ISSN 1226-9182

정보처리학회지

Korea Information Processing Society Review

www.kips.or.kr

KIPS

2017년 5월 | 제24권 제3호 |

블록체인과 관련한 기술 및 응용

- 사물인터넷과 블록체인 기술 적용 동향
- 블록체인 기반의 IoT 보안 취약점
- 핀테크 산업에서 블록체인 도입의 한계점
- 금융서비스를 위한 블록체인과 IoT의 통합

사단법인 한국정보처리학회
KIPS Korea Information Processing Society

글로벌 엔지니어의 길
공학교육인증제도가 있습니다

공학교육인증제도란?

- 공과대학교육과정에 대한 인증을 통해 해당 과정을 이수한 졸업생이 산업체의 요구와 Global Standard를 만족하는 역량을 갖춘 우수인재임을 보증하는 제도입니다.
- 인증졸업생은 Washington Accord회원국(18개국)졸업생과 그 학력의 동등성을 보장 받습니다.

글로벌 공학인재 양성을 선도하는-한국공학교육인증원

한국공학교육인증원은 2007년 워싱턴어코드 정회원으로 가입하고, 2008년에는 우리나라 주도로 서울어코드를 창립했습니다. (공학교육인증 졸업생은 회원국 졸업생과 동등한 자격 인정)
2013년, 시드니어코드 및 더블린어코드 정회원이 되었으며 2017년, 국내 83개 대학 510개 프로그램이 인증받았습니다. ▶자세한 사항은 홈페이지 www.abeek.or.kr참조

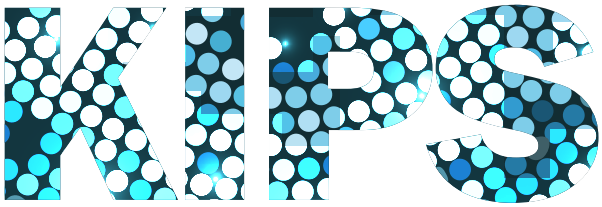
워싱턴어코드 4년제 공과대학 졸업자 학력의 상호인정을 목표로 설립된 회원국 인증기구간 다자간 국제협의체로 인증기구가 인증한 졸업생은 모든 정회원국에서 학력의 동등성을 보장함.

ABEEK 한국공학교육인증원
Accreditation Board for Engineering Education of Korea

정보처리학회지

Korea Information Processing Society Review

www.kips.or.kr



제 22대 임원명단

김수균 (배재대학교) 김영욱 (KETI) 김 용 (한국방송통신대학교) 김인철 (경기대학교)
김종국 (고려대학교) 김태근 (세종대학교) 김학만 (인천대학교) 노응기 (가천대학교)
노원우 (연세대학교) 문유진 (한국외국어대학교) 문현준 (세종대학교) 민세동 (순천향대학교)
민 홍 (호서대학교) 박능수 (건국대학교) 박상봉 (세명대학교) 박정민 (KIST)
박진호 (숭실대학교) 박찬열 (KISTI) 성연식 (동국대학교) 손태식 (아주대학교)
송왕철 (제주대학교) 신동일 (세종대학교) 아지즈 (충북대학교) 안상현 (서울시립대학교)
오세창 (세종사이버대학교) 유윤섭 (한경대학교) 유진호 (상명대학교) 윤주상 (동의대학교)
이경오 (선문대학교) 이경현 (부경대학교) 이기훈 (광운대학교) 이덕규 (서원대학교)
이원규 (고려대학교) 이은영 (동덕여자대학교) 이의신 (충북대학교) 이재광 (한남대학교)
이필우 (KISTI) 이화민 (순천향대학교) 임동혁 (호서대학교) 장종수 (ETRI)
전유부 (순천향대학교) 정수환 (숭실대학교) 정순영 (고려대학교) 정승원 (동국대학교)
정윤호 (한국항공대학교) 정창성 (고려대학교) 정화영 (경희대학교) 조수현 (홍익대학교)
최강선 (한국기술교육대학교) 최 성 (남서울대학교) 최은미 (국민대학교) 추현승 (성균관대학교)
허 경 (경인교육대학교) 허준범 (고려대학교)

협 동 이 사 |

강동석 (NIA) 강 신 (코스콤) 고범석 (㈜자이네스) 구태언 (테크앤로법률사무소)
권문주 (NIPA) 김교은 (㈜베스트케이에스) 김성동 (KETI) 김성엽 (㈜블루코어)
김완섭 (㈜넥스첼) 김우성 (호서대학교) 김태섭 (㈜바른전자) 김평중 (충북도립대학)
문정현 (한국정보산업연합회) 민석홍 (민데이터) 박철균 (에코메이텍) 박형우 (KISTI)
서재철 (KISA) 서준서 (대우정보시스템㈜) 신우현 (㈜경봉) 안유환 (㈜네오피엠)
오형근 (국가보안기술연구소) 우종정 (성신여자대학교) 유환조 (포항공과대학교) 윤두식 (㈜지란지교시큐리티)
이영구 (경희대학교) 이윤재 (SK텔레콤) 이재두 (NIA) 이종근 (㈜DSTi)
이현정 (중앙대학교) 이희승 (㈜티노스) 정경균 (㈜달라이브) 정성무 (KERIS)
정연수 (Korea IT Times) 정원용 (원광대학교) 조태남 (우석대학교) 지석구 (NIPA)
진성철 (유넷시스템) 최동근 (롯데카드) 최지윤 (㈜한국IT컨설팅) 황일선 (KISTI)

지회

강원지회 **김상춘** (강원대학교) 영남지회 **김태철** (포위즈시스템)
제주지회 **김형수** (제주한라대학교) 충청지회 **류근호** (충북대학교)
호남지회 **방상원** (송원대학교) 일본지회 **백영선** (코스모컨설팅)

연구회 위원장

e-Bridge **이정배** (부산외국어대학교) IT융합서비스 **박석천** (가천대학교)
IT정책 **오길록** (숭실대학교) 빅데이터컴퓨팅 **이필규** (인하대학교)
소프트웨어공학 **박용범** (단국대학교) 스토리지시스템 **신범주** (부산대학교)
에너지그리드정보처리 **이봉재** (전력연구원) 우정기술 **정 훈** (ETRI)
전산교육 **김형진** (전북대학교) 전산수학 **박진홍** (선문대학교)
전자정부 **이재두** (NIA) 정보통신응용 **오진태** (ETRI)
지식 및 데이터공학 **진병운** (ETRI) 컴퓨터소프트웨어 **박두순** (순천향대학교)

IT시니어봉사단

단 장 | 유기홍 (명지전문대학)

위 원 | 김홍진 (가천대학교) 이준상 (한국IT전문가협회) 정상근 (연성대학교) 정진욱 (인터넷윤리실천협의회)

IT장학사업본부

본 부 장 | 이상범 (단국대학교)

부 본 부 장 | 박정호 (선문대학교)

IT평가인증본부

본 부 장 | 김병기 (전남대학교)

부 본 부 장 | 이상범 (단국대학교) 이영천 (호남대학교)

위 원 | 김우성 (호서대학교) 김응수 (대전대학교) 김점구 (남서울대학교) 박석천 (가천대학교)
박정호 (선문대학교) 박진양 (인하공업전문대학) 박태홍 (LG전자) 윤용익 (숙명여자대학교)
이병수 (인천대학교) 이임영 (순천향대학교) 조동섭 (이화여자대학교) 조성갑 (前 인천정보산업진흥원)
최상록 (생산성본부) 최재혁 (신라대학교) 허문행 (안양대학교)

인터넷윤리진흥본부

본 부 장 | 정진욱 (인터넷윤리실천협의회)

부 본 부 장 | 박정호 (선문대학교)

한민족IT평화봉사단

위 원 장 | 최 성 (남서울대학교)

선거관리위원회

위 원 장 | 구원모 (전자신문)

위 원 | 유헌창 (고려대학교) 김상훈 (한경대학교) 최유주 (서울미디어대학원대학교) 원유재 (충남대학교)
조경은 (동국대학교) 박종혁 (서울과학기술대학교) 문남미 (호서대학교) 한연희 (한국기술교육대학교)
이장호 (홍익대학교)

인사위원회

위 원 장 | 정영식 (동국대학교)

부 위 원 장 | 남석우 (콤텍시스템)

위 원 | 유헌창 (고려대학교) 김상훈 (한경대학교) 최유주 (서울미디어대학원대학교) 문남미 (호서대학교)
황광일 (인천대학교) 길준민 (대구가톨릭대학교) 신창선 (순천대학교) 이장호 (홍익대학교)

간 사 | 한연희 (한국기술교육대학교)

포상위원회

위 원 장 | 김상훈 (한경대학교)

위 원 | 최유주 (서울미디어대학원대학교) 원유재 (충남대학교) 문남미 (호서대학교) 한연희 (한국기술교육대학교)
이장호 (홍익대학교)

전임회장 운영위원회

위 원 장 | 성기중 (프리CEO)

위 원 | 조이남 (엑스게이트) 오길록 (숭실대학교) 정진욱 (인터넷윤리실천협의회) 오해석 (가천대학교)
김홍기 (KTds) 이상범 (단국대학교) 변재일 (국회의원) 김병기 (전남대학교)
최헌규 (前 다우기술) 이정배 (부산외국어대학교) 금기현 (청년기업가정신재단) 정태명 (성균관대학교)
오경수 (前 롯데정보통신) 박석천 (가천대학교) 조성갑 (前 인천정보산업진흥원) 박두순 (순천향대학교)
구원모 (전자신문)

여성위원회

위 원 장 | 문남미 (호서대학교)

위 원 |
길아라 (숭실대학교), 박정민 (KIST), 안상현 (서울시립대학교), 이유부 (성균관대학교), 임지영 (성서대학교), 최유주 (한독미디어대학원대학교), 홍헬렌 (서울여자대학교), 김경아 (명지전문대), 성해경 (한양여자대학교), 안은영 (한밭대학교), 이은영 (동덕여자대학교), 조경은 (동국대학교), 최은미 (국민대학교), 김미혜 (충북대학교), 송은하 (원광대학교), 오수현 (호서대학교), 이정원 (아주대학교), 최미정 (강원대학교), 한영신 (성결대학교), 김미희 (한경대학교), 신은경 (날리지큐브), 윤회진 (협성대학교), 이화민 (순천향대학교), 최수미 (세종대학교), 한정란 (협성대학교)

학회지편집위원회

위 원 장 | 김종완 (삼육대학교)

부 위 원 장 |
금득규 (유한대학교), 최유주 (서울미디어대학원대학교), 오세창 (세종사이버대학교), 박중오 (성결대학교), 전정훈 (동덕여자대학교)

위 원 |
강경태 (한양대학교), 김기연 (목원대학교), 박병호 (국방부), 이준환 (극동대학교), 장상현 (KERIS), 조두산 (순천대학교), 금득규 (유엔진솔루션즈), 김영환 (전자부품연구원), 박현주 (CIoT), 이해연 (국립금오공과대학교), 전정훈 (동덕여자대학교), 최경주 (충북대학교), 김기범 (국가보안기술연구소), 김혜영 (홍익대학교), 오세창 (세종사이버대학교), 임유진 (숙명여자대학교), 정원용 (원광대학교), 김기병 (서울특별시정보시스템담당관), 김호원 (부산대학교), 윤종희 (영남대학교), 임승호 (한국외국어대학교), 조광문 (목포대학교)

JIPS 편집위원회

Editor-In-Chiefs
Jong Hyuk Park (Leading Editor) (Seoul National University of Science and Technology, Korea)
Vincenzo Loia (University of Salerno, Italy)

Executive Editors
Doo-Soon Park (Soonchunhyang University, Korea)
Young-Sik Jeong (Dongguk University, Korea)
Hamid R. Arabnia (The University of Georgia, USA)

Advisory Editor
Han-Chieh Chao (National Ilan University, Taiwan)
Jianhua Ma (Hosei University, Japan)
Laurence T. Yang (St. Francis Xavier University, Canada)
Mo-Yuen Chow (North Carolina State University, USA)
Victor Leung (The University of British Columbia, Canada)
Yang Xiao (The University of Alabama, USA)
Javier Lopez (University of Malaga, Spain)
Jiannong Cao (The Hong Kong Polytechnic University, Hong Kong)
Mohammad S. Obaidat (Fordham University, USA)
Qun Jin (Waseda University, Japan)
Witold Pedrycz (University of Alberta, Canada)

Managing Editor
Gangman Yi (Dongguk University, Korea)
Neil Y. Yen (The University of Aizu, Japan)

Senior Editors
Houcine Hassan (Universitat Politecnica de Valencia, Spain)
Kim-Kwang Raymond Choo (The University of Texas at San Antonio, USA)
Muhammad Khurram Khan (King Saud University, Kingdom of Saudi Arabia)
Naveen Chilamkurti (La Trobe University, Australia)
Youn-Hee Han (Korea University of Technology and Education, Korea)
Ka Lok Man (Xi'an Jiaotong-Liverpool University, China)
Luis Javier Garcia Villalba (Universidad Complutense de Madrid, Spain)
Muhammad Younas (Oxford Brookes University, UK)
Stefanos Gritzalis (University of the Aegean, Greece)

Associate Editor
Abderrezak Rachedi (University Paris Est, France)
Ah Young Lee (University of South Dakota, USA)
Ana Nieto Jiménez (University of Malaga, Spain)
Arun Kumar Sangaiah (VIT University, India)
BASIT SHAHZAD (King Saud University, Saudi Arabia)
Afrand Agah (West Chester University of Pennsylvania, USA)
Ali Shahrabi (Glasgow Caledonian University, UK)
Aniello Castiglione (University of Salerno, Italy)
Aziz Nasridinov (Chungbuk National University, Korea)
BeomSeok Kim (Changshin University, Korea)

Journal Secretary

컴퓨터 및 통신 시스템(KTCCS) 논문지 편집위원회

위 원 장 | 정광식 (한국방송통신대학교)

부 위 원 장 | 김용석 (서남대학교), 백상헌 (고려대학교), 이관용 (한국방송통신대학교), 이덕규 (서원대학교), 최종명 (목포대학교)

위 원 | 강윤희 (백석대학교), 공기식 (남서울대학교), 김경백 (전남대학교), 김승주 (고려대학교), 김진욱 (한국방송통신대학교), 문병인 (경북대학교), 박광진 (원광대학교), 박능수 (건국대학교), 박재성 (수원대학교), 박희완 (한라대학교), 송두희 (원광대학교), 윤종희 (영남대학교), 이태규 (원광대학교), 이화민 (순천향대학교), 이훈재 (동서대학교), 조정호 (광주대학교), 최성곤 (충북대학교), 한영선 (경일대학교), 허 경 (경인교육대학교)

소프트웨어 및 데이터 공학(KTSDE) 논문지 편집위원회

위 원 장 | 길준민 (대구가톨릭대학교)

부 위 원 장 | 김영갑 (세종대학교), 박용범 (단국대학교), 전재욱 (성균관대학교), 조용윤 (순천대학교), 한연희 (한국기술교육대학교)

위 원 | 김상근 (성결대학교), 김성석 (서경대학교), 김영철 (홍익대학교), 김우열 (대구교육대학교), 김익수 (숭실대학교), 김인택 (명지대학교), 김정아 (가톨릭관동대학교), 김종호 (순천대학교), 박기남 (고려대학교), 박상준 (군산대학교), 오세창 (세종사이버대학교), 오효정 (전북대학교), 유지환 (한국기술교육대학교), 이공주 (충남대학교), 이대원 (서경대학교), 이상곤 (전주대학교), 이성욱 (한국교통대학교), 이준호 (성균관대학교), 이현아 (금오공과대학교), 정영애 (선문대학교), 정재화 (한국방송통신대학교), 조상현 (네이버), 최종선 (숭실대학교), 한경호 (단국대학교)

2017년 5월호 특집 담당위원

특 집 위 원 | 전정훈 (동덕여자대학교)

ISSN 1226-9182

정보처리학회지 KIPS

Korea Information Processing Society Review

www.kips.or.kr

2017년 5월 | 제24권 제3호 |

KIPS

권두언

“블록체인과 관련한 기술 및 응용” 특집을 발간하며...

이번 특집호에서는 세계적인 이슈거리로 많은 관심을 보이고 있는 블록체인 기술에 대해 알아보고, 어떻게 미래를 준비해야할 지를 함께 고민해 보기 위해 “블록체인과 관련한 기술 및 응용”이라는 주제로 원고를 모집하게 되었습니다.

최근 블록체인 기술이 급부상하고 있는 가운데 유명 리서치 회사인 가트너(Gartner)의 하이프 사이클에서는 향후 유망 기술임을 전망하고 있으며, 글로벌 기업들은 여러 산업분야에 블록체인 기술을 응용할 수 있을지를 연구 및 실험 중에 있습니다.

블록체인은 가상화폐로 시작하여, 분산원장과 탈중앙화라는 블록체인만의 특징만으로도 전 세계 이슈가 되었으며, 침체된 IT분야에 떠오르는 기술로 매우 높이 평가하는 이들도 많이 생겨나고 있습니다.

그러나 이를 바라보는 시선들은 긍정적이지만은 않습니다. 가상화폐로 인한 불신과 사회적 범죄에 악용되고 있다는 영향 때문인지 많은 사람들이 발전가능성만을 보고 긍정적인 시각으로 바꾸는 데에는 다소 시간이 필요하다고 생각됩니다. 이러한 이유에서 우리는 이 시기가 어느 때 보다 긍정적인 사고와 관찰이 필요한 시기라고 생각합니다.

4차 산업혁명을 준비할 지식의 습득과 능력의 배양을 준비해야할 이때, 우리는 블록체인의 특징을 활용하고 보완하여 응용 기술로의 진화를 이루어야 할 것입니다. 이에 이번 특집호의 주제로서 매우 적절하였다고 생각됩니다.

본 특집호에서는 블록체인의 기술동향과 금융 및 사물인터넷의 향후 활용가능성을 알아보는데 중점을 두었으며, 이와 같은 노력은 향후 미래 산업과 기술을 이끌어 갈 초석을 마련해 줄 것으로 기대합니다.

아울러 4차 산업혁명을 준비해야할 우리에게 다양한 시각에서의 분석이 함께 진행되어야 함을 상기시켜 주는 기회를 갖게 되었다고 생각합니다. 특히 이번 특집호는 많은 필자들의 관심과 새로운 기술에 대한 큰 호기심을 알 수 있었으며, 미래를 준비하고자 하는 열정을 느끼고 확인할 수 있는 자리였다고 생각됩니다.

마지막으로 글을 마무리하면서 이번 특집호에 원고를 집필해주신 모든 저자들께 감사의 말씀을 전해 드리며, 많은 분들의 원고를 함께 하지 못한 저자 분들께 아쉬움과 함께 다음 기회를 약속드리겠습니다. 아울러 한국정보처리학회의 위원장님을 비롯 여러 편집위원님들과 학회 관계자 분들께도 진심으로 감사의 말씀을 전합니다.

2017년 5월

동덕여자대학교 교수 전정훈

특집 01

사물인터넷과 블록체인 기술 적용 동향

유소망 (고려대학교), 김종완 (삼육대학교)

목차

1. 서 론

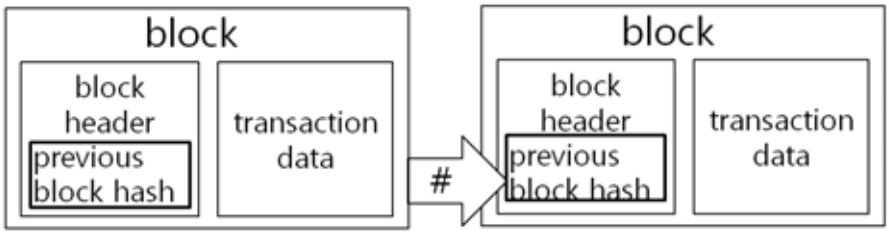
개인 간(P2P) 거래에 사용되는 암호 화폐인 비트코인(Bitcoin)은 2009년에 서비스를 시작한 이후 현재까지 거래량이 700억 달러에 이른다. 블록체인은 비트코인의 보안성에 기반이 되는 공개거래장부에 해당하며 비트코인에 적용된 블록체인은 아직까지 해킹에 노출된 적이 없는 만큼 보안에 강하다.

블록체인(Blockchain)의 보안성에 따라 최근에는 암호 화폐 뿐 아니라 공유 경제 애플리케이션, 저작권료 지급 시스템과 같이 보안성, 신뢰성이 필요한 다양한 기술에 블록체인을 적용하고 있다.

IoT는 물리적인 장비와 웹을 결합해 장비, 서비스 그리고 사용자 간의 상호작용을 활성화한다. 블록체인으로 해결할 수 있는 IoT 보안 기술에는 권한 관리, 데이터 스트림(Data Stream) 보안성 그리고 서로 다른 장비 사이의 식별 기능이 있다. 이 경우, 다음과 같은 장점이 있다. 먼저, 블록체인은 P2P 네트워크 규모에 따른 높은 데이터 신뢰성, 분산형 방식으로 많은 장비를 수용할 수 있는 확장성이 있다. 그리고 블록체인에서 공개키 인프라를 제공하기 때문에 별도의 공개키 인프라를 위한 서버 유지비용을 줄임으로써 IoT를 위한 경량의 높은 보안성을 유지할 수 있다.

하지만 블록체인이 연산을 소모하고, 네트워크 트래픽이 많이 요구되는 특성이 있어 자원이 한정된 IoT 기기에서 구동할 수 없는 한계가 있다. 또한 보안성이 작업증명이라는 채굴 조건에 따라 P2P 네트워크의 전체 연산능력에서 기인하기 때문에 규모있는 네트워크 구축의 가능성을 고려해야 한다.

이러한 맥락에서 본 논문의 구성은 다음과 같다. 2절에서 블록체인의 구조와 그에 따른 보안



(그림 1) 블록체인의 구조

성에 대해 설명한다. 3절에서는 사물인터넷에 블록체인이 적용된 연구들을 소개하며 오버레이 네트워크의 구성 방식과 그것의 최적화 방식을 소개한다. 4절에서는 P2P 네트워크 구축에 강점이 있는 스마트 컨트랙트의 응용 사례를 소개한다. 5절에서는 다양한 응용 분야를 소개하며 마지막으로 iot보안을 위한 블록체인의 추가연구를 포함한 방향을 제시하면서 6절에서 결론을 맺는다.

2. 블록체인의 구조와 보안성

이 장에서는 사물인터넷에 블록체인이 적용된 배경을 알아보기 위해 블록체인의 구조를 통해 보안성 원리를 설명한다. 미리 언급하자면, 충분한 채굴자들을 확보해 전체 블록체인 네트워크가 큰 연산 능력이 있어야 보안성을 유지할 수 있다.

2.1 블록체인의 구조

블록체인의 기본 구조는 다음과 같다. 먼저, 블록(Block)에는 (그림 1)과 같이 트랜잭션(Transaction)이라고 불리는 거래 내역이 저장된다. 블록들의 헤더(Header)는 이전 블록 데이터를 암호화하는 해시(Hash)값을 연결고리로 하는 체인 형태로 이어져있다. 또한 전체 네트워크의 모든 노드(Node)에 데이터가 중복 저장되어 있으므로 위변조가 불가능하다. 더욱이 블록은 일정 난이도를 갖고 생성되어 체인이 길어질수록 블록의 신뢰도가 증가한다.[2]

2.2 블록의 채굴 과정

거래를 위조할 수 없도록 채굴자(Miner)[1]들은 트랜잭션 내역을 수집해 검증하고 작업증명(PoW, Proof of Work)이라는 연산 능력 경쟁을 통해 블록을 생성한다. 해시 함수는 역산으로 각 출력 값에 대응하는 입력 값을 찾기 어려운 일방향(One Way) 연산을 수행한다. 이러한 특성을 이용하여 채굴자들이 서로 연산 능력을 경쟁할 수 있는 조건이 주어진다. 작업증명은 해시연산을 반복하면서 특정 난이도[2](Difficulty)가 출력 값으로 나오는 입력 값(넌스, Nonce)을 찾는 것이다. 작업 증명을 성공해 생성한 블록을 후보블록이라고 한다.

