17th Annual International
STC 2017
Software Testing Conference
December 07 - 08, 2017
Bangalore
Organised by QAI

Quality Assurance in Blockchain

By **Arpan Sarkar,** Senior Manager – Business Development
&
Jibendu Narayan Mazumder – Associate Director – Business Development

Cognizant Technology Solutions

Cognizant

Abstract

Blockchain is rapidly revolutionizing the way enterprises conduct their business processes. A new paradigm of trustless business transactions is fast evolving that needs no intervention from central regulatory authorities. And, this is made possible with a decentralized peer-to-peer network of nodes, each maintaining a local copy of transaction ledger and mutually synchronizing on a near real-time basis.

The genesis of this Distributed Ledger Technology was in Bitcoin, but gradually others have evolved - Ethereum, Hyperledger, Corda, Monax etc. These have varying features/tech stack, but ensures security / immutability / decentralization to align to trustless model. Based on respective needs, enterprises across industries are choosing from this basket. Be it Document Management or Trade Finance, Blockchain in ubiquitous today.

Quality Assurance in Blockchain needs close examination because of its fundamental difference from Traditional QA. Blockchain QA involves a balanced combination of:

- **White-box Testing –** *Involves testing the core of the framework (e.g. automated unit testing of smart contracts using frameworks like Embark/Truffle/Dapple/Populus)*
- **Grey-box Testing -** *Involves testing integrations between blockchain framework & applications (e.g. API Testing for validating access control, wallet balances etc)*
- **Black-box Testing -** *Involves testing of blockchain application functionalities / business rules (e.g. issuance of cryptocurrencies)*
- **Non-Functional Testing –** *Involves performance and security testing (e.g. validation of performance on pumping large transaction volume into the blockchain network, secured blockchain access, wallet signature etc.)*

Additionally, this paper will also explore areas like Blockchain-as-a-Service, Blockchain Cloud, Blockchain IoT etc.

Overview Of Blockchain

What is it?

Blockchain *is a decentralized ledger of all transactions across a peer-to-peer network. Using this technology, participants can confirm transactions without the need for a central certifying authority. Potential applications include fund transfers, setting trades, voting etc.*

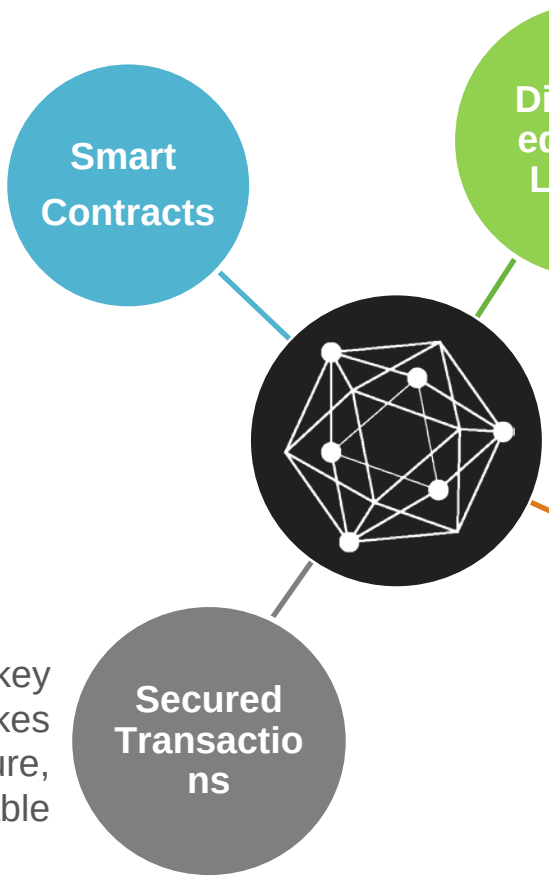
The first blockchain was conceptualized by Satoshi Nakamoto in 2008 and implemented the following year as a core component of the digital currency BITCOIN, where it serves as the public ledger for all transactions

An analysis by Gartner predicts that by 2020, the annual traded volume of electronic currency transactions will exceed 5% of all electronically traded transactions, amounting to **17.9 billion US$**

According to a study by Santander InnoVentures, banks' transactional costs could be reduced by **20 billion US$** using Blockchain technologies.

