(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2021 년 2 월 4 일 (04.02.2021)

WIPO | PCT

(10) 국제공개번호
WO 2021/020794 A3

(51) 국제특허분류:
H04L 9/32 (2006.01) *H04L 9/06* (2006.01)
H04L 9/08 (2006.01) *G06F 16/901* (2019.01)

(21) 국제출원번호: PCT/KR2020/009588

(22) 국제출원일: 2020 년 7 월 21 일 (21.07.2020)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2019-0093684 2019 년 8 월 1 일 (01.08.2019) KR

(71) 출원인: 주식회사 블룸테크놀로지 (**BLOOM TECHNOLOGY, INC.**) [KR/KR]; 13487 경기도 성남시 분당구 판교로228번길 15, 2동 10층 1003호(삼평동, 판교세븐벤처밸리), Gyeonggi-do (KR).

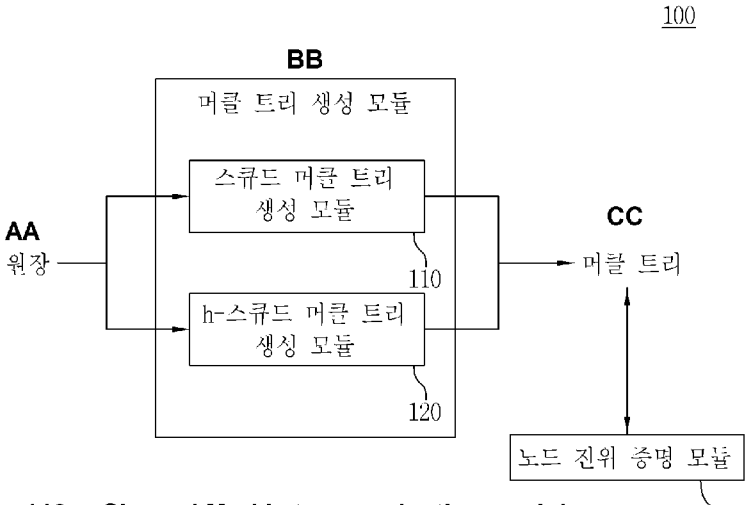
(72) 발명자: 주영현 (**JOO, Young Hyun**); 16862 경기도 용인시 수지구 심곡로 18, 505동 901호 (상현동), Gyeonggi-do (KR).

(74) 대리인: 고영갑 (**KO, Young Kap**); 13554 경기도 성남시 분당구 정자일로 248, 705호 (정자동, 파크뷰타워), Gyeonggi-do (KR).

(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD,

(54) **Title:** LEDGER VERIFIABLE-PRUNING SYSTEM

(54) **발명의 명칭:** 원장의 증명 가능 프루닝 시스템



110 ... Skewed Merkle tree production module
120 ... h-skewed Merkle tree production module
130 ... Node integrity verification module
AA ... Ledger
BB ... Merkle tree production module
CC ... Merkle tree

(57) **Abstract:** A ledger verifiable-pruning system is disclosed. According to a linked list scheme, root hash value R_{n-1} of a previous sub-tree is included in data block T_n. Data block T_n in which root has value R_{n-1} is included is hashed, thereby obtaining $h(T_n)$. Obtained $h(T_n)$ and root hash value R_{n-1} of the previous sub-tree are summated and then hashed, thereby obtaining $h(h(T_n)|R_{n-1})$. Obtained $h(h(T_n)|R_{n-1})$ is successively added to respective nodes of a binary Merkle tree structure, thereby configuring a skewed Merkle tree production module for expanding/producing a skewed Merkle tree. The above-mentioned ledger verifiable-pruning system is advantageous in that a ledger structure is configured as a skewed Merkle tree such that latest data is solely stored and managed,

WO 2021/020794 A3

[다음 쪽 계속]

SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) **지정국** (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

공개:

— 국제조사보고서와 함께 (조약 제21조(3))

(88) **국제조사보고서 공개일:**

2021 년 3 월 25 일 (25.03.2021)

and the integrity of a transaction submitted by another node is authenticated, thereby minimizing the increase in the ledger size and then maintaining same accordingly. Particularly, the ledger verifiable-pruning system is advantageous in that a distributed ledger is managed by converting a skewed Merkle tree into an upgraded h-skewed Merkle tree, thereby substantially reducing the size of the proof which increases over time. The ledger verifiable-pruning system is also advantageous in that, in addition to the proof size reduction, the integrity of multi-year-old data can be authenticated through a smaller number of calculation steps, thereby further improving the authentication speed.

