Understanding and Testing Blockchain

John Cvetko

John.Cvetko@Tekasc.com

Abstract

Cryptocurrency, especially Bitcoin has received a lot of attention in the past couple of years. No matter what you think of cryptocurrency, the underlying technology known as blockchain, is finding its way into mainstream enterprise systems. When there is a business need to have distributed, secure and immutable transaction records between various organizations, blockchain is a natural fit. Understandably, the first to see the potential value of this technology has been the financial industry.

Blockchain was originally designed to enable untrusted parties to transact business using cryptocurrency. Instead of using a trusted middleman (like a bank) to complete the transaction, this role was shifted to technology. This, however, came at a cost; it can take several hours or even days to validate a single transaction, in addition to a significant amount of compute power and electricity to operate each node on the network.

But, what if blockchain technology was modified to accommodate different levels of trust and expanded to do more than just transfer cryptocurrency? Blockchain is now being tailored to achieve shorter transaction times, require less power, and provide integrated multi-use flexibility. As the technology is enhanced and shaped to specific markets, more organizations are seeing potential value for their operations.

Blockchain is a paradigm shift in the way we think of traditional networking, application development and deployment. Like all new disruptive technologies, it will require extensive testing, conducted by skilled and agile resources throughout its lifecycle. This paper looks at blockchain from many perspectives and discusses what the testing needs will be over time.

Biography

As a Principal of TEK Associates, Mr. Cvetko works with companies and government agencies to improve their organizations by helping them manage the IT challenges they face. He applies state of the art solutions to evolve business processes, creating more efficiency and productivity, all while maintaining and/or improving quality. In the span of 25 years he has held positions in systems engineering, product and program management and management consulting. The last 12 years have been primarily focused on assessing and implementing large enterprise software systems. He has worked with the state governments of Washington, Oregon, North Carolina, North Dakota, Mississippi, Utah, Kentucky, and Oklahoma. Earlier in his career he worked as a technical consultant for firms such as NIKE and Boeing, and in product development and program management for Tektronix, PGE/Enron and ASCOM.

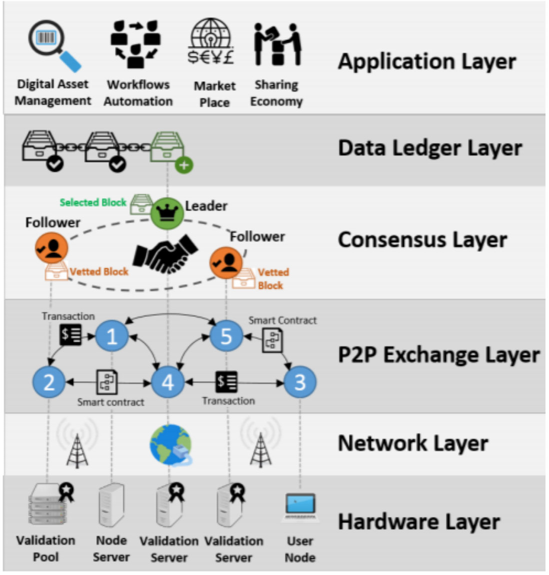
1 Introduction

Many transaction workflows span a series of different companies, often with each company entering the same data into their systems. It is also not uncommon to have several intermediaries in the workflow that impose delays and charge fees for marginal services. Aside from being inefficient, it makes the transaction and all the companies in the workflow vulnerable to compromise by the least secure system in the network. If a centralized system (for example, a bank) is compromised due to fraud, cyberattack, or even a simple mistake, the entire business network can be affected.

Blockchain, also known as distributed ledger technology (DLT), is emerging as more than just a cryptocurrency platform. Its unique characteristics are fostering new ideas in the minds of technologist and business executives alike. The expectations are that it will be a platform consisting of peer-to-peer, consensus and data ledger layers that will usher in a new breed of Distributed Applications (DApps), see figure 1. This combination of technologies will change how commerce is conducted, assets are tracked, products and services are delivered. Moving beyond recording transactions, DLT can track and manage assets. These assets may be tangible (cars, packages, lettuce), or intangible (trade settlements, intellectual property, identity, software).

