Journal of Digital Convergence
Vol. 19. No. 6, pp. 233-238, 2021

ISSN 2713-6434 / eISSN 2713-6442
https://doi.org/10.14400/JDC.2021.19.6.233

블록체인 기반의 트랜잭션 향상을 위한 영지식 증명 연구

안병태
안양대학교 교양대학 교수

A Study of Zero-Knowledge Proof for Transaction Improvement based Blockchain

Byeongtae Ahn
Professor, Liberal & Arts College, Anyang University

요 약 블록체인 기술은 모든 거래를 축적하고 저장하며 모든 트랜잭션의 내용을 확인하기 위해 데이터 자체는 압축되지만 확장성이 제한된다. 또한 거래 유형별로 별도의 검증 알고리즘을 사용하기 때문에 거래 규모가 커질수록 검증 부담이 커진다. 기존 블록체인은 사양이 낮은 서버를 사용하여 블록 싱크가 되지 않기 때문에 네트워크에 참여할 수 없다. 이러한 문제로 인해 시간이 지날수록 블록체인 네트워크의 데이터 크기가 커지고 자원이 풍부한 사용자를 제외하고는 네트워크 참여가 불가능하다. 따라서 본 논문에서는 일반 동작 검증을 위한 영지식 증명 알고리즘을 연구함으로써 트랜잭션을 향상시켰다. 이 시스템에서는 일반 동작 검증이 가능한 영지식 회로 생성기 설계와 검증자 및 검증자의 최적화도 수행하였다. 그리고 키 생성을 최적화하기 위한 알고리즘을 개발하였다.

주제어 : 영지식, 검증, 트랜잭션, 블록체인, 이더리움

Abstract Recently, blockchain technology accumulates and stores all transactions. Therefore, in order to verify the contents of all transactions, the data itself is compressed, but the scalability is limited. In addition, since a separate verification algorithm is used for each type of transaction, the verification burden increases as the size of the transaction increases. Existing blockchain cannot participate in the network because it does not become a block sink by using a server with a low specification. Due to this problem, as the time passes, the data size of the blockchain network becomes larger and it becomes impossible to participate in the network except for users with abundant resources. Therefore, in this paper, we are improved transaction as studied the zero knowledge proof algorithm for general operation verification. In this system, the design of zero-knowledge circuit generator capable of general operation verification and optimization of verifier and prover were also conducted.

Key Words : Zero-Knowledge, validation, transaction, BlockChain, Ethereum

1. 서론

블록체인 기반 분산 애플리케이션 시장은 2019년 약 32억 달러에서 2024년 600억 달러 이상으로 성장할 것으로 예상된다. 이 중 수익 모델로 '트랜잭션 처리'시장은 전체의 55 %에 이를 것으로 예상된다. 즉, 블록체인 기반의 분산 애플리케이션은 일반적으로 오픈소스 기반으로 제공되기 때문에 콘텐츠 사용료가 아닌 거래 수수료를 사용자가 받아들일 수 밖에 없다. 따라서 거래를 효율적으로 처리하는 기술의 경제적 가치는 매우 긍정적이다.

*Corresponding Author : Byeongtae Ahn(ahnbt@anyang.ac.kr)
Received April 6, 2021 Revised April 29, 2021
Accepted June 20, 2021 Published June 28, 2021

