iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** IX **Month of publication:** September 2022

DOI: https://doi.org/10.22214/ijraset.2022.46919

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IX Sep 2022- Available at www.ijraset.com

Digital Health Passport Using Blockchain

Prof. Merwyn D'Souza[1], Vedangi Barve[2], Priti Devdas[3], Aarti Katke[4], Shweta Kotharkar[5], Sweeney Mascarenhas[6]
[1, 2, 3, 4, 5, 6]*Computer Department (of Don Bosco College of Engineering) Goa, India*

Abstract: The recent outbreak of the COVID 19 pandemic has transformed everyone's lives. Dramatically, and society has gone through a new stage with new needs. In this article,
A solution to one of these needs to provide a system of digital certificates for secure storage to share medical data related to COVID 19 for the purpose of demonstrating immunity or deficiency is provided. A clear, unbreakable and safe way to infect a virus. The proposed system is based on Blockchain and its unique benefits, decentralized mobile and cross-platform app development for its use.
Keywords: Blockchain, Hyperledger Fabric, Smart Contracts, Digital Passport, COVID-19.

I. INTRODUCTION

More than two years have passed since the World Health Organization announced COVID 19 as a pandemic, and more than 115 million cases have been reported worldwide. Vaccinations have been open to the public in recent months. After vaccination, each person will receive a paper vaccination certificate and the data will be stored in the Ehealth app run by the Ministry of Health. Paper-based vaccination cards are easy to counterfeit and digital registration is generally considered a good solution.

Centralized data storage means that personal data must be disclosed and trusted by third parties in order to safely store and properly distribute personal health information. You also need to allow your personal ID, which poses a serious privacy issue. Recently 16000 Covid19 test results were lost in the UK which were stored on a simple Excel spreadsheet. This problem can be solved by using blockchain technology. The blockchain behaves differently and is a distributed ledger across the nodes. This node is a complete and updated record in your ledger. That is, if one of the nodes is centralized, the data will be backed up by the other node. The stored data is immutable. That is, the stored data cannot be modified and has end-to-end encryption security. We are trying to set up a digital health passport with the goal of immutably storing verifiable data in a distributed warehouse. An important factor is to respect the privacy of each individual and each individual must retain the sovereignty of the data. A trusted, open and transparent authorship to find out who wrote data to the chain and created fully verifiable and traceable data for transactions on the chain.

Using open source tools, we strive to develop blockchain technology that can be used by a wide range of people. One such tool is Hyperledger, a set of technologies used to create new blockchains. Applying Hyperledger blockchain technology to business processes provides greater transparency, increased accountability, and algorithms guarantee trust between business partners. The technology developed as part of the Hyperledger project is increasingly referred to as the 3rd generation blockchain system, with the 1st generation being considered Bitcoin and the 2nd generation being considered Ethereum. This white paper specifically refers to the Hyperledger fabric and presents the findings of the Hyperledger project. The first part is an overview of the basic concepts and principles behind blockchain technology that enable a way to distribute and store data.

After teaching the basics of blockchain technology, the second part of the work goes in the direction of the Linux Foundation's Hyperledger initiative. The third part specializes in Hyperledger Fabric. That is, Hyperledger Fabric network concepts, architecture, organizational focus, private channels, smart contracts, and transactions

II. BLOCKCHAIN TECHNOLOGY

A. Introduction

Blockchain technology is a distributed replicated database. It is organized in the form of a single-linked list (chain), where nodes are blocks with data on transactions, protected by cryptographic methods after grouping. Therefore, the name is blockchain. It is a system that makes realization of digital transactions without mediation possible. It is based on P2P architecture in which the nodes participating in implementation contains a copy of all the records and always communicate with each other and synchronize recordings. The Blockchain network uses smart contracts to offer regulated access to the ledger in order to ensure consistent updating of information and to enable a full range of functions in the general ledger (transactions, queries, and so on). Smart contracts can be written to allow participants to automatically execute some portions of transactions, in addition to encapsulating information and retaining online simplicity.

©IJRASET: All Rights are Reserved

Consensus is the process of synchronizing general ledger transactions online to ensure that the general ledger is updated only after the transactions have been approved by the individual participants and that the transactions are updated in the same sequence.

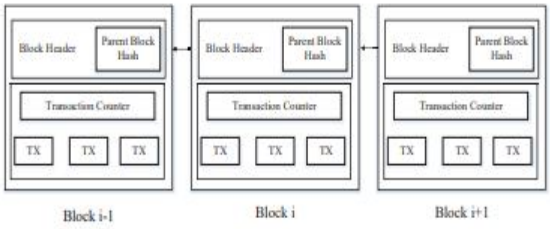


Fig 1: An example of a blockchain, which is made up of a series of blocks.

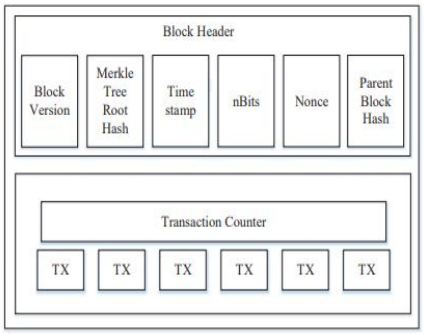


Fig 2: Block Structure

Figure 1 is an example of a blockchain. With the previous block hash contained in the block header, a block has just one parent block. The genesis block is the initial block in a blockchain that has no parent block.

B. Block

As shown in figure 2, a block consists of the block header and the block body. In particular, the block header includes:

1) *Block Version*: indicates which set of block validation rules to follow.
2) *Merkle Tree Root Hash:* the hash value of all the transactions in the block.
3) *Timestamp:* current time as seconds in universal time since January 1, 1970.
4) *nBits:* target threshold of a valid block hash
5) *Nonce:* a 4-byte field, which usually starts with 0 and increases for every hash calculation
6) *Parent Block Hash:* a 256-bit hash value that points to the previous block.

