***The emergence of cybersecurity with the rise of blockchain technology***

Vivek Singh Dudy 20BCE1306

Vipul Tiwari   20BCE1467

SCOPE                                                                                           Vit Chennai

**Abstract-**

Due to its popularity, blockchain has been a trending topic in the technological world in recent times. Through the use of blockchain technology, any type of data or digital asset is rendered unalterable and transparent. A brief description at the start of the paper explains the workings of "blockchain technology," and the paper tries to explain the basic terminologies of the technology and reasons why it is on trend today. In the following part, the paper focuses on the topic of cyber security. Since the first computer bug was discovered, potential hackers have always tried to take advantage of those bugs in order to access important data like bank details in order to create chaos in the system. Therefore, there is a constant need to modify the security to ensure breach-less data transactions. Finally, the research sheds light on the feasibility of using Blockchain technology in cybersecurity and how it can be strengthened with the use of this trending technology in the coming years.

**Key-word**: Blockchain, Ethereum, Solidity, Truffle, spoofing, ddos attack

**Introduction-**

The largest and most well-known cryptocurrencies today are Bitcoin and Ethereum. One of these currencies is mentioned in the news almost weekly, and many people are interested in learning more about them. The paper presents blockchain technology and outlines the fundamental ideas behind how a secure electronic transaction system will operate. Ethereum is a new cryptocurrency built on the Bitcoin blockchain. Ethereum is much more versatile than just an internet currency. Even though the names of the currencies are well-known, few people are aware of how these cryptocurrencies actually operate. Therefore, by describing and comparing the two cryptocurrencies, we provide insight into Bitcoin and Ethereum via this study. We will explore-

·        All the algorithms these cryptocurrencies use.

·        Requirements for an online currency to function.

·        Comparison of the two cryptocurrencies.

Attack vectors at the application, contract, and network layers The application layer is responsible for transporting blockchain technology and providing solutions for a variety of business scenarios. Security flaws in various trading platforms and user accounts seriously jeopardise the asset security of blockchain wallet users.

Ethereum is an open-source public chain platform that executes intelligent contracts using Ethereum virtual machines. These machines carry out intelligent contracts by consuming Ethereum coins. The cryptocurrency Ethereum is frequently referred to as "the world's computer." etgereum  uses blockchain to sync up and store system state, and Ether cryptocurrency to calculate and limit execution resource cost. Ethereum developers can use Ethereum virtual machines to create decentralised applications and smart contracts. While maintaining stable and normal operation, it can also minimize or eliminate examination procedures, saving resources and lowering risks by removing third-party participation.

Ethereum provides utility and creates value in a wide range of industries. From healthcare to entertainment to real estate, industries are developing novel protocol-based tools to improve efficiency, trust, and democratise access to various types of services.

By distributing tokens that represent ownership rights, Ethereum provides an ideal solution for handling royalty payments in the music industry by facilitating computer controlled and effortless distribution of royalty payments.  Mediachain, and the Open Music Initiative are all Ethereum projects that work in the music industry.

Through verifiable blockchain-based cryptography, Ethereum's tamper-proof blockchain-based ledger can reassure supply chain and logistics managers about the provenance of products.

**Related works-**

In-depth assessments of the differences between Bitcoin and Ethereum have not yet been made. Various publications and discussions compare a few minor components, and Ethereum was created in response to Bitcoin interest. A user-friendly architectural design for blockchain-focused apps is proposed, as well as a method for determining which components of local application architecture can benefit from using Ethereum. The first dependency to set up is the Node Package Manager (NPM), which comes with Node.js. Truffle, on the other hand, is a development environment that assesses Ethereum's framework.  The package includes an auto launching local blockchain development server for Truffle.`1 In DApps applications, solidity is utilised to create smart contracts. Solidity is primarily made to construct contracts for the Ethereum platform and incorporates object-oriented characteristics. Programs written in Solidity can be tested and debugged on Remix and Visual Studio Code. When using Remix in a web browser, VS code can be installed on a PC and used offline. It is now easier to write and debug Solidity contracts. Because it is written in JavaScript, Remix can be used both locally and in the browser. Smart contracts are deployed, tested, and debugged using Remix. [1]

Ethereum is a public, distributed ledger that is both popular and decentralized. Ethereum's decentralized nature means that the final state is determined by the Ethereum network itself, using a consensus procedure that does not depend on a single, authoritative coordinator. No transaction in the network, not even the genesis block, can be trusted without being scrutinized by other nodes. [2] For many mobile devices with insufficient processing power or spotty internet access, this is just not feasible. Ethereum proposes a light client protocol to address this problem by having the light client acquire the blockchain state from a node performing the role of a light protocol server. For this reason, light clients can only validate some of the blocks of a transaction since they cannot store the whole blockchain locally. Consequently, they depend on the lite server to provide them with the latest blockchain state and to do comprehensive block validation. To prevent trusting a single potentially fraudulent server, light clients establish connections with many light servers.The blockchain is a data structure based on timestamps. Each block consists of a header and a body. The genesis block is the first block of the Blockchain, and it has no parent block.  The body of the block consists of transaction counters and transactions.

