PTO-1390 (10-20)
Approved for use through 10/31/2022. OMB 0651-0021
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A SUBMISSION UNDER 35 U.S.C. 371

Attorney Docket No.	
HANMIR-1073	
U.S. Application No. (if known, see 37 CFR 1.5)	

International Application No.	International Filing Date	Priority Date Claimed
PCT/KR2019/017571	12 December 2019	24 May 2019

Title of Invention
TRANSACTION VERIFICATION SYSTEM FOR BLOCKCHAIN, AND TRANSACTION VERIFICATION METHOD FOR BLOCKCHAIN

First Named Inventor
Jehyuk Jang

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information.

1. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). NOTE: The express request under 35 U.S.C. 371(f) will not be effective unless the requirements under 35 U.S.C. 371(c)(1), (2), and (4) for payment of the basic national fee, copy of the International Application and English translation thereof (if required), and the oath or declaration of the inventor(s) have been received.
2. ☒ A copy of the International Application (35 U.S.C. 371(c)(2)) is attached hereto (not required if the International Application was previously communicated by the International Bureau or was filed in the United States Receiving Office (RO/US)).
3. An English language translation of the International Application (35 U.S.C. 371(c)(2))
   a. ☒ is attached hereto.
   b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
4. An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4))
   a. ☒ is attached.
   b. ☐ was previously filed in the international phase under PCT Rule 4.17(iv).

Items 5 to 8 below concern amendments made in the international phase.

PCT Article 19 and 34 amendments

5. ☐ Amendments to the claims under PCT Article 19 are attached (not required if communicated by the International Bureau) (35 U.S.C. 371(c)(3)).
6. ☐ English translation of the PCT Article 19 amendment is attached (35 U.S.C. 371(c)(3)).
7. ☐ English translation of annexes (Article 19 and/or 34 amendments only) of the International Preliminary Examination Report is attached (35 U.S.C. 371(c)(5)).

Cancellation of amendments made in the international phase

8a. ☐ Do not enter the amendment made in the international phase under PCT Article 19.

8b. ☐ Do not enter the amendment made in the international phase under PCT Article 34.

NOTE: A proper amendment made in English under Article 19 or 34 will be entered in the U.S. national phase application absent a clear instruction from applicant not to enter the amendment(s).

The following items 9 to 17 concern a document(s) or information included.

9. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
10. ☐ A preliminary amendment.
11. ☒ An Application Data Sheet under 37 CFR 1.76.
12. ☐ A substitute specification. NOTE: A substitute specification cannot include claims. See 37 CFR 1.125(b).
13. ☒ A power of attorney and/or change of address letter.
14. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13*ter*.3 and 37 CFR 1.821-1.825 (not required if sequence listing in text format was indicated on the PCT Request as part of the International Application and the sequence listing was published as part of the international application).
15. ☐ Assignment papers *(cover sheet and document(s))*. Name of Assignee: _____
16. ☐ 37 CFR 3.73(c) Statement *(when there is an Assignee)*.

U.S. APPLN. No. (if known – see 37 CFR 1.5)	INTERNATIONAL APPLICATION No.	ATTORNEY DOCKET No.
	PCT/KR2019/017571	HANMIR-1073

17. ☐ Other items or information:

The following fees have been submitted.	CALCULATIONS
18. ■ Basic national fee (37 CFR 1.492(a)) **$320**	$ 320.00
19. ■ Examination fee (37 CFR 1.492(c)) • If the written opinion prepared by ISA/US or the international preliminary examination report prepared by IPEA/US indicates all claims satisfy provisions of PCT Article 33(1)-(4)..... **$0** • All other situations **$800**	$ 800.00
20. ■ Search fee (37 CFR 1.492(b)) • If the written opinion prepared by ISA/US or the international preliminary examination report prepared by IPEA/US indicates all claims satisfy provisions of PCT Article 33(1)-(4)..... **$0** • Search fee (37 CFR 1.445(a)(2)) has been paid on the international application to the USPTO as an International Searching Authority ..... **$140** • International Search Report prepared by an ISA other than the US and provided to the Office or previously communicated to the US by the IB..... **$540** • All other situations **$700**	$ 540.00
TOTAL OF 18, 19, and 20 =	$ 1660.00
☐ Additional fee for specification and drawings filed in paper over 100 sheets (excluding sequence listing in compliance with 37 CFR 1.821(c) or (e) in an electronic medium or computer program listing in an electronic medium) (37 CFR 1.492(j)). Fee for each additional 50 sheets of paper or fraction thereof **$420**	$

Total Sheets	Extra Sheets	Number of each additional 50 or fraction thereof (round **up** to a whole number)	RATE
- 100 =	/ 50 =		x **$420**

Surcharge for furnishing any of the search fee, examination fee, or the oath or declaration after the date of commencement of the national stage (37 CFR 1.492(h))..... **$160**	$

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	
Total claims	20 - 20 =	0	x **$100**	$
Independent claims	3 - 3 =	0	x **$480**	$
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			**+ $860**	$

Fee for submission of Sequence Listing text file of 300 MB to 800 MB (37 CFR 1.21(o)(1))..... **$1,060**	$
Fee for submission of Sequence Listing text file of more than 800 MB (37 CFR 1.21(o)(2))..... **$10,500**	$
Processing fee for furnishing the English translation later than 30 months from the earliest claimed priority date (37 CFR 1.492(i))..... **$140 +**	$
TOTAL OF ABOVE CALCULATIONS =	$ 1660.00
■ **Applicant asserts small entity status.** See 37 CFR 1.27. Fees above are reduced by ½.	
☐ **Applicant certifies micro entity status.** See 37 CFR 1.29. Fees above are reduced by ¾. Applicant must attach form PTO/SB/15A or B or equivalent.	
TOTAL NATIONAL FEE =	$ 830.00
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31)..... **$50.00** per property **+**	$
TOTAL FEES ENCLOSED =	$ 830.00

a. ☐ A check in the amount of $_____ to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. _____ in the amount of $_____ to cover the above fees.

c. ☒ The Director is hereby authorized to charge additional fees which may be required, or credit any overpayment, to Deposit Account No. 50-5240 as follows:

i. ☐ any required fee.

ii. ☒ any required fee except for excess claims fees required under 37 CFR 1.492(d) and (e) and multiple dependent claim fee required under 37 CFR 1.492(f).

d. ☒ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038. The PTO-2038 should only be mailed or faxed to the USPTO. However, when paying the basic national fee, the PTO-2038 may NOT be faxed to the USPTO.

ADVISORY: If filing by EFS-Web, do **NOT** attach the PTO-2038 form as a PDF along with your EFS-Web submission. Please be advised that this is **not** recommended and by doing so your **credit card information may be displayed via PAIR**. To protect your information, it is recommended to pay fees online by using the electronic payment method.

NOTE: Where an appropriate time limit under 37 CFR 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the International Application to pending status.

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

☐ 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.

NOTE 1: 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**.

NOTE 2: A U.S. national stage application may not claim priority to the international application of which it is the national phase. The filing date of a U.S. national stage application is the international filing date. See 35 U.S.C. 363.

Correspondence Address

☒ The address associated with Customer Number: 71572 **OR** ☐ Correspondence address below

Name					
Address					
City		State		Zip Code	
Country		Telephone			
Email					

Signature	/Heidi Eisenhut/	Date	11/15/2021
Name (Print/Type)	Heidi Eisenhut	Registration No. (Attorney/Agent)	46812

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 disclosure of these records is required by the Freedom of Information Act.
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 inspection 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.

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	HANMIR-1073
	Application Number	
Title of Invention	TRANSACTION VERIFICATION SYSTEM FOR BLOCKCHAIN, AND TRANSACTION VERIFICATION METHOD FOR BLOCKCHAIN	

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.

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
	Je Hyuk		Jang	

Residence Information (Select One) US Residency ● Non US Residency Active US Military Service

City	Gwangju	Country of Residence [i]	KR

Mailing Address of Inventor:

Address 1	123 Cheomdan-gwagiro (Oryong-dong) Buk-gu
Address 2	

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 ◉ Non US Residency Active US Military Service

City	Gwangju	Country of Residence [i]	KR

Mailing Address of Inventor:

Address 1	123 Cheomdan-gwagiro (Oryong-dong) Buk-gu
Address 2	

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:

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	HANMIR-1073
	Application Number	
Title of Invention	TRANSACTION VERIFICATION SYSTEM FOR BLOCKCHAIN, AND TRANSACTION VERIFICATION METHOD FOR BLOCKCHAIN	

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-pto@lozaip.com	Add Email	Remove Email

Application Information:

Title of the Invention	TRANSACTION VERIFICATION SYSTEM FOR BLOCKCHAIN, AND TRANSACTION VERIFICATION METHOD FOR BLOCKCHAIN		
Attorney Docket Number	HANMIR-1073	**Small Entity Status Claimed**	☒
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:	● Customer Number	US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	71572		

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	HANMIR-1073
	Application Number	
Title of Invention	TRANSACTION VERIFICATION SYSTEM FOR BLOCKCHAIN, AND TRANSACTION VERIFICATION METHOD FOR BLOCKCHAIN	

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)
	a 371 of international	PCT/KR2019/017571	2019-12-12

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)
10-2019-0061493	KR	2019-05-24	

Remove

Application Number	Country[i]	Filing Date (YYYY-MM-DD)	Access Code[i] (if applicable)
10-2019-0120655	KR	2019-09-30	

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

☐ 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.
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.

