논문 2019-1-14 http://dx.doi.org/10.29056/jsav.2019.06.14

블록체인 기반 시스템의 구조적 분석과 취약점 도출

김장환*

Structural Analysis and Derivation of Vulnerability for BlockChain based System

Jang-Hwan Kim*

요 약

지속적으로 확산되어져 가고 있는 블록체인 시스템과 블록체인 기반의 서비스 시스템의 구조를 분석하였다. 거래 쌍방 간의 신뢰 확보를 위한 제 3 자를 필요로 하지 않는, 분산화된 장부 암호화 시스템 소프트웨어 기술이다. 블록체인은 자료 구조적으로는 링크드 리스트 구조로 되어 있다. 블록체인은 거래 정보를 블록화 하여 다른 블록들과 연결해서 거래 정보를 관리한다. 해시 함수를 사용하여 블록화와 연결을 하게 된다. 결과적으로, 현재의 블록체인 시스템과 블록체인 기반의 서비스 시스템의 구조적 취약성을 발견하였다. 본 논문에서 제시한 블록체인 시스템과 블록체인 기반의 서비스 시스템의 구조적인 문제점 등이 해결되어지게 되면, 다양한 산업적 기여가 예상된다.

Abstract

I analyzed the structure of a block-chain system and a block-chain-based service system. It is a decentralized book encryption system software technology that does not require a third party to secure trust between the two parties. Block chains are structured in a linked list structure. The block chain manage transaction information by blocking the transaction information, in conjunction with other blocks. As a result, I have discovered structural weaknesses in current block-chain systems and block-chain-based service systems. Once these possible structural problems are resolved, I expect that the block-chain-based service system will make various industrial contributions.

한글키워드 : 노드, 블록 체인, 탈중앙화, 연결리스트, 작업 증명

keywords : node, Block-Chain, decentralization, linked list, Proof-of-Work

1. 서 론

블록체인 기술은 거래 쌍방 간의 신뢰 확보를 위한 제 3 자를 필요로 하지 않는, 분산화된 장부 암호화 시스템 소프트웨어 기술이다. 블록체인은 자료 구조적으로는 링크드 리스트 구조로 되어 있다. 앞으로 큰 영향과 변화를 가져올 블록체인에 대해서 분석하였다. 어떠한 배경에서 등장하게 되었으며 그 속에 담겨있는 원리와 기술들은 어떻게 동작하는지 또 어떻게 이루어져 있는지를 분석하였다. 또한 블록체인 기술의 활

* 성결대학교 공과대학 미디어소프트웨어학부
(email: jhkim@sungkyul.ac.kr)
접수일자: 2019.06.02. 심사완료: 2019.06.15.
게재확정: 2019.06.20.

용 현황과 앞으로의 과제는 무엇인지를 분석하였다. 가상화폐는 법정 화폐가 아닌 화폐로서 2000년대부터 등장하기 시작했다. 가상화폐는 금속화폐나 지폐와 같은 실물이 있는 것이 아닌, 전기적인 네트워크로 연결된 가상의 공간에서 전자적인 모습으로 통화 기능을 수행하는 가상의 디지털 형태의 화폐이다.