The size of block and the length of each transaction determine the maximum volume of transactions in one block. Furthermore, to validate data transaction authentication, Blockchain employs an asymmetric encryption mechanism. In an unreliable environment, an asymmetric cryptographic digital signature is used. [3]

Data can be added to a distributed ledger thanks to blockchain technologies. One crucial point is that confidence is dispersed among all nodes, negating the necessity for a single, centrally located trusted party. Consequently, a consensus must be obtained among all (or enough) engaged nodes in order to add data to the ledger. [10]

Individuals' sensitive personal information as well as other expensive resources held by third parties are constantly at risk. There are more opportunities for resource misuse. The use of best practices to execute processes successfully is more crucial and necessary to overcome problems with interoperability. The cryptocurrency has been broadly accepted and used in a multitude of sectors where users don't really trust service providers and seem to be aware of how their personal data is being acquired and used.[4]

There is no way to prevent hostile nodes from connecting to the network, making these network attacks unavoidable. By looking at the infrastructures of wallets and the various storage methods, we furthered our investigation into storage security. We concluded that storage security and usability are trade-offs. We also aimed to increase reader awareness of new altcoins with cutting-edge security and privacy features.[5]

When Ethereum is implemented over a WAN, an adversary with direct authority over their boundary gate could quickly double-spend using Node hijacking, with a success rate of up to 80%. Similarly, using ARP spoofing, an attacker can double-spend with an achievement rate of up to 80%.  The number of confirmations can be increased as a short-term strategy. The long-term ones involve actively monitoring the network. We will continue to work on active monitoring in the future.[6]

 One attack that has the potential to expose holes in the authentication procedure is the MITM attack. Block hashing, a feature of blockchain technology, can be utilised to prevent [12] MITM attacks and other authentication process flaws. The hash block technique transforms the plaintext authentication payload data into ciphertext data by block hashing it. Based on the outcomes, it can be concluded that the use of Blockchain technology has been successful in protecting an information system's authentication payload data against MITM attacks. [7]

Through the development of RF embedded technology, drivers can instantly access a variety of services. However, these systems are susceptible to assaults like MIMA, impersonation, and major disclosure over public channels. For radio frequency networks, the most widely used encryption methods, such DES and AES, are perfect. In order to protect users' privacy, there are strong security standards for secure authentication and a key agreement. To address these concerns, a secure authentication method based on smart blockchain contracts that provides high efficiency, personal privacy, untraceability, and secure mutual verification has been developed. [8]

Ethereum can be thought of as the Bitcoin blockchain's expansion to support more varied applications. Therefore, blockchain technology makes it possible to create contracts using cryptography and eliminates the need for third parties (like a notary) who were previously required to establish confidence. Blockchain's ability to execute contracts automatically in a safe, transparent, and cost-effective manner has the potential to upend the entire transaction process.[13]

[15] Ganache is used to create a private Ethereum Blockchain for evaluating Solidity contracts. When compared to Remix, it has more features. When you use Ganache, you will discover about the features. You must first simply download the Blockchain on your local machine before you use Ganache.

There is no uniform set of guidelines or constant procedures that applies to the international supply chain. These regulations allow for cross-national monitoring of certain economic sectors. [17] To solve this problem, the Blockchain age has emerged. Currently, assets can be tracked more precisely than ever before. Throughout this research, we propose a commodity traceability network based on blockchain technologies, which completely stores all commodity history in a global database via clever contracts and creates a chain that can hint back to the supply of goods. To confirm the events' authenticity and guarantee the validity of the deal, we built an incident management system. To further monitor conflicts and punish responsible companies, detailed records of all occurrences are kept. [19] First, the Blockchain incorporates a user login form; next, it adds the capability to include an entry of the inventory-keeping unit into the distributed ledger.

Blockchain is a zero believe network and this makes it a totally powerful tool for various services provided that people are prepared to believe and spend money on it. [20] In the Ethereum global, the blockchain runs on clever contracts which can be self-executing programs that come at a cost of protection. This zero-consider network is capable of changing the various debated process or sports in our each day existence.

