BOTM™

*Codeless Testing Automation*

# BLOCKCHAIN TESTING: ENSURING INTEGRITY AND SECURITY

# INDEX

# INTRODUCTION

The last few decades have witnessed widespread transition, thanks to giant strides in digital technology. From manual processes and procedures, to software packages for almost everything. In a world where digital transactions, Cryptocurrencies, Electronic Health Records (EHRs), and much more are on a rapid upswing, protection of sensitive and confidential data becomes pivotal to building user confidence. Trust once broken, is very difficult to beget. This is why Data Integrity and Security gain immense importance, and become two non-negotiable sides of the same coin.

It is against this backdrop that an urgent need arose, to safeguard the integrity, security, and reliability of digitally recorded, transmitted, and stored data. Blockchain Testing emerged out of this vital need. Blockchain technology is based on the three principles of **Cryptography, Decentralization, and Consensus**, to create a highly secure underlying software system that is almost impossible to manipulate. There is no single point of failure, and a single user cannot change the transactions/data records.

However, what is important to note, is that blockchains being decentralized, unchangeable, and often public ledger, any flaw has the potential of having far-reaching consequences, including but not restricted to financial loss, data breaches, and operational failures. Blockchain Testing therefore needs to be meticulously done, so that integrity and security of data in the blockchain ecosystem is assured, and losses to individuals and organizations are kept at bay.

This Whitepaper systematically unravels relevant information related to Blockchain Testing, with a view to helping Testers achieve the essential twin goals of Data Integrity and Security.

# ABSTRACT

Blockchain is a fast-developing technology which facilitates great convenience of doing transactions and handling sensitive and confidential information, in a very secure environment, where data is cryptographically transmitted to rule out any tampering or leakages. Blockchain Testing is therefore extremely important, in order to ensure a comprehensive risk management system, that ensures data integrity and security for the blockchain network.

This Whitepaper explores this important technology, reviewing it in three sections.

I. The first section titled '**Introduction to Blockchain Technology**', provides basic insights into this novel technology, explores its important principles, reviews the different types of blockchains, and presents the practical applications of blockchain technology

II. The second section titled '**Beating the Cheats through Blockchain Testing**', comprises of the following:

- **Getting into the Mind of Fraudsters**
- **Learning from Blockchain Frauds**
- **Essential Tests for Ensuring Blockchain Integrity and Security**

III. The third section titled '**Benefits, Challenges, and Best Practices in Blockchain Testing**' presents the advantages of Blockchain Testing; the many challenges involved; and best practices for efficient and effective Blockchain Testing.

It is hoped that this comprehensive treatise will provide clearer insights into this novel technology, and the various aspects of its security.

# INTRODUCTION TO BLOCKCHAIN TECHNOLOGY

**Understanding Blockchain Technology**

Before exploring Blockchain Testing, it is important to understand the term 'Blockchain'. It is primarily a decentralized and distributed ledger technology that registers transactions throughout a network of computers, in a secure and unchangeable manner. With each transaction or 'block' being cryptographically linked to the previous 'block', a chronological chain of blocks is formed, which explains its nomenclature. The feather in the cap of this technology, is that it promotes transparency and immutability, both of which are pivotal for protecting the integrity of transactions, and safeguarding them too.

