WHITE PAPER

Assuring success in blockchain implementations by engineering quality in validation

Arvind Sundarraman, *Business Development Executive, Infosys Validation Solutions*

Introduction to blockchain and smart contracts

A blockchain is a decentralized and distributed database that holds a record of transactions linked to it in blocks which are added in a liner and chronological order. It provides a secure, transparent, and immutable source of record by its design that has technology and infinite possibilities to change and revolutionize the way transactions are managed in a digital world.

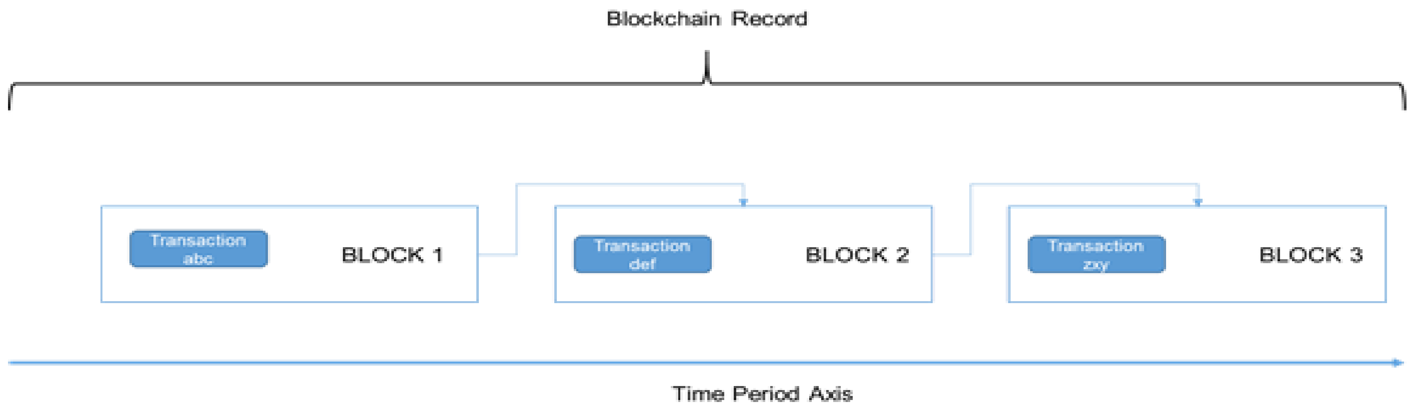

Figure 1: Transaction linkage within blocks in a blockchain

The implementation of this technology is generally carried out in a decentralized peer-to-peer architecture with a shared ledger that is made available to the authorized participants in the private and public network. This ensures that the transactions are captured within the blocks of information which are continually updated and securely linked to chain, thereby ensuring visibility of the changes as well as providing a foolproof way of handling transactions mitigating the possibility of double spending or tampering.

Smart contracts are protocols or rule sets embedded within the blockchain which are largely self-executing and enforce a contract condition. They ensure that the terms specified within the contract are executed on their own when the transactions fulfil the specified condition within the contract rules and made visible to everyone on the network without any intervention, thereby guaranteeing autonomy, safety, and trust. Smart contracts also ensure that the transactions are carried out instantaneously on the preconditions set within the contract being met.