Key Tenets Of Blockchain

Business logic (rules) embedded in Blockchain that can be triggered when certain conditions are met



Everyone in the network can see the ledger and every node in the network has a synchronized copy of the digital ledger

Private-Public key cryptography makes transactions are secure, authenticated & verifiable

No transaction can be added without consensus from everyone in the network. Special nodes, called Miners, can validate and add a transaction in a block and add to the blockchain

Benefits & Potential Applications

- **Cost Reduction**
- **Increased Transparency and "Third Party" Elimination**
- **Reduced Settlement Time**
- **Secure Transaction Ledger with no double spending or transaction repudiation**

Healthcare

Patients' encrypted health information could be shared with multiple providers without the risk of privacy breaches

Financial Services

Faster, cheaper payments could save billions of dollars from transaction costs while improving transparency

File Storage

Peer to Peer file sharing networks removes the need for centralized databases and heavy storage areas

Voting

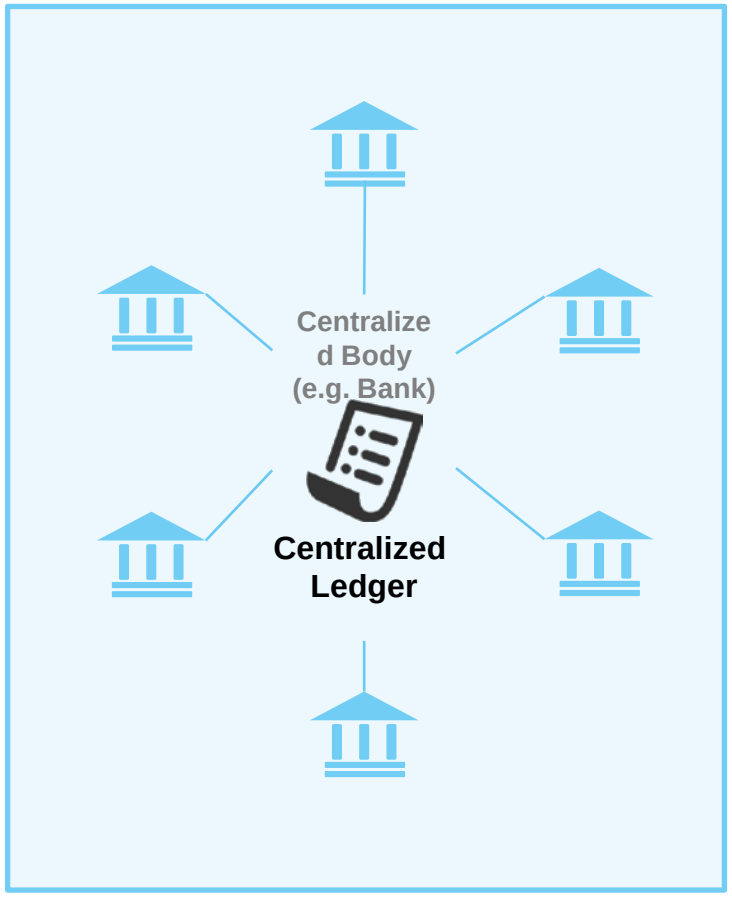
Using a blockchain code constituents could **cast votes** via smartphone, tablet or computer resulting in immediately verifiable results

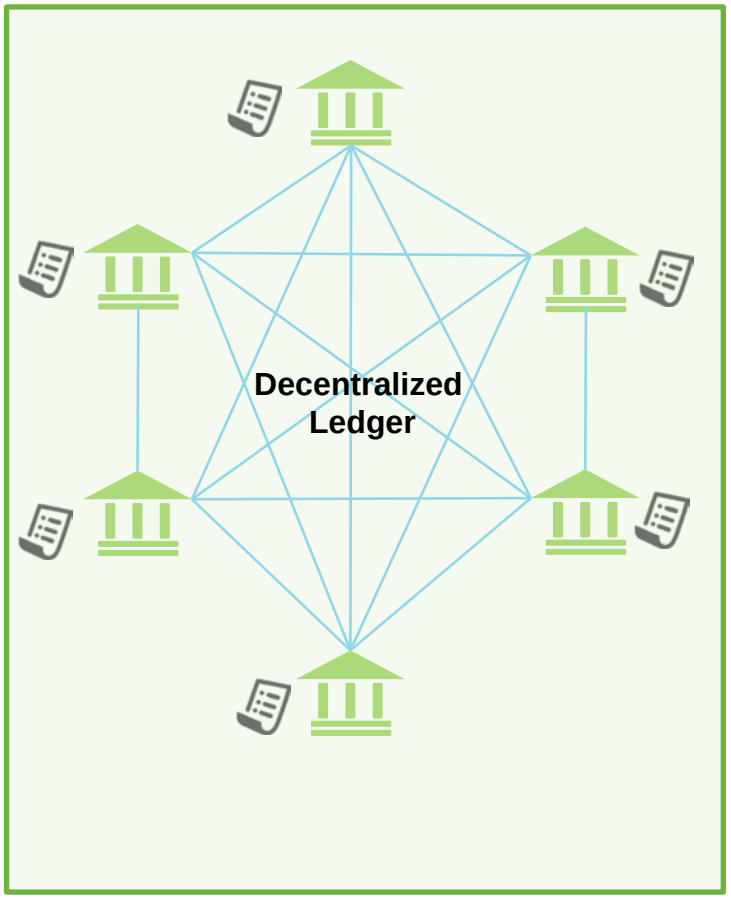
First and Second Generation Blockchains

First Generation Blockchains	Second Generation Blockchains
Blockchains based on cryptocurrencies and asset ownership	*Blockchains based on smart contracts and autonomous decisions*
Example - Bitcoin	**Example - Ethereum**
Public	*Public, Permissioned, Private*

