

Electronic Acknowledgement Receipt

EFS ID:	44188046
Application Number:	17517563
International Application Number:	
Confirmation Number:	3763
Title of Invention:	BLOCKCHAIN E-VOTING SYSTEM AND OPERATING METHOD THEREOF
First Named Inventor/Applicant Name:	Jehyuk Jang
Customer Number:	71572
Filer:	Heidi Eisenhut/Kathleen Smith
Filer Authorized By:	Heidi Eisenhut
Attorney Docket Number:	HANMIR-1074
Receipt Date:	02-NOV-2021
Filing Date:	
Time Stamp:	19:31:05
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	\$ 830
RAM confirmation Number	E2021A2J31373898
Deposit Account	505240
Authorized User	Kathleen Smith

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	HANMIR-1074_ADS.pdf	1226510	no	8
			534b7a374e800badd6e871f0ed4d11fd7e8b2f0		

Warnings:

Information:

2	Oath or Declaration filed	HANMIR-1074_Declarations.pdf	2179018	no	2
			ca1990c84eb727c2cbb2c9cc7a64a5c5fb58d1a1a0		

Warnings:

Information:

3	Power of Attorney	HANMIR-1074_POA.pdf	3107734	no	2
			90802bdb1c098b0a6b3f844088aa97d3c5abdaa5		

Warnings:

Information:

4		HANMIR-1074_EN_Translation.pdf	286371	yes	40
			8383ccc2c746f17ec70c0998baa2e79e961dde1		

Multipart Description/PDF files in .zip description

Document Description	Start	End
Translation of Foreign Priority Documents	1	1
Specification	2	32
Claims	33	39
Abstract	40	40

Warnings:

Information:

5	Drawings-only black and white line drawings	HANMIR-1074_Drawings.pdf	129958	no	3
			5b57d2d837acc35a1f29e94ee4e596368efa1d1e		
Warnings:					
Information:					
6	Foreign Reference	HANMIR-1074_IDS_KR20200008413A.pdf	1860638	no	14
			f829780134d0d6ea57d66304bdcdadac50a7ac43		
Warnings:					
Information:					
7	Non Patent Literature	HANMIR-1074_IDS_NPL.pdf	1537531	no	16
			61593c8203675122bf06eab8a445cade42dd77a1		
Warnings:					
Information:					
8	Information Disclosure Statement (IDS) Form (SB08)	HANMIR-1074_IDS.pdf	1034026	no	4
			0f4f2bb46336199711d47b34d23f9b62ae2e7be2		
Warnings:					
Information:					
<p>A U.S. Patent Number Citation or a U.S. Publication Number Citation is required in the Information Disclosure Statement (IDS) form for autoloading of data into USPTO systems. You may remove the form to add the required data in order to correct the Informational Message if you are citing U.S. References. If you chose not to include U.S. References, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.</p>					
9	Fee Worksheet (SB06)	fee-info.pdf	44016	no	2
			0e86fad289496eec9815e55bfd7cb4485d1a9ec		
Warnings:					
Information:					
Total Files Size (in bytes):			11405802		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

CERTIFICATION OF TRANSLATION

I, Kimoon KIM of
6th Fl. Hyunjuk Bldg., 114, Yeoksam-ro, Gangnam-gu, Seoul, 06252, Republic of
Korea do hereby declare that:


I am well acquainted with English languages and that the document listed below has
been accurately translated, to the best of my knowledge and ability:

Korean Patent Application No. 10-2020-0146369 (2020-11-04)

Korean Patent Application No. 10-2020-0171424 (2020-12-09)

U.S. Application No. 63/112723 (2020-11-12)

I declare under penalty of perjury that the foregoing is true and correct.

Signature  _____

Date October 27, 2021

BLOCKCHAIN E-VOTING SYSTEM AND OPERATING METHOD THEREOF

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present application claims priority under 35 U.S.C. 119 and 35 U.S.C. 365 to Korean Patent Application Nos. 10-2020-0146369, filed on November 4, 2020, and 10-2020-0171424, filed on December 9, 2020, and U.S. Provisional Application No. 63/112723, filed on November 12, 2020, which are incorporated by reference herein in their entireties.

BACKGROUND

[0002] The present disclosure relates to an electronic voting (e-voting) system using a blockchain.

[0003] As an example, the present disclosure relates to an e-voting system using a blockchain capable of zero-knowledge proof that does not require trusted tallying authorities.

[0004] As an example, the present disclosure relates to an e-voting system using a blockchain based on a smart contract.

[0005] As an example, the present disclosure relates to a voting system based on a smart contract, capable of zero-

knowledge proof that does not require trusted tallying authorities.

[0006] An e-voting system using an online system is cost-effective and allows opinions to be expressed anytime anywhere. However, it is difficult to keep various basic principles of voting.

[0007] In this background, Korean Patent Laid-Open No. 1020200008413 discloses an e-voting system using a blockchain and an operating method thereof. Although the possibility of realization of an online voting has been enhanced by the above patent document, there is a problem in that it largely depends on the trust of the voting commission. In view of the nature of e-voting, depending on the trust of the voting commission is a big problem that makes the practical application of e-voting difficult.

[0008] Specifically, the fairness of voting system of the above patent document depends on the trust of voting commission, i.e., a trusted third-party. For example, a third party stores digital IDs (DIDs) of voters and voting rights data corresponding thereto. Therefore, a third party may use the voting rights of

others. In other words, the basic principles of e-voting may be damaged by the manipulation of a third party.

[0009] In addition, if a third party is a computer program and a server, the possibility that all records may be stolen by hackers cannot be excluded.

[0010] Furthermore, a third party may omit specific votes at will.

[0011] As described above, if a third party operating on the basis of trust is corrupted, fraudulent voting may occur. In particular, it is a big problem for non-governmental or private organizations with no public trust.

SUMMARY

[0001] The present disclosure proposes a blockchain e-voting system, of which the fairness does not depend on trusted third parties, and an operating method thereof.

[0002] The blockchain e-voting system of the present disclosure may include at least two vote nodes each having an identification private key, an identification public key, a group encryption private key, and a group encryption public key.

[0003] The blockchain e-voting system may include a voter management node that uploads identification data and the public keys of the vote node to the blockchain.

[0004] The blockchain e-voting system may include a first smart contract module that receives the public and private keys and the identification data of the vote node, identifies the vote node, generates an identification number, performs group encryption on a vote result, and generates zero-knowledge proofs that ensure correctness of the process.

[0005] The blockchain e-voting system may include a second smart contract module that downloads the vote result from the blockchain and confirms the correctness and tallying result of voting without decrypting the vote result.

[0006] The first smart contract module may upload the vote result and zero-knowledge proof, on which the group encryption has been performed, to the blockchain.

[0007] The operation method of the blockchain e-voting system according to the present disclosure may include generating, by the vote node, an identification public key, an identification private key, a group encryption public key, and a group

encryption private key.

