(12) INNOVATION PATENT (11) Application No. **AU 2021105670 A4**
(19) AUSTRALIAN PATENT OFFICE

(54) Title
A Blockchain-Based Method For Domain Name Auction By Means Of Sealed-Bid

(51) International Patent Classification(s)
G06Q 30/08 (2012.01) ***H04L 9/32*** (2006.01)

(21) Application No: **2021105670** (22) Date of Filing: **2021.08.17**

(45) Publication Date: **2021.10.14**
(45) Publication Journal Date: **2021.10.14**
(45) Granted Journal Date: **2021.10.14**

(71) Applicant(s)
Zhejiang Gongshang University

(72) Inventor(s)
WEI, Guiyi;ZHANG, Yi;LU, Genhua;LU, Zhongxiang;SHAO, Jun

(74) Agent / Attorney
WRAYS PTY LTD, L7 863 Hay St, Perth, WA, 6000, AU

2021105670 17 Aug 2021

Abstract

The present invention relates to the technical field of blockchain, particularly to a blockchain-based method for domain name auction by means of sealed-bid, i.e.,: the owner of domain name creates a domain name auction contract on the blockchain, and then checks the validity of the domain name auction contract by means of a consensus mechanism as well as records the information of bidder; if the bidder is aware that there is a domain name auction contract exists on the blockchain, the bidder shall verify the commitment by means of calling operation. Thus, if the verification is successful, participate in the bidding; and then, each bidder who has passed the check of the consensus mechanism would reveal the bidding when the bidding duration expires. Furthermore, anyone can check the bidding records after revealing the bidding, and the bidders shall complete the bidding according to their own state respectively. After that, the auction would be closed. The present invention can guarantee the fairness of transaction, the fairness of bidding, the funds security and the funds privacy of the domain name auction and transfer process.

2021105670 17 Aug 2021

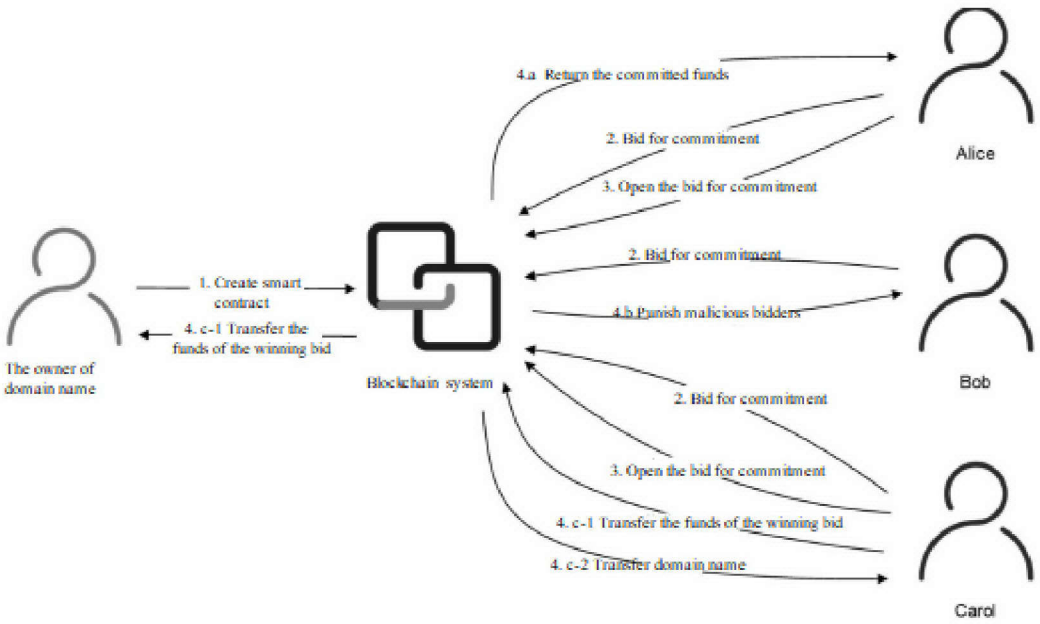

Figure 1

A blockchain-based method for domain name auction by means of sealed-bid

Technical Field

[0001] The present invention relates to the technical field of the blockchain, particularly to a blockchain-based method for domain name auction by means of sealed-bid.