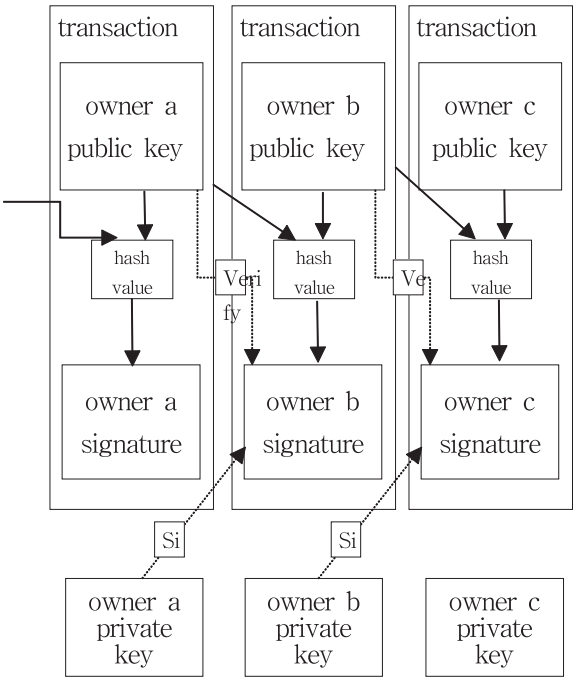

그림 1. 트랜잭션
Fig. 1. Transaction

그림 1과 같은 전자 서명 비대칭키 암호화 기술을 채택하여, 신규 가상화폐를 생성하고 거래 내역을 유지하는 시스템이다. 그동안의 금융 거래의 흐름은 제 3의 누군가와 자금 거래를 할 때 은행이라는 기관을 통해서 3자에게 전달했다. 그동안 우리가 흔히 사용해 온 이 시스템은 거래 은행에서 소유한 고객의 정보를 타 금융 기관들과 공유하지 않고, 원장 기록만 중앙 전산기의 데이터베이스에서 관리한다. 또 금융 기관은 고객의 자금 거래 시의 처리를 해주는 업무를 수행하는 일로 수수료를 징수한다. 이 시스템은 이용자가 금융 기관을 신뢰하고, 은행을 관리하는 중앙 정부가 금융 기관 감독업무를 제대로 하고 있다는 것을 전제로 한 것이다. 기존 금융 기관 시스템은 원장 기록을 중앙 전산기에 관리하면서 거래를 유지해 나간다. 또 송금 절차를 수행하는 과정에서도 모든 절차가 금융 기관에서 수행 되어 진다. 만약 금융 기관의 중앙 전산기의 데이터베이스가 오동작하거나, 금융 기관의 중앙 전산기의 데이터베이스의 기록이 사라지게 되거나, 해커에 의해서 해킹을 당하게 된다면 그 재산을 잃게 되는 것이다. 따라서 금융 기관은 중앙 전산기의 보수 및 유지에 많은 비용을 투입하고, 중앙 전산기가 해커에 의해서 해킹을 당하지 않고 조작된 거래 정보가 기록되지 않도록 막대한 보안 기능 시스템을 설치 운용하고 있는 것이다. 상당한 자금을 들여서 인력을 고용하고 중앙서버와 시스템 구축을 하고 있다. 또한 이와 같은, 단일 실패 지점 문제를 해결하기 위한 방법으로 다중화 시스템 구축을 하고 있다. 복제나 분산 처리를 통한 2중, 3중의 다중화 시스템 구축을 통하여 단일 실패 지점을 없애 버리는 방법이다. 그러므로 기존 금융 기관 시스템에서는 이러한 다중화 처리가 되어 있으므로 어느 순간에 금융 기관 시스템 기록이 망실되는 사고는 쉽게 발생되지는 않는다. 거래 정보를 모든 참여자에게 공개하여 누구나 거래 정보를 만들 수가 있고, 거래 정보를 모든 참여자에게 복제하여 사본을 유지하고, 또한 사본 들끼리 동기화를 시켜서, 기존 금융 기관의 다중화 시스템 정도가 아닌 수만중화, 수 억중화 처리를 통해 거래 기록이 변질되는 상황을 근본적으로 막아버릴 수 있는 방법이 바로 블록체인 기술이다[1]. 본 연구에서는 이러한 블록체인 시스템의 개념과 블록체인 기반 서비스 시스템의 현황을 살펴보고, 현재의 관련

기술이 가지고 있는 구조적인 문제점에서 발견할 수 있는 과제들을 모색해 보고자 한다.