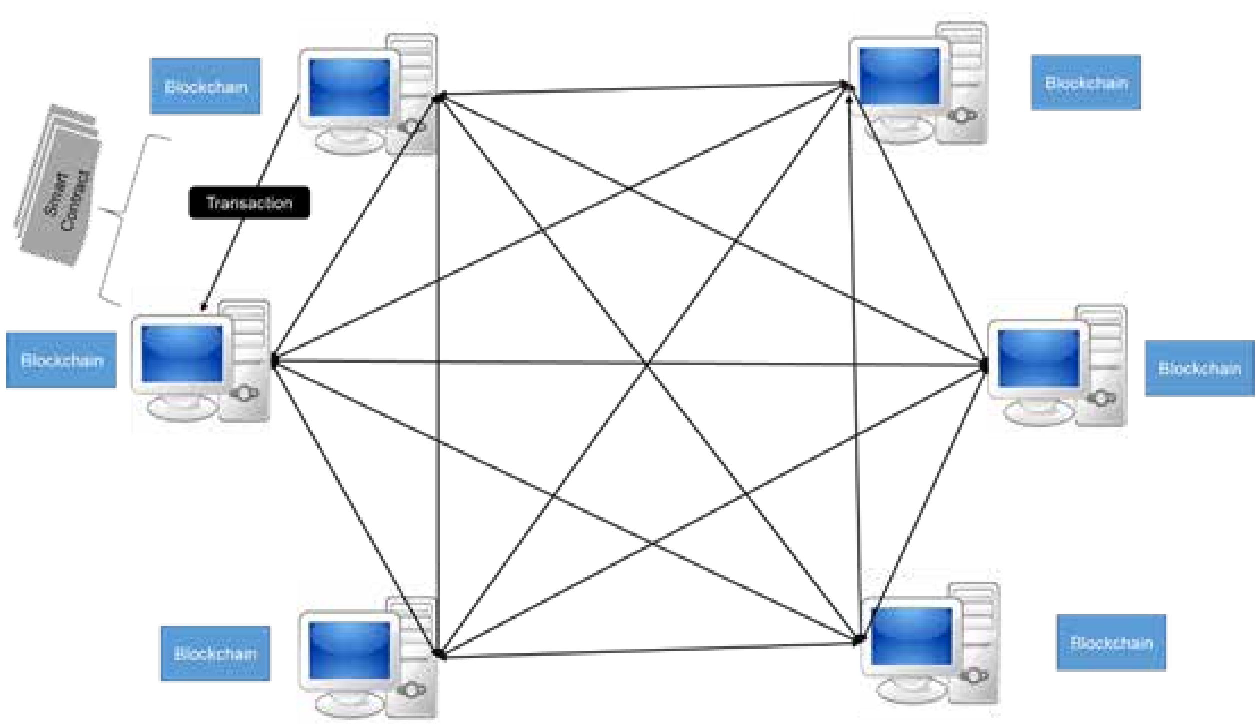

Figure 2: Peer-to- peer architecture of blockchain using smart contracts in public and private network

Smart contracts are an integral part of the blockchain and go hand in hand in ensuring the success of the distributed nature of the ledger that is the core of blockchain.

Blockchain and the digital ecosystem

In today's world, digital transactions are growing exponentially and the phenomenon is predicted to sustain and even outperform its climb in the next decade. Digital transactions are gaining popularity globally due to ease of use, improved security, and faster mechanism of managing transactions.

Blockchain technology provides a secure way of handling transactions online and hence is of enormous relevance. The most widely known implementation of blockchain technology is in the financial sector and Bitcoin as a crypto currency payment system was the pioneering system developed on this technology.

The value of blockchain technology though it is not limited to digital wallets and payments systems, its application in a wider context has gained more relevance in the recent times. Transactions through blockchain have also had an impressive surge similar to the growth in digital transactions. The graph below highlights the rise in usage of blockchain in terms of transactions. This also reflects the increase in adoption and usage of this technology across domains for various uses that initially was perceived to be mainly in the financial sector of payments and transactions.

Source : https://en.wikipedia.org/wiki/Blockchain_(database)

Figure 3: Graph highlighting the rise in the adoption of blockchain in terms of transaction per day

A number of possible use cases across various domains where blockchain technology can be applied are detailed below and this shows the potential that blockchain holds across various industries and segments.

Financial services

- Post-trade settlement, person-to-person (P2P) payments, trade finance, know your customer (KYC), global remittance, syndicated loans, asset leasing, gifting, and mortgage services

Insurance

- Automated claims processing, fraud detection, P2P insurance, travel insurance, Reinsurance, and KYC

Healthcare

- Patient records and automated claim processing through smart contracts

Manufacturing – Supply chain

- Tracking product origin, inventory management, smart contracts for multi-party agreements, and digitization of contracts / documents

Retail

- Retail supply chain, reward points tracking, blockchain based market place, and inventory management
- Energy and utility
- Energy trading and P2P power grid

Media and entertainment

- Anti-piracy / copy rights management, royalty management, and crowd funding of new content
- Transportation
- Rider passenger coordination, review authentication, and Bitcoin payment

Communication

- Billing systems and call detail record (CDR)
- Roaming and network sharing access control
- Provisioning and identity management
- Mobile wallets and money

Challenges in testing blockchain implementations

Validating and verifying that an implementation of blockchain offers a number of challenges due to the inherent structure of technology as well as the distributed nature of the system.

- **Technology stack**

  A primary factor that influences the required level of validation is dependent on whether the implementation is on a public platform like Etherum or Openchain or on a self-setup or customized platform that is purpose built for the needs of the organization. The latter needs more setup and effort in testing.

  Open source and popular platforms like Etherum have recommendations and guidance on the level of tests and have more mature methods where an in-house implementation needs a detailed test strategy frame based on the functionality that is customized or developed.

- **Test environment**

  The availability and utilization of a test platform that provides a replica of the implementation is also a need and if it is not available, considerable time needs to be spent on setting up or spawning from the real implementation.