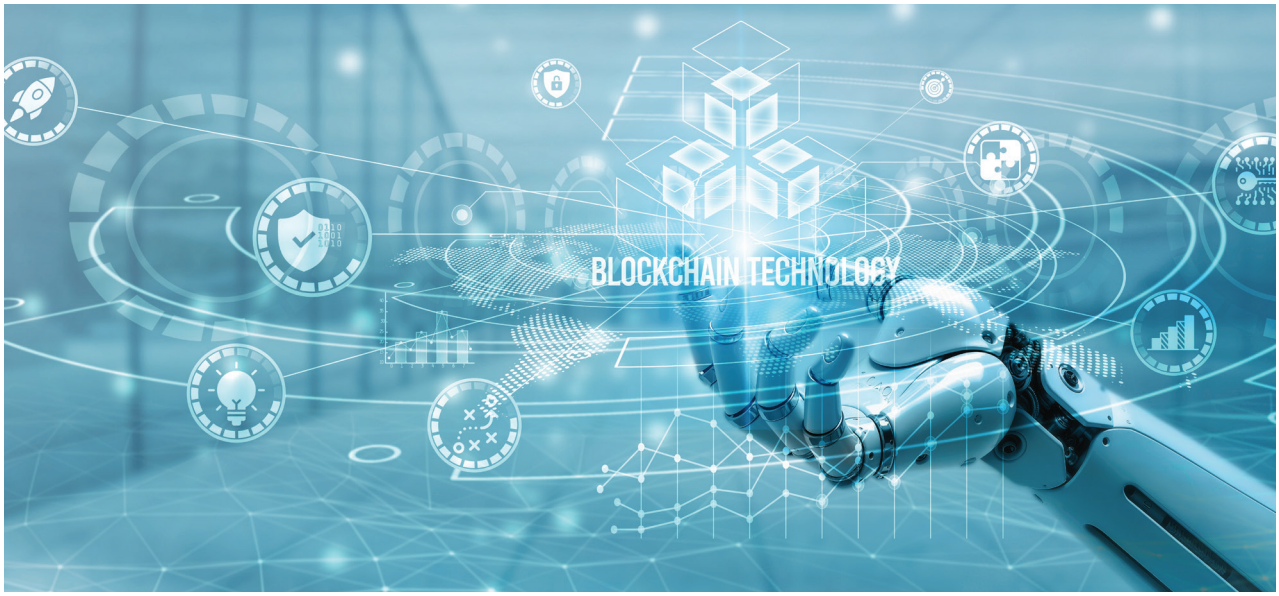
**Blockchain Technology – The Stamp for Data Integrity**

As already stated, Blockchain systems rest on the firm foundation of **Cryptography, Decentralization, and Consensus.** A word about each of these:

**Cryptography:** Cutting-edge cryptographic security practices are employed by blockchain systems, to safeguard data and prevent it from being altered in any way. Every user in the network has a unique cryptographic key, which confirms their identity and ensures data authenticity.

**Decentralization:** Blockchain uses decentralization to protect data, using a peer-to-peer network principle, whereby data is stored and validated on several nodes, to prevent single points of failure. This greatly brings down the risk of data manipulation, and unauthorized access.

**Consensus:** The Consensus principle of blockchain technology ensures that data recorded on the blockchain system cannot be deleted or changed in the slightest manner, without consensus or approval from the other network participants. This mandatory consensus safeguards data integrity, and promotes traceability even over the longer horizon.