A Deep Dive Into The Key Tenets

Distributed Open Ledger

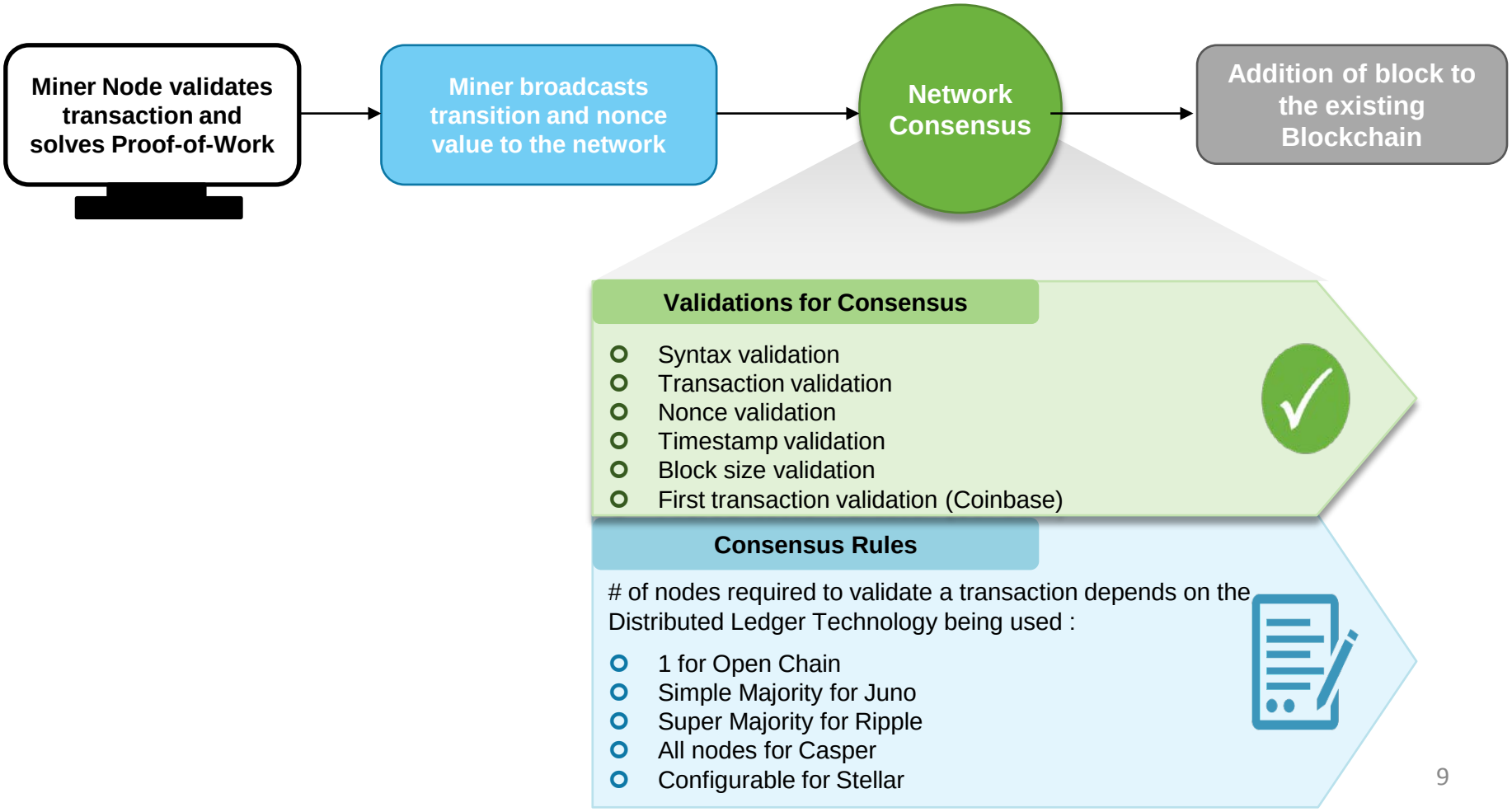




- Every node in the decentralized system has a copy of the ledger (blockchain)
- No centralized "official" copy exists and no user is trusted more than the other
- Transactions are broadcast to network
- Eliminates risk of data stored centrally