  Blockchain implementations like BitCoin (testnet) and Etherum (modern) provide test instances that are distinct and separate from the original while providing means to test advanced transaction functionalities in a like for like mode.

- **Testing for integration**

  An implementation of blockchain within a stack of a company is expected to have interfaces with other applications. Understanding the means of interface and ensuring the consistency with the existing means is key to assure that there are no disconnects on launch. A detailed view of the touch points and the application programming interfaces (APIs) that act as points of communication need to be made available to the testing team in advance so that the appropriate interfaces can be exercised and tested during the validation phases.

- **Performance testing**

  Major problems that could affect an implementation is in estimating and managing the level of transactions that are anticipated on the production systems. One of the key issues with the Bitcoin implementation has been with delays in processing transactions due to a surge in the usage. This has led to business withdrawing from accepting this form of crypto currency as well as partners leaving the consortium.

  The need within the chain for verification of the transactions by miners can complicate the time taken to process and confirm a transaction and hence during validation, a clearly chalked out strategy to handle this needs be outlined and applied.

- **Security**

  Though the blockchain technology has inherent security features that has made the protocol popular and trusted, this also places a lot of importance on the intended areas where this is applied that are generally high-risk business domains with a potential for huge implications if security is compromised

Validation in real-world situation

The construct of validating a real world implementation and ensuring that the testing verifies the intended use case is of paramount importance as this is more complex and requires specific focus in understanding the needs as well as drafting the coverage that is required within the test cycle.

For a more detailed view of how the testing space spans on the ground, let us consider an example of an application of this technology with an assumed integration of the feature for a telecom operator who implements this application to manage user access and permissions and handover in roaming within the operations support systems (OSS) business support systems (BSS) stack of the operator. It is assumed that the communication service provider (CSP) and the partner CSPs providing service to the customer during the roaming have an agreement for implementing a common blockchain based platform as a solution to manage the transaction in each other's network as well as communicating with the CDR of the subscribers. The implementation should ensure that the authentication of the user, authorization of the service, and billing systems are managed between the CSPs while the user moves from the home mobile network to the visited mobile network of the partner CSP.

A depiction below shows the illustration of the management system employed in this scenario that would be built on blockchain technology.