Ethereum blockchain's security threats, attack scenarios, and mitigation strategies. Ten security breaches were investigated at Ethereum has several layers, the most important of which are the application layer, the smart contract layer, and the network layer. The automatic cross-chain attack detection is another important research direction for us.[21]

P2P cryptocurrency network dependability is built on a strong redundant mechanism for system information. Each network node stores all relevant network data. The accessibility of a single node in a network holds the data needed to keep all processes operational with this method. Because this method is inefficient in terms of storage space, it is not used by any other P2p framework. Furthermore, in order to provide all nodes with the same correct information, such things are made the development of new synchronisation mechanisms. Information duplication can also be used to protect network topology. Eclipse attacks are the most popular type of cryptocurrency attack, in which a defendant or a fraction of the network is separated. Such attacks can occur when an attacker takes advantage of his location in the topology of the network. To avoid this possibility, the entire network must be secured, and cryptocurrency networks use two distinct methods to accomplish this. Cryptocurrency channels are not multihop networks, and nodes in the network are only conscious of one-hop neighbours. Because information is replicated in every network node, this method removes providing routing information to nodes in the network and eliminates information availability constraints. When endpoints connect to the network, network topology disclosure must be protected. To obstruct the network's topology structure, cryptocurrency P2P networks use a randomly generated technique to estimate each node connection during this phase. It's important to note that this topographic secrecy estate of P2P cryptocurrency networks isn't as essential in other P2P network paradigms, so the mechanisms for achieving it also are unique to such surroundings. Furthermore, because of the nature of the data flowing in cryptocurrency channels, some mechanisms designed specifically for other P2p frameworks are not needed. This is an instance of multiple secure safeguards trying to prevent various attacks. Inherent cryptographic properties of blocks and transactions.[22]

A significant portion of current Ethereum research focuses on smart contract vulnerabilities and Ethereum-specific issues. This article investigated the attacker and proposed a method for tracking the attacker using graph analysis. Traceability assessment of re-entry threats, Denial - of - service, short address threats, and Ponzi contracts reveals that the attackers are interrelated, and a large number of active accounts remain. Finally, we can use the RPC mechanism to determine the Ip's of particular attackers. With these findings, we can investigate specific attacker behaviour in order to enhance Ethereum's safety. [23]

Security flaws in the Ethereum blockchain, the attack vectors such flaws open up, and the solutions to those flaws. The 10 identified security concerns mostly affected Ethereum's application layer, smart contract layer, and network layer. The research provides extensive detail on the matched preserved techniques, which are categorized in terms of their various attack conceptions. Improving the quality of all Ethereum smart contracts might go a long way toward preventing attacks. Finally, we put these numerous safeguards to the test via a battery of tests. DDoS Attacks on the App Layer The blockchain technology is transmitted and many business problems are addressed via the application layer. Inadequate security measures on a myriad of exchanges and user accounts pose a significant risk to the funds stored in blockchain wallets. So, we'll check over three of the most common attack strategies.

When executing a replay attack, information from previously completed transactions may be re-played. The user composes some preliminary text, sends it to the contract, and finally verifies the signature by consulting the terms of the agreement.

On the other side, anybody may have access to the user's signature data since it is publicly available online. An attacker may preserve the user's signature and counterfeit transactions to their benefit if the signed message does not contain random variables that vary dependent on the number of transactions, such as a timestamp, nonce, and so on. This is due to the fact that the attacker may now authenticate the user's signature inside the contract. It's often believed to mean making many transactions with the same payment information (the same credit card, for example). Following the hard split, two separate blockchains, Ethereum and Ethereum Classic, were created, and it was discovered that transactions made on Ethereum could be replayed without issue on Ethereum Classic. As a result of the hard split, we uncovered this.

An offensive against the top-up hoax. The status field in a transaction receipt for Ethereum tokens indicates whether or not an error occurred while the transaction was being processed. If the user calls the token contract's transfer function and it runs without throwing any problems and at the expected frequency, the transaction is regarded to have succeeded. There will be a massive sham top-up attack if digital currency exchanges, wallets, and other systems can't reliably tell whether token recharge operations were successful. The program will go on to the else logical block even if balances[msg.sender] returns a false result without throwing an exception. The transaction was completed successfully, and the user was issued a legitimate recharge record, despite the fact that the exchange was not supplied with the genuine tokens throughout the attack. In this case, users may take real things from a physical location. As the so-called fraudulent top-up assault has developed, it has become a kind of attack that cannot be disregarded in the blockchain system.

Aiming to Disrupt the Dependence on the Sequence of Events in a Transaction.