Background Technology

[0002] The Domain Name System (DNS) is one of the important infrastructures of the Internet. Thanks to the appearance of the DNS, people can use domain names which are easy to understand and remember instead of using IP addresses, which are hard to remember, to visit websites. The basic function of DNS is to manage root domains and top-level domains. Currently, root domains and top-level domains are basically maintained by the Internet Corporation for Assigned Names and Numbers (ICANN). Thus, such centralized architecture is vulnerable to attacks including single points of failure and abuse of power. The famous single point of failure event of DNS is the Dyn Network Attacks Incident occurred in 2016. Due to the DNS provided by Dyn being invalid, many websites including Amazon.com, GitHub, Twitter, and Reddit have been converted to being inaccessible when accessing corresponding domain names. The solution can be adopted to address the aforesaid problems is absolutely to introduce a decentralized architecture into the DNS. Furthermore, after more than ten years of development, the blockchain technology has become the most famous and successful decentralized architecture. Thus, quite a lot of scholars suggest introducing the blockchain into DNS. Furthermore, for the DNS, the main approach to obtain domain names is domain name auction. However, the existing blockchain-based DNS systems cannot provide corresponding functions, and thus they all fail to achieve the expected results:

[0003] • Namecoin, ConsortiumDNS, EmerDNS and Blockstack mainly focus on domain name registration rather than the process of domain name auctions;

[0004] • Ethereum Name Service (ENS) implemented the auction function of cryptocurrency addresses, which cannot provide the function of domain name auction;

[0005] • Handshake implemented the domain name auction by means of sealed-bid, which would not disclose the bids made by anyone until the commitment of all bids has been made. Thus, the domain name auction by means of sealed-bid has the advantage of causing bidders to be more willing to bid according to the true value of the assets. However, as the latest highest bid is predictable, the last bidder in Handshake always has the

2021105670 17 Aug 2021

opportunity to win the auction through a reasonable bid.

[0006] Thus, the existing blockchain-based DNS schemes either lack the domain name auction process or cannot guarantee fairness during the process of domain name auction.

Summary of the Invention

[0007] For the purpose of addressing the aforesaid technical problems existed in the prior art, the present invention provides a blockchain-based method for domain name auction by means of sealed-bid, which adopts specific technical schemes as follows:

[0008] The blockchain-based method for domain name auction by means of sealed-bid comprises the following stages:

[0009] During the first stage, the owner of domain name creates a domain name auction contract on the blockchain, and then checks the validity of the domain name auction contract by means of a consensus mechanism as well as records the information of bidder;

[0010] During the second stage, if the bidder is aware that there is a domain name auction contract exists on the blockchain, the bidder shall verify the commitment by means of calling operation. Thus, if the verification is successful, participate in the bidding;

[0011] During the third stage, each bidder who has passed the check would reveal the bidding by means of the consensus mechanism when the bidding duration expires;

[0012] During the fourth stage, anyone can check the bidding records after revealing the bidding, and the bidders shall complete the bidding according to their own state respectively. After that, the auction is closed.

[0013] Further, the said owner of domain name calls the function (Create (T1, T2, name, δ)) to create a domain name auction contract, wherein, the T1 of the said function (Create(T1, T2, name, δ)) represents the deadline for bidding, and T2 represents the deadline for bid opening, and name refers to the domain name which would be auctioned by the owner of domain name, as well as δ refers to the signature of the account owner who owns the domain name signed on the smart contract by utilizing the public key;

[0014] The said process of checking the validity of the domain name auction contract by means of a consensus mechanism specifically refers to: if the consensus nodes in the blockchain receive the calling of the Create function, the consensus nodes would check the validity of (T1, T2, name, δ), and determine whether there is an auction contract corresponding to the name in the blockchain. If passed, the consensus nodes would continue to run the Create function, otherwise, the consensus nodes would stop running the function;

[0015] Then, recording the information related to the bidder by utilizing the bidder [ ] array, wherein, the

information comprises the public key corresponding to an account of the bidder, the commitment made by the bidder to the tendered amount and the data used to reveal the bid by the bidder.