A transaction counter and transactions make up the block body. The maximum number of transactions that can be stored in a block is determined by the block size and the transaction size. To verify transaction authenticity, Blockchain employs an asymmetric cryptography technique.

C. Key Characteristics Of Block Chain

In conclusion, the fundamental qualities of blockchain are as follows:

1) *Decentralization:* Each transaction in traditional centralized transaction systems must be validated by a central trusted agency, resulting in cost and performance bottlenecks at the central servers. In contrast to the centralized option, blockchain does not require the use of a third party. Consensus algorithms are employed in blockchain to keep data consistent across a distributed network.
2) *Anonymity:* Each user interacts with the blockchain using a randomly generated address that hides the user's true identity. Due to the inherent constraint of blockchain, it cannot ensure absolute privacy protection.
3) *Persistency:* Transactions can be validated fast, and honest miners would not accept invalid transactions. Once a transaction is included in the blockchain, it is nearly impossible to delete or rollback the transaction. Blocks containing incorrect transactions might be identified right away.

4) *Auditability:* The Unspent Transaction Output (UTXO) model is used to store data on user balances on the Bitcoin blockchain: Any transaction must reference some previously unspent funds. The state of those referred unspent transactions changes from unspent to spent once the present transaction is recorded into the blockchain. As a result, transactions could be easily tracked and validated.
5) *Encryption:* Blockchain is encrypted, and it employs a sophisticated encryption technology that employs private and public keys to provide practically perfect security in the transmitted data's validity.

D. Taxonomy of Blockchain systems

There are three sorts of blockchain: public blockchain, private blockchain and consortium blockchain. The ability of a node to access or add a new block to the network determines its classification. Blockchain networks open to the public are generally available; any node can join and participate in the network. create blocks and transactions.

The following are some examples of public blockchain. Bitcoin, Ethereum, Dash, and Litecoin are all digital currencies.

1) *Consortium Determination:* Each node in a public blockchain might participate in the consensus process. In a consortium blockchain, only a limited number of nodes are responsible for validating the block. In the case of a private chain, it is entirely controlled by one entity, which can decide on the ultimate consensus.
2) *Read Permission:* A public blockchain's transactions are visible to the public, but a private blockchain or a consortium blockchain's transactions are not.
3) *Immutability*: Since data is stored on a large number of participants, it is impossible to tamper transactions in public blockchain. Transactions in a private blockchain or a consortium blockchain can be tampered easily as there are only limited number of participants.
4) *Efficiency*: It takes lot of time to propagate transactions and blocks since there are a large number of nodes on public blockchain network. With fewer validators, consortium blockchain and private blockchain could be extra efficient.
5) *Centralized:* The difference between the three types of blockchains is that the public blockchain is decentralized whereas consortium blockchain is partially centralized and private blockchain is fully centralized as it is controlled by a single group.
6) *Consensus process:* Everyone in the world can join the consensus process of the public blockchain network. Different from public blockchain, consortium blockchain and private blockchain are permissioned.

Every day, new public blockchains arise. The consortium blockchain could be used in a variety of business applications. Hyperledger is currently working on blockchain frameworks for business consortiums. Ethereum has also made tools available for creating consortium blockchains.

III. CRYPTOGRAPHY IN BLOCKCHAIN

Cryptography is the system of securing important data from unauthorized access. In the blockchain, cryptographic ways are a part of security protocols. It secures a sale taking place between two nodes in a blockchain network. As we know from our former conversations, blockchain technology is grounded on three main pillars; Distributed ledger, Peer- to- peer network, and Cryptographic security.

The successful and safe working of a distributed tally system and the point- to- point network is insolvable without a robust security fashion in place. There are two types of security approaches i.e. Cryptography and Hashing. The introductory difference between these two is that cryptography is used to cipher dispatches in a P2P (Point-to-Point) network. Whereas, mincing is used to secure block information and link blocks in a blockchain.

So, in this discussion, we keep our focus on how we can use these cryptographic ways, keys, and algorithms. How we can use them to secure a communication or information at one node and transferred to the other. We can break down the word cryptography into two corridor; Crypto meaning " hidden " and Graphy meaning " jotting ". thus, cryptography is a system of converting plaintext into undecipherable enciphered text.

Two main generalities behind cryptography are Encryption and Decryption. Encryption is rendering information in such a way that we cannot understand what it means just by looking at it. Decryption is reverse of encryption, i.e. decoding of the enciphered information. The translated textbook or information is also known as ciphertext. And this ciphertext is decrypted through specific ways known as a cipher (way of garbling). Thus, cryptography is a security system that secures a transition or exchange of information between two nodess and prevents it from third- party intervention. Crucial encryption is a cryptographic system that ensures safe transmission of information from point A to point B. This is like an external subcaste of protection. The internal subcaste is mincing. Mincing is a process of unrecoverable encryption of data in a block.

All the data present in the block is translated using the SHA256 mincing algorithm which is unrecoverable. Therefore, applying cryptography at two situations in a blockchain network makes it absolutely secure.

A. *Key Cryptography*

Crucial encryption or cryptography is a system of securing a point to point transition using a key. This key is a unique series of figures and letters which is like a word used to grease a sale between two parties. Crucial encryption canons the communication or information to be transferred to the other side in an undecipherable format. The other side will have to use the same or a different key (depending on asymmetric or symmetric) to crack the communication to bring it in a readable format. Therefore, we use crucial cryptography system to insure the identity of the sender and receiver and to secure the information from attack and abuse. Crucial cryptography is of two types grounded on the number of keys used by the nodes to carry out a secure exchange of information between them.

The first is “Symmetric cryptography” and second one is “Asymmetric cryptography” also known as Public- crucial cryptography.