When executing a replay attack, information from previously completed transactions may be re-played. The user creates a message from scratch, uploads it to the contract, and ultimately verifies the signature with the data stored there. On the other side, anybody may have access to the user's signature data since it is publicly available online. An attacker may preserve the user's signature and counterfeit transactions to their benefit if the signed message does not contain random variables that vary dependent on the number of transactions, such as a timestamp, nonce, and so on. This is due to the fact that the attacker may now authenticate the user's signature inside the contract. It's often believed to mean making many transactions with the same payment information (the same credit card, for example).

Transactions made on the Ethereum chain are remain valid when replayed on the Ethereum Classic chain, which was created after the hard split. The issue was identified after the hard split. In the replay attack, the settings may remain constant, but many transfers can take place. [24]

Since Bitcoin's rise to prominence, the idea of smart contracts has seen a renaissance. As both blockchain and smart contract technologies continue to develop and mature, they have become intrinsically intertwined. Consequently, this has made blockchain technology and smart contracts inseparable. One of the most important features of the blockchain is the ability to execute smart contracts, which is also the main reason why the blockchain may be considered a disruptive technology. Compared to the rapid evolution of commercial blockchain solutions, academic research on smart contracts is still in its infancy; hence, it is crucial that foundational technologies be researched and followed. This study did more than just establish the feasibility and show that it was possible to implement a smart contract model for a semi-public chain based on the Hyperledger architectural model and the Ethereum development environment. To demonstrate the evolution of blockchain technologies and the practical enhancements to smart contracts, we utilize two widely-used examples, Ethereum and Hyperledger. With the growth of blockchain technology in supply chain business circumstances and application areas, smart contract technology is expected to improve further in the near future. However, there are several opportunities to improve the system. To begin, just two blockchain technologies, Ethereum and Hyperledger, are considered by semi-public chain smart contracts. None of the other blockchain services are considered. Second, we failed to take into account the potential financial implications of the deals. As the price of Ether rises, the amount spent on transaction fees might become rather large. Finally, we assume a consistent supply chain process and don't account for a supply chain with numerous processes, which may be more representative of the reality. Research presented in this journal confirms the simulation's results, showing that smart contracts built on a semi-public chain may be used to effectively reduce user costs via better control of such costs. This method's limitations may be adjusted as needed. Smart contracts on semi-public chains are first examined only from a financial standpoint. It is possible that including revenue into this evaluation framework may allow for a more comprehensive analysis of the smart contract solution's value to its end users. Secondly, this article only takes into account the case where there is no centralized organization and the primary body of the centralized organization can be expanded in some way, such as by using the services of an impartial third party as a platform for providing services to the primary body of the centralized organization. Finally, we only include the most important parts of the supply chain; however, we may expand the supply chain business scenarios to incorporate additional supply chain modes, such as the closed-loop supply chain (CLSC) and environmental supply chain dynamics (ESCD). Finally, the paper solely covers Ethereum technology, which may be utilized to augment application infrastructure. Use cases include RFID (radio-frequency identification) management and double-chain architecture, both of which make use of blockchain technology.

This not only broadens the scope of the business situations described in this study, but also makes recommendations for future research. [25]

**Existing system**

Modern times are home to high-end laptops and powerful computers with parallel processors capable of doing calculations and computations at lightning speed. Although DES is an efficient algorithm, these gadgets may have compromised its security. So, the transposition cryptographic approach is added to the DES set of rules to give the highest possible security for the DES algorithm. Since the DES algorithm uses a 56-bit key, it is not necessarily secure against a Brute-force attack. The DES transposition technique is a sophisticated cryptographic procedure that may be used before of the DES ruleset to increase the key's strength.

Information is encrypted in 64-bit blocks using DES, making it a block cipher. The key length is 56 bits, and although 64 bits were used originally, it has since been reduced. We do not count bits 8, 16, 24, 32, 40, 48, 56, 64 as essential.

DES is based totally on fundamental attributes of cryptography:

Substitution (confusion) and transposition (Diffusion). DES consists of sixteen steps, every of that's referred to as as a Round

Algorithm: -

1. In the first step, the initial 64-bit simple textual content block is surpassed over to the Initial Permutation (IP) feature.

2. The Initial permutation is achieved on the apparent textual content.

3. The preliminary permutation produce two halves of permuted block: Left Plain textual content (LPT) and Right Plain Text (RPT).

4. Now, each of LPT and RPT is going through sixteen rounds of encryption manner, each with its own key:

a. From the 56-bit key, a one of a kind forty-eight-bit Sub-secret's generated using Key Transformation.

