Blockchain application testing – challenges and fixes

Blockchain is a distributed ledger technology which records information in a secure manner that prevents data alteration or hacking. It is a distributed database, or an immutable ledger, which facilitates the process of recording transactions and tracking assets in a network. To put it simply, blockchain can be thought of as an electronic database that stores digitised data in blocks. These blocks have a defined storage capacity. Once filled, one block can connect to another block, and this goes on to create a chain-like structure known as blockchain. Any changes made to a block are visible to the authorised personnel, and thus, any tampering with the same will not go unnoticed. Virtually, anything that has value can be tracked and traded on a blockchain network.

Due to its highly secure nature, blockchain is increasingly gaining popularity in the global market. However, it is important to understand that any flaws in a blockchain network may result in huge losses. Therefore, it is necessary to thoroughly test each block and adopt testing approaches that eliminate risks.

pwc

Use cases of blockchain technology

Different industries and sectors are increasingly implementing blockchain technology to secure organisational processes. A few of these use cases have been highlighted below.

Banking

The banking sector considerably benefits by implementing blockchain into its processes. Transactions can be done easily and quickly. Transferring money across organisations can be made safe. Moreover, blockchain can be implemented in trading and automating transactions.

Insurance

Blockchain can help to automate claim functions by verifying the coverage between companies and reinsurers. Payments for claims between different parties can also be automated, thus reducing the administrative costs of companies. Furthermore, blockchain can be used in fraud detection and client onboarding processes.

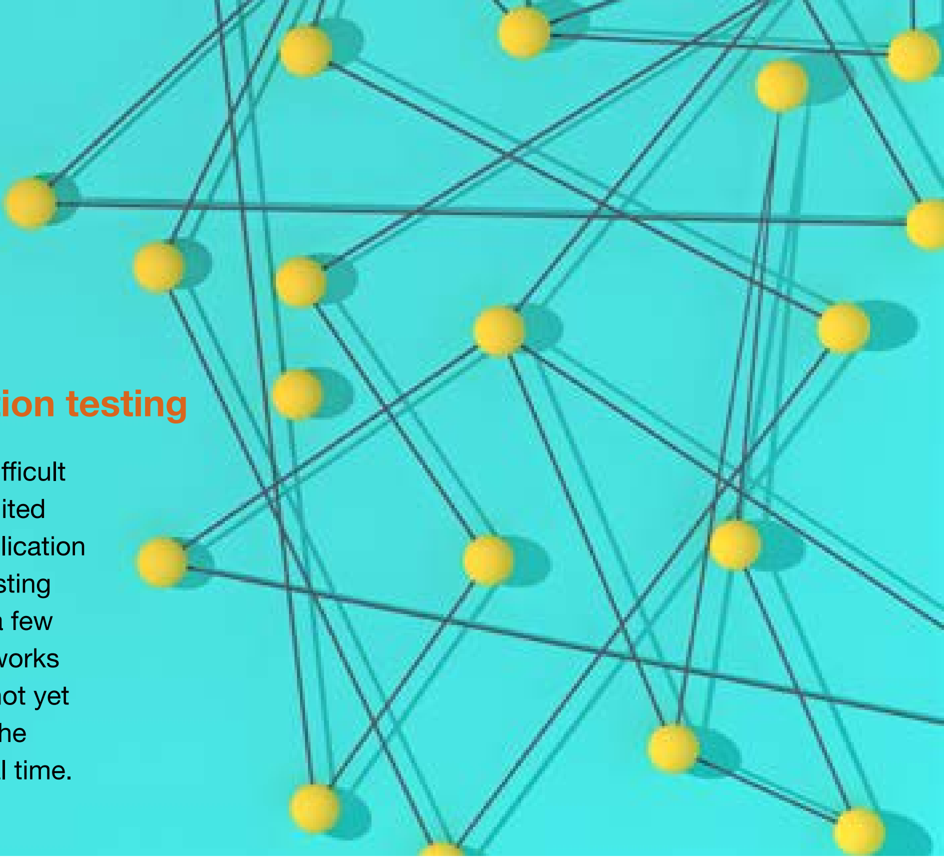
Healthcare

Blockchain can be incorporated in healthcare management systems to securely store patient medical records/data. Once a medical record is created on the blockchain, it can’t be altered. Further, such records are stored in the form of a secret key which can only be accessed by an authorised person. Other key areas where blockchain can be implemented are:

- auto claim processing
- cryptocurrency as a payment option.

Real estate

Blockchain can be used in real estate to maintain property records, which may reduce the challenges faced by both sellers and buyers – e.g. sharing property-related data securely, physical presence of both parties in every single event, too much paperwork, etc.



Blockchain application testing

In order to build a robust blockchain application, it is necessary to thoroughly test the system to determine and remove any flaws. Testing a public blockchain is very important as any bugs in the system may result in huge financial losses.

Challenges in blockchain application testing

As blockchain is a relatively new technology, it's difficult to find experts in the field due to skill gaps and limited resources. End-to-end testing of a blockchain application also requires multiple tools. Further, blockchain testing is time consuming and costly. Although there are a few available frameworks, it's difficult to test all frameworks in one go. Moreover, load/performance testing is not yet possible in blockchain applications, which raises the question on how such applications will work in real time.