2. 블록체인

블록체인 기술은 거래 쌍방 간의 신뢰 확보를 위한 제 3 자를 필요로 하지 않는, 분산화된 장부 암호화 시스템 소프트웨어 기술이다. 거래 내역이 기록된 것을 수억 명이 넘는 사람들이 공유하도록 하는 것이다. 기존 시스템에서는 중앙 전산기의 데이터베이스만 해킹하여 데이터를 조작하면 되지만, 이 블록체인 시스템 내 거래 정보 데이터를 조작하려고 해도, 블록체인 상에 연결된 다수의 컴퓨터 정보를 조회하면 조작 사실을 바로 알아 챌 수 있다. 조작을 하려면 블록체인으로 연결되어 있는 모든 노드의 정보를 모두 조작해야 가능하다. 사실상 이것을 모두 조작하는 일은 매우 어려운 일이하다. 블록체인은 매우 많은 노드가 데이터를 공유하게 함으로써 실제 부정행위가 발생되지 않도록 시스템이 작동되게 하는 것이다. 블록체인은 블록체인을 구성하는 노드들이 체인처럼 기존의 노드에 연결을 시켜 나간다. 구조적이고 기술적인 측면에서 보면 블록체인은 블록으로 이루어진 링크드 리스트이다. 블록은 블록 헤더와 거래정보, 기타 정보로 구성된다. 블록 해쉬는 블록의 식별자 역할을 한다. 블록 해쉬는 블록 헤더를 해쉬 함수로 계산한 값으로, 블록 헤더가 중요한 정보 역할을 하는 이유는 블록의 식별자 역할을 하는 블록 해쉬가 바로 이 블록 헤더의 6가지 정보를 입력 값으로 하여, 그림 2에서와 같이 구해지기 때문이다. 블록 해쉬는 32바이트의 숫자 값이다.

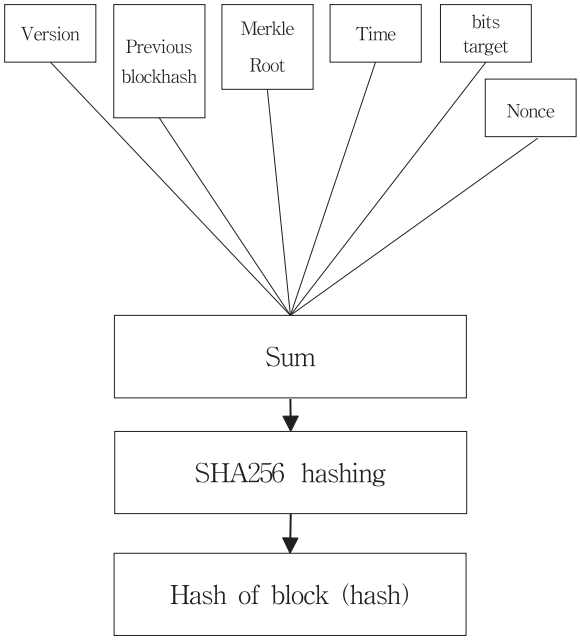

그림 2. 블록해시를 도출해내는 대략적 과정
Fig. 2. Approximate process of deriving a hash of a block

블록 해쉬 값은 블록 헤더를 해쉬한 값이다. 자료 구조적 관점에서 블록체인은 오직 링크드 리스트이고, 그런 블록체인이 신뢰를 얻을 수 있게 된 첫 번째 핵심적인 요소인 작업 증명이란 그림 3에서와 같이 블록 헤더 요소들 중 하나인 논스(nonce)값을 구해서 마지막으로 블록 해쉬 값을 구하고, 이 블록 해쉬 값을 식별자로 가지는 새로운 블록을 만들어내는 것이다. 해쉬 함수의 특성상, 어떤 해쉬 값이 될 때까지 무작위로 입력 값을 계속 바꿔가며 해쉬 값을 계산해보면서 찾아내야 한다.

