Design and Practice of Automatic Test Framework for Blockchain

Yi Wang[1]

[1] Department of Control Science and Engineering, Tongji University, Shanghai 201804, China
1631665@tongji.edu.cn

Abstract. With the rapid development and popularization of Bitcoin in recent years, the research and application of blockchain technology has shown explosive growth. There is no fast and effective test method for various blockchain projects in the market. In this paper, the following work is done: firstly, the existing blockchain technology types and characteristics are analyzed, and the transaction, block and smart contracts are selected from the aspects of function, performance and reliability to design relevant test indicators; then based on the test indicators construct a loosely coupled test framework; last, use this method to actually test the three blockchain projects and analyze the results.

Keywords: Blockchain, Test Indicators, Test Framework.

1 INTRODUCTION

Since Satoshi Nakamoto [1] first proposed the concept of blockchain in 2008, blockchain technology has been receiving much attention. Blockchain has the characteristics of decentralization, collective maintenance, hyper-transparency, trustfree, anonymity and so on. It has not only been applied in the Bitcoin system, but also become a hot topic in the governments and enterprises around the world. The blockchain is considered to be the fifth disruptive innovation of the computer paradigm following the mainframe, computer, Internet, and mobile social networks [2, 3]. The blockchain is the fourth milestone after the blood credits, precious metal credits, and central banknote credits in the history of human credit evolution. According to the level of openness of the blockchain, the blockchain can be divided into public blockchain, consortium blockchain and private blockchain [4]. Various blockchain projects are booming, and more than 86,000 blockchain projects are stored on the GitHub platform [5]. Various blockchain projects are mixed, among which the more notable ones are Bitcoin, Ethereum [6] and Hyperledger [7].

From the history of blockchain technology, it is not difficult to see that: First, the research of blockchain technology will continue to develop. Distributed systems, encryption technologies, consensus and smart contracts will be further research in terms of resource consumption, system scalability, performance and so on; second, based on the decentralization, transparency, openness, autonomy, tamper proof, anonymity and other characteristics of the blockchain, more and more applications will be researched and even entered our daily life. Therefore, whether it is for the development of the blockchain itself or the implementation of various blockchain-based applications, it is very necessary to design an efficient blockchain automated test framework.

1.1 Blockchain Introduction

Narrowly speaking, blockchain is a chained data structure that combines data blocks in a sequential manner in a chronological order, and cryptographically guaranteed tamper proof and unforgeable distributed ledgers [8]. Broadly speaking, blockchain technology is a completely new distributed infrastructure and computational paradigm by using blockchain data structures to validate and store data, using distributed node consensus algorithms to generate and update data, and using cryptography to ensure data transmission and access security, using automated scripts code consists of smart contract to program and manipulate data [9]. From the data structure, the ledger of the blockchain is a linear linked list. As shown in Fig 1, the linked list is formed by "blocks", and each block has version number, previous hash, transaction hash and other information, the previous hash is used to form a chain relationship between the blocks [10]. According to its different physical functions, the basic hierarchical structure of the blockchain can be divided into data layer, network layer, consensus layer, incentive layer, contract layer and application layer. Each layer involves related technologies.

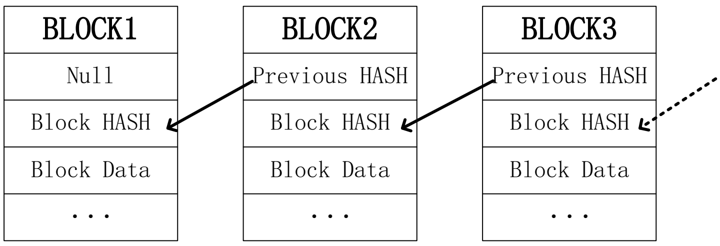

Fig. 1. Chain Structure of Blockchain

1.2 Types of Blockchains

According to the openness of the blockchain, the blockchain can be divided into public blockchain, consortium blockchain and private blockchain [4]. However, with the rapid development of blockchain technology, the boundaries between various types of chains will gradually become blurred, especially as the business logic of the smart contracts running on the nodes becomes more and more complex, some nodes on the private chain must be open to the outside nodes in order to execute the complete business logic, while some consensus and commit nodes will restrict the openness of the licensed nodes, to guarantee efficiency and controllability. And the business boundaries between the various chains will gradually become blurred. The comparison between the three blockchain is shown in Table 1.