(57) 요약서: 원장(ledger)의 증명 가능 프루닝(verifiable pruning) 시스템이 개시된다. 링크드 리스트(linked list) 방식에 따라 상기 이전 서브 트리의 루트 해쉬(root hash)값 R_{n-1}을 상기 데이터 블록(data block) T_n에 포함시키고, 상기 루트 해쉬값 R_{n-1}이 포함된 데이터 블록 T_n을 해쉬하여 $h(T_n)$을 산출하고, 산출된 $h(T_n)$과 이전 서브 트리의 루트 해쉬값 R_{n-1}을 합산한 후 해쉬하여 $h(h(T_n)|R_{n-1})$을 산출하고, 산출된 $h(h(T_n)|R_{n-1})$을 이진 머클 트리(binary merkle tree) 구조의 각 노드에 순차적으로 추가하여 스큐드 머클 트리(skewed merkle tree)를 확장 생성하는 스큐드 머클 트리 생성 모듈을 구성한다. 상술한 원장의 증명 가능 프루닝 시스템에 의하면, 원장 구조를 스큐드 머클 트리로 구성하여 최신의 데이터만을 저장하여 관리하고 타 노드에서 제출하는 트랜잭션의 진위를 검증하도록 구성됨으로써, 원장 크기의 증가를 최소화하여 유지할 수 있는 효과가 있다. 특히, 스큐드 머클 트리에서 업그레이드된 h-스큐드 머클 트리로 변환하여 분산 원장을 관리하도록 구성됨으로써, 시간이 갈수록 커지는 증명용 데이터(proof)의 크기를 획기적으로 줄일 수 있는 효과가 있다. 프루프의 크기 축소와 함께 수 년 전 이상의 오래된 데이터의 진위 검증을 더 적은 횟수의 연산 스텝으로도 가능하게 하여 검증 속도를 더 높일 수 있는 효과가 있다.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2020/009588

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)i; **H04L 9/08**(2006.01)i; **H04L 9/06**(2006.01)i; **G06F 16/901**(2019.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 9/32(2006.01); H04L 29/08(2006.01); H04L 9/00(2006.01); H04L 9/06(2006.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models: IPC as above
Japanese utility models and applications for utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & keywords: 스큐드 머클 트리(skewed merkle tree), 증명(verification), 링크드 리스트(linked list), 서브 트리(sub tree), 루트 해쉬(root hash), 데이터 블록(data block), 이진 머클 트리(binary merkle tree)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WOO, Seung. Skewed Merkle Trees. 21 June 2018. [Retrieved on 29 December 2020]. Retrieved from <https://medium.com/codechain/skewed-merkle-tree-259b984acc0c>. See pages 2-3.	1-2
A		3-7
Y	VIG, Saru et al. Customizing Skewed Trees for Fast Memory Integrity Verification in Embedded Systems. 2017 IEEE Computer Society Annual Symposium on VLSI (ISVLSI). 2017. See page 215; and figure 3.	1-2
A	KR 10-1937188 B1 (COINPLUG, INC.) 09 April 2019 (2019-04-09) See paragraph [0041]; claim 1; and figure 2.	1-7
A	WO 2019-116248 A1 (NCHAIN HOLDINGS LIMITED) 20 June 2019 (2019-06-20) See claims 1-8.	1-7

☑ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"D" document cited by the applicant in the international application
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
05 January 2021	**05 January 2021**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office **Government Complex-Daejeon Building 4, 189 Cheongsa-ro, Seo-gu, Daejeon 35208**	
Facsimile No. **+82-42-481-8578**	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2020/009588

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2014-0245020 A1 (GUARDTIME IP HOLDINGS LIMITED) 28 August 2014 (2014-08-28) See claims 1-4.	1-7

