

Demo: Light-Weight Programming Language for Blockchain

Junhui Kim
Chung-Ang University
Seoul, Republic of Korea
jkhkim.cau@gmail.com

Joongheon Kim
Chung-Ang University
Seoul, Republic of Korea
joongheon@gmail.com

ABSTRACT

This demo abstract introduces a new light-weight programming language *koa* which is suitable for blockchain system design and implementation. In this abstract, the basic features of *koa* are introduced including working system (with playground), architecture, and virtual machine operations. Run-time execution of software implemented by *koa* will be presented during the session.

CCS CONCEPTS

• **Software and its engineering** → **Extensible languages**; *Virtual machines*; *Translator writing systems and compiler generators*; *Runtime environments*.

KEYWORDS

Blockchain; Programming Language; Smart Contract

ACM Reference Format:

Junhui Kim and Joongheon Kim. 2019. Demo: Light-Weight Programming Language for Blockchain. In *The 17th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys '19)*, June 17–21, 2019, Seoul, Republic of Korea. ACM, New York, NY, USA, 2 pages. <https://doi.org/10.1145/3307334.3328567>

1 INTRODUCTION

Recently, blockchain technologies are getting a lot of attentions due to its decentralized scalable nature. Among them, Bitcoin and Ethereum are major leading blockchain technologies. The Bitcoin is a blockchain-based cryptocurrency system which was initiated by Nakamoto Satoshi in 2008 [1, 2]. The trading in Bitcoin conducts via peer-to-peer networking under the encryption/description with SHA-256. All transactions are stored as a data structure called Merkle tree by every node participating in blockchain. The Bitcoin solves the double-spending problem using Proof-of-Work (PoW) consensus algorithm for generating blocks. The Ethereum is a distributed computing platform based on blockchain developed by Vitalik Buterin in 2015. Similar to the Bitcoin, All transactions are stored by every node in Ethereum. However, it can execute applications on the blockchain using *Smart Contract* as well as *trading cryptocurrency*. Thus, Ethereum applies the blockchain to various areas such as SNS, e-mail, games, and etc.

In this paper, we propose a new programming language which is easy to understand and write a code that implements the blockchain

system in a scalable way. This language, called *Koa*, solves difficulties of understanding and analyzes the code what the script language of the Bitcoin has with high-level language style. Since the script language is a sequence of instructions, it is difficult to understand the flow of codes at a glance. In addition, it is tricky to implement complicated logics as instructions. For example, when expressing a branch of conditional statement in script language, there is no distinction between the parts to compare a condition, to execute *if-true*, and to execute *if-false*. Besides, it is not easy to figure out what each instruction is used for. The verifying process is performed by sequentially running the unlocking and locking script. It is difficult to understand what kind of actions to perform because this script code is not distinguishable by semantic units. Furthermore, when scripts are implemented, there is a difficulty to program considering the status of stack. If the function is defined in *koa*, it can be distinguishable by semantic units. When verifying a value, it needs to define a new instruction or to assemble many instructions complicatedly. On the other hand, *Koa* can implement this by combining supported operators. Using *Koa*, it has better readability than script languages and is easier to write the code simply.

Meanwhile, *solidity* is used as a smart contract language for Ethereum. If a transaction is executed and the state changes, the Ethereum uses *gas*. Applying *gas* as a kind of transaction fees, Ethereum prevents infinite loop attack. However, the *gas* makes *solidity* code more complicated and hinder usability. Furthermore, the state of Ethereum makes the static analysis of *solidity* code difficult. Since the result of executing function differs according to state, it is difficult to predict *gas* consumption. However, because the *Koa* is a stateless language, it can be statically analyzed. Since there are not any branches of code execution depending on state nor loop, static analysis for the code is easy. In addition, it can prevent the infinite loop attack. This allows the *Koa* to predict the costs associated with running the smart contract. Therefore, the *Koa* which is high-level language helps programmers to implement the blockchain quickly and easily.

2 SYSTEM OVERVIEW

The structure of the *Koa* programming language proposed in as Fig. 1 and it is mainly divided into two parts. First of all, *Koa* that performs *lexing*, *parsing*, *compiling*, and *vm* running steps sequentially, as shown in Fig. 2. In addition, *Koa* playground is a kind of IDE environment software platforms and its corresponding web IDE is as presented in Fig. 3. When users write and compile a source code, it generates a bytecode through *lexing*, *parsing*, and *compiling* steps. If users deploy this bytecode, it would be registered in blockchain and users receive an address where the program is deployed. When users conduct execution call to the address for the desired functions, they can get execution results.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

MobiSys '19, June 17–21, 2019, Seoul, Republic of Korea

© 2019 Copyright held by the owner/author(s).

ACM ISBN 978-1-4503-6661-8/19/06.