Because this technology will be evolving for many years, it will have challenges that IT professionals will need to work through to make it a reality. By relying on standard business and engineering practices, these systems will be deployed in a reliable and secure manner. Developing, deploying and testing these systems will require a shift in thinking about traditional networks and applications. This shift in thinking will require new testing strategies, methods, skills and technologies, some of which have yet to be conceived. This paper will discuss the characteristics of DLT, the technology lifecycle, and the potential challenges faced by IT testing professionals throughout this lifecycle.

Figure 1. Blockchain Transactions



Source: Consortium Blockchains: Overview, Applications and Challenges [DIB 2018]

2 Blockchain Fundamentals

The blockchain architecture gives participants the ability to share a ledger, i.e., a permanent transaction record that's updated through peer-to-peer replication and validation. Peer-to-peer replication means that each node in the network acts as both a publisher and a subscriber. A node can receive or send transactions to other nodes, and the data is synchronized across the network as it's transferred. This information is available to all pertinent parties simultaneously, eliminating duplication of effort and reducing the need for intermediaries. It's also less vulnerable because it uses consensus algorithms to validate the information, prior to it being recorded on the blockchain.

A blockchain platform has the following key characteristics:

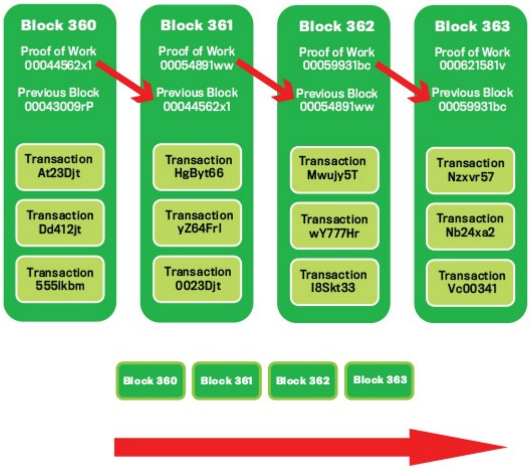
- Consensus: For a block to be appended to the chain, all participants must agree on its validity.
- Provenance: Participants know where the asset came from and how its ownership has changed over time.
- Immutability: No participant can tamper with a transaction after it has been recorded to the ledger. If a transaction is in error, a new transaction must be used to reverse the error, and both transactions are then visible.
- Finality: A single, shared ledger provides one place to go to determine the ownership of an asset or the completion of a transaction.

The Block and Chain

Blockchain owes its name to the way it stores data - in blocks that are linked together to form a chain. As the number of blocks grow, so does the blockchain. Blocks record and confirm the time and sequence of transactions, which are then are appended to the blockchain network, that is governed by rules agreed on by the network participants (consensus). A *transaction* represents an interaction between parties. With cryptocurrencies for example, a transaction represents a transfer of the cryptocurrency between network users. For business-to-business scenarios, a transaction is a way of recording activities occurring on digital or physical assets.

Each block contains a hash (a digital fingerprint), timestamped batches of recent valid transactions, and the hash of the previous block. The previous block hash links the blocks together and prevents any block from being altered or inserted between two existing blocks (see figure 2 below). In this way, each subsequent block strengthens the verification of the previous block, and therefore, the entire blockchain. This method renders the blockchain tamper-evident, lending to the key attribute of immutability. To be clear, while the blockchain contains data, it's not a replacement for databases, messaging technology, transaction processing, or business processes. Instead, the blockchain contains verified proof and security of the data; these benefits extend far beyond those of a traditional database. For example, it removes the possibility of tampering by a malicious actor, e.g., a disgruntled database administrator.

Figure 2. Blockchain



In a blockchain, network participants submit candidate transactions to the blockchain network via software (desktop applications, smartphone applications, digital wallets, web services, etc.). The software sends these transactions to a node or nodes within the blockchain network to create a candidate block.

Each network node will take any number of transactions, validate that they are “legitimate” – and put them into a candidate block. The candidate blocks generated by the participant nodes will vary arbitrarily, due to network latency, or intentionally because of network rules or incentives. So essentially, each node is building their own unique candidate block for presentation to all other nodes on the network. A candidate block is then selected by the network nodes to be appended to the chain based on the consensus method used. [Yaga 2018]

Chaincode

Chaincode, also known as a Smart Contract, is essentially code or business logic that can reside in a block transaction that has been appended to the blockchain. There are two classes of chaincode in blockchain, system and application.