B. Using the Expansion Permutation, the RPT is expended from 32 bits to 48 bits.

C. Now, the 48-bit key is XORed with forty-eight-bit RPT and ensuing output is given to the next step.

D. Using the S-field substitution 32-bits are constituted of forty-eight-bits.

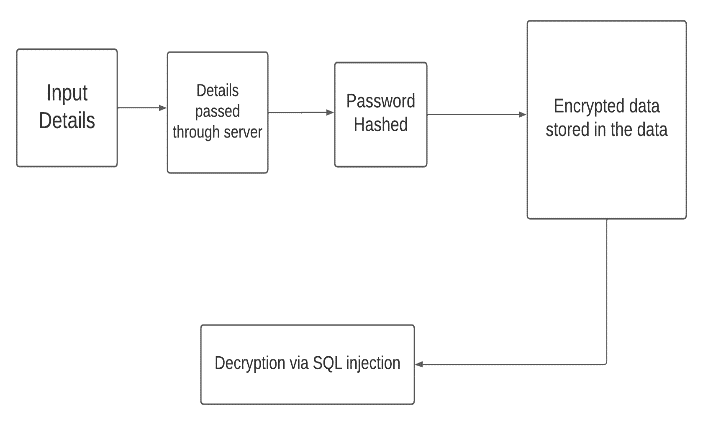
E. These 32 bits are permuted using P-Box Permutation.

F. The output of P-Box is XORed with the LPT that is of 32 bits.

G. The result of the XORed (32 bits) turns into the RPT and vintage RPT end up the LPT. This method is called as Swapping.

As an injection attack, SQL Injection (SQLi) allows malicious SQL queries to be performed. Using these directives, you may manage the database server behind your favorite web app. By exploiting SQL Injection flaws, attackers may simply get around application security measures. If the database is in SQL format, they may see all of its contents without registering or being given any special access. SQL Injection allows for a variety of changes to be made to the database, including the creation of new entries and the alteration or removal of existing ones. A website or web app may be vulnerable to SQL Injection if it interacts with a SQL database like MySQL, Oracle, SQL Server, or others. Theft of intellectual property, client information, and other sensitive data is a real risk if criminals get access to it. An SQL injection vulnerability is one of the most common and serious threats to websites and web-based applications. According to the 2017 OWASP Top 10 document, injections are the most serious vulnerability in online applications. Despite the common perception that blockchains provide a very high level of security, that level of safety really increases in direct correlation with the hash rate of the network. If there are many miners and their mining equipment is robust, it will be more challenging to launch a network attack. The most common forms of attack against public blockchains are covered here. Even while blockchains have a solid reputation for security, such security is only as strong as the hash rate of the underlying network. The network's defenses strengthen in proportion to the quantity of miners and the sophistication of their mining hardware.**Proposed system-**

*Architecture diagram-*

****

**Fig.1**

A Distributed Denial-of-Service (DDOS) assault is a kind of cyberattack in which the attacker tries to overwhelm a network in order to make a service it provides inaccessible to its consumers. It's an assault that doesn't only target blockchains, but any internet service.

All of these requests originate from the same machine in a Denial-of-Service (DOS) assault, which is the simplest kind of network intrusion. Because of this, avoiding it is easy. It is possible to implement a system that automatically rejects requests from a certain IP address if that address repeatedly makes requests that cannot be explained by valid use cases. The "distributed" aspect of a DDOS assault refers to the fact that the malicious requests come from many distinct places.*SQL injection attack – Algorithm-*

Print header information

for URL in target URLs

for payload in get request payloads

response = send get request probe to server

if response.status code == 500

print payload and exist for manual attack

for paylaod in post request payloads

response = send post request probe to server

*SQL injection attack [figure 1]*

Using the http 'get' method, this function sends a payload to the server. To accomplish this, the payload is appended to the URL. The request is sent to @params payload string via the url. The request parameters, such as requests.get t('http://www.test.com/', params=payload) will map to http://www.test.com/?key=value

###

def http\_get(url, payload):

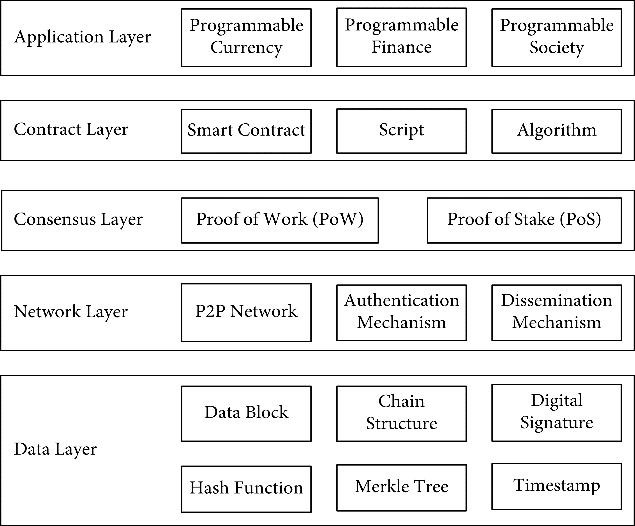
r = requests.get(url, params=payload)

return process\_responds(r)

###

This function examines the request to determine whether or not the probe is positive or negative.