[0016] Further, the bidder participates in the bidding by calling a commitment function ($Commit(pk, \{c'_i\}_{i=0}^{\ell}, \sigma, ZKP_1, ZKP_2)$), wherein, pk represents a public key of an account of the bidder, and $\left\{c'_i = g^{c'_i \cdot 2^i}\right\}_{i=0}^{\ell}$ represents the commitment to the bid $\sum_{i=0}^{\ell} c'_i \cdot 2^i$; and the σ represents the signature signed on the smart contract by utilizing the pk; in addition, ZKP represents the zero-knowledge proof of $c > \sum_{i=0}^{\ell} c'_i \cdot 2^i > 0$, wherein, c represents the balance of the account corresponding to the pk;

[0017] If the consensus nodes in the blockchain receive the calling of the Commit function, the consensus nodes would check whether the array bidder [ ] does not contain the pk, and determine whether the time T of calling the function is within the validity period, as well as check the validity of (σ, ZKP). If passed, the consensus node continues to run the Commit function; otherwise, the consensus nodes would stop running the function.

[0018] Further, the said third stage specifically refers to: after the bidding duration expires, the bidding stage stops, and each bidder can reveal the bid by means of calling the bidding reveal function $Reveal(pk, \{(\bar{m}'_i, \bar{r}'_i)\}_{i=0}^{\ell})$, wherein, pk is the same public key that used by the bidder when calling the Commit function, and $\{(\bar{m}'_i, \bar{r}'_i)\}_{i=0}^{\ell}$ is used to open the commitment $\{c'_i\}_{i=0}^{\ell}$;if the consensus nodes receive the calling of the Reveal function, the consensus nodes would check whether the time T to call the function is within the validity period, and determine whether there is a commitment $\{c'_i\}_{i=0}^{\ell}$ corresponding to the pk exists in the array bidder[ ], as well as check whether $\{(\bar{m}'_i, \bar{r}'_i)\}_{i=0}^{\ell}$ can open the commitment. If passed, the consensus nodes would run the Reveal function; otherwise, the consensus nodes would stop running the Reveal function.

[0019] Further, the said fourth stage specifically refers to: after the bid has been revealed, anyone can judge who is the successful bidder according to the records in the array bidder [ ], wherein, the said successful bidder would call the Finalize function. Then, if the consensus node receive the calling of the function, the consensus nodes would check whether the bidding duration for the auction is due according to the deadline for revealing the bid, and then check whether the current smart contract is in a running state. If passed, the consensus nodes would continue to run the Finalize function, wherein, the second-highest tendered amount would be transferred to the owner of the domain name, and the domain name would be transferred from the owner to the successful

2021105670 17 Aug 2021

bidder; otherwise, the process would be stopped; in addition, if the said bidder fails to reveal the bid, such bidder will be punished by deducting part of the funds; furthermore, if the bidder fails to win the bid, no operation would be done by system.

[0020] All the operations related to funds are all conducted on the blockchain of the present invention based upon accounts, and all the funds are operated in an anonymous form in the system; and thus, the function of domain name auction can be implemented. Furthermore, it guarantees that the owner of domain name can obtain the corresponding money once the transfer of domain name to the successful bidder is completed, and vice versa. In addition, there is no correlation between the probability of winning an auction and the bidding duration, that is, the later bidder would not have any advantages over the former one; furthermore, no one can infer how much money the bidder has in the blockchain system from the auction process, although anyone can verify whether the bidder has enough funds to bid during the auction process.

Brief Description of the Drawings

[0021] Figure 1 is a schematic diagram of a system model of an embodiment of the present invention.

Detailed Description of the Presently Preferred Embodiments

[0022] For the purpose of making the objectives, technical schemes, and technical effects of the present invention clear, the text below will describe the present invention in detail in conjunction with the accompanying drawings of the specification.

[0023] The present invention established an account-based blockchain system, which supports smart contracts, and all the funds are operated in an anonymous form in this system. In addition, the consensus mechanism adopted, which can be implemented through a consortium blockchain, is no longer limited to PoW. Thus, a blockchain-based method for domain name auction by means of sealed-bid which can guarantee the fairness of transaction, the fairness of bidding, the funds security and the funds privacy, is proposed based upon combining the account-based consortium blockchain with anonymous funds, smart contracts, zero-knowledge proof and ring signatures.