1) *Symmetric Cryptography:* The symmetric cryptography fashion was the first crucial cryptography that was put to use in a blockchain network. In this system, both the nodes use the same key to render and crack (or cipher and decipher). Suppose node A wants to send some non public information to node B. To grease this transition using the symmetric crucial system, Node A will cipher the information into an undecipherable cipher text using a crucial k1 and shoot it to node B. Node B will admit the cipher text and decipher it using the same crucial i.e. k1. This means both node A and node B need to have the same crucial k1. In the same way, if node A wants to communicate with node C, they both will need a new crucial k2 between them. Or node B and node C will need yet another new crucial k3 to carry out a sale. Therefore, one major debit of this system despite being the fastest system is that a node will need to have a lot of keys to interact with different nodes in the network. Also, the nodes need to make sure that they partake the key securely else a third node might know the key. Due to these downsides there came another system of asymmetric crucial cryptography.
2) *Asymmetric Cryptography:* Asymmetric cryptography doesn't involve participating the same key between two nodes. Rather, in this type of crucial encryption, there are two keys for a nodes; Private key and a Public key. These keys always live in a brace as they work in tandem. That is, we use the public key to cipher the communication and the corresponding private key to decipher the communication. Suppose we've a network of three nodes; A, B, and C. Each node will have its separate brace of private and public keys. The public key is made public i.e. every other node in the network knows this key. Whereas, a private key mustn't be shown to others and kept private by the node. Now let us take an illustration of how a transaction takes place using the brace of keys between two nodes. Let’s say node A has to shoot non public information like bank account details to node B. Now, Node A will first cipher the text using its own i.e. A’s private key and also again cipher it using B’s public key. When this translated text reaches node B, it'll first decipher it using its own i.e. B’s private key and also again using A’s public key. What we need to understand is that the first subcaste of encryption where node A uses its own private key to cipher the communication. It's for Node B to corroborate that the communication is actually coming from node A.

   The coming subcaste of encryption ensures the safety of the communication in a way that only node B’s public key can decode it and only node B’s private key can crack it. By this, the information is defended from any vicious third party attack. This is how the two crucial system works in asymmetric crucial cryptography. This fashion is popularly known as Public Key Cryptography.

B. *Wallet And Digital Signature*

A blockchain portmanteau is a software(e.g. Electrum, Bitcoin core) or indeed a special tackle device(e.g. Trezor, Ledger) that's used to keep transaction information and particular information (private and public key) of the stoner. It's important to know that similar holdalls don't contain factual currency in it (e.g. Bitcoin, Ethereum). These holdalls are just used as a secure place to keep one’s keys (especially private keys) and maintain a sale balance. Also, we can say that we bear a blockchain portmanteau to carry out deals with other druggies. That is, a portmanteau is only a communication tool and the blockchain stores the real information/data/currency in blocks. Also, the digital hand is like evidence that we give to the receiver and the entire network that you're a licit node in the blockchain network. Whenever you initiate a transaction with another node, you have to produce a unique digital signature by combining your transaction data and your private key using a special algorithm. This will guarantee the authenticity of your node and the integrity of the information you're transferring. When the entering node gets the hand communication they can corroborate the transaction by using the public key of the transferring node.

C. Cryptographic Hashing

Mincing is another pivotal factor in securing the blockchain and making it inflexible. Cryptographic mincing refers to rendering the information or data on blockchain into an undecipherable, unhackable text. This is done using a special kind of mincing algorithm known as SHA- 256 (Secure Hash Algorithm). 32- byte long hash value is created. The hash is always of a fixed length regardless of length of the input value was. But it's insolvable to have the same hash values for different inputs. If our input data is " dataflair " the hash value will be "07e42324292ec3bfc150958da854dd8d0357b021dc5e4cfd75e65eed43bfe382 "

But if we change our input to " dataFlair " with one letters made capital, the hash will be "64a5c3a ade4 99eabcc677bd5445c 8463 6ea64fbf0c7c01a49e469ff05da179ef "

This is how specific the process of mincing is, if there's any nanosecond change of indeed a letter in the input, the event will be different. This makes discovery of pitfalls on data and security veritably quick and easy.

IV. HYPERLEDGER

A. Introduction

Hyperledger is collaboration of the Linux Foundation's open-source blockchain. Hyperledger Fabric is an open-source technology for deploying and operating permissioned blockchains that is modular and adaptable. Fabric is presently used in over 400 distributed ledger prototypes and proofs-of-concept, as well as multiple production systems, in a variety of sectors and use cases.

Also, Fabric is the first blockchain system to run distributed applications built in general purpose programming languages without relying on a cryptocurrency in a systemic way. Furthermore, it implements the permissioned model using a portable idea of membership that can be coupled with industry-standard identity management. Fabric rethinks how permissioned blockchains deal with non-determinism, resource exhaustion, and performance threats by taking a fresh approach to the construction of a permissioned blockchain.

B. Why Hyperledger Fabric

1) Modularity

Hyperledger Fabric has been particularly architected to have a modular architecture. Whether it's pluggable consensus, pluggable identification control protocols consisting of LDAP or OpenID Connect, key control protocols or cryptographic libraries, the platform has been designed at its core to be configured to fulfil the variety of employer use case requirements.

a) A pluggable ordering service establishes agreement on the order of deals and also broadcasts blocks to peers.
b) A pluggable class service provider is responsible for associating realities in the network with cryptographic individualities.
c) An voluntary peer- to- peer gossip service disseminates the block's affair by ordering service to other peers.
d) Smart contracts ("chain law") run within a vessel terrain (eg, Docker) for insulation. They can be written in standard programming languages but don't have direct access to the tally state.
e) The tally can be configured to support a variety of DBMSs.
f) A pluggable countersign and confirmation policy enforcement that can be singly configured per operation.