Table 1. Three Blockchain Comparisons

	Public Blockchain	Consortium Blockchain	Private Blockchain
Participants	All	Authorized Organization	Single Organization
Committing Peers	All	Participants Coordination Authorization Control	Customization
Trust Mechanism	PoW etc.	Collective Endorsement	Self-endorsement
Level of Centralization	Decentralization	Multi-centralization	Centralization
Outstanding Advantages	Credit Self-establishment	Efficiency, cost optimization	Transparent and traceable
Typical Scenarios	Bitcoin	Clearing	Auditing

1.3 Introduction to Mainstream Blockchains

The development of blockchain technology is changing with each passing day. The key technologies around the application of blockchains are innovating and iterating. A lot of blockchain platforms are emerged such as BitCoin, Ethereum, Hyperledger, DFINITY, BCOS, AnnChain, DNA and so on. The mainstream blockchain frameworks are BitCoin, Ethereum, and Hyperledger [11]. Bitcoin is the origin of the blockchain, and it is the most stable and important application scenario of the blockchain technology. It has not been a serious security incident for more than eight years. Its security and stability are the solid foundation of the blockchain. Subsequently, developers began to pay attention to the blockchain technology itself, intending to expand the possibility of more application scenarios. In 2013, the Ethereum white paper was released, and the first time the smart contract was introduced into the blockchain, making the blockchain become a Turing Complete platform that can run any form of application. In 2015, the Hyperledger project was established, access control and security assurance were introduced into the blockchain.

Table 2. Mainstream Blockchain Platform

Blockchain Platform	Key Technology	Feature
Bitcoin	PoW, Merkle tree	anonymity, stability
Ethereum	PoW, smart contract, Merkle tree, Casper	Support the self-design of complex smart contract logic
Hyperledger	PBFT, authority management, multichannel	complete access control, pluggable, scalable framework

2 Test Indicators

Combined with the technical characteristics of the blockchain, the quality model in the *GB/T 25000.10-2016 System and Software Engineering System and Software Quality Requirements and Evaluation (SQuaRE) Part 10: System and Software Quality Models* is also considered. The requirements of automated test, this section is designed from the aspects of function, performance and reliability. Other aspects of test can be carried out through document review, code review, etc. This article does not do research. Function refers to a combination of input, operations and output. Here, when used under specified conditions, the blockchain information system has the ability to complete the corresponding processing or process capability; performance refers to when used under specified conditions. The results of the blockchain information system for various performances can be considered in terms of resource utilization, time characteristics and capacity; reliability refers to the level of reliability requirements that the blockchain information system satisfies when used under specified conditions. It can be considered in terms of maturity and availability, fault tolerance and recoverability.

Transaction is the most common and widely used transaction logic unit in the blockchain. The initiation and query of transactions are the most basic use scenarios in blockchain applications. The level of support and ease of use of transactions is the basic indicators of whether blockchain technology is mature. Block is one of the foundations of blockchain technology. The size and the organizational structure of the block, and the average time of block generation are important indicators of reflecting the technical characteristics of the blockchain. Smart contracts are one of the cores of blockchain technology. The level of support and ease of use of smart contracts is an important indicator of whether a blockchain technology is mature. In this paper, we will select transaction, block and smart contracts as test indicators to design in terms of function, performance and reliability. The details are shown in Table 3, Table 4, and Table 5.

Table 3. Functional Evaluation Indicators

Evaluation Indicators	Evaluation Contents
Transaction	The transaction query is idempotent, that is, the query result is consistent in any case for the same transaction; the transaction is persistent after the transaction is successfully initiated, that is, the transaction needs to be persisted into the blockchain system.
Block	Query the average generation time of the block; query the specified block information
Smart Contract	Lifecycle management of smart contracts, including registration, invocation, query, update, etc.; whether to support calls between smart contracts

Table 4. Performance Evaluation Indicators

Evaluation Indicators	Evaluation Contents
Transaction	Transaction throughput; transaction broadcast speed; transaction query speed.
Block	Transaction packing block speed; block capacity; block synchronization speed
Smart Contract	Smart contract registration, call speed

Table 5. Reliability Evaluation Indicators

Evaluation Indicators	Evaluation Contents
Transaction	Whether the transaction can be carried out in the case of single or multiple nodes failure; whether the transaction can be performed in the case of a single or multiple nodes damaged; whether the transaction can be performed in the case of network jitter
Block	Whether the node block information can support failover synchronization; whether single or multiple node block information damage affects the entire network
Smart Contract	Whether there are vulnerabilities in smart contracts, etc.

3 Test Framework

Compared with traditional software, blockchain applications have the characteristics of decentralization, transparency, openness, autonomy, tamper proof, anonymity and so on. These characteristics put forward new requirements for test. We need to design a loosely coupled test framework. The design of the platform is based on cloud computing, and building virtual nodes on the cloud platform. They can greatly improve the reliability of testing, save test time and achieve automated test.

The framework is divided into three parts, the test center, the blockchain center and the data center, as shown in Fig 2. The test center is the central brain of the entire test framework, and is responsible for initiating script commands to the blockchain center of the cloud platform to unified manage the corresponding node information. At the same time, the test center also needs to be responsible for obtaining the corresponding data from the data center, analyzing, processing and obtaining the corresponding test report; the blockchain center is designed on the cloud platform, accepts commands from the test center, allocates resources, and is responsible for the operation of the virtual node; The data center can use cloud storage to collect data from the blockchain center and provide it to the test center, which can also provide services to other applications.