[0008] The operating method of the blockchain e-voting system may include transmitting, by the vote node, the identification public key and the group encryption public key to the voter management node.

[0009] The operating method of the blockchain e-voting system may include uploading, by the voter management node, the identification public key, the group encryption public key, and the identification data of the vote node to the blockchain.

[0010] The operating method of the blockchain e-voting system may include connecting, by the vote node, to the first smart contract module and identifying the vote node by comparing the identification data held by the vote node with the identification data uploaded to the blockchain.

[0011] The operating method of the blockchain e-voting system may include generating a unique vote node identification number by using the identification public key.

[0012] The operating method of the blockchain e-voting system may include generating a first zero-knowledge proof that guarantees the correctness of the identification process and the

uniqueness of the vote node identification number.

[0013] The operating method of the blockchain e-voting system may include writing one's own choice and performing group encryption thereon.

[0014] The operating method of the blockchain e-voting system may include generating a second zero-knowledge proof that guarantees the correctness of one's choice writing process and the group encryption process.

[0015] The operating method of the blockchain e-voting system may include uploading, by the first smart contract module, the first zero-knowledge proof and the second zero-knowledge proof for the vote node to the blockchain.

[0016] The operating method of the blockchain e-voting system may include uploading the vote result of the vote node to the blockchain.

[0017] The operating method of the blockchain e-voting system may include verifying, by the second smart contract module, the first zero-knowledge proof and the second zero-knowledge proof.

[0018] The operating method of the blockchain e-voting system may perform tallying based on the vote results.

[0019] According to the present disclosure, it is possible to implement e-voting that keeps the basic principles of voting, maintains zero-knowledge proof, and does not depend on the trust of the third party such as the voting commission.

BRIEF DESCRIPTION OF THE DRAWINGS

[0020] Fig. 1 is a configuration diagram of a blockchain e-voting system according to an embodiment.

[0021] Fig. 2 is a flowchart for describing an operating method of the e-voting system according to an embodiment.

[0022] Fig. 3 shows upload data of a vote node which is uploaded to a blockchain.

DETAILED DESCRIPTION OF THE EMBODIMENTS

[0023] First, various technical elements used in the description of embodiments of the present disclosure are defined.

[0024] <Blockchain>

[0025] A blockchain is a database that exists on an Internet peer-to-peer network. The blockchain includes blocks connected to each other, and each of the blocks includes a plurality of

transactions. At least one of data or smart contract is recorded on the transaction. An unverified transaction pool exists outside the blocks. The unverified transaction pool is a temporary storage for storing unverified transactions. Data recorded on the blockchain cannot be forged or altered. No permission is required to read the data recorded on the blockchain. That is, anyone can access the data.

[0026] A procedure for a user to upload data to the blockchain undergoes a propagation step, a verification step, and a publication process. Details thereof are as follows. First, the user converts data into the form of transaction, inserts the transaction into an unverified transaction pool, and propagates the unverified transaction pool. A number of verifier nodes in the network verify transactions of the unverified transaction pool. If the verification of the unverified transactions is finished, the unverified transaction is published in the block through consensus among the verifiers. If the blockchain used is a public blockchain, the verifier nodes may be a number of unspecified nodes, and if the blockchain used is a private blockchain, the verifier nodes may be a preselected blockchain

manager.

[0027] <Zero-Knowledge Proof>

[0028] The zero-knowledge proof is a proving protocol in which a prover convinces a verifier that a certain statement is true. In this case, the zero-knowledge proving protocol must have zero-knowledge property that does not transmit, to the verifier, private information other than the fact that the statement is true.

[0029] When a statement including public information and private information is S , the necessary and sufficient conditions for a proving protocol to be a zero-knowledge proving protocol are completeness, soundness, and zero-knowledge.

[0030] The zero-knowledge proving protocol may be divided into two processes: a proving process and a verification process. The proving process is a process of generating a proof after the prover verifies that the statement S is true. The verification process is a process in which the verifier receives a proof from the prover and confirms whether there is any problem in the proof. If there is no problem in the proof, it must be mathematically guaranteed that the prover has correctly performed the self-

verification of the statement S.

[0031] <vote node Identification Number>

[0032] The present disclosure includes a signature algorithm used when a vote node generates an identification number. The vote node may be, for example, a terminal that the voter uses to vote.

[0033] Examples of the signature algorithm may include Rivest-Shamir-Adleman (RSA) cryptosystem and Elliptic Curve Digital Signature Algorithm (ECDSA) cryptosystem. Other methods may also be applied.

[0034] In an embodiment, a signing algorithm using RSA may be used. RSA will be described below in detail.

[0035] Each vote node has an identification public key of p and q , and an identification private key of s . The keys are required for generating the identification number of the vote node. A process (sign) of generating a unique identification number by signing personal identification data m of the vote node may be defined as $\text{sing}(m,s) := m^s \pmod{q}$. In this document, the operator \wedge stands for power. p , q , and s may be provided according to the RSA system by using any two prime numbers.

[0036] A process of verifying the uniqueness of a certain identification number M is $\text{verify}(M, p, q) := (M^p \pmod{q}) =? (m \pmod{q})$, where $=?$ is an operator that outputs 1 if the two operands are equal to each other and outputs 0 if the two operands are different from each other. Since only one identification public key for one vote node is uploaded to the blockchain, the verification process may prove the uniqueness of the vote node identification number.

[0037] <Group Encryption>

[0038] The group encryption is used for the tallying and encryption of vote contents. The group encryption is an encryption that enables to add up vote results without decrypting the vote contents. The group encryption of the embodiment is only an example, and other methods may be applicable.

[0039] The process of group encryption will be described below.

[0040] There is a group G of N vote nodes. First, each vote node may have two group encryption public keys and one group encryption private key. The keys are required for group encryption. Each i -th vote node in G may have an arbitrary

integer sk_i as the group encryption private key. Using the group private key, each i -th vote node may upload its group encryption public key (e.g., $pk_i := g^{sk_i}$) to the blockchain. g is an encryption base for the group G , and is information disclosed to all vote nodes. The encryption base g is an integer. The encryption base g may be generated and distributed by a voter management node.

[0041] Group signing key yk_i may be computed by using the public keys of all vote nodes. Formally, the group signing key yk_i of the i -th vote node may be provided by using Equation 1.

[0042] [Equation 1]

$$yk_i := \frac{\prod_{j=i+1}^N pk_j}{\prod_{j=1}^{i-1} pk_j}$$

[0043] yk_i is the group signing key of the i -th vote node, pk_i is the group public key of the i -th vote node, and N is the number of vote nodes belonging to the group G .

[0044] The group encryption ENC of the group G may be given by Equation 2.

[0045] [Equation 2]

$$ENC_{G(i)} = (yk_i)^{sk_i} g^{m_i}$$

[0046] m_i is a message that the i -th vote node of the group G wants to carry, that is, the vote contents, and sk_i is the group private key of the i -th vote node.

[0047] Tallying may be performed by Equation 3.