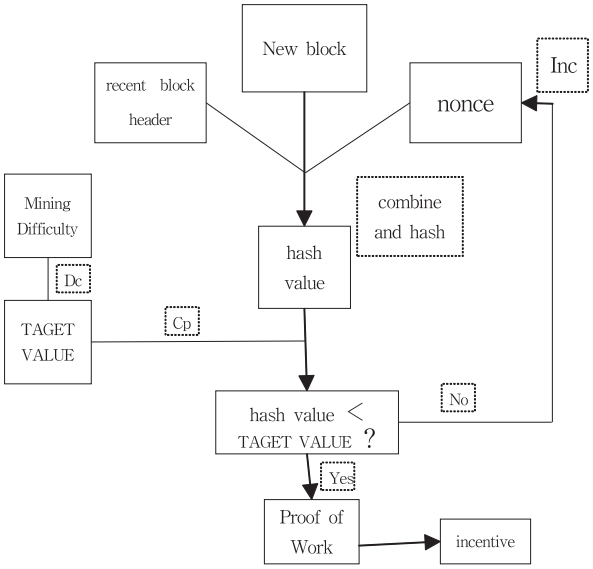

그림 3. 작업증명 도식화
Fig. 3. The Diagram of Proof-of-Work

블록 체인의 두번째 핵심적인 요소는 충돌 해소이다. 블록 체인에서는 신규 거래 정보가 생성되면, 이 정보는 체인 네트워크로 연결되어져 있는 다른 노드로 전파되어지게 된다. 그 거래 정보를 전파 받은 노드에서는 당해 거래가 유효한 거래인지를 판정한 다음, 그 정보를 아직 블록 생성이 시작되기 전의 블록에 추가한 후에, 연결된 다른 노드에 그 정보를 전달한다. 전달받은 다른 노드 같은 작업을 반복하여, 또 다른 노드에게 정보를 전달한다. 이와 같은 반복 작업을 통하여 네트워크 상의 모든 노드에 전달된다. 이때 네트워크 상의 분기가 일어나 충돌이 발생될 때에는, 작업 증명이 많이 수행되어 노드 연결 길이가 더 길어져 있는 쪽을 선택한다. 즉, 충돌 해소의 기준은 작업 증명이 상대적으로 많이 수행되어져서, 노드 연결 갯수의 길이가 더 길어진 쪽을 선택하여 충돌을 해소해 나간다.

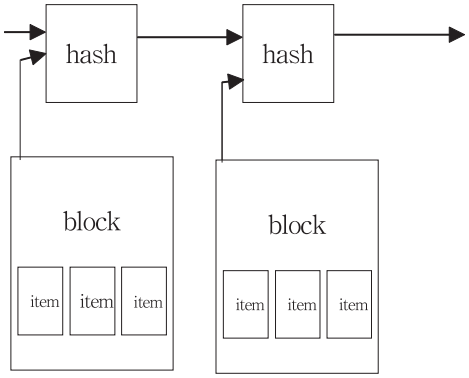

그림 4. 타임스탬프 서버
Fig. 4. Timestamp Server

블록체인은 그림 4에서와 같이 타임스탬프 서버의 운용을 통해 당해 자료가 해쉬 처리 과정에 진입하기 위해서 당해 시각부터 존재했음을 입증한다.

블록이 평균 10분당 하나가 생성되는 이유는 그림 5의 난도의 조절 과정과 타임 스탬프서버에 있다. 블록 생성은 평균 10분이 소요될 정도의 연산량이 큰 작업이다.

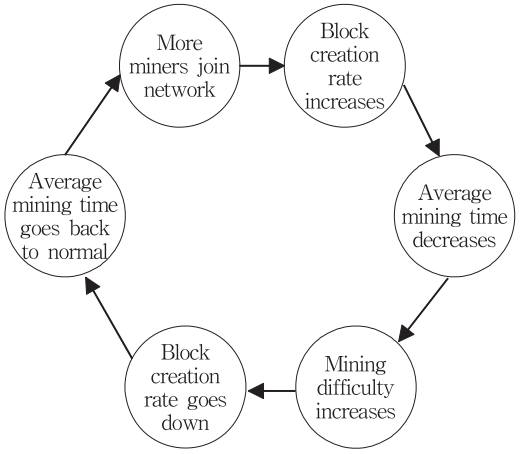

그림 5. 난도의 조절 과정
Fig. 5. The Process of Control of Difficulty

거래 정보의 해쉬 값은 당해 거래가 포함된 블록의 머클해쉬(merklehash) 계산의 입력 값으로 사용되며, 머클해쉬는 블록 해쉬의 계산에서 입력 값으로 사용된다.