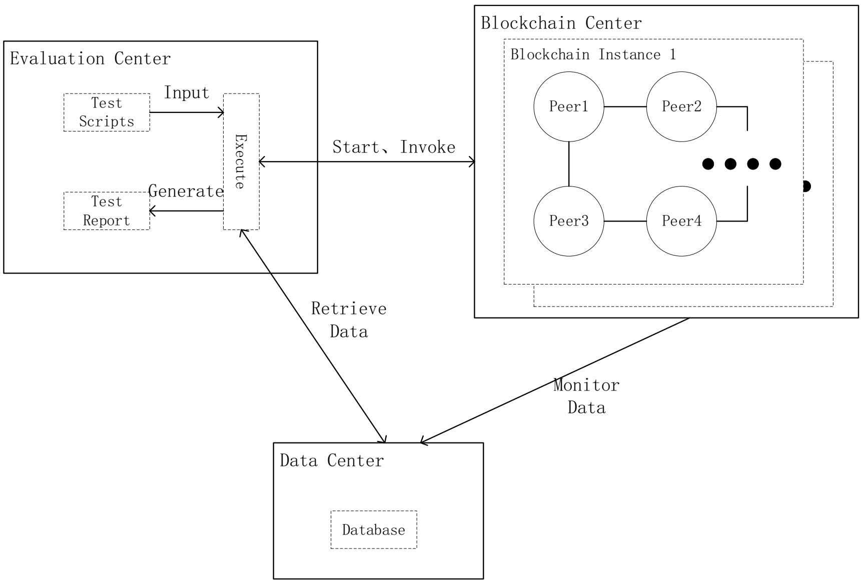

Fig. 2. Test Framework

4 Practice

The test framework is deployed on a cloud platform, which has Intel Xeon Skylake 6133 (2.5 GHz), 1.5 Gbps bandwidth, and running Ubuntu 16.04. The test center node has 4 core, 8G RAM and 100G hard drive. The data center has 2 core, 4G RAM and 100G hard drive, and using MongoDB database. Each blockchain center node has 4 core, 8G RAM and 100G hard drive.

This practice tests blockchain products A, B, and C in terms of function, performance, and reliability. The results of the test indicate that blockchain products have the following basic characteristics:

1. The transaction is idempotent and persistent;

2. Under the number of nodes meeting the consensus requirement, the transaction can be performed in the case of single or multiple node failures and network jitter. The block information of the node can support failover synchronization, and the damage of single or multiple node block information will not affect the entire network.

There are still large gaps in performance between the three blockchain products(conditions: 4 nodes; mean of an hour data):

1. In terms of block generation rate, the product A generates a block of about 15 seconds. The product B and the product C are related to the capacity of the block in the configuration and the block generation time;

2. In terms of transaction rate, the product A has a transaction volume of 20 per second, the product B has a transaction volume of 350 per second, and the product C has a transaction volume of more than 500 per second.

In terms of smart contract detection, all three products meet the specifications of smart contracts.

5 Conclusion

With the development of blockchain technology, various blockchain projects have emerged one after another. The blockchain automated test framework constructed in this paper is an attempt to quickly evaluate the relevant indicators of the blockchain. The test framework proposes three aspects of test based on the typical blockchain technology architecture, which helps users to quickly understand product performance and guarantee blockchain product quality. However, the current test framework still has shortcomings. For example, the selection of test indicators is limited, and some test contents such as smart contract vulnerability assessment cannot achieve automatic test. In the following, the author will continuously improve the relevant test indicators and test methods according to the actual operating conditions; try to customize the test content to meet the commercialization needs; and automate the smart contract vulnerability test.

References

1. Nakamoto, S.: Bitcoin: A Peer-to-peer Electronic Cash System. Consulted (2008).
2. Yuan Y., Wang F.: Blockchain: The State of the Art and Future Trends. Zidonghua Xuebao/Acta Automatica Sinica 42(4), 481-494 (2016).
3. Swan M.: Blockchain: Blueprint for a New Economy. O'Reilly (2015).
4. Wu G., Zeng B., Li R.: Research on the Application of Blockchain in the Integrated Demand Response Resource Transaction. Proceedings of the Csee 37(13), 3717-3728 (2017).
5. Jesus LT., Stephen F., Val S.: Evolution of Blockchain Technology Insights from the GitHub Platform. Deloitte Center for Financial Services (2017).
6. Buterin V.: Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform. Nick Szabo, Formalizing and Securing Relationships on Public Networks (2013).
7. Androulaki E., Barger A., Bortnikov V.: Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. Consulted (2018).
8. Milutinovic M., He W., Wu H.: Proof of Luck: An Efficient Blockchain Consensus Protocol. Consulted (2017).
9. Technical report by the UK government chief scientiflc adviser Homepage: https://www.gov.uk/government/uploads/system/uploads/attachmentdata/flle/492972/gs-16-1-distributed-ledger-technology.pdf, last accessed 2016/02/21.
10. Ametrano F. M.: Bitcoin, Blockchain, and Distributed Ledger Technology. Social Science Electronic Publishing (2016).
11. Dinh T. T. A., Wang J., Chen G.: BLOCKBENCH: A Framework for Analyzing Private Blockchains. Association for Computing Machinery, Part F127746, 1085-1100 (2017).