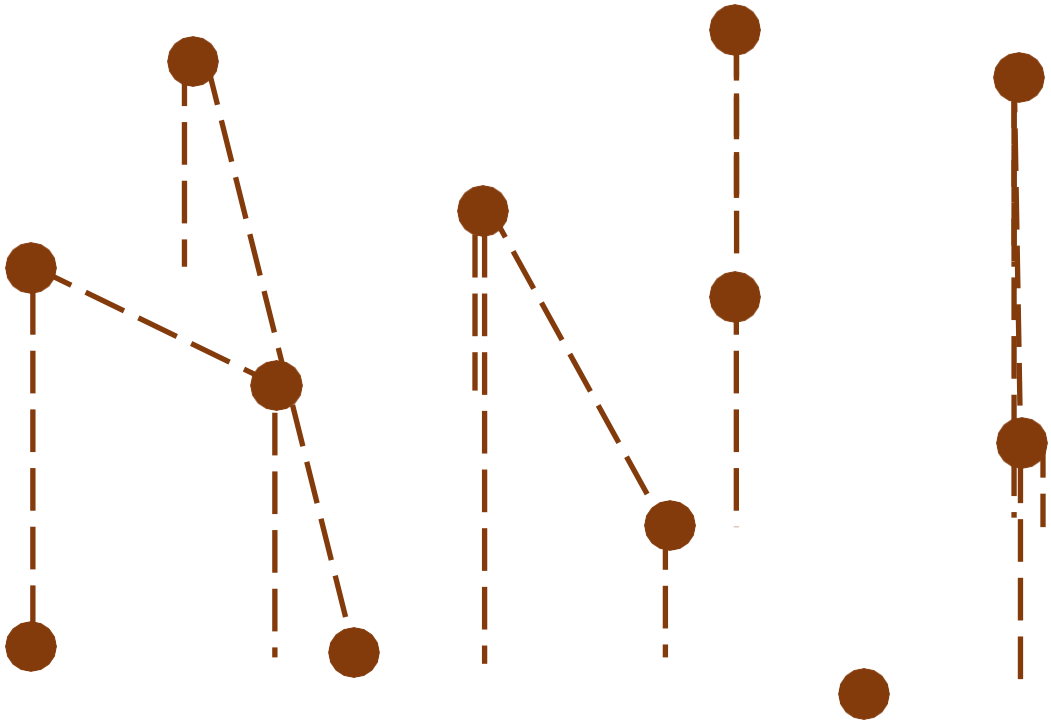
Blockchain Testing

Testing Practice @ Qtek Systems



Authored by: Jayachandra Parasu

Vishwanatha Reddy

1. Overview - Blockchain Technology

This white paper talks about Blockchain technology and test approach with effective methods and tools available for testing the Blockchain applications.

1.1. What is Blockchain?

Blockchain is the technology or platform which can be used to secure, store, and manage data in a decentralized and cryptic format which addresses the current concerns or challenges of trust or data breach between B2B, B2C, and C2B entities.

1.2. Why Blockchain?

Imagine someone is checking into a hotel and if the hotel blocks their credit card for the amount of total stay and the current block on credit card can be removed only after check-out. Is it required? Yes, as there is a lack of trust between the customer and business. This can be addressed through Blockchain and there is no need for blocking the amount unnecessarily or reaching out to the central bank to check the card. Similarly, an Import & Export company needn't perform SWIFT transfers as the bank provides a guarantee until the goods reach the importer. This can be addressed through Blockchain's decentralized ledgers and transactions can be stored using cryptography and by making payments in real-time.

A recent study by the World Economic Forum estimates that 10% of the GDP will be in Blockchains or Blockchain-based technologies by 2025. With this data, Blockchain technology can be perceived as the future, and every business should assess if it can be leveraged for their business growth. Blockchain is a highly secure and encrypted digital ledger, which is in the form of a chain of blocks, and these blocks are linked to each other through cryptography.