2) Permissioned vs Permissionless Blockchains

In a permissionless blockchain, nearly anyone can share, and every party is anonymous. In such a environment, there can be no trust other than that the state of the blockchain, previous to a certain depth, is inflexible. In order to alleviate this absence of trust, permissionless blockchains generally employ a " booby-trapped " native cryptocurrency or sale freights to give profitable incitement to neutralize the extraordinary costs of sharing in a form of intricate fault tolerant agreement grounded on " evidence of work " (PoW). Permissioned blockchains, on the other hand, operate a blockchain amongst a set of known, linked and frequently vetted actors operating under a governance model that yields a certain degree of trust. A permissioned blockchain provides a way to secure the relations among a group of realities that have a common thing but which may not completely trust each other. By counting on the individualities of the actors, a permissioned blockchain can use more traditional crash fault tolerant (CFT) or intricate fault tolerant (BFT) agreement protocols that don't bear expensive mining. Also, in such a permissioned environment, the threat of a party designedly introducing vicious law through a smart contract is lowered. First, the actors are known to one another and all conduct, whether submitting operation deals, modifying the configuration of the network or planting a smart contract are recorded on the blockchain following a countersign policy that was established for the network and applicable sale type. Rather than being fully anonymous, the shamefaced party can be fluently linked and the incident handled in agreement with the terms of the governance model.

3) Smart Contracts

There are three crucial points that apply to smart contracts, especially when applied to a platform. Numerous smart contracts run coincidently in the network, they may be stationed stoutly (in numerous cases by anyone), and operation law should be treated as untrusted, potentially indeed vicious.

Utmost being smart contract able blockchain platforms follow an order-execute armature in which the agreement protocol validates and orders deals also propagates them to all peer nodes, each peer also executes the deals successionally. The order-execute armature can be set up in nearly all being blockchain systems, ranging from public/ permissionless platforms similar as Ethereum (with PoW- grounded agreement) to permissioned platforms similar as Tendermint, Chain, and Quorum.

Smart contracts executing in a blockchain that operates with the order- execute armature must be deterministic; else, agreement might no way be reached. To address the non-determinism issue, numerous platforms bear that the smart contracts be written in a non-standard, or sphere-specific language (similar as reliability) so that non-deterministic operations can be excluded. This hinders wide- spread relinquishment because it requires inventors writing smart contracts to learn a new language and may lead to programming crimes. Farther, since all deals are executed successionally by all nodes, performance and scale is limited. The fact that the smart contract law executes on every nodes in the system demands that complex measures be taken to cover the overall system from potentially vicious contracts in order to insure resiliency of the overall system.

4) Privacy and Confidentiality

In a public, permissionless blockchain network that leverages PoW for its agreement model, deals are executed on every node. This means that neither can there be confidentiality of the contracts themselves, nor of the transaction data that they reuse. Every transaction, and the law that implements it, is visible to every node in the network. In this case, we've traded confidentiality of contract and data for intricate fault tolerant agreement delivered by PoW. This lack of confidentiality can be problematic for numerous business/enterprise use cases. For illustration, in a network of force- chain mates, some consumers might be given favored rates as a means of either solidifying a relationship, or promoting fresh sales. However, it becomes insolvable to maintain similar business connections in a fully transparent network If every party can see every contract and sale. Cracking data is one approach to furnishing confidentiality; still, in a permissionless network using PoW for its agreement, the translated data is sitting on every node. For numerous enterprise use cases, the threat that their information could come compromised is inferior. Zero knowledge attestations (ZKP) are another area of exploration being explored to address this problem, the trade- off then being that, presently, calculating a ZKP requires considerable time and computational coffers. In a permissioned environment that can work alternate forms of agreement, one might explore approaches that circumscribe the distribution of non public information simply to authorized nodes.

Hyperledger Fabric, being a permissioned platform, enables confidentiality through its channel armature and private data point. In channels, actors on a Fabric network establish a sub-network where every member has visibility to a particular set of deals. Therefore, only those nodes that share in a channel have access to the smart contract (chaincode) and data transacted, conserving the sequestration and confidentiality of both. Private data allows collections between members on a channel, allowing much of the same protection as channels without the conservation outflow of creating and maintaining a separate channel.

5) Pluggable Consensus

The ordering of deals is delegated to a modular element for agreement that's logically severed from the peers that execute deals and maintain the tally. Specifically, the ordering service. Since agreement is modular, its perpetration can be acclimatized to the trust supposition of a particular deployment or result. This modular armature allows the platform to calculate on well- established toolkits for CFT (crash fault-tolerant) or BFT (intricate fault-tolerant) ordering. Fabric presently offers a CFT ordering service perpetration grounded on the etcd library of the Raft protocol.

6) Performance and Scalability

Performance of a blockchain platform can be affected by numerous variables similar as transaction size, block size, network size, as well as limits of the tackle, etc. The Hyperledger Fabric Performance and Scale working group presently works on a benchmarking frame called Hyperledger Caliper.

Combined, the secerning capabilities of Fabric make it a largely scalable system for permissioned blockchains supporting flexible trust hypotheticals that enable the platform to support a wide range of assiduity use cases ranging from government, finance, supply- chain logistics, healthcare and so much more.

The community erecting around the platform is growing steadily, and the invention delivered with each consecutive release far out-paces any of the other enterprise blockchain platforms.

V. IMPLEMENTATION

The COVID19 pandemic paralyzes access to the world's healthcare systems with unprecedented blockades and forced physical distances, rapidly accelerating the development of these digital technologies to meet the diverse medical needs of the world. A wide range of digital technologies are being adopted for large-scale operational coordination such as high-population-level screening, rapid contact tracing, vaccine and drug supply chain management, telemedicine consultations, and e-commerce expansion. The COVID-19 outbreak highlights the need for a secure, decentralized, multi-purpose platform for coordinating the large-scale transmission of sensitive information, such as contact tracing, vaccination status monitoring, and COVID-19 health certificate issuance. Decentralized medical data management that handles on-chain events (transactions recorded in the blockchain ledger) and off-chain events (occurs outside the blockchain and is usually too large to handle) by integrating blockchain technology.