- System chaincode

System chaincode is distinguished as software that defines operating parameters and rules for some or all nodes within the network. For example, a Configuration System Chaincode (CSC) can be utilized to enforce network identity policies, ensuring that all participants meet specific security conditions before their digital signatures are considered valid, thus allowing them to operate on the network.

- Application chaincode

Application chaincode is also known as user chaincode and is used to execute business logic when a specific condition is valid. Application chaincode incorporates business logic with metadata about its function, including the name, version, and counterparty signatures required to ensure the integrity of the code. Additionally, application chaincode can't be invoked directly by other chaincode on the blockchain; however, it can be queried.

Application chaincode can be as simple as a data update, or as complex as executing a business contract with conditions attached. For example, a contract can be written between two parties on the network that stipulates the terms and cost of shipping an item based on the desired delivery date and mode of transport. When this information is agreed on by both parties, it is permanently written to the blockchain, and when the item is received by the purchaser, the appropriate funds can then be automatically sent to the supplier. [Hyperledger VII 2018]

3 Consensus Models

Consensus is a central component of the blockchain technology. Without a trusted, central intermediary, the network of participating users that implement the decentralized system need to agree on the validity of what's being added to the chain. Consensus algorithms are used to validate that the block of transactions meets the requirements set forth by the network participants to append blocks to the chain.

There are a variety of consensus protocols that can be deployed and are dependent on the requirements of the participants. International standards' organizations are working towards defining standards for consensus protocols; this will allow product vendors the ability to implement whichever consensus mechanism is deemed best for the system in which it is deployed, and, in a more modular fashion. [Hyperledger VI 2017] [Morris 2019]

A consensus protocol has three main characteristics that determine its use in the network design.

- **Security**

  A consensus protocol is defined to be safe if enough nodes offer the same valid outputs as the algorithm dictates. This is also known as "consistency of the shared state".

- **Real-time**

  A consensus protocol requires a sufficient number of nodes participating in real-time to provide consensus that a candidate block is valid.

- **Participants**

  A consensus protocol operates best in environments where there is a large number of diverse participants…the more, the better. This ensures network "fault tolerance".

Balancing all the elements above is challenging, and each consensus protocol has characteristics that emphasize specific elements for the environments in which they are deployed. For example, public cryptocurrencies may focus more on security than on the time it takes to validate a block.

There are many different consensus mechanisms and only a few are discussed here.

Proof of Work

Proof of work (PoW) is a network consensus protocol utilized most notably by Bitcoin. This protocol is not desirable for general business use due to its significant operational costs. The proof of work comes in the form of an answer to a mathematical problem, one that requires considerable work to arrive at, but is easily verified to be correct once the answer has been found.

The problem to be solved is that the node must generate a block hash number that is below the "target hash" set in the network, in order to be selected to append their candidate block to the chain.

A target hash is generated as part of the PoW algorithm. Each node calculates this based on the level of desired difficulty. The target hash is continually adjusted and updated by the network nodes to keep the work needed to a specific range. For the Bitcoin blockchain this target was originally set so that it would take 10 minutes to solve the problem.

The only way to solve this problem is by the nodes on the network running a long and random process of generating block hashes, for the candidate block, on a trial and error basis. The result of the original hash function on the block is completely unpredictable, so there is no control over what the initial block hash value will be. To change the initial block hash value, the node will vary one specific value in the block header known as a nonce. The nonce will be changed, and the block contents will be rehashed until a block hash is found that is below the network target hash. The node that manages to solve the problem the quickest wins the right to append their candidate block to the chain. [De Angelis 2018]

Proof of Elapsed Time (PoET)

This concept was first introduced by Intel through the HyperLedger consortium and is considered a "lottery" protocol. The PoET consensus mechanism was developed specifically for Internet of Things (IoT) applications. This protocol is highly efficient and capable of scaling to thousands of nodes. The key element enabling the PoET model relies on Intel's Software Guard Extension (SGX) technology, currently available in some Intel CPUs. SGX is considered a Trusted Execution Environment (TEE) within the CPU that ensures that the code executing within the TEE cannot be tampered with by external software.