[0024] The said blockchain system comprises: an account structure module, a transaction structure module, a transaction propagation module, and a transaction packaging module.

[0025] The said account structure module has:

[0026] Account ID: The public key of the user or a hash function of the public key;

[0027] Funds fund: The amount of funds owned by this address, which is recorded in an anonymous form;

[0028] Domain name list (name): Used to store the domain names owned by the account.

[0029] The said transaction structure module comprises the following data messages:

[0030] Transaction source: The account ID of the transaction initiator;

[0031] Transaction amount: The value expressed in the form of an anonymous or plaintext method;

[0032] Transaction destination: The account ID of the transaction recipient;

[0033] Signature: The initiator needs to sign the entire message with its own private key;

[0034] Zero-knowledge proof: The zero-knowledge proof of the transaction initiator proved that the account amount was greater than the transaction amount.

[0035] The said zero-knowledge proof specifically refers to: the present invention adopts a zero-knowledge proof related to the inequation between two positive integers, i.e., assume $c_1 = g^{x_1}h^{r_1}$, $\{c'_{2i} = g^{a_i \cdot 2^i}h^{r'_{2i}}\}_{i=0}^{\ell}$, wherein, the definition of g and h are the same as that used in the Pedersen commitment, and l represents a large integer, which is greater than all possible funds in the system. In addition, known x1, r1 and $\{a_i, r'_{2i}\}_{i=0}^{\ell}$, proofs $x_1 > \sum_{i=0}^{\ell} a_i \cdot 2^i$。Furthermore, the whole process is divided into two parts as follows:

[0036] In the first part, given c, $\{c'_{2i}\}_{i=0}^{\ell}$和$\left\{c'_{3i} = g^{b_i \cdot 2^i}h^{r'_{3i}}\right\}_{i=0}^{\ell}$ and $\left\{c'_{3i} = g^{b_i \cdot 2^i}h^{r'_{3i}}\right\}_{i=0}^{\ell}$, the prover shall proof $x_1 = \sum_{i=0}^{\ell} a_i \cdot 2^i + \sum_{i=0}^{\ell} b_i \cdot 2^i$, by providing a signature corresponding to the public key $\left(h, \frac{c}{\left(\prod_{i=0}^{\ell} c'_{2i} \cdot c'_{3i}\right)}\right)$. If $x_1 = \sum_{i=0}^{\ell} a_i \cdot 2^i + \sum_{i=0}^{\ell} b_i \cdot 2^i$, the prover may figure out $log_h\{c/\prod_{i=0}^{\ell} c'_{2i} \cdot c'_{3i}\} = r_1 - \sum_{i=0}^{\ell}(r'_{2i} + r'_{3i})$, otherwise, due to the loghg is unknown to anyone, the prover cannot draw a conclusion.

[0037] In the second part, the prover shall proof that all ai and bi belong to {0, 1}. Wherein, taking ai as an example, the prover only needs to provide a ring signature which takes (h, c′2i) and $(h, c'_{2i}/g^{2^i})$as the public keys.

[0038] The said ring signature scheme allows the verifier to check the validity of the signature without exposing the public key corresponding to the real signature key. Specifically, if ai=0, the prover should know loghc ′2i=r ′2i; if ai=1, the verifier should know $log_h(c'_{2i}/g^{2^i}) = r'_{2i}$; in other cases, due to the loghg is unknown to anyone, the prover cannot figure out loghc ′2i or $log_h\left(\frac{c'_{2i}}{g^{2^i}}\right)$. Finally, the verifier can check ai $\in$ {0, 1}.

[0039] Wherein, the said Pedersen commitment is a widely used cryptographic commitment, and the construction of which is divided into 3 stages:

2021105670 17 Aug 2021

[0040] The initialization stage: select the multiplicative group G with a large prime order q, wherein, g and h are two generators in the cyclic group, and then open the tuple (g, h, q);

[0041] The commitment stage (camm): the commitment party selects a random number r as the blind factor, and then calculates the commitment value comm=gmhr mod q for the message m, after that, sends comm to the receiver;

[0042] The open stage (open): the commitment party sends (m, r) to the receiver, and then the receiver verifies whether camm is equal to gmhrmod q, and thus, if they are equal, accept the commitment, otherwise, reject the commitment.