블록 해쉬는 다음 블록의 프리비어스 블록해쉬(previous blockhash)값으로 저장되고, 이 프리비어스 블록해쉬는 다음 블록의 블록 헤더 정보로서, 다음 블록의 블록 해쉬를 계산하는데 있어서 입력값으로 사용된다. 따라서, 그림 6에서와 같이 어떤 거래에 관한 정보가 변경되면 그 거래에 관한 정보가 포함된 머클트리의 머클해쉬가 변경되고, 연쇄적으로 머클해쉬가 변경되면 블록 해쉬가 변경된다.

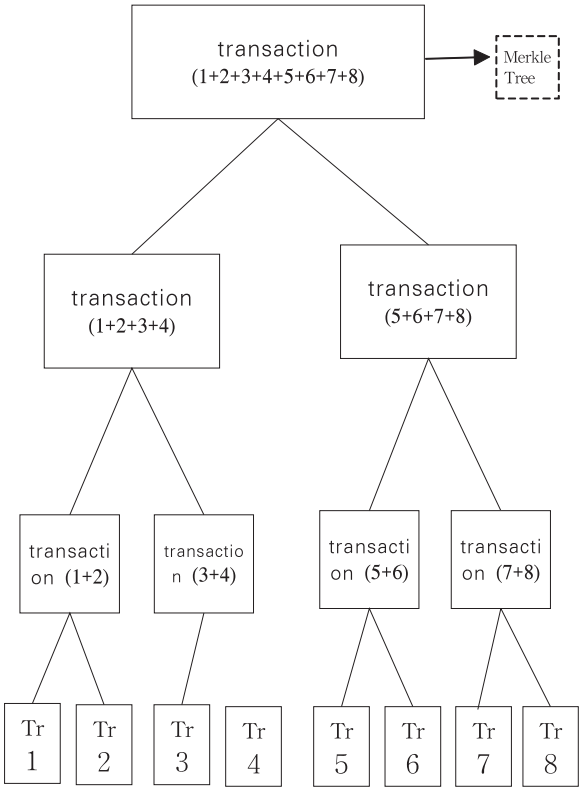

그림 6. 머클트리
Fig. 6. Merkle Trees

3. 블록체인 서비스 시스템의 구조적 결함 분석

블록체인의 핵심요소 중 첫 번째는 작업 증명이다. 그러나, 시중에 구현되어져 있는 블록체인 기반의 저작권 관리 시스템[2]의 경우, 논스 값을 사용하지 않고 있다. 따라서, 예외적 상황 처리가 발생할 경우에는 정상적인 작동을 보장할 수가 없다. 또한 저작물로 보호되어져야 할 가치 판단을 수행할 인증 기관이 없으므로, 탈 중앙화 응용으로서는 한계성을 가지게 된다.

블록체인 기반 스마트 계약 시스템[3]의 경우, 악의적인 계약 위배 사항 발생에 대한 법적 장치가 없어서 한계성을 가지게 된다.

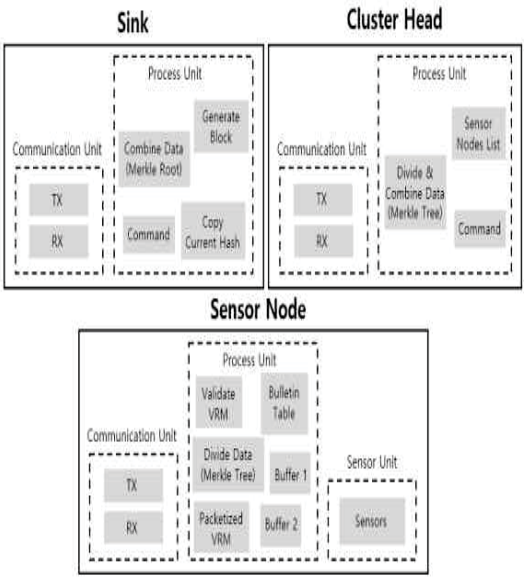

그림 7. Bulletin기법의 블록체인을 적용한 무선 센서 네트워크 아키텍처
Fig. 7. Blockchain with Bulletin Scheme in Wireless Sensor Networks

