2018 3rd International Conference for Convergence in Technology (I2CT)
The Gateway Hotel, XION Complex, Wakad Road, Pune, India. Apr 06-08, 2018

Blockchain Oriented Software Testing - Challenges and Approaches

Rohan Koul
Quality Associate
Suite Test Engineering
SAP Labs India Pvt. Ltd.
Gurgaon, Haryana-122002, India
rohan.koul@sap.com

***Abstract*—The distributed ledger technology presents a very innovative and secure way of managing transactions online. Hailed as one of the greatest inventions after the Internet, blockchain is set to pioneer changes in the way businesses are conducted today through its promise of secure, tamper-proof, peer-to-peer decentralized networks with distributed consensus. These fundamental features built into the very fabric bring in a host of additional dimensions and present greater challenges in their testing. Not only are the technological changes significant, but also significant are changes from a business standpoint. A new wave of blockchain oriented software development is emerging at an unprecedented rate. This places an additional responsibility on the Quality Assurance teams to deliver first-time quality while minimizing the impact of testing on the teams delivery. This paper highlights the challenges currently faced in testing such applications. It also acknowledges the need to devise specialized tools and techniques for blockchain oriented software testing in order to ensure high standards of quality.**

***Index Terms*—Blockchain, Bitcoin, BaaS, Ethereum, Software Testing**

I. Introduction

Digital transactions are gaining popularity globally and the volume is growing at an exponential rate. With improved security mechanism, ease of use and faster way of managing transactions the phenomenon is predicted to grow at an even higher rate in the next decade as well. As a vast majority of people are shifting towards digital transactions, security becomes a major concern for everyone. Blockchain provides users with a safe and secure way of managing their transactions online. It creates an environment of trust without the need of any external middle parties. The emerging concepts of blockchain and Smart Contracts have garnered a lot of attention in the last few years. Many organizations including financial institutions and regulatory bodies are explicitly investing their capital and time into this technology.

Blockchain is a distributed ledger which is shared, replicated and synchronized among the members of a public or private peer-to-peer network. Distributed to all the members in the network, the ledger permanently records the history of asset exchanges amongst the members of the network in a linear and chronological order. Every transaction recorded in the ledger has a timestamp and unique cryptographic signature associated with it. All the participating nodes in the network agree on a common consensus protocol to verify and update records in the shared ledger and hence eliminate the need of relying on a third party such as a financial institution to mediate transactions. Once the information gets stored in the blockchain, it cannot be changed or tampered. All the confirmed and verified transactions are combined together into a block and chained to the most current block to form a blockchain. Blockchain presents infinite possibilities to change the way transactions are managed in the digital world.

The blockchain technology presents a completely new approach to software development. The decentralized nature along with the anonymous nature of the nodes involved further adds to the complexity of the testing process. The traditional methods of software testing may not be valid anymore. The immutable nature of the blockchain further implies that if a bug goes into the production system, it may require complete revision of the code. Thus, using correct testing techniques and methodologies becomes more critical in this case. This paper aims at identifying the challenges faced and the approaches that can be followed for blockchain oriented software testing to ensure high standards of quality.

The rest of paper is organized as under: Section II presents a detailed survey regarding the emergence of blockchain based applications. In Section III we take a look at Smart Contracts. Section IV introduces Blockchain as a Service (BaaS). Section V identifies some challenges involved in testing and Section VI talks about approaches that can be followed for testing blockchain based applications. Section VII reports the conclusion.

II. Literature Survey

In 2008 an anonymous person under the alias Satoshi Nakamoto published a paper on Bitcoin: A Peer to Peer Electronic Cash System[1]. In this paper, he argued that he had solved the double-spend problem for digital currency via a distributed database that combined cryptography, game theory, and computer science. As this cryptographic currency started gaining momentum, it became clear that actual driving force behind Bitcoin was an ingenious technology called blockchain. Bitcoin was the first killer app of the blockchain,

978-1-5386-4273-3/18/$31.00 ©2018 IEEE

as email was to the Internet.

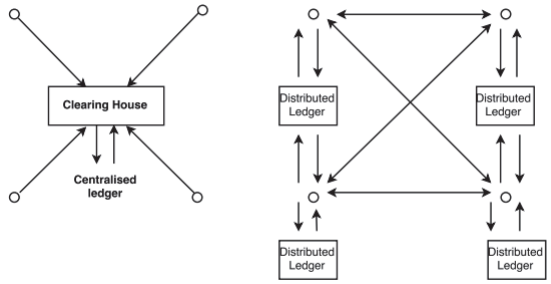

Fig. 1. Centralised Ledger vs Distributed Ledger.