[0043] The said transaction propagation module specifically refers to: the transaction initiator commits the transaction to the consensus nodes, and each consensus node immediately verifies the validity of the transaction, including the validity of the zero-knowledge proof and the validity of the digital signature, after receiving it. If it is valid, the consensus nodes would save a copy and spread it to all neighbor nodes, as well as update the amount of the corresponding account at the same time.

[0044] The said transaction packaging module is used to include valid transactions in a transaction block ultimately, and thus, these transactions can be record in the blockchain permanently.

[0045] The system model of the embodiment of the present invention as shown in figure 1, a blockchain-based method for domain name auction by means of sealed-bid can be obtained which comprises the following stages specifically:

[0046] In the first stage, create an auction:

[0047] After deploying the smart contract, the owner of domain name calls the function (Create(T1, T2, name, δ))to create an auction, wherein, T1 and T2 represent two time points specified by the system, i.e., T1 represents the deadline for bidding, and T2 represents the deadline for revealing the bid; in addition, name refers to the domain name which would be auctioned by the owner of domain name; and δ refers to the signature of the account owner who owns the domain name signed on the smart contract by utilizing the public key. Specifically, if the consensus nodes in the blockchain receive the calling of this function, the consensus nodes would check the validity of (T1, T2, name, δ), and determine whether there is an auction contract corresponding to the name in the blockchain. If passed, the consensus nodes would continue to run the Create function, otherwise, the consensus nodes would stop running the function. Then, the information related to the bidder by utilizing the bidder [ ] array, comprises the public key corresponding to an account of the bidder, the commitment made by the bidder to the tendered amount (commit) and the data used to reveal the bid by the bidder (m, r) would be recorded. Furthermore, the status of the smart contract comprises: active and closed.

[0048] In the second stage, commit the bid:

[0049] When a bidder is aware that there is an auction contract for certain domain names on the blockchain, the bidder participates in the bidding by calling a commitment function $Commit(pk, \{c_i'\}_{i=0}^{\ell}, \sigma, ZKP_1, ZKP_2)$, wherein, pk represents a public key of an account of the bidder, and $\left\{c'_i = g^{c'_i \cdot 2^i}\right\}_{i=0}^{\ell}$ represents the commitment to the bid $\sum_{i=0}^{\ell} c'_i \cdot 2^i$; and the σ represents the signature signed on the smart contract by utilizing the pk; in addition, ZKP represents the zero-knowledge proof of $c > \sum_{i=0}^{\ell} c'_i \cdot 2^i > 0$, wherein, c represents the balance of the account corresponding to the pk;

[0050] If the consensus nodes in the blockchain receive the calling of the Commit function, the consensus nodes would check whether the array bidder [ ] does not contain the pk, and determine whether the time T of calling the function is within the validity period, as well as check the validity of (σ, ZKP). If passed, the consensus nodes would continue to run the Create function, otherwise, the consensus nodes would stop running the function.

[0051] In the third stage, reveal the bidding:

[0052] After the bidding duration T1 expires, the bidding stage stops, and each bidder can reveal the bid by means of calling the bidding reveal function $Reveal(pk, \{(\bar{m}'_i, \bar{r}'_i)\}_{i=0}^{\ell})$, wherein, pk is the same public key that used by the bidder when calling the Commit function, and $\{(\bar{m}'_i, \bar{r}'_i)\}_{i=0}^{\ell}$ is used to open the commitment $\{c'_i\}_{i=0}^{\ell}$;if the consensus nodes receive the calling of the Reveal function, the consensus nodes would check whether the time T to call the function is within the validity period, and determine whether there is a commitment $\{c'_i\}_{i=0}^{\ell}$ corresponding to the pk exists in the array bidder[ ], as well as check whether $\{(\bar{m}'_i, \bar{r}'_i)\}_{i=0}^{\ell}$ can open the commitment. If passed, the consensus nodes would run the Reveal function; otherwise, the consensus nodes would stop running the Reveal function.