지난 10 년 동안 수많은 블록체인 구현이 플랫폼으로 등장했지만 거래 축적 및 저장 측면에서 큰 혁신은 없었지만 복잡한 운영을 지원하기 때문에 체인 데이터를 검증해야하는 부담이 증가했다. 따라서 향후 등장할 다양한 블록체인 플랫폼에서 공통적으로 사용할 수 있는 검증 모듈을 만들어 블록체인의 구조 혁신을 주도 할 필요가 있다. 이더리움의 경우 개인이 풀 노드를 운영하기는 이미 어렵고, 앞으로는 충분한 컴퓨팅 자원을 보유 할 수 있는 대기업이나 대기업만이 풀 노드를 운영 할 수 있다. 이러한 요인들은 블록체인의 중앙 집중화로 이어질 것이며,이 문제는 지식 증명 기술이없는 가상 머신을 통해 데이터 저장 및 검증에 필요한 리소스를 줄임으로써 해결할 수 있다. 따라서 본 논문에서는 일반 동작 검증이 가능한 영 지식 증명 알고리즘을 개발하고 일반 동작 검증이 가능한 영 지식 회로 생성기를 설계 하였다. 또한, 영 지식 증명 알고리즘을 가상 머신에 적용하고 테스트하여 트랜잭션 성능을 향상시킬 수 있다. 이 논문의 2장에서는 관련 연구를 소개하고 3 장에서는 국내외 사례를 소개한다. 4 장에서는 거래 검증이 가능한 알고리즘을 제안하고, 5 장에서는 가상 머신에 적용할 영 지식 회로를 설계한다. 마지막으로 섹션 6은 결론과 향후 작업을 제시한다.

2. 관련연구

블록체인 기술은 UTXO (Unspent Transaction Output)로 만든 단순한 유형의 블록체인과 State Tree를 다루는 복잡한 유형의 블록체인으로 나눌 수 있다[2]. 현재 단순한 형태의 블록체인에서 영 지식 증명은 일부 트랜잭션 처리에서만 프로토콜 수준에서 사용된다. 그러나 일부 복잡한 형태의 블록체인은 스마트 컨트랙트를 사용하지만 상위 레이어에서 구현되기 때문에 성능 및 활용 측면에서 제한이 있다. 제안된 SNARK 알고리즘을 통해 생성된 단일 작업의 증명 크기는 약 1,500 바이트 (1.5KB)이다[1]. 이러한 블록체인 기반의 분산 애플리케이션은 일반적으로 오픈 소스 기반으로 제공되기 때문에 콘텐츠 사용료가 아닌 거래 수수료를 사용자가 받아 들일 수밖에 없다. 따라서 거래를 효율적으로 처리하는 기술의 경제적 가치는 매우 긍정적이다. 모든 검증 노드가 블록 검증에 참여하지 않더라도 모든 노드가 참여한 것과 동일한 보안 강도로 일반 동작을 검증하고 영 지식 증명 기술을 사용하여 검증함으로써 모든 트랜잭션을 저장하지 않고 전체 트랜잭션을 저장하는 것과 동일한 효과를 제공한다[2].

현재 개인 정보 이용 가치가 높아지면서 개인 정보 제공 방안에 대한 논의가 활발히 진행되고 있다. 현재 개인 정보를 제공하는 가장 일반적인 방법 중 하나는 개인 정보를 이용하여 개인의 동의를 얻고 개인 정보를 이용하는 단체다. 그러나 위의 방법에는 두 가지 문제가 있다. 첫째, 개인 정보를 위해 기관에서 요구하는 정보 이상의 정보가 노출되고 있다. 회사가 개인 정보를 요청할 때마다 신뢰할 수 있는 당사자가 해당 정보에 대한 인증 정보를 회사에 제공해야하는 문제가 있다. 위의 문제점을 해결하기 위해 본 논문에서는 zk-SNARK (zero-knowledge Succinct Non-interactive ARgument of Knowledge) 기법과 블록체인을 이용한 개인 정보 보호 개인 정보 관리 방법을 제안한다[5]. zk-SNARK는 기존 ZKP보다 간결하고 비대화 형 환경에서 적용할 수 있도록 수정한 것이다. 이 로직은 2012년에 처음 제안되었으며, 그 특성상 ZKP는 블록체인 환경에서 구현될 수 있다. zk-SNARK를 사용하는 블록체인 거래의 경우, 거래의 유효성은 수신자, 발신자, 이체 금액과 같은 정보를 노출하지 않고 송수신 노드 이외의 노드로 전달할 수 있다. ZCash는 zk-SNARK의 첫 번째 응용 프로그램이며 관련 내용은 이더리움의 Byzantium 하드 포크에 적용되었다 [3]. zk-SNARK는 크게 두 부분으로 나뉘는데, 하나는 증명할 문제를 특정 형태로 변환하는 과정이고 다른 하나는 변환 된 문제를 이용한 실제 교정 과정이다. 개인 정보가 보호되는 개인 정보 관리 기술은 zk-SNARK를 통해 개인 정보를 제공 할 때 정보의 개인 정보 보호와 신뢰성을 보장 할 수 있다. 또한 블록체인을 통해 데이터의 무결성을 확보하면서 개인 정보 데이터를 관리 할 수 있으며, 기존 인증 방식보다 개인 정보 공유를 보다 쉽게 수행 할 수 있다[4].