2.3 장부 내역에 대한 합의 과정

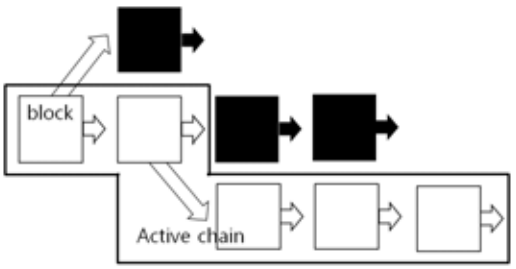
블록의 생성에 성공한 채굴자는 해당 후보 블록을 브로드캐스팅(Broadcasting)하며 이웃 채굴자는 수신한 블록을 검증한다. 검증 과정에서는 수신한 후보 블록에 포함된 트랜잭션들을 개별

1) 채굴자들은 P2P 노드로서 작업증명을 수행하여 블록을 생성한다. 비트코인에서 블록생성에 성공하는 채굴자는 새로 발행된 비트코인을 보상으로 받는다. 채굴자가 새 코인을 보상으로 받는 거래 내역도 새 블록에 포함된다.

2) 난이도는 블록 채굴의 어려운 정도를 조절하며 모든 노드가 알고 있는 전체 네트워크의 설정 값이다.

적으로 확인하고 작업증명 연산을 다시 수행한다. 후보 블록에 문제가 없으면 검증되었다는 의미로 자신의 블록체인에 포함시키고 이후에 블록체인에 저장된 데이터를 기반으로 새 블록을 채굴한다. 비트코인에서는 이 과정이 6번 반복되면 해당 블록에 포함된 거래가 승인된다.

앞서 설명한 연산 능력의 경쟁 조건을 이용해 안전하게 블록체인에 합의하기 위한 최장체인 알고리즘이 있다. 이 알고리즘에서 블록체인은 (그림 2) 와 같이 나뭇가지 모양으로 분기하며 비트코인에서는 분기된 가지 중 (그림 2)의 하얀 블록들로 표시된 부분과 같이 가장 긴 체인을 선택한다. 이때, 선택된 체인을 액티브 체인(Active Chain)이라고 부른다[1].



(그림 2) 최장체인 알고리즘

2.4 이중지불 공격과 블록체인의 보안성

블록체인을 공격하는 방법에는 대표적으로 이중지불 공격이 있다. 공격자가 가진 잔고를 한 번 사용한 뒤 해당 거래 데이터를 무력화 시키는 가짜 체인을 발표해 다시 지불에 사용하는 것이다. 공격자가 가짜 블록체인을 배포해 거래 내역을 조작하려면 네트워크가 변조된 블록을 받아들이게 해야 한다. 이를 위해서는 가장 긴 체인을 만들기 위해 빨리 블록을 만들어 전파해야 한다. 또한 가짜 체인보다 긴 체인이 생성되는 것을 막기 위해 공격자의 트랜잭션에 반하는 트랜잭션과 그것을 저장한 다른 채굴자의 블록이 승인되는 것을 막아야 한다. 따라서 이중지불 공격을 막기 위해서는 공격자가 전체 네트워크 연산 능력 중 50% 이상을 소유하고 있어야 한다.

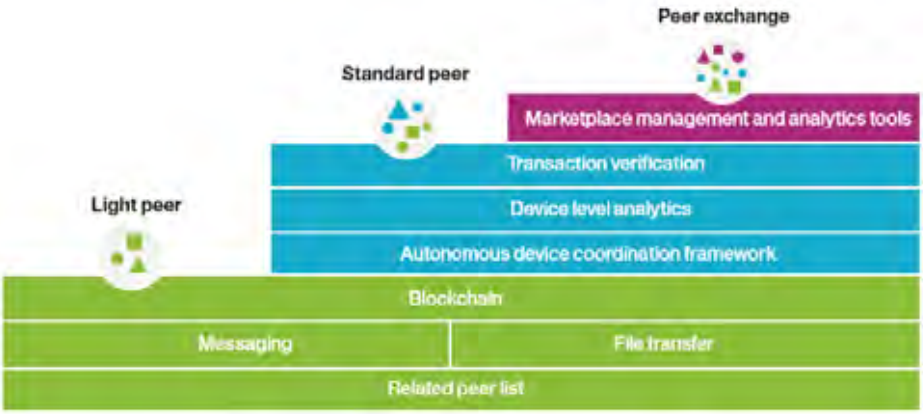
그런데 비트코인의 경우 컴퓨팅 파워(Computing Power)가 약 2800만 펩타플롭스(PetaFLOPS)가 넘는다[3]. 이는 세계에서 연산 능력이 가장 높은 슈퍼컴퓨터인 중국의 선웨이 타이후라이트(Sunway TaihuLight)가 93펩타플롭스인 것을 고려할 때 비트코인 메인 네트워크의 공격이 사실상 불가능한 것을 알 수 있다.

이와 같은 블록체인의 보안성을 적용하는 분야가 다양하다. 최근에는 암호 화폐 뿐 아니라 에어비앤비(Airbnb)와 같은 공유 경제 앱(App), 은행이나 저작권료 지급 시스템과 같이 보안성 및 신뢰성이 필요한 다양한 분야에 적용하고 있다.

3. 연산 오버헤드 문제의 해결 방안

IoT 환경에 블록체인을 적용하면 단일 서버로 IoT 기기들을 관리하는 것보다 많은 기기를 수용할 수 있고 서버가 다운될 우려가 없어 안정적이다. 하지만 블록체인이 작업증명을 수행하기 위해 해시 연산을 반복적으로 수행해 컴퓨팅 오버헤드가 크기 때문에 사물인터넷에 블록체인을 적용하려면 필연적으로 연산 오버헤드 문제를 해결해야 한다. 따라서 이 장에서 채굴의 기능을 담당하는 노드와 트랜잭션 생성을 담당하는 노드를 구분하는 해결 방법이 대표적인 해결방법을 소개한다.

블록체인을 IoT에 적용한 대표적인 사례로 어뎁트(Adept)가 있다. 블록체인을 응용해 사물인터넷 기기가 서로 직접 소통하는 P2P 네트워크를 구축하는 목적이다. 스마트 홈과 같은 환경에



(그림 3) Adept의 3가지 피어 타입[4]

서 프라이버시가 침해되거나 안전상의 위험이 없기 위해 블록체인을 사용해 IoT 기기의 설정 파일을 암호화한다.

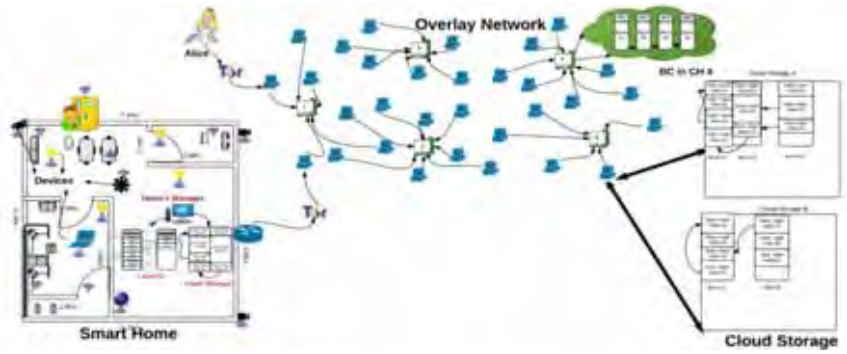
어뎁트는 (그림 3)과 같이 IoT기기의 한정된 자원으로 블록체인 기능을 사용하기 위해 채굴 기능을 하는 피어를 따로 두는 3가지의 피어 타입(Peer Type)을 제공하고 있다. 그 중 라이트 피어(Light Peer)와 스탠다드 피어(Standard Peer)는 메모리와 저장 공간이 제한적인 IoT 기기에서 블록체인을 구동해야 하는 문제를 해결하기 위한 것이다.

라이트 피어(Light Peer)는 메모리(Memory)와 저장 공간에 한계가 있는 IoT 장비에 사용되며 지갑 보유, 메세징, 트랜잭션 수행 기능을 할 수 있다. 스탠다드 피어(Standard Peer)는 라이트 피어의 기능을 포함해 트랜잭션 검증 기능을 추가적으로 수행한다[4].

[5]도 같은 방식을 사용하는데, 이것은 비트코인에서 단순지불검증3) 방식과 같다. IoT 기기에서는 트랜잭션만 수행하고 나머지 블록 채굴을 하는 기능은 일반 서버로 구성된 P2P 네트워크에서 수행한다. 논문에서는 스마트 홈(Smart Home) 사용자의 프라이버시(Privacy) 보안성과 확장성을 위해 블록체인을 적용하고 블록체인의 보안성에 대해 설명한다. DDOS 공격의 경우 모든 장비들의 트랜잭션이 채굴자에게 검사되므로 공격자로 의심되는 IoT 노드들을 차단할 수 있다. 또한 링킹 어택(Linking Attack)은 같은 공공키를 사용하는 거래들을 연결해 실제 ID를 유추하는 공격이다. 프라이버시 문제가 발생할 수 있어 채굴자가 트랜잭션 마다 다른 개인키를 사용해 해결한다.

하지만, 트랜잭션이 발생하거나 후보 블록이 생성되었을 때 브로드캐스팅(Broadcasting)하는 특성이 있어 네트워크 트래픽이 많이 발생한다. 그에 따라 [6]은 (그림 4)와 같이 네트워크 오버헤드와 지연 시간을 줄이기 위해 오버레이 노드를 클러스터로 그룹 짓는다. 각 클러스터에서는 클러스터 헤드(CH, Cluster Head) 노드를 선출한다. 클러스터 헤드는 공공키 리스트를 가지고

3) 풀 노드는 블록체인 전체를 저장하며 트랜잭션 기능과 채굴 기능을 모두 수행하지만 단순지불검증 노드는 트랜잭션 기능만 수행한다. 단순 지불검증 노드는 주로 스마트폰과 같은 자원이 한계적인 기기를 의미한다. 단순지불검증 노드는 트랜잭션 정보와 블록 헤더의 머클 루트(Root)를 가지고 풀 노드에게 머클 경로의 증명을 요청하여 해당 트랜잭션이 블록에 포함되었는지 유무를 확인할 수 있다.



(그림 4) 클러스터가 있는 오버레이 네트워크 구조[6]

블록을 생성하는 권한을 부여하고 IoT 기기의 접근을 허용한다. 또한 블록체인 데이터의 크기 문제를 해결하기 위해 블록체인 데이터를 블록 번호에 맵핑(Mapping)되도록 구성해 클라우드 스토리지(Cloud Storage)에 저장한다.

이 장에서 설명한 방식을 사용하면 블록을 채굴자들이 감소하여 전체 네트워크의 연산 능력 감소와 그에 따른 보안성의 약화의 우려가 있다. 실제로 비트코인의 경우에도 단순지불검증 노드가 가장 많다. 채굴자와 블록체인 사용자의 역할을 따로 설정하지 않고 병합하면 채굴자 네트워크를 유지하기가 수월할 것이다.

또한 블록체인의 채굴 네트워크를 구축해 단일 서버 구축 비용을 줄일 수 없다. 블록체인 기반의 암호화폐들은 채굴자들이 보상으로 발행한 화폐를 지급받는다. 하지만 외부 채굴자가 없는 프라이빗 네트워크에서 블록체인은 오히려 모든 노드가 같은 데이터를 중복 저장하며, 연산 능력 경쟁을 위해 소모적으로 작업 증명을 수행하기 때문에 단일 서버에 비해 비용이 적다고 볼 수 없다.

4. 스마트 컨트랙트와 응용

스마트 컨트랙트(Smart Contract)[7]는 블록체인에 거래 내역 뿐 아니라 변수와 함수를 저장할 수 있도록 해 블록체인을 응용할 수 있는 다양한 가능성을 열어 주목받고 있다. 이 장에서는 보안성을 제공할 수 있는 큰 규모의 프라이빗 네트워크(Private Network)[4]를 구축하지 않고 스마트 컨트랙트를 사용해 이미 구축된 퍼블릭 네트워크(Public Network)를 IoT환경에 적용하는 연구를 소개한다. 하지만 아직 매 트랜잭션이 인증되는데 소요되는 지연 시간이 있는 단점이 있다.

이더리움(Ethereum)은 블록체인을 프로그래밍할 수 있는 플랫폼(Platform)이다. 즉, 프로그래머들이 블록체인 위에서 코인(Coin)의 거래 방식을 규정할 수 있도록 스마트 컨트랙트라는 스크립트(Script)를 구동할 수 있다. 예를 들어, 스마트 컨트랙트를 가지고 클라우드 펀딩(Cloud Funding)과 같은 제3자 간의 거래를 구현할 수 있다. 그러므로 스마트 컨트랙트를 통해 블록체인의 다양한 적용 가능성이 제공된다. 또한 이더리움의 메인 네트워크(Main Network)를 사용할 수 있다는 장점이 있다.

비트코인과 이더리움에서 블록체인의 상태

4) 비트코인, 이더리움과 같은 누구나 네트워크에 참여할 수 있는 블록체인 환경을 퍼블릭 네트워크라고 한다. 반대로 하나의 기관에서 독자적으로 사용하는 블록체인 환경을 프라이빗 네트워크라고 한다. 여러 기관들이 협력해서 구성하는 블록체인 환경은 컨소시움 네트워크(Consortium Network)라고 하며, 허가된 기관만 네트워크에 참여할 수 있다.

(State)는 블록체인에 저장된 모든 변수와 그 값이다. 변수 중에는 모든 계정들이 소유한 이더리움 잔고와 컨트랙트의 내부 변수가 있다. 새 트랜잭션의 입력 값은 이전 상태이며 출력 값은 새로운 상태이다. 이더리움은 이 상태 개념을 기반으로 튜링완전성을 제공해 블록체인의 무한한 응용 가능성을 제공한다.

앨런 튜링은 튜링완전언어를 사용하며 무한한 저장공간이 있다면 이 세상의 모든 문제를 풀 수 있는 기계를 만드는 것이 가능하다고 주장했다. 이더리움에서 블록체인이 무한에 근접한 저장공간의 역할이다. 튜링완전언어는 프로세스를 분할해 아주 작은 단위로 사용할 수 있으며, 조건 설정과 반복문이 있다. 이더리움에서는 솔리디티(Solidity)라는 프로그래밍 언어를 지원한다.

비트코인에서 스크립트를 제한했던 이유는 블록체인이 무한루프에 빠지지 않게 하기 위해서이다. 이 문제를 해결하기 위해 이더리움에서는 스마트컨트랙트의 등록과 트랜잭션마다 수수료[5]가 요구된다. 하지만 이 소비를 계산하는 것도 네트워크에서 합의 과정을 거쳐야 하므로 오버헤드가 된다.

[8]은 다수의 IoT 장비에 대해 장비의 설정과 사용자 인증을 지원하며 동기화 문제없이 수용하기 위해 블록체인을 적용했으며 장비 설정 방법을 쉽게 구현하기 위해 이더리움의 스마트 컨트랙트를 적용했다. [7]에서 세터(Setter), 게터(Getter)함수를 만들어 LED, 에어컨의 설정 값을 블록체인에 저장하도록 구현했는데 이 연구는 스마트 컨트랙트를 사용한 구현이 상당히 단순하다는 것을 설명하고 있다. 하지만 이러한 방식은 12초의 트랜잭션 시간을 기다려야 한다. 또한 자원이 한정적인 IoT 장비에 블록체인을 구동할 수 없어 블록체인을 구동하는 프록시(Proxy) 역할을 하는 별도의 서버가 필요하다.

[9]는 스마트 시티(Smart City)의 주민들이 센서 모니터링을 할 때 환경 데이터에 누구나 접근 가능하지만 수정은 불가능하도록 권한을 제한하기 위해 블록체인을 적용한 CitySense시스템을 제안했다. 이 시스템은 날씨, 습도, 온도와 같은 환경 데이터를 주민들이 받아볼 때 정확한 정보를 전달하기 위해 주민들이 데이터를 수정할 수 없고 접근만 할 수 있도록 설계했다. 특히, 트랜잭션을 통해 노드 간에 통신하도록 구현하고 있으며 컨트랙트를 포함한 트랜잭션을 통해 계정 간에 메시지를 주고받을 수 있게 했다. 이 메시지는 수신자의 주소, 호출할 컨트랙트 함수, 파라미터(Parameter)의 리스트(List)를 포함한다. 스마트 컨트랙트를 이용해 센서(Sensor)로부터 메시지(Message)를 받는 함수, 정보를 다시 받아 블록체인에 저장하고 사용자의 질의를 받아 정보를 제공하는 함수를 구현했다.

5. 다양한 적용 가능성

이 장에서는 사물인터넷과 블록체인 기술이 응용된 연구들을 소개한다. 블록체인 기술은 사물인터넷 분야에서 스마트 그리드와 SD-IoT와 같이 다양한 적용가능성이 있다.

5.1 스마트 그리드

스마트 그리드(smart Grid)는 전기 및 정보통신 기술을 활용하여 전력망을 지능화·고도화한 것인데, 신재생에너지의 사용을 확대하여 소비자의 참여로 설비가 운영되면서 에너지 이용효율

5) 거래수수료는 송금자가 지불하며 해당 거래가 포함된 블록을 생성한 채굴자에게 주어진다. 이더리움에서는 가스(Gas)를 거래수수료로 사용하며 가스는 이더리움을 가지고 사고 팔 수 있다.

을 극대화하는 전력망이다 [10]. 스마트그리드에 블록체인을 적용하면 비용을 줄이면서 안정성 있는 관리 시스템을 구축 수 있다.

(그림 5) 비중앙집중형 스마트그리드[10]

골드만 삭스(Goldman Sachs)의 보고서에서 블록체인을 스마트 그리드(Smart Grid)에 적용할 것을 제안했다. (그림 5)와 같이 에너지(Energy) 생산자가 소비자인 양방향식 환경을 구성한다. 비중앙집중적인 시스템을 통해 전력 중개자의 비용을 줄이며 안정성 있는 에너지 마켓을 만들 수 있다는 장점이 있다 [11].

DeviceChain[12]은 이러한 접근 방법의 프로토타입 구현을 위해 블록체인을 이용해 스마트그리드 기기를 인증하는 방식을 제안했다. DeviceChain은 AMI 6)기기 인증 내용을 블록체인에 저장하고 검침 서버들이 블록을 검증한다. 기존의 PKI(Publick Key Infrastructure, 공개 키 인프라)는 최소 4단계를 거쳐 인증처리를 하고 서버도 용도에 맞게 독립적으로 4개 이상이 필요하다. 이에 반해 DeviceChain은 서버와 기기 간에만 일어나는 절차로 비교적 간단하다.

구현에는 비트코인 테스트넷(Testnet)을 사용했다. 테스트넷은 개발자들이 실제 비트코인을 소유하지 않으며 메인 블록체인을 망가뜨릴 위험 없이 비트코인을 테스트할 수 있는 별도의 블록체인이다. 이러한 구현 방식은 블록에 트랜잭션들이 저장되고 남는 여유 데이터 공간이 한계적이기 때문에 비트코인을 커스터마이징(Customizing)하는 데 한계가 있다. 또한 비트코인이 메인 네트워크를 사용하는 것이 아니므로 전체 네트워크의 연산 능력을 유지하는 비용이 많이 소요되며 네트워크 규모가 작을수록 보안성이 약화된다. 따라서 적절한 네트워크 구성 방식이 연구될 필요성이 있다.

5.2 네트워크 관리 보안성

소프트웨어 정의 네트워크(SDN, Software Defined Networking)는 트래픽(Traffic) 목적지를 결정하는 컨트롤 플래인(Control plain)과 포워딩(Forwarding)을 담당하는 데이터 플래인(Data Plain)을 분리함으로써 네트워크 관리를 추상화한다. 그에 따라 SDN의 네트워크 관리 가능성에 보안성을 결합하는 장점이 있다.

(그림 6) SD-IoT에서 가상 자원[13]

SDN을 IoT에 적용한 것을 SD-IoT라고 하며 이는 가상 자원을 노출 시켜 장비의 권한 관리와

6) AMI(Advanced Metering Infrastructure, 원격검침인프라)는 스마트 미터(smart meter)에서 측정한 전력 사용량 데이터를 전송해 원격에서 전력 사용을 분석하는 기술이다.

IoT 컴포넌트의 커스터마이징을 쉽게 한다. [13]는 (그림 6)과 같이 클라우드 상에서 Bluemix 플랫폼을 사용해 블록체인으로 가상 자원을 허가받을 수 있는 시스템을 제안했다.

5.3 사물인터넷 기기 관리의 보안성

[14]는 사물인터넷 기기의 소유자가 프라이버시를 침해 받지 않고 센서 데이터를 판매해 수수료를 받을 수 있는 ChainAnchor 시스템을 제안한다. 블록체인에서 각 사용자에게 해쉬 값 기반의 공공키가 아이디로 부여되며 트랜잭션에 사용된다. 익명성을 사용해 기기 소유자의 프라이버시를 보호한다는 장점이 있다.

[15]는 펌웨어 기기를 블록체인을 통해 안전하게 업데이트 할 수 있는 시스템을 제안한다. 펌웨어 기기가 블록체인 노드에 업데이트를 요청하면, 블록체인 노드는 해당 기기의 업데이트 여부를 확인한다. 기기가 최신 버전으로 업데이트 되지 않은 경우 블록체인 노드가 최신 펌웨어의 피어 리스트를 제공한다. 그 다음 업데이트를 요청한 노드는 최신 펌웨어를 가진 노드에게 다운로드를 받는다. 반대로 최신 버전의 펌웨어가 업데이트 요청을 한 경우에는 펌웨어가 검증되고 해당 노드가 최신 피어 리스트에 추가된다. 펌웨어의 완전성(integrity)과 최신 버전의 업데이트 여부를 검증하는 보안적인 장점이 있지만 취약성과 버그의 진단은 포함하지 않는다.

사물인터넷 기기 관리의 보안성에 블록체인을 적용한 방식들은 각 사물인터넷 기기가 주기적으로 블록체인에 트랜잭션을 생성한다는 공통점이 있다. 하지만 블록체인은 한 블록에 저장될 수 있는 트랜잭션 데이터의 양의 제한이 있다. 트랜잭션 처리량을 늘이기 위해 블록을 크게 만들면 블록을 브로드캐스팅하기 때문에 네트워크 트래픽이 증가하며, 스토리지의 블록체인 크기가 증가하는 트레이드 오프(trade off)가 있다. 따라서 사물인터넷 기기가 생성하는 트랜잭션을 효율적으로 수용할 수 있는 연구가 필요하다.

6. 결론 및 향후 전망

본 논문에서는 사물인터넷의 보안을 위해 사용된 블로체인의 응용과 연구를 조사했다. 블록체인은 IoT 기기의 인증, 설정, 센서 데이터 교환의 보안 등을 위해 사용되고 있다. 이는 블록체인이 제공하는 장부의 신뢰성에 의한 보안성, 분산형 방식으로 많은 장비를 수용할 수 있는 확장성, 공개키 인프라로 인한 낮은 서버 유지비용 그리고 생산자와 소비자가 소통하는 양방향 시스템 구성의 장점을 이용한 것이다.

사물인터넷과 관련된 보안 기능을 신속하게 지원하기 위해 트랜잭션 검증 시간의 지연 문제를 해결하는 연구가 필요하다. 또한 IoT 보안 기능을 위해 공격자가 데이터를 위조할 수 없게 하기 위해서는 공격자가 연산 능력의 과반을 소유하는 것을 막아야 한다. 그러므로 블록체인 네트워크의 규모를 유지할 수 있는 연구가 지속적으로 필요하다. 예를 들어, 큰 규모의 채굴 네트워크를 유지하기 위해서는 자원이 한정적인 기기에서 블록체인을 구동할 수 있도록 CPU 자원을 많이 소모하는 작업 증명은 지분 증명(PoS, Proof of Stake)[7]과 같이 낮은 CPU 자원을 소모하는 증명 방법의 적용에 대한 연구도 추가되어야 한다. 마지막으로 블록체인의 트랜잭션 처리량을 늘려서 사물인터넷이 생성하는 데이터를 수용할 수 있는 연구도 필요하다.