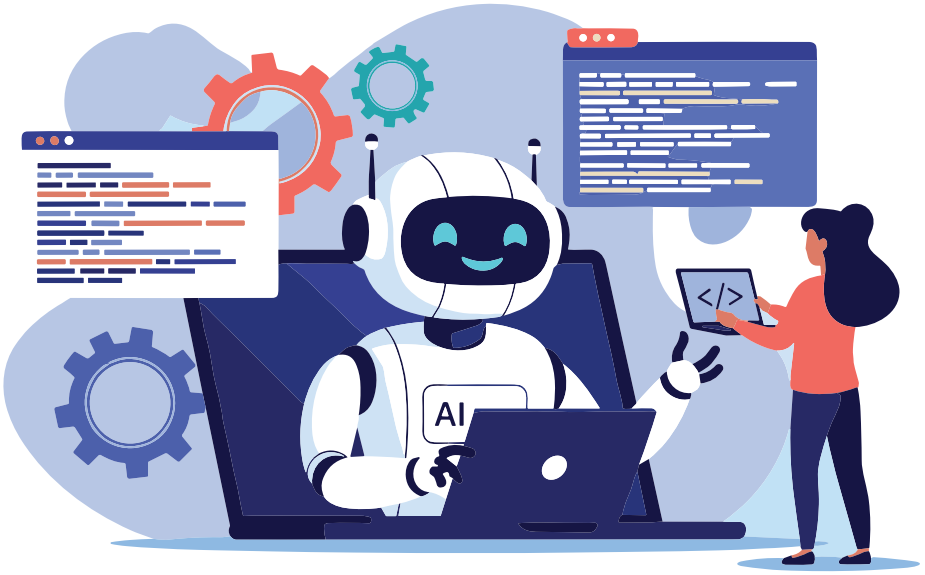
## TYPES OF BLOCKCHAINS

Blockchain networks are of two types i.e. Public Blockchains, and Private Blockchains, based on the level of accessibility to users or participants.

**Public Blockchain Networks:** Public Blockchains have no restriction on who can join the network, hence anyone with an internet connection can join the network, read data and, participate in transaction validation. Internet-connected computers are used to validate transactions and achieve consensus. Participants may even choose anonymity on this network. Thus, Public Blockchains are **Permissionless Blockchains** with no restrictions on processors. Bitcoins and Ethereum are two of the better known Public Blockchains.

**Private Blockchain Networks:** These are networks with restricted access, where only members are allowed to participate, with a single entity, or consortium, controlling membership. Each participant has an identity which acts as confirmation of membership. This is a must to participate and use the privileges offered to members. Membership is restricted to known entities, who together form the Private Blockchain. In other words, Private Blockchains are **Permissioned Blockchains** where access is given to a select group of users, via individual identity certificates. Consensus is obtained through selective endorsement, whereby identified users verify the transaction. Levels of access differ; and transaction ledger maintenance is restricted only to those members who have special permission.

**Choosing between Public and Private Blockchains:** Developers and Testers involved in creating apps for blockchains, need to determine the needs and functionality of the app in conjunction with the business goals, and then take a call on whether to build a Public Blockchain or a Private one. If high levels of control are paramount then a Private Blockchain is the way forward. This is also the case when there is high amount of compliance and regulation required. However, if decentralization and greater distribution takes precedence over strict control, then obviously Public Blockchains have more to offer.



## PRACTICAL APPLICATIONS OF BLOCKCHAIN TECHNOLOGY FOR DATA INTEGRITY AND SECURITY

**Financial Transactions:** Blockchain technology has played a pivotal part in popularizing cryptocurrencies like Bitcoin and Ethereum. Transactions in these networks take place devoid of middle-men, and are kept secure through blockchain technology. Data integrity, security, and transparency are promoted by smart contracts which automate and enforce transaction rules, without outside interference, thus reducing the risk of fraud, and/or compromise of financial data.

**Healthcare Records:** Blockchain technology has ushered in a new era in healthcare, introducing Electronic Health Records (EHRs), which facilitate ease in consultation even if doctors and patients are based in different parts of the world. Blockchain in healthcare makes possible the safe, secure storage and management of medical records, making patients the guardians of their personal medical records, and putting the controls in their hands, for sharing the same as needed. Thus, blockchain introduces data integrity in healthcare by giving patients control, in order to avoid data breaches, and pr ovide ease in accessing medical guidance.

**Digital Identity Verification:** Blockchain-based identity platforms have taken convenience to new levels, by offering decentralized immutable solutions for confirming digital identities. Confidential personal information that gets into wrong hands, can have far reaching negative consequences. Blockchain technology, hands over the controls of digital identities to the concerned individual, with access to cryptographically share it securely whenever required. Thus, blockchain has enabled data integrity in digital identity verification, greatly reducing identity theft and unauthorized access.

**Supply Chain Management:** Blockchain technology plays an important role in tracking transactions all through the supply chain, by registering every transaction and movement of goods. There's transparency too, as identities of those involved at each stage are also recorded. Thus, data Integrity on supply chains is fortified to ensure authentic product information, and genuineness of products, which in turn increases the trust and reliability quotient for all concerned.