We implement a blockchain-based digital health passport. The system ensures that the generated covid19 certificate is valid and has not been tampered with by other sources. This system helps to preserve and share the health of an individual while at the same time protecting the privacy of the individual for migration purposes.

In figure 3, the user registers himself to the vaccination authority by entering his details , here Aadhaar number is considered as the primary key. A registered vaccinator of vaccination center will enter users Aadhaar number and will update users vaccination details in the vaccination center and also provide the update to users. Similarly, a registered covid tester of testing center will enter users Aadhaar number and will update users testing details in the testing center and also provide the result to users. If test result is positive , the users goes in recovery mode and his details are entered in the recovery center. All this is done through a permissioned blockchain which is a chain of various health centers connected together to form a network. Aadhar number is used to register to health center, to see and update vaccination details, Covid testing results, Recovery details and also for verification purpose.

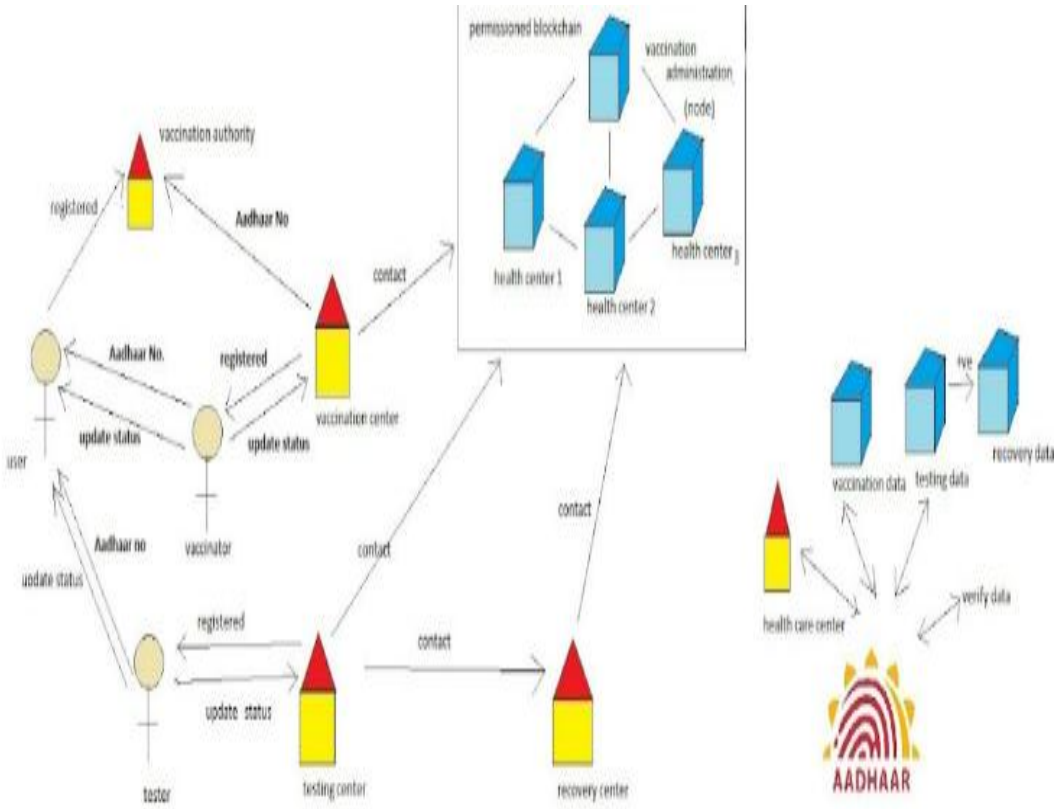


Fig 3: An architectural framework for Digital Health Passport

VI. TESTING

A. Introduction

Since blockchain is a public distributed ledger, there is always a possibility that someone observing or mining your transaction could obtain your private key or steal cryptocurrency from your wallet. Because of this, blockchain uses encryption and decryption to secure your wallet and ensure that only the owner can see the private information in it. The digital signature required for a successful transaction on the blockchain network is performed by your pair of asymmetric keys, but your private key is not visible when reading your transaction on another network. Other than that asymmetric cryptography is used to secure the blocks on the blockchain.

The majority of blockchain networks don't guarantee anonymity or use encryption (instead opting for pseudonymity - the pseudonym being your wallet address).

However, they all employ cryptography (digital signatures, hashing, stuff like that).

A hash is a fixed-length text that adds an encryption layer over a block to prevent manipulation of the blockchain. It is a process that changes input data of any length into an output of a specific length.

The hash generated by given set of data which remains same. However, even a small change in the data will cause the hash to change. As was previously indicated, each block contains the hash of the block before it, thus we will use our hashing method to obtain the hash of the current block from the data of the prior block. If a blockchain has been modified, it can be determined by comparing the thus obtained hash to the hash already contained in the current block

B. Blockchain Testing Life Cycle

The block-chain technology has a unique testing lifecycle known as the Blockchain oriented software (BOS) life cycle, which primarily entails four distinct phases.

1) Phase 1: Analysis

The first stage of testing is completed in this phase, which also involves the functional workflow and system component mapping.

2) Phase 2: Mapping

The preparation of the test strategy document occurs at the end of this phase, which is the second in the testing workflow. Here, blocks are mapped, use cases are outlined, and the security of the system is verified.

3) Phase 3: Apply Methodologies

In the third phase, testing methodologies, coverage estimates, tool testing, automation testing, use case mapping, and the creation of the final test strategy and test case are all completed.

4) Phase 4: Test EXECUTION

The test execution, low-level verification, and validation of blocks, smart contracts, and transactions take place in this phase, which is also the last in the testing lifecycle. The result is the final report, test results, and defect report.