7) 계산능력이 아닌 각 노드의 지분 보유량에 따라 합의 결정권이 달라져 작업 증명의 과도한 CPU 소모를 피할 수 있다.

참 고 문 헌

[1] Nakamoto, Satoshi. “Bitcoin: A peer-to-peer electronic cash system”, 2008년.

[2] 이혁준, 이수미. “비트코인의 신뢰구조와 이중지불의 위협” 정보보호학회지. 2016년.

[3] 비트코인 차트, http://www.vnbitcoin.org/bitcoincharts.php

[4] IBM, https://www-935.ibm.com/services /multimedia/GBE03662USEN.pdf

[5] Dorri, Ali, et al. “Blockchain for IoT security and privacy: The case study of a smart home.” Pervasive Computing and Communications Workshops (PerCom Workshops), 2017년.

[6] Dorri, Ali, Salil S. Kanhere, and Raja Jurdak. “Towards an Optimized BlockChain for IoT.” Proceedings of the Second International Conference on Internet-of-Things Design and Implementation. ACM, 2017년.

[7] Wood, Gavin. “Ethereum: A secure decentralised generalised transaction ledger.” Ethereum Project Yellow Paper , 2014년.

[8] Huh, Seyoung, Sangrae Cho, and Soohyung Kim. “Managing IoT devices using blockchain platform.” Advanced Communication Technology (ICACT), 2017 19th International Conference on. IEEE, 2017년.

[9] Ibba, Simona, et al. “CitySense: blockchain-oriented smart cities.” Proceedings of the XP2017 Scientific Workshops. ACM, 2017년.

[10] 한국전력공사, http://home.kepco.co.kr/kepco/KO/C/htmlView/KOCDHP001.do?menuCd=FN05030501

[11] Goldman Sachs, Blockchain Putting Theory into Practice, pp.25-32, the-blockchain.com, 2016년.

[12] 이성훈, 김광조. “블록체인을 이용한 스마트 그리드 시스템의 기기 인증 방안”, 한국통신학회 하계종합학술발표회. 한국통신학회, 2016년.

[13] Samaniego, Mayra, and Ralph Deters. “Using Blockchain to push Software-Defined IoT Components onto Edge Hosts.” Proceedings of the International Conference on Big Data and Advanced Wireless Technologies. ACM, 2016년.

[14] Thomas Hardjono, Ned Smith. ”Cloud-based commissioning of constrained devices using permissioned blockchains.“ IoTPTS '16 Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security. ACM, 2016년.

[15] Boohyung Lee, Jong-Hyouk Lee. “Blockchain-based secure firmware update for embedded devices in an Internet of Things environment.” The Journal of Supercomputing. Springer, 2017년.

저 자 약 력

유 소 망

이메일 : somang4819@gmail.com

- 2011년~2015년 동덕여자대학교 문헌정보학과 (학사)
- 2015년~2017년 고려대학교 컴퓨터학과 (석사)
- 관심분야 : 블록체인, 핀테크

김 종 완

이메일 : kimj@syu.ac.kr

- 현재 삼육대학교 교양대학 조교수 (컴퓨터과학전공)
- 관심분야 : 빅데이터, Skyline, IoT응용

특집 02

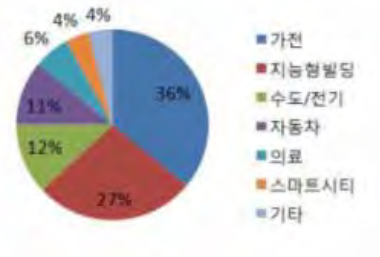
블록체인 기반의 IoT 보안 취약점

박현정 · 양혜임 · 전정훈 (동덕여자대학교)

목차

1. 서 론

최근 시장조사기관 가트너(gartner)에서는 2017년 세계 IoT(internet of things) 기기가 84억대에 달할 것이라고 예상하였다[1]. 이런 전망에 힘입어 금년 미래창조과학부는 블록체인과 IoT분야에 총 40억 원을 투자하고, 대학IT연구센터 신규 지원을 하는 등 여러 정책을 선보이고 있다[2]. 뿐만 아니라 Machina Research의 2011년도 자료에 따르면 2020년에 분야별 IoT 기기의 수는 (그림 1)과 같이 가전, 지능형 빌딩 등 다양한 분야로 확대 적용 될 것으로 기대된다[3].



(그림 1) 분야별 IoT 연결 수(2020)

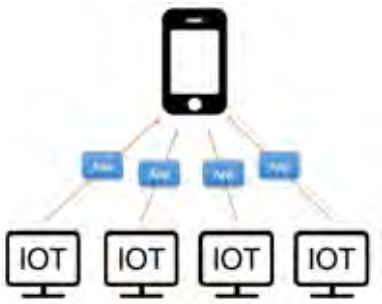
이에 따라 IoT 보안에 대한 관심 또한 높아지고 있으며, 여러 기업들이 블록체인 기술을 기반으로 IoT 기기의 보안성을 끌어올리기 위하여 노력하고 있다. 그러나 블록체인 기반의 IoT 기술을 개발할 때 각 기술의 특성이 결합하면서 새로운 취약점이 발생한다. 특히 IoT기기는 실생활과 밀접한 경우가 많기 때문에 기기의 취약점은 큰 문제로 이어질 수 있다. 따라서 블록체인과 IoT의 결합이 시너지 효과를 일으킬 수 있도록 취약점에 대한 보완방법이 필요한 실정이다. 그러므로 본 논문에서는 현재 각광받고 있는 IoT과 블록체인의 각 특성 및 보안 취약점뿐만 아니라 두 기술의 결합에 따른 문제점과 이러한 문제점을 해결하기 위한 대응 방안들을 알아본다. 먼저 2장에서는 기술의 보안 취약점들을 알아보고, 3장은 보완 기술, 4장에서는 결론으로 글을 마무리하도록 한다.

2. 블록체인과 IoT의 동향과 취약점

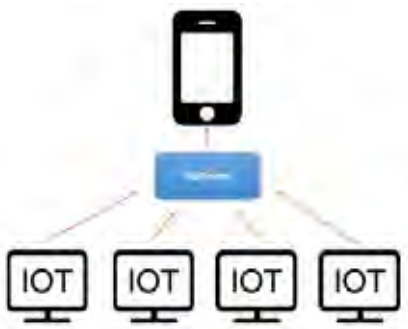
2.1 블록체인 기반 IoT의 기술 동향

2015년 초, 삼성은 IBM과 함께 블록체인(blockchain) 기반 IoT 플랫폼(platform) 어뎁트(ADEPT, Autonomous Decentralized Peer-to-Peer Telemetry)를 개발하였다. 이전의 IoT 환경은 (그림 2)처럼 각 IoT기기를 서로 다른 어플리케이션을 사용하여 제어하였다.

그러나 새롭게 개발된 IoT 플랫폼은 (그림 3)과 같이 여러 IoT기기와 핸드폰을 연결하여 사용자에게 편리한 환경을 제공한다. 여러 IoT 플랫폼들 중 어뎁트는 블록체인 아키텍처와 텔레해시 프로토콜, 비트토렌트 프로토콜 등을 결합하여 개발되었다[4]. IoT 플랫폼 외에도 스타트업 회사인 Ubirch가 2017 MWC에서 블록체인 기반의 IoT 기기를 개발하여 요트의 온·습도 값을 실시간으로 블록체인에 기록하는 등의 기술을 선보인 바 있다[5]. 이처럼 최근 블록체인 기반의 IoT에 대하여 다양한 연구가 진행되고 있는 상황이다.



(그림 2) 기존의 IoT 환경



(그림 3) Platform을 활용한 IoT 환경

2.2 블록체인 기술

블록체인의 보안 취약점에 대해 언급하기 전에 우선 블록체인의 특징과 원리를 알아본다. 블록체인은 '공공 거래 장부'라고도 부르며 가상화폐로 거래할 때 발생할 수 있는 공격에 대응이 가능한 기술로 알려져 있다[6].

블록체인은 거래가 발생할 때마다 거래 내역을 서비스 참여자 모두에게 전송하고 전체 이용자가 보관하는 분산장부 형식을 띈다. 그리고 거래 내역은 (그림 4)와 같이 블록 형태로 저장되며 블록은 헤더(header)와 바디(body)로 이루어져 있다. 헤더는 버전, 이전 블록의 해시(hash), 페이로드(payload), 시간 등을 기록하고 바디에는 거래 정보 등 주요한 데이터를 저장한다. 블록이 생성될 때마다 기존의 블록에 이어 연결되

(그림 4) 블록의 구조

(그림 5) 블록 연결 에러 예시

고, 새로 추가되는 블록에는 앞 블록의 내용이 포함되므로 이전에 연결된 블록의 경우 수정이 불가능하다. 예를 들어 (그림 5)에서 Block2의 두 번째 트랜잭션이 누군가에 의해 변경되었다면 헤더에 있는 haskMerkleBlock 값은 블록 바디에 있는 트랜잭션들을 머클 해시(merklehash)한 값이므로 변경한 이는 hashMerkleBlock의 값도 변경해야 한다. 그러나 Block2의 헤더는 Block3의 hashPrevBlock값이 되기 때문에 Block2의 바디 내용을 변경하기 위해서는 Block2 이후 모든 블록을 수정해야 한다. 또한, 블록체인은 분산장부의 형식을 가지기 때문에 트랜잭션을 완벽하게 변경하기 위해 모든 서비스 사용자의 블록을 수정해야 한다. 그러나 이는 사실상 불가능하기 때문에 결과적으로 블록체인은 거래 내역에 대한 무결성을 유지할 수 있다. 이와 같은 특성에 의해 블록체인은 보안성이 높은 기술로 인정받고 있다.

2.3 IoT의 보안 취약점

본 절에서는 IoT의 특성에 의해 발생하는 취약점에 대해 알아본다. IoT는 각종 사물에 센서(sensor)와 통신 기능을 내장하여 인터넷에 연결하는 기술을 의미한다. 최근 IoT 기기의 수요가 늘면서 생활 속 깊은 곳까지 맞닿아 있게 되었다. 이와 같은 상황에서 2016년 2월, 전 세계 약 7만 3000여개의 CCTV가 해킹되어 실시간으로 인터넷상에 생중계 되는 사건이 발생하였다. 이 사건에서 해커는 직장과 학원, 헬스장, 음식점 등에 설치된 웹캠 영상을 관리자나 촬영 대상자의 동의 없이 인터넷상에 공개한바 있다[7]. IoT에는 사용자의 사생활에 깊게 관여하는 기기들이 다수 존재하고 있어, 개인정보가 유출될 경우 큰 피해가 발생한다. 또한 해킹 공격이 발생했을 때 일반 소비자가 피해를 즉시 알아채고 확인하는 것이 쉽지 않아 더욱 취약하며 IoT 기기 사이의 통신이 무선으로 이루어지므로 유선 통신 IT기기에 비해 연결이 안정적이지 않다. 또한, IoT 서비스에서 사용하는 통신 기술의 경우, 표준이 정해지지 않아 네트워크 구조가 복잡하게 형성되어 있어, 현재 이종 네트워크 간의 상호 연동 과정에서 일정 보안 수준을 유지하는 것이 어려운 실정이다[8]. 이 외에도 간단한 기능만 탑재된 IoT 단말의 경우, 자체의 성능이 좋지 않기 때문에

개별적인 보안 SW와 같은 고도의 보안 솔루션을 도입하기가 어렵고[8], 배포 및 설치 후에는 보안 패치 등의 업데이트가 사실상 불가능하거나 큰 비용이 수반된다는 취약점들을 포함하고 있다[9].

2.4 블록체인의 보안 취약점

앞서 언급한 바와 같이 블록체인은 보안 요소 중 하나인 무결성을 높게 보장하지만, 몇 가지 특징으로 인해 보안에 취약한 부분이 존재한다. 본 절에서는 그 중 3가지 취약점에 대해 알아본다.

첫째, 기본 블록체인의 경우 콘텐츠와 레코드 자체는 암호화하지 않거나 쉽게 해독할 수 있는 형태로 이루어져 있고, 분산 장부 형식으로 인해 거래에 참여한 모든 이가 블록의 내용을 볼 수 있게 된다. 따라서 해커가 거래 참여자 중 한명의 컴퓨터를 해킹하여 블록을 획득할 경우, 해커는 콘텐츠와 레코드의 내용을 쉽게 볼 수 있게 된다. 이때 해커가 블록의 주소 소유자를 알게 될 경우, 블록 생성자 정보를 추가로 획득하게 된다. 이는 기밀성을 유지할 수 없게 되는 취약점이 발생함을 의미한다[10]. 이와 같은 상황에서 블록에 개인정보가 저장되어 있을 경우 개인정보가 유출되는 상황이 발생한다. 따라서 현재의 블록체인은 콘텐츠가 유출되더라도 영향이 크지 않도록 사생활과 직접적으로 연관이 없는 데이터만 들어가야 한다는 단점이 존재한다.

둘째, 블록체인의 '수정 불가' 특징에 의해 취약점이 발생하게 된다. 앞서 언급한 바와 같이 블록체인에 연결된 블록은 수정이 불가능하다. 이러한 특징은 높은 보안성을 보장하지만, 오류나 실수에 의해 잘못 작성된 블록 또한 수정할 수 없다는 문제점을 가지고 있다. 잘못 작성된 블록들은 모든 참여자에게 전달되고 결과적으로 네트워크 전역에 잘못된 데이터가 저장되게 된다[11]. 수정 불가 특징에 의해 잘못된 트랜잭션 처리 등의 문제가 발생하게 된다.

마지막으로, 거래 검색의 속도가 저하되는 문제가 발생한다. 블록체인의 경우, 전체를 검증하기 위해서는 모든 블록이 필요하기 때문에 블록체인의 첫 노드부터 마지막 노드까지 모두 저장된다. 따라서 비트코인의 경우 현재 130GB의 블록체인이 누적되어 있고 월 평균 3.9GB의 증가율을 보이고 있으며[12], 거래가 지속되면서 블록체인의 크기는 계속 증가하고 있다. 이때 거래 내역을 확인하기 위해서는 전체 데이터 내에서 차례로 검색해야한다. 현재는 검색 기능에 문제가 발생하지 않았지만 블록의 양이 증가할수록 원하는 트랜잭션을 검색하는 속도가 저하될 것임을 쉽게 유추해 볼 수 있다. 이는 블록체인 사용에 있어서 가용성이 떨어지는 취약점이 발생함을 의미한다.

앞서 언급한바와 같이 블록체인은 위·변조가 불가능하기 때문에 높은 무결성을 가지고 있지만 데이터의 암호화를 제공하지 않아 기밀성이 결여되어 있고, 저장 공간 부족 문제에 의해 가용성이 저하되는 취약점을 가지고 있다. 이밖에도 데이터 수정의 어려움과 같은 부분으로 인해 기술이 다양한 분야에 적용되지 못하고 있다.

2.5 블록체인 기반의 IoT 보안 취약점

최근 글로벌 기업들은 블록체인 기술을 IoT를 비롯한 여러 산업분야에 보안성을 향상시킬 목적으로 활용하는데 노력을 기울이고 있다. 따라서 본 절에서는 기술 적용 시 고려되어야 할 보안 취약점들을 알아본다. 블록체인을 기반으로 하는 IoT 기기의 경우, 기기는 레코드 내용을 블록의 바디 내부에 저장한다. 앞서 2.2절에서 언

급되었던 블록체인의 취약점에 따르면, 블록체인 특성상 IoT 기기에서 받아온 사용자의 사생활 정보들은 암호화를 전혀 하지 않고 블록 내부에 들어간다. 추가적인 보안 솔루션을 도입하려 해도 IoT 기기 자체의 성능이 좋지 않을 뿐만 아니라 비용적인 측면에서도 많은 오버헤드가 발생한다. 이러한 이유로 인해 해커가 블록을 탈취한다면 손쉽게 사용자에 대한 정보를 얻을 수 있게 된다. 또한, IoT 기기는 불안정한 네트워크 환경을 가지고 있어 통신을 하여 받아오는 값이 정확하다는 보장을 하기 어렵다. 2.3절에서 언급했듯이 IoT 기기는 저성능일 뿐만 아니라 통신 기술 표준 부재와 같은 문제가 있기 때문이다. 그러나 블록 체이닝 이후 데이터의 오류를 발견한다면 블록체인의 특성에 따라 실수를 되돌리는 것은 불가능하다. 해커는 이 점을 이용하여 복잡한 네트워크 구조를 통해 기기에 접근한 뒤 악의적으로 기존의 값과 다른 값을 줄 수 있으며, 사용자는 해킹 당한 사실을 알게 되더라도 이미 잘못 생성된 정보를 변경할 수 없게 된다. 이 외에도 IoT 기기의 데이터 검색 성능 부족에 대한 단점이 존재한다. IoT 기기 내부의 컴퓨터는 최소의 비용으로 필요한 연산만 수행하기 때문에 블록체인 내부의 데이터를 검색하려 할 경우 검색 속도가 매우 느리거나 검색이 사실상 불가능할 수도 있다. 그러나 블록체인 기술을 IoT와 결합할 경우, 사용자는 IoT기기의 센서가 측정한 데이터를 확인할 수 있어야 하기 때문에 이에 대한 해결책이 필요하다. 결과적으로 블록체인 기술을 IoT분야에 적용할 경우, 앞서 언급한 보안 취약점으로 인한 문제가 발생할 뿐만 아니라, 보안 취약점들과 연관된 복합적인 취약점들이 발생할 가능성이 있다.

3. 대응 기술

3.1 블록 암호화

개인정보 유출의 경우, 블록체인 내의 데이터에 대한 보안성을 철저하게 유지해야 한다. 기존의 블록체인은 헤더 부분만 해시하여 저장하고 바디 부분은 정보를 그대로 저장한다. 그런데, IoT기기의 경우 기기 특성에 따라 데이터에 개인정보가 입력될 수밖에 없으므로 보안 위험을 방지하기 위하여 내부의 데이터 또한 암호화가 필요하다. 이와 같은 점을 보완하기 위하여 스타트업 기업 Ubirch는 데이터를 블록에 기록할 때 독자적인 공개 키 암호 방식을 사용하여 각 IoT 센서들이 Ubirch로 데이터를 보낼 때 발생할 수 있는 해킹의 위협을 차단하였다. 그러나 위 문단에서 언급한 내용을 제외하면 블록체인 암호화에 대한 연구는 미흡한 실정이다. 블록체인은 높은 무결성을 갖지만 기밀성은 제공하지 않기 때문이다. 보통 IoT 기기의 보안성을 강화하는 경우 MQTT와 SSL/TLS를 사용하는데[13], SSL/TLS는 대칭키 암호화 방식을 채택하여 기밀성을 보장할 뿐만 아니라 해시 알고리즘을 사용하여 무결성 또한 보장한다. 따라서 블록체인 기반 IoT기기를 상용화하기 위해서는 블록 바디의 콘텐츠를 암호화하여 기밀성을 보장하는 방안에 대해 더 많은 연구가 필요하다.

3.2 데이터의 신뢰성 보장

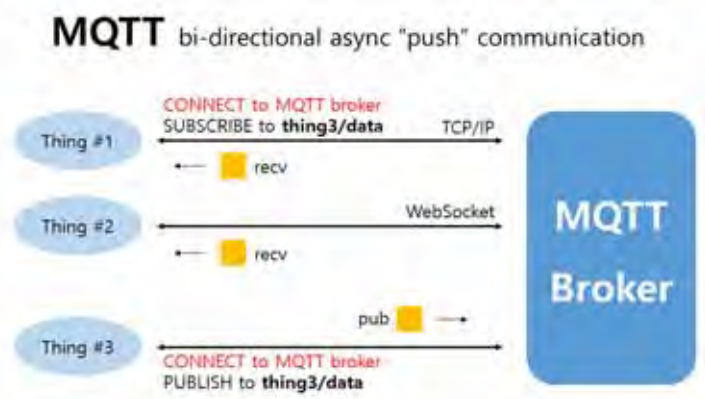
블록체인에 오류 또는 변조된 데이터가 들어가는 경우를 방지하기 위해서 데이터는 반드시 신뢰성이 보장되어야 한다. 원본 데이터가 변경되거나 소실되는 것을 막기 위하여 TCP 환경을 제공하는 IoT 프로토콜을 사용한다. 연결지향성

프로토콜을 이용하여 통신한다면 전송 도중 발생할 수 있는 오류를 확인하고 수정할 수 있다. 그러나 현재 IoT의 '저 전력', '저성능', '저가형' 등의 특성에 의해 모든 프로토콜이 TCP 환경을 제공하지는 않는다. 따라서 현재 존재하는 여러 IoT 프로토콜 중 (그림 6)의 MQTT와 같은 프로토콜의 사용이 필요하다.

MQTT는 (그림 6)에서 볼 수 있듯 토픽을 발행하는 기기(Thing #3)와 토픽을 구독하는 기기(Thing #1)들이 MQTT Broker에 연결되어 통신을 하게 되는데, 이때 통신이 TCP/IP환경에서 실행되어 전송 중 데이터에 발생한 오류를 발견하게 된다. 또한, IoT기기에 여러 개의 센서를 부착해 각 센서가 기기의 상태에 대해 정확한 데이터를 생성하고 있는지 판단하도록 하여 데이터의 신뢰성을 보장할 수 있다. 즉, 같은 행동을 하는 여러 개의 센서를 부착하여 그 센서들의 값이 모두 같은지 확인하도록 하는 것이다. 그 예로 농기계 업체 존 디어(John Deere)의 제품인 이그제트이머지(ExactEmerge) 플랜터(파종하는 트랙터 뒤에서 땅을 다지는 기계)에는 얼마나 많은 씨를 얼마나 빠른 속도로 파종했는지 측정하는 3개의 센서가 존재한다. 이 센서들을 통해 기기는 스스로 제대로 작동하고 있는지 감지하게 된다[14]. 앞에서 언급한 방법을 통해 데이터를 한번 검증한 뒤에 블록체인에 저장한다면 그렇지 않은 경우에 비해 데이터의 신뢰성이 크게 증가한다.

3.3 블록 사이즈의 확장

블록체인은 거래가 승인되거나 원본 데이터가 갱신될 때마다 블록이 추가되기 때문에 블록의 양이 지속적으로 증가하며, 블록 바디의 내용 검색 시 생성된 블록의 전수 검사가 필요하다는 특징을 지닌다. 그러나 IoT 환경의 경우 '저 전력', '저성능'의 특징을 가지고 있기 때문에 블록체인을 활용한 IoT기기에서 성능 및 저장 공간의 부족으로 인하여 메모리에 대한 오버헤드가 발생할 뿐만 아니라 실시간으로 데이터를 확인하지 못하는 가용성 문제점이 발생하게 된다. 따라서 IoT 기기의 보안에 블록체인을 사용하기 위해서는 대표적으로 블록 자체의 사이즈를 확장하는 방법이 있다. 이 방법은 블록이 생성되는 개수가 줄어들어 검색 시간도 짧아지기 때문에 가용성 문제의 해결책이 될 수 있다. 블록 사이즈의 확장은 실제로 논의되고 있는데, 2017년 8월 블록체인을 활용한 비트코인이 부상하면서 세계에서 발생하는 거래량이 크게 증가하여 당시 블록 크



(그림 6) MQTT 프로토콜의 전송 방식

기로 감당할 수 없는 상황이 발생하였다. 이에 비트코인 측은 블록 사이즈 확장에 대해 검토하고 있다[15]. 언급한 해결방법을 채택할 경우 블록의 총 개수가 적어지게 되어 거래 정보 검색 시간 감소에 긍정적인 영향을 주게 된다. 다음으로 최근 새롭게 적용된 방법인 세그윗(segwit)을 이용해 검색 속도를 증가시킬 수 있다. 세그윗은 블록의 트랜잭션에 존재하는 전자서명을 위한 공간을 제거하여 한 블록에 더 많은 트랜잭션을 저장할 수 있도록 하는 기능이다. 이 기능을 사용할 경우, 블록의 크기를 증가시킨 것과 같은 효과를 주게 되므로 검색 속도 저하 및 용량 부족의 해결책이 될 수 있다[16]. 따라서 본 절의 방법을 고려한다면 '저 성능'의 IoT 기기에서도 블록체인 기술을 충분히 사용할 수 있을 것으로 기대된다.