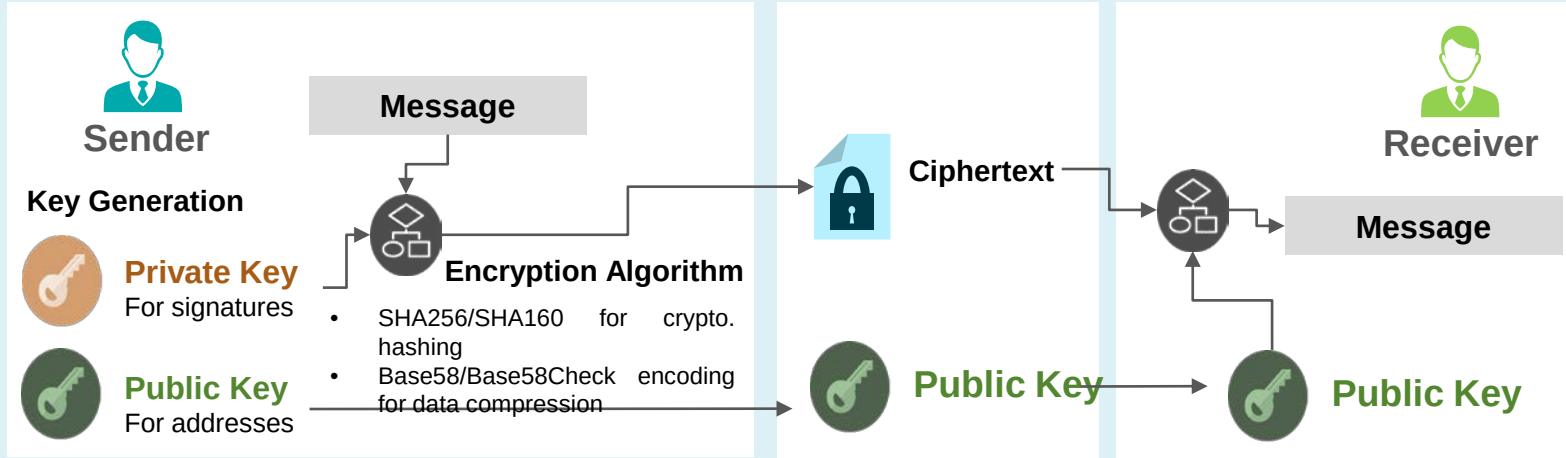
Network Consensus

Consensus Mechanism is central to the functioning of Blockchain – *there is no need to "trust" a central authority*



Secured Transactions

Wallet & Transaction Security



Block # 1

Nonce - 16651

Coinbase - $100 -> Anders
Transactions:

NULL

Prev Txn – 000000….

Hash – 000043D….

Block # 2

Nonce - 37284

Coinbase - $100 -> John

Transactions:

$10 from Anders to Sophie
$5 from John to Sophie

Prev Txn – 000043D….

Hash – 0000A5A….

- Every block identified by hash (SHA 256) value with Coinbase, Transactions, Previous transaction as inputs
- All transactions hashed (Merkle root)
- All these hashes are Base58 encoded
- Nonce is a 32 bit field whose value is set so that hash of a block has run of leading 0s
- Any alteration in any block will make subsequent blocks invalid

Block and Chain Security

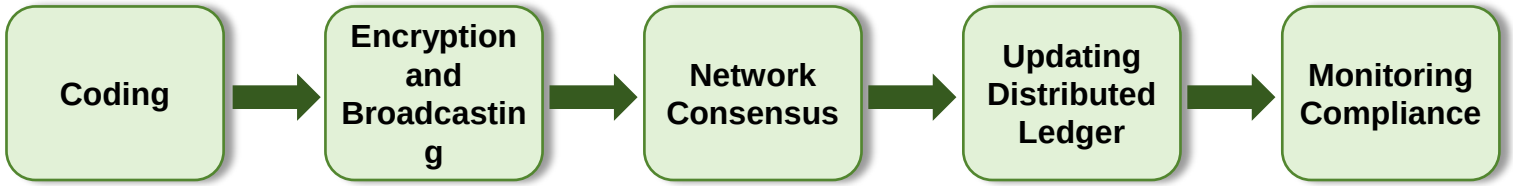
Smart Contracts

What are Smart Contracts ?

A computer program capable of facilitating, executing and enforcing the negotiation or performance of an agreement (contract) using Blockchain; the process is automated and can act as a substitute for legal contacts.

Implication: *Future contracts will be on a hybrid paper-plus- code model where contracts will be verified for authenticity via Blockchain and paper backups will be filed for traditional recourse.*