Updated with this information on blockchain technology, this Whitepaper moves to its central theme of Blockchain Testing.

# BEATING THE CHEATS THROUGH BLOCKCHAIN TESTING

## Getting into the Mind of Fraudsters

'To catch a thief, you must think like a thief.' – So goes a wise old saying.
With this in mind, this Whitepaper will first explore how fraudsters and scammers target blockchain technology for their nefarious motives. Their modus operandi is through Phishing, Routing, Sybil, or 51% attacks. A word about each of these.

**Phishing:** Phishing is an attempt by fraudsters to gain access to user's credentials, by sending official-looking emails or messages with a fraudulent hyperlink, which is made to look official. They hoodwink their victim into believing that the message is from a legitimate source and needs urgent attention. If the user clicks on the fake hyperlink, the scammers get access to the user's credential and other confidential information, through which the scammer can dupe the victim big time.

**Routing:** Routing attacks are unleashed on unsuspecting blockchain participants, without any indication, or direct involvement of the victim. Fraudsters hack into blockchain systems while large volumes of data are transferred real-time to internet service providers. The hackers thus gain access to highly sensitive data and route it to their own devices or destinations. They then use this data or this access to defraud victims of money. Being a 'behind-the-scene' activity, the victim is quite oblivious of the attack when it is happening.

**Sybil Attacks:** This fraudulent strategy of scammers, consists of creating and using several fake network identities or nodes, to flood the network and gain excessive influence over it, with the purpose of disrupting normal operations. Having spammed the network, they use it to disseminate misinformation, or block legitimate nodes. Here's an aside: This attack got its name from a famous fictional character who, in the story, had a multiple identity disorder.

**51% Attacks:** This attack focuses on gaining more than 50% of the blockchain network's mining power, in order to gain control over the ledger, which then gives hackers access to exploit the blockchain for their advantage. The modus operandi is for a single miner or a group of miners to gather enough mining resources on the network, garnering more than 50% mining power, so as to monopolize the computing power of the blockchain. While private blockchains are safe, public blockchains can become targets of 51% Attacks.

## Learning from Blockchain Frauds

The question that pops up is that if blockchains are cryptographic, immutable, and secure, then how do hackers strike. The answer is that blockchain networks and infrastructure can be potential weak spots where hackers can strike. This is why Blockchain Testing is important, to ensure blockchains are indeed secure. A look at past blockchain frauds, will throw light on the vulnerabilities that can be exploited.

**Attack on The Decentralized Autonomous Organization (DAO) Blockchain**

DAO – a venture capital fund, following in the footsteps of Bitcoin, conducted their operations through a decentralized blockchain. However, hackers used code exploitation to siphon off Ether digital currency worth over USD 60 million which was a huge loss, considering that it amounted to a third of its value. Code exploitation was what wreaked this havoc on the blockchain network.

**Bithumb Blockchain Attack**

Hackers even managed to attack Bithumb – one of the largest Ethereum and Bitcoin Cryptocurrency Exchanges. This attack resulted in bitcoins worth USD 870,000 being drained from the exchange, and even put at risk the data of 30,000 users. While the primary servers were all secure, the hackers exploited the vulnerability in an employee's computer, to unleash this great loss that affected so many. This reveals the importance of ensuring security of every bit of infrastructure used on the blockchain. Such compromises must be avoided at all costs, as it puts at risk the financial resources and confidential data of numerous participants. The entire infrastructure whether hardware, software, or networking, which is in any way part of the blockchain network, must be thoroughly tested, to secure the integrity of the blockchain. Thus, Blockchain Testing will be successful only when every aspect and layer of technology is thoroughly tested. The smallest flaw can irreversibly compromise the entire blockchain system.