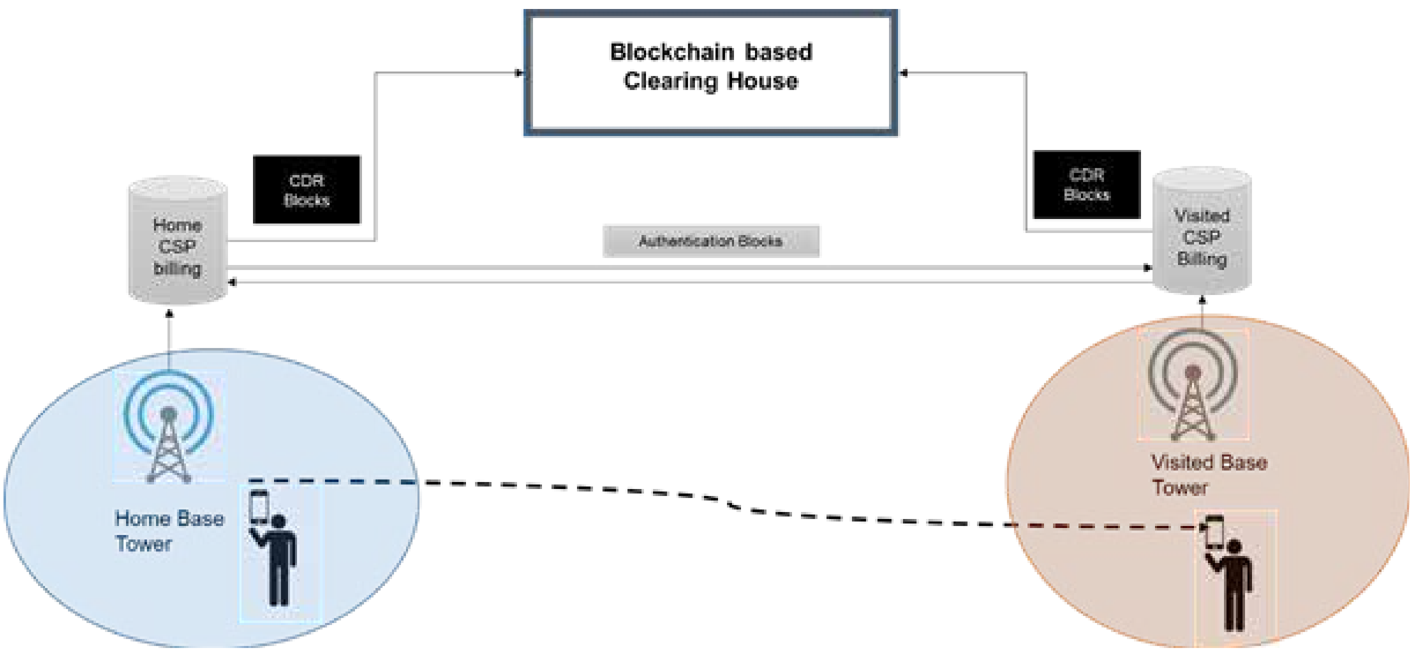

Figure 4: Illustration of the management system built on blockchain technology

The above model provides a secure medium of authentication of the user who is entering the partner network assuming that the identity of the user can be verified over a shared ledger system and signed by the respective base owners of the users. Similarly, the CDRs that relate to the roaming duration can be cleared over a joint system of clearing house that is built on blockchain technology. This would ensure instantaneous management of transactions and charges can be setup based on contracts to ensure that the information is relayed back to the customer instantaneously providing far more agility and trust in the management of the subscribers in other networks.

With this system in design, let us look at the key activities that are needed to ensure that the implementation meets the desired objectives outlined.

- System appreciation

  The early involvement of the testing team is extremely important since there should be a view of the applications within the stack that would be modeled on the new technology along with the affected system components. A detailed view of the impacted components needs to be included in the testing plan and a strategy put up in place for each of these components that are impacted. For example, in the above case, the billing systems as well as the user identity managed systems are impacted where the customer relationship management (CRM) system may not be directly affected by the change. Testing scope for the impacted components would be higher than the others where a functional workflow with regression test on the CRM systems could suffice.

- Test design assurance

  In this phase, with an early system view, the team needs to put up a detailed level test strategy and assign a traceability to the requirements. Specifically to blockchain testing, the key components that need to be checked in this phase include

- Build a model of the structure of the blocks, the transactions, and the contracts that need to be tested
- Outline a use case for each individual section and end points to be validated, i.e. if the transaction is to pass the user credentials to the visiting network for authentication, then detail the scenarios under which testing could be required.
- Estimate non-functional requirements (NFRs) as well as security testing needs. In the above example, the number of CDRs logged in the clearing house over a month should give a fair idea of the number of transactions which are expected and hence performance tests can be considered at this level. For security testing, the APIs that are exposed need to be considered as well measuring the inherent level of security in the blockchain technology (private or public)

- Test planning

Test planning needs to consider the full test strategy as well as other the methodology to test and place to conduct the testing.

For the above examples, a full test strategy should outline the availability or non-availability of a test environment or a testnet and if one is not available, a view of how a private one can be setup.

Also a low level view of how testing is conducted along with the approach to it in each phase from unit till integration, functional tests needs to be finalized. It is recommended that the volume of tests follow a pyramid structure and there is a good amount of lower level tests (unit) to identify and correct the systems prior to integrating them with the rest of the systems in the stack. From the illustration below, it is assumed that an Etherum based blockchain solution has been implemented for managing user handling during roaming and there is an existing Amdocs billing system that it integrates with.

Testing phase	Volume of tests	Test methodology and tools
Developer / Unit testing	2500	Test-driven development (TDD) approach with a suitable framework
System testing	1000	Verify contracts, blocks, and blockchain updates with auto triggered roaming use cases setup on contracts through scripts
Billing integration testing	275	Verify reflection of CDRs from clearing house on the billing system (Amdocs)
Functional verification / UI tests	50	Automated tests for front end verification of bills logged to the customers. For E.g. Selenium scripts for web testing

Table 1: Test phases with volumes of tests, methodologies, and tools

- Use cases map

The test plan needs to be verified and validated by business for inclusion of the user scenarios which map to detailed level test cases.

A complete coverage can be ensured only when all the functional validation covers testing across the transactions, i.e., the user moving from the home-based network to the visited or the external network, the blocks, i.e., the CDRs that are transmitted between the network partners and the contracts i.e. the rule allowing the user roaming permissions on a partner network are tested in all the different scenarios that govern the functionality.

- Test execution and result verification

Execution can be ideally automated with scripting following a TDD approach for unit testing on a suitable framework and following a similar approach as outlined in the test plan. The results then need to be consolidated and verified back. A list of defects identified needs to be reported along with the test execution status and conformance. Focus in test execution should be on unit and system tests as a higher level of defects can be detected in the core blockchain adoption in these phases. The integration and functional level tests can then be carried out to verify the integration of the core with the existing framework. However, the rule set for the blockchain needs to be verified within the unit and system testing phases.