C. Test Strategies For Blockchain

1) One of the key challenges is the Block Size Testing, which is done on block load. Block testing is done to test each block with respect to the information stored in it, the hash present on each block, content of previous hash, and so on are tested in the block testing as misplacing of hash may leads to the breakage of the chain.
2) The major purpose of security testing, which is a non-functional test, is to assure system security and to look for threats like viruses and other dangerous programs. Confidentiality, denial of service, availability, and integrity are a few crucial components of security testing, which is considered as being the most crucial testing.

D. Hyperledger Testing Tool

In order to test an app before it is released, it is helpful to use the testing tool known as Hyperledger Composer, which is primarily useful for interactive and automated unit testing. Hyperledger Composer is an open source, collaborative project that is used in the use of industrial Blockchain technology.

1) API Testing

API testing is performed in order to keep a check on the interaction of the Blockchain application ecosystem. It is done to see that requests and responses sent are valid.

Function	status	Time(online)	Size(online)	Time(curl)	Size(curl)
queryalldata	200(ok)	182ms	2.86kb	347ms	3.14kb
Querydetails	200(ok)	143ms	0.26kb	332ms	0.26kb
Queryvaccdetials	200(ok)	169ms	0.10kb	139ms	0.10kb
Register	200(ok)	2674ms	0.03kb	109ms	0.03kb
update	200(ok)	2466ms	0.03kb	2497ms	0.03kb

Fig 4: Size comparison of online tool with Curl tool

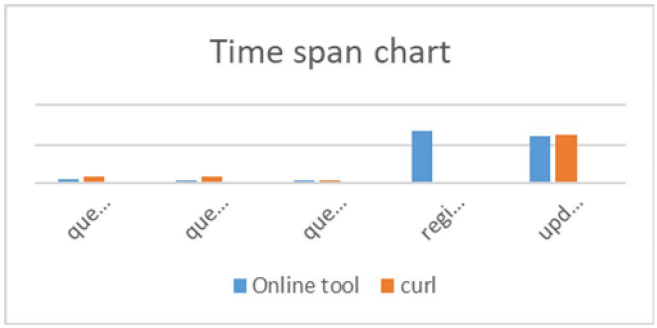


Fig 5: Time comparison of online tool with Curl tool

API Tester affords millisecond correct timings for API requests and server responses. Curl Client affords millisecond correct timings for Curl requests and server responses, consisting of DNS Resolution, Connection, TLS Setup, and facts switch times. As we can see that the time varies while testing through online tool and through curl command.

We can get bad request when: You selected 'application/json' content type, but the provided string is not a valid JSON string so by applying proper string we can get valid result.

When we receive status above 200 that is bad request which will be encounter when there is no valid string

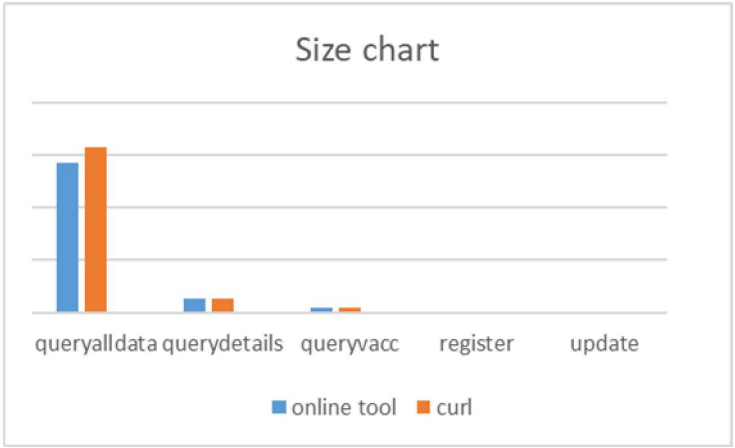


Fig 6: Size comparison of online tool with Curl tool

Size of the transaction are shown above have in KBs and can also receive in MBs and may vary with respect to time.

As we can see that there is no much difference between the size in curl tool representation also in online tool.

2) Architectural Testing

Hyperledger Fabric is an open- source platform for erecting distributed tally results, with a modular armature that delivers high degrees of confidentiality, inflexibility, resiliency, and scalability. This enables results developed with fabric to be acclimated for any assiduity

Workflow:

a) For each and every transaction in the fabric, the following steps are followed-
b) Creation of the proposal
c) Endorsement of the transaction
d) Submission to ordering service
e) Updating the ledger

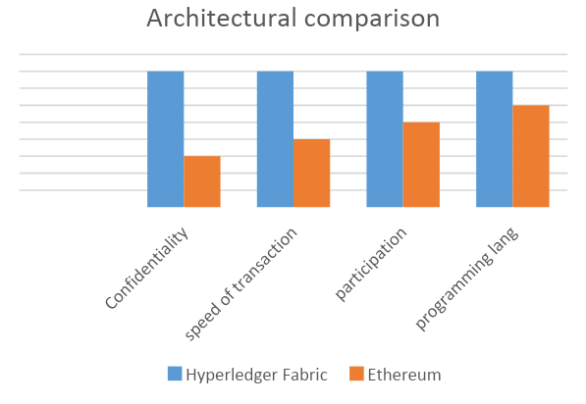


Figure 7: Overview of Hyperledger comparison to Ethereum

3) Security Testing

The purpose of performing security testing is to make sure that the blockchain application is completely secure against any malware and viruses.

The hash- function takes some block title information (timestamp, nonce, a hash of all deals) and returns similar a hexadecimal value. There's no way to crack such a hash. Its reason is just to identify a unique block (and deciding whether someone gets the block price or not).

Data on a blockchain will never be deleted. A omission is just another transaction saying certain data is deleted, so that the world state database (the DB with then on-deleted word) can remove that data.

Since a blockchain is a Merkle Tree in the background it plays by those rules and is inflexible. Data will always be there unless the tally and deals are removed from the machines, similar as resuming the network and removing all the information from the peers. That is principally a wipe of every machine that was used for the network structure holding the tally.