In their famous book Blockchain Revolution, the authors Don Tapscott and Alex Tapscott quote ”The first generation brought us the internet of information. The second generation, powered by blockchain, is bringing us the internet of value, a new, distributed platform that can help us reshape the world of business and transform the old order of human affairs for the better[2]”. Bitcoin has had a roller coaster ride since 2008, experiencing a massive multi-year crash and recovery. The number of transactions per day has seen a huge surge since its inception. The current market cap of blockchain stands at $76 billion[3] with a transaction volume of $1.1 billion per day.

Fig. 2. Market Capitalization of Bitcoin since inception.

The blockchain technology is still in its nascent stage and is predicted to move past the Innovators phase in 2017 and reach the 13.5% of early adopters within financial services. The tipping point, according to Accenture[4], is then expected to happen in 2018 when the early majority of financial services begin to see the benefits of the early adopters and new models emerge. This growth phase is predicted to last until 2025 when blockchain will finally become mainstream within financial services.

Fig. 3. Growth prediction of Blockchain over the years.

As the technology continues to grow, many industries across the globe have started investing significant amount of capital into it. In the second quarter of 2017, the global venture capital industry continued the trajectory set by the first quarter. According to Crunchbase[5] on an annual basis the number of funding rounds has increased by 8.8% as compared to 2016. It is projected that the global venture capital market will continue its upward journey by investing more into this technology. The number of blockchain startups are mushrooming with an equally solid support from the investors. At this rate by 2020 it is predicted that majority of the global organizations will be making a shift towards blockchain.

III. Smart Contracts

Blockchain is much broader and diverse than just Bitcoin. With Bitcoin being the first successfull app, the two terms were thought to be synonyms until recently. The degree of robustness and security that public cryptocurrencies have shown is a good indicator of infinite technological benefits this technology has to offer. Blockchain is not just limited to calculating the number of bitcoins in your digital wallet. It is a very powerful technology capable of performing complex operations as well. One of the interesting properties of blockchain is to attach business logic called Smart Contracts to the transactions. Blockchain can not only be used to exchange assets and transfer ownership but also to run code defined in full fledged programming language. Since the program is recorded on a blockchain it inherits immutability and censorship resistance. This allows automation of business processes that can execute beyond organizational boundaries in a decentralized and secure fashion.

Smart Contract in simple words is a piece of code, a set of instructions capable of self execution when specific conditions are met. ”We could think of a vending machine as a kind of a contract: put in quarters, dollars and get a soda back plus exchange”[6]. The terms and conditions which are agreed upon by the involved parties is coded into the blockchain. It is akin to a series of if-then statements where the ***ifs*** are preconditions which must be fulfilled to trigger the : ***thens***. A triggering event is hit and the contract executes autonomously as per the coded terms. We can understand the concept better with the help of an example. Suppose a party X rents an apartment from party Z. This can be simulated using blockchain by paying in cryptocurrency. X will get a rent agreement which can be simulated by using a virtual contract held in the blockchain. At the same time Z will provide X with a digital entry key. X will receive the key on the start date as per the virtual contract. If X does not receive the key on time, the function coded into the blockchain will initiate a refund. If Z sends the key before the actual date, the function will hold it till the actual date arrives. A fascinating thing about this arrangement is that it is witnessed by hundreds of people, so one can expect a flawless delivery. If Z gives X the key, Z is surely to be paid. If X sends a particular amount of fees using bitcoins, it will surely receive the key.

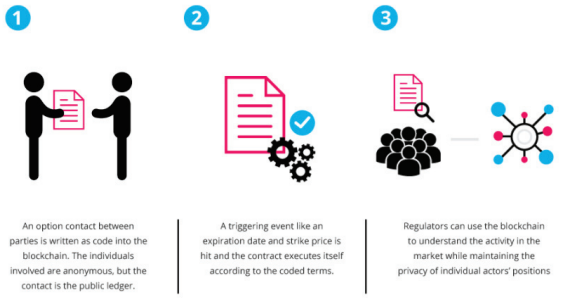

Fig. 4. Working of a Smart Contract.

