Non-Functional Requirements for Blockchain: Challenges and New Directions

Tahmina Akter Tisha and Mir Moynuddin Ahmed Shibly

Department of Computer Science and Engineering
East West University, Dhaka, Bangladesh
Email: shiblygnr@gmail.com

Abstract. Blockchain is one of the breakout technologies of the 21st century and it is destined to rule the field of cybersecurity. Eventually, all applications and software will adopt blockchain for being the most secure technology ever existed. Unlike other fields of computer science, blockchain too has functional and non-functional requirements (NFRs). As it is an emerging technology, Blockchain’s non-functional requirements are yet to be well-defined. From requirements engineering perspectives, the NFRs for blockchain should be well-established. In this study, some of the major non-functional requirements of blockchain are thoroughly analyzed. And, challenges of NFRs for blockchain and new research directions have been proposed. Five non-functional requirements challenges are presented – lack of knowledge about NFRs for blockchain, the necessity of feasibility analysis, integration with software engineering, NFRs measurement metrics, and its formal language representation. Based on those challenges, four new research directions have also been proposed. If those challenges are dealt with properly, the world will surely march towards a safer future in terms of cybersecurity.

1. Introduction

Blockchain is one of the emerging technologies that is going to have a significant impact in the world where any sort of transaction happens. It is changing the way people interact with each other in terms of currency transactions. It is a system where a record of Bitcoin [1] or other cryptocurrency transactions is maintained through several computers that are connected to a peer-to-peer network. Blockchain technology is transforming the economy, finance, and money to the degree that its revolutionary power is being compared to that of the web and the internet in their early stages. As a consequence, all the development of software that revolves around blockchain technology is advancing at a spectacular rate [2]. As a revolutionary technology, it is expected to deliver substantial cost reductions by allowing transactions to be carried out directly between the users as peer-to-peer (P2P) processes. It provides an alternative to the conventional way of using a trustworthy third-party entity as an intermediary, for example, a financial institution like BBVA, Amazon, etc. Governments may use blockchain technology to deliver cybersecurity, automate processes, and incorporate hyperconnected services while improving trust and transparency. E.g., HACKMX, a project that uses
blockchain technology to track and verify bids for public contracts, was launched in the digital government unit of the Mexican Ministry of Public Administration [3].

A blockchain is a kind of diary or spreadsheet that contains transaction information, and each transaction generates a hash. When the majority of the nodes approve a transaction then it is written into a block. Each block refers to the previous block and together make the blockchain. It is a growing chain of blocks where each block contains three fields – transaction info, participants involved in that transaction, and a cryptographic unique identifier i.e., a hash. Whenever a block is added to the chain, a copy of the block is stored in every computer that is connected to the network. Before adding a block to the chain, four criteria must have to be fulfilled – a transaction must have to take place, the transaction has to be verified, the transaction information has to be stored in a block and there has to be a hash associated with the transaction. Blockchain is a decentralized ledger system with no central authority [4]. For being decentralized, it is impossible to alter a transaction whose information block is already added to the chain. Because, to do that, the majority of copies of the block of that transaction has to be altered to prove that the altered one is the real one. Unless other users will not accept that as the right one.

Although blockchain is impenetrable in terms of the security of a transaction, other requirements should be explored too. In conventional requirements engineering, the functionalities that a system must offer and must persistently provide are known as functional requirements [5]. Besides those functionalities, the system should be able to provide some other attributes like how the system will serve the functionalities. Such requirements are known as non-functional requirements (NFRs) [5]. For example, the software is meant to provide an interface between users and a bank so that the users can perform various transactions. Here, the process of secured transactions between parties is the functional requirements. On the other hand, the speed of transactions, the reliability of the service, the consistency, etc. are the non-functional requirements of that system.

There are many studies conducted for analyzing, exploring, and reasoning about the NFRs for regular software. These covered the most prominent NFRs like customer satisfaction, privacy, performance, usability, reliability, maintainability, and security [6][7]. As those software systems have various NFRs, a blockchain system should also have some NFRs and as blockchain is becoming one of the significant parts of secured transactions, it is worth exploring the NFRs for it and formulates a proper understanding of how a blockchain system behaves. This study aims to explore the challenges for NFRs of blockchain and derive some new directions from the perspectives of requirements engineering. However, the NFRs for the software systems are well-defined and well-understood. But when it comes to the blockchain-based system, the existing knowledge of NFRs may not apply. The existence of blockchain implies that the definition of certain NFRs for blockchain varies from typical software. The non-functional requirements are lesser known for blockchain-based systems. For example, what does it mean to be maintainable for a blockchain-based system? Do NFRs like flexibility and modularity remain relevant for the blockchain-based system? Some NFRs may become less important for a blockchain system while some may become more important. There are several common qualitative trade-offs in traditional NFR studies, also called conflicting NFRs
For example, there could be a trade-off between performance and privacy. The blockchain-based system needs to find out these types of conflicting trade-offs.

