

Formal Modeling of Smart Contract-based Trading System

Woong Sub Park*, Hyuk Lee, Jin-Young Choi

School of Cybersecurity, Korea University, Seoul, 02841, Republic of Korea

wsub@korea.ac.kr, fmlab_hlee@korea.ac.kr, narnia@korea.ac.kr

Abstract— With the development of blockchain technology, the fields of use of smart contracts are diversifying. Blockchain-based smart contracts are suitable in areas where integrity and transparency must be guaranteed with distributed ledger technology as the core. However, once the system is deployed, it cannot be modified, so it is important to ensure that the system works with the requirements and principles of the smart contract at the design stage. Therefore, in this paper, we aim to show that the system is accurate without contradictions/errors through formal verification using UPPAAL, a formal verification tool for the public descending auction system (Dutch Auction).

Keyword— Blockchain, Smart Contract, Formal Specification, Formal Verification, Model Checking



Woong Sub Park received B.S. degree from the School of Computer Engineering, Dongguk University, Korea in 2020. He is currently a M.S. candidate in School of Cybersecurity, Korea University. His current research interests are in formal modeling and secure software engineering.



Hyuk Lee received the B.S. degree from the University of Technology Sydney, Sydney, Australia, in 2006, and M.S. degree in 2009 and the Ph.D. degree in 2019 from the Korea University, Seoul, Korea. He is currently a research professor with the Graduate School of Information Security, Korea University, Seoul, Korea. His current research interests are in formal methods, constraint problem solving, and secure software engineering.



Jin-Young Choi received the B.S. degree from Seoul National University, Seoul, Korea, in 1982, received the M.S. degree from Drexel University, Philadelphia, PA, in 1986, and the Ph.D. degree from the University of Pennsylvania, Philadelphia, in 1993. He is currently a Professor with the Graduate School of Information Security, Korea University, Seoul, Korea. His current research interests are in real-time computing, formal methods, programming languages, process algebras, security, and secure software engineering