Ethereum is considered as the next killer app of Blockchain after Bitcoin. Ethereum is a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference[7]. These applications run on top of a custom built blockchain which serves as a powerful shared platform capable of moving value around and represent the ownership of property. While in Bitcoin the blockchain technology is used to track the ownership of digital currency, the Ethereum blockchain is focused on running programming code of any decentralized application.

IV. Blockchain as a Service (BaaS)

Building business applications powered by blockchain is a complex task entailing infrastructure and development challenges. Blockchain-as-a-service(BaaS) could be the next big thing in the enterprise software development. By deploying the blockchain as a service on the cloud, a platform is created which can be used to prototype, test and build customized blockchain applications without any upfront capital investment.

The blockchain framework provides services like consensus and validations protocols in a plug and play fashion in order to help businesses develop their own specific solutions. Businesses can use BaaS to experiment and play with blockchain technology and focus only on the application development. In this manner customers and developers can start building blockchain extensions for existing applications across industries and realise the potential of this disruptive technology.

Major enterprise software providers like IBM , Microsoft and SAP have already started rolling out their cloud based blockchain solutions. In March 2017 IBM announced the release of IBM Blockchain, the first enterprise-ready blockchain service based on the Linux Foundation's Hyperledger Fabric version 1.0. The service enables developers to quickly build and host security-rich production blockchain networks on the IBM Cloud, and is underpinned by IBM LinuxONE, the industrys most secure Linux server[8]. IBM's High Security Business Network offers the worlds most secure Linux infrastructure that integrates security from the hardware up through the software stack, specifically designed for enterprise blockchains. Microsoft recently introduced the Coco Framework, an open-source system that enables high-scale, confidential blockchain networks that meet all key enterprise requirements - providing a means to accelerate production enterprise adoption of blockchain technology[9]. Coco presents a different approach to ledger construction, giving enterprises the scalability, distributed governance and enhanced confidentiality they need without sacrificing the inherent security and immutability they expect. Microsoft also provides BaaS - a rapid, low-cost, low-risk, and fail-fast platform for organization backed by a cloud platform in Microsoft Azure. In May 2017 SAP launched SAP Leonardo - a digital innovation system that meaningfully integrates next-generation technologies helping customers redefine their business - including ready-to-use blockchain technology and SAP Cloud Platform Blockchain service.

V. Challenges to Software Testing

A distributed system in simple words is a collection of independent computers that appears to its users as a single coherent system. In other words its a collection of autonomous computers which are interconnected by means of a network. These computers collaborate and coordinate with each other by sending messages to each other in order to achieve a common goal. Distributed systems can be difficult to design, difficult to program, difficult to manage and above all difficult to test. Testing on a single system even under the best of circumstances, no matter how good the tester is or how better the test suite and automation is, bugs can still get through. Now consider the same issues and multiply them with multiple processes written in multiple programming languages running on multiple boxes that could all be potentially be running different operating systems, and there is a potential for a great disaster.

As with other systems, testing begins with running unit tests against the smallest point of contact called components in the system. Following the successful execution of unit tests, integration tests are run to validate the behavior of the entire logical system as a whole. Since there is no limit on the number of systems that can constitute a distributed architecture, testing all possible configurations is a herculean task. In a normal scenario, testers can execute a test case, provide inputs and have some assertions about the expected output. In distributed systems, a tester can run the same test case with same inputs twice and get two different correct answers. Events in distributed systems do not occur synchronously. Similarly there are challenges like generating test data to cover all components, avoiding deadlocks and race conditions, deciding the test sequence and testing for scalability and performance.

Validating and verifying that an blockchain implementation is working fine presents some unique challenges. The inherent structure of this technology which includes distributed systems and anonymous nodes working together in P2P environment

demands the need for specialized testing tools and practices. The immutable nature of the blockchain further adds to the criticality and complexity of testing. We identify some of the major challenges and hurdles to testing in a blockchain based environment.