The aim of this study is to discuss whether the conventional understanding of NFRs and efficiency can be extended to blockchain-based systems from a requirements perspective. In order to do that, few research challenges and directions have been proposed related to the non-functional requirements of Blockchain technology. In this work, the justification has been presented that the conventional NFRs may need to be reorganized to cope up with the new technology like blockchain and the NFRs may need to be rethought or completely new techniques may need to be added to meet the paradigm change.

In the following section of this paper, state-of-the-art of blockchain technology with respect to non-functional requirements engineering has been described. After that, an example of blockchain in action has been illustrated. Then, the key research challenges of non-functional requirements for blockchain have been presented followed by the future directions. Finally, some concluding remarks have been presented.

2. Non-functional Requirements and Blockchain Technology

To make a system successful, it is very important to develop and consider the non-functional requirements properly [7]. On system can work just fine based on its functionality but can also fail for not handling the non-functional requirements (NFR) appropriately.

Non-functional requirements are product constraints or the features the system provides. They include constraints on timing, technology limits, and limitations imposed by standards. In certain cases, non-functional specifications refer to the device as whole systems or facilities, rather than individual device functions. This specific description, which describes something crucial in terms of what it is not, is not ideal, as many authors have discussed [8][9]. Our aim here is not to satisfactorily define NFRs but to explore their application to blockchain-based systems. NFRs can be treated as quality and the functional requirements can be recognized as an entity [10]. For example, a bus reservation system can be used to book seats using a secured transaction gateway. Here, booking the seats is functional requirements or entity of the system and security is the non-functional requirements or quality.

2.1 Qualities for Blockchain

Many works on blockchain have been described how blockchain works, how it is the most secure way to complete a transaction. These types of aspects are mainly analyzed and explained. Few works have been done regarding the non-functional requirements of a blockchain-based system. We are summarizing those works in this section.

UX Design. One unique obstacle to the creation of blockchain is the complexity of the user interface. The query is, how much of blockchain should you disclose to your consumers, as the enabling infrastructure? Do people need to know where they communicate with a blockchain anywhere on the application? Will they need to know what public and private keys are? How will it be kept secret if people do not know their private keys? Do they know about tokens, and need them to communicate with the application? These questions are relevant because people
trust their money into your blockchain application. The value of the blockchain assets is usually
backed by the value of a cryptocurrency coin, provided by an initial coin offering (ICO).

If the customer’s wealth is connected to the coin's value, then how do you tell them their net
worth increases and decreases as the value of the cryptocurrency increases and declines? When
they are using your website, are they now investors in cryptocurrency? It is critical from the
perspective of the user experience, too. Applications should be user friendly. For a new consumer,
this first experience is very significant. Launching and cluttering a website with blockchain-related
jargon is likely to put off most consumers. But dumbing it down can reduce the importance of it or
the visibility of blockchain’s main benefits that distinguish your application from the non-blockchain
competition.

**Scalability** [11]. If the platform is connected to an implementation of a blockchain such as
Ethereum then it is also connected to the scalability of the underlying network. Ethereum
currently runs up to a theoretical limit of 25 (based on proof of work) at 4 transactions a second.
When the next Ethereum game begins, a lot of transactions are created, would this affect the
consumers? If they needed it, could they get their assets out immediately? Consumers would
like to realize that they are not bound to something and will be able to return to the non-digital
world at any stage of their choosing. To this, it is important to choose the right underlying
platform.

**Development Operations.** As blockchain is still emerging, the technology to build a
blockchain-based system is still evolving. It takes time to integrate new functionality into the
system and improve the DevOps experience. Therefore, there should be enough amount of time
associated with the development phase.