The PoET model relies on randomly distributing the "leader" (block publisher) election among all available participating nodes. This randomness is a secure way for other nodes to verify that a given leader was correctly selected, i.e., without any manipulation.

In each round of the lottery, network nodes receive a signed, randomized timer object from the TEE code within their CPU's. Each node subsequently waits for their randomized timer to expire. The node's timer that is the first to expire propagates a signed certificate to the network indicating that they are the block leader for that round. The message is authenticated by other nodes in the network, and the block is appended to the chain. Once the block is appended to the chain the next network lottery round begins.

When a node wins the lottery and is determined the leader, other nodes can easily verify the nodes authenticity because the leader will produce a signed attestation from their TEE that provides proof that the code has been correctly initialized in a trusted environment. [Cachin 2017]

While PoET is highly efficient and not nearly as resource intensive as Proof of Work systems, the technology is not without its critics. The main concerns are that a single vendor would control the underlying technology (the CPU), and if a security vulnerability was detected, it would be very difficult to correct it at scale.

Proof of Authority

This protocol does not depend on nodes solving arbitrarily difficult mathematical problems or a lottery, but instead uses a specific set of "authority" or "validator" nodes in the network. These are nodes that are explicitly allowed to approve candidate blocks produced by non-authority nodes. The proposed block must be validated and approved by a majority of authorities to be appended to the chain. This approach can be utilized by a private chain (internal network) to keep the block issuers accountable.

With PoA, security is maintained by earning the right to become and remain a validating node, so there is an incentive to retain the position that has been achieved. By attaching a "reputation" to the node's identity, validator nodes are incentivized to uphold the transaction process by gaining and maintaining trust over time. If a node produces the wrong validation of a block, or does not act as expected, its reputation suffers, and the node is no longer trusted with the authority role.

Practical Byzantine Fault Tolerance

The Practical Byzantine Fault Tolerance (pBFT) model primarily focuses on providing a practical Byzantine state machine that tolerates faults or malicious nodes. The algorithm is designed from the perspective that there are node failures and/or compromised nodes in the network acting maliciously.

Essentially, all the nodes in the pBFT model are ordered in a sequence with one node being the primary node (leader) and the others referred to as the backup nodes. In this method, all the nodes participate in the voting process and consensus is reached when more than two-thirds of all nodes agree that the candidate block is valid. pBFT can tolerate malicious behavior from up to one-third of all nodes to perform normally. For instance, in a system with 1 malicious node, there should be at least 4 nodes to reach a correct consensus. Once a majority of the nodes agree, the leader appends the block to the chain. In this method, consensus is reached quicker and more economically compared to a number of other consensus models.

PBFT has high throughput, low latency, and low computational requirements – all of which are desirable for IoT networks. However, its high network overhead limits scalability, thus, it would likely be applied to only small IoT networks.

4 Blockchain System Classifications

A public blockchain's most native environment is where there is no central authority and no point of trust between participants on a network…this is the most challenging environment for any system. To accomplish this task, the system uses raw compute power and complex algorithms to establish a high degree of trust among network participants. Trust through technology, while an impressive feat of engineering, increases the cost of deployments to a point that it is not feasible for the average private or hybrid (public/private) environment.

In general, all blockchain systems are constrained by three main properties: (a) decentralization, (b) scalability and (c) security. This is referred to as the "trilemma" of elements that need to be balanced to ensure an optimum design is employed for its intended purpose. [Qin 2018] Each class of blockchain discussed below will struggle to find the needed balance for its intended purpose. For example, a small ecosystem of 100 private companies may need a global decentralized and secure system that doesn't need to scale beyond this size for many years. On the other end of the spectrum, you may have a single company that tracks many IoT devices and may value scalability and decentralization over security. These lopsided trilemma deployments will drive new methods and technologies to satisfy consumer needs, e.g., Intel's PoET consensus model.

At a high level, there are two main classes of blockchains - permissionless and permissioned. The needs of these classes vary greatly and will undoubtedly expand the current limits of the trilemma.

Permissionless

Permissionless blockchains are considered public, which means that anyone can join and use it for the intended purpose. Permissionless blockchains are designed and operate with the perspective that their environment is hostile. These systems require the use of crypto-techniques, and robust consensus models to protect against malicious actor's intent on exploiting or breaching the system.