*Ethereum architechture-*

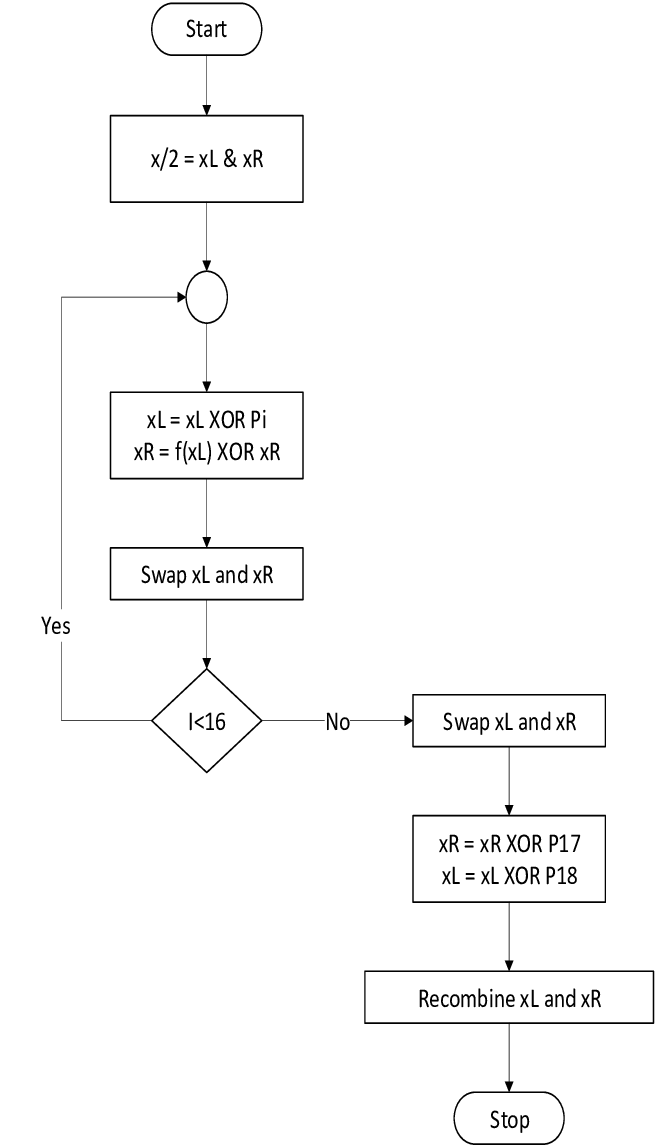
One common way to describe Ethereum is as "the world's computer." Ethereum is a globally accessible singleton state and a state-changing virtual machine, making it a deterministic but unbounded state machine in the context of computer science. Blockchain is used to synchronize and store the current state of the system, and Ether is used to determine and cap the cost of executing code. Ethereum allows developers to make decentralized apps and smart contracts that can be executed on Ethereum's virtual machines. While maintaining a safe and reliable system, this method can cut down on or even do away with the need for invasive inspections, saving time and money while also lowering risk by removing the need for outside parties.

**Figure 2**. Ethereum’s hierarchical structure.

***Web application architecture-***

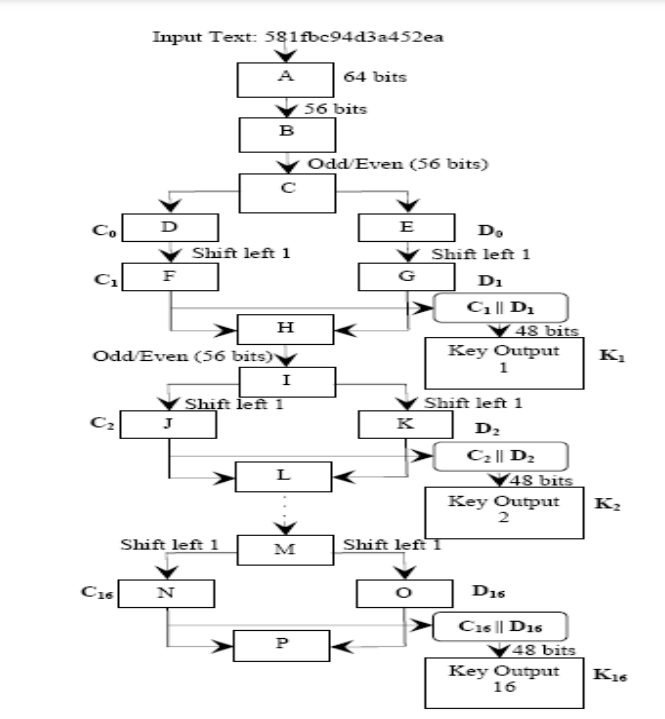
While it's important to bear in mind that Ethereum is a decentralized network, we need our frontend to be able to talk to our smart contracts so that they may call functions. The code and data associated with each smart contract are stored in a state machine that is replicated on every node in the Ethereum network.To access the information and programs stored in a blockchain, we must communicate with one of these nodes. This is because a request to execute an EVM transaction can be broadcast by any node. After a miner processes the transaction, the new state is broadcast across the network.