3. 국내.외 사례

블록체인 가상 머신 기술을 보유한 여러 회사가 있다. 가장 대표적인 가상 머신은 이더리움의 가상 머신 인 EVM다. EVM은 최초의 블록체인 가상 머신이며 EVM을 기반으로하는 이더리움은 스마트 계약, 토큰 및 분산 애플리케이션 (Dapps)을 위한 기본 플랫폼으로 성장했다. 그리고 많은 블록체인 프로젝트가 메인 넷을 만들 때 이더리움의 EVM을 사용하고 있다. 현재 이더리움은 이더리움 2.0으로 업그레이드 할 계획이며 이더리움 2.0이

도입되면 현재 가상 머신 EVM이 eWASM으로 변환된다. EOS-VM은 EOS.IO가 만든 가상 머신으로 블록체인 산업에 국한되지 않고 게임 엔진, 데이터베이스, 웹 프레임 워크와 같은 기존 소프트웨어 개발 분야에서 사용될 것으로 예상된다. EOS-VM은 블록체인 시스템 전용 가상 머신으로 최초의 블록체인 가상 머신인 EVM에 비해 개발 자원(CPU) 절약, 블록체인 확장성 향상, 개발 효율성 향상을 기대할 수 있다[5].

Tron의 가상 머신 TVM은 이더리움의 EVM을 기반으로 개발되었으며 이더리움과 호환됨으로써 특성화되었다. 고유한 가상 메모리 메커니즘을 설계함으로써 실제로 사용되는 메모리 양을 크게 줄일 수 있으며 개발자에게 거의 무제한의 메모리 용량을 제공하여 분산형 애플리케이션의 운영 비용을 크게 줄일 수 있다. 또한 컴파일러를 최적화하여 리소스를 절약할 수 있다. Table 1 은 국내. 외 사례를 나타낸 것이다.

Table 1. Domestic & International cases

Coin Name	Consensus Method	Characteristic	Total Amount	Compare
Ethreum	EVM	Turing completeness as the first blockchain virtual machine.	$13 billion	Focus on decentralization and security.
EOS	EOS-VM	Consensus algorithm similar to indirect democracy.	$2.4 billion	Value for scalability.
Tron	TVM	EVM-enhanced virtual machine featuring Ethereum compatibility.	$1.8 billion	

현재 국내 블록체인 기술은 주로 분산 원장 및 합의 알고리즘과 같은 메인넷과 관련된 기본 기술에 편향되어 있다. 국내 기술 생태계의 특성상 글로벌 시장을 주도 할 수 는 영역은 메인넷 영역이 아닌 분산 응용 영역이다. 그리고 현재 분산 애플리케이션에 필요한 복잡한 작업을 효율적으로 검증 할 수 있는 영 지식 증명 기반 가상 머신은 없다. 따라서 다양한 분산 애플리케이션과 스마트 컨트랙트 실행 환경에 적용 할 수 있는 영 지식 증명 기반의 코드 검증량 향상 시스템을 설계하여 향후 성장 잠재력이 큰 분산 애플리케이션 기반 기술이 될 것이다[6].