[0053] In the fourth stage, close the auction:

[0054] After completing operation the third stage, anyone can judge who is the successful bidder according to the records in the array bidder [ ], in this case, the successful bidder would call the Finalize function. Then, if the consensus nodes receive the calling of the function, the consensus nodes would check whether the bidding duration for the auction is due according to the deadline for revealing the bid T2, and then check whether the

2021105670 17 Aug 2021

current smart contract is in a running state. If passed, the consensus nodes would continue to run the Finalize function; otherwise, the process would be stopped.

[0055] Wherein, there are different treatment methods are proposed according to the three states of bidders: the first is that the bidder fails to reveal the bid in the third stage, and the bidder would be punished by deducting part of the funds. The second is related to the successful bidder, i.e., the second-highest tendered amount would be transferred to the owner of the domain name, and the domain name would be transferred from the owner to the successful bidder. Finally, the last case refers to those follow the agreement but have not won the bid. In this case, no operation needs to be done.

[0056] Finally, close the smart contract.

2021105670 17 Aug 2021

Claims

1. A blockchain-based method for domain name auction by means of sealed-bid, characterized in that comprising following stages:

During the first stage, the owner of domain name creates a domain name auction contract on the blockchain, and then checks the validity of the domain name auction contract by means of a consensus mechanism as well as records the information of bidder;

During the second stage, if the bidder is aware that there is a domain name auction contract exists on the blockchain, the bidder shall verify the commitment by means of calling operation. Thus, if the verification is successful, participate in the bidding;

During the third stage, each bidder who has passed the check would reveal the bidding by means of the consensus mechanism when the bidding duration expires;

During the fourth stage, anyone can check the bidding records after revealing the bidding, and the bidders shall complete the bidding according to their own state respectively. After that, the auction would be closed.

2. The said blockchain-based method for domain name auction by means of sealed-bid according to claim 1, characterized in that the said owner of domain name calls the function (Create (T1, T2, name, δ)) to create a domain name auction contract, wherein, the T1 of the said function (Create(T1, T2, name, δ)) represents the deadline for bidding, and T2 represents the deadline for bid opening, and name refers to the domain name which would be auctioned by the owner of domain name, as well as δ refers to the signature of the account owner who owns the domain name signed on the smart contract by utilizing the public key;

The said process of checking the validity of the domain name auction contract by means of a consensus mechanism specifically refers to: if the consensus nodes in the blockchain receive the calling of the Create function, the consensus nodes would check the validity of (T1, T2, name, δ), and determine whether there is an auction contract corresponding to the name in the blockchain. If passed, the consensus nodes would continue to run the Create function, otherwise, the consensus nodes would stop running the function;

Then, recording the information related to the bidder by utilizing the bidder [ ] array, wherein, the information comprises the public key corresponding to an account of the bidder, the commitment made by the bidder to the tendered amount and the data used to reveal the bid by the bidder.

3. The said blockchain-based method for domain name auction by means of sealed-bid according to claim 2, characterized in that the bidder participates in the bidding by calling a commitment function ($Commit(pk, \{c_i'\}_{i=0}^{\ell}, \sigma, ZKP_1, ZKP_2)$), wherein, pk represents a public key of an account of the bidder, and $\{c'_i = g^{c'_i \cdot 2^i}\}_{i=0}^{\ell}$ represents the commitment to the bid $\sum_{i=0}^{\ell} c'_i \cdot 2^i$; and the σ represents the signature signed on the smart contract by utilizing the pk; in addition, ZKP represents the zero-knowledge proof of $c > \sum_{i=0}^{\ell} c'_i \cdot 2^i > 0$, wherein, c represents the balance of the account corresponding to the pk;

If the consensus nodes in the blockchain receive the calling of the Commit function, the consensus nodes would check whether the array bidder [ ] does not contain the pk, and determine whether the time T of calling the function is within the validity period, as well as check the validity of (σ, ZKP). If passed, the consensus node continues to run the Commit function; otherwise, the consensus nodes would stop running the function.