**Blowfish encryption algorithm-**



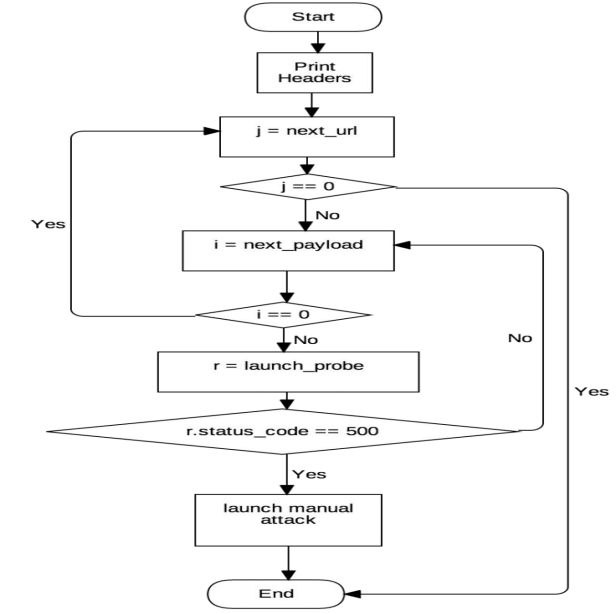
**Fig. 3** BlowFish Encryption Algorithm

In Figure 3, x is a 64-bit plaintext to be encrypted, and dummies are added to a plaintext that is less than 64 bits. X is divided into two equal 32-bit halves: leftmost plaintext (xL) and rightmost plaintext (xR) (xR). I is the number of iterations. p is an array of 18, 32-bit subkeys that are XORed with the leftmost 32-bits of plaintext and then passed to the blowfish f function. As shown in Figure 3, the result becomes the rightmost 32-bit for the next round, and the output of the F function is XORed with the original rightmost 32-bit of plaintext, becoming the leftmost 32-bit, and so on.



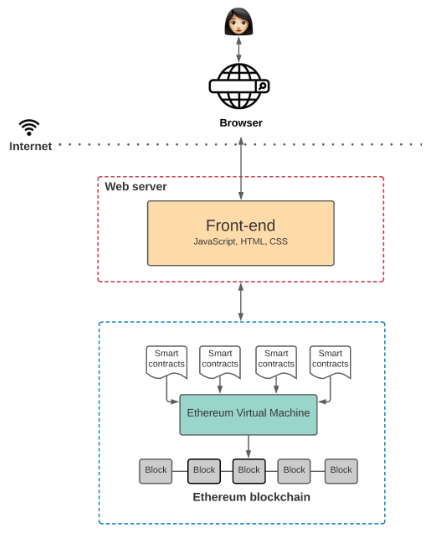
**Fig. 4** DES encryption algorithm

**DES encryption algorithm:  
In fig.[4],**Data encryption preferred (DES) has been determined susceptible to very effective assaults and consequently, the recognition of DES has been discovered barely at the decline. DES is a block cipher and encrypts statistics in blocks of length of 64 bits each, which means that sixty four bits of undeniable text move as the input to DES, which produces 64 bits of ciphertext. The identical set of rules and key are used for encryption and decryption, with minor differences. The key length is fifty six bits.

