Fujitsu Develops Technology to Verify Blockchain Risks

Risk detection is automatic and comprehensive to improve safety of smart contracts

Fujitsu Laboratories Ltd.,Fujitsu Research and Development Center Co., Ltd.

Kawasaki, Japan, and Beijing, China, March 07, 2018
Fujitsu Laboratories Ltd. and Fujitsu Research and Development Center Co., Ltd. today announced development of technology that can verify, in advance, risks associated with smart contracts, which are programs that automatically execute transactions on blockchain platforms. The technology also identifies relevant locations in the source code.

Blockchain technology, which was developed as the foundation for Bitcoin, is expected to have applications in a variety of fields beyond finance, including real estate and healthcare. Because smart contract risks are directly linked with business losses, however, there have been issues with improving their reliability as a system. Now, Fujitsu Laboratories and Fujitsu Research and Development Center have developed algorithms to identify risk-affected transaction sequences on Ethereum[1], a platform for executing blockchain applications, using symbolic execution technology[2]. Using these algorithms, they have developed technology that is able to comprehensively detect six types of risks in smart contracts (figure 1), which have the potential to be overlooked in a manual review, and can then identify the relevant locations in the source code. This technology will enable blockchain developers to rapidly develop even safer smart contracts.

Details of this technology were announced at the Blockchains and Smart Contracts Workshop 2018 (BSC 2018), an international conference that was held in Paris, France, February 26-28.

Development Background

Blockchain technology can ensure that, even without a trusted third-party intermediary, data has not been altered, and is expected to have applications not only in the field of finance, but also in securities management, real estate registration, healthcare, and electronic government.

Blockchain offers functionality known as smart contracts, in which a contract can be automatically formed in the system, and by using these, contacts can be checked and executed automatically. Because smart contracts are copied to multiple locations and executed in a distributed manner, once a contract has been executed, it cannot easily be stopped, and it cannot be revised even if risks are found in the smart contract. In fact, there has been an incident in which, because a smart contract to create an automatic investment trust application on a blockchain was flawed, a huge amount of capital was improperly transferred.

Issues

With Ethereum, one execution platform of blockchain application, smart contract risks are grouped into six categories (figure 1), but previous technologies to detect smart contract risks in advance were unable to detect all of the different types. For source call authentication through indirect calls via multiple smart contracts lead to changes in the information in the transaction's source call due to an Ethereum specification, which can be abused to illicitly evade authentication. Previous technologies could not detect the risk as they could not trace transaction internal information.
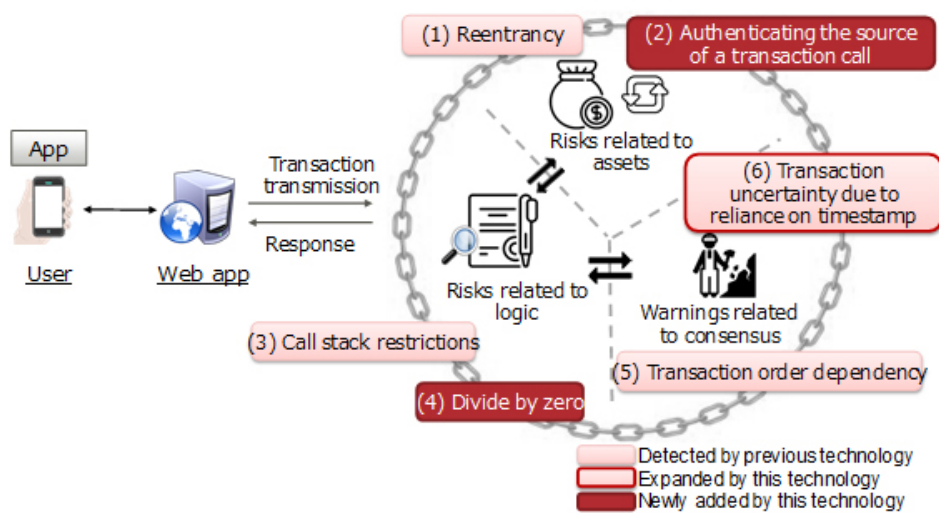
Figure 1: Types of risk that can be detected in smart contracts

About the Newly Developed Technology

Now, Fujitsu Laboratories and Fujitsu Research and Development Center have developed technologies to automatically detect risks in smart contracts for Ethereum that could not previously be detected, and also to identify the relevant locations in the source code (figure 2).
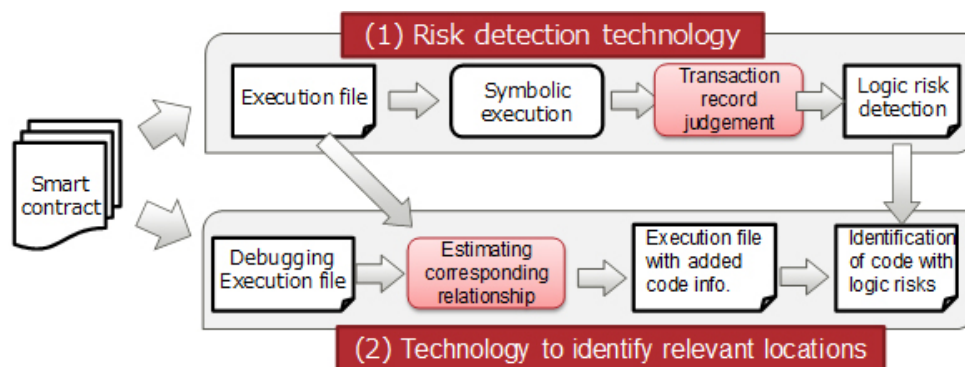