그림 7의 무선 센서 네트워크의 Bulletin 보안 기법[4][5]을 적용한 블록체인 시스템의 경우, AP

level에서 적용하면 될 보안 기능 처리를, 과도하게 센서 노드(Sensor Node)에 적용하므로 인하여, 그림 8에서 나타나고 있듯이[6], 전체 네트워크의 성능을 현저하게 감소시키게 되므로, 탈 중앙화 응용으로서는 한계성을 가지게 된다.

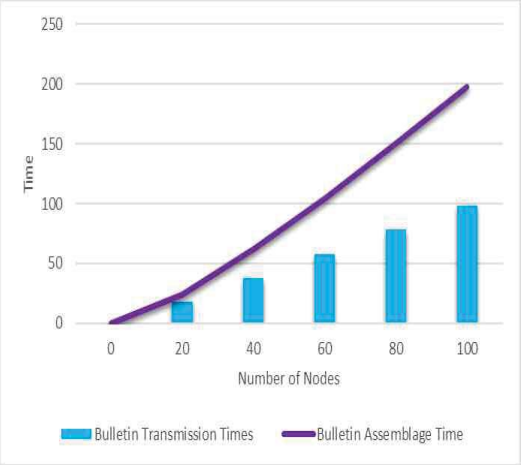

그림 8. 노드 수에 따른 소요 시간
Fig. 8. Time required by the number of nodes (Blockchain with Bulletin Scheme in Wireless Sensor Networks)

그림 9의 P2P 파일 공유 시스템에서의 블록체인을 활용한 멀웨어[7][8] 유포 방지 시스템[9]의 경우, 멀웨어가 네트워크상에서 어디에 있는지를 알아야만 블록체인을 적용할 수 있으므로, 탈 중앙화 응용으로서는 한계성을 가지게 된다.

결국, 블록체인 기술의 트랜잭션 프로토콜에 기반한 구조적 분석을 실시한 결과 다음과 같은 취약성이 도출된다.

모든 연산 자원의 25%가 나쁜 의도를 품었을 때 나머지 75%가 생성한 체인을 따라 잡을 확률은 블록이 6 개인 경우 약 0.137%, 블록이 13 개인 경우 약 1/10^6, 162개인 경우 1/2^256의 확률이다. 따라서 비트코인의 경우 어떤 거래로 송금한 암호 화폐를 다른 거래에서 사용하기 위해선 최소 6개의 블록을 생성해 확정될 때까지 기다려야하는 규칙이 적용되어 있다. 이처럼 누군가가 기존의 체인을 끊고 과거의 체인을 잇는 것은 상당히 낮은 확률이지만 100%가 아니고, 누구나 자원을 투입하면 합법적으로 가능하기 때문에 취약점이라고 생각된다.

비트코인 시스템에서는 익명 처리로 인하여 해킹이 훨씬 쉽게 발생하게 된다. 데이터베이스 회복 기술에서 개발되어져 있는 기술을 구비하고 있지 않아서, 거래의 전산 기록 중에 발생할 수 있는 시스템 오류에 대한 취약성에 노출되어져 있고, 또한 분산 데이터베이스 기술에는 구비되어져 있는 조정 기능이 결여되어져 있어서, 심각한 오류를 일으킬 수 있는 문제점을 가지고 있다. 지속적으로 각각의 노드 들에 축적되게 되는 블록 용량의 문제, 각각의 노드 들의 처리 성능 차이로 발생할 수 있는 문제점 등과 같은 많은 구조적인 결함을 가지고 있다.