4. 트랜잭션 검증을 위한 알고리즘

영점 증명은 다음 세 가지 조건을 충족해야 한다.

* 완전성 : 조건이 참이면 신뢰할 수 있는 검증자는 신뢰할 수 있는 증명자에 의해 이를 이해할 수 있어야 한다.
* 건전성 : 조건이 거짓 일 때, 부정직한 검증자는 거짓말로 조건이 참임을 검증인에게 결코 설득 할 수 없다.
* 영지식 : 조건이 참이면 검증자는 이 조건이 참이라는 사실 외에는 아무것도 알지 못한다[7].

이 연구는 사용자가 원하는 다양한 유형의 트랜잭션과 사전 정의된 유형의 트랜잭션에 대해 영 지식 증명을 활용하려고 한다. 현재 영 지식 증명의 증거를 생성 할 수 있는 회로는 미리 정의된 형식으로만 작업을 수행할 수 있다. 이를 사용자가 원하는 다양한 거래에 활용하기 위해서는 일반적인 동작을 확인할 수 있는 회로가 필요하다. 일반 작업은 특정 사전 정의 작업이 아니라 보편적이고 다양한 작업을 의미한다. 이에 연구팀은 일반적인 동작을 확인할 수 있는 회로를 연구하고 이를 가상 머신에 적용하는 방법을 설계했다[8]. Fig. 1.은 일반적인 작동 확인을 위한 회로 생성기와 키 생성기의 두 요소 조합을 보여준다. 회로의 출력 C는 프로그램 또는 주 입력 값에 의존하지 않고 l, n 및 T 값에만 의존하기 때문에 보편적이다[9]. 이 경우 프로그램 크기가 증가함에 따라 저장 비용이 크게 증가했다. 새로 생성된 영 지식 증명 알고리즘의 경우 데이터 크기가 증가한다. 회로 생성기와 영 지식 알고리즘은 서로 독립적이다. 회로에 적용할 회로 생성기와 영 지식 증명 알고리즘이 독립적이면 보다 유연한 시스템을 구축할 수 있다[10]. Fig. 3.은 일반적인 작동 확인을 위한 회로 생성기와 키 생성기의 두 요소 조합을 보여준다. 회로의 출력 C는 프로그램이나 주 입력 값이 아닌 값에만 의존하기 때문에 보편적이다. zk-SNARK와 같은 회로 검증 시스템과 결합하면 검증 시스템의 매개변수도 보편적이다. 이 경우 단일 키 생성으로 모든 프로그램을 검증 할 수 있으며 그 후 주어진 계산 범위에 적합한 키를 선택할 수 있다. 따라서 각 프로그램에 대한 키 생성 비용을 줄일 수 있다[11].

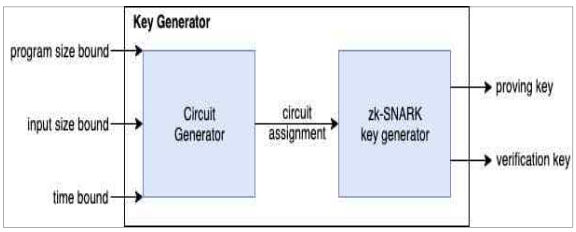

Fig. 1. Key Generator for General Operation Validation

Fig. 2.에서 블록 생성에 대한 권한은 일반 동작 검증을 위해 검증자와 검증자를 통해 부여된다.