**Essential Tests for Ensuring Blockchain Integrity and Security**

Blockchain Testing comprises of testing the entire ecosystem, including smart contracts, blockchain protocols, distributed ledger components, and network security. They can be broadly grouped under the following types:

## 01 Functional Testing

This is done to verify that all the functional areas of the blockchain application are working as expected. Functional tests focus on the following:

**Smart Contracts Testing:** Smart contracts being self-executing contracts, the terms and conditions of the contract are written directly into the code itself. Testing must therefore meticulously ensure that there are no logic errors, vulnerabilities, and flaws.

**Transaction Validity:** Testing must confirm that only valid transactions are processed and added to the blockchain, and that there is no data loss during the transmission of data from one block to another. Integrity of balances, and previous and current transaction details must also be verified. Testers further need to test for scenarios where invalid or fraudulent transactions are attempted, to rule out the possibility of fraudulent transactions.

**Consensus Mechanism:** This involves testing the consensus algorithm (e.g., Proof of Work, Proof of Stake) to ensure it functions correctly under diverse conditions like network delays or malicious attacks.

## 02 Peer/Node Testing

This testing is vital because blockchains use the principle of peer-to-peer distributed networks through network nodes, using authentication protocols. Hence by and large all the nodes must be tested to check that they approve the block for its legitimacy to do transactions. Heterogeneous nodes must be checked independently. Node testing comprises of the following tests:

**Node Synchronization:** Verifying the capability of nodes to synchronize with the blockchain, more so, after joining the network or recovering from a failure.

**Fault Tolerance:** Checking whether the blockchain is able to combat node failures, including testing for Byzantine fault tolerance, in networks that are intended to withstand malicious nodes.

## 03 Security Testing

This is important to ensure that there are no weak spots in the blockchain, which hackers can exploit. The importance of securing shared ledgers and nodes cannot be stressed enough, as an attack on a network node has the potential to shut down the blockchain and the applications hosted by it. A classic example is a Distributed Denial-of-Service (DDoS) Attack, where a hacker floods a server with internet traffic, to prevent users from accessing connected online services and sites. The following tests are important for ensuring blockchain security:

**Access and Authorization Testing:** Testing the blockchain application to permit only authorized access, authentication, security hash, wallet signatures, and private keys. This testing must aim at detecting loopholes and misconfiguration that could be potential threats to data integrity and security.

**Penetration Testing:** Simulating attacks to identify weaknesses in the blockchain network, nodes, and smart contracts; and also testing for common or known attack routes which hackers follow for Sybil attacks, DDoS attacks, and 51% attacks.

**Cryptography:** Cryptography being so central to blockchains, it's crucial to test the implementation of cryptographic algorithms used for transaction signing, hashing, and data encryption, to be absolutely sure that they are correctly implemented and can resist any attack.

**Data Integrity:** Testing that data stored on the blockchain is immutable and cannot be changed without consensus.

## 04 Integration Testing

Blockchain being based on a decentralized and distributed ledger technology that works throughout a network of computers, it's obvious that it comprises of several interfaces and components. Consistent integration is a must, to ensure that the blockchain network functions smoothly. Integration testing, is needed to confirm that all interfaces are syncing well with each other, and response time too is as expected. **Interoperability Testing** i.e. verifying the blockchain's ability to integrate well with existing systems or other blockchains gains importance, more so for applications requiring cross-chain communication or data exchange.

## 05 API Testing

API testing is vital for blockchains, to promote consistent and effective communication between the client's network and blockchain node. It consists of verifying that API response is error-free and that transaction data transfer is secure. It confirms that APIs exposed by the blockchain or associated applications function correctly, securely, and as intended.

## 06 Load and Performance Testing

With blockchains being interconnected and accessible to so many participants, more so in public blockchains, Load and Performance Testing are extremely important and must give a green signal to all possible performance parameters before deployment of the application. It includes the following areas of testing:

**Scalability Testing:** Determining the blockchain's ability to handle an increasing number of transactions or nodes. This includes checking on the quantum of transactions per block, speed of transactions, and also the response time from smart contracts. Latency, throughput, and resource usage under load, also need testing.