3.4 기술의 표준화

현재 블록체인과 IoT 기술에는 공통 표준이 없는 상태이다. 따라서 각 기업들은 두 기술을 기반으로 하는 아이템을 독자적으로 개발하고 있다. 그러나 이와 같은 현상이 지속된다면 각 산업의 발전에 부정적인 영향을 미칠 수 있다. 이에 따라 블록체인의 표준화를 위하여 2015년 9월 70개 이상의 금융 기관으로 이루어진 세계 최대의 블록체인 컨소시엄 'R3CEV'가 결성되었고[17], 작년부터는 W3C Blockchain CG과 ISO TC 307에서 블록체인의 국제표준화가 시작되었다[18]. 현재는 아마존, 마이크로소프트 등 큰 기업들이 블록체인 기술에 큰 관심을 가지고 독자적인 시스템을 개발하고 있다[19]. 또한, IoT의 경우에도 현재 오픈 커넥티비티 재단과 오픈 인터커넥트 컨소시움이 표준을 정하기 위하여 노력하고 있으며, IEEE의 IEEE p2413 표준 또한 IoT 아키텍처 정의를 위한 통합적인 방법론을 제공할 것으로 기대된다[20]. 이와 같이 IoT와 블록체인 영역에서 표준이 명확하게 정해진다면 현재 금융권에만 한정되게 이용되고 있는 블록체인 기술과 생활 곳곳의 IoT 기기를 안정적으로 접목할 수 있게 될 것이며, 블록체인을 기반으로 한 IoT 기술이 시장에 더 빠르게 자리 잡게 될 것이다.

4. 결론 및 향후 전망

최근 IoT 기기의 수요가 늘어남에 따라 이에 따른 보안 위협이 대두되고 있는 가운데, '합의 수렴 알고리즘'을 기반으로 하는 블록체인 아키텍처가 무결성을 강력하게 보장하는 새로운 기술로 제안되고 있다. 이와 같은 상황을 바탕으로 많은 기업들이 IoT 기기의 보안성 향상을 위해 블록체인 기반의 IoT 기술에 투자하고 있다. 그러나 더 높은 수준의 보안을 위해 IoT와 블록체인 기술이 결합될 때 발생할 수 있는 취약점에 대한 논의가 필요하다. 따라서 본 논문에서는 새로운 기술로 각광받고 있는 블록체인을 IoT에 적용시키며 특히 문제가 될 수 있는 세 가지 취약점과, 이에 대응할 수 있는 세 가지 방법을 제시하였고, 위 내용에서 현재의 블록체인 기술이 IoT 보안을 담당하기에는 기밀성, 가용성의 부족과 같은 취약부분들이 나타나고 있음을 알 수 있었다.

결과적으로 블록체인을 IoT 보안에 활용하기 위해서는 개인정보 유출 위험성, 데이터 오류의 위험성, 스토리지 부족 문제 등과 같은 취약점에 대해 좀 더 많은 연구가 필요하며, 향후 이와 같은 연구가 지속적이고 구체적으로 이뤄진다면, 블록체인을 기반으로 한 IoT 산업은 아주 빠르

고도 안전하게 성장하여 4차 산업혁명의 기폭제가 될 것으로 기대한다.

참 고 문 헌

[1] Rob van der Meulen, “Gartner Says 8.4 Billion Connected ‘Things’ Will Be in Use in 2017, Up 31 Percent From 2016,” Gartner, 2017.

[2] 김현아, “블록체인, 보안 넘어 IoT 인프라로..미래부, 올해 첫 30억 투자”, 이데일리, 2017.

[3] maru, “사물인터넷 가전관련 특허 아이디어, 신제품으로 속속 출시”, 디자인 로그, 2014.

[4] IBM ADEPT Practictioner Perspective - Pre Publication Draft - 7 Jan 2015, https://www.scribd.com/doc/252917347/IBM-ADEPT-Practictioner-Perspective-Pre-Publication-Draft-7-Jan-2015.

[5] Amy Nordrum, “Mobile World Congress 2017: Startup Ubirch Sails the Blockchain Into a New Application—IoT”, IEEE SPECTRUM, 2017.

[6] 이제영, “블록체인(Blockchain) 기술 동향과 시사점”, 동향과 이슈, 2017.

[7] 장우진, “IoT 보안 동향과 기술”, 공개SW포털, 2016.

[8] KISA, “사물인터넷 보안 위협 동향”, 2014

[9] 정용식, 차재상 “IoT 디바이스 보안 점검 기준”, 2017년 한국통신학회지(정보와통신) 34(2), pp 27-33.

[10] 박수민, 홍승필, “P2P 분산 네트워크 환경 내 프라이버시 및 정보보호 방안 - 블록체인 중심으로 -”, 보안공학연구논문지 Vol. 14 No. 2(2017), p170.

[11] 조수환, “사물 인터넷 데이터 무결성 보장을 위한 블록체인 기반의 합의 방법”, 고려대학교 컴퓨터학과 소프트웨어전공 석사학위논문, 2017년 7월, p17.

[12] 유소망, “Stateprune: reduce blockchain size by chainstate based block pruning”, 서강대학교 컴퓨터학과 공학석사 학위논문, 2016년 12월, p2.

[13] 정진희, 조대호, “무선 환경에서 SSL/TLS를 사용하는 IoT의 에너지 효율성 향상을 위한 기법”, 정보보호학회논문지 Vol. 26, No. 3 2016.06, pp 661-666.

[14] Stephen Lawson, “센서의 ‘벌레’, 저질 IoT 데이터로 일어나는 문제들”, CIO, 2016.

[15] 김흥록, “가상화폐, 패러다임 변화인가 신드롬일 뿐인가”, 서울경제, 2017.

[16] 이신철, “롤러코스터 탄 ‘비트코인·이더리움’...이거 대체 투자해야 돼, 말아야 돼?”, 이투데이, 2017.

[17] Stephen Lawson, “여전히 난장판일지라도... 2017년 IoT 표준 생태계 진단”, CIO, 2017.

[18] Jemima Kelly, “Exclusive: Blockchain platform developed by banks to be open-source”, REUTERS, 2016.

[19] 김영재, 김동호, “블록체인 표준화 동향 및 전략적 대응방안 연구”, 2017년 한국통신학회 하계종합학술발표회, pp 730-731.

[20] Bryan Gobin, “IBM Blockchain High security business network service plan”, 2016.

저 자 약 력

박 현 정

이메일 : lunar1123@naver.com

- 2014년~현재 동덕여자대학교 컴퓨터학과
- 관심분야 : 네트워크 보안, 시스템 보안

양 혜 임

이메일 : cheeezz_@naver.com

• 2015년~현재 동덕여자대학교 컴퓨터학과
• 관심분야 : 시스템 보안, 시스템 소프트웨어

전 정 훈

이메일 : nerdrandy@dongduk.ac.kr

• 2008년 2월 숭실대학교대학원 컴퓨터공학과 공학박사
• 2005년 3월~현재 동덕여자대학교 컴퓨터학과 부교수
• 관심분야: 정보보안, 네트워크 및 시스템 보안, 포렌식

특집 03

핀테크 산업에서 블록체인 도입의 한계점

이수정 · 변혜민 · 박유리 · 전정훈 (동덕여자대학교)

목차

1. 서 론

세계경제포럼(World Economic Forum, WEF)[1]은 제4차 산업혁명 시대를 이끌어갈 핵심기술의 하나로 블록체인(blockchain)을 선정하였으며, 글로벌 시장조사기관인 가트너(gartner)[2]와 딜로이트(deloitte)도 역시 블록체인을 2017년 핵심기술 트렌드로 꼽았다.[3]

특히 세계경제포럼에서는 2017년 안에 전 세계 은행의 80%가 블록체인 기술을 도입할 것으로 예측하며[4], 핀테크 산업에서 블록체인 활용 시 발생하는 거래비용의 효율성과 금융거래의 보안성 향상에 주목하였다. 낮은 비용으로 안전하고 일관성 있는 플랫폼을 제공할 수 있는 블록체인은 22개 해외 투자 은행(Investment Bank)이 연합체를 이루고 핀테크 스타트업인 'R3CEV'와 제휴를 맺어 국제표준화 작업에 착수하는 등 기존 핀테크 산업의 대안으로 떠오르고 있다.[5]

이렇게 핀테크 산업에서는 블록체인 기술 도입의 필요성이 부각되고 있지만, 여전히 국내 핀테크 산업에 블록체인을 도입하기에는 다양한 한계점이 존재한다. 따라서 국내 핀테크 산업에 블록체인의 도입이 효과적으로 실현될 수 있도록 본 논문은 2장에서 핀테크 산업의 동향과 블록체인 기술과 동향을 다루고, 3장에서는 핀테크 산업에서의 블록체인 기술 도입에 대한 동향과 한계점을 논하며, 4장의 결론으로 이글을 마치도록 한다.

2. 핀테크 산업과 블록체인

2.1 핀테크 산업에서 블록체인 기술 도입 배경

IT기술이 빠르게 발전함에 따라 핀테크 산업 역시 빅데이터(big data), 모바일 디바이스(mobile device), 소셜 미디어(social media) 등과 같은 기술을 활용하여 금융 산업 전 분야에서 새로운 형태의 서비스를 제공하고 있다. 핀테크 산업에서

제공하는 새로운 형태의 서비스의 분류와 특징은 <표 1>에서 살펴볼 수 있다.[6]

해당 서비스 중 특히 지급 결제 분야에서는 집중적인 투자와 개발이 이루어지고 있는데, 이와 같은 결과는 모든 금융 서비스 및 거래가 지급과 결제를 통해 이루어진다는 기본적인 특성에 기반한 것이다. 국내 지급결제 시장의 규모는 2014년 3분기 대비, 2015년 3분기에 58.4%로 급격히 증가하였고, 이에 따라 지급 결제 분야에 많은 투자와 연구 및 개발이 뒤따르면서 핀테크 산업에서는 지급 결제 과정상의 보안이 새로운 이슈로 대두되었다.[6]

이 같은 맥락으로, 핀테크 산업에서는 지급 결제상의 보안이 핵심 사안으로 떠올랐고 새롭게 주목받고 있는 핀테크 산업의 보안 기술로는 대표적으로 '생체 인식'과 '블록체인'이 있다. 지문이나 홍채, 얼굴 등 고유한 생체 정보를 이용한 생체 인식 기술 파이도(Fido, Fast Identity Online)와, 이어 2.2절에 기술할 블록체인은 핀테크 산업에서 새로운 보안 체계를 제시한다.

<표 1> 핀테크 산업 분류와 특징

구분	특징
지급결제	– IT 기술을 활용해 모바일 디바이스를 신용카드처럼 사용가능 – 공인인증서, 보안카드 등이 없이 송금이 가능
대출(P2P)	– 빅데이터 기반 신용평가 등을 통해 개인 대출자에게 돈을 투자하고 개인 투자자가 돈을 빌려주는 형식
전자화폐	– 지급결제를 위한 수단 – 자체로서의 가상화폐, 결제플랫폼 역할 수행
증권 및 금융정보	– 주식투자에 소셜기능을 더함 – 주가 및 관련 정보를 실시간으로 제공 – 개인의 은행, 카드, 보험 등 다양한 금융서비스를 애플리케이션을 통해 관리할 수 있는 기능 제공
인터넷 전문은행	– 오프라인 점포 없이 온라인을 통해 금융거래 진행

2.2 새로운 보안체계 블록체인

블록체인은 2008년 10월, 비트코인 개발자 사토시 나카모토(Satoshi Nakamoto)의 논문 "비트코인 : P2P 전자현금시스템"[7] 통해 처음 등장했다. 블록체인은 P2P(Peer to Peer) 기술을 사용하여 관리하는 '분산형 장부'이며 거래 장부를 공개해두고 관리한다는 점에서 '공공 거래 장부(public ledger)'라고 표현되기도 한다.

논문에서 표현된 블록체인의 설계 원리는 다음과 같다. 모든 비트코인 사용자는 P2P 네트워크에 접속해 똑같은 거래장부 사본을 나누어 보관하고, 가장 최근 10분 동안의 거래 내역을 갖고 있던 거래장부의 끝에 더한다. 해당 과정에서 기존 장부에 손상된 부분이 발생하면, 다른 사람의 장부를 복제해 빈 곳을 메우고 장부의 조작을 방지하기 위해 과반수가 인정한 거래내역만 장부에 기록한다. 이렇게 10분마다 최신 상태로 갱신된 거래장부는 다시 모든 비트코인 사용자가 나눠 가져가고, 이 때 10분에 한 번씩 생성되는 거래내역 묶음을 '블록(block)'이라고 부르며 해당 블록이 모인 거래장부 전체가 바로 '블록체인'이다.

이처럼 사토시 나카모토는 기존 방식과는 다르게 비트코인을 사용하는 모든 사용자가 함께 거래 장부를 관리하도록 설계하였고, 그 과정에서 거래비용의 효율성과 금융거래의 보안성 향상을 이루어 내었다.

2.3 핀테크에서 주목하는 블록체인 특징과 효과

블록체인 기술의 다양한 활용분야 중에서도 핀테크 산업에서 블록체인 기술 도입이 기대되는 이유는 바로 다음과 같은 세 가지 특징과 그

에 따른 효과에 있다.

핀테크 산업에서 주목 받는 블록체인의 첫 번째 특징은 바로 분산형 네트워크의 구축이다. 분산형 네트워크란 기존의 클라이언트-서버 방식에서 탈피하여 동등한 계층의 참여자들로 이루어진 네트워크를 의미한다.[8] 이는 참여자 간의 직접 거래를 가능케 하여 중개 수수료 절감 효과를 이끌어낸다.[9] 앞서 다루었던 대로 거래비용의 효율성을 향상시켰다는 점에서 블록체인이 핀테크 산업의 새로운 비전을 제시하였다고 할 수 있다.

두 번째 특징은 블록체인에서 사용되는 암호화 기술이다. 블록체인에서 사용되는 암호화 기술은 데이터의 무결성 검증을 위한 머클 트리(merkle tree)와 거래의 부인방지를 위한 공개키 기반 디지털 서명 기법이다. 이는 거래의 유효성을 검증 가능케 하여 블록체인이 보안을 중요시하는 핀테크 산업에서 주목받을 수 있는 배경이 되었다[10].

세 번째 특징은 분산 합의 프로토콜이다. 블록체인의 분산장부는 기록에 대한 참여자들의 합의가 필요하다는 특징을 가지며, 분산 합의 프로토콜을 이용함으로 인해 모든 참여자는 동일한 정보를 유지하게 된다. 이는 곧 거래나 정보를 검증 할 시에 유용하게 작용하며, 거래나 정보의 정확성과 확실성을 높여 핀테크 산업에서 그 가치를 인정받고 있다.[11]

3. 국내 핀테크 산업에서의 블록체인 도입의 한계점

3.1 관련 법적 규제의 한계

국내 핀테크 산업에 블록체인 도입 한계점으로는 가장 먼저 미흡한 규제 환경이 꼽힌다. 국내의 미흡한 규제 환경은 많은 전문가들이 핀테크 산업의 발전을 위하여 개선되어야 할 보완점으로 지목하고 있으며, 빠르게 변화하는 핀테크 산업 육성을 위해 다양한 정부 정책과 적절한 규제 완화 및 구축이 뒷받침되어야 한다는 것이 공통적인 의견이다.

관련 법적 규제의 한계가 블록체인 도입의 한계점으로 작용한 사례로는, 최근 국민·신한·우리·하나·기업 등 5개 시중은행이 세계 최대 블록체인 컨소시엄인 R3과 함께 고객확인 정보를 블록체인으로 저장·관리하는 분산원장기술 프로젝트에 성공한 사례를 들 수 있다. 은행들은 프로젝트를 통해 한 은행에서 고객 확인 절차를 거치면 다른 은행과 정보를 공유해 추가 고객 확인이 필요 없게 하는 기능을 구현하였다. 그러나 개인정보보호 현행법상 금융사들이 분산원장기술로 고객 정보를 공유할 수 없어 기술 구현에 성공했음에도 불구하고 해당 기술을 국내 핀테크 산업에 도입하지 못하고 있다.[12]

해당 사례 이외에도 블록체인 도입을 제한하는 국내 법적 규제 환경의 한계는 다양한 관련 연구와 논문들에서도 입증되고 있어, 앞의 사례와 관련 내용을 <표 2>로 정리하였다. <표 2>에서는 대표적으로 개인정보보호법 측면에서 블록체인 도입의 한계점을 다루었으며, <표 2>에서 다루지 않은 기타 법규에서의 한계점은 참고문헌으로 대체한다[13-15].

<표 2> 블록체인 도입 관련 법규 한계점(개인정보보호법)

법	조항	블록체인에 적용 시에 나타나는 한계
개인정보보호법	제2조 제3조	블록체인을 통한 개인정보 보유 시, 모든 분산원장 보관자가 개인정보처리자 또는 위탁관리자에 해당하는지 모호.
	24조	블록체인을 통한 개인정보 저장 시, 비식별화된 정보로만 저장될지라도 금융기관 보유의 다른 개인정보와 결합되어 개인 식별이 가능하므로 익명성 보호가 불가능.

3.2 기술 공유의 부족

현재 핀테크 산업에서 블록체인 네트워크는 약 800개 이상 존재한다. 이와 같은 블록체인의 다양성은 곧 블록체인 기술 공유의 부재를 의미하며, 업계 간의 기술 공유 부족은 블록체인을 국내 핀테크 산업에 도입하는 데 큰 장애요인이 되고 있다. 이에 따른 대표적인 예로는 'R3CEV'을 기반으로 컨소시엄을 구축하여 공동 사설 인증 방식을 개발 중인 국내 금융투자업계와 은행업계의 상황을 들 수 있다.

금융투자업계의 경우, 2016년 12월 출범한 금융투자업권 블록체인 컨소시엄은 현행 공인인증서의 사용상 불편함을 개선하는, 블록체인을 기반으로 한 공동사설인증을 개발하는 것에 주요 목표를 두고 있다.

<표 3>에서 알 수 있듯이, 금융투자업권의 공

<표 3> 금융투자업권 블록체인 컨소시엄의 공동사설인증 특징15)

	공인 인증서	사설 인증서	금투업권 공동 인증서
발급자	공인인증기관	개별 금융기관	블록체인 참여사 (합의/ 공동서명)
거래 가능 범위	증권거래 및 보험거래 전 자정부 민원 서비스	발행기관 단독 사용	참여사 전체
인증서 유효성 확인	온라인인증서 상태프로토콜 (OCSP) 이용. 비실시간 인증서 폐기목록(CRL) 검증 필요	내부 구축된 인증서 목록 활용	블록체인에 기록된 인증서 정보 활용
인증서/ 개인키 저장 위치	디바이스의 정해진 위치	자체정책으로 결정(안전한 저장공간 선택 가능)	물리적으로 분리된 안전한 저장공간
개인키 접근방식	복잡한 패스워드 방식 (생체인증 추진 중)	생체, 핀(PIN), 패턴 등 다양한 방식 가능	생체, PIN, 복잡한 비밀번호 등 다양한 방식 가능

장점 단점

통사설인증은 기존 공인인증서 및 사설인증서의 단점을 보완하였다[16]. "기존 인증서비스는 타기관 인증서 사용 시 별도의 추가등록 절차가 필요하고 1년 단위로 갱신이 필요해 불편했다"며 "블록체인을 기반으로 한 공동사설인증은 금융권 한 곳에서만 인증을 마치면 등록된 모든 금융권에서 동일하게 서비스를 이용할 수 있고 다중요소 인증 체계를 통해 보안성은 더 강화된다."는 것이 금융투자업권의 설명이다[17]. 또한 인증수수료도 기존의 1/10 수준으로 줄여 인증관련 비용절감과 신뢰성, 실시간성을 확보한 정보 공유를 통한 고객서비스 향상 및 업무효율화가 이뤄질 것이라는 예측 역시 금융투자업권의 입장이다[17].

금융투자업계와 더불어 국내 은행업계에서도 블록체인 활용 노력은 진행되었다. <표 4>와 같은 독자적 노력을 시작으로 최근에는 은행권 컨소시엄을 구축하며 타 업계와 공동 개발을 하고자 노력중인데[18], (그림 1)과 같이 2016년 11월 출범한 은행권 블록체인 컨소시엄의 목표는 금융투자업권과 마찬가지로 블록체인을 기반으로 한 공동사설인증이다[19]. 해당 시스템이 구축되면 은행들은 고객의 인증 정보를 블록체인에 저장하고, 고객들은 여기서 발급받은 하나의 인증으로 모든 은행에서 사용할 수 있게 되는 간편함을 얻을 수 있다[20].

(그림 1) 은행권 블록체인 컨소시엄 체계

<표 4> 국내 은행권의 블록체인 활용 독자적 노력

KRX 한국거래소	자본시장 최초 장외주식 시스템에 블록체인기술 도입 상용화를 추진하고 있다. 블록체인 전문기업 '블로코(Blocko)'와 협력하여 장외주식 거래를 위한 'KSM(KRX Startup Market) 시스템' 개발('16.9.) • 블록체인 기술 발전을 위한 글로벌 협력조직인 '하이퍼레저(Hyperledger)' 가입('17.4.)
KB국민은행	해외송금서비스, 비대면 실명확인 증빙자료 보관시스템 구축 국내 핀테크 업체 '코인플러그(coinplug)'에 15억 원 투자, 인증 및 송금 서비스 관련 파트너쉽 체결('15.9.) • 비대면 실명확인 증빙자료 보관시스템 구축('16.4.) • KB국민카드는 국내 금융사 중 최초로 블록체인 기술을 활용한 간편 개인인증 시스템을 도입('16.10.)
NH농협은행	골드바 구매 교환증 및 보증서 발급에 블록체인 기술을 활용하고 있다. FIDO(Fast Identity Online)기반의 공인인증서 대체 기술 및 생체인증 솔루션을 자사 전체 금융 플랫폼에 탑재('16.8.) • 기존의 지문인증 서비스에 블록체인 기술을 결합해 보안성을 높여 인터넷 뱅킹으로까지 확대('16.10.)
KEB 하나은행	현재 공인인증서를 대체하는 생체인증서비스, 디지털 Cash 출시를 계획하고 있다. 핀테크 스타트업 인큐베이팅 센터인 '원큐랩(1Q Lab)'을 통해 센트비 등 핀테크 기업과 함께 블록체인 기술을 활용한 해외송금 서비스 구축('15.6.) • 국내 지급 결제 및 인증 관련 프로젝트를 진행하고 기술검증을 완료('16.11.)
우리은행	핀테크 사업부를 중심으로 블록체인 활용 가능성 및 타당성을 검토하고 있는 수준이다. • 미국 송금 전문업체 '머니그램(MoneyGram)'과 협약해 전 세계 200여 개국으로 24시간 송금 가능한 서비스 개시('17.2.) • 디지털전략부 신설을 통해 블록체인과 접목한 사업모델 개발 계획('17.4.)
신한은행	• 블록체인 외환송금 서비스 개발 스타트업 '스트리미(Streami)'와 협업('16.7.) • '신한 골드 안심 서비스' 출시를 통해 금 실물거래가 이뤄질 때 블록체인 기술을 바탕으로 구매 교환증과 보증서 발급('16.8.)
IBK 기업은행	핀테크 기업 '코빗(Korbit)'과 협력해 블록체인 기반 금융서비스 개발 착수('16.3.) • 유럽과 아프리카간 비트코인 송금서비스를 제공하는 케냐의 비트코인 스타트업 '비트페사(BitPesa)'와 공동협력을 위한 업무협약 체결('16.7.)