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2020/009588

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
KR	10-1937188	B1	09 April 2019	CA	3032682	A1	06 August 2019
				KR	10-2019-0095067	A	14 August 2019
				US	10528756	B2	07 January 2020
				US	2019-0243986	A1	08 August 2019
WO	2019-116248	A1	20 June 2019	CN	111316594	A	19 June 2020
				CN	111316595	A	19 June 2020
				CN	111316615	A	19 June 2020
				CN	111345004	A	26 June 2020
				CN	111345005	A	26 June 2020
				CN	111406379	A	10 July 2020
				CN	111466095	A	28 July 2020
				CN	111466100	A	28 July 2020
				CN	111801910	A	20 October 2020
				EP	3707623	A1	16 September 2020
				EP	3707852	A1	16 September 2020
				EP	3707855	A1	16 September 2020
				EP	3707856	A1	16 September 2020
				EP	3707871	A1	16 September 2020
				EP	3707872	A1	16 September 2020
				EP	3725028	A1	21 October 2020
				EP	3725031	A1	21 October 2020
				EP	3725032	A1	21 October 2020
				KR	10-2020-0079503	A	03 July 2020
				KR	10-2020-0080263	A	06 July 2020
				KR	10-2020-0080265	A	06 July 2020
				KR	10-2020-0086281	A	16 July 2020
				KR	10-2020-0086282	A	16 July 2020
				KR	10-2020-0086284	A	16 July 2020
				KR	10-2020-0094173	A	06 August 2020
				KR	10-2020-0096248	A	11 August 2020
				KR	10-2020-0096790	A	13 August 2020
				SG	11202005596	A	29 July 2020
				TW	201923567	A	16 June 2019
				TW	201923648	A	16 June 2019
				TW	201924278	A	16 June 2019
				TW	201928743	A	16 July 2019
				TW	201928755	A	16 July 2019
				US	2020-0266985	A1	20 August 2020
				US	2020-0322132	A1	08 October 2020
				US	2020-0348916	A1	05 November 2020
				US	2020-0366492	A1	19 November 2020
				WO	2019-092542	A1	16 May 2019
				WO	2019-092543	A1	16 May 2019
				WO	2019-092544	A1	16 May 2019
				WO	2019-092545	A1	16 May 2019
				WO	2019-092552	A1	16 May 2019
				WO	2019-092561	A1	16 May 2019
				WO	2019-116187	A1	20 June 2019
				WO	2019-116246	A1	20 June 2019
US	2014-0245020	A1	28 August 2014	AU	2014-221033	A1	10 September 2015

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2020/009588

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
		AU	2017-272163	A1	21 December 2017
		AU	2017-272163	B2	05 December 2019
		CN	105164971	A	16 December 2015
		EP	2959631	A1	30 December 2015
		EP	2959631	B1	26 June 2019
		JP	2016-509443	A	24 March 2016
		WO	2014-127904	A1	28 August 2014

국 제 조 사 보 고 서

국제출원번호
PCT/KR2020/009588

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04L 9/32(2006.01)i; **H04L 9/08**(2006.01)i; **H04L 9/06**(2006.01)i; **G06F 16/901**(2019.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

H04L 9/32(2006.01); H04L 29/08(2006.01); H04L 9/00(2006.01); H04L 9/06(2006.01)

조사된 기술분야에 속하는 최소문헌 이외의 문헌

한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))

eKOMPASS(특허청 내부 검색시스템) & 키워드: 스큐드 머클 트리(skewed merkle tree), 증명(verification), 링크드 리스트(linked list), 서브 트리(sub tree), 루트 해쉬(root hash), 데이터 블록(data block), 이진 머클 트리(binary merkle tree)

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y	SEUNG WOO, `Skewed Merkle Trees', 2018.06.21 [검색일: 2020.12.29]. 출처 <https://medium.com/codechain/skewed-merkle-tree-259b984acc0c> 페이지 2-3	1-2
A		3-7
Y	SARU VIG 등, `Customizing Skewed Trees for Fast Memory Integrity Verification in Embedded Systems', 2017 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), 2017 페이지 215; 및 도면 3	1-2
A	KR 10-1937188 B1 (주식회사 코인플러그) 2019.04.09 단락 [0041]; 청구항 1; 및 도면 2	1-7
A	WO 2019-116248 A1 (NCHAIN HOLDINGS LIMITED) 2019.06.20 청구항 1-8	1-7
A	US 2014-0245020 A1 (GUARDTIME IP HOLDINGS LIMITED) 2014.08.28 청구항 1-4	1-7