Companies that provide services to the public will have monetary transactions and or sensitive information as part of their exchange with (B2C), and between, their consumers (C2C). These systems will require scalable, cost-efficient consensus methods to make their business models viable. [Qin 2018]

Permissioned

In permissioned blockchains, participants are more trusted, and the use of on-chain and off-chain authentication mechanisms are tolerated. These systems operate in a limited decentralized environment and have rules and policies that participants will adhere to for the right to use the network. To ensure compliance to these rules and policies, independent auditors are employed to review, validate and attest to the transactions on the blockchain. There are two sub-classes of permissioned blockchain, consortium and private networks.

- **Consortium**

Consortium networks have different companies operate in a specific context on a network, e.g., a manufacturer, transport company and a raw material supplier. Participant nodes are incentivized to behave honestly, because, if misbehavior is detected they may have their network privileges curtailed or even revoked.

An example of two independent companies formed by a consortium are Vakt and Komgo SA. These organizations will work in tandem to build a commodity exchange and settlement platform for oil companies, trading firms, banks and goods inspection companies. The companies associated with Vakt will handle the contract and terms processing and the companies associated with Komogo will act as the financial settlement arm of the exchange. This platform will be essential for the member companies to efficiently transact business in the future. [Rathod 2019]

- **Private**

Private blockchains are where participants are known, and access is extremely limited, to either internal operations or among a select few companies. In this scenario, there are a predetermined set of nodes that participate in the network and they operate in a very limited decentralized environment. This use of blockchain would likely be for large organizations that have the need to permanently record information between divisions or trusted partner companies. For example, BNP is an international banking firm that conducted a private blockchain trial to determine if it could be utilized by their Asset Liability and Management (ALM) Treasury department. The trial was used to determine blockchain's feasibility for improving existing internal processes and providing immutable records between different business units on an international level. [Sundararajan 2017]

5 Centralized and Decentralized Applications

Blockchain, in-and-of-itself, isn't very useful if applications can't leverage the technology. When organizations design blockchain networks they will have two application options. They can continue to use legacy applications, or they can deploy new Decentralized Applications (DApps).

Legacy Applications

Existing application vendors will look to adapt their legacy, (centralized products) to work with blockchain. Integration to legacy applications is done through connectors called "oracles". Oracles provide a method for legacy applications to quickly adapt to decentralization by enabling them to leverage whichever blockchain architectures emerge as the dominate approach within their target vertical market. Another approach that can be taken by an application vendor, is to integrate blockchain into their existing products to provide a packaged solution, e.g., SAP's Leonardo technologies.

Decentralized Applications

In addition to the legacy application vendors, there will be many new companies that will develop enterprise decentralized applications (DApps), exclusively from a decentralized perspective. DApps not only communicate with the underlying blockchain, but can also manage the state of network actors.

A good example of a DApp for supply chain management, is being developed by four Chinese entities, Xiamen, Innov, Corelink, and VeChain. Their intent is to integrate a DApp, blockchain, IoT (RFID), artificial intelligence and cloud technologies to track physical assets and inventories as they are being shipped and stored. [Nugent 2018] Supply chain management involves multiple stakeholders operating in a coordinated effort, often resulting in a complex workflow. There are multiple levels of suppliers, manufacturers, service providers, distributors, and retailers that make recordkeeping and communications inefficient. The integration of DApps, IoT and chaincode can simplify the process by coordinating sensory data, documentation, and transparency to regulations.

For example, a participating manufacturing company would utilize a DApp to order, pay and monitor a shipment of raw material to a factory. If the shipment was delayed, it would be detected by the RFID component of the system, which would relay the information to the chaincode and ultimately the DApp. Using Artificial Intelligence, the DApp may determine the delay is out of acceptable limits for the factory and initiate an order on a commodity exchange for new material from another vendor. The new supplier agrees to fulfill the order and the contract would be recorded in the blockchain. Once the new material is received and verified by the factory, the DApp then communicates this information to the chaincode, which releases payment to the supplier via the same blockchain network. In this case, numerous emails, telephone communications and intermediaries are replaced by a highly integrated network.