그러나 앞서 개발했던 금융투자업계와는 달리 은행업계의 컨소시움에서는 블록체인 도입이 기존 은행 소비자 이탈에 영향을 미칠 것을 우려하고 있다. 은행으로서는 블록체인 도입으로 얻게 되는 신규 사업 확장 범위가 넓지 않기 때문에 인증 고객을 타 업계와 공유한다는 발상이 부담이 되고 있는 것이다. 이러한 우려는 분산원장 체계를 지향하는 블록체인과는 거리가 다소 먼, 인증과 공유가 분리되는 방식으로 인증방식을 개발하겠다는 입장으로 이어져 앞으로 은행업계 컨소시움의 행보를 주목할 필요가 있을 것으로 보인다[21].

따라서 원래 금융투자업계와 은행업계는 각각의 공동인증 방식 개발이 끝나고 나면 내년 상반기 내에 이를 합쳐 확장을 진행키로 합의를 본 상황이었으나, 은행업계 컨소시움의 행보에 대해 금융투자업계 관계자가 "각 은행이 서버를 갖춘 상태로 PKI만 공유하는 것은 블록체인 효과를 제대로 살리지 못한 것"라고 지적하면서 해당 합의에도 난항을 겪고 있다[22].

특히 은행업계가 추진하고 있는 블록체인망 구축 방식에 대해서는 블록체인 기술업체 관계자 역시 "현행 방식은 사실상 개인 인증 공유를 위한 블록체인망과 인증서를 발급할 서버를 따로 구축하는 것과 다름없다", "블록체인 자체가 발급 기능을 갖고 있음에도 쓸데없는 비용을 써가며 불편을 감수하는 것"이라 지적하며 은행업계 컨소시움의 개선을 촉구했다[22].

따라서 국내 핀테크 산업에 블록체인 기술이 정상적으로 도입되기 위해서는, 은행업계를 중심으로 문제시되고 있는 타 업계와의 공동 구축 및 협력이 개선되어 기술 공유가 원활히 이루어져

야 한다.

3.3 대표성 있는 협회의 부재

마지막으로, 블록체인이 국내 핀테크 산업에 도입되기 위해서는 대표성 있는 협회의 부재 상황을 해결해야 한다. 지난 6일 공식 출범한 한국블록체인산업진흥협회(블록체인협회)에 블록체인 관련 중소벤처기업 20여 곳이 참여하였다. 하지만 정작 빗썸, 코인원, 코빗 등 주요 비트코인 거래소들은 협회의 멤버로 참여하지 않고 별도 이익단체인 '비트코인거래소협회(가칭)' 설립을 준비하고 있다는 것이 알려졌다.

해당 문제를 조명한 최근의 뉴스에서 한 거래소 관계자는 "현재 블록체인협회에는 비트코인 기술과 직접 관련된 업체가 거의 없다"며 "주요 거래소들이 힘을 합쳐 업계의 실질적인 이해관계를 대변할 수 있는 단체를 만들려고 준비 중"이라고 입장을 밝혔다. 해당 협회가 만들어지면 금융당국 등과 협상 시, 대표성을 놓고 블록체인 협회와 주도권 다툼을 할 것이라는 게 업계 진단이다.[23)]

이러한 상황에서 중심을 잡아야 할 블록체인 협회 역시도 협회 외에 한국블록체인학회와 더불어 지난 3월 한국인터넷진흥원(KISA) 주도로 출범한 민관 합동 '블록체인 오픈포럼'과, 은행권 중심의 '블록체인 협의회', 금융투자업계 중심의 '블록체인 컨소시엄' 등 다양한 단체가 활동하고 있어, 현재로서는 협회의 대표성을 보장받지 못하고 있다. 금융권 관계자는 "이해관계에 따라 지나치게 많은 단체가 설립되면 불합리한 규제에 맞서 한목소리를 내기 힘들다"며 "업계를 대표할 만한 공신력 있는 단체가 빨리 만들어져야 한다."고 지적했다[23].

이처럼 대표성 있는 협회의 부재는 블록체인 기술의 공유나 통합 및 의견 표출에 어려움을 초래하고 있다. 따라서 대표성 있는 협회의 확립은 국내 핀테크 산업에서의 블록체인 도입을 가속화시키기 위하여 반드시 해결되어야 할 문제이다.

4. 결론 및 향후 전망

블록체인은 제4차 산업혁명 시대를 이끌어갈 핵심기술 트렌드로 전 세계의 뜨거운 관심을 받고 있다. 거래 당사자끼리 서로를 감시 및 인증하는 것이 가능한 블록체인은, 핀테크 산업에서 새로운 보안 체계를 구축하고 거래비용을 절감시켜 향후 새로운 비즈니스 모델의 가능성을 연다는 점에서 그 존재가치가 매우 고무적이다.

그러나 블록체인이 국내 핀테크 산업에 안정적으로 정착하기 위해서는 가장 문제시되고 있는 세 가지 한계점을 해결할 필요가 있으며, 본고에서는 한계점과 그에 따른 대응 방향을 제시하였다.

결과적으로 정부 차원의 성장 정책 마련 및 블록체인 기술 도입을 위한 규제의 완화 및 구축이 필요하며, 각 업계 컨소시움 간의 의견 차이와 입장 정리를 통한 기술 공유가 이루어져야 한다. 또, 현재로서 보장받지 못하고 분산되어 있는 블록체인 협회의 대표성 역시 중심을 잡을 필요가 있다.

따라서 향후 해당 한계점과 대응 방향에 대한 연구가 보다 지속적이고 체계적으로 이루어진다면 앞으로 블록체인 기술 도입으로 인한 국내 핀테크 산업의 전망은 밝을 것이라 기대한다.

참 고 문 헌

[1] 세계경제포럼 (World Economic Forum, WEF), 2016.

[2] 가트너 심포지엄/ITxpo 2016, 가트너, 2016.

[3] 이제영, "블록체인(Blockchain) 기술동향과 시사점", 과학기술정책연구원, 2017.

[4] 김보림, "다보스포럼 선정 10대 유망 기술", 융합연구정책센터, 2017.

[5] 금융시장실 주혜원, 우희성, "글로벌 금융권 블록체인 도입 움직임 점검", 국제금융 inside, Vol. 46, pp. 045, 2016.

[6] 박병주, 최슬기, 김득훈, 곽진, "국내·외 핀테크 서비스 및 정책 동향 분석", 한국통신학회지(정보와통신) 34(3), pp. 4, 2017

[7] 사토시 나카모토, "Bitcoin: A Peer-to-Peer Electronic Cash System,", 2009.

[8] 이동영, 박지우, 이준하, 이상록, 박수용, "블록체인 핵심 기술과 국내외 동향", 정보과학회지 35(6), pp. 03, 2017.

[9] 과학기술정책연구원 이제영, "블록체인(Blockchain) 기술동향과 시사점", 동향과 이슈 제 34호, pp. 06, 2017.

[10] 이동영, 박지우, 이준하, 이상록, 박수용, "블록체인 핵심 기술과 국내외 동향", 정보과학회지 35(6), pp. 03, 2017.

[11] 이동영, 박지우, 이준하, 이상록, 박수용, "블록체인 핵심 기술과 국내외 동향", 정보과학회지 35(6), pp. 04, 2017.

[12] 조선비즈, http://biz.chosun.com/site/data/html_dir/2017/05/19/2017051900658.html, 2017년 5월.

[13] 서정호, 이대기, 최공필, "금융업의 블록체인 활용과 정책과제", 2017.

[14] 정승화, "블록체인 기술기반의 분산원장 도입을 위한 법적 과제-금융산업을 중심으로-", The Korean Journal of Financial Law, Vol. 13, No. 2, 2016.

[15] 김신정, 김하은, 염용진, "블록체인의 금융업에 상용화에 따른 이슈", 2017.

[16] 비즈니스워치, http://www.bizwatch.co.kr/pages/view.php?uid=32945, 2017년 8월.

[17] 내일신문, http://www.naeil.com/news_view/?id_art=248709, 2017년 8월.

[18] 과학기술정책연구원 이제영, "블록체인(Blockchain) 기술동향과 시사점", 동향과 이슈 제 34호, pp. 13, 2017.

[19] fntimes, http://www.fntimes.com/html/view.php?ud=186786, 2017년 8월.

[20] 한국경제, http://news.hankyung.com/article/2017081579261, 2017년 8월.

[21] etnews, http://www.etnews.com/20170802000176, 2017년 8월.

[22] etnews, http://www.etnews.com/20170810000413, 2017년 8월.

[23] 매일경제, http://news.mk.co.kr/newsRead.php?year=2017&no=555055, 2017년 8월.

저 자 약 력

이 수 정

이메일 : jenny_sj@naver.com

• 동덕여자대학교 컴퓨터학과 재학

• 관심분야 : 핀테크, 블록체인, 가상화폐

변 혜 민

이메일 : byunhm0406@hanmail.net

• 동덕여자대학교 컴퓨터학과 재학
• 관심분야 : 핀테크, 블록체인, 가상화폐

전 정 훈

이메일 : nerdrandy@dongduk.ac.kr

• 2008년 2월 숭실대학교대학원 컴퓨터공학과 공학박사
• 2005년 3월~현재 동덕여자대학교 컴퓨터학과 부교수
• 관심분야 : 정보보안, 네트워크 및 시스템 보안, 포렌식

박 유 리

이메일 : spdlqjdk1012@naver.com

• 동덕여자대학교 컴퓨터학과 재학
• 관심분야 : 핀테크, 블록체인, 가상화폐

특집 04

금융서비스를 위한 블록체인과 IoT의 통합

한효재 · 송민서 · 이종협 (가천대학교)

목차

1. 서 론

최근 금융서비스와 정보통신기술이 활발하게 융합되면서 핀테크의 새로운 발전이 시작되었다. 당장의 핀테크는 기존의 금융서비스를 발달한 현재의 정보통신기술을 통하여 강화한다는 것이 표면적인 변화를 보여주고 있지만, 전통적인 구조에 고정되어 있던 금융서비스가 새로운 변화를 적극 수용하고 변화하기 시작했다는 것이 진정한 핀테크가 가져오는 변화의 핵심이며 충격의 이유라 할 수 있다. 변화의 모멘텀을 가지기 시작한 금융서비스는 어느 때보다 다양한 가능성을 모두 타진하고 있다.

사물인터넷(Internet of Things, IoT)은 현실세계와 디지털 가상 세계를 연결하는 특성 덕분에, 현실의 금융서비스를 디지털 기술을 통하여 강화하고 있는 핀테크의 입장에서 가장 급선무로 적용하고자 하는 대표적인 기술이다. IoT를 통해서 금융서비스는 기존의 결제 공간을 확장하고, 진정한 고객 맞춤형 서비스와 개인 및 담보에 대한 새로운 신용 평가의 개념 등을 도입하고 있다. 하지만 이러한 변화가 다음 단계로 도약하기 위해서는 새로운 플랫폼으로써 IoT 환경이 태생적으로 가지고 있는 한계들을 해결해야 한다. IoT 환경은 실생활과 밀접하게 연관되어 있어 금융서비스의 최적의 조건이기는 하지만, 그와 동시에 높은 보안적인 위험성을 가지고 있다. 또한, 금융서비스에 필수적인 신뢰성을 보장하기 위해서는 각각 기기의 능력이 제한되어 있다는 것도 한계점으로 작용한다.

이러한 시점에서 새로운 신뢰의 개념을 제공하고 각광 받고 있는 블록체인은 금융서비스 플랫폼에서 IoT 환경이 가지는 문제점들에 대한 기술적 해결책으로써도 사용될 수 있을 것으로 예상하고 있다. 블록체인은 비트코인 암호화폐를 시작으로 소개되어 안전한 거래 기록의 제공 목

<표 1> IoT를 이용한 결제서비스의 예

	자동차	스마트홈
결제	◦ 알리바바·룽웨, 결제시스템 장착 ◦ 포드·포드패스, 주차장,공유,결제 ◦ 기아차, 기아페이(예정) ◦ VISA·혼다, 자동차 결제 서비스 ◦ 신한카드, 커넥티드 카 커머스(예정)	◦ Amazon, Alexa(Amazon Echo) ◦ Amazon, Dash button ◦ 페이민트, 단추 ◦ 삼성 프린터, 토너 자동주문(아마존) ◦ 삼성, 패밀리 허브2.0 냉장고 ◦ SKT·11번가, 스마트버튼꾹 ◦ SKT·11번가, 누구 – 음성쇼핑
	환경	산업
	◦ 케이스마트피아, IoT원격검침, 수도관리 자동화 시스템 (모바일 간편결제와 연계) ◦ 대구시, 상수도 원격검침 서비스	◦ IBM·삼성, ADEPT ◦ Amazon, Amazon Go ◦ IBM–비자의 비자 토큰 서비스 → IoT 기기에 적용 ◦ 롯데 엘페이와 신한의 음파결제 ◦ 대구파티마병원, '엠케어 서비스' 도입
	공간	개인
	◦ ㈜한국주차공유서비스, 스타파킹 ◦ 버틀러호텔(수원시), 키리스(스마트 체크인) ◦ 스웨덴, 모바일 주차 결제 서비스	◦ 크로이스, 스마트밴드 (간편 결제, 대중교통 결제) ◦ KB국민은행 사물인터넷 기반 저금통 리브통 ◦ 삼성, 스마트워치 '기어 S3' 삼성페이 연결

적으로 사용되었지만, 최근 스마트 컨트랙트(smart contract)의 적극적인 적용과 구조의 확장성과 유연성을 강화하면서 암호화폐의 하부구조로써의 역할을 뛰어넘는 또 다른 가능성을 보여주고 있다. 블록체인을 활용하면 데이터 네트워크를 안전한 금융 거래를 위한 환경으로 변화시킬 수 있을 뿐만이 아니라, 능동적인 기능을 내포하고 있는 스마트 컨트랙트의 도입으로 기능이 부여된 플랫폼으로써의 역할을 수행할 수 있다. 특히 IoT의 보안상의 위험성을 보조하기 위한 수단으로써 블록체인의 기술을 활용할 수 있어 금융서비스를 구현함에 있어 필수적 견인 기술의 역할을 할 것으로 예상된다.

본 고에서는 이러한 블록체인과 IoT의 도입에 따른 금융서비스의 변화를 살펴보고, 금융서비스의 변화 과정에서 IoT와 블록체인의 역할과 문제점, 그리고 지속적인 발전을 위한 개선 방향들을 알아보고자 한다.

<표 2> IoT 기능을 이용하는 보험서비스의 예

	자동차	개인
보험	◦ KT·흥국화재, UBI상품 ◦ KT·메리츠화재, UBI상품 ◦ Marmalade사(영국), IoT 블랙박스 – 보험료 측정 ◦ GMS(글로벌모빌리티서비스), 자동차 선불제공	◦ John Hancock·Vitality, 웨어러블기기 Fitbit ◦ BeamTechnologies, 커넥티드칫솔 (연계보험상품) ◦ Allianz사, 올라잇 코치앱(올라잇 페이백 제도) ◦ 현대해상, IoT 접목 '발열관리서비스' ◦ 도쿄해상일동안심생명보험·NTT도코모, IoT활용한 환급상품
	환경	산업
	◦ LG유플러스, 에너지미션(IoT에너지미터 사용)	◦ 교보생명, 블록체인과 IoT간편인증기술 이용한 보험료 지급 서비스

2. 금융서비스와 IoT

4차 산업혁명을 불러오는 여러 가지 기술 중에서 IoT는 우리의 삶에 스며들면서 가장 직접적으로 다가오는 기술이다. 미국 Amazon사의 Dash 버튼과 같은 단순한 기능에서 시작하여 Google의 Nest나 삼성전자의 냉장고까지, 실생활을 구성하는 IoT기기들이 점점 늘어나고 있는 추세이다. 사람들의 생활공간을 메워나가는 IoT의 변화는 기존의 금융서비스와도 활발하게 융합하기 시작하였다. IoT는 다양한 금융 서비스에서 적용되고 있지만 금융서비스를 기준으로 나누어 보면 크게 결제, 보험, 대출 분야 등을 생각해 볼 수 있다[1].

2.1 결제 서비스의 변화

결제의 경우, 인터넷 연결이 가능한 공간에 IoT기기를 설치하여 어디서든 기기가 있으면 결제가 이뤄질 수 있도록 하거나, 비콘(beacon)을 설치하여 IoT가 인지할 수 있는 공간을 구성하여 결제가 가능한 공간을 확장시켜 나간다. Amazon사의 Dash 버튼이나 SkT와 11번가의 '스마트 버튼 꾹'이 대표적으로 간편한 결제의 기능을 제공하거나 IoT를 이용하여 정보의 측정과 결제를 결합하는 형태의 새로운 서비스 방식들도 선보이고 있다. 특히 여러 센서를 이용할 수 있는 IoT의 특징을 활용하여 결제의 수단이 다양화하고 있으며, 결제가 바로 현실에 반영될 수 있는 서비스들이 도입되고 있다.

2.2 보험 서비스의 변화

IoT가 적용되고 있는 보험서비스는 크게 건강보험과 자동차보험을 둘 수 있다. 건강보험은 개인이 IoT기기 즉 웨어러블 기기를 착용하여 실생활에서의 행동 데이터를 받고 분석하여 인센티브를 주거나 보험료를 할인하여 보다 나은 건강한 생활을 할 수 있도록 한다. 건강보험의 대표적인 경우는 미국 보험사인 John Hancock과 건강업체인 Vitality이 연계한 생명보험상품이 있다. 이들은 신규가입 시 웨어러블 기기인 Fitbit을 제공하여 이를 통해 데이터를 받고 건강진단을 하여 점수를 부여하고 다양한 혜택을 제공한다. 자동차보험은 자동차에 부착된 센서나 IoT 블랙박스를 통해 자동차 운전 데이터를 받아 운전습관을 분석하여 보험료를 낮추거나 줄인다. 대표적인 경우로는 영국의 보험사 Marmalade의 IoT 블랙박스를 통한 자동차보험이 있다. 이 보험은 앞서 말한 것과 같이 IoT 블랙박스로 데이터를 받아 운전습관을 분석하여 보험료를 측정한다. 국내에서는 KT와 메리츠화제가 제휴하여 IoT기반의 차량운행기록(OBD)장치를 통해 보험료를 추가로 할인해주는 '마일리지 할인'특약상품을 개발 중에 있다.

2.3 대출 서비스의 변화

대출의 경우에는 주로 동산 담보 대출과 관련해서 IoT 기술 적용 방안이 많이 논의되고 있다. 동산 담보 대출은 등기제도가 없기 때문에 하나의 담보물건으로 여러 곳에서 중복으로 돈을 빌렸을 때 정확히 확인하기 어렵다는 문제점이 있다. 또한 이동이 가능한 동산 담보의 특성상 담보의 상태나 위치 변화에 대한 위험성을 가지고 있다. IoT 기술은 담보의 변화를 탐지하는 담보물관리시스템을 구성하는데 사용될 수 있다. 동산 담보에 부착된 IoT기기가 실시간으로 동산담보의 위치정보를 탐지하고, 관리하는 곳에 변화를 보고하는 것이다. 대표적으로는 씨앤테크사와

<표 3> IoT를 활용하는 동산담보 대출 서비스

	산업
대출	◦ SK, 동산자산관리서비스 ◦ 씨앤테크·SKT, IoT기반 동산담보 솔루션 ◦ 팅크웨어, IoT블랙박스 F800에어 ◦ 메이퍼딩, 담보물 관리시스템 ◦ 캐시로드, 귀금속 담보 대출시스템(스마트 전당포)

SKT IoT기반 동산담보 솔루션이 있다.

2.4 금융환경에서의 IoT의 한계점

IoT의 발달이 금융의 새로운 환경을 만들어 주고는 있지만, 금융서비스를 IoT에서 구현하는 과정에서 IoT 기기의 제한된 성능과 복잡한 구성 때문에 발생하는 한계점이 있다. 우선 기존의 IoT의 문제점이 금융서비스에서 두드러지게 나타나고 있는 것이 보안의 문제점이다. 태생적으로 IoT는 보안에 취약한 구조로 되어 있다. IoT는 센서 기술에서 네트워크 기술, 데이터 처리 기술 등이 여러 데이터 수집 장비에서 시작하여 인터넷과의 연결성을 항상 유지하고 있다. 또한 실생활에 밀접한 곳에 위치하여 있기 때문에 온/오프라인에서 쉽게 보안적 침해를 당할 수 있으며, 데이터의 수집 과정에서 잘못된 정보의 주입이 일어날 수도 있다[2][3]. 특히 금융서비스에서는 보안적 안전성과 서비스의 신뢰성이 중요하게 작용하기 때문에 IoT 보안의 취약점은 필수적으로 해결되어야 하는 문제이다.

IoT와 관련된 제품이 다양화되면서 IoT간의 상호연결성의 문제도 금융서비스에서 당면한 문제 중의 하나이다. 즉 여러 IoT 기기들이 서로 소통하며 하나의 서비스를 구성하기 위한 수단이 잘 정의되어 있지 않기 때문에 실질적인 연동을 위해서는 별도의 게이트웨이 형태의 장비를 필요로 하는 문제점을 가지고 있다. 이러한 문제는 결국 공통된 플랫폼의 부재로 연결된다. 하지만 연동을 위한 플랫폼은 IoT를 통한 서비스와 메시지를 위한 프로토콜을 정의하여 사용하기 위해서는 하드웨어에서부터 시작하여 소프트웨어(운영체제와 어플리케이션 인터페이스)에 이르는 연동의 문제에, 금융서비스를 위한 부가적인 보안의 기능도 제공해야 하는 어려움이 있다.

또한, IoT 장비 또는 기존의 전자제품에 IoT 기능들이 추가적으로 제공되면서, 각각의 제품을 통한 부가 서비스의 시장이 다양화되고 있다. IoT를 통해서 모든 것을 서비스화하는 과정이 활발하게 일어나면서, 서비스의 흐름과 함께 발생하는 결제의 흐름 또한 활발해질 것으로 예상되고 있다. 이러한 결제 흐름의 특징은 적은 액수의 결제가 빈번하게 일어나는 초소액 결제의 형태로 나타나게 되는데, 신용카드 기반의 기존 결제 프로세스는 이러한 초소액 결제 환경에서 고액의 수수료 때문에 적합한 형태라 할 수 없다.

3. 블록체인과 IoT의 결합

3.1 블록체인을 이용한 IoT 금융서비스의 한계점 극복

블록체인은 IoT와 금융서비스의 결합에서 생기는 한계점을 해결할 수 있는 역할을 할 수 있을 것으로 기대되고 있다. 블록체인의 분산구조는 많은 수의 장비로 구성되어 있는 IoT 환경에 적합하며 IoT에서 기대하기 힘든 높은 수준의 데이터 이력에 대한 보호 및 검증과 기기 인증에 적용할 수 있다. 또한 IoT의 금융서비스에서 필수적인 결제 및 송금 수단을 갖춘 통합 플랫폼으로써의 기능을 제공할 수 있다.

IoT는 각 기기의 성능은 제한되어 있지만, 사물인터넷이라는 이름에 걸맞게 각 기기들이 외

부 인터넷과 연결되어 동작하게 된다. 성능이 제한되어 있기 때문에 많은 연산량을 요구하는 고급의 기능들을 사용할 수는 없고, 쉽게 외부 공격을 받을 수 있는 한계점을 가지고 있다. 하지만 외부연결성을 가진다는 특징을 이용하여 블록체인을 보안 강화를 위한 외부 지원책으로 사용하고자 하는 시도가 많이 일어나고 있다. 블록체인은 분산형 구조로 되어 있어 높은 가용성을 가지고 있으며 다양한 암호학을 이용한 안전한 검증 체계를 갖추고 있어 이러한 용도에 적합하다. 특히 정보를 제공하는 주체에 대한 기본적인 인증과 정보의 이력이 안전하게 지켜진다는 점에서 IoT 금융에서 필수적인 안전한 데이터 보안의 기능을 제공할 수 있다.