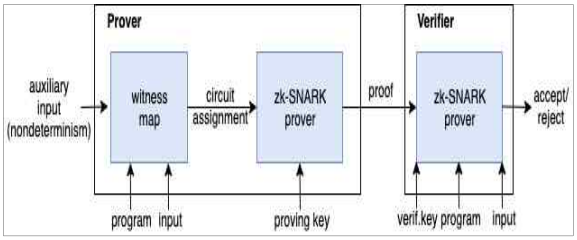

Fig. 2. Prover and verifier for general operation validation

검증자 V는 검증 키 vk,, 그리고 증거 π를 입력 값으로 사용하여 증거 π가 유효한지 확인한다. V에서의 작업은 두 부분으로 구성된다[12].

5. 영 지식 회로 설계

모든 거래 데이터를 저장하는 블록체인의 특성으로 인해 블록체인의 데이터는 시간이 지남에 따라 계속 증가한다. 거래 데이터 저장에 영 지식 증명 기술을 적용하면 실제 데이터를 잘라내고 데이터 증명만 남기고 데이터를 압축하여 데이터 저장 공간을 절약할 수 있다. 시간이 지남에 따라 블록체인의 데이터는 점진적으로 축적되고 이에 따라 전체 노드를 운영하는 데 필요한 컴퓨팅 리소스가 점차 증가할 것이다[14]. 가상 머신을 수정하기 위해서는 구조를 이해해야 한다. 따라서 Fig. 3.은 이더리움 가상 머신의 아키텍처 및 실행 흐름도를 보여준다. 가상 머신의 실행 방식을 이해 한 후에는 영 지식 기술을 적용하기 위해 가상 머신의 어떤 부분을 수정해야 하는지 파악해야 한다[13].

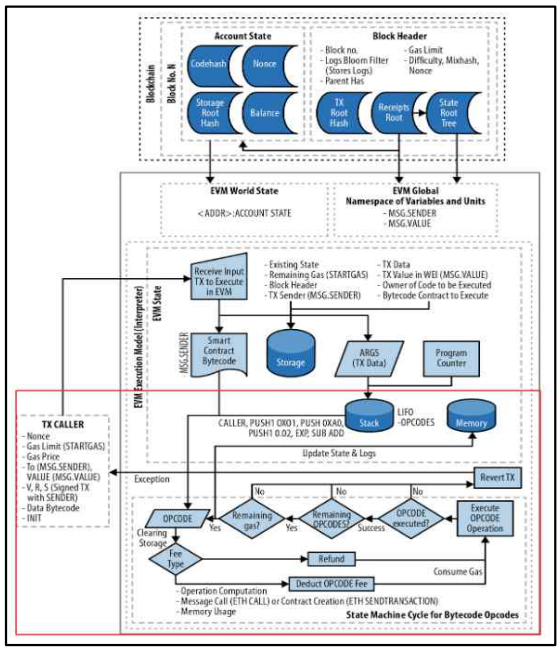

Fig. 3. Architecture & Excution Flow Chart of Ethereum Virtual Machine

트랜잭션을 실행하려면 앞서 언급 한대로 이더리움 바이트 코드로 변경해야 한다. 이러한 바이트 코드는 opcode라고 하는 것으로 분해되어 스택에 쌓여 하나씩 실행된다. opcode가 실행되기 전에 가상 머신을 실행하기 위한 가스 비용을 빼야한다. 이제 가스 비용이 충분하지 않은 경우 opcode가 실행된다. Fig. 4.은 opcode가 실행될 때 가상 머신에서 변경해야하는 부분을 보여준다[15].