[0048] [Equation 3]

For all member indices $i=1, \dots, N$ of G ,

$$\prod_{i=1}^N ENC_{G(i)}(m_i) = g^{\sum_{i=1}^N m_i}$$

[0049] $ENC_{G(i)}$ is an encrypted message of the i -th vote node of the group G .

[0050] The group encryption will be described as an example. Suppose a group of three vote nodes, i.e., i is from 1 to 3. Each vote node shares the group public key, the group signing key, and the group private key. The encryption base is, for example, 3.

[0051] The public key and the private key of each group member may be $sk_1 = 7$ and $pk_1 := g^{sk_1} = 3^7 = 2187$, $sk_2 = 5$ and $pk_2 := g^{sk_2} = 3^5 = 243$, and $sk_3 = 4$ and $pk_3 := g^{sk_3} = 3^4 = 81$.

[0052] When the private key and the public key of each group member are determined as described above, the group public key

yk_i of each group member may be generated by using Equation 1 above.

The group public key of each group member may

$$\text{be } yk_1 = pk_1 \cdot pk_2 = 3^5 \cdot 3^3 = 3^8, \quad yk_2 = \frac{pk_2}{pk_1} = \frac{3^4}{3^5} = 3^{-1}, \text{ and}$$

$$yk_3 = \frac{1}{pk_1 \cdot pk_2} = \frac{1}{3^5 \cdot 3^3} = 3^{-8}.$$

[0053] The voting of each group member is, for example, to attribute at most 5 points per query for three queries. Each group member voted, for example, with 2 points for m_1 , 4 points for m_2 , and 1 point for m_3 .

[0054] The group encryption ENC of the i -th group member may be performed by Equation 2 above.

[0055] The group encryption result of each group member performed by Equation 2 may be given as follows:

Decision-making encryption of first group member

$$ENC_{g(1)} = (yk_1)^{m_1} g^{m_2} = (3^8)^2 3^2 = 3^{68}.$$

Decision-making encryption of second group member

$$ENC_{g(2)} = (yk_2)^{m_2} g^{m_3} = (3^{-1})^4 3^1 = 3^{-11}.$$

Decision-making encryption of third group member

$$ENC_{g(3)} = (yk_3)^{m_3} g^{m_1} = (3^{-8})^1 3^5 = 3^{-47}.$$

[0056] Tallying may be performed by calculating Equation 3.

When the tallying of each group member is performed by using Equation 3, the tallying is given as follows:

$$\begin{aligned}\prod_{i=1}^3 ENC_{G(i)} &= ENC_{G(1)} \cdot ENC_{G(2)} \cdot ENC_{G(3)} \\ &= 3^{66} \cdot 3^{11} \cdot 3^{47} \\ &= 3^7.\end{aligned}$$

[0057] Consequently, if the tallying result is 3^7 and a discrete logarithm with a base of 3 (encryption base) is taken, 7 is calculated. According to this result, the intention of each vote node cannot be exposed because no message is decrypted during the tallying process. Nevertheless, the aggregation of vote results can be calculated.

[0058] Of course, the present disclosure can use other group encryption methods than that used in the embodiment.

[0059] <Smart Contracts>

[0060] Smart contracts may be provided in the form of programs. After an input is received and a specified operation is performed thereon, an output may be recorded and uploaded on a new transaction. The operations supported by smart contracts include all operations supported by turing-complete language, and include the operations used in the zero-knowledge proving

protocol. A program written in a smart contract may be referred to as a smart contract module. Smart contract modules may be provided by the voter management node.

[0061] In an embodiment, the smart contract module may include a first smart contract module that executes voting, and a second smart contract module that executes tallying.

[0062] Fig. 1 is a configuration diagram of a blockchain e-voting system according to an embodiment.

[0063] Referring to Fig. 1, a voter management node 2 may provide an encryption base g of a group G to each vote node (①). The voter management node 2 may obtain a public key of each vote node 1 (②), and may register the obtained public key to a blockchain 3 together with identification information (DID, iris, fingerprint, etc.) of each vote node 1 held by the voter management node (③). The voter management node 2 may upload the smart contract modules to the blockchain 3 (③).

[0064] The first smart contract module 41 downloads all registered identification information of all vote nodes (④). Then, each vote node 1 runs the first smart contract module 41 with a DID held by the vote node itself, a signature public key,

a signature private key, a group encryption public key, a group encryption private key (⑤), and vote content message ($vote_i$) as inputs.

[0065] Using the information from blockchain and inputs taken by each i -th vote node, the first smart contract module 41 may generate the certification of vote node identification test (Cert), vote node identification number ($voteID_i$), and zero-knowledge proof ($proof_voteID_i$) for the validity of the vote node identification certification. In addition, the first smart contract module 41 may generate a group signing key yk_i , may perform group encryption ($ENC_{G(i)}(vote_i)$), and may generate zero-knowledge proof ($proof_voteENC_i$) for the validity of group encryption.

[0066] The first smart contract module 41 uploads a vote result ($ballot_i$) of the i -th vote node to the blockchain 3 (⑥). The vote result ($ballot_i$) is an array of data including vote node identification number ($voteID_i$), the zero-knowledge proof ($proof_voteID_i$) for the validity of vote node identification certification, the vote execution time ($time_publish$), the group signing key (yk_i) generation, the group encryption ($ENC_{G(i)}(vote_i)$)

of vote, and the zero-knowledge proof (proof_voteENC_i) for the validity of group encryption. The group signing key is used for the group encryption. A vote content message vote_i of the i -th vote node may be encrypted as the form of the group encryption.

[0067] After the voting of all vote nodes is finished, the tallying may be performed. The tallying may be performed by the second smart contract module 42. The second smart contract module 42 obtains an initiation key s_0 for tallying from the voter management node 2. The second smart contract module 42 may perform a tallying of vote results recorded on the blockchain.

[0068] The second smart contract module accepts only the most recent vote result (ballot_i) if there are two or more results with the same vote node identification number (voteID_i). In this manner, the final intention expressed by the vote node may be determined by using the latest information when one vote node has voted more than once.

[0069] The second smart contract module 42 may output the sum of vote results without decrypt any message. This has been described in detail through the group encryption.

[0070] An operating method of the blockchain e-voting system

according to an embodiment will be described with reference to Fig. 1 and related technical elements.

[0071] Fig. 2 is a flowchart for describing the operating method of the e-voting system according to an embodiment.

[0072] The operating method of the embodiment does not require trusted tallying parties. The operating method of the embodiment does not require a trusted third party to keep the principles of voting. In the operating method of the embodiment, there are only a voter management node hosting the voting and vote nodes participating in the voting. The voter management node may have its own secret key (s_0) used to initiate the tallying. A voting may be a procedure of asking decisions of vote nodes for queries on the agenda defined in advance by the voter management node. The number of queries may be denoted by L . The number of votes that one voter can cast into all queries may be limited to S_{\max} . A list of N vote nodes may be determined before the voting is initiated. The voter management node may hold personal authentication data of all N vote nodes before the voting is conducted. The personal authentication data of the voter held by the voter management node may be referred to as S -

DID_i. Examples of the personal authentication data may be at least one of an iris image, a fingerprint image, an ID photo image, voice data, or public authentication data, but are not limited thereto. For each i-th vote node, personal authentication data may be referred to as DID_i. In the operating method of the embodiment, after each vote node performs self-verification on the correctness of all voting processes, related zero-knowledge proofs may be uploaded to the blockchain.