A. Public vs Private blockchain

There are two types of blockchain: public blockchain and private blockchain. A public blockchain is a blockchain that anyone in the world can read, anyone in the world can send transactions to see them included if they are valid and verified by nodes in the network. In such blockchain implementations anyone can participate in the consensus process - the process by which everyone in the network agrees to a set of transactions being included in the blockchain. Public blockchains are secured by using a combination of economic incentives and cryptographic verifications mechanisms like proof of work, proof of stake. On the other hand in case of private blockchain write permission is restricted to either one organization or a consortium of various organizations. Read permissions may be public or restricted to some nodes. The consensus process is controlled only by a predefined set of nodes. For example in a consortium of 10 financial institutions each of which is running a node, 8 of them must sign in order for a block to included in the blockchain.

One of the major factors that decides the scope and level of testing is whether the implementation is based on a public platform like Ethereum or customized platform that is built for an organization or consortium of organizations. In case of a private blockchain it is somewhat easy to simulate all the scenarios and test them internally. Since private blockchain operates in a controlled environment traditional testing methods can prove handy. A detailed test strategy can be designed since the functionality is customized. The complexity escalates when the implementation is on a public platform. In public blockchain implementation there is no upper limit on the nodes that can participate, nodes can join and leave in an ad-hoc manner, consensus may not be reached easily lowering the speed of transactions, a hard fork may get created and many more issues. It becomes very difficult to visualize, extrapolate and design test strategies and test cases covering all aspects.

B. Performance

Performance assumes even more importance in case of blockchain implementations considering the fact that it involves a distributed architecture connected together using a P2P network. The major problem that arises is in estimating and managing the number of transactions that are anticipated on the production systems. The blockchain network needs to be tested for performance and latency which can vary based upon the size of the network, expected size of transactions, the consensus protocol used and the latencies that it might generate. A major pitfall that led many businesses withdrawing from using Bitcoin implementation has been delay in the verification of transactions due to a sudden surge in its usage.

One of the major components of blockchain is consensus protocols. Bitcoin introduced Proof of Work (PoW) as the means of verifying transactions through a process called mining. The process of mining requires significant amount of computing power and resources as well as the difficulty of cryptographic puzzle needs to be adjusted time to time. It is very challenging to simulate the performance of the transaction validation mechanism in a sandbox environment considering the fuzziness involved. Performance starts to degrade due to sudden surge in number of transactions. Testing the scalability becomes important here to ensure good performance at all times. It is challenging to exhaustively test the performance as the diffculty level of cryptographic puzzle keeps increasing and the number of miners fluctuating. Even a small unanticipated delay can lead to huge business losses. A well defined test strategy needs to be outlined and applied in order to manage the validation of transactions without any performance issues.

C. Security

The huge popularity of blockchain can be credited to the security that is inbuilt in this technology. Though there are enormous security benefits but there are some security challenges as well. If they are not addressed properly it can have serious consequences especially in the finance industry. In case of both public and private blockchains, one of the major challenges is testing the security of the network architecture. Nodes in a network may become unresponsive or intermittently active for suspicious reasons. Proper testing needs to be done here considering various permutations and combinations so that the consensus process doesnt get affected and the consistency of the ledger is not violated.

In case of private blockchain there might be the need of transaction reversibility due to attempted theft or other reasons. In such cases proper validations must be done to ensure the integrity of the distributed ledger. Testing needs to ensure that the transactional data is not lost in this process. Private blockchain like any other distributed architecture depends upon network communication to provide read and write access to transactional data. It is prone to denial of service and false identity attacks, hence proper testing needs to be done here to prevent any backdoors into the system. Hence though the blockchain technology is built upon the principles of high security, it still faces some issues which are sometimes difficult to be exhaustively incorporated into the test strategy and test cases.

D. Test Environment

Proper testing can take place only if a proper test environment is available that is similar to the production environment. The availability and utilization of a test platform that provides a replica of the implementation is indispensable,

and if not available considerable amount of resources and time needs to be invested in setting up or spawning from the real implementation. Open source implementations provide test instances that are distinct from the original while providing means to test advanced transaction functionalities in a like for like mode. In case of private blockchain a proper test environment can be setup keeping in mind the customized functionality.

In the present scenario blockchain is used as an add-on to the existing business processes which necessitates the needs for efficient integration testing. There is a shift towards inclusion of blockchain in existing applications rather than developing them in isolation. An implementation of blockchain for a particular process within a company is expected to have interfaces with other applications. Understanding these interfaces and communication points to ensure consistency with the existing processes, so that there are no points of disconnect is a key challenge in testing these implementations. The Application Programming Interfaces (APIs) used to communicate with existing business proceses should be made available to the testing teams. The Quality Assurance teams can then use these interfaces to validate proper communication between legacy code and the blockchain implementations.