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	HANMIR-1073
	Application Number	
Title of Invention	TRANSACTION VERIFICATION SYSTEM FOR BLOCKCHAIN, AND TRANSACTION VERIFICATION METHOD FOR BLOCKCHAIN	

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.

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	HANMIR-1073
	Application Number	
Title of Invention	TRANSACTION VERIFICATION SYSTEM FOR BLOCKCHAIN, AND TRANSACTION VERIFICATION METHOD FOR BLOCKCHAIN	

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 — Remove

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.

Clear

● 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:

Name of the Deceased or Legally Incapacitated Inventor:

If the Applicant is an Organization check here. ☒

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	61005
Phone Number		Fax Number	
Email Address			

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

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	HANMIR-1073
	Application Number	
Title of Invention	TRANSACTION VERIFICATION SYSTEM FOR BLOCKCHAIN, AND TRANSACTION VERIFICATION METHOD FOR BLOCKCHAIN	

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.

Remove

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. Add

Signature:

Remove

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)	2021-11-15
First Name	Heidi	Last Name	Eisenhut	Registration Number	46812

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

PTO/AIA/14 (02-18)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	HANMIR-1073
	Application Number	
Title of Invention	TRANSACTION VERIFICATION SYSTEM FOR BLOCKCHAIN, AND TRANSACTION VERIFICATION METHOD FOR BLOCKCHAIN	

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 CooperationTreaty.

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.

PTO/AIA/01 (06-12)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

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

Title of Invention	TRANSACTION VERIFICATION SYSTEM FOR BLOCKCHAIN, AND TRANSACTION VERIFICATION METHOD FOR BLOCKCHAIN

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [x] The attached application, or
- [ ] United States application or PCT international application number _____

filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

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.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity 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.

LEGAL NAME OF INVENTOR

Inventor: Heung-No Lee Date (Optional): Oct. 15th, 2021

Signature: _____

Note: An application data sheet (PTO/SB/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.

PTO/AIA/01 (08-12)
Approved for use through 11/30/2020. OMB 0651-0032
U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

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

Title of Invention	TRANSACTION VERIFICATION SYSTEM FOR BLOCKCHAIN, AND TRANSACTION VERIFICATION METHOD FOR BLOCKCHAIN

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [x] The attached application, or
- [ ] United States application or PCT international application number _____

filed on _____.

The above-identified application was made or authorized to be made by me

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

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.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity 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.

LEGAL NAME OF INVENTOR

Inventor: Jehyuk Jang Date (Optional): Oct. 15th, 2021

Signature: [signature]

Note: An application data sheet (PTO/SB/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.

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:

PCT Application No. PCT/KR2019/017571 (December 12, 2019)

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

Signature_____
Kimoon Kim , Hanmir Patent & Law Firm

Date_____ October 14, 2021 _____

【DESCRIPTION】

【TITLE OF THE INVENTION】

TRANSACTION VERIFICATION SYSTEM FOR BLOCKCHAIN, AND TRANSACTION VERIFICATION METHOD FOR BLOCKCHAIN

【TECHNICAL FIELD】

[1] The present invention relates to a blockchain transaction confirmation system and a blockchain transaction confirmation method.

【BACKGROUND ART】

[2] Recently, cryptocurrency has reached the stage of performing the function of real-world currency in commercial transaction. The transaction through the cryptocurrency is finalized through block confirmation. The block confirmation is a technology that finalizes transactions after confirming that blocks corresponding to the pre-set block confirmation number are generated after the transaction in progress between traders has occurred. For example, when the block confirmation number is 6, the transaction is finalized after waiting for the generation of six additional blocks after the block in which the transaction between traders is recorded. The transaction finalization may exemplify that a person having a product sends the product to a cryptocurrency provider.

[3] Non-Patent Literature 1 proves that as the block confirmation number increases, the transaction is safer.

[4] The block confirmation may be utilized as a means for defending against double spending. The double spending refers to an attack action in which a malicious user cancels a true transaction by secretly providing a malicious blockchain longer than a blockchain of the true transaction by using the principle of the blockchain in which the longest blockchain survives.

[5] As the block confirmation number increases, the probability of being double-spent decreases. However, as the block confirmation number increases, it takes a longer time to finalize the transaction. For example, in the case of Bitcoin, an average block generation cycle is 10 minutes. Therefore, when the block confirmation number is 6, the transaction finalization time is 60 minutes. This means that a user needs to wait 60 minutes to buy a bottle of Coke. These problems are becoming a big obstacle to the practial use of cryptocurrencies in real-world.

[6] Under this background, in current transactions using cryptocurrency, it is common for traders to determine the block confirmation number at their own risk by referring to guidelines given for each transaction amount. However, traders are not sure how many block confirmations they need for their transactions, since the double attack success probability never becomes zero no matter how many confirmations have been performed.

[7] Citation List: (Non-Patent Literature 1) S Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" [Online] Available: https://bitcoinorg/bitcoinpdf

【DISCLOSURE OF INVENTION】

【Technical Problem】

[8] The present disclosure proposes a blockchain transaction confirmation system and a blockchain transaction confirmation method, which propose an appropriate block confirmation number for given real-time conditions.

[9] The present disclosure proposes a blockchain transaction confirmation system and a blockchain transaction confirmation method, which are capable of safely and quickly completing a transaction through cryptocurrency in response to various external environments as well as a transaction amount inputted by a trader.

[10] The present disclosure proposes a blockchain transaction confirmation system and a blockchain transaction confirmation method, which are capable of achieving both the secure transaction and the quick transaction finalization through cryptocurrency.

【TECHNICAL SOLUTION】

[11] A blockchain transaction confirmation system according to the present disclosure includes: a user information input interface to which user information is inputted; an external information input interface to which external information related to a cryptocurrency system is inputted; an appropriate confirmation number searcher configured to search for a block confirmation number appropriate for confirmation of a transaction in progress of creation by using the external information and the user information; and an appropriate confirmation number output interface configured to output the block confirmation number. According to the present disclosure, a user can automatically find out the block confirmation number required for safe and quick transaction.

[12] The user information may include at least an input transaction amount inputted by a user. Therefore, safe transaction can be quickly performed in response to the input transaction amount inputted by the user.

[13] The external information may include at least one of a reward paid for generating a block at the time, an average cost required for generating a block at the time, or an average rate per time of block generation at the time. It is possible to find out a more accurate block confirmation number by understanding the attack tendency of an attacker using a cryptocurrency system. Furthermore, it is possible to find out the optimal safe transaction limit amount for a given type of cryptocurrency system.

[14] The external information may include all of a reward paid

for generating a block at the time, an average cost required for generating a block at the time, and an average rate per time of block generation at the time. Therefore, a more accurate block confirmation number may be found.

[15] The appropriate confirmation number searcher may include: a safe transaction limit amount extractor configured to extract a safe transaction limit amount at the time by using the external information; and a safety determiner configured to determine safety by comparing the safe transaction limit amount with the input transaction amount. Therefore, it is possible to find out a safe amount that changes in real time by considering the external information. Furthermore, it is possible to find out the optimal safe transaction limit amount for a given type of cryptocurrency system.

[16] The safe transaction limit amount extractor may include a calculator configured to extract, as the safe transaction limit amount, an amount that makes an attacker's expected return to be zero. Therefore, since it is based on the attacker's benefit, and the attacker's attack tendency can be predicted, it is possible to find out the block confirmation number more accurately.

[17] The attacker's expected return may be provided by subtracting an attacker's expected cost from the attacker's expected profit.

[18] The safe transaction limit amount (C_{Req}) may be extracted by $C_{Req.}=(1-P_{AS})/P_{AS}*X(\gamma,t_{cut})+X(\gamma,T_{AS})-R(\beta,T_{AS})$.

[19] The safe transaction limit amount extractor may include a parameter optimizer, and the parameter optimizer may be configured to optimally estimate at least one of an attacker's cut time or an attacker's resource proportion. Therefore, it is possible to optimally predict the attacker's selection parameters, thereby suggesting a safer block confirmation number.

[20] When the safety determiner determines that it is not safe, a

process of increasing the block confirmation number to extract the safe transaction limit amount again may be repeated. Therefore, the user can find out the most secure and least block confirmation number.