Figure 2: Smart contract risk detection and highly accurate identification of relevant locations

Details of the technology are as follows:

1. Technology to detect smart contract risks using symbolic execution technology

Fujitsu Laboratories and Fujitsu Research and Development Center have now developed an algorithm to comprehensively identify bugs in the source code that might give rise to a risk of someone abusing the language specifications of Ethereum to fake the origin of a transaction call, by using symbolic execution to virtually execute transactions under a variety of circumstances according to the source code based on the sequence of improper processing up to the authentication rules set in advance, the results of a comparison with code patterns unique to Ethereum linked with fraud, and on the presence or absence of access to transaction records unique to blockchain technology. This technology provides comprehensive, highly accurate risk detection.

2. Technology to very accurately identify relevant places in source code for discovered risks

Fujitsu Laboratories and Fujitsu Research and Development Center have developed technology to identify to what part of the source code a newly discovered risk applies with high accuracy. This technology makes symbolic execution possible by deleting unused commands from a debugging execution file, appended with source-code information, that corresponds to Ethereum execution files, which makes it possible to identify source code locations that correspond to risks identified in the execution file by estimating the corresponding relationship between the execution file and the debugging execution file using information such as the types and sequence of virtually executed processing commands.

Results

Using this newly developed technology, the two companies found that where previous verification tools[3] had a detection rate of about 67%, this new technology was capable of 100% detection, excepting a few items, and that in terms of precision it achieved an accuracy rate of up to 88%, enabling both highly accurate risk detection as well as source code risk location identification. Because over-identification of risk is rare, this technology will enable more efficient smart contract development, and combined with the risk location identification technology, it is also expected to reduce the workload involved in tasks such as specification comprehension, code evaluation, and fixing the code. This technology will contribute to the efficient application of blockchain technology to a wide variety of fields.

Future Plans

Going forward, Fujitsu Laboratories will continue to develop verification technologies, not only for Ethereum, but also for Hyperledger Fabric[4], a blockchain framework implementation and one of the Hyperledger projects hosted by The Linux Foundation, with the goal of commercialization of this technology during fiscal 2018. In addition, Fujitsu Laboratories will not only continue to develop verification technology for smart contracts, but also broad technology development relating to building secure systems using blockchain.

---

[1] Ethereum

A primarily public-facing blockchain application execution platform. (https://www.ethereum.org/)

[2] Symbolic execution technology

Technology to thoroughly investigate the operation of a program in response to every possible variable of a value.

[3] Previous verification tools   Verification using Oyente, a smart contract analysis tool for Ethereum.

[4] Hyperledger Fabric

A blockchain framework implementation and one of the Hyperledger projects that is Intended to be a foundation for developing applications or solutions with a modular architecture. Hyperledger Fabric allows components, such as consensus and membership services, to be plug-and-play and leverages container technology to host smart contracts called "chaincode" that comprise the application logic of the system. (https://hyperledger.org/projects/fabric)

About Fujitsu Laboratories

Founded in 1968 as a wholly owned subsidiary of Fujitsu Limited, Fujitsu Laboratories Ltd. is one of the premier research centers in the world. With a global network of laboratories in Japan, China, the United States and Europe, the organization conducts a wide range of basic and applied research in the areas of Next-generation Services, Computer Servers, Networks, Electronic Devices and Advanced Materials. For more information, please see: http://www.fujitsu.com/jp/group/labs/en/.

About Fujitsu

Fujitsu is the leading Japanese information and communication technology (ICT) company offering a full range of technology products, solutions and services. Approximately 155,000 Fujitsu people support customers in more than 100 countries. We use our experience and the power of ICT to shape the future of society with our customers. Fujitsu Limited (TSE: 6702) reported consolidated revenues of 4.5 trillion yen (US$40 billion) for the fiscal year ended March 31, 2017. For more information, please see http://www.fujitsu.com.

Technical Contacts

Information Systems Technologies Laboratory
✉ E-mail: labs-bcdev-inquiry@dl.jp.fujitsu.com
Company:Fujitsu Laboratories Ltd.

Press Contacts

Public and Investor Relations Division
Inquiries
Company:Fujitsu Limited

Date: 07 March, 2018
City: Kawasaki, Japan, and Beijing, China
Company: Fujitsu Laboratories Ltd. ,Fujitsu Research and Development Center Co., Ltd.

Share this page

Top of Page

Services & Products

Business Services
Business and Application Services
Managed Infrastructure Services
Product Support Services
IT Products and Systems
Software
Network
Electronic Devices
Other Products

Solutions

Infrastructure Solutions
Industry Solutions
Business and Technology Solutions
Fujitsu Cloud

Support

IT Products and Systems
Software
Network
Electronic Devices
Other Products

Corporate Information

Corporate Profile
Brand and Values
Investor Relations
Activities
News and Resources
Events
Employment

Country Selector

Global | Change

Terms of Use   Privacy   Contact   Site Map

Copyright 1995 - 2018 FUJITSU