Problem statement: Identify which framework is best suited to a particular use case for testing.

Solution

For this problem statement, let's consider a smart contract as the application programming interface (API) and perform code mocking to eventually decrease the code coverage. Then, an API testing framework can easily be adapted, which a user can use to establish a two-way communication of messages from mocks to enhance the coverage.

Let's understand this with an example – here, a simple Solidity code is written using the getter-setter method:

```
pragma solidity 0.8.9;
contract MyContract {
  string private msg = “Lorem Ipsum”;
  function getMsg() public view returns(string memory) {
     return msg;
  }
  function postMsg(string memory newMsg) public {
     msg = newMsg;
  }
}
```

Then, we create the configuration as follows:

```
module.exports = {
networks: {
  development: {
    host: “127.0.0.1”,
    port: 8545,
    network_id: “*”
  }
 },
 mocha: {
 },
 compilers: {
  solc: {
    version: “0.8.9”,
    docker: false
  }
 }
}
```

Now, let’s deploy the code:

```
var contract = artifacts.require(“MyContract”);
module.exports = function(deployer) {
 deployer.deploy(contract);
};
```

The script below can be used like an API:

```
var abi = [
 {
  “constant”: true,
  “inputs”: [],
  “name”: “getMessage”,
  “outputs”: [
   {
    “name”: “”,
    “type”: “string”
   }
  ],
  “payable”: false,
  “stateMutability”: “view”,
  “type”: “function”,
  “signature”: “0xce6d41de”
 },
 {
  “constant”: false,
  “inputs”: [
   {
    “name”: “newMessage”,
    “type”: “string”
   }
  ],
  “name”: “postMessage”,
  “outputs”: [],
  “payable”: false,
  “stateMutability”: “non-payable”,
  “type”: “function”,
  “signature”: “0x368b8772”
 }
];
```

As shown, a blockchain contract can be tested by anyone who is familiar with API testing.

Problem statement: Create sufficient data for testing all possible scenarios.

Solution

To ensure sufficient data for testing, one needs to create samples of all possible transactions such as balances, withdrawals, purchases and expenses. However, implementing this in a public blockchain would be expensive and may remove predictability from testing. Thus, a private test environment can be set up, which will considerably ease the automation process.

Although public testnets can be used in place of public blockchains, they will not be sufficient in terms of breaking down or altering the data to make testing predictable. Thus, the only alternative is to use a private blockchain that can provide better coverage in terms of testing a blockchain app.

Problem statement: Ensure security when the blockchain application is integrated with third-party apps.

Solution

Standalone blockchain platforms have proved to be secure until now. However, the security of a blockchain-based solution also depends on all applications that are part of the ecosystem with which the blockchain is integrated. Often, such an ecosystem consists of multiple organisations and third-party service providers (e.g. smart contract developers and wallet and payment platforms). Moreover, different organisations may use different types of devices and protocols, which may cause various security concerns. The security considerations of a public blockchain differ from those of each organisation or service provider which is a part of the blockchain application ecosystem. Thus, to avoid leaks and prevent external attacks, it is recommended to vet all parties in the ecosystem thoroughly. The vetting phase should be followed by comprehensive testing to ensure that all risks associated with the use of third-party solutions integrated into the blockchain application have been checked for and appropriate measures have been put in place to minimise system vulnerabilities.

Conclusion

As discussed, blockchain applications offer secure storage systems but also require thorough testing in order to work effectively. Without proper testing, blockchain applications may have vulnerabilities that may result in huge losses. Presently, efforts to automate blockchain application are underway to check how such applications work with different loads in real time. In future, we can expect to get easier and faster solutions for testing blockchain applications, although a detailed test analysis will always play a pivotal role in testing.

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 152 countries with over 328,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

Contact us

Ashootosh Chand
Partner, Digital and Emerging Technologies
PwC India
ashootosh.chand@pwc.com

Indrojeet Bhattacharya
Managing Director, Digital and Emerging Technologies – Web 3.0
PwC India
indrojeet.bhattacharya@pwc.com

Contributors

Aniruddha Ghosh

Rashi Gupta

Shipra Gupta

pwc.in

Data Classification: DC0 (Public)

In this document, PwC refers to PricewaterhouseCoopers Private Limited (a limited liability company in India having Corporate Identity Number or CIN : U74140WB1983PTC036093), which is a member firm of PricewaterhouseCoopers International Limited (PwCIL), each member firm of which is a separate legal entity.

This document does not constitute professional advice. The information in this document has been obtained or derived from sources believed by PricewaterhouseCoopers Private Limited (PwCPL) to be reliable but PwCPL does not represent that this information is accurate or complete. Any opinions or estimates contained in this document represent the judgment of PwCPL at this time and are subject to change without notice. Readers of this publication are advised to seek their own professional advice before taking any course of action or decision, for which they are entirely responsible, based on the contents of this publication. PwCPL neither accepts or assumes any responsibility or liability to any reader of this publication in respect of the information contained within it or for any decisions readers may take or decide not to or fail to take.

SG/February 2023 - M&C 25537