**Managing Stakeholders.** There is a tendency to over-sell the benefits of governance while
marketing the advantages of a blockchain program. Possibly the actors of governance (e.g.
police, government, auditors) get the most benefits from being able to monitor what everybody
is doing and use it to control or test enforcement. It is necessary but other stakeholders need
opportunities to enter the network otherwise there would be no users and no regulatory or
control transactions. And there is the question of persuading all the stakeholders to get involved
so you can do market research and collecting requirements. Modeling and smart contract
concepts ensure that all various types of stakeholders recognize the company domains. It
requires the views of several stakeholders to address the problem of what should be held in the
blockchain [12].

Finally, who initiates and pays for the creation of the blockchain platform initiative?
Blockchain’s key advantage is that it can facilitate business and collaboration among
organizations that have never met. Over the platform's lifespan, this would attract many
organizations, but one company needs to take the initial step, see the benefit, and create the
platform for everyone else to use.

3. NFRs for Blockchain Examples

In this section, we are going to present an example of how blockchain can be used in a real-life
application. Suppose we are going to develop an application for an online retail shop a huge
multinational company. This multinational company has a branch, where people can buy stuff even beyond the borders. For example, if a user from Bangladesh wants to buy an item from a seller from India, he/she has to pay the price of the product. Since the seller is abroad and there is no way to ensure the seller's authenticity physically and the seller cannot ensure the authenticity of the buyer either, a blockchain-based payment system can resolve this issue easily.

The borderless payment system is susceptible to mistakes, is costly, and is vulnerable to money laundering. Crossing the world takes days if not longer for the currency. The blockchain system can provide a solution to these problems. Many companies already adopted blockchain for remittance services like Abra and Veem [13]. In 2004, Santander was one of the first banks to integrate blockchain into a payment app, enabling clients to make foreign payments 24 hours a day while clearing the next day and in 2019, they have launched the first-ever end-to-end blockchain bond [14]. These are just a few examples of using blockchain in the money transfer and banking sectors.

Now back to our example, if we want to ensure the trust persists between buyers and sellers, blockchain technology comes as the solution. Whenever a transaction happens, a new block will be added with the details of that transaction like date, time, the dollar amount in the first section of the block. In the second section of the block, there will be information about the participants of that transaction – in our case, the buyer from Bangladesh and the seller from India. Encrypted digital signatures of both parties will be there in the block and those digital signatures can be verified by a third party. Finally, the block will have a section consisting of a cryptographic hash. As the blockchain mechanism works, whenever the block will be added to the chain, millions of copies of that will be available online in an instance and the fraudulency in that transaction can never occur. In this way, the secure transaction between two parties that are thousands of miles away from each other and divided by borders can be secured and convenient. In this example, few non-functional requirements are needed to be considered. The developed application and interface for the money transactions should be user friendly. This NFR matches with the NFRs for a typical software. The other NFRs like managing stakeholders so that they do not have any confusion about the whole process should be acquired.

Another example of using blockchain can be in securing healthcare data. As we know, personal medical records and data are very sensitive and sophisticated. There is no alternative to securing and protecting those data. To ensure maximum security these data can be stored on the blockchain with a private key and the data will only be available to specific people who want to access the data after proper verification and validation. The same strategy could be used to ensure research is performed securely and confidentially through HIPAA laws [15]. Surgery receipts may be stored on a ledger and automatically submitted as evidence of delivery to the insurance companies. The ledger could be used for general health care administration, such as medication monitoring, compliance with legislation, test reports, and control of health care supplies too. For this secured medical records repository, the main NFR is security.

In both examples, we have discussed some common NFRs. But what if we add more blockchain-related NFRs to both systems like knowledge about the system. The users may not have an idea of how the system works, but they should be able to trust the system without any
doubt. Other requirements like trust requirements [16], fairness, and transparency are the most important for a blockchain-based system. While developing these types of blockchain-based systems, these non-functional requirements should be implemented with the highest priority.

4. Research Challenges

Based on our illustrations, in this section of the article, few research challenges of non-functional requirements are presented.

**Non-functional requirements identification challenge.** The knowledge of NFRs acquired so far for blockchain is inconsistent and not complete, such as the method of describing and refining NFRs in the sense of blockchain specifics. For example, managing stakeholders is an important non-functional requirement for a blockchain-based system. How much knowledge a user knows about the system and how he/she perceives the system is necessary to understand to increase the usability of the system. The users have the idea that the system provides them the secured transaction, but are they trading off something for security? There are many questions to ask like this in the area of NFRs in the blockchain. These NFRs should be justified in blockchain contexts and other typical non-functional requirements should be refined so that those can be used in blockchain technology too. The NFRs specific to blockchain should be considered to use in other fields like software engineering, machine learning, the internet of things, etc.