This cryptography involves a hashing function, which is the process of producing a unique key value on inputting a value into the hash function. Each block in the blockchain will have a unique hash value and every block will have the hash value of the previous block to stay connected. Blockchain was designed originally for digital currencies such as Bitcoin, but later its benefits led to its usage in recording not only financial transactions but, virtually everything of significant value.

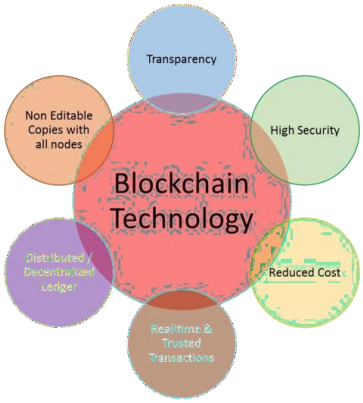


Fig 1.2 – Why Blockchain Technology – in a Nutshell

1.3. What is it used for and how?

Blockchain is used mainly by financial and automotive industries because of its secure nature of business. This technology supports cryptocurrencies like Bitcoin and Ethereum. The following diagram will help illustrate how the transaction works in blockchain technology.

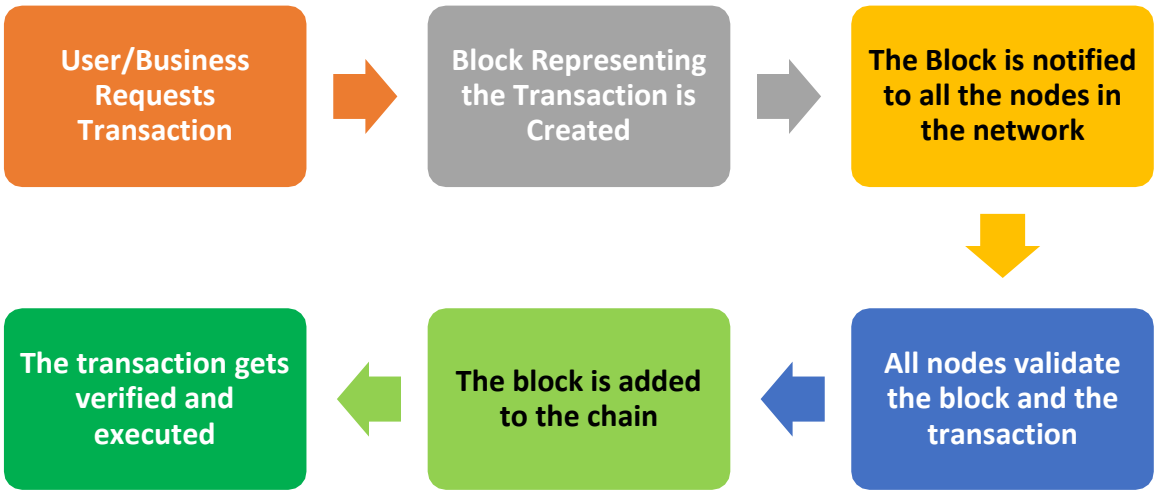


Fig 1.3 – How Blockchain Works

2. Current QA Approach - Blockchain Technology

Due to the change in technology, testing the applications developed based on Blockchain technology comes with numerous challenges. In addition to traditional testing and validation like Functional Testing, Non-Functional Testing, Performance Testing, Security Testing, and Integration Testing, we need to have specialized capabilities like Smart Contract Testing, Peer/Node Testing, own Mathematical & Cryptographic skills, and industry-leading tools.

2.1. Verification & Validation

A blockchain is usually present in a decentralized network of nodes, where the nodes are high configuration computer systems. Every node present in the decentralized network has a copy of the blockchain transaction history, and the verification process in the blockchain is a consensus mechanism based process. For verifying a new transaction and creating a new block for it, all the nodes must receive input values that they cross-verify against specific available data.

Due to its nature, and all the different entities that the blockchain system involves for its operation like a large number of nodes, different encryption techniques must be followed for the interaction between nodes sharing the transactional data. Validating all these various entities is a must for ensuring that the developed blockchain ecosystem is functioning as expected.