6 When Does Blockchain Make Sense?

Because there are countless news articles and videos describing the “magic” of blockchain, it is important to understand the limitations of the technology to balance expectations. The current hype around the use of blockchain is much greater than the understanding of it, and as with all new technology, there is a tendency to want to apply it to every sector in every way imaginable. [Wüst 2017]

If cost and return on investment are satisfactory for the business case, then from a functional perspective, considering blockchain as a solution today makes sense when:

- No single participant requires sole authority to write data to the blockchain.
- Immutability of the data is necessary.
- A high degree of data security and redundancy is needed.
- All participants have the same incentives to participate.
- All participants require data transparency.
- The transaction speed is not a paramount concern for the participants.

But the list above is only relative to a point-in-time in the Technology Adoption Lifecycle (TAL) (see figure 3 below). This lifecycle represents the adoption of the technology by consumers over time, and as the technology matures, the deployment guidance will change with it.

The adoption lifecycle is a descriptive framework that classifies the adoption of technologies into five consumer phases: innovators, early adopters, early majority, late majority and laggards. These phases overlap and are subject to market forces, technology innovations and business advances that can affect the speed of adoption. [Moore 1991] The first three stages of the Technology Adaption Lifecycle will be the most dynamic and challenging for consumers and are further discussed below.

- Innovators seek out novel technology. They experiment, demonstrate, conduct pilot deployments, develop business cases, cost analysis, etc., to investigate the feasibility of use. These companies are keenly aware that failure to identify technical issues and real costs before investing are the main causes for significant schedule delays and (potentially) project failure. As these consumers review the feasibility of the technology, they also assess high risk areas that will need to mature in order to reach their desired business goals. They develop a close relationship with their vendors and often will shape the vendor's short-term product roadmap.

  Non-technical challenges are addressed during this phase as well, e.g., how decentralized governance models, business relationships and legal liabilities need to be handled between participating entities. [Hogan Lovells 2016] [Zetzsche 2018] Even in this high-risk environment companies forge ahead, often because they are in hyper competitive markets or have needs that are not satisfied by existing technologies.

- Early adopters stand on the shoulders of the innovators. The failures and successes of the innovators are found through published case studies, total cost of ownership models and more viable products available in the market.

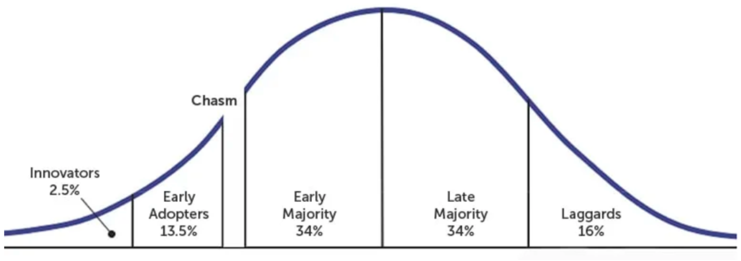
  The innovators have reduced the risk of failure for the early adopters by paving the way through fundamental technology and business barriers. For early adopters, the viability risk has been diminished and their concern turns to selecting the system that will become the "dominate design" over time…the BETA vs. VHS risk. [Kwong 2019] This risk is difficult to mitigate because many factors are out of the control of the consumer. The main risk mitigation technique is to limit the size and scope of deployments to non-core areas of the business.

- If the technology enters the Early Majority phase, it has "crossed the chasm," and the stage is now set for rapid deployment growth (see figure 3). [Moore 1991] Dominate designs and standards coalesce and begin to drive interoperability among product vendors, further reducing risk and driving down prices. Early Majority consumers are practical, and if a product provides obvious value with tolerable risk, they will use it.

DApps will also follow the same adoption lifecycle but will have a "chicken and egg" relationship with independent blockchain vendors. As DApp vendors create and deliver more features that can be utilized by the business, the underlying blockchain deployment may not be efficient or powerful enough to deliver the desired services. DApp vendors may vertically integrate by incorporating a desired blockchain as part of their solution, or partner with blockchain vendors to present a coordinated solution to their clients.

As the technology matures and finds its way towards industry vertical dominant designs, the "when does blockchain make sense" list (mentioned above), will also evolve and be tailored to specific industry applications.