<https://doi.org/10.1145/3307334.3328567>

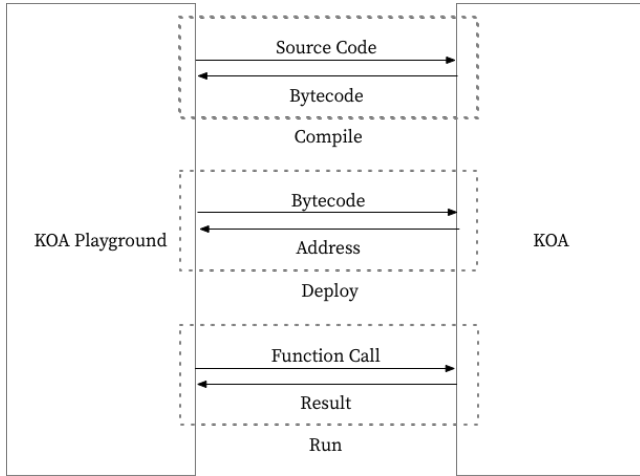


Figure 1: koa system.

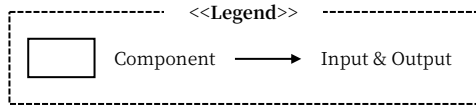
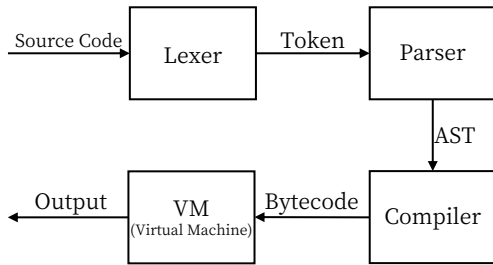


Figure 2: koa architecture.

3 IMPLEMENTATION

The form of abstract syntax tree (AST) can be illustrated as Fig. 4. Koa parser uses *Pratt Parsing* which is recursive parsing which uses the parsing function for each token instead of grammar rules. It makes the parser intuitive and easy to understand. Furthermore, Koa receives tokens from the lexer using *TokenBuffer*. This allows the parser to take responsibility for syntax analysis (parsing) without having tokens directly.

The bytecode generated by koa is passed to Virtual Machine (VM) and then executed. The VM operations include Stack, Memory, and Heap. First of all, the stack is used for storing the data and numerical operators. The, the memory is used to store the data, e.g., variables. Lastly, the heap is used to store the data which have dynamic sizes, e.g., string. When users send a call for requesting a function, VM stores this call data in *callfunc*. Then, it executes the bytecode with stack, memory, and heap. When all functions are called by users, it returns the output and the program exits.

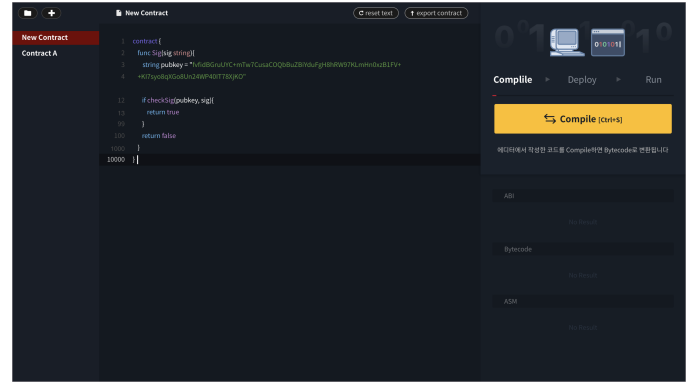


Figure 3: koa playground.

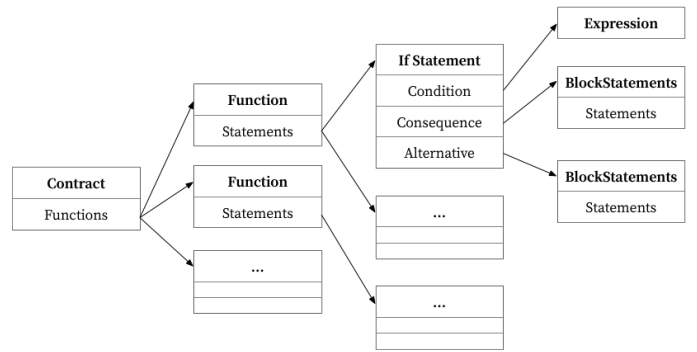


Figure 4: koa AST.

ACKNOWLEDGMENTS

This research was supported by the National Research Foundation of Korea (2016R1C1B1015406, 2017R1A4A1015675); Institute for Information & Communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) (No. 2018-0-00170, Virtual Presence in Moving Objects through 5G); and IITP grant funded by the Korea government (MSIP) (No. 2017-0-00068, A Development of Driving Decision Engine for Autonomous Driving using Driving Experience Information). J. Kim is the corresponding author of this paper.

REFERENCES

- [1] Sungmin Kim and Joongheon Kim. 2018. POSTER: Mining with Proof-of-Probability in Blockchain. In *Proc. of ACM Asia Conference on Computer & Communications Security (AsiaCCS'18)*. 841–843.
- [2] Hyunjae Lee, Myungjae Shin, Kyeong Seon Kim, Yeongeun Kang, and Joongheon Kim. 2018. Recipient-Oriented Transaction for Preventing Double Spending Attacks in Private Blockchain. In *Proc. of IEEE International Conference on Sensing, Communication and Networking (SECON'18)*. 454–455.