2.2. Testing Types

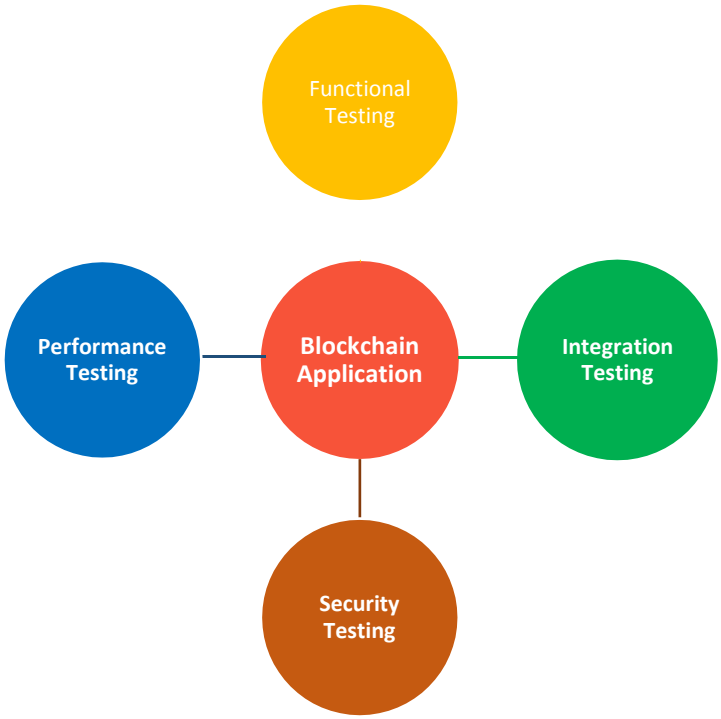


Fig 2.2 – Testing Types – Blockchain Application

2.2.1. Functional Testing

Functional testing plays a vital role in assessing the business circumstances and effectiveness of use-case scenarios. The following are the key considerations for performing functional testing in blockchain applications:

Block Size: Each block in a blockchain has a memory size in megabytes, and it was reduced to 1MB from 36MB for security reasons. Testers must focus on scenarios like if the transaction data stored in each block exceed 1mb, what encryption techniques should be used to connect these blocks, and similar complex scenarios.

Data Transmission: Data loss during transmission between blocks must be tested, as the main architecture of block chain revolves around data transaction and security.

Adding a block: The blocks which get added to the chain must be carefully evaluated, as once they are added to the chain they cannot be altered.

Smart Contract: Making sure that the parties involved in transactions are adhering to the rules of the smart contract will ensure the smooth functioning of the blockchain application.

Node Testing: All the diverse nodes present on the network must be tested independently to ensure their smooth functioning.

2.2.2. Integration Testing:

As blockchain is an ecosystem which comprises of different components, and all those components must be connected. Also, it's crucial that the different APIs associated with these components are tested for their compatibility with each other.

2.2.3. Performance Testing:

Performance testing in blockchain is significant from the perspective of number of transactions and the transaction size being tested for the performance of a block, or an application being prepared to be deployed to production. Other significant and dependent parameters include network, sequence of transactions at each node, transaction processing speed, and user and system interface along with the responses required from smart contracts.

Testing the size of the network and its ability to process transactions is critical, as it allows us to identify hardware and software bottlenecks before deployment, and also the cost incurred on running the application on cloud or any other suitable environment. The end-to-end scenarios are considered for overall performance of the blockchain environment.

2.2.4. Security Testing:

The agenda here is to guarantee that blockchain applications are tested extensively to identify if they are vulnerable to attacks, and if the authorization and authentication systems are credible.

Security testing additionally considers the other significant angles, for example, confidentiality, integrity, non-denial of services, availability etc. Security testing ends up being significant in case of hacking of identity layer of the blockchain application.