[21] A blockchain transaction confirmation method according to the present disclosure includes: receiving external information that is information about a cryptocurrency system and user information that is inputted by a user; searching for an appropriate confirmation number, which is appropriate for safe and quick transaction; and outputting the appropriate confirmation number. The user can safely and quickly perform transactions through the blockchain.

[22] The searching for the appropriate confirmation number may include: calculating a safe transaction limit amount, which is a safe transaction amount at the time, by using the external information and a block confirmation number; comparing the safe transaction limit amount with the input transaction amount inputted as the user information; and comparing the safe transaction limit amount with the input transaction amount, and if the safe transaction limit amount is greater than the input transaction amount, determining that it is safe and outputting the appropriate block confirmation number. Therefore, the user can find out the safe block confirmation number, or can actually apply the block confirmation number, so that safe transactions can be created.

[23] The blockchain transaction confirmation method may further include comparing the safe transaction limit amount with the input transaction amount, and if the safe transaction limit amount is less than the input transaction amount, determining that it is not safe, increasing the block confirmation number, and calculating the safe transaction limit amount again. Such iterative

calculations enable a user to find out the theoretically safest and minimum block confirmation number.

【ADVANTAGEOUS EFFECTS】

[24] According to the present disclosure, the trader can know the appropriate block confirmation number by inputting only the transaction amount. The term "appropriate" means that the two purposes of the safe transaction and the quick transaction can be achieved at the same time. The meaning of the term "appropriate" in this specification can be understood as above.

[25] According to the present disclosure, it is possible to suggest an appropriate block confirmation number by considering not only the transaction in progress between the parties, but also the environment information (also referred to as external information) of the entire cryptocurrency system that is placed outside the transaction between the parties. Therefore, it is possible to predict the choice of the attacker and suggest the block confirmation number more accurately.

[26] Effects of the invention from the other detailed configurations will be presented in more detail in BEST MODE FOR CARRYING OUT THE INVENTION.

【BRIEF DESCRIPTION OF DRAWINGS】

[27] Fig. 1 is a view showing a blockchain transaction confirmation system according to an embodiment.

[28] Fig. 2 is a view showing an appropriate confirmation number searcher in detail.

[29] Fig. 3 is a flowchart showing a part of a blockchain transaction confirmation method, describing the detailed operation of the appropriate confirmation number searcher.

[30] Fig. 4 is a view showing a detailed configuration of a safe transaction limit amount extractor.

[31] Fig. 5 is an exemplary graph of a safe transaction limit amount with a resource proportion p_A occupied by an attacker as a variable.

[32] Fig. 6 is an exemplary graph of an average time ($E_{T_{AS-ICT}}(p_A;N_{BC})$) required for attack success when a cut time is infinite with a resource proportion p_A occupied by an attacker as a variable.

[33] Fig. 7 is an exemplary graph of a safe transaction limit amount with a cut time as a variable.

【BEST MODE FOR CARRYING OUT THE INVENTION】

[34] Hereinafter, specific embodiments of the invention will be described in detail with reference to the accompanying drawings. The present disclosure of invention is not limited to the embodiments presented below, and those skilled in the art who understand the invention will be able to easily propose other embodiments falling within the scope of the same invention by adding, modifying, and deleting elements. However, they also fall within the present disclosure.

[35] Fig. 1 is a view showing a blockchain transaction confirmation system according to an embodiment.

[36] Referring to Fig. 1, the blockchain transaction confirmation system includes an appropriate confirmation number searcher 1 that searches for the confirmation number required for transaction confirmation, a user information input interface 2 that receives information inputted by a user of a system and outputs the received information to the appropriate confirmation number searcher 1, and an external information input interface 3 that receives environment information of a cryptocurrency system, that is, external information, and outputs the received environment information to the appropriate confirmation number searcher 1. The appropriate confirmation number searcher 1 may search for an appropriate block confirmation number and output the appropriate

block confirmation number to an appropriate confirmation number output interface 4.

[37] The user information input interface 2 may be an input means such as a computer having a display and an input device. The external information input interface 3 may be a communication means connected to a network and a computer that reads and stores public information on the network. The appropriate confirmation number output interface 4 may be an output means such as a computer having a display or a communication means. The appropriate confirmation number searcher 1 may be a computer having an arithmetic unit and a predetermined memory.

[38] The external information may include a reward paid for generating a block at the time, an average cost required for generating a block at the time, and an average rate per time of block generation at the time.

[39] The user information may include information about a transaction amount inputted by the user for a transaction in progress of creation.

[40] The user of the system can be said to be a trader.

[41] In the blockchain transaction confirmation system of the embodiment, the appropriate confirmation number searcher 1 searches for an appropriate block confirmation number by using the information about the transaction amount inputted from the user information input interface 2 and the external information inputted from the external information input interface 3. The found information may be outputted through the appropriate confirmation number output interface 4.

[42] The user can set the block confirmation number by himself or herself by using the appropriate block confirmation number outputted from the appropriate confirmation number output interface 4. Depending on the block confirmation number, the

transaction can be finalized after the block confirmations are performed.

[43] Without setting the block confirmation number by the user, the block confirmation number outputted from the appropriate confirmation number output interface 4 may be automatically applied and the blockchain transaction confirmation system may be operated.

[44] The blockchain transaction confirmation system presented in Fig. 1 may be mounted on a terminal of a trader.

[45] A unit block presented in Fig. 1 is provided to the terminal of the trader, and another unit block is provided to at least one of the terminal of the counterpart trader or a cryptocurrency exchange, so that the blockchain transaction confirmation system may be operated in a state of being connected through the network.

[46] Although not shown in Fig. 1, of course, it can be understood that the blockchain transaction confirmation system includes a network node where any other user of the cryptocurrency system chains blocks through block generation. That is, the terminal of at least one other node on the network cooperates and chains as many blocks as the block confirmation number required to finalize the transaction in progress by performing transaction confirmation.

[47] The blockchain transaction confirmation method according to the embodiment may search for the appropriate confirmation number after receiving the external information and the user information. Thereafter, it can be performed by outputting the found appropriate confirmation number.

[48] The output of the appropriate confirmation number searcher may be fulfilled by a user inputting a block confirmation number after the appropriate block confirmation number is outputted to the user. Alternatively, block confirmation may be automatically performed according to the appropriate block confirmation number.

[49] Fig. 2 is a view showing the appropriate confirmation number searcher in detail.

[50] Referring to Fig. 2, the appropriate confirmation number searcher 1 may include a safe transaction limit amount extractor 10 that extracts a safe level of transaction amount at the time, a safety determiner 12 that determines the safety of a transaction by comparing the safe transaction limit amount extracted by the safe transaction limit amount extractor 10 with a transaction amount inputted by a user, and a memory 11 that stores information necessary for the operation of the safety determiner 12 and the safe transaction limit amount extractor 10.

[51] Fig. 3 is a flowchart showing a part of the blockchain transaction confirmation method, describing the detailed operation of the appropriate confirmation number searcher.

[52] Referring to Figs. 2 and 3, the external information and the user information are inputted (S1). The external information may include a reward paid for generation of a block at the time, an average cost required for generating a block at the time, and an average rate per time of block generation at the time. The user information may include transaction amount information inputted by the user. The transaction amount may be information about the amount of currency or cryptocurrency used in each country. For example, a KRW amount or BTC amount may be included as the information.

[53] The safe transaction limit amount is calculated by using the input information (S2). The safe transaction limit amount may be calculated by comparing the cost and profit of the attacker predicted by the external information. The calculation of the safe transaction limit amount will be described in more detail later.

[54] It is determined whether the transaction in progress is safe

by comparing the safe transaction limit amount calculated in the safe transaction limit amount calculation operation (S2) with the input transaction amount inputted as the user information (S3).

[55] In the safety determination operation (S3), the input transaction amount and the safe transaction limit amount are compared with each other, and if the input transaction amount is smaller, the transaction is determined as safe and the current confirmation number is outputted (S4).

[56] Conversely, in the safety determination operation S3, if the input transaction amount is greater, the transaction is determined as not safe, and the confirmation number is increased (S5), and the safe transaction limit amount calculation operation (S2) is performed again. For example, when the current confirmation number is 1, the confirmation number may be increased to 2. Thereafter, the confirmation number becomes 2 and the safe transaction limit amount may be recalculated by using the user information and the real-time external information.

[57] In the safety transaction limit amount calculation operation (S2) performed again, since the confirmation number is increased, it may be expected that the safety transaction limit amount will increase.

[58] The safe transaction limit amount calculation operation (S2) and the operation of the safe transaction limit amount extractor 10 will be described in detail below.

[59] The safe transaction limit amount may be calculated by comparing the cost required for the attacker to perform a double spending attack (in this specification, when referred to as an attack, it means a double spending attack unless otherwise specified) with a profit obtained when the attacker succeeds in the double spending attack.

[60] For example, this is because, when the profit obtained by

the attacker when the attack is successful is smaller than the cost of the attack, the attacker will not try an attack, or even when the attacker pushes an attack, it will not be successful.