How They Work

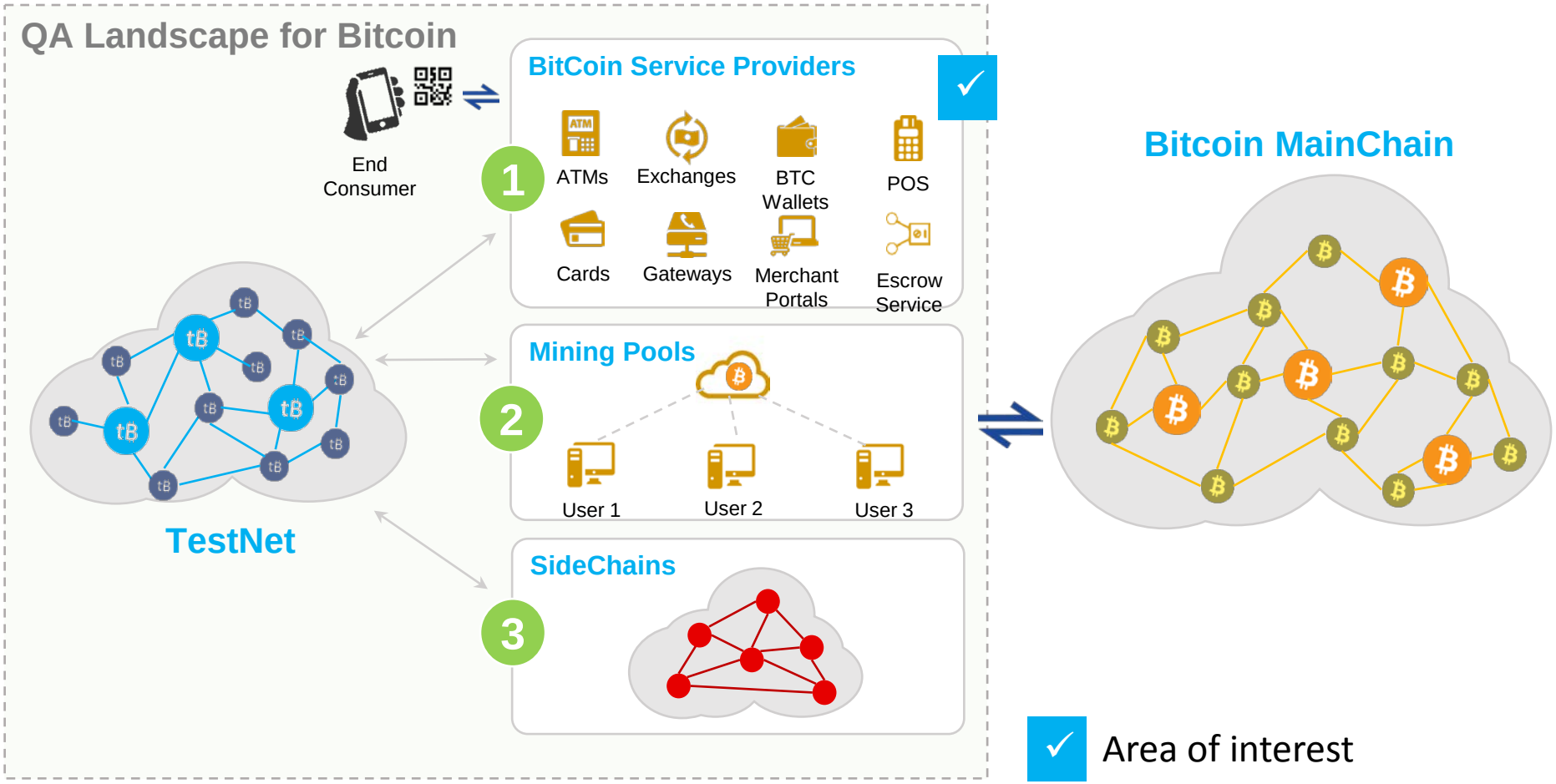


Example

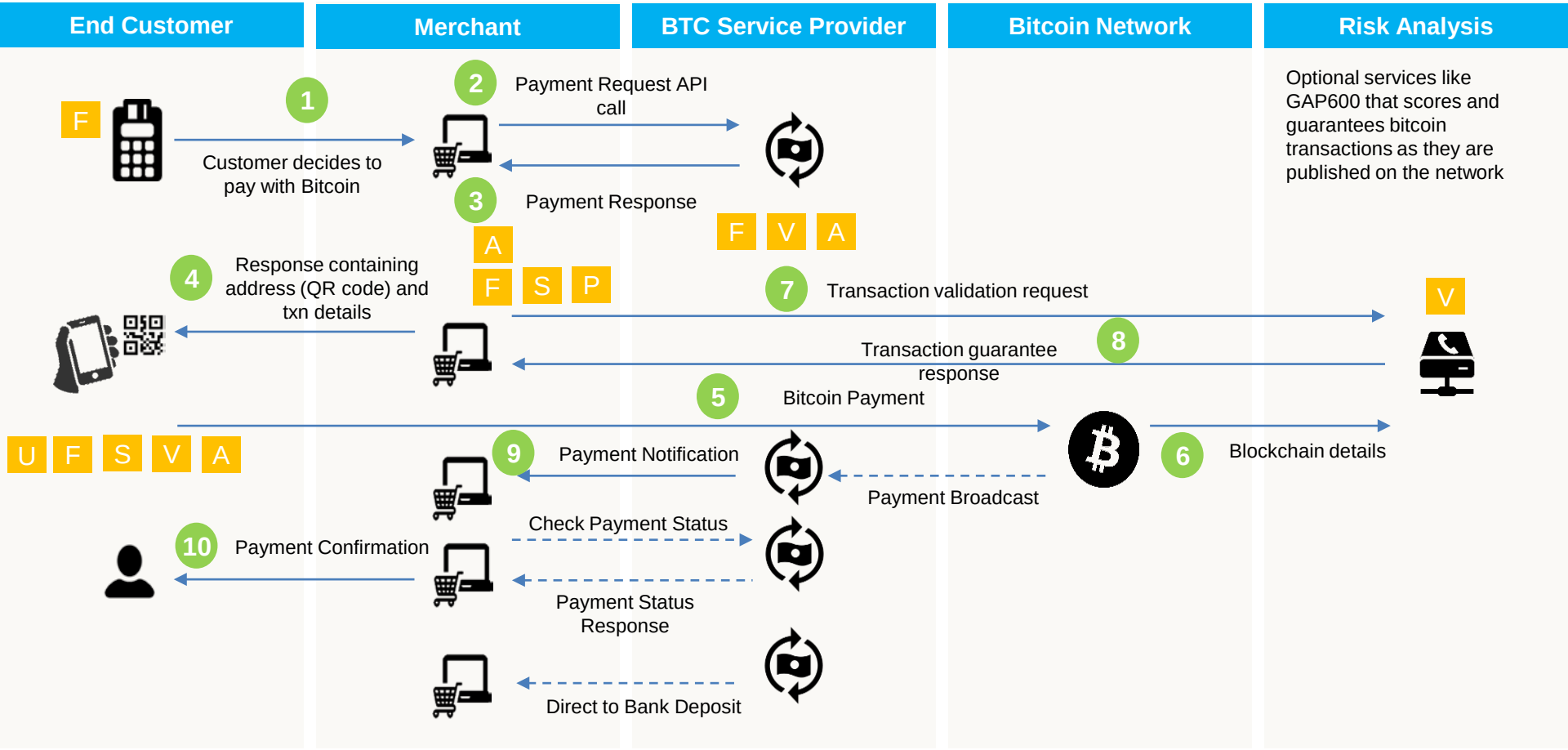
Use of smart contracts in music industry: Tracking ownership rights of music tracks on public Blockchain, real-time apportionment and payment of royalty as per set terms

First Generation Blockchain – Bitcoin

QA Landscape for Bitcoin



QA POV for BTC Service Provider Transactions



U Usability Testing F Functional Testing S Security Testing V Service Virtualization P Performance Testing A Automation Testing Services Testing

Type of Testing for BitCoin Applications

Sl No	Types of Testing	BTC Service Provider	Mining Pools	SideChains
1	*UI testing*	●	○	○
2	*Functional Testing*	●	◑	◕
3	*Validation transaction elements in blockchain console*	●	○	●
4	*Validate request/responses/risk analysis via APIs*	●	○	◑
5	*Performance testing*	◕	○	◑
6	*Security testing*	◕	○	◑
7	*Service virtualization*	◑	○	○
8	*Validate mining reward distribution algorithm*	○	●	○
9	*Validation of consensus protocol*	○	○	●
10	*Validation of two way peg - SPV algorithm*	○	○	●
11	*Device testing*	●	○	○
12	*Automation testing*	●	●	●
13	*Multi-Signature logic testing*	●	○	◕

