smart contract," *IEEE Access*, vol. 6, pp. 12240–12251, 2018.
[9] K.-H. Yeh, C. Su, J.-L. Hou, W. Chiu, and C.-M. Chen, "A robust mobile payment scheme with smart contract-based transaction repository," *IEEE Access*, vol. 6, pp. 59394–59404, 2018.
[10] L. Chen, L. Xu, Z. Gao, Y. Lu, and W. Shi, "Tyranny of the majority: On the (Im)possibility of correctness of smart contracts," *IEEE Security Privacy*, vol. 16, no. 4, pp. 30–37, Jul./Aug. 2018.
[11] Z. C. Kennedy, D. E. Stephenson, J. F. Christ, T. R. Pope, B. W. Arey, C. A. Barrett, and M. G. Warner, "Enhanced anti-counterfeiting measures for additive manufacturing: Coupling lanthanide nanomaterial chemical signatures with blockchain technology," *J. Mater. Chem. C*, vol. 5, no. 37, pp. 9570–9578, 2017.
[12] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," *IEEE Access*, vol. 6, pp. 11676–11686, 2018.
[13] Q. Lin, H. Yan, Z. Huang, W. Chen, J. Shen, and Y. Tang, "An ID-based linearly homomorphic signature scheme and its application in blockchain," *IEEE Access*, vol. 6, pp. 20632–20640, 2018.
[14] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 5, pp. 840–852, Sep./Oct. 2018.
[15] M. R. Asaar, M. H. Ameri, M. Salmasizadeh, and M. R. Aref, "A provably secure code-based concurrent signature scheme," *IET Inf. Secur.*, vol. 12, no. 1, pp. 34–41, 2018.
[16] J. Chen, Y. Hu, W. Gao, and H. Li, "Lattice-based threshold ring signature with message block sharing," *KSII Trans. Internet Inf. Syst.*, vol. 13, no. 2, pp. 1003–1019, 2019.
[17] A. K. Fedorov, E. O. Kiktenko, and A. I. Lvovsky, "Quantum computers put blockchain security at risk," *Nature*, vol. 563, no. 7732, pp. 465–467, 2018.
[18] E. A. Stinaff, M. Scheibner, A. S. Bracker, I. V. Ponomarev, V. L. Korenev, M. E. Ware, M. F. Doty, T. L. Reinecke, and D. Gammon, "Optical signatures of coupled quantum dots," *Science*, vol. 311, no. 5761, pp. 636–639, 2006.
[19] X.-J. Wen, Y. Liu, and Y. Sun, "Quantum multi-signature protocol based on teleportation," *Zeitschrift für Naturforschung A*, vol. 62, nos. 3–4, pp. 147–151, 2007.
[20] J. Shi, R. Shi, Y. Guo, X. Peng, M. H. Lee, and D. Park, "A (t,n)-threshold scheme of multi-party quantum group signature with irregular quantum Fourier transform," *Int. J. Theor. Phys.*, vol. 51, no. 4, pp. 1038–1049, 2012.
[21] X.-F. Niu, J.-Z. Zhang, S.-C. Xie, and B.-Q. Chen, "A practical E-payment protocol based on quantum multi-proxy blind signature," *Commun. Theor. Phys.*, vol. 70, no. 5, pp. 529–533, 2018.
[22] L. Yan, Y. Chang, S. Zhang, G. Han, and Z. Sheng, "A quantum multi-proxy weak blind signature scheme based on entanglement swapping," *Int. J. Theor. Phys.*, vol. 56, no. 2, pp. 634–642, 2017.
[23] W.-M. Shi, J.-B. Zhang, Y.-H. Zhou, and Y.-G. Yang, "A new quantum blind signature with unlinkability," *Quantum Inf. Process.*, vol. 14, no. 8, pp. 3019–3030, 2015.
[24] X.-F. Niu, J.-Z. Zhang, S.-C. Xie, and B.-Q. Chen, "A third-party E-payment protocol based on quantum multi-proxy blind signature," *Int. J. Theor. Phys.*, vol. 57, no. 8, pp. 2563–2573, 2018.

ZHENGYING CAI received the bachelor's, master's, and the Ph.D. degrees from the Huazhong University of Science and Technology, China. He is currently a Professor with the College of Computer and Information Technology, China Three Gorges University. He has published more than 80 academic articles in conferences and journals, and he holds more than 40 patents. His research interests include artificial intelligence, cloud manufacturing, and quantum computing.

JING QU received the bachelor's degree from China Three Gorges University, where she is currently pursuing the master's degree with the College of Computer and Information Technology. Her research interests include artificial intelligence and quantum communication.

PINGPING LIU received the bachelor's degree from China Three Gorges University, where she is currently pursuing the master's degree with the College of Computer and Information Technology.

JIAO YU received the bachelor's degree from China Three Gorges University, where she is currently pursuing the master's degree with the College of Computer and Information Technology.