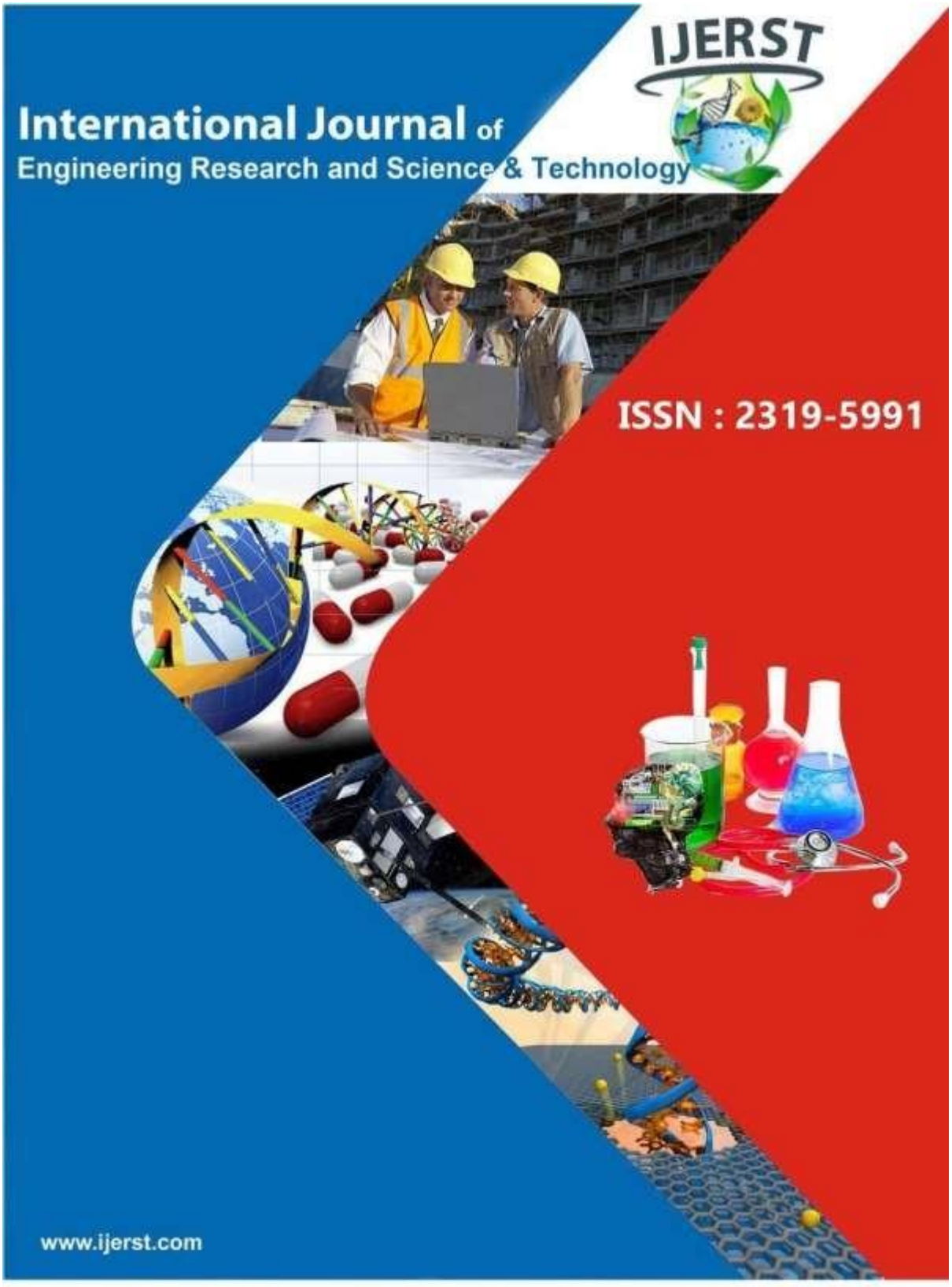


Email: editor@ijerst.com or editor.ijerst@gmail.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 19, Issuse.2,April 2023

A BLOCKCHAIN AND QR CODE BASED MALICIOUS TRANSACTIONS ANALYSIS AND DETECTING THE VULNERABILITY

MS.G.NAGA RANI , 1,Gundra Mounika 2,Valluri Madhu Ramakrishna 3,Akula Veera Venkata Ramana 4,Gopalapurapu Bhargav Sanjay 5,Adurthy Geethika Sree Alekhya 6