● High
◕ Medium
◑ Low
○ None

Second Generation Blockchain - Ethereum

Ethereum Overview

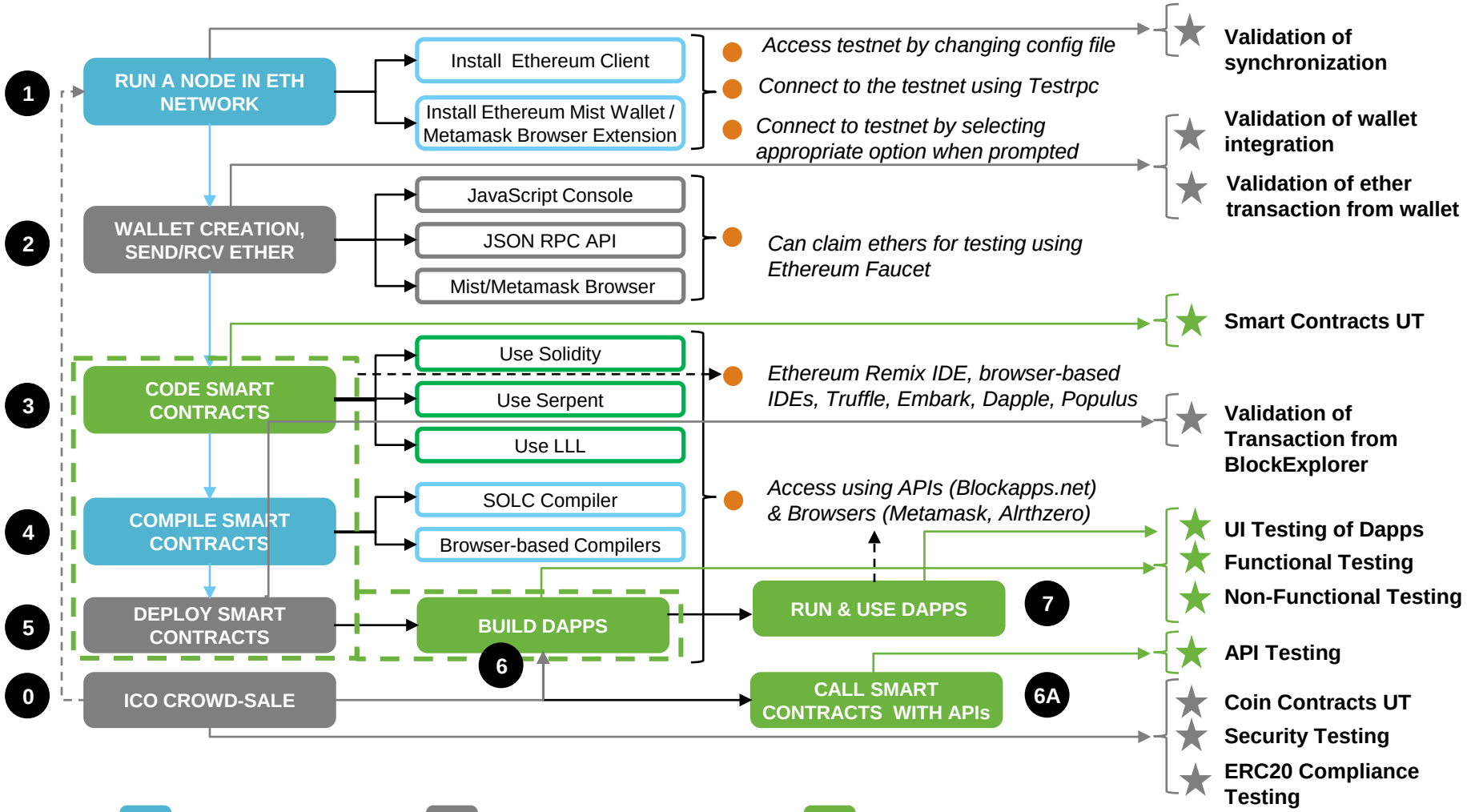
Email : Internet :: Bitcoin : Blockchain → ***2nd Generation Dapps***

Key Tenets

1. **Platform for any application building & hence SCALABLE**
2. **Dapps are JOINTLY OWNED**
3. **Smart Contract based & hence NO CENSORSHIP, DOWNTIME, 3RD PARTY INTERFERENCE**
4. **Based on ETHERS & TOKENS**

ethereum

QA Needs For Dapp Lifecycle



LEGEND No/Low Testing Need | Medium-grade Testing Need | High-grade Testing Need

Ethereum QA POV

Unit Testing of Smart Contracts

- TDD approach using Truffle / Embark / Dapple / Populus
- UT of smart contracts through other contracts

Peer Sync Validation

- Comparing the latest block at the top of stats.ethdev.com with block number output in client node's log

Functional Testing

- Wallet Integration
- Wallet Interface
- Dapp Business Rules
- Dapp Workflows
- Cross-browser/device Testing

Non-Functional Testing

- Performance Testing for txn. throughput validation
- Security Testing – key-based signing & token-based Dapp access
- Usability & Accessibility Testing

Transaction Validation

- Leverage BlockExplorer for
  - ✓ Txn. Validation for receiving/sending ether
  - ✓ Txn. Validation of smart contract deployment
  - ✓ Txn. Validation of token contract

API Testing

- Dapp API calls for internal smart contract methods
- Dapp API calls for interfacing application integration

User Interface Testing

- Validation of UI aspects like colour, logo, resolution, labels etc.
- Validation of navigability aspects