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☑ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌
"D" 본 국제출원에서 출원인이 인용한 문헌
"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌
"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌
"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌
"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌
"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌
"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.
"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.
"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2021년01월05일(05.01.2021)	**2021년01월05일(05.01.2021)**

ISA/KR의 명칭 및 우편주소	심사관
대한민국 특허청 **(35208) 대전광역시 서구 청사로 189, 4동 (둔산동, 정부대전청사)**	**양정록**
팩스 번호 **+82-42-481-8578**	전화번호 **+82-42-481-5709**

서식 PCT/ISA/210 (두 번째 용지) (2019년 7월)

국 제 조 사 보 고 서
대응특허에 관한 정보

국제출원번호
PCT/KR2020/009588

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-1937188 B1	2019/04/09	CA 3032682 A1	2019/08/06
		KR 10-2019-0095067 A	2019/08/14
		US 10528756 B2	2020/01/07
		US 2019-0243986 A1	2019/08/08
WO 2019-116248 A1	2019/06/20	CN 111316594 A	2020/06/19
		CN 111316595 A	2020/06/19
		CN 111316615 A	2020/06/19
		CN 111345004 A	2020/06/26
		CN 111345005 A	2020/06/26
		CN 111406379 A	2020/07/10
		CN 111466095 A	2020/07/28
		CN 111466100 A	2020/07/28
		CN 111801910 A	2020/10/20
		EP 3707623 A1	2020/09/16
		EP 3707852 A1	2020/09/16
		EP 3707855 A1	2020/09/16
		EP 3707856 A1	2020/09/16
		EP 3707871 A1	2020/09/16
		EP 3707872 A1	2020/09/16
		EP 3725028 A1	2020/10/21
		EP 3725031 A1	2020/10/21
		EP 3725032 A1	2020/10/21
		KR 10-2020-0079503 A	2020/07/03
		KR 10-2020-0080263 A	2020/07/06
		KR 10-2020-0080265 A	2020/07/06
		KR 10-2020-0086281 A	2020/07/16
		KR 10-2020-0086282 A	2020/07/16
		KR 10-2020-0086284 A	2020/07/16
		KR 10-2020-0094173 A	2020/08/06
		KR 10-2020-0096248 A	2020/08/11
		KR 10-2020-0096790 A	2020/08/13
		SG 11202005596 A	2020/07/29
		TW 201923567 A	2019/06/16
		TW 201923648 A	2019/06/16
		TW 201924278 A	2019/06/16
		TW 201928743 A	2019/07/16
		TW 201928755 A	2019/07/16
		US 2020-0266985 A1	2020/08/20
		US 2020-0322132 A1	2020/10/08
		US 2020-0348916 A1	2020/11/05
		US 2020-0366492 A1	2020/11/19
		WO 2019-092542 A1	2019/05/16
		WO 2019-092543 A1	2019/05/16
		WO 2019-092544 A1	2019/05/16
		WO 2019-092545 A1	2019/05/16
		WO 2019-092552 A1	2019/05/16
		WO 2019-092561 A1	2019/05/16
		WO 2019-116187 A1	2019/06/20
		WO 2019-116246 A1	2019/06/20
US 2014-0245020 A1	2014/08/28	AU 2014-221033 A1	2015/09/10

국 제 조 사 보 고 서
대응특허에 관한 정보

국제출원번호
PCT/KR2020/009588

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
		AU 2017-272163 A1	2017/12/21
		AU 2017-272163 B2	2019/12/05
		CN 105164971 A	2015/12/16
		EP 2959631 A1	2015/12/30
		EP 2959631 B1	2019/06/26
		JP 2016-509443 A	2016/03/24
		WO 2014-127904 A1	2014/08/28