[61] In other words, if there exists an expected return of an attacker by 'attacker's expected return = attacker's expected profit - attacker's expected cost', it can be expected that the attacker will attack, and conversely, if there is no expected return of the attacker, it can be expected that the attacker will not attack. The transaction amount in a state in which the expected return of the attacker becomes zero may be defined as the safe transaction limit amount.

[62] The expected profit of the attacker may be given as the sum of the return (C+R) when the attack is successful and the return (zero) when the attack fails. For simplicity, it can be written as $P_{AS}*(C+R(\beta,T_{AS}))$.

[63] The expected cost of the attacker may be given as the sum of the cost for certain time duration (T_{AS}) when the attack is successful and the cost for the cut time (t_{cut}) when the attack fails. Briefly, it can be given as $P_{AS}*X(\gamma,E[T_{AS}])+(1-P_{AS})*X(\gamma,t_{cut})$. The cut time may refer to the time to stop the attack after taking a certain amount of loss so as to prevent a larger loss with estimating that the probability of success in the attack is slim after the cut time has elapsed.

[64] Consequently, the expected return of the attacker may be calculated as $P_{AS}*(C+R(\beta,E[T_{AS}])-X(\gamma,E[T_{AS}]))-(1-P_{AS})*X(\gamma,t_{cut})$.

[65] The safe transaction limit amount (C_{Req}) may be defined as a transaction amount at which the expected return of the attacker becomes zero. Therefore, when the transaction amount (C) is rearranged on the left-hand side of the equation and the remaining terms are rearranged on the right-hand side of the equation while keeping the expected return of the attacker equals zero, one can

obtain $C_{Req.}=(1-P_{AS})/P_{AS}*X(\gamma,t_{cut})+X(\gamma,T_{AS})-R(\beta,T_{AS})$.

[66] Table 1 summarizes the meanings of each symbol presented in the above description and various symbols used in the actual calculation of the safe transaction limit amount below.

[67] [Table 1]

Symbol (unit)	Description	Remarks
C($, BTC)	Transaction amount of a transaction targeted by a double-spending attack	User input value
β($, BTC)	Reward paid for generating a block	External input value
γ($, BTC)	Average cost required for generating a block	External input value
λ_A(No./T)	Attacker's average block generation rate per time (the best of the different and known may be used depending on the attacker) (the attacker may join a pool, perform block generation, and perform collusion between pools)	External input value
λ_H(No./T)	Honest nodes' average block generation rate per time	External input value
λ_T(No./T)	The total rate of block generation per time	External input value
t_{cut}(T)	Attack cut-time to prevent loss from growing indefinitely	Estimated confirmation value
p_A(%)	Percentage of computational resources occupied by attacker	Estimated confirmatio

		n value
N_{BC}(No.)	Block confirmation number a trader confirms block generations before finalizing a transaction	Output value
$E[T_{AS}](T)$	Average time taken until a double spending attack is successful, less than t_{cut}.	Calculated value
P_{AS}(dimensionless)	Probability that a double spending attack will be successful within t_{cut}	Calculated value
R(β,t)($, BTC)	Average reward of an attacker when generating blocks for time t (function that increases by β and t)	Calculated value
X(γ,t)($, BTC)	Average cost of an attacker when generating blocks for time t (function that increases by γ and t)	Calculated value

[68] The remarks column indicates the source of the values of each symbol.

[69] User input value is user information inputted by the user and means a transaction amount herein.

[70] External input value is a value that is posted in the system of each cryptocurrency and changes in real time. For example, the external input value is posted on btc.com in the case of Bitcoin and in etherscan.io in the case of Ethereum.

[71] The estimated confirmation value is a value that is selectable by an attacker and may be selected as the safest value while calculating the safe transaction limit amount. The estimated confirmation value may be optimally estimated by a parameter

optimizer 16, which will be described later.

[72] The output value is a value that is outputted for one purpose in this embodiment, and represents the block confirmation number as a safe confirmation number.

[73] The calculated value is a value that is used in the middle of the calculation of the safe transaction limit amount.

[74] The process of calculating the safe transaction limit amount and the configuration of the safe transaction limit amount detector 10 that detects the safe transaction limit amount at the time will be described in more detail.

[75] Fig. 4 is a view showing a detailed configuration of the safe transaction limit amount extractor.

[76] Referring to Fig. 4, the safe transaction limit amount extractor 10 includes a calculator 15 that calculates the safe transaction limit amount, and a parameter optimizer 16 that optimizes the parameters required for executing the calculator 15.

[77] The parameter optimizer 16 is a block for optimizing the estimated confirmation value, and is a value capable of predicting an attack from an attacker's point of view.

[78] The detailed operation of the safe transaction limit amount extractor 10 will be described in detail with a number of equations. In the following description, it can be understood that all parts that are not referring to the parameter optimizer 16 are performed by the operation interface 15.

[79] Equation 1 below exemplifies converting the unit of the average block generation cost from cost per time into cost per block.

[80] [Equation 1]

$$\gamma = 4.63 \cdot 10^{-22}\ [\text{BTC/hash}]$$
$$\times 456\text{E}[\text{hashes/block mining}]$$
$$\approx 0.21\ [\text{BTC/block mining}].$$

[81] Referring to Equation 1, the block generation cost per block may be obtained by multiplying the number of hashes/block by the block generation cost/hashes known as the external information. The result of Equation 1 may be stored in a memory.

[82] Equation 2 below exemplifies finding out the attacker's block generation rate per time.

[83] [Equation 2]

$$p_A := \Pr(S_i = n+1 \mid S_{i-1} = n) = \frac{\lambda_A}{\lambda_T},$$

$$p_H := \Pr(S_i = n-1 \mid S_{i-1} = n) = \frac{\lambda_H}{\lambda_T},$$

[84] In Equation 2, λ stands for speed, H (honest) stands for honest nodes, T (Total) stands for total, A (attacker) stands for the attacker, p_A is the proportion of resources the attacker has, and p_H is the proportion of resources the honest nodes have. The lowercase p in p_H can be understood as an acronym for proportion.

[85] It is possible to find out the attacker's block generation rate per time (λ_T) through Equation 2 above. The result of Equation 2 may be stored in the memory 11. The memory 11 may store

information necessary for calculation as well as the block generation cost and the block generation rate per time.

[86] Equation 3 below is the probability of successful attack when the attack is made with the infinite cut time, and is disclosed in the paper of Satoshi Nakamoto cited in Non-Patent Literature.

[87] [Equation 3]

$$\mathbb{P}_{AS-ICT}(p_A;N_{BC})=\begin{cases}1, & p_H \le p_A,\\ 1-{p_A}^{N_{BC}+1}{p_H}^{N_{BC}}\sum_{j=N_{BC}}^{2N_{BC}}\binom{j-1}{N_{BC}-1}A_j, & p_H > p_A,\end{cases}$$

where

$$A_j \triangleq {p_A}^{j-2N_{BC}-1}-{p_H}^{j-2N_{BC}-1}.$$

[88] In Equation 3, P represents probability, AS stands for attack success, ICT stands for the infinite cut time meaning that the cut time is infinite, and N_{BC} represents the block confirmation number for confirmations.

[89] Equation 4 below is an equation derived by Equation 3, and represents a probability distribution regarding the probability of successful attack within a given time.

[90] [Equation 4]

$$f_{T^{(1),(2)}}(t)=\frac{p_A\lambda_T e^{-\lambda_T t}\left(p_A p_H(\lambda_T t)^2\right)^{N_{BC}}}{(2N_{BC})!}$$
$$\cdot\sum_{j=N_{BC}}^{j=2N_{BC}}\binom{j-1}{N_{BC}-1}\,{}_2F_3\left(\mathbf{a};\mathbf{b};p_A p_H(\lambda_T t)^2\right)$$
$$+\frac{e^{-\lambda_T t}\left(p_H\lambda_T t\right)^{N_{BC}}}{t\quad(N_{BC}-1)!}\left(e^{p_A\lambda_T t}-\sum_{i=0}^{N_{BC}}\frac{(p_A\lambda_T t)^i}{i!}\right)$$
$$+(1-\mathbb{P}_{AS-ICT})\delta(t-\infty),$$

[91] In Equation 4, ${}_pF_q$ is a generalized hypergeometric function defined in [G Gasper and M Rahman, "Basic Hypergeometric series, " in Basic hypergeometric series, Second, vol 96, Cambridge University Press, Cambridge, 2004], and a and b are defined in Equation 5.

[92] [Equation 5]

$$\mathbf{a}=\begin{bmatrix} N_{BC}+1-j/2 \\ N_{BC}+1/2-j/2 \end{bmatrix}$$

$$\mathbf{b}=\begin{bmatrix} 2N_{BC}+2-j \\ N_{BC}+1 \\ N_{BC}+1/2 \end{bmatrix}.$$

[93] By taking the first integration on the probability distribution of Equation 4, it is possible to find out the probability of successful attack within the cut time of Equation 6 below.