하지만 무엇보다 블록체인이 IoT 금융서비스에서 발전을 가져다줄 것으로 예상되는 것은 공통 금융 플랫폼으로써의 역할이다. 기존의 환경에서는 IoT 장비간의 기능적 연동을 위한 메시지의 전달을 위한 공통 플랫폼과 금융서비스에서 필수적인 금융거래를 위한 별도의 공통 플랫폼을 필요로 했다. 더욱이 각각의 공통 플랫폼을 통한 연동 자체에 대한 어려움을 겪고 있는 상황에서 목적별로 분리된 플랫폼을 운영한다는 것이 실질적인 시스템의 복잡도를 높이는 요인으로 작용하고 있다. 비트코인이나 이더리움과 같이 대표적인 암호화폐에서 사용되는 블록체인은 내부 상태(state)에 변화를 일으킬 수 있는 기본적인 메시지 전달 단위가 하나의 거래(transaction)이고, 각 거래는 검증되며 메시지와 금전적인 재화를 동시에 전달할 수 있다. 이러한 특징을 활용하여 IoT 장비가 블록체인 내의 각각의 개체가 되고 거래를 생성하여 블록체인 개체간의 정보의 전달과 결제 또는 송금의 역할을 함께 수행하면서 진정으로 통합된 플랫폼을 구성할 수 있다. 또한 검증된 타임라인으로써의 블록체인의 특징은 보험과 같이 수집된 정보의 이력과 추이 변화가 중요하게 요구되는 금융서비스에 적합하다.

3.2 블록체인의 IoT 금융서비스로의 도입의 어려움

이러한 장점에도 불구하고 암호화폐 하부구조로써 동작했던 블록체인 기술을 IoT 환경의 금융서비스에 바로 적용하기에는 고려할 사항들이 있다. 특히 블록체인의 분산 합의(distributed consensus) 구조는 다수결의 원칙을 따로 있으며, 공정한 투표를 위하여 실제 높은 연산량을 요구하는 연산을 직접 수행하여 결과를 제시하는 작업증명(proof of work) 방식이 일반적으로 사용하고 있다. 이러한 작업 과정에서 발생한 거래들의 정합성을 살펴보는 검증과정을 거치게 되고 해시 체인형태의 구조를 통해 이전 블록들을 누적하여 검증해주는 효과를 얻을 수 있다. 하지만 작업증명에 참여하는 채굴자(miner) 또는 full 노드들은 높은 연산량을 요구하기 때문에, 처리장치의 성능이 제한되어 있고 에너지 사용에 민감한 IoT 노드들이 참여하기 어렵다. 결국 IoT 장비들은 다른 full 노드들에 연결하여 사용하는 SPV 또는 경량 노드로써 참여해야 하는데, 이렇게 참여하는 IoT 장비들이 늘어날수록 상대적으로 적은 수의 채굴자 또는 full 노드들이 많은 수의 다른 경량 노드들을 책임져야 하는 과정에서 높은 가용성의 분산 시스템의 장점이 퇴색되게 된다[4]. 이러한 한계를 개선하기 위하여 연산량 위주의 작업증명과는 다른 형태의 분산 합의 구조를 가지고 있는 블록체인 들이 개발되고 있으며 IoT 노드들만으로도 안전한 블록체인을 구성하기 위한 노력이 계속 이루어지고 있다.

또한 금융서비스를 실제로 구현하는 과정에서

여러 가지 여러움이 따르게 된다, 앞서 설명한 대로 블록체인의 시작은 암호화폐의 하부구조로써, 암호화폐의 거래에 대한 검증을 기본으로 하여 스마트 컨트랙트와 같은 기능적 요소로 구성되어 있는 것이 블록체인의 일반적인 형태이다. 따라서 다양한 금융서비스에 적용하기 위해서는 해당 서비스를 블록체인에서 동작할 수 있고 추가적인 검증에 대한 블록체인 내부적인 구현과 외부적인 구현이 모두 필요하다[5]. 블록체인 외부에 위치한 IoT 장비에서의 구현은 블록체인의 API를 사용하며 기존의 소프트웨어 개발 절차와 동일하게 수행되지만 블록체인 내부의 기능 개발은 개념적으로 생소한 스마트 컨트랙트를 통해 구현되어야 한다. 특히 최근 스마트 컨트랙트의 버그를 이용한 두 건의 해킹 사고[6][7]를 통하여 각각 5천만불, 3천만불 가량의 금전적 피해가 발생하였다는 점을 고려해 볼 때, 금융서비스에 적용을 위한 신뢰성 있는 구현을 위해서는 새로운 접근 방법의 구현이 필요함을 보여주고 있다.

4. 금융서비스를 위한 Blockchain-IoT 플랫폼의 발전

4.1 현황

블록체인을 IoT에 도입하기 위한 여러 가지 시도가 일어나고 있다 이 중에서 대표적으로는 블록체인 기반 IoT 산업 구성된 컨소시엄인 CoT(Chain of Things)가 있다. CoT에서는 블록체인을 이용하여 IoT 환경의 신원, 보안, 상호운용성의 문제점들을 해결하고자 하고 있으며 다양한 IoT 업체들과의 협력을 통하여 여러 가지 접근 방법들을 강구하고 있다.

블록체인과 IoT의 새로운 플랫폼에서의 금융서비스들이 해외를 중심으로 나타나기 시작했다. 몇 가지 사례들을 살펴보면 Slock.it은 자신이 소유하고 있는 집, 자동차 등의 자산 중에서 현재 사용하지 않는 것들의 정보를 블록체인에 올려 해당 자산이 필요한 다른 사람과 공유하는 서비스를 제공한다. 그를 통하여 공유경제를 실현할 수 있으며, 보안에 있어서도 블록체인을 활용하여 더욱 신뢰성을 높이고자 하고 있다.[8] 이외에 21.co, Ubirch, RWE, Chronicled, Filament, Catenis, Kinno 등에서 블록체인과 IoT를 활용한 간편 결제, 이력 관리 기능 등을 선보이고 있다.

또한 국내에서도 블록체인과 IoT의 플랫폼을 이용한 사례들이 나타나기 시작했다. 교보생명은 고객이 보험금을 청구하지 않아도 병원비 수납 내역과 보험사의 보험 계약 정보만으로 보험금을 자동으로 지급할 수 있는 서비스를 개발하고 있다. SK텔레콤은 IoT-블록체인 융합 컨소시엄에서 스마트 계약에 기반한 보험서비스를 추진 중이다. 이 서비스는 웨어러블 기기를 통해 사용

<표 4> 국내외 블록체인-IoT 활용한 금융서비스

		특징
해외	Slock.it	집, 자동차 등 본인의 소유자산 중 사용하지 않고 있는 것들을 블록체인에 접근권한 등의 정보를 올려 신청자가 일정의 금액과 보증금을 내면 자산에 대한 권한을 얻을 수 있음.
	RWE	Slock.it과 제휴하여 이더리움 전자지갑이 장착된 전기 자동차, Smart contract를 통해 Share&Charge 앱에서 결제하고, 신호등에서 대기하는 동안 도로 아래 지점에서 전기자동차를 충전
국내	교보생명	고객이 보험금을 청구하지 않아도 병원비 수납 내역과 보험사의 보험 계약 정보만으로 보험금을 자동으로 청구할 수 있는 서비스
	SK텔레콤	웨어러블 기기를 통해 고객의 건강 정보를 수집하여 블록체인에서 저장, 관리하고 해당 데이터를 보험료 측정에 활용하는 서비스

자의 실생활 활동 데이터를 수집하여 블록체인에서 저장 및 관리를 하고 보험료 산정에 활용하는 서비스를 추진할 계획이다[9].

특히 주목할 만한 블록체인 기반 IoT서비스와 플랫폼으로 IOTA재단의 'Tangle'이 있다. IOTA는 블록체인 연구를 목적으로 설립된 비영리 오픈소스 프로젝트로써, 개발된 Tangle은, IoT를 위한 새로운 백본(Backbone)으로써 거래 청산 및 데이터 전송을 제공하고 있다. 특히 Tangle은 IoT에 최적화 되어 있는 새로운 검증 방법을 제시한다. 각 거래를 생성할 때마다 다른 복수의 거래들을 검증하게 하고 검증의 관계를 DAG(Directed Acyclic Graph)형태로 유지함으로써 기존의 작업증명과 채굴방식에서 벗어나고 있다. 즉 모든 참여 개체들이 검증 과정에 참여할 수 있으며 고정된 채굴자와 검증자가 필요하지 않기 때문에 이들을 위한 인센티브 구조나 거래 수수료가 필요하지 않는다는 장점을 가지고 있다[10]. 따라서 극도로 낮은 수수료를 요구하는 IoT 금융환경의 소액결제와 같은 다양한 서비스에 적용될 수 있을 것으로 예상된다.

4.2 발전의 진행 방향과 해결해야할 과제

IoT와 금융서비스의 결합 과정은 점점 더 가속화되고 있다. 아직은 대부분이 시범서비스나 일회성의 실험적인 시도로 끝나는 경우가 반복적인 실정이지만, 현재의 도입 단계를 거치고 본격적으로 IoT의 중요도가 금융서비스가 높아지는 경우에는 IoT의 문제점들이 서비스 실현과정의 큰 한계점으로 다가오게 될 것이다. 따라서 이를 완성하기 위한 블록체인의 도입 또한 중점적으로 고려될 것으로 보인다. 이미 블록체인 시스템은 새로운 금융서비스를 구성하기 위한 중요한 대안적 선택으로 자리 잡고 있으며, 이는 더 진보된 금융서비스를 구성하고 있는 IoT 금융서비스에서는 분리하여 생각할 수 없는 상황이 되었다.

IoT 금융서비스에서는 주요 참여 주체가 IoT 기기이기 때문에 합의 방식이나 검증 구조의 변화를 통해 IoT 기기가 적극적으로 참여할 수 있는 블록체인의 구성 방안에 대하여 논의하면서, IoT에서 수집된 정보의 신뢰성을 금융서비스에 걸맞은 수준으로 높이기 위해 블록체인을 사용하는 접근 방법이 활발하게 진행 중이다. 또한, 주변의 모든 기기를 서비스 제공 수단으로 탈바꿈하고 있는 IoT의 특성에 걸맞는 새로운 초고효율의 결제 방식에 대한 노력도 이어지고 있다.

새로운 시도가 한참 일어나고 있음에도 불구하고, 아직도 블록체인-IoT의 통합 플랫폼에서 금융서비스를 활성화하기 위해서 해결해야 할 문제들이 있다. IoT 환경과 블록체인 양쪽 모두 아직도 한참 개선을 반복하며 문제를 해결하고 있지만, 금융서비스 측면에서 중점적으로 관심을 가져야 할 문제들이 반복적으로 나타나고 있다.

다양한 금융서비스로의 도입과정에서 블록체인이 겪고 있는 허가없는(permissionless) 참여를 통한 안전성 보장과 접근 제어를 통한 정보의 기밀성 보장이라는 역설적 요구의 문제를 해결해야 하는 것은 블록체인-IoT 플랫폼도 마찬가지인 상황이다. IoT를 통해 수집된 정보의 누출은 심각한 사생활 침해의 소지도 함께 내포하고 있어 기밀성을 보장하는 정보를 전달하는 방식이 필수적인 데 비하여, IoT에서 적용할 수 있는 합의 방식에서는 구조적인 단순화를 더 강조하고 있는 상황이라 이러한 역설이 더욱 가중되어 나타나고 있다.

블록체인을 이용한 금융서비스의 보안은 크게 블록체인의 내부 기능의 보안과 외부 기능의 보

안으로 분리하여 생각할 수 있다. 블록체인 내부의 기능을 구현하는 스마트 컨트랙트에서 시작하여 블록체인 서비스를 사용하는 IoT 기기의 엔드포인트 보안까지를 포함하는 셈이다. 스마트 컨트랙트의 보안은 이미 심각한 보안 사고 등을 통하여 시험대에 올라와 있는 상황이지만, 정형 검증(formal verification)에서 시작하여 다양한 테스팅 방식들이 폭넓게 탐구 중이다. 더욱이 IoT의 엔드포인트 보안이 쉽게 침해받을 수 있다는 약점이 있는 상황에서 금융서비스의 안전성 검증을 위해서는 서비스의 시작에서 운영에 이르는 전체적 관점에서의 보안성 제공 방안이 마련되어야 한다.

또한 비슷한 맥락에서 현재 블록체인-IoT 플랫폼 기반 금융서비스들은 IoT를 통해 데이터를 수집하고 블록체인을 통해 기록하며, 블록체인의 스마트 컨트랙트를 통해 검증된 자동화를 이루려고 하는 시나리오를 가지고 있으나 IoT의 데이터와 블록체인 사이의 데이터 전달 과정에서의 신뢰성 확보도 필요하다. 블록체인은 닫힌 공간으로써의 무결성을 가지고 있지만, 외부 정보의 유입 과정에서 고질적으로 발생하는 검증 미비의 문제점을 가지고 있다. 적극적으로 IoT 기기 등을 통하여 생성되는 정보들은 수집단계에서부터 발생하는 정보의 오염에서 시작하여 별도의 검증과 인증 등을 요구하기 때문에 블록체인-IoT 플랫폼을 통한 금융서비스의 신뢰도 확보에 복잡성을 가중시키는 문제 등을 가지고 있다.

5. 결 론

현재 금융서비스의 변화는 '핀테크로의 진화'라고 표현할 수도 있지만, 실질적으로 내포하고 있는 의미는 금융서비스와 일반 IT서비스와의 차이가 사라졌다는 점이라 할 수 있다. 금융서비스는 기존의 정해진 틀을 벗어나면서 가장 사람들이 활발하게 사용하고 관심을 갖는 환경과 플랫폼이라면 무엇이든 금융서비스를 구현하기 위한 기반으로 삼고 있다. 이러한 맥락에서 금융서비스를 위한 블록체인과 IoT의 만남은 사람들에게 직접적인 영향력을 높이고자 하는 블록체인 측면과 제한된 자원에서 신뢰성과 상호운용성을 높이고자 하는 IoT 측면 모두에서 당연한 발전의 다음 단계라고 할 수 있다. 아직 여러 가지 해결해야 할 문제점들이 남았지만, 현재의 발전 속도와 발전에 대한 요구를 고려하면 단기간에 극복할 수 있을 것으로 예상된다. 블록체인과 IoT의 새로운 플랫폼을 기반으로 기존에 볼 수 없던 새로운 조합의 금융서비스들의 탄생을 기대한다.

참 고 문 헌

[1] 이종협, 'IoT 기술과 금융 및 지급서비스', 한국은행 지급결제제도 컨퍼런스, 2016.

[2] 배상태, 김진경, '사물인터넷(IoT) 발전과 보안의 패러다임 변화', 2016.07.

[3] 금융보안원, '국내외 블록체인 기반 사물인터넷 동향', 2017.06.

[4] 강희정 외 2인, 'IoT기반 안전한 블록체인 시스템을 위한 연구', 2017.

[5] 조수환, '사물 인터넷 데이터 무결성 보장을 위한 블록체인 기반의 합의 방법', 2016.

[6] Coindesk, 'Understanding the DAO attack', https://www.coindesk.com/understanding-dao-hack-journalists/, 2016.06.

[7] cryptocoins, 'Hackers Seize $32 Million in Ethereum in Parity Wallet Breach', https://www.cryptocoinsnews.com/hackers-seize-32-million-in-parity-wallet-breach/, 2017.07.

[8] 시큐리티월드 이중엽, '블록체인의 IoT 적용과 융합보안 성장 가속화', http://www.securityworldmag.co.kr/news/articlePrint.html?idxno=4943

[9] 연합뉴스, '코인플러그, SKT IoT-블록체인 융합 컨소시엄 참여', http://www.yonhapnews.co.kr/bulletin/2017/04/24/0200000000AKR20170424123200848.HTML
[10] IOTA, https://learn.iota.org/faqs

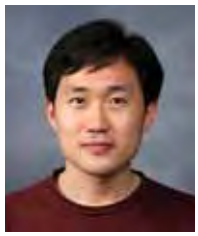
저 자 약 력

한 효 재
이메일 : hyojae1101@naver.com

- 2014~현재 가천대학교 금융수학과
- 관심분야 : 디지털금융, IoT, 블록체인

송 민 서
이메일 : sms074@naver.com

- 2014~현재 가천대학교 금융수학과
- 관심분야 : 빅데이터, 데이터 보안, IoT



이 종 협
이메일 : jonghyup@gachon.ac.kr

- 2009년 8월 연세대학교 컴퓨터과학과 졸업 (공학박사)
- 2009년 9월~2012년 2월 Carnegie Mellon, CyLab 연구소 (박사후연구원)
- 2012년 3월~2015년 2월 한국교통대학교 소프트웨어학과 조교수
- 2015년 3월~현재 가천대학교 금융수학과 조교수
- 관심분야 : 금융 보안, 소프트웨어 보안

정보처리학회지 2017년도 3월호 게재 목차

■ 2017년 3월 (제24권 제2호)	■ 특집명 : 소프트웨어 교육과 컴퓨팅 사고

정보처리학회논문지 2017년도 3월호 게재 목차

■ 제6-CCS권 제3호(통권 제54호) 2017년 3월

■ 제6-SDE권 제3호(통권 제54호) 2017년 3월

정보처리학회논문지 2017년도 4월호 게재 목차

■ 제6-CCS권 제4호(통권 제55호) 2017년 4월

■ 제6-SDE권 제4호(통권 제55호) 2017년 4월

JIPS(정보처리학회영문지) 2017년도 4월호 게재 목차

■ Volume 13, Number 2(Serial Number 44), April, 2017

학회동정

[학회 주최/주관 행사]

◈ 2017년도 제1차 단기강좌 개최

1. 일 시 : 2017년 3월 24일(금) 09:30
2. 장 소 : CNN the Biz 교육연수센터 301호
3. 참석자 : 99명(일반 : 41명, 학생 : 58명)
4. 내 용 : 빅데이터와 딥러닝 구현을 위한 Apache Spark 및 TensorFlow 튜토리얼

[2017년도 제1차 단기강좌에서 한연희 프로그램 위원장의 인사말 모습]

[2017년도 제1차 단기강좌에서 정영식 회장의 인사말 모습]

[2017년도 제 1차 단기강좌 발표 모습 - 장형석 교수(국민대학교)]

[2017년도 제1차 단기강좌 개최 모습]

◈ 2017년도 춘계학술발표대회 개최

1. 일 자 : 2017년 4월 28일(금) ~ 29일(토)
2. 장 소 : 제주대학교 아라컨벤션홀 및 공대4호관
3. 위원회 :
   학 회 장 : 정영식 교수(동국대학교)
   수석부회장 : 남석우 대표이사(콤텍시스템)
   조직위원장 : 김도현 교수(제주대학교),

이상준 교수(제주대학교)
학술위원장 : 박종혁 교수(서울과학기술대학교)

4. 발 표 : 총394편 발표(초청강연 1명, 튜토리얼 3명, 신진학자 4명, 구두발표 165편, 포스터발표 229편)
5. 참가자 : 521명(일반 223명, 학생 348명)
6. 시 상 : 최우수논문상 2편, 우수논문상 32편, 상 3편, 동상 6편, 장려상 12편
7. 학부생논문경진대회 : 대상 1편, 금상 2편, 은상 3편, 동상 6편, 장려상 12편
8. 초청강연 : 박현제 총괄CP(정보통신기술진흥센터)
9. 튜토리얼 : 허정 박사(ETRI), 김호원 교수(부산대), 이기혁 교수(중앙대)
10. 신진학자 : 손윤식 교수(동국대), 김한수 교수(서원대), 김석훈 교수(순천향대), 서승현 교수(한양대)

<table>
<tr><th>일자</th><th>시 간</th><th colspan="2">행사 내용</th></tr>
<tr><td rowspan="8">4/28
(금)</td><td>12:00 - 17:00</td><td colspan="2">등 록</td></tr>
<tr><td>12:30 - 13:00(30)</td><td colspan="2">포스터 논문발표 1</td></tr>
<tr><td>13:00 - 13:50(50)</td><td rowspan="3">튜토리얼 1~3

허 정 박사(ETRI)
김호원 교수(부산대)
이기혁 교수(중앙대)</td><td>13:50 - 14:20</td></tr>
<tr><td>14:00 - 14:50(50)</td><td>포스터 논문발표 2
14:50 - 15:20</td></tr>
<tr><td>15:00 - 15:50(50)</td><td>포스터 논문발표 3</td></tr>
<tr><td>16:00 - 18:20(140)</td><td colspan="2">✱ 신진학자 워크숍 ✱
• 손윤식 교수(동국대 컴퓨터공학과)
• 김한수 교수(서원대 융합보안학과)
• 김석훈 교수(순천향대 컴퓨터소프트웨어공학과)
• 서승현 교수(한양대학교 전자공학부)

✱ 초청강연 ✱
• 박현제 총괄CP (정보통신기술진흥센터)

✱ 개회식 및 임시총회 ✱
• 시상 및 임시총회</td></tr>
<tr><td>18:30 - 19:30(60)</td><td colspan="2">리 셉 션</td></tr>
</table>

<table>
<tr><th>일자</th><th>시 간</th><th>행사 내용</th></tr>
<tr><td rowspan="5">4/29
(토)</td><td>09:00 - 14:00</td><td>등 록</td></tr>
<tr><td>09:10 - 10:40(90)</td><td>구두 논문발표 1</td></tr>
<tr><td>10:50 - 12:20(90)</td><td>구두 논문발표 2</td></tr>
<tr><td>12:20 - 13:20(60)</td><td>중 식</td></tr>
<tr><td>13:20 - 15:05(105)</td><td>구두 논문발표 3</td></tr>
</table>

[2017년도 춘계학술발표대회 참가자 등록 모습]

[2017년도 춘계학술발표대회에서 여성위원회
세미나 개최 모습]

[2017년도 춘계학술발표대회 포스터 논문 발표 모습]

[2017년도 춘계학술발표대회에서 신진학자 워크샵 발표 모습
- 손윤식 교수(동국대학교)]

[2017년도 춘계학술발표대회 튜토리얼 발표 모습
- 허정 박사(ETRI)]

[2017년도 춘계학술발표대회에서 초청강연 발표모습
- 박현제 총괄CP(정보통신기술진흥센터)]

[2017년도 춘계학술발표대회 리셉션 개최 모습
- 김도현 조직위원장(제주대학교)]

[2017년도 춘계학술발표대회 구두논문 발표 모습]

[공동 주최/주관 행사]

◈ 제245회 스마트 사회 지도자 포럼 개최

1. 일 시 : 2017년 3월 3일(금) 07:00
2. 장 소 : 밀레니엄힐튼호텔 3층 아트리움
3. 주 관 : 도산아카데미 공동 주관
4. 참석자 : 정영식 회장 외 32명
5. 강연자 : 정재진 단국대 미래인터넷융합정책 연구센터장
6. 제 목 : 농업 빅데이터와 인공지능 기술 서비스

[제245회 스마트 사회 지도자 포럼 개최 모습]

◈ 제246회 스마트 사회 지도자 포럼 개최

1. 일 시 : 2017년 4월 7일(금) 07:00
2. 장 소 : 밀레니엄힐튼호텔 지하 1층 그랜드볼룸 A
3. 주 관 : 도산아카데미 공동 주관
4. 참석자 : 정영식 회장 외 42명
5. 강연자 : 김정원 미래창조과학부 지능정보사회 추진단 부단장 강연
6. 제 목 : 제4차 산업환경에 대응한 지능정보사회 중장기 종합 대책 추진 방향

[제246회 스마트 사회 지도자 포럼 개최 모습]

[제회의]