Compliance Testing

- ERC20 guidelines compliance

Blockchain QA Catalogue

Blockchain QA Catalogue

Testing Categories	Bitcoin	Ethereum
White Box Testing	• Unit testing of SPV algorithm for SideChains • Unit testing of incentive distribution algorithm for mining pools • Unit testing of the consensus protocol for SideChains	• Peer synchronization validation • Unit Testing of Smart Contracts (including Token Contracts)
Grey Box Testing	• Validation of the REST APIs and JSON files for calls between wallets, merchant applications, BTC Service Providers and BitCoin network	• Validation of APIs o Dapp API calls for internal smart contract methods o Dapp API calls for interfacing application integration
Black Box Testing	• Transaction validation from Blockchain Console • Wallet integration and interface testing • Device Testing • UI Testing of Bitcoin Wallet • Functional validation of multi-signature escrow services functionality • Integration and interface testing for merchant portals and POS terminals and interfaces • Functional validation of direct to bank deposit feature of BTC service providers and associated exchange rates • Bitcoin ATM and cards testing and associated fees • Functional validation of SPV algorithm • Functional validation of incentive distribution algorithm for mining pools	• Transaction Validation from BlockExplorer • Functional Testing of Dapps o Wallet integration & interface testing o Business rules testing o Workflow testing o Cross-browser/device testing • UI Testing of Dapps • ERC20 compliance validation
Non-Functional Testing	• Usability testing of BTC Wallets and merchant portals • Access controls testing for multi-user wallets • Security testing of transaction message signing and encryption • Performance testing of transaction confirmation speed settings • Service Virtualization	• Usability Testing of Dapps • Accessibility Testing of Dapps • Performance Testing for smart contract transaction throughput validation • Security Testing o Key based wallet access o Token-based Dapp access

Emerging Areas

Emerging Areas In Blockchain

BLOCKCHAIN-AS-A-SERVICE

BLOCKCHAIN

IBM Bluemix™ Microsoft Azure + CONSENSYS + =

RUBIX

ETH BaaS Ethereum Blockchain as a Service

Key QA Needs

- *Functional QA for decentralized applications*
- *Performance / Security Testing*
- *DR/ Failover / Resilience Testing*
- *Inter operability and Integration Testing*

BLOCKCHAIN IoT

chain of things

Gearing Towards →

Smart Contracts +

Smart Devices

Key QA Needs

- *Functional QA for connected devices*
- *Device Interoperability Testing*
- *Network Testing*
- *Security Testing for device authentication, data transmission etc.*
- *IoT Analytics Testing*

Bibliography

1. http://biccur.com/blog/2016/12/16/three-generations-of-blockchain/
2. http://www.oodlestechnologies.com/bitcoin-ebook
3. http://www.oodlestechnologies.com/blogs/Bitcoin-To-Get-More-Anonymous-With-The-New-BIP-Called-Dandelion
4. https://bitcoinj.github.io/testing
5. https://bitpay.com/docs/testing
6. https://bitpay.com/integrations/drupal-commerce
7. https://bitpay.com/integrations/opencart
8. https://blockchain.info/api
9. https://blockchain.info/api/api_receive
10. https://en.bitcoin.it/wiki/Multisignature
11. https://en.wikipedia.org/wiki/Mining_pool
12. https://gendal.me/2014/10/26/a-simple-explanation-of-bitcoin-sidechains/
13. https://medium.com/@BrettNoyes/public-permissioned-and-private-blockchains-3c32965e33c9
14. https://www.blocktrail.com/api
15. https://www.programmableweb.com/news/46-bitcoin-apis-bitstamp-bitcoin-charts-markets-and-50btc/2013/06/11
16. https://www.slideshare.net/Tracxn/tracxn-sector-report-bitcoin-sept-2014
17. https://www.youtube.com/watch?annotation_id=annotation_2972284497&feature=iv&src_vid=vWt9wRZ3Hhk&v=ASCz5uLs5EE
18. https://www.youtube.com/watch?v=5ROp9Ac3UqE
19. https://www.youtube.com/watch?v=LLZNvl90PC0
20. https://www.coindesk.com/price/
21. https://medium.com/@ConsenSys/
22. https://blockgeeks.com
23. https://monax.io/docs/tutorials/solidity/solidity_4_testing_solidity/
24. https://dzone.com/articles/what-blockchain-can-do-for-the-internet-of-things
25. https://letstalkpayments.com/3-companies-leading-the-blockchain-as-a-service-baas-revolution/

Author Biographies

Arpan Sarkar

Senior Manager – Business Development
Cognizant Technology Solutions

Arpan has an industry experience of 10+ years and works with Cognizant as a senior Business Development professional in the Banking and Financial Services (BFS) Quality Engineering and Assurance (QE&A) practice. His gamut of experience ranges from software development to technology consulting, core banking and business development.

Arpan holds a BE degree in Mechanical Engineering from Jadavpur University and an MBA degree from XLRI Jamshedpur. Prior to joining Cognizant, he has worked with other esteemed institutions like Bank of Baroda & Pricewaterhouse Coopers.

Jibendu Narayan Mazumder

Associate Director – Business Development
Cognizant Technology Solutions

Jibendu heads the Business Development group within the Banking and Financial Services (BFS) Quality Engineering and Assurance (QE&A) practice and has around 13 years of industry experience. He specializes in architecting and overseeing implementation of transformational strategies & road maps for large and complex QA programs and has helped several clients achieve their vision of becoming world class QA organizations. Prior to joining Cognizant he worked with companies like PricewaterhouseCoopers and KPMG.

Jibendu holds BE and ME degrees in Electronics and Telecom Engineering from Jadavpur University and an MBA degree from Questrom School of Business, Boston University, USA

Thank You!!!

Q & A