[0073] First, the voter management node 2 may provide the encryption base g to each vote node (S1). The vote node 1 may generate a signature public key (p_i, q_i) and a signature private key (s_i) . The vote node 1 may generate a group encryption public key (pk_i) and a group encryption private key (sk_i) by using the encryption base g . The vote node may transmit the public key to the voter management node (S2).

[0074] The voter management node 2 may upload data of each vote node to the blockchain 3 as shown in Fig. 3 (S3). Other data uploaded to the blockchain 3 may also be uploaded in the same structure although different in contents.

[0075] The voter management node 2 may upload a smart

contract (S3). Smart contracts may include a smart contract module for voting and proving and another smart contract module for tallying and verification. Identification information (DID) of each vote node 1 previously held by the voter management node may be registered in the blockchain.

[0076] The voting may be performed by the first smart contract module 41. The vote node may perform the voting by using the first smart contract module 41.

[0077] The first smart contract module 41 may be executed by each vote node to identify the right to vote, to generate a unique identification number, and to create an intention choice of each vote node (S4). Zero-knowledge proofs may be generated for the validity of the identification number and the intention choice.

[0078] More specifically, the first smart contract module 41 may confirm voting rights of vote nodes by comparing the personal identification information of each vote node (Cert), may generate identification number (voteID_i) for each vote node, may generate zero-knowledge proof (proof_voteID_i) for the vote node identification, and may upload the vote result (ballot_i).

[0079] In creating the intention choice of L queries on the agenda, an $(L+1)$ th field may be added in addition to the L queries. If this additional field is filled by a nonzero, the corresponding ballot may be treated as a blank ballot later. In this manner, the vote node may cast a blank ballot.

[0080] Thereafter, it may be determined whether the sum of the field values does not exceed a maximum value (S_{\max}). If the sum of the field values exceeds the maximum value, the corresponding ballot may be invalidated as an abnormality.

[0081] Thereafter, the group public key (yk_i) may be generated, the group encryption (ENC) may be performed by using the group public key, and zero-knowledge proof (proof_voteENC_i) for the group encryption may be generated.

[0082] Thereafter, the voting may be performed again if an error occurs in either the last confirmation of the voting rights of the vote node (Cert), the zero-knowledge proof (proof_voteID_i) for the vote node identification, or the zero-knowledge proof (proof_voteENC_i) for the group encryption.

[0083] If the voting is finished, the personal identification information (DID_i) and the private key (s_i, sk_i) are deleted from

the smart contract modules.

[0084] If the voting is finished, the first smart contract module 41 uploads the vote result (ballot_i) of the i -th vote node to the blockchain 3 (S5). The uploaded vote result may include the vote node identification information (voteID_i), the zero-knowledge proof (proof_voteID) for the vote node identification, the vote execution time (time_publish), the generation of the group public key (y_{k_i}), the group encryption information ($\text{ENC}_{G(i)}(\text{vote}_i)$), and the zero-knowledge proof (proof_voteENC_i) for the group encryption.

[0085] The voting process (S4) and the vote result uploading process (S5) are performed by the first smart contract module. For details, see Algorithm 4.

[0086] [Algorithm 4]

INPUTS: $DID_i, p_i, q_i, s_i, \mathbf{vote}_i = (x_{i,1}, \dots, x_{i,L_i}), pk_i, sk_i$.

INITIALIZATION: $voteID_i = null$ and $invalid = 0$.

PROCESS:

1. - Download $\mathbf{voter}_i = (\text{hash}(S_DID_i), pk_i, p_i, q_i)$ for all i from blockchain.

2. - $Cert = \text{hash}(DID_i) \wedge \text{hash}(S_DID_i)$.

3. - if $Cert = 1$, do

A. - $voteID_i = \text{sign}(\text{hash}(DID_i), s_i)$.

B. - $proof_voteID_i = \text{ZKP}(\text{process2}, \text{verify}(voteID_i, p_i, q_i))$.

C. - If $x_{i,L_i} \neq 0$, do $x_{i,1} = 0, x_{i,2} = 0, \dots, x_{i,L_i} = 0$.

D. - If $\sum_{i=1}^L x_{i,j} \leq S_{max}$, do $invalid = 1$.

E. - $pk_i = \left(\prod_{j=1}^n pk_j \right) / \left(\prod_{j=1}^{i-1} pk_j \right)$.

F. - $ENC_{G_{ij}}(\mathbf{vote}_i) = (pk_i)^{x_i} g^{vote_i}$.

G. - $proof_voteENC_i = \text{ZKP}(\text{process3-C}, \text{process3-D}, \text{DEC}_{G_{ij}}(ENC_{G_{ij}}(\mathbf{vote}_i)))$.

4. - if $Cert = 0$ or $\text{ZKP_verify}(proof_voteID_i) = 0$ or $\text{ZKP_verify}(proof_voteENC_i) = 0$, then return an error message.

5. - Delete $\mathbf{vote}_i, DID_i, s_i, sk_i$.

OUTPUT: Upload $voteID_i, ENC_{G_{ij}}(\mathbf{vote}_i), proof_voteID_i, proof_voteENC_i$ to blockchain.

[0087] In Algorithm 4, $\text{ZKP}(\text{operation})$ is a function of generating zero-knowledge proof that guarantees the correctness of the operation processes of the input operations.

[0088] In Algorithm 4, $\text{ZKP_verify}(\text{proof})$ is a function of verifying the validity of the input zero-knowledge proof.

[0089] After the voting of all vote nodes is finished, the

tallying may be performed.

[0090] The tallying may be performed by the second smart contract module 42. The second smart contract module 42 may obtain the private key s_0 for initiating the tallying from the voter management node 2 and the vote result from the blockchain (S6).

[0091] The second smart contract module 42 may reject the tallying if the obtained private key s_0 is incorrect.

[0092] The second smart contract module 42 may obtain information from the blockchain and find out the information recorded thereon. In this case, the information may mean generating a single piece of information by linking pieces of information about all blocks of the blockchain. In this case, the information may not mean individually decrypting the group encryption of vote results.

[0093] The second smart contract module 42 may find out the tallying result of the intention choices without decrypting the intention choices (S7). As described above, this operation is performed by the group encryption.

[0094] The second smart contract module 42 may perform the

verification ($ZKP_verify(\text{proof_voteID}_i)$) of the zero-knowledge proof (proof_voteID_i) for the corresponding vote node and the verification ($ZKP_verify(\text{proof_voteENC}_i)$) of the zero-knowledge proof (proof_voteENC_i) for the group encryption.