◈ 2017년도 제 2차 이사회 개최

1. 일 시 : 2017년 4월 14일(금) 17:00
2. 장 소 : KCC정보통신 9층 컨퍼런스룸
3. 참석자 : 정영식 회장 외 38명
4. 내 용 : 2017년도 춘계 및 IT 21 행사 진행사항 점검

[2017년도 제2차 이사회에서
한정섭 대표(KCC정보통신) 인사말 모습]

[2017년도 제2차 이사회에서 정영식 회장의 개회사 모습]

[2017년도 제2차 이사회에서 회무 발표 모습]

[2017년도 제2차 이사회에서 1분기 감사보고 모습]

[2017년도 제2차 이사회 개최 모습]

◈ 2017년도(제 46차) 임시총회 개최

1. 일　시 : 2017년 4월 28일(금) 17:30
2. 장　소 : 제주대학교 아라컨벤션홀 대회의실
3. 참석자 : 김상훈 총무부회장 외 154명
4. 내　용 : 2017년도 회무 보고 및 시상

[2017년도(제46차) 임시총회에서 김강훈 총무부회장의
개회사 대독 모습]

[2017년도(제 46차) 임시총회에서
오경수 사장(제주도개발공사)의 환영사 모습]

[2017년도(제46차) 임시총회에서
허향진 총장(제주대학교)의 축사 모습]

[2017년도(제46차) 임시총회에서 우수 논문상 시상 모습]

[2017년도(제46차) 임시총회에서 감사패 수여 모습
- 허향진 총장(제주대학교)]

[2017년도(제46차) 임시총회에서 학부생
논문 경진대회 시상 모습]

[2017년도(제46차) 임시총회에서 공로상 시상 모습
- 유헌창 교수(고려대학교)]

[2017년도(제46차) 임시총회 개최 모습]

[지회 및 연구회]

– 호남지회

◈ 2017년도 제1차 워크샵 개최

1. 일 시 : 2017년 4월 5일(수) 18:00
2. 장 소 : 광주광역시 다연
3. 주 관 : 호남지회(지회장: 방상원 교수)
4. 참석자 : 27명
5. 내 용 : 호남지역 ICT 발전 방안

– 이브릿지연구회

◈ 2017년도 제3차 이브릿지편집위원회 회의 개최

1. 일 시 : 2017년 4월 19일(수) 11:00
2. 장 소 : LG CNS 25층 회의실
3. 참석자 : 안문석 위원장 등 11명
4. 내 용 : 2017년 포럼 개최 준비 외

[이브릿지 편집위원회 LG CNS 사옥 방문]

[2017년도 제 3차 이브릿지 편집위원회 회의 개최 모습]

[학술사업 추진 활동]

– 춘계학술발표대회

◈ 2017년도 춘계학술발표대회 제2차 학술위원장단 회의 개최

1. 일 시 : 2017년 3월 31일(월) 16:30
2. 장 소 : 학회 회의실
3. 참석자 : 박종혁 위원장 외 16명
4. 내 용 : 2017년도 춘계학술발표대회 논문 심사 및 우수논문상 선정 외

[2017년도 춘계학술발표대회 제2차 학술위원장단 회의에서 박종혁 학술위원장의 인사말 모습]

[2017년도 춘계학술발표대회 제2차 학술위원장단 회의 개최 모습]

[기타 활동]

◈ 2017년도 1/4분기 감사 시행

1. 일 시 : 2017년 4월 11일(화) 11:00
2. 장 소 : 학회 회의실
3. 참석자 : 이재일 감사외 1명
4. 내 용 : 학회 2017년도 1/4분기 회무 및 재무 감사

신규회원 명단

2017년 3월 1일 ~4월 30일

회원구분	회원번호	성명	직장명
종신회원	2017-21113-01	허준호	부산가톨릭대학교
	2017-21155-01	정준호	동국대학교
	2017-21214-01	정영섭	순천향대학교
	2017-21230-01	임동혁	호서대학교
	2017-21271-01	정창원	원광대학교
	2017-21326-01	안동혁	계명대학교
	2017-21331-01	권혁준	순천향대학교
	2017-21390-01	최준열	삼성디스플레이
갱신된 종신회원	2003-9784-01	서동만	대구가톨릭대학교
	2004-11545-01	손윤식	동국대학교
	2011-16975-02	윤창표	경기과학기술대학교
	2013-19110-01	임효상	연세대학교
	2015-19856-01	김태준	충북대학교
	2016-20974-01	곽정훈	동국대학교
정회원	2017-21114-02	정관수	호원대학교
	2017-21115-02	신의섭	순천향대학교
	2017-21118-02	정명수	경북차량융임베디드 기술연구원
	2017-21127-02	조성의	오토웨어
	2017-21141-02	김지언	원광대학교
	2017-21142-02	백영현	유니온커뮤니티
	2017-21144-02	이정훈	포항공과대학교
	2017-21147-02	서민석	아이렉스넷
	2017-21149-02	김대솔	육군3사관학교
	2017-21150-02	김영식	유니텍
	2017-21151-02	김용일	유니텍
	2017-21153-02	이은관	육군3사관학교
	2017-21156-02	신용철	아이티맨
	2017-21157-02	백정열	미래융합정보기술
	2017-21158-02	주성용	애그로닉스
	2017-21163-02	이혁주	이노그리드
	2017-21165-02	김바울	이노그리드

회원구분	회원번호	성명	직장명
정회원	2017-21176-02	김진욱	한국방송통신대학교
	2017-21177-02	김명국	유정시스템
	2017-21178-02	이창욱	유정시스템
	2017-21182-02	이관용	한국방송통신대학교
	2017-21184-02	홍선영	고려대학교
	2017-21193-02	고명숙	부천대학교
	2017-21194-02	김지심	명지전문대학
	2017-21198-02	류재호	그립
	2017-21205-02	김기두	한국정보통신기술협회
	2017-21216-02	이상훈	한국토지주택공사 토지주택연구원
	2017-21219-02	정재희	홍익대학교
	2017-21220-02	최재용	리얼타임테크
	2017-21225-02	염기선	애그로닉스
	2017-21226-02	한혁	리얼타임테크
	2017-21240-02	유종호	경북IT융합산업기술원
	2017-21241-02	장성봉	금오공과대학교
	2017-21254-02	김기현	한국과학기술정보연구원
	2017-21256-02	신정훈	숭실대학교
	2017-21260-02	한찬명	엠플러스비전
	2017-21261-02	석성우	한국전자통신연구원
	2017-21296-02	박은주	안동대학교
	2017-21333-02	김성찬	한국과학기술정보연구원
	2017-21338-02	정유채	숙명여자대학교
	2017-21339-02	이은규	인천대학교
	2017-21389-02	박선희	아이에이치테크
	2017-21396-02	손현승	홍익대학교
	2017-21397-02	신진섭	한국과학기술정보연구원
준(학생) 회원	2017-21116-03	원성연	고려대학교
	2017-21117-03	송영택	경기대학교
	2017-21119-03	황수현	충북대학교
	2017-21121-03	지현정	세종대학교

회원구분	회원번호	성명	직장명
준(학생)회원	2017-21123-03	윤현수	세종대학교
	2017-21124-03	이현우	세종대학교
	2017-21125-03	신경일	세종대학교
	2017-21126-03	김도연	세종대학교
	2017-21128-03	김진성	고려대학교
	2017-21129-03	성정훈	단국대학교
	2017-21131-03	Mehari Marta Rezene	연세대학교
	2017-21132-03	김영훈	동국대학교
	2017-21133-03	김성진	한양대학교
	2017-21134-03	김형균	과학기술연합대학원대학교
	2017-21135-03	심철	충북대학교
	2017-21136-03	박동하	동국대학교
	2017-21138-03	Zhou Xiang	인하대학교
	2017-21139-03	강원민	서울과학기술대학교
	2017-21140-03	이지성	부산대학교
	2017-21143-03	최순혁	충북대학교
	2017-21145-03	조재현	서경대학교
	2017-21146-03	최찬휘	서경대학교
	2017-21148-03	서준배	경기대학교
	2017-21154-03	김진석	숭실대학교
	2017-21159-03	이홍재	숭실대학교
	2017-21160-03	Ismoilov Nusrat	금오공과대학교
	2017-21161-03	Aman Jaffari	전북대학교
	2017-21162-03	김준혁	숭실대학교
	2017-21164-03	변주성	인하대학교
	2017-21166-03	손아영	경희대학교
	2017-21167-03	조현욱	순천대학교
	2017-21169-03	Myrah Naeem	세종대학교
	2017-21170-03	이성훈	한국전자통신연구원
	2017-21171-03	최현영	금오공과대학교
	2017-21172-03	양우석	한경대학교
	2017-21173-03	박준학	경희대학교

회원구분	회원번호	성명	직장명
준(학생)회원	2017-21175-03	윤상민	한양대학교
	2017-21179-03	김민채	순천향대학교
	2017-21180-03	김민상	순천향대학교
	2017-21181-03	김한슬	순천향대학교
	2017-21183-03	Lumme Juha Aadolf Herman	인하대학교
	2017-21185-03	정상원	고려대학교
	2017-21186-03	김창덕	충남대학교
	2017-21187-03	이석원	계명대학교
	2017-21188-03	염성규	세종대학교
	2017-21189-03	변준영	경희대학교
	2017-21190-03	김남용	서울과학기술대학교
	2017-21191-03	권병욱	서울과학기술대학교
	2017-21192-03	박경엽	서울과학기술대학교
	2017-21195-03	안예찬	백석대학교
	2017-21196-03	김건우	중앙대학교
	2017-21197-03	한효준	동국대학교
	2017-21199-03	지수현	강릉원주대학교
	2017-21200-03	이민석	과학기술연합대학원대학교
	2017-21202-03	노경미	한국방송통신대학교
	2017-21203-03	용찬호	경희대학교
	2017-21204-03	양현정	중앙대학교
	2017-21206-03	최효린	서울시립대학교
	2017-21208-03	최석준	아주대학교
	2017-21210-03	유요셉	건국대학교
	2017-21212-03	신상길	에스에스알
	2017-21215-03	백현지	경희대학교
	2017-21217-03	이수형	경북대학교
	2017-21218-03	박진욱	연세대학교
	2017-21221-03	조성환	가천대학교
	2017-21222-03	김상조	부산대학교
	2017-21223-03	임종호	부산대학교
	2017-21224-03	성한승	연세대학교

회원구분	회원번호	성명	직장명
준(학생)회원	2017-21227-03	김화목	부산대학교
	2017-21228-03	안형준	부산대학교
	2017-21229-03	Liu Xiao	부산대학교
	2017-21231-03	장정현	충북대학교
	2017-21233-03	정승원	고려대학교
	2017-21234-03	진하연	충북대학교
	2017-21235-03	김상혁	한밭대학교
	2017-21236-03	김영재	충북대학교
	2017-21237-03	김수진	중앙대학교
	2017-21238-03	황나윤	고려대학교
	2017-21239-03	정희윤	충북대학교
	2017-21242-03	고성윤	포항공과대학교
	2017-21243-03	주은진	충북대학교
	2017-21244-03	김계영	인천대학교
	2017-21245-03	남승완	인천대학교
	2017-21246-03	서인	포항공과대학교
	2017-21247-03	이훈기	서울시립대학교
	2017-21248-03	김덕엽	경북대학교
	2017-21249-03	윤보람	경북대학교
	2017-21251-03	강경목	경상대학교
	2017-21252-03	나원철	중앙대학교
	2017-21253-03	박리원	중앙대학교
	2017-21255-03	김정환	포항공과대학교
	2017-21257-03	정승주	숭실대학교
	2017-21258-03	한진	충북대학교
	2017-21259-03	곽용섭	경북대학교
	2017-21262-03	김경미	공주대학교
	2017-21263-03	변운조	공주대학교
	2017-21264-03	임문택	공주대학교
	2017-21265-03	이태성	포항공과대학교
	2017-21266-03	강명균	국민대학교
	2017-21268-03	류동균	한밭대학교
	2017-21269-03	조정훈	서경대학교

회원구분	회원번호	성명	직장명
준(학생)회원	2017-21270-03	최우용	경북대학교
	2017-21273-03	박세영	전남대학교
	2017-21274-03	조문영	전남대학교
	2017-21275-03	Sinh Ngoc Nguyen	전남대학교
	2017-21276-03	김만수	연세대학교
	2017-21277-03	김대원	연세대학교
	2017-21278-03	류재민	부산대학교
	2017-21280-03	김가영	전남대학교
	2017-21281-03	조성모	전남대학교
	2017-21282-03	정승완	전남대학교
	2017-21283-03	안성범	과학기술연합대학원대학교
	2017-21284-03	박정훈	인하대학교
	2017-21285-03	김지용	전남대학교
	2017-21286-03	손영우	계명대학교
	2017-21287-03	석병진	서울과학기술대학교
	2017-21288-03	우시재	아주대학교
	2017-21289-03	지병규	동국대학교
	2017-21290-03	박인규	아주대학교
	2017-21291-03	김동엽	아주대학교
	2017-21292-03	김세송	동국대학교
	2017-21293-03	김동욱	동국대학교
	2017-21294-03	이기택	원광대학교
	2017-21295-03	박예슬	아주대학교
	2017-21297-03	조상현	안동대학교
	2017-21298-03	정예린	안동대학교
	2017-21299-03	정동유	안동대학교
	2017-21301-03	이재인	안동대학교
	2017-21302-03	도혜미	안동대학교
	2017-21303-03	김형범	안동대학교
	2017-21304-03	최규호	안동대학교
	2017-21305-03	정성훈	안동대학교
	2017-21306-03	이수정	안동대학교

회원구분	회원번호	성명	직장명
준(학생)회원	2017-21307-03	이은지	아주대학교
	2017-21308-03	최슬기	아주대학교
	2017-21309-03	황규본	아주대학교
	2017-21311-03	김재홍	과학기술연합대학원대학교
	2017-21312-03	민가영	충북대학교
	2017-21313-03	윤준호	부산가톨릭대학교
	2017-21314-03	임현지	동국대학교
	2017-21315-03	이성현	안동대학교
	2017-21316-03	최유림	아주대학교
	2017-21317-03	강시영	한밭대학교
	2017-21318-03	이재근	전남대학교
	2017-21319-03	박수지	전남대학교
	2017-21320-03	한상진	전남대학교
	2017-21321-03	노동근	전남대학교
	2017-21322-03	박병주	아주대학교
	2017-21323-03	배원일	아주대학교
	2017-21324-03	서민지	숭실대학교
	2017-21325-03	신희진	숭실대학교
	2017-21327-03	Ammar UL Hassan	숭실대학교
	2017-21328-03	이복주	한국기술교육대학교
	2017-21329-03	이기훈	호서대학교
	2017-21330-03	안정호	고려대학교
	2017-21332-03	김동현	금오공과대학교
	2017-21334-03	윤현노	호서대학교
	2017-21335-03	김현지	포항공과대학교
	2017-21336-03	김형석	공주대학교
	2017-21337-03	안형욱	금오공과대학교
	2017-21340-03	조준혁	전북대학교
	2017-21341-03	강지훈	고려대학교
	2017-21342-03	이규영	서경대학교
	2017-21343-03	최인렬	부산가톨릭대학교
	2017-21344-03	배근표	부산가톨릭대학교
	2017-21345-03	김태중	부산가톨릭대학교

회원구분	회원번호	성명	직장명
준(학생)회원	2017-21346-03	강혜정	계명대학교
	2017-21347-03	권덕호	계명대학교
	2017-21348-03	김기윤	계명대학교
	2017-21349-03	김민석	계명대학교
	2017-21350-03	김상원	계명대학교
	2017-21351-03	김시영	계명대학교
	2017-21352-03	김용재	계명대학교
	2017-21353-03	김은솔	계명대학교
	2017-21354-03	김혜원	계명대학교
	2017-21355-03	박소연	계명대학교
	2017-21356-03	박수진	계명대학교
	2017-21357-03	서승우	계명대학교
	2017-21358-03	신현지	계명대학교
	2017-21359-03	여아영	계명대학교
	2017-21360-03	오수진	계명대학교
	2017-21361-03	윤대우	계명대학교
	2017-21362-03	윤형조	계명대학교
	2017-21363-03	이재성	계명대학교
	2017-21364-03	전영진	계명대학교
	2017-21365-03	전현덕	계명대학교
	2017-21366-03	정승우	계명대학교
	2017-21367-03	지윤호	계명대학교
	2017-21368-03	최성환	계명대학교
	2017-21369-03	최용혁	계명대학교
	2017-21370-03	최은수	계명대학교
	2017-21371-03	최재욱	계명대학교
	2017-21372-03	최혜정	계명대학교
	2017-21373-03	홍현표	계명대학교
	2017-21374-03	표지혜	계명대학교
	2017-21375-03	안다솜	계명대학교
	2017-21376-03	양세영	서울여자대학교
	2017-21377-03	문선예	군산대학교
	2017-21378-03	김수정	군산대학교

회원구분	회원번호	성명	직장명
준(학생) 회원	2017-21379-03	최진우	군산대학교
	2017-21380-03	유영식	군산대학교
	2017-21381-03	오선영	군산대학교
	2017-21382-03	나철원	군산대학교
	2017-21383-03	남수민	군산대학교
	2017-21384-03	박선영	군산대학교
	2017-21385-03	최민성	군산대학교
	2017-21386-03	나윤석	한국전자통신연구원

회원구분	회원번호	성명	직장명
준(학생) 회원	2017-21387-03	양영욱	고려대학교
	2017-21388-03	이재웅	호서대학교
	2017-21391-03	허병문	국립보건연구원
	2017-21392-03	안진현	고려대학교
	2017-21420-03	권동우	계명대학교
	2017-21489-03	김하진	강원대학교
	2017-21502-03	유기성	동국대학교

특별 법인회원 명단

구 분	대표자	주 소
(주)경봉	윤석원 대표	경기도 안양시 만안구 예술공원로 153-32
(주)베스트케이에스	김교은 대표	서울시 금천구 범안로 1130 가산디지털엠파이어빌딩 501, 502호
(주)블루코어	이동화 대표	서울시 강남구 역삼동 682 남전빌딩 4층
삼성SDS(주)	정유성 대표	서울시 송파구 올림픽로35길 123(신천동) 삼성SDS타워
(주)영화조세통람	서동혁 대표	서울시 중구 동호로 14길 5-6 이나우스빌딩
(주)LG CNS	김영섭 대표	서울시 영등포구 여의대로 24, FKI타워
(주)자이네스	고범석 대표	서울시 구로구 디지털로33길 55 904호(E&C벤처드림타원 2차)
정보통신산업진흥원	윤종록 원장	충북 진천군 덕산면 정통로 10
정보통신정책연구원	김도환 원장	충북 진천군 덕산면 정통로 18
(주)지란지교시큐리티	윤두식 대표	서울시 강남구 역삼로 542(대치동 신사S&G 5층)
(주)G.I.G기업	이용기 대표	서울시 광진구 능동로40길8 정암빌딩 100호
KCC정보통신	이상현 대표	서울시 강서구 공항대로 665 KCC오토타워(염창동 260-4번지)
한국인터넷진흥원	백기승 원장	서울시 송파구 중대로 135 IT벤처타워 4층
한국정보화진흥원	서병조 원장	대구시 동구 첨단로 53
한국전자통신연구원	이상훈 원장	대전시 유성구 가정로 218

한국정보처리학회 기관지 원고 집필 안내

한국정보처리학회는 학회지 「정보처리학회지」와 논문지 「정보처리학회논문지A·B·C·D」를 발행하고 있습니다. 「정보처리학회지」는 새로운 기술동향을 비롯해서 각종 정보를 게재하고, 회원의 지식 향상을 목적으로 하며, 「정보처리학회논문지A·B·C·D」는 회원의 연구 결과를 발표하는 장입니다.

본 안내는 학회 기관지의 원고 집필 요령을 정리한 것으로, 집필 시 참고로 하시기 바랍니다.

『정보처리학회지』 원고 집필 안내

제 1 조 학회지에 게재할 원고의 종류는 특집, 특별기고, 기획기사, 정보 관련 기술 동향 및 편집위원회가 인정하는 것으로 한다.

제 2 조 투고자는 원칙적으로 본 학회 회원으로 한다. 단, 회원과의 공동기고자 및 초청기고자는 예외로 한다.

제 3 조 원고는 수시로 접수하며 접수일은 원고가 본학회 편집위원회에 도착한 날로 하고, 접수된 원고는 편집위원회에서 게재여부를 결정한다.

제 4 조 원고는 가장 많이 사용되는 워드프로세서로 작성한 파일을 함께 제출한다.

제 5 조 원고의 내용은 정보처리 관련자가 이해할 수 있는 정도로 작성한다.

제 6 조 투고자는 200자 이내의 약력을 제출하여야 한다. 게재가 확정된 원고에 대해서는 추후 저자의 사진을 제출해야 한다.

제 7 조 본 학회지에 게재된 내용은 본 학회의 승인없이 영리목적으로 무단 복제하여 사용할 수 없다.

제 8 조 원고 작성 방법은 다음과 같다.

(1) 1페이지 기술 분량 : A4용지 30행×40자 내외

(2) 원고분량 : 6~8페이지 내외

(3) 참고문헌 : 참고 문헌은 저자명에 의한 사전식으로 기술하되, 각 참고 문헌은 잡지의 경우 “번호저자명, 제목, 잡지명, 권, 호, 페이지, 연도”의 순으로 기술한다. 단, 참고문헌 인용시에는 대괄호를 이용할 것(예 [1], [2], [3], [4] 등)

(예) [1] 김철수, 김수철, “한국 정보 처리 산업에 관한 연구”, 한국정보처리논문지, 제 1권, 제 1호, pp.23-43, 1997.

[2] 이영희, 컴퓨터입문, pp.234, 출판사, 1997.

[3] L. Lanomt, “Synchronization Architecture and Protocols”, IEEE Trans. on Comm., Vol. 23, No. 3, pp.123-132, 1997.

[4] Steinmetz, Multimedia : Computing, Communications & Applications, PII, 1995.

(4) 내용표기에 있어서, 장, 절 등의 표시는 ‘ 1, 1.1, 1.1.1, 가, 1), 가), (1), (가)’의 순서로 한다.

(5) 원고는 ‘제목-소속-성명-목차-본문-참고문헌’의 순으로 기술하며, 첫장 하단에는 회원 구분을 명기한다.

(6) 표의 제목은 “<표1>대한민국” 과 같이 표의 상단에 기술하고, 그림의 제목은 “(그림1)서울”과 같이 그림의 하단에 기술하며, 사진판으로 사용할 수 있도로 백지에 정서해야 한다.

본 규정은 1997년 1월 1일부터 효력을 발생한다.

기타 원고 모집 안내

당 학회지 편집위원회에서는 학회지 「정보처리학회지」에 게재할 각종 원고를 회원 여러분으로부터 모집하고 있습니다. 많은 투고와 참여있으시기 바랍니다.

1. 모집내용

다음에 대한 원고를 모집합니다.

(1) 해 설 : 정보처리에 관련된 신기술 또는 이론으로서 당 학회 회원의 관심도가 높은 내용
(2) 외국기사 : 외국 잡지에 게재된 기사로서 당 학회 회원에게 유익한 내용
(3) 서 평 : 최근에 출판된 책으로서 당 학회 회원에게 유익한 도서의 소개 또는 비평
(4) 뉴 스 : 정보처리에 관한 국제규모의 회의, 대회의 보고 등 시사성이 높고 당 학회 회원에게 널리 알릴 가치가 있는 내용
(5) 기관소개 : 국내 기관 또는 외국 기관
(6) 기 타 : 당 학회 회원에게 유익한 내용

2. 응모 자격

당 학회 회원으로 한다.

3. 응모 절차

원고는 학회지 편집위원회에서 정한 투고 규정에 의거하여 다음 순서로 기술하여 주시기 바랍니다.