**Feasibility analysis challenge.** Our knowledge about the feasibility of using blockchain in various systems is limited. Some studies explore the prospects of using this technology in different fields. Such Singh I and Lee S W [17] analyzed the feasibility of using blockchain for a secure cloud. To analyze the viability of using blockchain technology with the cloud, the authors in this study analyzed cloud and blockchain's security and trust Requirements and NFRs to satisfy cloud users' security and trust requirements. In another study [18], the feasibility and the sustainability of blockchain techniques in E-voting systems have been surveyed. This study demonstrated that blockchain technology can resolve issues with security concerns, integrity, anonymity, confidentiality, etc. The authors claimed and verified that the blockchain can ensure these attributes of E-voting systems. However, these are just two potential fields where blockchain can be used. There are other areas where blockchain fits and may perform well. Finding those and testing the feasibility of blockchain on them can be a challenging task.

**Integration challenge.** Another challenge in the field of studying NFRs for blockchain is to realize how it integrates with various software in terms of quality. Blockchain will have eventually be incorporated in every software which has some sort of payment system or has something that needs any sort of security for its betterment. A software engineer and a cybersecurity specialist or in our case a blockchain specialist have to work together to make an application that will serve its customers with maximum possible security. There are some examples where prospects of these two technologies working together have been analyzed.

Porru S et al. [2] have described the challenges and new directions of blockchain-oriented software engineering. The authors have explained some new challenges of implementing
blockchain into software engineering and demonstrated a few new directions as well. In another study [19], an agile software development method for designing a blockchain application has been described. As software engineering is one of the primary disciplines and blockchain being one of the emerging disciplines in computer science, filling the gap between them can be pretty challenging.

Identifying measurement metrics challenge. As we have mentioned about the refinement of NFRs in the light of blockchain in our first challenge, we also need to understand the way to measure the non-functional requirements for blockchain-based systems. Working on software metrics in typical software engineering has established a range of potential metrics, connected to the required system NFRs, quantifiable at design or runtime e.g., to measure reliability by the number of runtime errors or mixed references measure modularity between components indirectly. These metrics are still applicable for blockchain-based systems, but are all the other measurement techniques still applicable? It is a question worth considering and deeper knowledge about it is desirable.

Non-functional requirements representation challenge. Researchers and stakeholders of blockchain lack a blockchain-specific way to articulate and define blockchain quality specifications, including goals and trade-offs, and the impact of domain background. While it is possible to reuse many of the current NFR-aware methods in a blockchain setting, we expect that the emergence of blockchain will expose several new concepts and challenges that alter the structural layout of extracting non-functional requirements for blockchain-based software. Formulating domain-specific ways to express those non-functional requirements can be helpful to understand the actual meaning of NFRs in the blockchain context.

5. New Research Directions

In the previous section, we have described five challenges concerning non-functional requirements for blockchain and we are acknowledging the fact that these are not the only challenges regarding the matter. There could be and must be many other challenges in the field of NFRs for blockchain. Now, in this section, we are going to present some research directions based on our proposed challenges. The directions that we are going to propose only reflect our thought process. The challenges can be solved by following other objectives too.

Obj1. To explore, identify, and define the non-functional requirements for blockchain. Under this objective, there is another sub-objective which is to refine already existing prominent NFRs for various fields like software engineering, so that some of those NFRs can be used in the context of blockchain. There are some ways by following which, this objective can be achieved. First, to know deeper insights about NFRs for blockchain, the specialists in this field should be asked through interviews, surveys, or any other data collection method. Secondly, a systematic literature review of all blockchain requirements can be conducted. And, finally, for the refinement purpose, the specialists from other fields can be asked and each domain-specific NFRs can be studied.

Obj2. In accordance with our second challenge, the second research direction is to conduct a feasibility study of blockchain technology in the areas where blockchain has not yet been implemented. If the feasibility study is conducted in every potential field where blockchain can
be used, the new NFRs for it based on that specific scenario will come to light and the overall NFRs will be richer.

**Obj3.** The third objective is to analyze the gap between software engineering and implementing blockchain in software effortlessly. More studies should be conducted on how to use blockchain in an application on a general level. To make sure that blockchain will work along with software engineering, new frameworks can be developed.