4. The said blockchain-based method for domain name auction by means of sealed-bid according to claim 2, characterized in that the said third stage specifically refers to: after the bidding duration expires, the bidding stage stops, and each bidder can reveal the bid by means of calling the bidding reveal function $Reveal(pk, \{(\bar{m}'_i, \bar{r}'_i)\}_{i=0}^{\ell})$, wherein, pk is the same public key that used by the bidder when calling the Commit function, and $\{(\bar{m}'_i, \bar{r}'_i)\}_{i=0}^{\ell}$ is used to open the commitment $\{c'_i\}_{i=0}^{\ell}$;if the consensus nodes receive the calling of the Reveal function, the consensus nodes would check whether the time T to call the function is within the validity period, and determine whether there is a commitment $\{c'_i\}_{i=0}^{\ell}$ corresponding to the pk exists in the array bidder[ ], as well as check whether $\{(\bar{m}'_i, \bar{r}'_i)\}_{i=0}^{\ell}$ can open the commitment. If passed, the consensus nodes would run the Reveal function; otherwise, the consensus nodes would stop running the Reveal function.

5. The said blockchain-based method for domain name auction by means of sealed-bid according to claim 2, characterized in that the said fourth stage specifically refers to: after the bid has been revealed, anyone can judge who is the successful bidder according to the records in the array bidder [ ], wherein, the said successful bidder would call the Finalize function. Then, if the consensus node receives the calling of the function, the consensus nodes would check whether the bidding duration for the auction is due according to the deadline for revealing the bid, and then

2021105670 17 Aug 2021

check whether the current smart contract is in a running state. If passed, the consensus nodes would continue to run the Finalize function, wherein, the second-highest tendered amount would be transferred to the owner of the domain name, and the domain name would be transferred from the owner to the successful bidder; otherwise, the process would be stopped; in addition, if the said bidder fails to reveal the bid, such bidder will be punished by deducting part of the funds; furthermore, if the bidder fails to win the bid, no operation would be done by system.

2021105670 17 Aug 2021

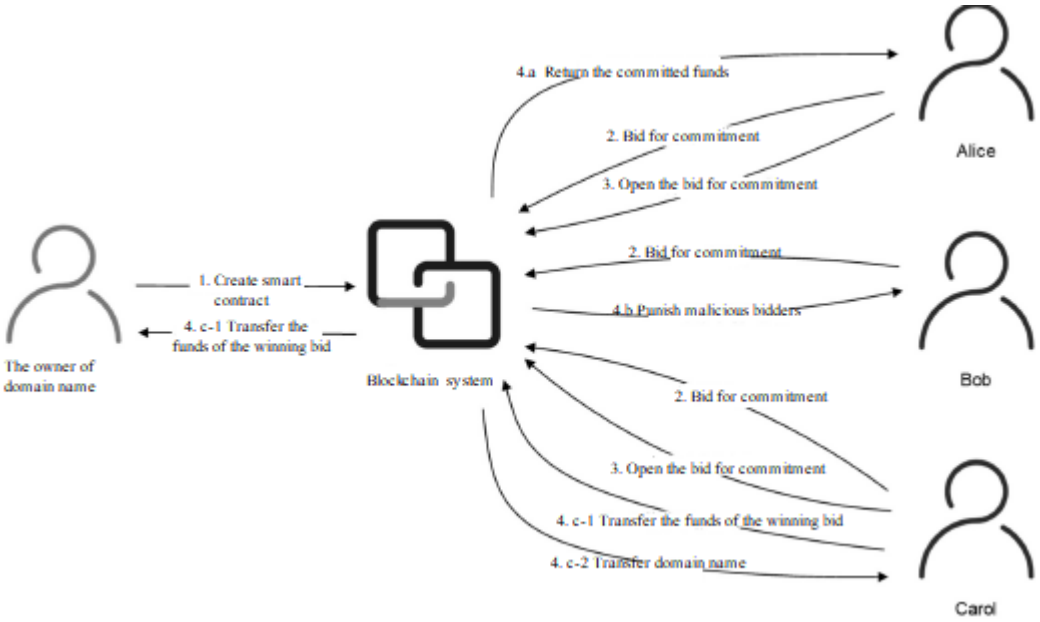

Figure 1