[0095] The second smart contract module uses the most recent vote result (ballot_i) if there are two or more ballots from the same vote node identification number. In this manner, the final intention of the vote node may be determined by using the latest information when a vote node has voted more than once.

[0096] Thereafter, the second smart contract module 42 may upload the tallying result to the blockchain 3 (S8).

[0097] The basic principles of the voting that the voting system should have may include the followings.

[0098] Correctness: All valid votes are counted accurately in the tallying result.

[0099] Integrity: A means for verifying the vote result is required to prevent forgery of the vote result.

[00100] Soundness: Interference by fraudulent voters is blocked and fraudulent votes are not counted.

[00101] Legality: The right to vote is required to vote.

[00102] Singleness: A valid voter can participate only once.

[00103] Confidentiality: The confidentiality of voters and vote results is ensured.

[00104] Independency: The tallying result during voting does not influence the remaining votes.

[00105] The following describes that the system and the operating method according to the present disclosure keep the above-described principles.

[00106] First, the correctness can be addressed by the following reason.

[00107] Voters can self-verify the validity of their votes by using the voting smart contract. The proof on which the validity self-verification of the voting is performed can be generated. The voting validity proof can be verified by an unspecified number of blockchain verifiers (miners). The tallying smart contract module can verify the validity of the voting once more. The verified proof and encrypted voting contents can be recorded together on the blockchain, making it immutable. All votes can be counted collectively by the tallying smart contract.

[00108] The integrity can be addressed by the following reason.

[00109] The proof that the voting contents were written by the voter can be recorded on the blockchain together with the encrypted voting data, making it immutable. If the voting data is manipulated, the verification of the proof is impossible. Thus, it can be treated as an invalid vote. Anyone can reproduce the tallying result after the voting data and the proofs are verified.

[00110] The soundness can be addressed by the following reason.

[00111] All voters can write the voting contents, can self-verify that the vote is legal, and can record the proof on the blockchain. If the voting contents are false, the proof is unverifiable. The voting contents recorded together with the unverifiable proof may be invalidated.

[00112] The legality can be addressed by the following reason.

[00113] All voters can self-execute personal authentication and can record the proof on the blockchain together with the voting contents. If the personal authentication proof is unverifiable, the voting contents recorded together are invalidated by the tallying smart contract module.

[00114] The singleness can be addressed for the following reason.

[00115] Each voter has a unique vote node identification number. The vote node identification number is generated by using the DID and the private key of the voter, and it has to be verifiable by using the public key of the pre-registered voter. Since one voter pre-registers only one public key, one voter can generate only one identification number. The voters can self-verify the validity of the identification number by using their public keys, can generate the proof, and can record the proof on the blockchain together with the identification number. If the proof for the validity of the identification number is unverifiable, the votes recorded together are invalidated by the tallying smart contract module.

[00116] The confidentiality can be addressed by the following reason.

[00117] The voters can directly generate the vote node identification number by using their private keys. Since the voter records only the vote node identification number on the blockchain, the third party who does not know the private key

cannot infer the relationship between the voter and the identification number. Since the voting contents are encrypted and disclosed and the voting contents are not decrypted even during the tallying, the third party cannot infer the relationship between the identification number and the voting contents.

[00118] The independency can be addressed by the following reason.

[00119] All voting contents can be encrypted and uploaded. The voting contents are not decrypted throughout the entire voting process, including the tallying and vote verification. If all votes are not completed by group encryption, the tallying may be impossible, and therefore every vote cannot be influenced by the other votes.

[00120] According to the above description, the advantages of the voting system and the operating method thereof according to the present disclosure can be understood.

[00121] According to the present disclosure, the e-voting system can be operated in a state of maintaining the zero-knowledge proof and being not affected by the trust of the third

party.

What is claimed is:

1. A blockchain e-voting system comprising:

at least two vote nodes each having a private key and a public key;

a voter management node configured to provide an encryption base to the vote node;

a first smart contract module configured to perform a smart contract, so that the vote node receives a group encryption public key and a group encryption private key generated by using the encryption base, performs group encryption on the voting of the vote node, and uploads a vote result, on which the group encryption has been performed, to a blockchain; and

a second smart contract module configured to download the vote result from the blockchain and confirm the vote result without decrypting the vote result.

2. The blockchain e-voting system of claim 1, wherein the voter management node is configured to pre-register personal identification information of the vote node and upload the first

personal identification information to the blockchain,

wherein the vote node is configured to input personal identification information asserted by the vote node to the first smart contract module, and

wherein the first smart contract module is configured to confirm the vote node by comparing the pre-registered personal identification information with the asserted personal identification information.

3. The blockchain e-voting system of claim 1, wherein the voter management node is configured to provide a tallying public key to the second smart contract module.

4. The blockchain e-voting system of claim 1, wherein the first smart contract module is configured to generate vote node identification information (voteID_i) for the vote node and perform zero-knowledge proof (proof_voteID_i) for the vote node identification information (voteID_i).

5. The blockchain e-voting system of claim 1, wherein the first smart contract module is configured to perform zero-knowledge proof (proof_voteENC_i) for the group encryption.

6. The blockchain e-voting system of claim 1, wherein the smart contract is provided through the blockchain by the voter management node.

7. The blockchain e-voting system of claim 1, wherein the first smart contract module is configured to upload, to the blockchain, vote node identification information (voteID_i), zero-knowledge proof (proof_voteID_i) for the vote node identification information, vote execution time (time_publish), group encryption information ($\text{ENC}_{G(i)}(\text{vote}_i)$), and zero-knowledge proof (proof_voteENC_i) for group encryption information.

8. The blockchain e-voting system of claim 1, wherein the second smart contract module is configured to tally.

9. The blockchain e-voting system of claim 1, wherein the second smart contract module is configured to upload the tallying result to the blockchain.

10. An operating method of a blockchain e-voting system, the operating method comprising:

providing, by a voter management node, a same encryption base to each of at least two vote nodes;

generating, by the vote node, a group encryption public key (pk_i) and a group encryption private key (sk_i) by using the encryption base;

transmitting, by the vote node, the group encryption public key to the voter management node;

uploading, by the voter management node, data of the vote node to a blockchain;

executing, by the vote node, the first smart contract module, identifying the vote node, performing signature, writing intention choice thereof, and performing group encryption;

uploading, by a first smart contract module, a vote result to the blockchain; and

performing, by a second smart contract module, tallying.

11. The operating method of claim 10, wherein the vote node generates a signature public key (p_i, q_i) and a signature private key (s_i) , and transmits the signature public key (p_i, q_i) and the signature private key (s_i) to the voter management node and the first smart contract module.

12. The operating method of claim 10, wherein the smart contracts of the first and second smart contract modules are uploaded to the blockchain by the voter management node.