[94] [Equation 6]

$$\mathbb{P}_{AS}\left(p_A, t_{cut}; N_{BC}\right) := \Pr\left(T^{(1),(2)} < t_{cut}\right)$$

[95] By taking the second integration on the probability distribution of Equation 5, it is possible to find out the average time required to succeed in the attack within the cut time of Equation 7 below.

[96] [Equation 7]

$$\mathbb{E}_{T_{AS}}\left(p_A, t_{cut}; N_{BC}\right) = \frac{\int_0^{t_{cut}} t f_{T^{(1),(2)}}(t)\,dt}{\mathbb{P}_{AS}\left(p_A, t_{cut}; N_{BC}\right)}$$

[97] E is the expectation, P is the probability, and f is the probability distribution in probability theory.

[98] Using Equations 6 and 7, the average attack cost of the attacker can be found as Equation 8.

[99] [Equation 8]

$$\mathbb{E}_X\left(p_A, t_{cut}; N_{BC}\right) := \mathbb{P}_{AS}\left(p_A, t_{cut}; N_{BC}\right)\mathbb{E}\left[X\left(\lambda_A, T_{AS}\right)\right] + \left(1-\mathbb{P}_{AS}\left(p_A, t_{cut}; N_{BC}\right)\right)X\left(\lambda_A, t_{cut}\right)$$

[100] X represents the block generation cost. The provision of the block generation cost X as a linear function illustrates the cost of renting block generating equipment through a rental agency on the Internet (e.g., nicehach.com) as a linear function. In response to various cases, such as a case in which the block generation cost is not a rental cost but an electricity usage fee for equipment, the cost function X is an n-square function, an n-root function, a logarithmic function, an exponential function, or an n-root function.

[101] On the other hand, using Equation 3, the average time ($\mathbb{E}_{T_{AS-ICT}}(p_A; N_{BC})$) required for attack success when the cut time is infinite can be found as Equation 9.

[102] [Equation 9]

$$\mathbb{E}_{T_{AS-ICT}}(p_A;N_{BC})=\frac{\lambda_T^{-1}\left(\sum_{j=N_{BC}}^{2N_{BC}}\binom{j-1}{N_{BC}-1}Z_j+\frac{N_{BC}}{p_H}\right)}{\mathbb{P}_{AS-ICT}(p_A;N_{BC})}$$

where

$$Z_j := p_A {p_m}^{N_{BC}} {p_M}^{-(N_{BC}-j+1)}\left(\frac{2N_{BC}-2jp_m+1}{p_M-p_m}\right) - jp_A{}^{-(N_{BC}-j)}{p_H}^{N_{BC}}.$$

[103] Using Equation 9, it is possible to find out the resource proportion p_A occupied by the attacker, which predicts the resource occupied by the attacker and presents the most stable confirmation amount.

[104] Specifically, referring to Equation 9 above, if the cut time is infinite, the average time ($\mathbb{E}_{T_{AS-ICT}}(p_A;N_{BC})$) required for attack success is a function using the resource proportion p_A occupied by the attacker as a variable. In this case, when the average time ($\mathbb{E}_{T_{AS-ICT}}(p_A;N_{BC})$) required for attack success is calculated when the cut time is infinite using the resource proportion p_A occupied by the attacker as a variable, the average time ($\mathbb{E}_{T_{AS-ICT}}(p_A;N_{BC})$) appears as a downwardly convex function as shown in Fig. 6.

[105] Therefore, on the graph of Fig. 6, by taking the resource proportion p_A occupied by the lowest attacker, it is possible to most stably optimize the resource proportion occupied by the attacker. This is because the attacker will select the occupied resource proportion that can obtain the effect of quick attack at

the lowest cost.

[106] In this case, the optimization of the resource proportion occupied by the attacker may be performed by the parameter optimizer 16 through a separate operation from the operation interface 15. The resource proportion occupied by the attacker, which is optimized in the parameter optimizer 16, is fed back to the operation interface 15 and may be used to obtain the safe transaction limit amount.

[107] Thereafter, the following Equation 10 is applied to obtain the safe transaction limit amount.

[108] [Equation 10]

$$C_{\text{Req.}} = \frac{\mathbb{E}_X\left(p_A, t_{cut}; N_{BC}\right)}{\mathbb{P}_{AS}\left(p_A, t_{cut}; N_{BC}\right)} - \mathbb{E}\left[R\left(\lambda_A, T_{AS}\right)\right]$$

[109] In Equation 10, R is the reward, and R may be given as in Equation 11 below.

[110] [Equation 11]

$$R\left(\lambda_A, t\right) := \beta\lambda_A t\left(\log_{r_1} r_2\right)^{\lambda_A}\left(\log_{r_3} r_4\right)^{t}$$

[111] In Equation 11, the logarithm factor indicates that the reward can be a log function or an exponential function with respect to time. However, when given as a function linear to time, all logarithm factors may be given as 1.

[112] However, similarly to the block generation cost (X), the reward R may also be an n-square function, an n-root function, a log function, an exponential function, or an n-root function.

[113] Referring back to Equation 10, the cut time t_{cut} is still unknown, and Equation 10 can be given as a function using the cut time as a variable. Therefore, it is possible to find the value of the cut time that optimizes the safe transaction limit amount

C_{req}.

[114] Fig. 7 is a graph showing the safe transaction limit amount with respect to the cut time as a variable.

[115] Referring to Fig. 7, the safe transaction limit amount with respect to the cut time is shown as a downwardly convex graph. As the safest transaction limit amount, the minimum confirmation amount may be outputted. The operation of obtaining the optimum value of the safe transaction limit amount with respect to the cut time may be performed by the parameter optimizer 16.

[116] The parameter optimizer 16 may output the minimum safe transaction limit amount to the operation interface 15.

[117] On the other hand, the above description can be applied if the resource proportion of the attacker is 50% or less.

[118] In contrast, if the resource proportion of the attacker is greater than 50%, the attacker may set the cut time to infinity, as described above. This is because, if the resource proportion is greater than 50%, it is guaranteed that the attacker will make a longer blockchain one day, and therefore the attack will ever succeed one day.

[119] We will describe the details how to optimize the cut time (t_{cut}) of the attacker and the resource proportion p_A of the attacker, which should be estimated, for each of two cases where the resource proportion of the attacker is less than 50% (hereinafter referred to as 50% attack) and where the resource proportion of the attacker is greater than 50% (hereinafter referred to as a 51% attack).

[120] The optimization of the cut time t_{cut} of the attacker and the resource proportion p_A of the attacker may be performed by the parameter optimizer 16.

[121] In general, the appropriate block confirmation number for the 51% attack is greater than that for the 50% attack. In a network with huge computational resources such as Bitcoin, it is

very difficult for a specific group to get more than 51% of computational resources. Therefore, it is sufficient to prepare for the 50% attack. In contrast, in a network with small computational resources, the 51% attack may be possible, and thus more thorough preparation is required.

[122] First, in the case of the 51% attack, the optimal cut time for the attacker is infinite, and the optimal attack resource proportion is calculable.

[123] The returns may be compared for the two cases of a finite cut time and the infinite cut time. For example, if the reward β for block generation is greater than the cost γ for block generation, that is, if the reward per time for block generation is greater than the cost per time for block generation, the attack return is maximized when the cut time is set to infinite.

[124] In contrast, if the reward β for block generation is less than the cost γ for block generation, it is not true that an infinite cut time always makes the attack return maximized, but in many practical cases it can be true. In addition, in normal networks, it is natural that β is formed greater than γ by the market economy.

[125] When the cut time is infinite in the 51% attack case, the safe transaction limit amount C_{Req} is a function that is downwardly convex with respect to the resource proportion p_A of the attacker. This has been proven mathematically and is exemplified in Fig. 5.

[126] That is, there exists the minimum of the safe transaction limit amount C_{Req} with respect to the resource proportion p_A of the attacker. When $C<C^*_{Req}$ is satisfied by comparing the input transaction amount C with the safe confirmation amount C_{Req}, it always holds that $C<C_{Req}$ for all the other resource proportions, and thus it can be seen that the transaction is safe. In other words, the trader only needs to consider the worst case of attack

resource proportion in order to check the safety. For example, it is sufficient to select the minimum of the safe transaction limit amount in Fig. 5.

[127] Second, even in the 50% attack case, it is possible to consider the optimal cut time t_{cut} and the optimal attack resource proportion p_A of the most reasonable attacker.

[128] In the case of the 50% attack, the resource proportion p_A of the attacker at which the average attack success time is minimized is a reasonable attack resource proportion. In the case of the 50% attack, unlike the 51% attack, there is no need to consider the infinite cut time, because in that case the attacker's expected loss becomes infinitely large.