**Latency Testing:** Calculating the time taken for transactions to be processed and confirmed on the blockchain, to verify it meets the application's prerequisites.

**Throughput Testing:** Gauging the number of transactions per second supported by the blockchain, and how it scales with additional nodes or changes in network conditions.

## 07 Compliance Testing

With blockchains dealing with cryptocurrencies and/or confidential and private data, it's vital that all legal and statutory compliances and industry standards are met. This is done through Compliance Testing which consists of the following:

**Regulatory Compliance Testing:** Verifying that the blockchain system is compliant with all applicable regulations of concerned authorities – local and international; and that relevant industry standards are met. E.g. GDPR for data protection, or financial regulations for transactions; Healthcare confidentiality guidelines/standards for EHR.

**Auditability Testing:** Testing that the blockchain system permits and supports the audit of transactions and smart contract executions, for compliance purposes. Ensuring there's a proper immutable audit trail for all interactions on the blockchain.

## 08 Usability Testing

This is very important as user satisfaction is pivotal for success in the digital world.

**User Interface (UI) Testing:** It's important to check that the UI is intuitive, secure, and facilitates all required functionalities, for smooth interaction, especially for blockchain applications with user-facing components.

**User Experience (UX) Testing:** Assess the overall user experience, especially in key areas like wallet management, transaction processing, and error handling.

## 09 Regression Testing

Blockchains will need additions or modifications, but since codes are inter-dependent, well tested new codes can still create issues when integrated, and become negative catalysts in the blockchain ecosystem. Regression Testing is therefore important to reduce the risk of modification failures on the blockchain as explained below:

**Continuous Testing:** Each time the blockchain system is updated, it's necessary to verify that new codes or features do not introduce new bugs or vulnerabilities, and that they don't adversely affect existing codes, keeping existing functionalities intact.

## 10 Data Privacy Testing

Data integrity and security are two non-negotiables for blockchain systems. This can be ensured through the following tests:

**Confidentiality Testing:** Thorough testing of all processes that keep sensitive data on the blockchain private, especially in cases of permissioned blockchains.

**Access Control Testing:** Ensuring that only authorized participants can access specific data or perform specific actions on the blockchain, as per pre-defined access levels.

Before concluding this section, it must be reiterated that Blockchain Testing needs to be a continuous process, as technology keeps moving forward at a rapid rate. Besides, hackers and fraudsters are always on the prowl and therefore QA specialists cannot let their guard down. Given the decentralized and often immutable nature of blockchains, meticulous testing is vital for ensuring the security, performance, and reliability of blockchain systems.

# BENEFITS, CHALLENGES, AND BEST PRACTICES IN BLOCKCHAIN TESTING

This section sets off on a positive note, enlisting the many benefits of Blockchain Testing; moves on to explore its challenges; and then presents the Best Practices in Blockchain Testing, to help build robust and safe blockchain systems, that ensure integrity, security, and reliability of blockchain-based applications.