13. The operating method of claim 10, wherein the data of the vote node includes identification information of each vote node previously pre-registered by the voter management node,

wherein the vote node inputs asserted identification information thereof to the first smart contract module, and

wherein the first smart contract module confirms the voting rights of the vote node by comparing the pre-registered identification information and the asserted identification information.

14. The operating method of claim 10, wherein the vote node executes the first smart contract module, and further performs zero-knowledge proof for the signing operation and zero-knowledge proof for the intention choice operation.

15. The operating method of claim 10, wherein a field for identifying a blank ballot is added to the intention choice.

16. The operating method of claim 10, wherein after the voting is finished, the personal identification information (DID_i), the signature private key (s_i), and the group encryption private key (sk_i) are deleted.

17. The operating method of claim 10, wherein the information uploaded to the blockchain by the first smart contract module includes a vote execution time ($time_publish$).

18. The operating method of claim 10, wherein the second smart contract module obtains a tallying private key (s_0) from the voter management node.

19. The operating method of claim 10, wherein the second smart contract module performs verification ($ZKP_verify(\text{proof_voteID}_i)$) of zero-knowledge proof (proof_voteID_i) for vote node identification and verification ($ZKP_verify(\text{proof_voteENC}_i)$) of zero-knowledge proof (proof_voteENC_i) for the group encryption.

20. The operating method of claim 10, wherein the second smart contract uploads a tallying result to the blockchain.

ABSTRACT

We disclose a blockchain e-voting system, where keeping the basic principles of voting does not require trusted-third parties. The system includes at least two vote nodes each having two sets of private and public keys, a voter management node, two smart contract modules, and a blockchain. A voter management node is configured to provide a cryptographic base for public key generation and to pre-register DIDs of vote nodes. A first smart contract module is configured to perform self-identification of vote nodes, encryption of votes, and generation of zero-knowledge proofs for the validity of their results, and to upload all the outputs to a blockchain. For the purpose, a vote node executes the first smart contract module, taking a voting decision, an asserted DID, the two sets of public and private keys as inputs, where one set of keys is for the self-identification, and another set is for the encryption. A second smart contract module is configured to download the votes from the blockchain, check the validity of proofs, tally up the results without decrypting them, and finally upload the results to blockchain.