[129] Therefore, the attacker is forced to select a finite cut time. From the attacker's point of view, when selecting the cut time, the average time required for a success of attack, that is, the attack success average time, has to be taken into consideration. For example, when the average attack success time is known, the cut time when attempting the attack may be set to be equal, slightly greater, or several times greater than the average attack success time.

[130] In the case of the 50% attack, the attack success probability is not very high, and thus an attacker will make a return by attempting the attack several times. Therefore, the time it takes to turn from a deficit to a surplus will be delayed as each attack attempt takes the longer time. In order to find the cut time quickly and accurately, the attacker will search the optimal attack resource proportion p_A at which the average attack success time is minimized.

[131] It is numerically checked that the attack success time is a downwardly convex function as shown in Fig. 6, that is, a function having the minimum. Therefore, in the case of the 50% attack, it

can be assumed that the optimal attack resource proportion p_A at which the average attack success time is minimized is a reasonable estimation of the attack resource proportion.

[132] In addition, for a fixed attack resource proportion p_A, it is checked as shown in Fig. 7 that the safe transaction limit amount C_{Req} is a downwardly convex function with respect to t_{cut}. That is, there is the minimum of the safe transaction limit amount at some cut time. Therefore, in order to determine the safety, the trader only needs to consider the case in which the cut time is the worst case, that is, the case in which the safe trade limit amount is the minimum.

[133] When the resource proportion of the attacker is greater than 50%, the attacker may set the cut time to infinity, as described above.

[134] In this case, the safe transaction limit amount can be found as in Equation 12 below by using the average time $\mathbb{E}_{T_{AS-ICT}}(p_A;N_{BC})$ required for attack success when the cut time is infinite, which is presented in Equation 9. In other words, in this case, the cut time is infinite.

[135] [Equation 12]

$$C_{\text{Req.}} = \max\left(0,(\gamma-\beta)\lambda_T p_A \mathbb{E}_{T_{AS-ICT}}(p_A;N_{BC})\right)$$

[136] Referring to Equation 12, the resource proportion p_A occupied by the attacker is unknown, and Equation 12 may be given as a function using the resource proportion p_A occupied by the attacker as a variable. Therefore, it is possible to optimize the safe transaction limit amount C_{req} by using the resource proportion p_A occupied by the attacker as a variable. The optimization may be performed by the parameter optimizer 16.

[137] The graph exemplifies the safe transaction limit amount as a

function with respect to the attack resource proportion p_A has already been described with reference to Fig. 5.

[138] Referring to Fig. 5, the safe transaction limit amount with respect to the attack resource proportion p_A is shown as a downwardly convex graph. The minimum of the safe transaction limit amount may be outputted as the safest transaction limit amount.

[139] According to the invention described in this disclosure, the user can output the appropriate block confirmation number by inputting only the transaction amount, and can set the block confirmation number according to the appropriate confirmation number. Due to this, there is an advantage that safe and quick commercial transaction using cryptocurrency is possible.

[140] In addition, in the process of calculating the safe transaction limit amount, the parameters as criteria for determining the stability of the transaction that need to be estimated are optimized. Therefore, even when the user inputs only the transaction amount, the appropriate block confirmation number can be found.

【Industrial Applicability】

[141] According to the present disclosure of invention, the invention enables to further promote the commercialization of actual trading using the cryptocurrency system by guaranteeing the safety and quickness of transactions.

【CLAIMS】

【Claim 1】

A blockchain transaction confirmation system comprising:

a user information input interface to which user information is inputted;

an external information input interface to which external information related to a cryptocurrency system is inputted;

an appropriate confirmation number searcher configured to search for a block confirmation number appropriate for confirmation of a transaction in progress of creation, by using the external information and the user information; and

an appropriate confirmation number output interface configured to output the block confirmation number.

【Claim 2】

The blockchain transaction confirmation system of claim 1, wherein the user information includes at least an input transaction amount inputted by a user.

【Claim 3】

The blockchain transaction confirmation system of claim 1, wherein the external information includes at least one of a reward paid for generating a block at the time, an average cost required for generating a block at the time, or an average rate per time of block generation at the time.

【Claim 4】

The blockchain transaction confirmation system of claim 3, wherein the external information includes all of a reward paid for generating a block at the time, an average cost required for generating a block at the time, and an average rate per time of block generation at the time.

【Claim 5】

The blockchain transaction confirmation system of claim 2, wherein the appropriate confirmation number searcher comprises:

a safe transaction limit amount extractor configured to extract a safe transaction limit amount at the time by using the external information; and

a safety determiner configured to determine safety by comparing the safe transaction limit amount with the input transaction amount.

【Claim 6】

The blockchain transaction confirmation system of claim 5, wherein the safe transaction limit amount extractor comprises a calculator configured to extract, as the safe transaction limit amount, an amount that makes an attacker's expected return to be zero.

【Claim 7】

The blockchain transaction confirmation system of claim 6, wherein the attacker's expected return is provided by subtracting an attacker's expected cost from the attacker's expected profit.

【Claim 8】

The blockchain transaction confirmation system of claim 6, wherein the safe transaction limit amount (C_{Req}) is extracted by $C_{Req.}=(1-P_{AS})/P_{AS}*X(\gamma,t_{cut})+X(\gamma,T_{AS})-R(\beta,T_{AS})$,

wherein P_{AS} (dimensionless) is a probability that double spending attack will succeed within t_{cut},

$X(\gamma,t)$ is an average block generation cost (function increasing for γ and t) for a time duration t,

γ is an average cost required for a single block generation,

T_{AS} is a time taken until an attack is successful,

β is a reward paid for a single block generation, and

$R(\beta,t)$ is an average block generation reward (function increasing for β and t) for a time duration t.

【Claim 9】

The blockchain transaction confirmation system of claim 5, wherein the safe transaction limit amount extractor comprises a parameter optimizer, and

the parameter optimizer is configured to optimally estimate at least one of an attacker's cut time or an attacker's resource proportion.

【Claim 10】

The blockchain transaction confirmation system of claim 9, wherein the safe transaction limit amount extractor comprises a parameter optimizer, and

the parameter optimizer is configured to optimally estimate an attacker's cut time or an attacker's resource proportion.

【Claim 11】

The blockchain transaction confirmation system of claim 5, wherein, if the safety determiner determines that a transaction is not safe, the safe transaction limit amount is extracted again.

【Claim 12】

The blockchain transaction confirmation system of claim 11, wherein the safe transaction limit amount is extracted again by increasing the block confirmation number.

【Claim 13】

A blockchain transaction confirmation method comprising:

receiving external information that is information about a cryptocurrency system and user information that is inputted by a user; and

searching for an appropriate confirmation number, which is an appropriate block confirmation number aiming to safe and quick transaction, by using the external information and the user information.

【Claim 14】

The blockchain transaction confirmation method of claim 13 , further comprising outputting the appropriate confirmation number.

【Claim 15】

The blockchain transaction confirmation method of claim 12, wherein

the searching for the appropriate confirmation number comprises:

calculating a safe transaction limit amount, which is the upper limit of amount for a safe transaction at the time, by using the external information and an arbitrary current block confirmation number;

comparing the safe transaction limit amount with the input transaction amount inputted as the user information; and

comparing the safe transaction limit amount with the input transaction amount, and if the safe transaction limit amount is greater than the input transaction amount, determining that it is safe and outputting the current block confirmation number.

【Claim 16】

The blockchain transaction confirmation method of claim 15, wherein the current block confirmation number is an arbitrary variable value.

【Claim 17】

The blockchain transaction confirmation method of claim 15, further comprising the comparison of the safe transaction limit amount with the input transaction amount, and if the safe transaction limit amount is less than the input transaction amount, then determining that it is not safe, increasing the current block confirmation number, and calculating the safe transaction limit amount again.

【Claim 18】

The blockchain transaction confirmation method of claim 13,

wherein the user information includes at least an input transaction amount inputted by a user.

【Claim 19】

The blockchain transaction confirmation method of claim 13, wherein the external information includes at least one of a reward paid for generating a block at the time, an average cost required for generating a block at the time, or an average rate per time of block generation at the time.

【Claim 20】

A blockchain transaction confirmation method comprising:

receiving external information that is information about a cryptocurrency system and user information that is inputted by a user;

searching for an appropriate confirmation number, by using the external information and the user information; and

outputting the appropriate confirmation number,

wherein the external information includes at least one of a reward paid for generating a block at the time, an average cost required for generating a block at the time, or an average rate per time of block generation at the time, and

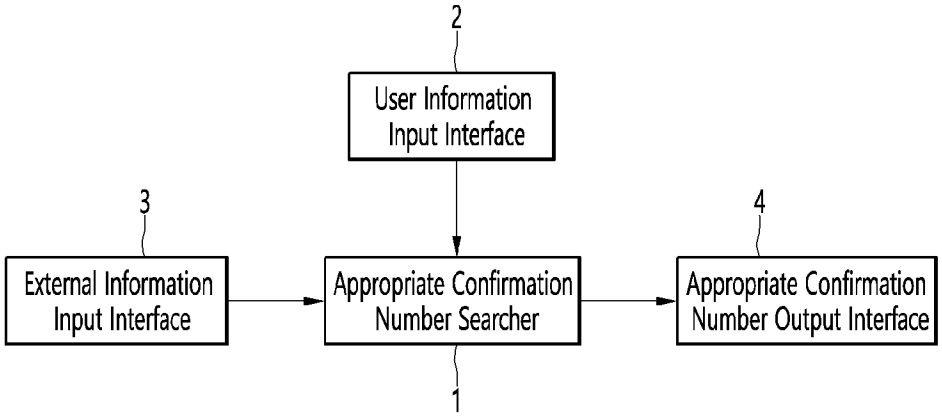
the user information includes a transaction amount.