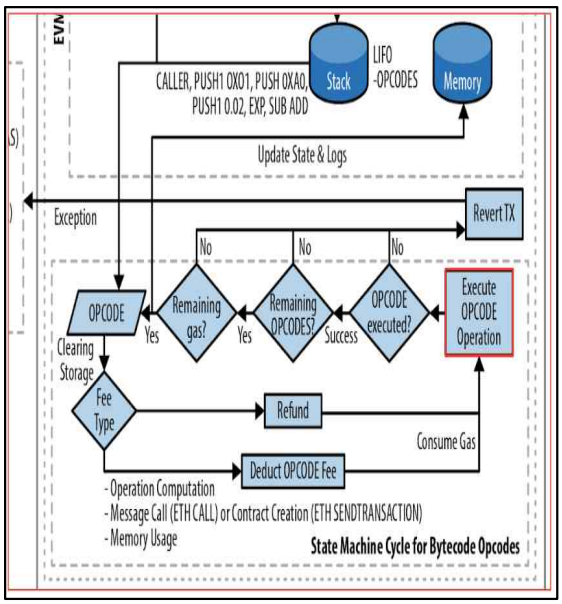

Fig. 4. Change Part in Virtual Machine

위 그림에서 빨간색 상자로 표시된 부분은 영 지식 증명 기술을 적용해야하는 부분이고, opcode를 실행할 수 있는 범용 회로를 만드는 부분이다. Fig. 5.은 영 지식 증명 기술을 적용한 후 저장된 데이터의 변화를 보여준다. opcode를 수행하는 부분에 영 지식 증명 기술을 적용한 후 기존 저장소에 저장된 데이터 중 TX 데이터를 영 지식 증명으로 대체한다. 그리고 지식 증명이 전혀 없는 가상 머신을 만들고 테스트할 것이다[16].

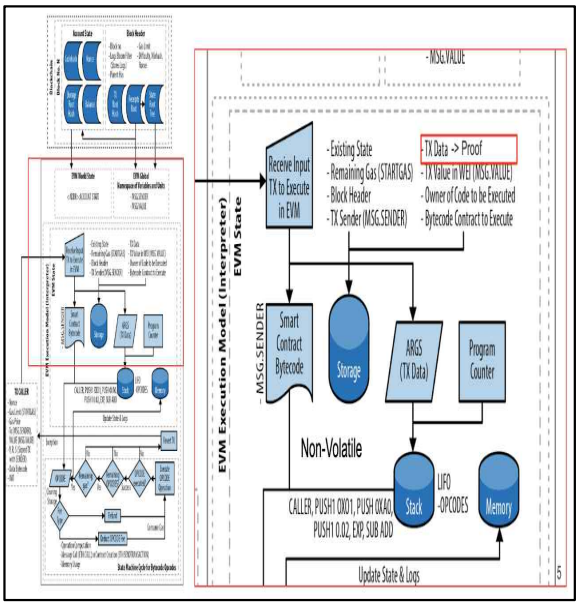

Fig. 5. Data Changes after zero knowledge proof technology

6. 결론 및 향후 과제

본 논문에서는 일반 동작 검증을 위한 영 지식 증명 알고리즘 회로를 설계하였다. 이 백서의 핵심은 기존 시스템에서 체인 데이터 크기 및 블록 검증량 증가 문제를 해결했다. 또한 일반적인 동작 검증을 위해 영 지식 증명 알고리즘이 설계되었다.

마지막으로 검증인과 검증인을 최적화하기 위한 연구를 수행하고 키 생성을 최적화하기 위한 연구를 수행했다. 본 연구는 동작 검증이 가능한 영 지식 증명 알고리즘을 적용한 실제 사례이며, 향후 두 개의 서로 다른 블록체인을 개발할 수 있다. 또한 일반 운영 검증을 위한 영 지식 증명 알고리즘을 이용한 암호화폐 구현을 개발할 수 있다. 향후 과제로는 설계를 바탕으로 일반 동작 검증이 가능한 영 지식 증명 시스템을 개발한다. 그리고 이 연구를 바탕으로 자체 플랫폼을 개발한다.