Article Info

Received: 17-01-2023 *Revised: 16-02-2023* *Accepted: 14-03-2023*

ABSTRACT

Today's rapidly changing world, is observing fast development of QR-code and Blockchain technologies. It is worth noting that these technologies have also received a boost for sharing. The user gets the opportunity to receive / send funds, issue invoices for payment and transfer, for example, Bitcoin using QR-code. This paper discusses the security of using the symbiosis of Blockchain and QR-code technologies, and the vulnerabilities that arise in this case. The following vulnerabilities were considered: fake QR generators, stickers for cryptomats, phishing using QR-codes, create Malicious QRCodes for Hack Phones and Other Scanners. The possibility of creating the following malicious QR codes while using the QRGen tool was considered: SQL Injections, XSS (Cross-Site Scripting), Command Injection, Format String, XXE (XML External Entity), String Fuzzing, SSI (Server-Side Includes) Injection, LFI (Local File Inclusion) / Directory Traversal.

1.INTRODUCTION

Blockchain could be a data structure that could be a growing list of information blocks. The knowledge blocks area unit coupled along, such recent blocks can‟t be removed or altered. Blockchain is the backbone Technology of Digital CryptoCurrencyBitCoin. The blockchain is a distributed database of records of all transactions or digital event that have been executed and shared among participating parties. Each transaction verified by the majority of participants of the system. It contains every single record of each transaction. BitCoin is the most popular cryptocurrency an example of the blockchain. Blockchain Technology first came to light when a person or Group of individuals name „Satoshi Nakamoto‟ published a white paper on “BitCoin: A peer-to-peer electronic cash system” in 2008. Blockchain Technology Records Transaction in Digital Ledger which is distributed over the Network thus making it incorruptible. Anything of value like Land Assets, Cars, etc. can be recorded on Blockchain as a Transaction. One of the famous use of Blockchain is Bitcoin. Bitcoin is a cryptocurrency and is used to exchange digital assets online. Bitcoin uses cryptographic proof instead of third-party trust for two parties to execute transactions over the internet. Each transaction protects through digital signature.

ASSISTANT PROFESSOR
DEPT OF COMPUTER SCIENCE AND ENGINEERING
PRAGATI ENGINEERING COLLEGE(A),SURAMPALEM(EAST GODAVARI)A.P,INDIA

2. LITERATURE SURVEY

TITLE: QR code generator scam steals thousands in Bitcoin.

ABSTRACT: Every once in a while an attack comes along that is so simple to set up, and yet so effective, that it makes your jaw drop. Here‟s one: fake bitcoin QR generators. According to cryptocurrency enthusiast and Director of Security at MyCrypto, Harry Denley, a wily scammer has been operating a network of fake bitcoin QR code generators to dupe people out of their bitcoins.

TITLE: Fraudsters have mastered stealing bitcoins through cryptomats using a fake CR code

ABSTRACT: US Federal Bureau of Investigation (FBI) has issued a warning against cybercriminals that are using Bitcoin ATMs and QR codes to defraud unsuspecting individuals. The FBI in a recently released Public Service Announcement (PSA), said that it has witnessed an increase in scammers directing victims to use physical cryptocurrency ATMs and digital QR codes to complete payment transactions.

TITLE: Create Malicious QR Codes to Hack Phones & Other Scanners.

ABSTRACT: QR codes are machine-readable data formats that are useful for anything that needs to be scanned automatically. Before QR codes, there were several other formats called linear barcodes, which also stored data in a way that was easy for machines to read. You've probably seen a UPC barcode like theone below on products, as it's often used to identify items for sale so cashiers can scan them to enable faster checkout

TITLE: “Development of the Application for Diploma Authenticity Using the Blockchain Technology,”

ABSTRACT: Global digitalization of society implies the availability of information, as well as verification of its authenticity from anywhere in the world. Providing digital diplomas.the analogue of paper ones, is an actual task. In the current paper the step- by-step development of an application for authentication of diplomas using blockchain technology is considered. Also the concept, structures and operation mechanism of the blockchain are described.

3. EXISTING SYSTEM

In general transaction needs the third party so Blockchain technology introduces the transaction without

Need of any third party usage . This transactions are more secure than the general transaction but in some cases there is chance of attacker to tamper the receiver wallet address and transaction details .Toovercome the problem QR code technology isimplemented in the bitcoin transaction.