【ABSTRACT】

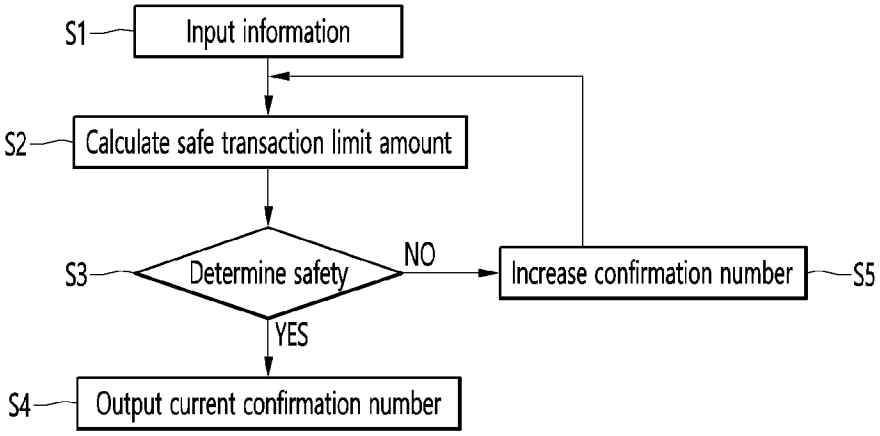
A blockchain transaction confirmation system according to the present disclosure includes: a user information input interface to which user information is inputted; an external information input interface to which external information related to a cryptocurrency system is inputted; an appropriate confirmation number searcher configured to search for a block confirmation number appropriate for confirmation of a transaction in progress of creation by using the external information and the user information; and an appropriate confirmation number output interface configured to output the block confirmation number. According to the present disclosure, a user can automatically find out the block confirmation number required for safe and quick transaction.

