Analysis for Blockchain Application Quality

Jiajin Xu
Shanghai Key Laboratory of Computer Software Evaluation. Shanghai Computer Software Technology Development Center
Shanghai, China
xujj@sscenter.sh.cn

Huan Zhang
Shanghai Key Laboratory of Computer Software Evaluation. Shanghai Computer Software Technology Development Center
Shanghai, China
zhangh@sscenter.sh.cn

Jiayu Gong
Shanghai Key Laboratory of Computer Software Evaluation. Shanghai Computer Software Technology Development Center
Shanghai, China
gjy@sscenter.sh.cn

***Abstract*—With the maturity and popularity of blockchain technology, it has applied to many industries, such as financial sector, logistics, notarization and so on, but there is no correct quality model to describe the brockchain software. This paper we combined with the general software quality model(SQuaRE), formed a suitable quality model of the blockchain platform (Hyperledger Fabric) and expound its special quality measure. The research result of this paper can be applied to test or evaluate of blockchain application.**

Keywords—Hyperledger Fabric, blockchain, software quality, software quality model

I. INTRODUCTION

Recently blockchains attract the interests of stakeholders across a wide span of industries: finance， healthcare， real estate, and government, because of its decentralization, non-tampering, traceability, collective maintenance, openness and transparency. As a new infrastructure, blockchains application testing is quite different from the traditional ways. General software quality models may not quite compatible with the blockchain applications since their different features from other software. This paper introduces general software model ISO/IEC 25010[2] and describes blockchain application's features and its special quality measures. They can be used as a supplement to ISO/IEC 25023:2016[1].

II. GENERAL SOFTWARE QUALITY MODEL

Due to the different requirements, the stakeholders may have different quality perspectives. For users, software quality is to meet the needs of users. For developers, software quality is consistent with requirements. In order to give a reasonable evaluation of the quality of software products, a software quality model is necessary

Last decade, ISO/IEC JTC1 SC7 has designed a new generation of software quality standards, namely ISO/IEC 25000 SQuaRE or Software Product Quality Requirements and Evaluation. ISO/IEC 25010 software product quality model is a general model for judging software's quality, which includes eight quality characteristics, functional suitability, performance efficiency, compatibility, usability, reliability, security, maintainability and portability[2]. For each characteristic, it contains several sub characteristics. Fig.1 shows the details of System and software product quality model.

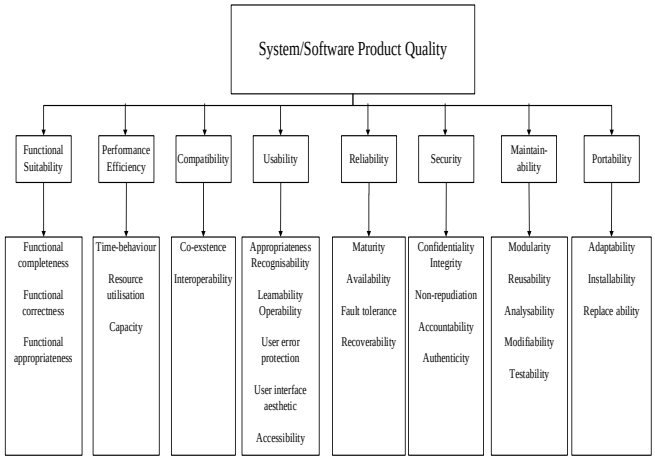

Fig. 1. System/Software Product Quality Model—ISO/IEC 25010:2011

Based on the software product quality model, ISO/IEC 25023:2016 "Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - Measurement of system and software product quality" provides measures for quality characteristics. But ISO/IEC 25023:2016 cannot cover the quality measurement for blockchain application, so more quality testing measures should be added.

III. HYPERLEDGER FABRIC BLOCKCHAIN SOFTWARE FEATURES

In the blockchain application, Hyperledger is an excellent implementation of the union chain, and Hyperledger Fabric is the kernel of Hyperledger project.

Hyperledger Fabric is essentially a distributed ledger, using a high availability modularization as its design concept. The modules, such as MSP, Ordering Service, Ordering Service, Ordering Service are deployed separately. This way can configure the requirement flexibly. The key technologies of Hyperledger Fabric as follow.

This work was supported by National Key R&D Program of China (No.2018YFB1403404).