VI. Approaches to Testing

There is more trust in the world today than any other point in history owing to our growing dependence on software to carry out almost every type of transaction. Blockchain has brought more visibility to these networks of transactions. Information about an asset which was localized initially to separate owners is now shared between all the stakeholders. Testing teams face an unprecedented demand for first-time quality while minimizing the impact of testing on the teams delivery.

The criticality of the testing can be understood by the example of Smart Contract whose acceptance in the business world has increased exponentially. From technology standpoint, Smart Contract is nothing but an API. It has public functions which can be called by anyone registered on the blockchain network. Once a contract is created, it is immutable and once deployed it stays there forever. If a defect is leaked and detected in the production system, the contract is rendered useless and a new version needs to be created and deployed. Once we deploy a new version, the old data created is not automatically transferred; it needs to be manually initialized and transferred which is very cumbersome. The immutable nature further implies that updating a existing contract is not possible. This greatly increases the complexity of implementation and places a huge responsibility on the quality assurance team to get it right the first time. With the Advent of DevOps, the role of tester is changing and focus is more on continuous testing. The best strategy for continuous testing involves testing as early as possible in production like environments (shift-left), include testing as part of every deployment process (shift-right) and execute continuously throughout the lifecycle (automation).

Software quality is very critical and there are several testing approaches for it:

A. Consensus

In a business network where the participants are known and trusted, transactions can be verified and appended to the ledger using various means like Proof-of-Stake, Multi-party signature and Practical Byzantine Fault Tolerance algorithms(PBFT). Whatever maybe the consensus protocol followed, validated data is appended to the ledger and acts a single source of truth. For a tester it means ensuring the consistency and validity across multiple stakeholders. It also means taking into consideration the dynamic nature of nodes as well its impact on both data flow and performance on the blockchain ecosystem. A good approach here would be to use service virtualization. The interaction between different components should be switched on and off using API's to simulate real scenario and gauge its impact on the implementation. For example when a party is added back into the network, a short data update might be required for synchronization purposes. This can impact the speed of verification if the number of nodes increases. In order to avoid breakdown it is essential to follow a exhaustive approach by covering as many scenarios as possible.

B. External Interaction

In majority of business scenarios today blockchain is deployed at a particular stage in the complete process. This clearly suggests blockchain needs to interact and integrate with other components connected to it in a seamless way. A blockchain may output an event to an external system or a specific event in an external system may trigger code in the blockchain. Also blockchain execution might require the help of an external service or routine while it executes a hold function. A good testing approach here would be to test each and every interaction between the blockchain ecosystem and other external systems. A tester should ensure that at each and every joint correct data is flowing in and out. Consider the example of submitting a completed transaction to an API. Once the transaction is validated against a specific set of rules, a consensus is agreed upon and the data is appended in the ledger. A confirmation is received via an API for the same. A correct approach would not only be to check for the confirmation received but also validated for consistency of data and information. An omission of a validation at even a single step may corrupt the records in the ledger and propagate false information to the next stages. Most blockchains use REST based APIs for interactions which can be tested to ensure seamless integration.

C. Functional Testing

Smart Contracts are code that gets self executed with every transaction. It first assesses the transaction against a set of

rules coded into the contract before allowing consensus. A point to note here is that it becomes more important to test the behavior of the contract as compared to the pervasive data. The functional correctness is equally important as the data. A good approach for testing Smart Contracts would be to lay more emphasis on functional testing. The tester needs to ensure that the terms and conditions are correctly coded into the contract and that they are self triggered on arrival of the legit data. Unit testing can be performed for each and every condition and once they work completely in isolation, integration testing can test the entire logic of contract as a whole. It is a good practice to test Smart Contracts on a dummy blockchain or a virtualized service before deployment considering its immutable nature.

D. Performance Testing

There are two major ways to measure performance: from the perspective of the external end user using a blockchain solution and response from internal system interfaces. Performance testing should also be performed against the services provided by the blockchain ecosystem in order to gauge the impact of failures. It is a good approach to keep a watch on the performance when there are high chances of failure like data update across nodes, synchronization across nodes or during the consensus process. These scenarios are largely influenced by data location and latency. It is a good practice to have automated performance testing to assess the scalability of the blockchain ecosystem for all these cases. The tester needs to ensure that speed is of utmost importance and inspite of horizontal and vertical scaling performance should not hamper at all. In applications like Bitcoin where anyone is free to open a digital wallet and perform exchanges, continuous performance testing and monitoring is indispensable. Testers need to design scenarios which can combine all aspects across the blockchain ecosystem and should include compound testing as well.