Figure 8: Hyperledger Explorer Blockchain Insight

To decrypt any hash value, we need a secret key so deletion and malfunctioning with the hash values is quite difficult. As the data hash are immutable no value will be changes hence every time new block will get added to node.

VII. RELATED WORK

Mauro Alberto de los Santos Nodar 1, and Tiago Manuel Fernández Caramés proposed a system with automated intelligence for the storage of the COVID-19 medical information (vaccines and tests) using blockchain technology and includes a DApp to make use of the system and a cryptocurrency to offer as a reward to the users who employ the system.

Mohamed Torky and Aboul Ella Hassanien proposed an approach to automatically detect infected cases and estimate the infection risk of the COVID-19 in society using blockchain. The decentralisation property of blockchain is utilised by the authors to store the information and medical data of the confirmed COVID-19 cases.

Jose L. Hern ´ andez-Ramos, Georgios Karopoulos, Dimitris Geneiatakis, ´ Tania Martin, Georgios Kambourakis, and Igor Nai Fovino proposed a system which uses a blockchain technology to store all relevant information about the vaccination process and registration of national medical centres.

Haya R. Hasan , Khaled Salah 1, Raja Jayaraman, Junaid Arshad et al proposed a blockchain based system that offers tracking and tracing of COVID-19 test-takers. The proposed solution implements digital medical passports (DMP) and immunity certificates for COVID-19 test-takers which leverages the use of the immutable events and logs of the distributed blockchain ledger without relying on any on-chain storage.

An EU Digital COVID Certificate is a digital proof that an EU citizen has either been vaccinated against COVID-19, has received a negative COVID test result or recovered from COVID-19. It contains a QR code with a digital signature which protects it against falsification.

VitalPass is the first blockchain-based system used to track COVID-19 vaccination through advanced blockchain technology and was launched in Colombia. It guarantees security, traceability, and transparency during the vaccination process.

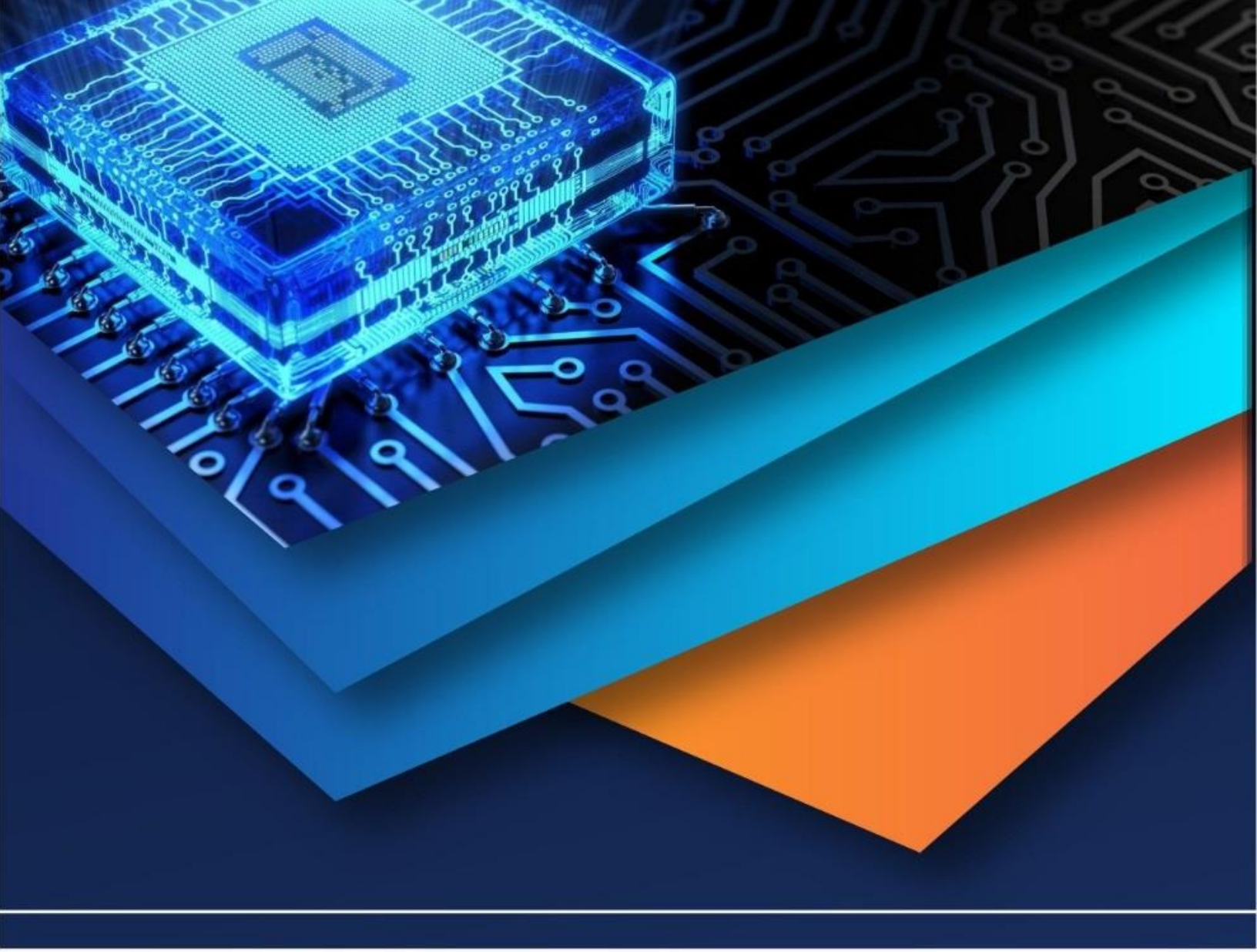
VIII. CONCLUSION

We are trying to set up a digital health passport with the aim of having verifiable data, immutably stored on decentralized distributed lager with key component of maintaining privacy of every individual and every individual maintaining self-sovereignty of their data and data should be trustworthy, open and transparent authorship to know who wrote the data on to the chain and an entirely auditable and traceable data of the on chain transaction. We are working on blockchain technology with a test network on an Hyperledger Fabric blockchain, interacting with chaincode (Smart contracts).