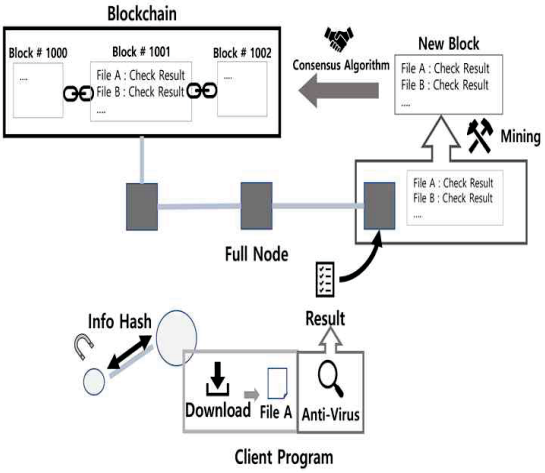

그림 9. P2P 파일 공유 시스템에서의 멀웨어 유포 방지 블록체인 시스템
Fig. 9. The prevention of Malware Distribution on P2P File Sharing System Using Blockchain

4. 결 론

블록체인은 자료 구조적으로는 연결 리스트 구조로 되어 있다. 블록체인은 블록 형태의 거래 정보가 연결 리스트 구조로 이어져 만들어진 블록들의 모음이다. 본론에서 서술한 해결되어져야 할 많은 구조적인 취약점 들을 보완해 나가게 되면, 블록체인 기술은 공급 체인 관리, 은행 업무, 사이버 보안 등의 수 많은 서비스 산업 분야에 점진적으로 확대되어 사용될 것으로 예상된다.

참 고 문 헌

[1] Jiao Li, Gongqian Liang, and Tianshi Liu, “A Novel Multi-link Integrated Factor Algorithm Considering Node Trust Degree for Blockchain-based Communication”, KSII Transactions on Internet and Information Systems (TIIS), Vol. 11, No. 8, pp.3766-3788, Aug. 2017.

[2] J.S. Hwang and H.G. Kim, “Design and Implementation of Copyright Management System based on the Blockchain”, the 2018 KICS proceedings, Nov. 2018.

[3] G. J. Tak and I. R. Jeong, “Survey on Pseudo-Random number generator based on Smart Contract”, the 2018 KICS proceedings, Nov. 2018.

[4] Gabin Lee, Inwhee Joe, and Jinho Cho, “A Safe Key Distribution Mechanism in DTN protocol using the concept of BSP”, Korean Society for Internet Information, pp.133-134, Nov. 2016.

[5] Sunggyun Jang, Jinyeong Kang, and Inwhee Joe, “An Efficient Device Authentication Protocol Without Certification Authority for Internet of Things”, Wireless Personal Communications, Vol. 91, pp.1681-1695, Dec. 2016.

[6] Y. J. Lee, J. Y. Kang, and In Whee Joe, “Blockchain with Bulletin Scheme in Secure Wireless Sensor Networks”, the 2018 KICS proceedings, Nov. 2018.

[7] David Dittrich and Sven Dietrich, “P2P as botnet command and control: a deeper insight”, 2008 3rd International Conference on Malicious and Unwanted Software (MALWARE), Virginia, USA, pp.41-48, Oct. 2008.

[8] Ganorkar, Shaunak Sanjay, and Kamalanathan Kandasamy, “Understanding and defending crypto-ransomware”, ARPN Journal of Engineering and Applied Sciences, Vol. 12, No. 12, pp.3920-3925, Jun. 2017.

[9] S.H. Kim and I.R. Jeong, “The prevention of Malware Distribution on P2P File Sharing System Using Blockchain”, the 2018 KICS proceedings, Nov. 2018.

저 자 소 개

김장환(Jang-Hwan Kim)

1980년 서울대학교 경제학학사
1997년 한국과학기술원 전산학석사
2003년 충북대학교 전산학박사
1984년～1988년 쌍용정보통신 연구원
1988년～1993년 Qnix Data System 연구원
1993년～1998년 SK Telecom 중앙연구원 연구원
1998년～2005년 대덕대 교수
2005년～현재 성결대 공대 미디어소프트웨어학부 교수
2011년 9월～2012년 8월 University of California, Los Angeles/ Faculty (Professor)
2017년 9월～2018년 2월 University of California, Los Angeles/ Faculty (Professor)