FIG. 1

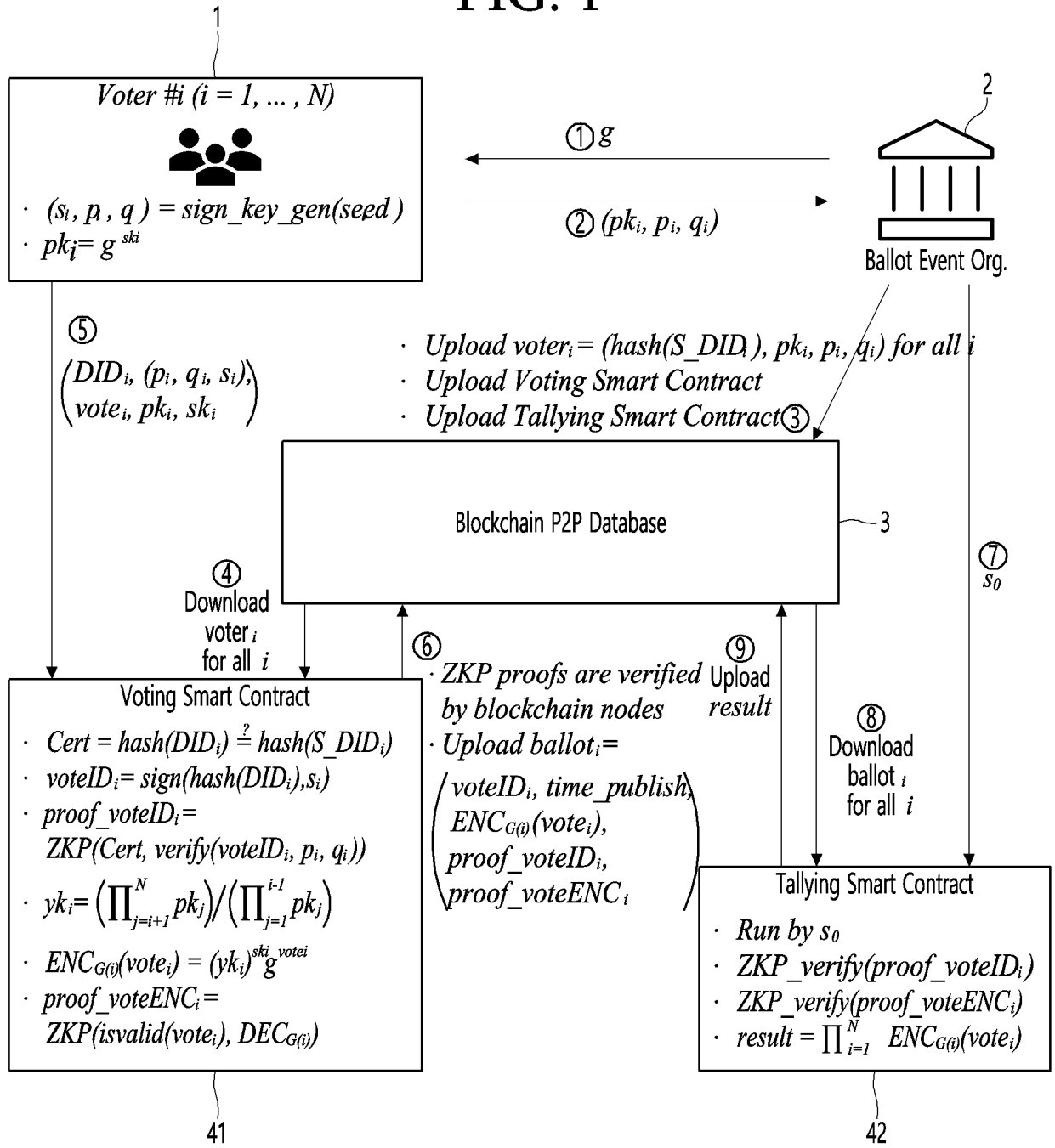


FIG. 2

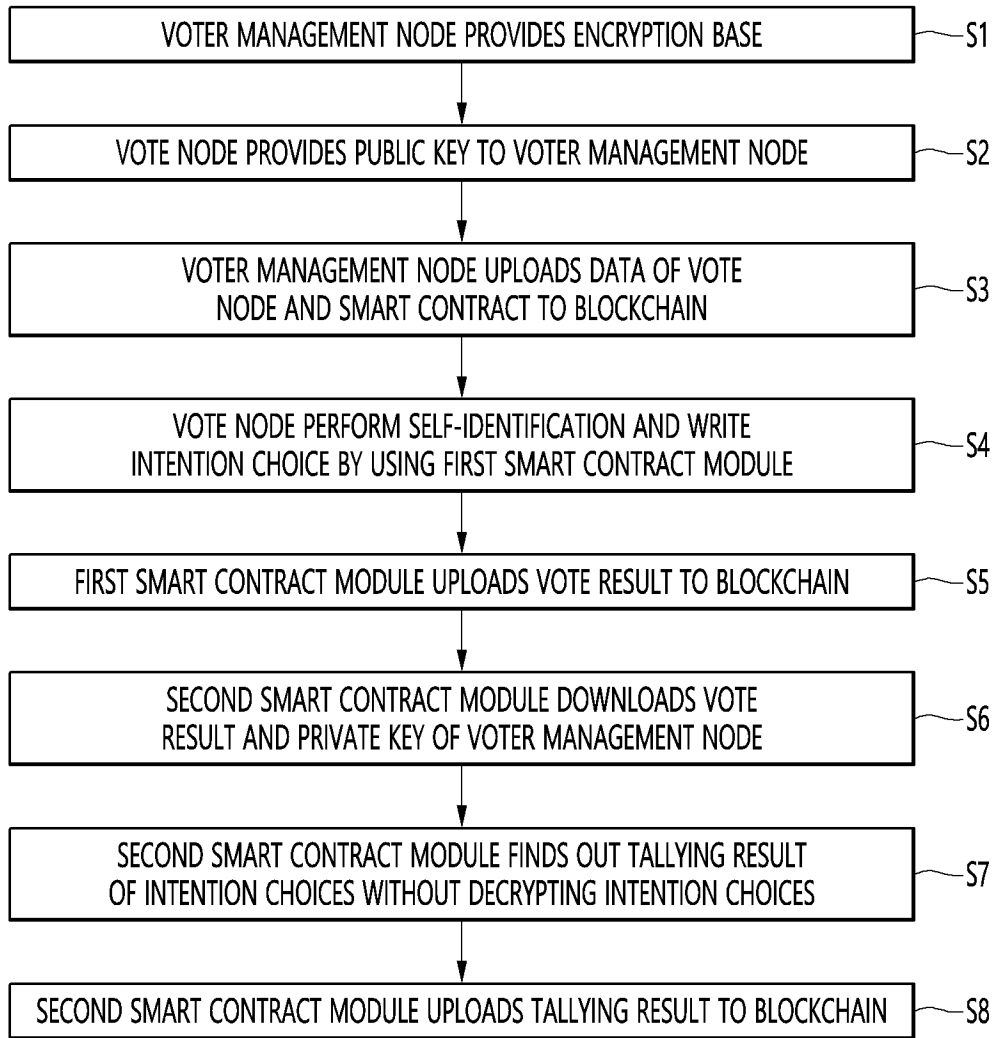
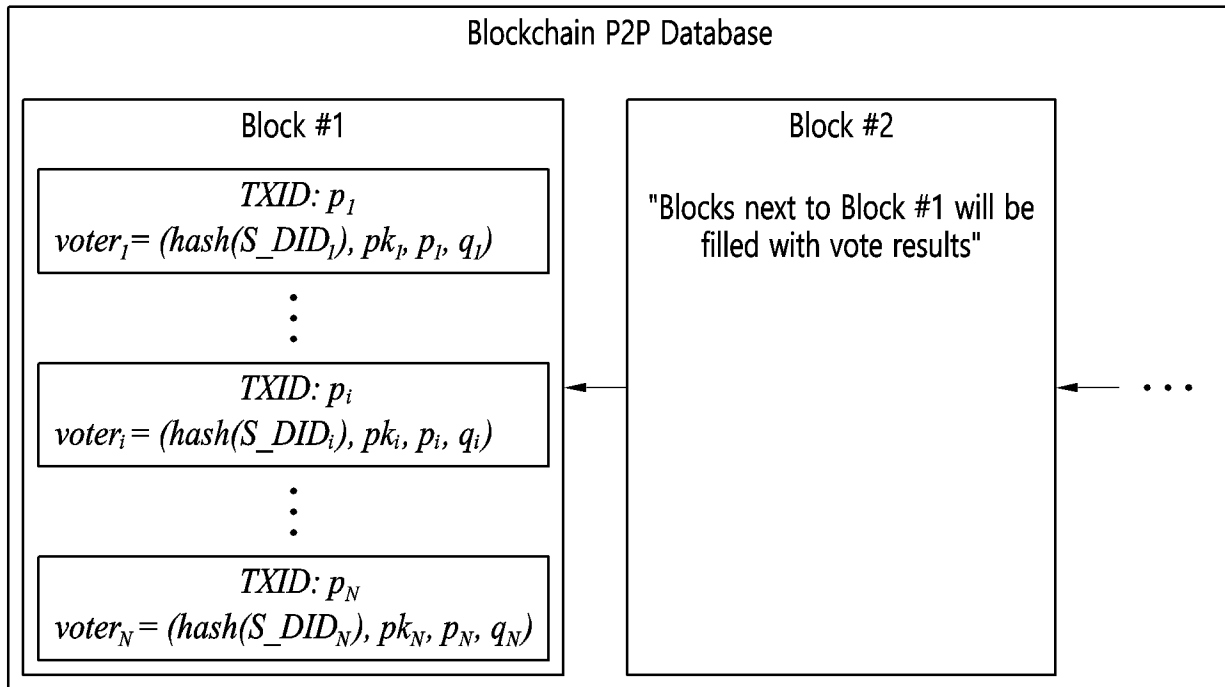


FIG. 3



INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		
	Filing Date		
	First Named Inventor	Jehyuk Jang	
	Art Unit		
	Examiner Name		
	Attorney Docket Number		HANMIR-1074

U.S.PATENTS							Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1						

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS							Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1						

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² i	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	20200008413	KR	A	2020-01-28	UCF HYU		

If you wish to add additional Foreign Patent Document citation information please click the Add button. Add

NON-PATENT LITERATURE DOCUMENTS				Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.		T ⁵

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		
	Filing Date		
	First Named Inventor	Jehyuk Jang	
	Art Unit		
	Examiner Name		
	Attorney Docket Number	HANMIR-1074	

1		YANG ET AL. "Blockchain voting: Publicly verifiable online voting protocol without trusted tallying authorities." Future Generation Computer Systems 112, 859-874 (June 2020)
---	--	--

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number		
Filing Date		
First Named Inventor	Jehyuk Jang	
Art Unit		
Examiner Name		
Attorney Docket Number	HANMIR-1074	

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Heidi Eisenhut/	Date (YYYY-MM-DD)	2021-11-02
Name/Print	Heidi Eisenhut	Registration Number	46812

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	HANMIR-1074
		Application Number	
Title of Invention	BLOCKCHAIN E-VOTING SYSTEM AND OPERATING METHOD THEREOF		
<p>The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76. This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.</p>			

Secrecy Order 37 CFR 5.2:

Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor	1				Remove
Legal Name					
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Jehyuk		Jang		
Residence Information (Select One) US Residency <input type="radio"/> Non US Residency Active US Military Service					
City	Gwangju	Country of Residence ⁱ		KR	
Mailing Address of Inventor:					
Address 1	c/o GWANGJU INSTITUTE OF SCIENCE AND TECHNOLOGY				
Address 2	123 Cheomdan-gwagiro (Oryong-dong) Buk-gu				
City	Gwangju	State/Province			
Postal Code	61005	Country ⁱ	KR		
Inventor	2				Remove
Legal Name					
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Heung-No		Lee		
Residence Information (Select One) US Residency <input checked="" type="radio"/> Non US Residency Active US Military Service					
City	Gwangju	Country of Residence ⁱ		KR	
Mailing Address of Inventor:					
Address 1	c/o GWANGJU INSTITUTE OF SCIENCE AND TECHNOLOGY				
Address 2	123 Cheomdan-gwagiro (Oryong-dong) Buk-gu				
City	Gwangju	State/Province			
Postal Code	61005	Country ⁱ	KR		
All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the Add button.					
					Add

Correspondence Information:

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	HANMIR-1074
	Application Number	
Title of Invention	BLOCKCHAIN E-VOTING SYSTEM AND OPERATING METHOD THEREOF	

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

An Address is being provided for the correspondence information of this application.