A guidance on the test strategy across various test phases is provided below with a call-out on the key activities to be catered to manage within each phase.

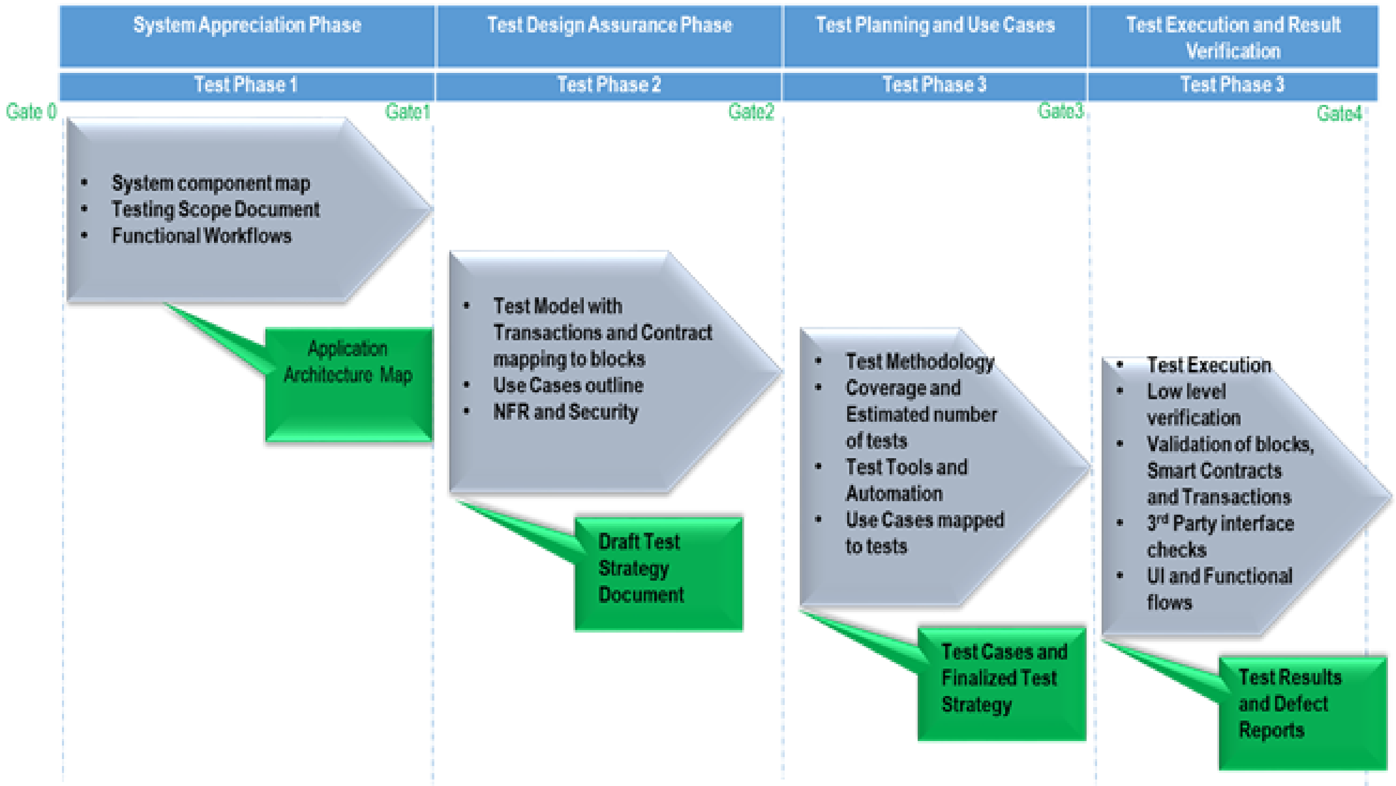

Figure 5: Test strategy across various test phases with a call-out on the key activities

Summary

The key to successfully adopt a blockchain methodology rests in a well-balanced detailed approach to design and validation. While the mechanism of validating and verifying is largely similar to any other system, there is a necessity to focus on specific areas and evolving a test strategy in line with the implementation construct that is applied for the domain.

Infosys Validation Solutions (IVS) as a market leader in quality assurance offers next-generation solutions and services and engages with more than 300 clients globally. With focussed offerings across various domains and segments and with key offering focussed in digital assurance space, Infosys Validation Solutions are committed to deliver high-quality products by adopting newer methodologies and solutions for partnering enterprises across the globe.

For more information, contact askus@infosys.com