Figure 3. Technology Adoption Lifecycle



Source: Crossing the Chasm [Moore 1991]

7 Technology Adoption Lifecycle and Testing Lifecycle

The technology adoption lifecycle has a direct relationship to the quality assurance skillsets, testing strategies and tools needed to ensure that stable and secure systems are put into production. In general, when testing tools and strategies are immature then the testing staff knowledge, judgement and skillsets will be highly leveraged. As the testing tools and strategies mature the reliance on tester skillsets are greatly reduced. As mentioned above, the first three stages of the adoption lifecycle will be the most dynamic and challenging and will require QA teams to be agile.

- **Innovator Phase:** The innovator phase is primarily used by consumers to learn and evaluate new technology. It is marked by consumer demonstrations and trials that are often intense and run for short periods of time. System requirements at this stage will be fluid as consumers struggle to understand the technology and its application in their environment, i.e., they don't know what they don't know on a variety of fronts. As consumers refine their requirements and developers adjust and readjust their design approaches, testing is heavily focused on basic operation and stability.

  This stage of the lifecycle will require highly skilled testers that can move across many domains and at a deep level. These individuals will be adept at programming, have a sound understanding of system engineering and will be working side by side with the system developers, designers, and client technical staff. This is sometimes referred to as "shifting left," but shifting left in this context is not done to increase productivity, quality, etc., but rather out of basic necessity.

  Testing tools at this stage are usually "home-grown", minimal and not deployed for simulating large system loads or precision regression testing, but rather, they'll be used as coarse monitors and simulators for working through specific development problems.

- **Early Adopter Phase:** In this phase, product vendors will seek out "friendly" consumers that believe their products and long-term vision will be the dominate design or product in their specific industry. The systems will be deployed into limited production environments and will have constant system refinements. The pre-deployment testing periods will be much longer and will be conducted in close collaboration with other participants using the system. System testing will focus on the elements of the trilemma most applicable to the network deployment objectives.

  The network products will come with more internal monitoring capabilities allowing testers to validate and monitor many system elements during testing. Product vendors will support these consumers with a high degree of attention due to the immaturity of their products and the semi-custom nature of each deployment.

  QA teams will begin to segment and specialize in core system areas, i.e., the DApp or the blockchain. These segmented teams will further specialize between new feature testers and regression testers. New feature or core system changes will require testers with a high degree of system knowledge to develop increasingly nuanced tests that may be heavily instrumented.

  In decentralized deployments, there may be many companies, sometimes competitive, simultaneously testing a release for deployment. [ACT-IAC 2017] This will require a high degree of coordination and be conducted by cross company teams or independent firms, i.e., consortiums.

  Permissioned system deployments will have an inherent need for independent, continuous security and accounting audits. These audits will focus on processes, products, software releases and system operations. [Smith 2018] [Jefferson 2019] Consortium participants will require testing teams to leverage these tools for assurance that the appropriate battery of standardized audit tests will be conducted for all releases.

- **Early Majority Phase:** In this phase there will be tremendous growth in system deployments by consumers that need to keep pace with their competitors. These consumers will look to deploy products that conform to technology standards when they can, even at a premium. These premiums can be justified by ensuring that when these systems are built, participants can deploy any vendor product they prefer to use on the chain. This modularity will be further driven by consumers needing products that can be easily configured by technicians and that best suit the multiple needs of business and enterprise roadmaps.

  Consumers will expect to find sufficient IT resources to execute their business strategies. This will create more demand for skilled, specialized resources to work in the decentralized networking field. Quality assurance strategies and processes will be mature at this point and the focus will be on finding greater efficiencies through the utilization of independent testing tools that are geared more towards non-developers.

8 Conclusion

As decentralized systems are introduced, companies will need quality assurance teams comprised of highly skilled testers to ensure these systems meet the desired quality expectations. This paper provided an overview of the technology and its lifecycle as it relates to quality assurance.

The pace of decentralized system adoption will be slow at first, and there will many setbacks and retrenching. Any estimate as to the time required for significant adoption by consumers is foolhardy, at best. However, understanding some of the high-level challenges will help to stimulate awareness and discussion among QA professionals early in the process. Hopefully, QA teams will document their decentralized testing experiences for public consumption and inclusion into the QA body of knowledge.

There are many additional aspects of blockchain and DApps that are not addressed in this introductory paper, e.g., specific industry case studies, Blockchain as a Service (BaaS), side chains, etc. These topics will be addressed by the author in future work.