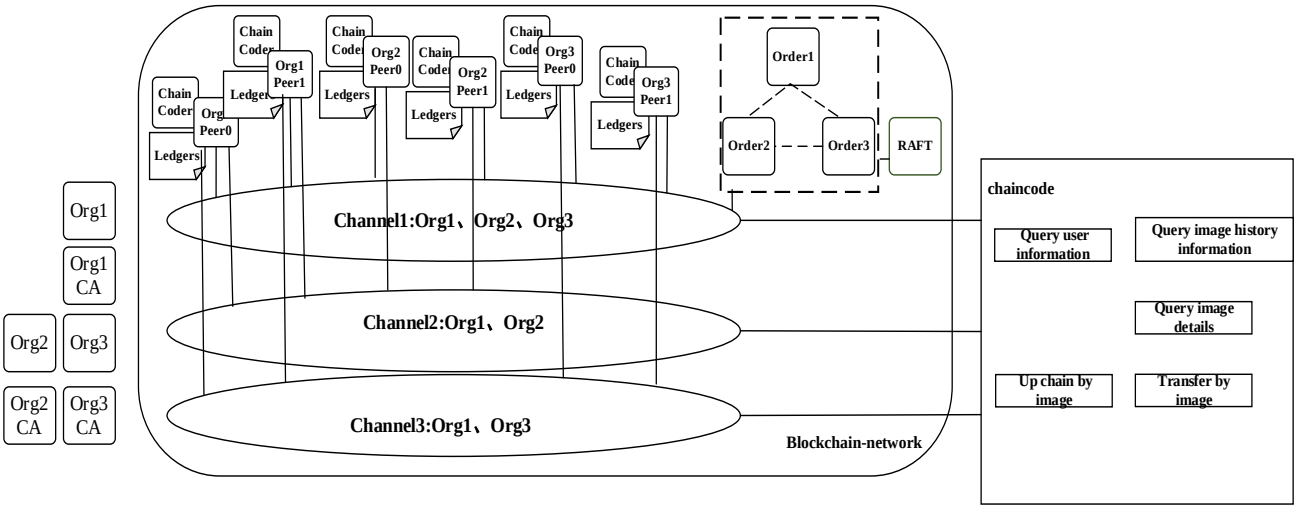

Fig. 2. Structure Chart

A、*Ledger[3]*

A Fabric Ledger is a series of orderly and immutable records which states has been transformed. Its inside structure is been comprised of a block which stores the immutable, ordered records, and simultaneously contains a state database to record the current state.

B、*Blockchain[3]*

The Block chain is based on the local file system, and its blocks are put in local hard disk which store the file system. The previous block hash is pointed to the current block hash, so they can connect with a block chain.

C、*Peer[3]*

Peer is the main body to do the operation of trade processing and maintain ledger, which is mainly responsible for the consensus process, and does ledger's reading and writing operation through chaincode. Peers can be divided into Endorser Peer and Committer Peer, according to different functions.

D、*Channel[3]*

A channel is a private space which is used to communicate information between two or multiple peers. The transaction data in the channel is separated from the data outside the channel, so we can ensure that the data in the channel is safe enough. Transactions on the network must be executed on the Channel. Each member of the transaction needs authorization and certification, otherwise they cannot be allowed to trade on the Channel.

E、*Orderer[3]*

Orderer is sorting the transactions which is generated by different channels in the blockchain network, and at the same time broadcasting to the peer. Orderer is implemented as a pluggable component and has two kinds of algorithms (SOLO and Kafka).

The fig2 is the structure chart of software which use the technology of Hyperledger Fabric, we can know the composition of this blockchain network clearly. In this blockchain network, there are three organizations(Org1, Org2, Org3), and each organization maintains 2 peers(peer0, peer1) at the same time. The consensus algorithm is Raft, it consists of three orders (Order1、Order2、Order3). And then there are three channels (Channel1, Channel2 and Channel3) in the network, each channel contains different organization, the organizations(Org1, Org2, Org3) have joined Chanel1, the organizations(Org1, Org2) have joined Chanel, the organizations(Org1, Org3) have joined Chanel3. The functions of chaincode are up chain by image, transfer by image, query user information, query history of image and query detail of image.