【DRAWINGS】

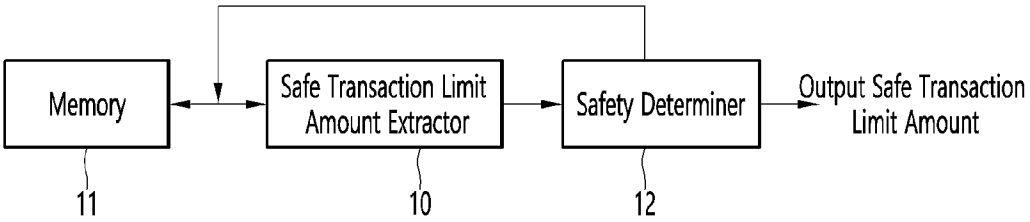
【figure 1】



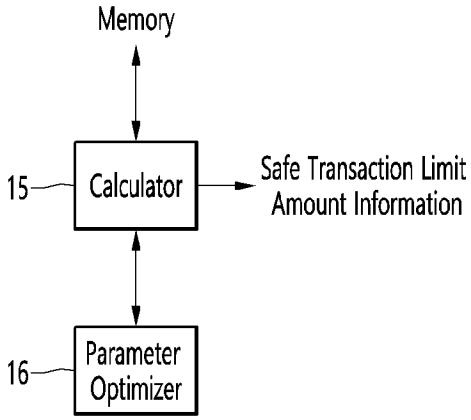
【figure 2】



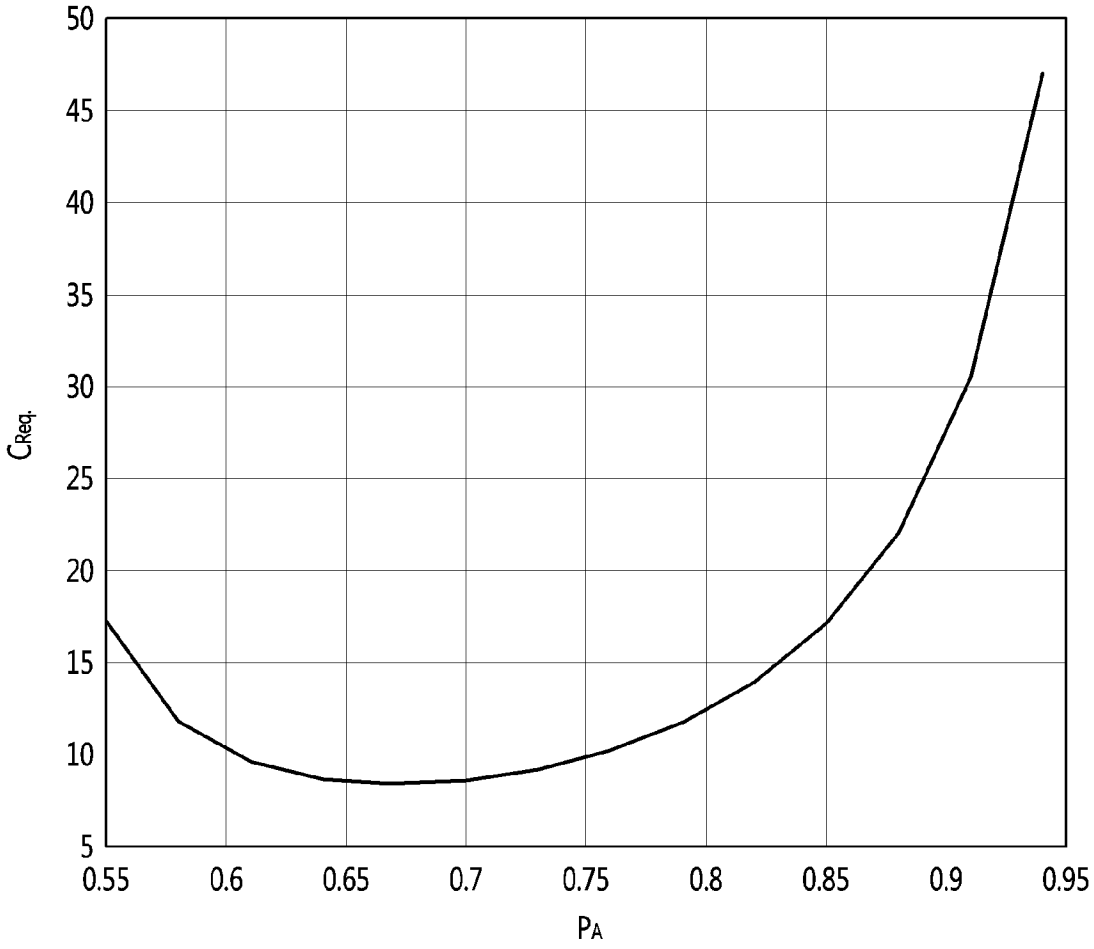
【figure 3】



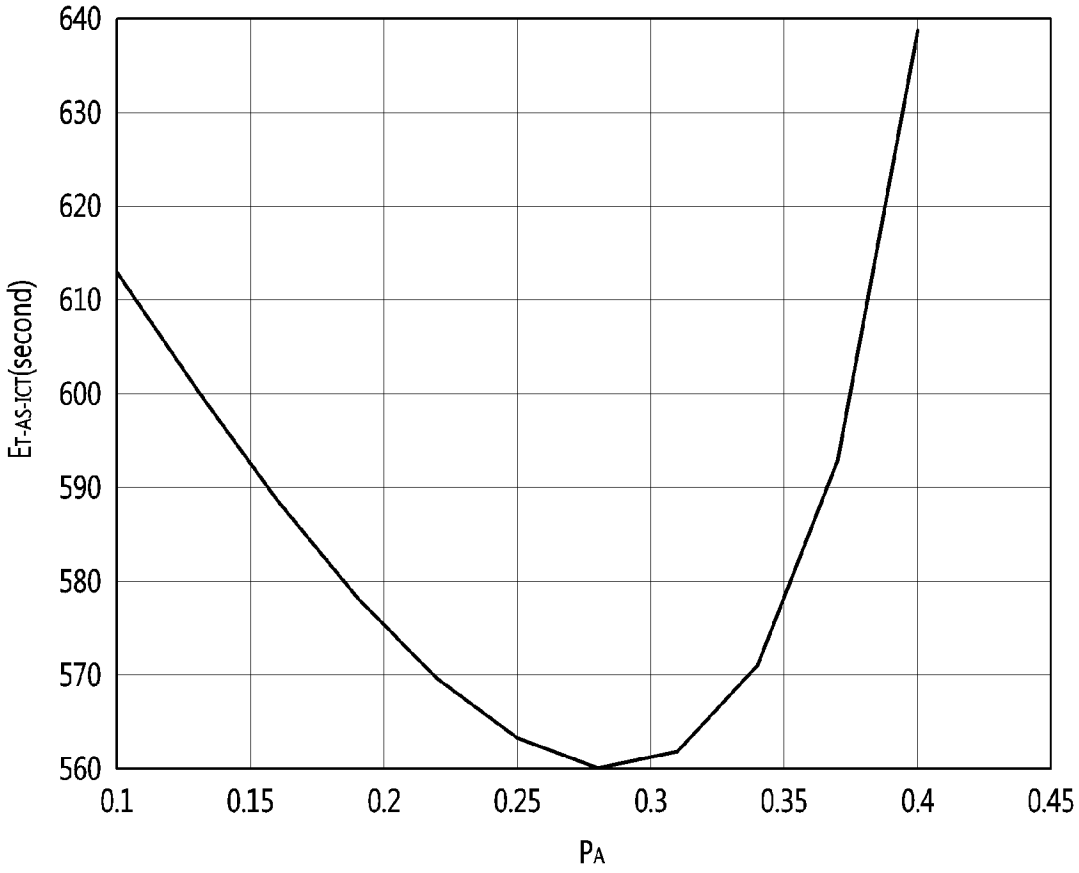
【figure 4】



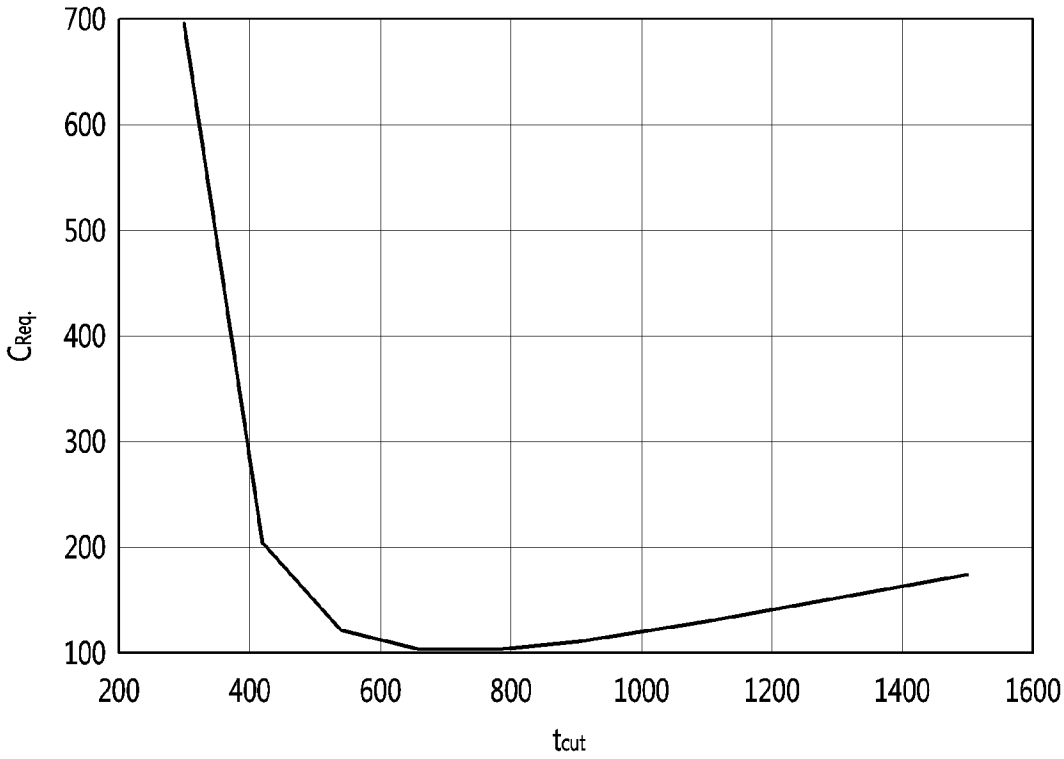
【figure 5】



【figure 6】


640
630
620
610
600
590
580
570
560
ET-AS-ICT(second)
0.1
0.15
0.2
0.25
0.3
0.35
0.4
0.45
PA

【figure 7】


700
600
500
400
300
200
100
CReq.
200
400
600
800
1000
1200
1400
1600
tcut

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
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.

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-1073

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	20180191502	A1	2018-07-05	KARAME	
	2	20160283920	A1	2016-09-29	FISHER ET AL.	

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	20180014534	KR	A	2018-02-09	UNIV SOGANG RES FOUNDATION		
	2	101951408	KR	B1	2019-02-22	BAEK JONG YUN		

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-1073

	3	101796690	KR	B1	2017-11-10	SANGMYUNG UNIV CHEONAN COUNCIL FOR INDUSTRY		

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]
	1	PCT/KR2019/017571. International Search Report (March 31, 2020).	
	2	JANG ET AL. "Profitable Double-Spending Attacks." Appl. Sci. 2020 10(23), 8477 (November 27, 2020).	

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

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-1073

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)	2021-11-15
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 record s.

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.

Electronic Acknowledgement Receipt

EFS ID:	44286862
Application Number:	17611506
International Application Number:	PCT/KR2019/017571
Confirmation Number:	9530
Title of Invention:	TRANSACTION VERIFICATION SYSTEM FOR BLOCKCHAIN, AND TRANSACTION VERIFICATION METHOD FOR BLOCKCHAIN
First Named Inventor/Applicant Name:	Jehyuk Jang
Customer Number:	71572
Filer:	Heidi Eisenhut/Kathleen Smith
Filer Authorized By:	Heidi Eisenhut
Attorney Docket Number:	HANMIR-1073
Receipt Date:	15-NOV-2021
Filing Date:	
Time Stamp:	18:40:04
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$830
RAM confirmation Number	E2021AEI40333054
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 1.492(a) (Basic national fee only)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal of New Application	HANMIR-1073_371_Transmittal.pdf	325088 a2d31cfb9ad462243195a8c6428f90979caa9f1a	no	4
Warnings:					
Information:					
2	Application Data Sheet	HANMIR-1073_ADS.pdf	1226516 52888fd645324eda801047ca98d01e85ab69d1df	no	8
Warnings:					
Information:					
3	Oath or Declaration filed	HANMIR-1073_Declarations.pdf	2239096 f5b178d90ce9c1bc833a69c65299dc3534855d9c	no	2
Warnings:					
Information:					
4	Power of Attorney	HANMIR-1073_POA.pdf	3107734 90802bdb1c098b0a6b3f844088aa97d3c5abdaa5	no	2
Warnings:					
Information:					
5	Documents submitted with 371 Applications	WO2020241995A1_KR_Publication.pdf	978419 b1c8922d2c0d4cdbc374adaa54133a32665db07e	no	25
Warnings:					
Information:					
6		HANMIR-1073_Translation_EN.pdf	1262762 2d8166d05b849fc3da8a33854e79528aae3763e8	yes	39
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	

	Transmittal Letter		1		1
	Specification		2		28
	Claims		29		33
	Abstract		34		34
	Drawings-only black and white line drawings		35		39
Warnings:					
Information:					
7	Information Disclosure Statement (IDS) Form (SB08)	HANMIR-1073_IDS.pdf	1034241 d1b93d78bbac9b1260eff711ef287b00a418df0b	no	4
Warnings:					
Information:					
8	Foreign Reference	HANMIR-1073_IDS_KR101796690.pdf	1942592 0a6c5f640a17135664d88de2027a8c94ed6eaf8c	no	19
Warnings:					
Information:					
9	Foreign Reference	HANMIR-1073_IDS_KR101951408.pdf	1047976 ba344bf7528f0dc9dd22b38717fec8e5302c9249	no	18
Warnings:					
Information:					
10	Foreign Reference	HANMIR-1073_IDS_KR20180014534.pdf	1678544 d1989e6a357de262314e4aa4c8c34441fbc42ecf	no	16
Warnings:					
Information:					
11	Non Patent Literature	HANMIR-1073_IDS_NPL.pdf	430499 cb6b3c5d4963ef0125ed23cbfa18ccc18464d0b7	no	23
Warnings:					
Information:					

12	Other Reference-Patent/App/Search documents	HANMIR-1073_IDS_ISR.pdf	298382 cdfaf2b906e2e1b0e90d1b2b3c80eb49f9fa164d	no	3
Warnings:					
Information:					
13	Fee Worksheet (SB06)	fee-info.pdf	43865 e13f6c8e70456f4e73d96c6c3066fece3eb8c744	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	15615714	

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.