REFRENCES

[1] Mauro Alberto de los Santos Nodar 1 and Tiago Manuel Fernández Caramés, " COVID 19 Digital Vaccination Passport Based on Blockchain with Its Own Cryptocurrency as a Reward and Mobile App for Its Use" ,October 2021
[2] M. Torky and A. E. Hassanien, ''COVID-19 blockchain framework: Innovative approach,'' 2020, arXiv:2004.06081. [Online]. Available: http:// arxiv.org/abs/2004.06081/
[3] Jose L. Hern ´ andez-Ramos, Georgios Karopoulos, Dimitris Geneiatakis, ´ Tania Martin, Georgios Kambourakis, and Igor Nai Fovino, " SHARING PANDEMIC VACCINATION CERTIFICATES THROUGH BLOCKCHAIN: CASE STUDY AND PERFORMANCE EVALUATION", January 2021
[4] Haya R. Hasan , Khaled Salah 1, Raja Jayaraman, Junaid Arshad, Ibrar Yaqoob Mohammed Omar and Samer Ellahham, "Blockchain-Based Solution for COVID-19 Digital Medical Passports and Immunity Certificates" , December 2020
[5] Neeraj Kumar Muhammad Khurram Khan Shuyun Shi Debiao He and Kim-Kwang Raymond Choof. "Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey." In: NCBI. 2020.doi: 10.1016/ j. cose.2020.101966.
[6] Dr. Stefan Beyer. Blockchain Before Bitcoin: A History.
[7] Different Types of Hyperledger Technologies. https://medium.com/@vinshublockcluster/ different-types-of-hyperledger-technologies 929a67c98c32
[8] Ying-Chang Liang. "Blockchain for Dynamic Spectrum Management." In: Dynamic Spectrum Management, Signals and Communication. Research Gate. 2020. doi: 10.1007/978-981-15-0776-2_5.
[9] AKM Bahalul Haque , Bilal Naqvi , A. K. M. Najmul Islam and Sami Hyrynsalmi "Towards a GDPR-Compliant Blockchain-Based COVID Vaccination Passport " 1 July 2021
[10] Constantinos Marios Angelopoulos , Amalia Damianou and Vasilis Katos "DHP Framework: Digital Health Passports Using Blockchain"19 may 2020
[11] Ravens-Sieberer, U.; Kaman, A.; Erhart, M.; Devine, J.;Schlack, R.; Otto, C. Impact of the COVID-19 pandemic on quality of lifeand mental health in children and adolescents in Germany. Eur. Child Adolesc. Psychiatry 2021, 1–11. [CrossRef]
[12] Coronavirus Update (Live): 74,746,810 Cases and 1,659,186 Deaths from COVID-19 Virus Pandemic—Worldometer. Available online: https://www.worldometers.info/coronavirus/ (accessed on 5 May 2021).
[13] Dash, D.P.; Sethi, N.; Dash, A.K. Infectious disease, human capital, and the BRICS economy in the time of COVID-19. MethodsX 2021, 8, 101202. [CrossRef]
[14] Alfano, V.; Ercolano, S. The Efficacy of Lockdown Against COVID-19: A Cross-Country Panel Analysis. Appl. Health Econ. Health
[15] Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2009. Available online: https://bitcoin.org/bitcoin.pdf (accessedon 10 April 2021).
[16] https://bbrc.in/wp-content/uploads/2021/03/Spcial-Issue-13-13-39.pdf
[17] Huaqun Guo, Xingjie Yu "A survey on Blockchain technology and its security" June 2022
[18] Hai Wong, Yong Wng, Zigang Cao, Zhen Li, Gang Xiong "An Overview of Blockchain Security Analysis" 20 February 2019

[19] Dr. Stefan Beyer "Blockchain Before Bitcoins" 23 August 2018
[20] Wei Yan Ng, Tien-En Tan, Prasanth V H Movva, Andrew Hao Sen Fang, Khung-Keong Yeo, Prof Dean Ho "Blockchain applications in health care for COVID-19 and beyond: a systematic review" 12 October 2021
[21] Sheikh Mohammad Idrees, Mariusz Nowostawski, Roshan Jameel, Ashish Kumar Mourya "Security Aspects of Blockchain Technology Intended for Industrial Applications" 16 April 2021
[22] Haya Hasan, Khaled Salah, Raja Jayaraman, Junaid Arshad "Blockchain based Solution for COVID-19 Digital Medical Passports and Immunity Certificates" August 2020
[23] Gwyneth Iredale "What Problems does Blockchain solve?" 05 January 2021
[24] Rizwan Khan, Akhilesh Kumar Srivastava, Dilkeshwar Pandey" Agile approach for Software Testing Process" January 2016
[25] Soumya, Naresh E, Vijaya Kumar B P, Ravi B C "Test Strategies for Blockchain Technology" 15 October 2021
[26] KC Tam "Deep-Dive into Fabcar" 29 August 2019
[27] Aakanchha Keshri "How to perform BlockchainPenetration Testing" 5 March 2022
[28] Graham Shaw "Penetration Testing Technical Report" 8 August 2019
[29] Tevora Threat Research Group "2021 Hyperledger Fabric Penetration Test" 22 March 2021
[30] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends" June 2017
[31] Mohammed Zubair "Blockchain: Internet 3.0" May 2018
[32] Aakanchha Keshri "How to perform Blockchain Penetration testing?" July 2022
[33] Akash Kumarsen "Hyperledger Fabric in Blockchain"11 May 2022



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)