Acknowledgement

The author would like to thank Dima Itkis, David E. Burgess and Tom Kapusta for their insight and constructive comments.

References

[DIB 2018] Dib, O., et. al., “Consortium Blockchains: Overview, Applications and Challenges” International Journal on Advances in Telecommunications, vol 11 no 1 & 2, year 2018, http://www.iariajournals.org/telecommunications/

[Yaga 2018] Yaga, D., Mell, P., Roby, N., Scarfone, K., “Blockchain Technology Overview,” National Institute of Standards and Technology Internal Report 8202, October 2018

[Hyperledger VII 2018] Hyperledger Architecture Workgroup Volume II, Smart Contracts, Linux Foundation, 2018. Available: Hyperledger Architecture VII

[Hyperledger V1 2017] Hyperledger Architecture Workgroup Volume II, “Introduction to Hyperledger Business Blockchain Design Philosophy and Consensus,” Linux Foundation 2017 Available: https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf

[Morris 2019] Morris, N., 2019, “ISO Blockchain Standards Planned for 2021,” Ledger Insights, June 2019 Available: https://www.ledgerinsights.com/iso-blockchain-standards/

[De Angelis 2018] De Angelis, D., 2018, “Assessing Security and Performances of Consensus Algorithms for Permissioned Blockchains,” Rome, Sapienza University.

[Cachin 2017] Cachin, C., Vukoli´c, M., Whitepaper “Blockchain Consensus Protocols in the Wild,” 2017, Zurich, IBM Research

[Qin 2018] Qin, K., Gervis, A., 2018, “An overview of blockchain scalability, interoperability and sustainability,” Imperial College London

[Rathod 2019] Rathod, A., 2019, “Oil Giants BP and Shell Launch Oil-Trading Blockchain Platform,” Toshi Times, January. Available: https://toshitimes.com/oil-giants-launch-oil-trading-blockchain-platform/

[Sundararajan 2017] Sundararajan, S., “BNP, EY Complete Blockchain Trial for Internal Treasury Operations” CoinDesk, October 17th. Available: https://www.coindesk.com/bnp-ey-complete-blockchain-trial-for-internal-treasury-operations

[Nugent 2018] Nugent, D., 2018, “Smart Corelink Joins VeChain’s Strategic Partnership with Xiamen Innov” Cointrust, April 14th. https://www.cointrust.com/news/smart-corelink-joins-vechains-strategic-partnership-with-xiamen-innov

[Wüst 2017] Wüst, K., Gervais, A.,2017,” Do you need a Blockchain?” 1st Crypto Valley Conference on Blockchain Technology. Available: https://eprint.iacr.org/2017/375

[Moore 1991] Moore, G.A. Crossing the Chasm, Harper Business, New York, 1991.

[Hogan Lovells 2016] Hogan Lovells 2016, “Blockchain Bites... twenty key legal issues to navigate,” Hogan Lovells Blockchain Blog, June 7th https://www.hoganlovells.com/en/blogs/blockchain-blog/blockchain-bites-twenty-key-legal-issues-to-navigate

[Zetzsche 2018] Zetzsche, D., Buckley, R., Arner, D., The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain,” University of Illinois Law Review Vol. 2018 p. 1362 – 1407 Available: https://illinoislawreview.org/wp-content/uploads/2018/10/BuckleyEtAl.pdf

[Kwong 2019] Kwong, Y., Lew, P., McDowell, J., 2019 “Software Based Disruptive Change Initiatives Require a Culture of Quality,” Excerpt from PNSQC 2019 Proceedings.

[ACT-IAC 2017] 2017 “Enabling Blockchain Innovation in the Federal Government,” American Council for Technology – Industry Advisory Council October 16, 2017

[Smith 2018] Smith, M., 2018 “The blockchain challenge nobody is talking about.” Price Waterhouse Coopers blog, March 15th. http://usblogs.pwc.com/emerging-technology/the-blockchain-challenge/

[Jefferson 2019] Jefferson, D., et. al., 2019, “What We Don’t Know About the Voatz “Blockchain” Internet Voting System,” https://cse.sc.edu/~buell/blockchain-papers/documents/WhatWeDontKnowAbouttheVoatz_Blockchain_.pdf

Unknown
Field Code Changed

Unknown
Field Code Changed