REFERENCES

[1] K. Park, C. O. Kim, and H. Y. Youm, "Countermeasures against Security Threats to Online Voting Using Distributed Ledger Technology", Journal of the Korea Institute of Information Security & Cryptology, vol. 27,no. 5, pp. 1201-1216, 2017.
DOI: http://doi.org/10.13089/JKIISC.2017.27.5.1201

[2] Lennart Ante. (2020) "Smart contracts on the blockchain - A bibliometric analysis and review", Telematics and Informatics, In press, corrected proof, Avaiable online.
DOI: https://doi.org/10.1016/j.tele.2020.101519

[3] Ahmed S. Almasoud, Farookh Khadeer Hussain, Omar K. Hussain, (2020) "Smart contracts for blockchain-based reputation systems: A systematic literature review", Journal of Network and Computer Applications, Vol. 15.
DOI: https://doi.org/10.1016/j.jnca.2020.102814

[4] Armagan, Ramazan (2019) "Yeni Ekonomi ve Turkiye", Suleyman Demirel Universitesi IIBF Dergisi, 5(2):139-153

[5] Akyazı, Haydar - Adem Kalca (2018) "Yeni Ekonomi ve Iktisat Bilimi", Liberal Dusunce, 29(7):221-242

[6] Barısık, Salih - Oya Yirmibescik (2019) "Turkiye'de Yeni Ekonomi'nin Olusum Surecini Hızlandırmaya Yonelik Uyum Cabaları", ZKU Sosyal Bilimler Dergisi, 2(4): 39-62

[7] Viskari, Sari - Pekka Salmi - Marko Torkkeli (2007) "Implementation of Open Innovation Paradigm, Cases: Cisco Systems, Dupont, IBM, Intel, Lucent, P&G, Philips and Sun Microsystems", Lappeenranta University of Technology Research Report 189, Finland.

[8] Conboy, K., Mikalef, P., Dennehy, D., & Krogstie, J. (2020). Using business analytics to enhance dynamic capabilities in operations research: A case analysis and research agenda. European Journal of Operational Research, 281(3), 656-672.

[9] Mikalef, P., Boura, M., Lekakos, G., & Krogstie, J. (2019). Big data analytics capabilities and innovation: the mediating role of dynamic capabilities and moderating effect of the environment. British Journal of Management, 30(2), 272-298.

[10] Taylor, Timothy (2001) "Thinking About A New Economy", The Public Interest, (Spring):3-19.

[11] Addo-Tenkorang, R., & Helo, P. T. (2016). Big data applications in operations/supplychain management: A literature review. Computers & Industrial Engineering, 101, 528-543.

[12] Bobo Huang,Li Jin,Zhihui Lu,Ming Yan, RDMA-driven MongoDB: An approach of RDMA enhanced NoSQL paradigm for large-Scale data processing, Information Sciences, Volume 502, October 2019, Pages 376-393

[13] Eike Schäffer, Andreas Mayr, Jonathan Fuchs, Martin SjarovMicroservice-based architecture for engineering tools enabling a collaborative multi-user configuration of robot-based automation solutions, Procedia CIRP, Volume 86, 2019, Pages 86-91

[14] Fabian Kaimer, Philipp Brune, "Return of the JS: Towards a Node.js-Based Software Architecture for Combined CMS/CRM Applications", Procedia Computer Science, Volume 141, 2018, Pages 454-459

[15] Boran, F. E., Genç, S., Kurt, M., & Akay, D. (2009). A multi-criteria intuitionistic fuzzy group decision making for supplier selection with TOPSIS method. Expert Systems with Applications, 36(8), 11363-11368.

[16] Meriem Amina Zingla, Latiri Chiraz, "Short Query Expansion for Microblog Retrieval", Procedia Computer Science, Volume 96, 2016, Pages 225-234.

안 병 태(Byeongtae Ahn) [정회원]

· 1999년 2월 : 국민대학교 컴퓨터과학부(이학사)
· 2006년 8월 : 경상대학교 컴퓨터과학부(공학박사)
· 2012년 3월 ~ 현재 : 안양대학교 교양대학 컴퓨터전공 교수
· 관심분야 : 블록체인, 전자상거래, 암호화폐, 스마트 컨트랙트
· E-Mail : ahnbt@anyang.ac.kr