DISADVANTAGESOFEXISTINGSYSTEM

- We need to pay transaction charges to the third party
- We must depend on them and wait until our transaction completes
- We need a third party like bank/phone pay

PROPOSEDSYSTEM

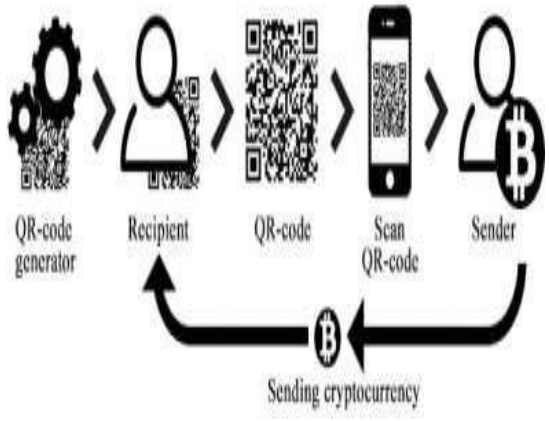
QR-code has clearly surpassed the conventional barcode in popularity in some areas. This is largely due to the fact that a regular barcode can contain a maximum of 20 digits, while a QR code can contain up to 7089 characters. Combined with variety and extensibility, this makes using a QR-code more attractive than using a regular barcode.

Payment by QR-code simplifies the payment process and gives a guarantee of its correct execution, saves time and eliminates errors in manual data entry, since the sender does not need to copy or manually enter the crypto wallet address.

Proposed system implements the web based application consists of two modules such as Admin and user. Admin module describes the maintainance of bit market, Detect Attack analysis and user management. User module for transaction of bitcoins in which receiver needs to verify before accepting sender request based on QR code.

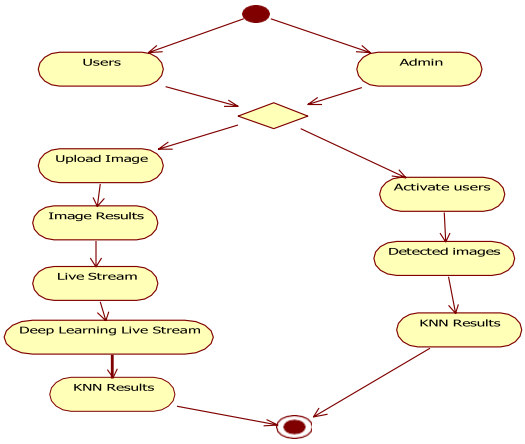
4.SYSTEM ARCHITECTURE .

Belowdiagramdepictsthewholesystemarchitecture oftheproject.



Activity Diagram

A graphical representations of work process of stepwise exercises and activities with support for decision, emphasis and simultaneousness, used to depict the business and operational well-ordered stream of parts in a framework furthermore demonstrates the general stream of control.



5.SYSTEM IMPLEMENTATION

There are 2 modules:

1.Admin
2.User

Admin:-

- Login
- User Management
- **Pending Users**
- **All users**
- Bit Market
- Malicious Qr-Code
- Logout

User:-

- Register
- Login
- Purchase Coin
- Transfer Coin
- Notification
- My Profile
- Logout