## BENEFITS OF BLOCKCHAIN TESTING

1. **Robust Security** that protects sensitive transactions and data, by detecting and rectifying smart contract flaws, network security issues, and other threats.
2. **Smart Contracts Validation** ensures that these self-executing contracts function perfectly as expected, thus averting time and cost-intensive errors. This is vital as the terms of agreement are directly written into the code and are later immutable.
3. **Performance Boosted** by testing performance of blockchain apps under various network conditions; and determining transaction speed, throughput, latency, and scalability under diverse loads.
4. **Consensus Mechanism Integrity** secured through meticulous Proof of Work, Proof of Stake, etc. which is pivotal to the functioning of blockchains, and averts disputes through digitally verified consensus.
5. **Promotes Data Integrity via Transparency,** since participants can view and verify transactions in real-time.
6. **Promotes Interoperability** by ensuring compatibility between all the components involved in the blockchain ecosystem.
7. **Assures Compliance** by confirming that all regulations and laws whether legal, ethical, industry standards etc. are met.
8. **Cost Containment** via detection of bugs early in the SDLC, due to which expensive rework is avoided, and time and other resources too are saved, as the complexities increase when bugs are detected late. Efficient blockchain testing averts downtime, data breaches, or other failures that can be a drain on resources.
9. **Increases User Confidence** – Well-tested blockchains will be secure, reliable and efficient, generating user confidence. This will mitigate the reservations that potential users may have, which in turn will lead to widespread acceptance of blockchain systems.
10. **Expedites Updates/Upgrades** – Blockchain Testing verifies updates and upgrades in any of the components or even in the protocols, and has a system in place for quick and timely adoption of these into the blockchain ecosystem, without adversely impacting existing functionalities or causing disruptions.

With this awareness of the manifold benefits of Blockchain Testing, this Whitepaper moves on to explore the challenges involved.

## CHALLENGES IN BLOCKCHAIN TESTING

Blockchain Testing being a relatively new field, there are challenges linked to limited information availability, rapid technological evolution, developing expertise, etc. Being aware of the challenges can help push abilities further, to successfully combat them.

1. **Immutability of Blockchain Transactions** – Blockchains have the terms of agreement of the smart contracts written into the code, which make them irreversible. Hence all care must be taken to ensure that comprehensive and custom sets of tests are meticulously done to weed out errors that cannot be later fixed. Initial identification and mitigation of these errors is vital, because if detected later in production, the smart contract can't be updated or rolled back, and a new version must necessarily be created and deployed, which is an expensive and time-consuming process.

2. **Limited Technological Expertise and Knowledge** is another challenge in Blockchain Testing, considering it is a relatively novel field. The scarcity of personnel with in depth domain knowledge, coupled with the fact that it is a rapidly evolving field, makes it difficult to find the required level of expertise.

3. **Continuous Addition of Blocks** is a must for blockchains, as they store and process consistently growing quantum of data. This can create logjams and create delays in the testing process.

4. **Integration Testing** is another consistent challenge, as multiple components interact on the blockchain, and the success of the blockchain ecosystem depends on the error-free integration of every component with every other component, that connects on the blockchain.

5. **Managing Cryptographic Data** is yet another challenge as encrypted data is the backbone on which confidence is built in blockchain systems. Any testing lapse can have far reaching consequences, as secure transmission of cryptographic data is paramount for blockchain success.

6. **Performance Testing** of blockchain apps can pose a challenge, as it's important that the blockchain has the capability to endure heavy load levels or bandwidth constraints. Lack of awareness on this count can lead to user dissatisfaction, which can be detrimental to blockchain success.

These challenges can be successfully combatted, with meticulous and comprehensive testing, and executing all the contemporary tests recommended for Blockchain Testing. A look at the best practices is a step in the right direction, to achieve a good degree of confidence in the blockchain system.

## BEST PRACTICES IN BLOCKCHAIN TESTING

1. **Check that Primary Requirements are in Sync** – Ensure that the blockchain design meets the primary purposes that were intended. This could relate to governance model for participating organizations or members, what data is to be captured in each block, relevant regulatory requirements, checking how identity details are managed, whether block payloads are encrypted, how keys are managed and revoked. It's also important to test the disaster recovery plan for the blockchain participants, and the logic for resolving blockchain block conflicts.

2. **Comprehensive Test Coverage** – Ensure that all functional and non-functional requirements are thoroughly tested, which includes testing of transactions, smart contracts, security features, and performance assessment. Thus, the entire gamut of tests must be included – unit testing, integration testing, functional testing, performance testing, security testing, and usability testing.

3. **Test Early and Frequently** – Blockchain Testing must start early in the SDLC and be consistently done throughout the development process, as errors detected later can be highly detrimental to the functioning of the blockchain, and result in huge damage and loss to the participants. Smart Contracts should be extra specially tested from all angles, as the terms of agreement are written directly into the code and are immutable. Late detection of errors will be a huge strain on the time, money and manpower resources.