Customer Number	71572		
Email Address	heidi-pt@lozaip.com	<input type="button" value="Add Email"/>	<input type="button" value="Remove Email"/>

Application Information:

Title of the Invention	BLOCKCHAIN E-VOTING SYSTEM AND OPERATING METHOD THEREOF		
Attorney Docket Number	HANMIR-1074	Small Entity Status Claimed	<input checked="" type="checkbox"/>
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	3	Suggested Figure for Publication (if any)	

Filing By Reference:

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

Request Early Publication (Fee required at time of Request 37 CFR 1.219)

Request Not to Publish. I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32). Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer number will be used for the Representative Information during processing.

Please Select One:	<input checked="" type="radio"/> Customer Number	<input type="radio"/> US Patent Practitioner	<input type="radio"/> Limited Recognition (37 CFR 11.9)
Customer Number	71572		

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	HANMIR-1074
	Application Number	
Title of Invention	BLOCKCHAIN E-VOTING SYSTEM AND OPERATING METHOD THEREOF	

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.

When referring to the current application, please leave the "Application Number" field blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Claims benefit of provisional	63112723	2020-11-12
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the Add button.			Add

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)ⁱ the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

			Remove
Application Number	Country ⁱ	Filing Date (YYYY-MM-DD)	Access Code ⁱ (if applicable)
10-2020-0146369	KR	2020-11-04	FFB1
			Remove
Application Number	Country ⁱ	Filing Date (YYYY-MM-DD)	Access Code ⁱ (if applicable)
10-2020-0171424	KR	2020-12-09	685B
Additional Foreign Priority Data may be generated within this form by selecting the Add button.			Add

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

<p>This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.</p> <p><input type="checkbox"/> NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.</p>
--

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	HANMIR-1074
	Application Number	
Title of Invention	BLOCKCHAIN E-VOTING SYSTEM AND OPERATING METHOD THEREOF	

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	HANMIR-1074
	Application Number	
Title of Invention	BLOCKCHAIN E-VOTING SYSTEM AND OPERATING METHOD THEREOF	

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant	1	<input type="button" value="Remove"/>
<p>If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.</p>		
<input type="button" value="Clear"/>		
<input checked="" type="radio"/> Assignee	Legal Representative under 35 U.S.C. 117	Joint Inventor
Person to whom the inventor is obligated to assign.		Person who shows sufficient proprietary interest
If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:		
<div style="border: 1px solid black; height: 20px; width: 100%;"></div>		
Name of the Deceased or Legally Incapacitated Inventor: <input style="width: 90%;" type="text"/>		
If the Applicant is an Organization check here. <input checked="" type="checkbox"/>		
Organization Name	GWANGJU INSTITUTE OF SCIENCE AND TECHNOLOGY	
Mailing Address Information For Applicant:		
Address 1	123 (Oryong-dong), Cheomdan-gwagiro, Buk-gu	
Address 2		
City	Gwangju	State/Province
Country	KR	Postal Code
Phone Number		Fax Number
Email Address		
Additional Applicant Data may be generated within this form by selecting the Add button. <input type="button" value="Add"/>		

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	HANMIR-1074
	Application Number	
Title of Invention	BLOCKCHAIN E-VOTING SYSTEM AND OPERATING METHOD THEREOF	

Assignee	1
-----------------	---

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

If the Assignee or Non-Applicant Assignee is an Organization check here.

Prefix	Given Name	Middle Name	Family Name	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1				
Address 2				
City		State/Province		
Country ⁱ		Postal Code		
Phone Number		Fax Number		
Email Address				

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.

Signature:

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). However, if this Application Data Sheet is submitted with the **INITIAL** filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/Heidi Eisenhut/		Date (YYYY-MM-DD)	2021-11-02	
First Name	Heidi	Last Name	Eisenhut	Registration Number	46812

Additional Signature may be generated within this form by selecting the Add button.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	HANMIR-1074
	Application Number	
Title of Invention	BLOCKCHAIN E-VOTING SYSTEM AND OPERATING METHOD THEREOF	

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

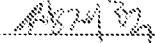
The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN
APPLICATION DATA SHEET (37 CFR 1.76)**

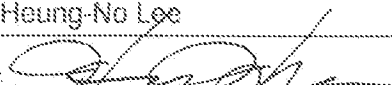
Title of Invention	BLOCKCHAIN E-VOTING SYSTEM AND OPERATING METHOD THEREOF
<p>As the below named inventor, I hereby declare that:</p> <p>This declaration is directed to: <input checked="" type="checkbox"/> The attached application, or <input type="checkbox"/> United States application or PCT international application number _____ filed on _____.</p> <p>The above-identified application was made or authorized to be made by me.</p> <p>I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.</p> <p>I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.</p> <p style="text-align: center;">WARNING:</p> <p>Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identify theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.</p>	
<p>LEGAL NAME OF INVENTOR</p> <p>Inventor: <u>Jehyuk Jang</u> Date (Optional): <u>2021-10-29</u></p> <p>Signature: <u></u></p>	
<p>Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventor entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/D1 form for each additional inventor.</p>	

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN
APPLICATION DATA SHEET (37 CFR 1.76)**

Title of Invention	BLOCKCHAIN E-VOTING SYSTEM AND OPERATING METHOD THEREOF
<p>As the below named inventor, I hereby declare that:</p> <p>This declaration is directed to: <input checked="" type="checkbox"/> The attached application, or <input type="checkbox"/> United States application or PCT international application number _____ filed on _____.</p> <p>The above-identified application was made or authorized to be made by me.</p> <p>I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.</p> <p>I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.</p> <p style="text-align: center;">WARNING:</p> <p>Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identify theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.</p>	
<p>LEGAL NAME OF INVENTOR</p> <p>Inventor: <u>Heung-No Lee</u> Date (Optional): <u>2021-10-29</u></p> <p>Signature: </p>	
<p>Note: An application data sheet (PTO/ISB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.</p>	

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-6198 and select option 2.