IV. HYPERLEDGER FABRIC SOFTWARE QUALITY MODEL

Based on the above characteristics of Hyperledger Fabric, we tested with the application scenario of Hyperledger Fabric, and established a software quality requirement system which is suitable for HyperLedger Fabric as the fig3. It also contains eight quality characteristics which is the same as ISO/IEC 25010-2011. But many quality characteristics have different sub characteristics, such as functional suitability, performance efficiency; and many sub characteristics have different test measures, such as compatibility , reliability and security, the details as fig3.

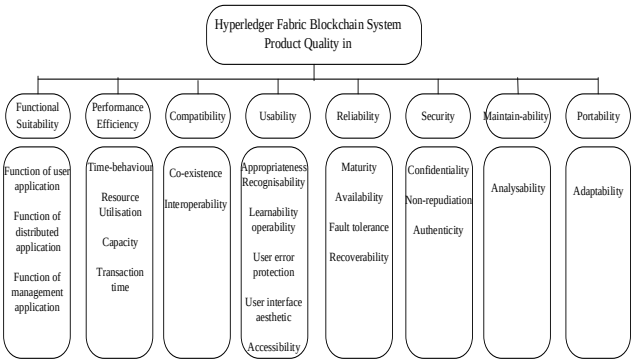

Fig. 3. Hyperledger Fabric Blockchain System Product Quality

A. *Functional suitability*

In ISO/IEC 25023-2016[1], there are two sub characteristics, functional completeness, functional correctness. But for Hyperledger Fabric, we add some new sub characteristics to replace the normals'. The new sub characteristics can be defined as function of user application function, distributed application function and function of management application [5], the detail definition as follow;

1) *Functiong of user application:* It is the interaction between the blockchain customer and the blockchain service, including two user operation mode, the command line interface and image interface.
2) *Function of distributed application:* It is the distributed apply function of blockchain, including selection or cancellation of blockchain service, ordering and unordering of blockchain services and the business operation of ledger.
3) *Function of management application:* It is the management application function of blockchain, including manage by member and manage by monitor.

B. Performance efficiency

In ISO/IEC 25023-2016, there are three sub characteristics, time-behaviour, resource utilisation and capacity. But for Hyperledger Fabric, except these normal sub characteristics, we add a additional indicator which called transaction time. It can be defined as time of sorting the consensus algorithm, time of completing the block broadcast for transaction, time of completing verification and submission for transaction, and time of completing submission for transaction, the detail definition as follow;

1) *Time of sorting the consensus algorithm:* The average time difference between WriteBlock and Propose in order's log file;
2) *Time of completing the block broadcast for transaction:* The average time difference between StoreBlock in peer's log file and WriteBlock in order's log file;
3) *Time of completing verification and submission for transaction:* The average time difference between Validate and StoreBlock in peer's log file;
4) *Time of completing submission for transaction:* The average time difference between CommitWithPvtData and Validate in peer's log file.

C. Compatibility

In ISO/IEC 25023-2016, there are two sub-characteristics, co-existence and interoperability, interoperability is defined as data formats exchangeability, data exchange protocol sufficiency and external interface adequacy. But for Hyperledger Fabric, interoperability has different test measures, it can be defined as the description of system interaction interface[4]. The detail definition as follow;

1) *Description of system interaction interface:* It needs to give a detailed description with the interface name, request system, response system, method of the interface be used , parameters of the interface and return results of the interface.

The example as follow:

The image resource is stored in the file system while the image encryption is stored in the application system. When the user wants to put image on chain, they must interact with file system, application system and block chain system. Firstly, the user fills in the basic information, chooses the image which would be uploaded, and finally presses the upload button, enabling the file system to send the image information to application system that will automatically fill the encrypt attribute to the image. Then, the application will send the basic information on image and encrypted information to block chain system after the user presses the on chain button. The detailed interactions of this blockchain system as the fig4, and the interface specification of this blockchain as the table1.