4. **Automate Testing** – Testing should be automated as far as is possible, and definitely for repetitive and important test cases, to verify that results are always consistent and accurate. Available Test Automation Frameworks include Truffle, Hardhat, Ganache (for Ethereum), Hyperledger Composer, etc. Integrating Blockchain Testing into the CI/CD pipeline will definitely go a long way in confirming that all tests are automatically executed at each code change, thus reducing the risk of escaped bugs.

5. **Security-focused Testing** – Security being pivotal for blockchain success, it must be ensured that all aspects of security are thoroughly tested. It's best to adopt the latest advanced tools and methods. Ensure that all risks are taken care of – business risks, governance risks, technology risks , process risks, etc. Business risks have financial, reputational, and compliance-related repercussions. Governance risks revolve round the fact that blockchains are decentralized in nature, which means that adequate care and controls should be in place for decision criteria, governing policies, identity and access management. Technology and process risks comprise of the plethora of vulnerabilities related to compromised networks, components, integrations etc. For private blockchains, it's vital to ensure that deployment is done on secure and resilient infrastructure. Blockchain solutions must have in place a security model, risk model, and threat model. Based on these, multi-faceted security controls must be set up to alleviate risks and threats, by implementing controls that are unique to blockchains, as well as conventional security controls, and furthermore, business controls too for blockchains.

6. **Real-World Conditions** – It's important to test in real world conditions related to network performance, load, and transaction volumes, because that's where the volatility exists. If the cost of real-world conditions is out of budget, the same must be simulated using the relevant tools, which help speedy testing and debugging.

7. **Monitor and Evaluate Blockchain Performance** – Blockchains deal with sensitive data and financial transactions, and therefore their performance should be monitored on a regular basis to rule out any glitches or even bottlenecks that mar smooth operations. Performance testing tools can help in this endeavor.

8. **Collaboration** – For efficient functioning of the blockchain, all teams must be in sync. Effective and regular communication between the development, testing, and operations teams will help all to work in tandem towards common goals.

These best practices are foundational, setting the tone for designing, developing, testing, and operating blockchain networks, that holistically tackle all essentials related to technology, governance, and business; and simultaneously intensify confidentiality, trust, and security in the blockchain ecosystem.

# CONCLUSION

Blockchain technology, though a more recent arrival in the digital space, is on the growth trajectory, because of the conveniences it offers in financial transactions, and other areas that deal with sensitive and confidential data. The data is basically structured into blocks, with each new block linking to all the blocks before it, in a cryptographic chain that makes the data tamper-proof. Blockchains come with inbuilt security as they rest on the firm pillars of cryptography, decentralization and consensus – the basis on which trust in transactions is built. However, all this needs to be certified through Blockchain Testing.

Smart contract validation is vital, as the terms of agreement are directly written into the code and are immutable. The importance of robust security, meticulous consensus mechanisms, and data integrity too, cannot be underlined enough. Interoperability of the various components is crucial, given the gamut of diverse components that participate in the blockchain. Smooth performance in volatile real-world conditions can be challenging, but must be ensured. Thus, given the sensitive nature of blockchain data, consistent Blockchain Security and Testing is a must, if this new technology is to ensure integrity and security, which are imperative for winning confidence and widespread acceptance.

Introducing you to BOT™-a tried and tested automated platform for your mobile and Web apps. Visit us at **www.botmtesting.com**, and avail of the **Free Trial** that will help you experience the power of our AI and ML driven holistic app testing platform. Explore the wide array of testing services, that offer you error-free testing, and speed to go with it.

## GET IN TOUCH

022 4050 8200

sales@botmtesting.com | www.botmtesting.com

**BOT™** is the accelerator BOT for automated and manual testing of Mobile and Web applications – developed for both Android and iOS devices.