Transactions which are in progress during the event of detection of identity layer hack can't be halted immediately. Thus, security testing should be performed to reveal all such potential identity layer hacks.

Security testing of blockchain (crypto currency-based) applications also include challenges or testing of components such as wallet signatures methods, private keys, consensus algorithm, and application platform dependencies.

The other significant factor for security testing is that fraudulent transactions are irreversible as transaction reversal is nearly impossible in blockchain technology.

3. Recommended QA Approach

The determination of the correct testing tool for testing blockchain applications is a vital step for effective and successful testing.

Fig 3 – Critical Phases – QA Approach

4. Tools, Accelerators, and Business Benefits

4.1. Tools

The following are a few tools that help in testing blockchain applications and guarantee that they are functioning properly.

Blockchain Tool / Framework	Tool Capabilities / Details
Ethereum Tester	Ethereum, one of the most utilized platforms for building blockchain apps, and is packed with tools that can facilitate both app development and testing. Ethereum Tester is reliable for Web3 Integration, API, Smart Contracts, Backend, and several other blockchain tests. Testnets (Ropsten, Kovan, and Rinkeby) simulates production like blockchain (where your real Ether and tokens reside). This helps both developers and testers to simulate.
Ganache (Testrpc)	This tool is mainly used to test Ethereum contracts locally. It creates a simulation of a blockchain that allows anyone to use multiple accounts for testing. Since the test results are from a simulation and not a live event, the test results will be satisfactory but not perfect.
Hyperledger Composer	It is an open-source tool that allows you to model and test your blockchain network with a minimal set of tools like Docker and a browser. It's done through Hyperledger Composer, which facilitates blockchain development with a modeling language, a UI, and a CLI. It allows automated system tests, interactive testing, and automated unit tests.
Exonum Testkit	Testing the activity of the entire service of the blockchain application is the specialty of Exonum Testkit. The tool allows us to do API testing and transaction execution without the need of the network operation and consensus algorithm.
BitcoinJ	This is an open-source Bitcoin client library, built using Java and implements the Bitcoin network protocol. It can maintain a wallet, send/receive transactions without needing a local copy of Bitcoin Core, and has many other advanced features. Though it's developed in JAVA, it

	can be used from any JVM compatible language like Python, JAVAScript, etc.
Populus	Populous is a peer-to-peer invoice platform. It makes use of blockchain's distributed ledger technology to provide a global trading platform for invoice financing. Invoice Finance is a form of funding that instantly unlocks the cash tied up in outstanding sales invoices. Business owners allow invoice buyers to buy invoices at a discounted rate to unlock their cash quicker.
Manticore	This tool is used to perform security testing on blockchain applications. Manticore is a symbolic execution tool for analysis of binaries and smart contracts.
Corda Testing Tools	Corda is a blockchain-based and open-source distributed ledger platform. It has a built-in testing feature to help with: • Writing contract tests • Integration testing • Writing flow tests • Load testing
Embark Framework	Embark is a framework for building, testing, and deploying a blockchain app. It allows to develop and deploy decentralized applications. A decentralized application uses one or more decentralized technologies. Embark currently integrates with decentralized storages (IPFS), EVM blockchains (Ethereum), and decentralized communication platforms (Whisper and Orbit). Swarm is supported for deployment.
Truffle	Truffle is a very familiar tool for Ethereum developers with a variety of testing features, including automated contract testing. This framework has functionality beyond just testing and worth adding to the testing toolbox.

4.2. Accelerators

We can leverage the following test scenarios and reduce the effort in test design.

Block_Chain_Stand
ard_Test_Scenarios.x

4.3. Business Benefits

Proper identification of manual & automation test tools can save 30% of the test execution effort.

5. Potential Use Cases

Large Syndicate Loans to Corporates/Individuals	Claims Processing in Insurance Industry
Import/Export Transactions	Underwriting in Insurance Industry
Cross Border Transactions	Healthcare Policy Issuing
Cryptocurrency Payments	Mobile Wallets and Money