**Obj4.** The final research direction in this study will cover the 4th and 5th challenge from the previous section. The challenges were to introduce the metrics for measuring NFRs for blockchain and to define the NFRs for blockchain in a domain-specific way. The direction to solve both challenges is to create, develop, and define a language representation to express the non-functional requirements for blockchain. The first step to develop this is to develop the semantics for the non-functional requirements concepts for blockchain appropriately. When the development of semantics is done, the graphical and textual syntax can be designed. In this way, a complete language representation of NFRs for blockchain can be developed. This well-documented representation can surely open many other prospects of NFRs in the blockchain-specific NFRs research.

### 6. Conclusion

This study was an attempt to find out more about the non-functional requirements for a newly emerged technology – blockchain. NFRs change and vary from one technology to another. Some change and some remain the same for all. In this paper, we tried to outline the challenges of NFRs study in a specific domain. And, based on those challenges, we proposed some objectives and new research directions. Those challenges and objectives have significant potential to look at and carry on further research from the requirement engineering perspectives. Conducting more research on this field of blockchain will surely lead us to a more secure and reliable user experience.

### Acknowledgment

We are acknowledging the study titled “Non-Functional Requirements for Machine Learning: Challenges and New Directions” by Jennifer Horkoff [20]. Because we have conducted this study based on the pattern of that article.

### References

[1] Nakamoto S 2008 A Peer-to-Peer Electronic Cash System *J. Gen. Philos. Sci.*

[2] Porru S, Pinna A, Marchesi M and Tonelli R 2017 Blockchain-oriented software engineering: Challenges and new directions *Proc. - 2017 IEEE/ACM 39th Int. Conf. Softw. Eng. Companion, ICSE-C 2017* 169–71

[3] Floyd D 2018 Mexico Tests Blockchain to Track Public Contract Bids *CoinDesk*

[4] Zheng Z, Xie S, Dai H, Chen X and Wang H 2017 An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends *Proc. - 2017 IEEE 6th Int. Congr. Big Data,*
Sindhgatta R and Thonse S 2005 Functional and non-functional requirements specification for enterprise applications Lecture Notes in Computer Science

Chung L, Nixon B A, Yu E and Mylopoulos J 2000 Non-Functional Requirements in Software Engineering

ISO/IEC 2011 ISO/IEC 25010:2011 - Systems and software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE) -- System and software quality models

Glinz M 2007 On non-functional requirements Proceedings - 15th IEEE International Requirements Engineering Conference, RE 2007

Chung L and Do Prado Leite J C S 2009 On non-functional requirements in software engineering Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)

Li F L, Horkoff J, Mylopoulos J, Guizzardi R S S, Guizzardi G, Borgida A and Liu L 2014 Non-functional requirements as qualities, with a spice of ontology 2014 IEEE 22nd International Requirements Engineering Conference, RE 2014 - Proceedings

Croman K, Decker C, Eyal I, Efe Gencer A, Juels A, Kosba A, Miller A, Saxena P, Shi E, Gün Sirer E, Song D and Wattenhofer R 2016 On Scaling Decentralized Blockchains Initiative for CryptoCurrencies and Contracts (IC3) Int. Conf. Financ. Cryptogr. Data Secur. 106–25

Hardwick P Non functional requirements and Blockchain Capagemini

Levy A 2018 There’s a lot of blockchain hype, but money-transfer start-up Veem is using it today CNBC

Huillet M 2019 Santander Issues $20 Million End-To-End Blockchain Bond on Ethereum Cointelegraph

DOH 2002 Department of Health and Human Standards for Privacy of Individually Fed. Regist. 1–93

Khalifa D, Madjid N A and Svetinovic D 2019 Trust requirements in blockchain systems: A preliminary study 2019 6th Int. Conf. Softw. Defin. Syst. SDS 2019 310–3

Singh I and Lee S W 2018 Comparative requirements analysis for the feasibility of blockchain for secure cloud Communications in Computer and Information Science

Çabuk U C, Adıgüzel E and Karaarslan E 2018 A Survey on Feasibility and Suitability of Blockchain Techniques for the E-Voting Systems Ijarce 7 124–34

Marchesi M, Marchesi L and Tonelli R 2018 An Agile Software Engineering Method to Design Blockchain Applications 1–8

Horkoff J 2019 Non-functional requirements for machine learning: Challenges and new directions Proc. IEEE Int. Conf. Requir. Eng. 2019-Septe 386–91