6.TESTING

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

6.1 TYPES OF TESTING

■ Unit testing

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

■ Integration testing

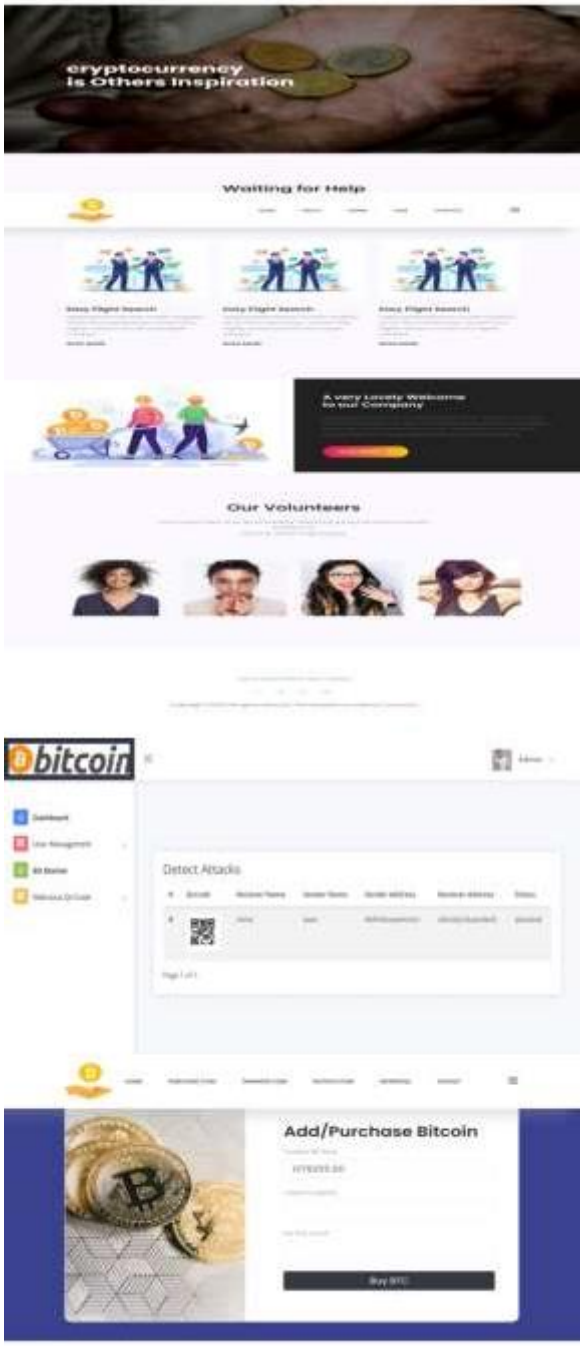
Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

■ Functional test

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Functional testing is centered on the following items:

7.RESULTS



International Journal of Engineering Research and Science & Technology

8. CONCLUSION & FUTURE WORK

This article has studied the security of using the symbiosis of Blockchain and QR-code technologies, and the vulnerabilities that arise in this case. Moreover, the order of operations in the process of transferring or paying with cryptocurrency using a QR-code is considered.

In the course of the study the following vulnerabilities were considered:

A. Fake QR generators

B. Stickers for cryptomats

C. Phishing using QR-codes

D. Create Malicious QR-Codes for Hack Phones and Other Scanners

The possibility of creating the following malicious QR codes while using the QRGen tool was considered: A. SQL Injections

B. XSS (Cross-Site Scripting)

C. Command Injection

D. Format String

E. XXE (XML External Entity)

F. String Fuzzing

G. SSI (Server-Side Includes) Injection

H. LFI (Local File Inclusion) / Directory Traversal

In the course of the study, we have developed a web based application which is used for bitcoin transaction based on the QR code technology .when bitcoin transfers from sender to receiver some time fake QR generated using QR gen tool.

This project verifies receiver wallet address is modified or not , if modified then receiver decline the transaction. In this project only number of bitcoins transfer can be embedded in QR code .Futurework can be implemented by hiding the
Receiver wallet address in the QR code.

REFERENCES

[1] QR code generator scam steals thousands in Bitcoin. [Online]. Available: https://nakedsecurity.sophos.com/2020/04/01/qr-codegenerator-scam-steals-thousands-in-bitcoin/

[2] Fraudsters have mastered stealing bitcoins through cryptomats using a fake CR code. [Online]. Available: https://bits.media/moshennikiosvoili-krazhu-bitkoinov-cherez-kriptomaty-s-pomoshchyu-falshivogoqr-koda

[3] Create Malicious QR Codes to Hack Phones & Other Scanners. [Online]. Available: https://null-byte.wonderhowto.com/how-to/createmalicious-qr-codes-hack-phones-other-scanners-0197416/

[4] SQL injection. [Online]. Available: https://en.wikipedia.org/wiki/SQL_injection

[6] Command Injection. [Online]. Available: https://owasp.org/wwwcommunity/attacks/Command_Injection#:~:text=Command%20injection%20is%20an%20attack,.)%20to%20a%20system%20shell

[7] Os command injection primer: how they work and how to prevent attacks. [Online]. Available: https://www.veracode.com/security/oscommand-injection

[8] Format string attack. [Online]. Available: https://owasp.org/wwwcommunity/attacks/Format_string_attack

[9] XML External Entity (XXE) Processing. [Online]. Available: https://owasp.org/wwwcommunity/vulnerabilities/XML_External_Entity_(XXE)_Processing

[10] D. Aitel Immunity Inc. SPIKE The Advantages of BlockBased Protocol Analysis for Security Testing. [Online]. Available: http://immunity.com