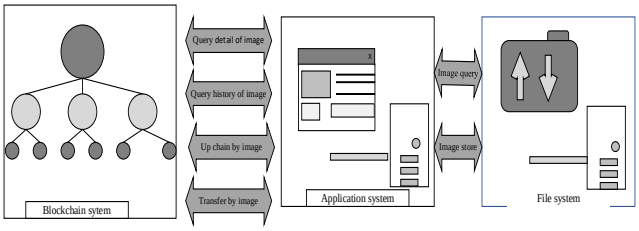

Fig. 4. Interaction of System

TABLE I. INTERFACE SPECIFICATION

Interface Name	Request System	Response System	Interface Specification	Returned Result
Up chain by image	File System	Application System, Blockchain system	Method: EnrollAsset(ctx，assetID，assetName，assetUrlHash，ownerID，metadata) Parameter: assetName, assetID, assetUrlHash, ownerID, Metadata	transaction result
Query detail of image	Application System	Blockchain system	Method: QueryAssetsByUserID(ctx，userID) Parameter: userID	Image detail
Query history of image	Application System	Blockchain system	Method: QueryAssetsHistoryByAssetID(ctx，assetID) Parameter: assetID	Image history
Transfer by image	Application System	Blockchain system	Method: ExchangeAsset(ctx，assetHistoryID，assetID，origenUserID，currentUserID) Parameter: assetHistoryID, assetID, origenUserID, currentUserID	Result of transfer

D. Reliability

In ISO/IEC 25023-2016, there are four sub-characteristics, maturity, availability, fault tolerance and recoverability. For Hyperledger Fabric, it is a peer-to-peer network, with equivalent nodes, each node of the block should reach a consensus and then to go to the next operation, in the end all nodes make up a distributed ledger, complete a command or result which cannot be changed. Because of this consensus mechanism, the blockchain system allows partial node or ledger to be incorrect. As long as most of them are correct, the system also can works normally. So the fault tolerance in Hyperledger Fabric can be defined as node abnormal tolerance and ledger abnormal tolerance, the detail definition as follow;

1） *Node abnormal tolerance:* Node tolerance rate of the block chain system, the purpose is to find out the maximum error number of endorsement nodes and verification nodes, while not affecting the normal use of the application;

2） *Ledger abnormal tolerance:* Ledger tolerance rate of the block chain system, the purpose is to find out the maximum number of the ledger file which is been deleted or tampered, while not affecting the normal use of the application;

E. Security

In ISO/IEC 25023-2016, confidentiality, non-repudiation and authenticity are all the security's sub-characteristic. Confidentiality is defined as the correctness of data, access control; Non-repudiation is defined as data signature utilization quality metrics; Authenticity is defined as the adequacy of the identification mechanism and the conformity of the identification rules. But for Hyperledger Fabric, there are different test measures, confidentiality can be defined as unauthorized access restrictions, channel isolation, and node confidentiality; Non-repudiation can be defined as non-repudiation of operations on the chain and non-repudiation of log data; Authenticity can be defined as the identification mechanism, the detail definition as follow;

1） *Unauthorized access restrictions:* When there is unauthorized data access, the data privacy processing of the block chain;

2） *Channel isolation:* Isolation measures in block chain channels;

3） *Node confidentiality:* Confidentiality measures for block chain ledger data and node data;

4） *Non-repudiation of operations on the chain:* All chain operations can be logged and traced;

5） *Non-repudiation of log data:* All log data only can be viewed but cannot be tampered;

6） *Identification mechanism:* The identification mechanism adopted by block chain;

V. CONCLUSION

This paper analyzed the characteristics of Hyperledger Fabric, formed a software quality management system which is suitable for Hyperledger Fabric, and then explained its special quality measure. We hope that can provide a reference when testing with the blockchain software, and improve the blockchain's software quality.

REFERENCES

[1] ISO/IEC 25023: Systems and software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE) -- Measurement of system and software product quality, Geneva, Switzerland: International Organization for Standardization, 2016.

[2] ISO/IEC 25010: Systems and software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE) -- System and software quality models, Geneva, Switzerland: International Organization for Standardization, 2011.

[3] Bellaj Badr, Richard Horrocks, Xun (Brian) Wu, "Blockchain By Example" England, Birmingham:Packt Publish, 2018.

[4] CBTCA-001: Grading Evaluation Specification for Blockchain Distributed Ledger Information System (Chinese), Chaoyang District, Beijing: China Blockchain Evaluation Alliance, 2019.

[5] CBD-Forum-001: Blockchain-Reference Architecture (Chinese), Dongcheng District, Beijing: China Academy of Electronic Technology Standardization, 2017.