(1) 제 목
서평의 경우에는 저자명, 책이름, 페이지수, 출판사, 발행년도, 가격 등으로 기술한다.
어느 장르에 속하는지를 첫페이지 오른쪽 상단에 표시한다.
(2) 필자명, 소속, 필자 연락처
(3) 본 문
본문은 서평의 경우 2,000자 정도, 뉴스의 경우 1,000자 정도로 한다.
(4) 참고문헌, 부록, 그림, 표
(5) 필자 소개
이름, 경력과 학력을 기술한다.

4. 원고 취급

투고된 원고는 학회지 편집위원회에서 심사를 한 후 게재여부를 결정합니다. 게재가 결정되었을 경우에는 원고 수정을 부탁하는 경우가 있습니다. 서평의 경우에는 필자의 사진이 필요하므로 게재 결정 후 학회 사무국으로 우송해야 됩니다.

5. 원고료

학회지 규정에 의거하여 소정의 원고료를 지급합니다.

6. 보낼 곳

140-750 서울특별시 용산구 한강대로 109, 1002호(한강로 2가 용성비즈텔)
한국정보처리학회 학회지 편집위원회
uskim@kips.or.kr

정보처리학회 논문지 투고 규정

1. 원고의 전자 투고

모든 원고는 전자 형태(MS Word, 아래아 한글, 혹은 PDF 형태)로 학술지 웹사이트 (http://acoms1.kisti.re.kr/kips/index.jsp?publisher_cd=kips&cid=&cid_year=2006&cid_seq=A&lang=kor)를 통해 온라인으로 투고하여야 한다. 투고 규정은 해당 웹사이트에서도 볼 수 있으며, 본 학술지에 투고하는 모든 원고들은 이 규정을 준수하여야 한다. 그렇지 않을 경우 원고가 반송되게 되며 이로 인해 출판이 지연될 수도 있다. 원고 투고에 관한 문의는 이메일(kips@kips.or.kr)이나 전화(+82-2-2077-1414), 팩스(+82-2-2077-1472)를 통해 학회 사무국으로 한다. 저자 중에 1인은 학회 회원으로 가입되어야 함을 원칙으로 한다.

2. 연구 및 출판 윤리

본 학술지는 Guidelines on Good Publication (http://publicationethics.org/static/1999/1999pdf13.pdf)에 기술된 연구 및 출판 윤리 지침을 따른다.

2.1 이해갈등관계 명시

저자는 기업으로부터의 재정적 지원 또는 연계, 이익집단으로부터의 정치적 압력 등과 같은 이해 갈등 관계가 있으면, 이에 관한 정보를 밝혀야 한다. 특히, 연구에 관계된 모든 지원금의 출처를 명백히 진술해야 한다.

2.2 저자 요건

1) 연구의 기본개념설정과 설계, 자료수집, 또는 자료분석과 해석에 지대한 공헌을 하고, 2) 원고를 작성하거나 내용의 중요 부분을 변경 또는 개선하고, 3) 최종 원고의 내용에 동의한 세 가지 조건을 모두 충족한 사람만이 논문 저자로서 원고에 나열되어야 한다. 원고의 최초 투고 후, 어떠한 저자 변경 사항(저자 추가, 저자 삭제, 혹은 저자 순서 변경)도 편집인에게 편지로 알려주고 승인을 받아야 한다. 이 편지에는 해당 논문의 모든 저자들의 서명이 포함되어야 한다.

2.3 이중게재/이중투고 금지

투고 된 모든 원고는 다른 학술지에 이미 실렸거나 또는 심사 중이어서는 안 된다. 채택된 원고의 모든 부분은 편집위원회의 허가 없이 다른 과학학술지에 이중게재 하여서는 안 된다. 본지에 실린 논문의 이중게재 발각 시에는 저자 및 소속기관에 이를 알릴 것이며, 저자에게 제재가 가해 질 것이다.

3. 상호심사 절차

모든 원고는 편집위원이 위촉한 2인 또는 3인의 심사위원들이 평가하며, 연구의 질과 독창성, 그리고 과학적 중요성을 바탕으로 심사하여 채택 여부를 결정한다. 원고투고 후 심사결과를 이메일로 통보 받게 되며 심사자의 의견이 교신저자의 이메일로 전달된다. 교신저자는 수정된 원고를 온라인으로 재투고해야 하며 심사자의 지적에 따라 변경된 내용을 각 항목별로 진술해야 한다. 편집위원회 결정 이후 8주가 경과해도 수정된 원고를 재투고하지 않을 시에는 철회로 간주한다. 저자는 학술지 웹사이트에서 투고 논문의 심사 진행 현황을 확인할 수 있다.

4. 저작권

출판된 모든 원고는 한국정보처리학회의 자산이 되며, 서면허가 없이 다른 곳에 출판되어서는 안 된다. 출판이 결정되면 저자는 저작권양도 서식을 기재하여 팩스, 우편 또는 이메일로 학회 사무국에 보내야 한다.

5. 원고 작성

5.1 언어

모든 원고는 국문 또는 영문으로 작성하여야 한다. 국문 논문의 경우, 서지 정보(제목, 저자, 소속, 교신저자의 주소와 이메일), 표, 그림, 감사의 글, 참고문헌 등은 모두 영문으로 기술하여야 한다. 심사를 위한 초기 투고 원고에는 저자 정보를 포함시키지 말아야 한다. 하지만, 논문 수락 판정을 받은 후 제출하는 최종본에는 저자 정보를 포함시켜야 한다.

5.2 일반적인 사항

1) 원고는 MS Word나 한글문서로 작성한다.

2) 원고는 A4 (21.0×29.7cm) 용지에 10point 글씨크기로 행 사이를 2행 간격(double space)으로 하여 작성하되, 상하좌우 모두 2.5cm의 여백을 둔다.

3) 모든 단위는 International System(SI) of Units 에 따라 기술하여야 한다. 퍼센트(%)와 온도(℃)를 제외한 모든 단위는 한 칸의 공백 다음에 기술해주어야 한다.

5.3 출판 유형

한국정보처리학회논문지는 연구논문(research paper), 편집인의 글(editorial), 편집인과의 서신(letters to the editor) 등을 출판한다.

1) 연구논문(research paper): 본 학술지가 다루는 범위 안에서 새로운 학술적 발견들을 상호 심사과정을 거쳐 연구논문으로 출판할 수 있다. 연구논문에는 이론이나 실험에 관한 새롭고 중요한 결과들이 기술되어야 한다. 연구논문 중 일반논문(regular paper)과 단편논문(short paper)의 길이 제한은 각각 20쪽과 4쪽 이내이다.

2) 편집인의 글(editorial): 편집인의 글은 초빙에 의해서만 원고를 투고할 수 있으며, 본 학술지 편집위원회에서 결정하는 주제들을 다룬다.

3) 편집인과의 서신(letters to the editor): 본 학술지에 이미 출판된 학술 논문에 관한 간략한 평가나 흥미로운 새로운 아이디어를 편집인과의 서신으로 투고할 수 있다. 학술지 편집위원회에서는 투고된 서신을 편집할 수 있으며, 필요한 경우 해당 논문의 저자에게 회신을 요청할 수도 있다.

5.4 연구논문

원고는 국문제목, 국문요약과 국문키워드, 영문제목, 영문요약과 영문키워드, 본문, 감사의 글(필요 시), 참고문헌을 순서대로 포함한다.

1) 영문제목
제목은 공백을 포함해 길이가 40자를 초과하지 않도록 한다.
2) 영문요약과 키워드
요약은 무슨 연구를 어떻게 수행하였는지, 주된 연구결과와 그 중요성에 관해 간결하게 기술하여야 한다. 요약은 300단어를 초과해서는 안되며, 표나 참고문헌 번호를 포함하지 않은 하나의 문단으로 기술되어야 한다. 초록의 하단부에는 연구분야와 내용을 나타낼 수 있는 3 ~ 5단어 이내의 키워드를 기재하여야 한다.
3) 본문
a) 장절 제목: 장이나 절의 제목은 1. , 1.1, 1), a) 와 같이 4 단계 레벨로 표기할 수 있다.
b) 본문 중 참고문헌 인용: 참고문헌은 본문에서 처음 인용되는 순서대로 번호를 붙인다. 그리고 본문에서 참고문헌을 인용할 때는 해당 참고문헌의 번호를 [1, 4, 7] 혹은 [6-9]와 같이 각괄호 안에 기재한다.
c) 약어: 약어는 저자의 편의성보다는 독자에게 도움을 줄 수 있는 방식으로 사용되어야 한다. 따라서 약어는 가급적 제한적으로 사용하는 것이 바람직하다. 표와 그림을 포함해 본문에서 세 번 이상 등장하지 않는 약어의 사용은 가급적 파하라. 약어는 본문에서 처음 사용될 때 축약 이전의 형태로 정의되어야 한다.
d) 표: 표는 본문에서 인용되는 순서대로 아라비아 숫자로 번호를 붙인다. 표의 제목과 설명은 영어로 작성하며, 본문 내용을 읽지 않고도 이해할 수 있도록 간결 명료하게 작성한다
e) 그림: 그림은 본문에서 인용되는 순서대로 아라비아 숫자로 번호를 붙인다. 동일한 번호에 두 개 이상의 그림이 있는 경우, Fig. 1A, Fig. 1B와 같이 아라비아 숫자 뒤에 알파벳 대문자를 기입하여 구분한다. 자신이 그린 그림이 아니면 저작권자의 허락을 받아야 하며 각주에 이를 밝혀야 한다.
4) 감사의 글
필요한 경우, 본문 뒤에 감사의 글을 포함시킬 수 있으며, 연구비 지원 또는 다른 지원에 대한 내용을 명시할 수 있다.
5) 참고문헌
모든 참고문헌은 영어로 기술하며, 제출 원고의 내용과 분명히 관련이 있는 것들이어야 한다. 참고문헌은 본문에서 처음 인용되는 순서대로 번호를 붙인다. 참고문헌들은 반드시 원저 확인을 통해 출처를 검증하는 것이 필요하다.
다음 예시들을 참고하여 참고문헌들을 작성한다.

Journal Article

[1] S. Y. Hea and E. G. Kim, "Design and implementation of the differential contents organization system based on each learner's level," *The KIPS Transactions: Part A*, vol. 18, no. 6, pp. 19-31, 2011.

[2] S. Y. Hea, E. G, Kim, and G. D. Hong, "Design and implementation of the differential contents organization system based on each learner's level," *KIPS Transactions on Software and Data Engineering*, vol. 19, no. 3, pp. 19-31, 2012.

Book & Book Chapter

[3] S. Russell, P. Norvig, *Artificial Intelligence: A Modern Approach*," 3th ed., New York: Prentice Hall, 2009.

[4] J. L. Hennessy and D. A. Patterson, "Instruction-level parallelism and its exploitation," in *Computer Architecture: A Quantitative Approach*, 4th ed., San Francisco, CA: Morgan Kaufmann Pub., ch. 2, pp. 66-153, 2007.

[5] D. B. Lenat, " Programming articitical interlligence," in *Understanding Artificial Intelligence*, Scientific American, Ed., New York: Warner Books Inc., pp. 23-29, 2002.

Conference Proceedings

[6] A. Stoffel, D. Spretke, H. Kinnemann, and D. A. Keim, "Enhancing document structure analysis using visual analytics," in *Proceedings of the ACM Symposium on Applied Computing*, Sierre, 2010, pp. 8-12.

Dissertations

[7] J. Y. Seo, " Text driven construction of discourse structures for understanding descriptive texts," Ph.D. dissertation, University of Texas at Austin, TX, USA, 1990.

Online Source

[8] Thomas Claburn, Google Chrome 18 brings faster graphics [Internet], http://www.techweb.com/news/232800057/google-chrome-18-brings-faster-graphics.html.

6. 투고료 및 게재료

6.1 투고료

본 학술지에 원고를 투고할 때, 투고자는 1편당 일반 심사의 경우 50,000원(US $50), 급행 심사의 경우 350,000원(US $350)을 학회에 납부하여야 한다.

6.2 게재료

채택된 논문의 투고자는 논문의 게재를 위해 다음과 같은 논문 게재료를 학회 사무국에 납부하여야 한다.
- 인쇄쪽수가 1 ~ 6쪽인 경우, 100,000원
- 인쇄쪽수가 7쪽 이상인 경우, 100,000원 + 50,000원 추가 / 쪽당

6.3 은행계좌

- 한국외환은행: 232-13-01249-5 (예금주: 한국정보처리학회)
- 우체국: 012559-01-000730 (예금주: 한국정보처리학회)

7. 본 투고 규정은 2012년 9월 1일부터 효력을 발생한다.

입회 안내

국가가 지향하는 첨단 정보처리 산업과 기술혁신의 시대에 부응하여 첫째, 정보처리 학술활동의 활성화, 둘째, 정보처리 기술의 산학연 협동의 내실화, 셋째, 정보처리 기술의 국제화와 표준화 등 회원봉사 활동에 역점을 두고 정보화사회를 선도하는 명실상부한 정보처리 분야의 정통학회인 사단법인 한국정보처리학회에서는 정보처리분야에 종사하고 계시는 여러분들의 많은 입회를 바라고 있습니다.

주 요 목 적 사 업

1. 정보처리에 관한 각종 학술발표회 및 전시회 개최
2. 정보처리에 관한 지식 및 기술 보급에 관한 사업
3. 정보처리 기술의 상호 협조 및 정보 교환
4. 정보처리에 관한 표준화 사업
5. 국제적 학술 교류 및 기술 협력
6. 학회지 및 논문지 발간
7. 정보처리에 관한 문헌 발간
8. 기타 본 학회 목적 달성에 필요한 사업

(정관 제4조)

회 원 의 종 류 및 자 격

1. 특별회원 : 정보처리 분야 발전에 기여하고 본학회의 취지에 찬동하는 법인 및 단체.
2. 명예회원 : 학식과 덕망이 높고 본 학회의 발전에 크게 기여한 자.
3. 정 회 원 : 정보처리 관련 분야를 전공하여 학사학위 이상을 취득한 자 또는 정보처리 관련분야에서 2년이상 근무한 자.
4. 준 회 원 : 정보처리 관련학과 학생 또는 대학원생
5. 단체회원 : 도서관 또는 초·중·고 교육기관

(정관 제6조)

회 원 의 혜 택

1. 정보처리학회지(논설, 기술보고, 해설, 전망, 강좌, 단편정보 등 게재) 발행. 무료배포
2. 정보처리학회논문지 및 특집호(학술연구논문, 심사완료 후 게재) 발행.
3. 춘추계 학술발표회와 각종 학술행사에 참가 및 논문발표
4. 전문분과연구회의 활동자격과 각종 학술행사에 참가 및 논문발표
5. 국제 학술회의 활동 및 외국 학회에 참가 및 추천
6. 정보처리 및 기술발전에 업적이 있는 회원에게는 각종 학회상 수여

회 비

1. 특별회원 회비는 이사회의 결정에 따르면 종신회원·정회원·준회원·단체회원 회비는 다음과 같다.

구 분	종 신 회 원	정 회 원	준 회 원	단 체 회 원
연 회 비	600,000원	60,000원	40,000원	300,000원

※ 논문 구독료 각권 별도 2만원 (필요시 구독)

2. 회원가입은 학회 홈페이지를 통하여 회원정보를 입력하신후 회비를 신용카드 결제 및 아래의 은행으로 입금하여 주시기 바랍니다.
   한국외환은행 계좌번호 : 232-13-01249-5 예금주 : (사단)한국정보처리학회
   우 체 국 계좌번호 : 012559-01-000730 예금주 : 한국정보처리학회

문의처 : 140-750 서울특별시 용산구 한강대로 109, 1002호(한강로 2가 용성비즈텔)
사단법인 한국정보처리학회 사무국 귀하
전 화 : (02) 2077-1414(代) 팩 스 : (02) 2077-1472
홈페이지 : www.kips.or.kr e-mail : ysyun@kips.or.kr

연구회 안내

당 학회에는 현재 다음과 같은 연구회가 구성되어 있으며, 이들 연구회는 위원장을 중심으로 하여 현재 활발한 연구 활동을 하고 있습니다. 연구회에 가입을 원하시는 회원은 연구회 가입 원서를 작성하셔서 당 학회 사무국 또는 각 위원장에게 보내주시기 바랍니다. 회원 여러분의 많은 가입을 부탁드립니다. 연구회 발족 등에 관한 의견이 있으시면 학회로 연락 주시기 바랍니다.

e-Bridge 연구회

위원장 : 이정배 부총장 (부산외국어대학교)
전 화 : 051)509-5033
e-mail : jblee1120@naver.com

우정기술연구회

위원장 : 정 훈 부장 (ETRI)
전 화 : 042)860-6470
e-mail : hoonjung@etri.re.kr

IT 융합서비스연구회

위원장 : 박석천 교수 (가천대학교)
전 화 : 031)750-5328
e-mail : scpark@gachon.ac.kr

전산교육연구회

위원장 : 김형진 교수 (전북대학교)
전 화 : 063)270-4783
e-mail : kim@chonbuk.ac.kr

IT 정책연구회

위원장 : 오길록 교수 (숭실대학교)
전 화 :
e-mail : gilrokoh@paran.com

전산수학연구회

위원장 : 박진홍 교수 (선문대학교)
전 화 : 041)530-2224
e-mail : chp@omega.sunmoon.ac.kr

빅데이터컴퓨팅연구회

위원장 : 이필규 교수 (인하대학교)
전 화 : 032)860-7448
e-mail : pkrhee@inha.ac.kr

전자정부연구회

위원장 : 이재두 수석 (NIA)
전 화 : 02)2131-0370
e-mail : leejaedu@gmail.com

소프트웨어공학연구회

위원장 : 박용범 교수 (단국대학교)
전 화 : 031)8005-3220
e-mail : ybpark@dankook.ac.kr

정보통신융용연구회

위원장 : 오진태 부장 (ETRI)
전 화 : 042)860-4977
e-mail : showme@etri.re.kr

스토리지시스템연구회

위원장 : 신범주 교수 (부산대학교)
전 화 : 055)350-5417
e-mail : bjshin@pusan.ac.kr

지식및데이터공학연구회

위원장 : 진병운 박사 (ETRI)
전 화 : 042)860-6544
e-mail : bwjin@etri.re.kr

에너지그리드정보처리연구회

위원장 : 이봉재 센터장 (전력연구원)
전 화 : 042)865-5700
e-mail : leeboja@kepco.kco.kr

컴퓨터소프트웨어연구회

위원장 : 박두순 교수 (순천향대학교)
전 화 : 041)530-1317
e-mail : parkds@sch.ac.kr

한국정보처리학회 신용카드 결제신청서

◈ **납입방법 : 신용카드**

◈ **결재내용 : 학회 회비 / 세미나 참가비 / 논문 구독료 / 논문 게재료**

학 회 회 비	종신회원 ₩600,000( ) 정회원 ₩60,000( )
	준 회 원 ₩40,000( ) 기 타 (₩)
행 사 등 록 비	(₩)
논 문 구 독 료 (각 권당 2만원)	□소프트웨어 및 데이터 공학(KTSDE) □컴퓨터 및 통신 시스템(KTCCS) (₩)
논 문 게 재 료	( )권 ( )호 (₩)
기 타	(₩)

◈ **신용카드 사용내역서**

카 드 명	□ 신한카드 □ 국민카드 □ 비씨카드		결 재	일시불( )	※ 타카드 사용 불가
카드번호	□□□□ □□□□ □□□□ □□□□				
지불금액	원	카드유효기간	년 월	전 화	
소 속		성 명		서 명	
"상기 금액을 정히 지불합니다" 사단법인 한국정보처리학회					

※ 신한카드, 국민카드 및 비씨카드만 사용이 가능합니다.

※ 반드시 팩스로 회송바랍니다.

※ 학회 연회비 및 논문 구독료는 홈페이지에서 로그인 후 모든 카드로 온라인 카드 결재가 가능합니다.

☞ 보내실곳 : **한국정보처리학회**

전화 : (02)2077-1414 팩 스 : (02)2077-1472

http://www.kips.or.kr e-mail : ysyun@kips.or.kr

140-750 서울특별시 용산구 한강대로 109, 1002호(한강로 2가 용성비즈텔)

학 회 사 무 국

선임국장	송영민 (내선 5)	min@kips.or.kr	업무총괄 / 제회 / CUTE 행사 / SQMS 행사
국 장	김은순 (내선 2)	uskim@kips.or.kr	학회지 / 춘계학술대회 / 단기강좌 / 연구과제
과 장	이주연 (내선 1)	joo@kips.or.kr	JIPS(영문지) / IT21컨퍼런스 / 추계학술발표대회
과 장	윤영숙 (내선 3)	ysyun@kips.or.kr	회원 / 재무 / 국문지 / 홈페이지 및뉴스레터

- **사무국주소** : (04376) 서울특별시 용산구 한강대로 109, 1002호(한강로2가 용성비즈텔)
- **전 화** : 02) 2077-1414
- **팩 스** : 02) 2077-1472
- **대 표 메 일** : kips@kips.or.kr
- **홈 페 이 지** : www.kips.or.kr

정보처리학회지

제 24 권 제 3 호

등록일자 : 1994년 3월 31일
서기 2017년 5월 25일 인쇄
서기 2017년 5월 31일 발행

발 행 인 : 정 영 식

편 집 인 : 김 종 완

발 행 처 : 사단법인 한국정보처리학회 KIPS Korea Information Processing Society

(140-750) 서울특별시 용산구 한강대로 109, 1002호(한강로 2가 용성비즈텔)
전 화 : (02)2077-1414(代) 팩 스 : (02)2077-1472
홈페이지 : www.kips.or.kr 이메일 : kips@kips.or.kr

* 제작 : (주)이환디앤비 Tel : (02)2254-4301(代) <비매품>

정보처리학회지 특집원고 모집 안내

한국정보처리학회 학회지편집위원회에서는 '정보처리학회지'의 특집주제에 관련된 원고를 아래와 같이 모집하고 있습니다. 아래의 특집 주제에 관심있는 회원들의 많은 투고와 참여를 바랍니다.

게재호	특집주제
제24권 4호 (2017년 7월)	**드론 관련 기술과 응용**
세부내용	**1. 드론 고장 진단 기술** **- 안전성 확보를 위한 각종 safety 관련 기술 소개** **2. 드론 센서 기술** **- GPS, 고도계, 가속도계, 자이로스코프 등 관련 제품 및 기술 소개** **3. 드론 배터리 기술** **- 배터리 관련 기술 소개** **4. 드론 시스템 소프트웨어** **- 드론 제어 알고리즘 및 관련 소프트웨어 기술 소개** **5. 드론 프로세싱 시스템** **- 주제어 장치 제품 및 기술 소개** **6. 기타** **- 기타 드론과 관련된 응용 제품 및 기술 소개**
제출마감	담당편집위원(문의)
2017년 8월 27일(일)까지	조두산 교수(순천대학교) Tel. 061-750-3577 e-mail : mew26@snu.ac.kr

- 제출내용 : 특집원고 제목, 저자(성명, 소속, 연락처), 약력이 포함된 6~8페이지 원고
- 제출된 원고는 학회지편집위원회의 심사를 거쳐 게재여부를 결정합니다.
- 게재된 원고는 학회지 규정에 의거하여 소정의 원고료를 지급합니다.
- 접수 및 문의처 : 한국정보처리학회 사무국 김은순 국장 e-mail: uskim@kips.or.kr / Tel. 02-2077-1414(2)
- 원고 포맷은 e메일로 요청시 보내드립니다.

한국어 ▾ ⇌ 영어 ▾

새는 알에서 나오려고 투쟁한다. 알은 세계이다.
태어나려는 자는 하나의 세계를 깨뜨려야 한다.

The bird struggles to get out of the egg. The egg is the world. A man who is born must break a world.

언어는 달라도 똑같은 마음이 잘 전달되도록
네이버 인공 신경망 번역 기술(NMT)이 적용된 통/번역앱 파파고는
한국어/영어/일본어/중국어/스페인어/프랑스어 번역을 지원합니다

NAVER