E. Security Testing

The invention of blockchain has ushered us in an era where all stakeholders are equally contributing to the integral security of the data and network. Though blockchain is built on the principles of security and immutability, it is still prone to security threats. The private blockchain owners should be cautious about security of their existing business solutions interacting continuously with the blockchain. Smart Contracts pose a even greater challenge for regulators or consensus bodies because it is embedded into the execution of every transaction on the blockchain. Testers need to analyze the code for implementation based security flaws as well as the distributed architecture for threats that could lead of Denial of Service(DOS) or vulnerability exploitation. The threats need to be modelled and anticipated properly in order to provide mitigation strategies and detailed fixes. Automated security testing is a better approach to ensure the integrity of the ledger with multiple applications. Application fuzz testing can also prove handy to automate the process of finding vulnerabilities by knowingly injecting faults into the system. Security testing needs to be incorporated in the entire cycle of implementation and deployment as part of DevOps.

VII. Conclusion

The advent of Blockchain has brought us the Internet of value and ushered us into a new era of managing transactions in a secure way. Its impact can be gauged from the fact that almost every major financial institution and organization is interested in this concept. With technology and software giants like IBM, Microsoft and SAP rolling out BaaS, its adoption will see an upsurge in the coming years. Blockchain presents some unique challenges to the software development lifecycle owing to its inherent design. The widespread deployment of blockchain based applications places huge responsibility on the Quality Assurance team to get it right the first time. The key to successfully adopt a blockchain methodology rests in a well-balanced and detailed approach to design and validation. While the mechanisms of testing are largely similar to any other system, there is a necessity to focus on specific areas and evolve a test strategy which is in line with the principles and implementation construct that is applied to the domain.

References

[1] Satoshi Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", http://bitcoin.org/bitcoin.pdf

[2] Don Tapscott and Alex Tapscott , "Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World", ISBN:1101980133 9781101980132

[3] Bitcoin Block Explorer Blockchain , Available online at https://blockchain.info/

[4] Laurie McGraw , Claus Helbing , Chris Brodersen , "Blockchain Technology : Preparing for Change" , Available online at https://www.accenture.com/in-en/ /media/Accenture/next-gen/top-ten-challenges/challenge4/pdfs/Accenture-2016-Top-10-Challenges-04-Blockchain-Technology.pdf

[5] Inside the Q2 2017 global venture capital ecosystem TechCrunch , Available online at https://techcrunch.com/2017/07/11/inside-the-q2-2017-global-venture-capital-ecosystem/

[6] SZABO, Nick , "Formalizing and Securing Relationships on Public Networks". September 1997, ISSN 13960466. Available Online at http://firstmonday.org/ojs/index.php/fm/article/view/548/469 DOI : http://dx.doi.org/10.5210/fm.v2i9.548.

[7] Ethereum Project, Available online at https://www.ethereum.org

[8] IBM News Room 2017, Available online at https://www-03.ibm.com/press/us/en/pressrelease/51840.wss

[9] Announcing Microsofts Coco Framework for enterprise Blockchain Networks, available online at https://azure.microsoft.com/en-in/blog/announcing-microsoft-s-coco-framework-for-enterprise-blockchain-networks/

[10] Simone Porru, Andrea Pinna, Michele Marchesi, Roberto Tonelli, "Blockchain-oriented software engineering: challenges and new directions". Proceedings of the 39th International Conference on Software Engineering Companion Pages 169-171 , Buenos Aires, Argentina May 20 - 28, 2017 , ISBN: 978-1-5386-1589-8 DOI : 0.1109/ICSE-C.2017.142

[11] Michael Crosby, Nachiappan, Pradhan Pattanayak, Sanjeev Verma , Vignesh Kalyanaraman, "Blockchain Technology Beyond Bitcoin ", Sutardja Center for Entrepreneurship & Technology Technical Report October 2015

[12] Blockchain technology: 9 benefits and 7 challenges — Deloitte, Available online at https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/blockchain-technology-9-benefits-and-7-challenges.html