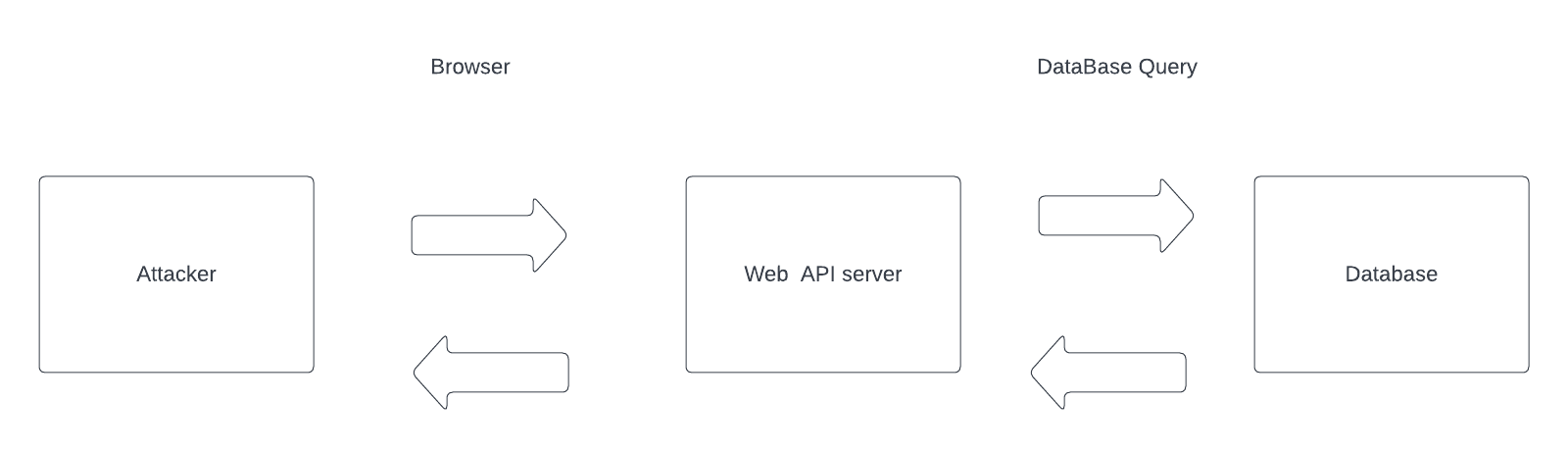


**Fig. 5** SQL injection attack-Flowchart SQL injection attack-Python script

When attackers are able to influence the queries sent by a website to a database, the website becomes vulnerable to SQL injection. [Fig. 5] This allows the attacker to extract information from the database or change its contents using, for example, a simple query.



**Fig. 6** The Architecture of a Web 3.0 application

****

**Fig. 7** The above figure gives a rough sketch about the SQL attack

**Algorithms**

**Algorithm1 :Python MD5/SHA password hash Generator sample code-**

**Input:** password (sequence of bytes)

**Output: 128-bit hash value**

1. Initialization:

import hashlib

s='password'

1. sb=s.encode("utf8")
2. print (hashlib.md5(sb).hexdigest())
3. (hashlib.sha256(sb).hexdigest())

Hashing is essentially a one-way ticket to data encryption. Hashing is a one-way transformation that converts a password into another String known as the hashed password. Because it is nearly impossible to recover the original text from a hash, it is referred to as one way hashing.

**Algorithm 2: blowfish algorithm**

**Input:** Plain text**,**18 subkeys in an array P, input key, Substitution boxes

**Output:** Cipher text(encryption), decrypted text(decryption)

1. Initialization:

uint32\_t P[18];

uint32\_t S[4][256];

1. uint32\_t f (uint32\_t x) {

   uint32\_t h = S[0][x >> 24] + S[1][x >> 16 & 0xff];

   return ( h ^ S[2][x >> 8 & 0xff] ) + S[3][x & 0xff];

}

1. **procedure** blowfish\_encrypt(uint32\_t \*L, uint32\_t \*R) {

**for** r = 0 to 16 **do**

                           \*L = \*L ^ P[r];

                           \*R = f(\*L) ^ \*R;

**swap**(L, R);

            }

**swap**(L, R);

            \*R = \*R ^ P[16];

            \*L = \*L ^ P[17];

}

1. **procedure** blowfish\_decrypt(uint32\_t \*L, uint32\_t \*R) {

**for** r = 17 to 1 **do**

                           \*L = \*L ^ P[r];

                           \*R = f(\*L) ^ \*R;

**swap**(L, R);

**swap**(L, R);

            \*R = \*R ^ P[1];

            \*L = \*L ^ P[0];

**End for**

1. **for** i = 0, p = 0 to 18 **do**

                           k = 0x00;

**for** j= 0 to 4 **do**

          k = (k << 8) | (uint8\_t) key[p];

                                        p = (p + 1) % key\_len;

**end for**

                   P[i] ^= k

**End for**

1. uint32\_t l = 0x00, r = 0x00;

**for** i = 0 to 18 **do**

**procedure** blowfish\_encrypt(&l, &r);

                           P[i] = l;

                           P[i+1] = r;

**End for**

**for** i = 0 to 4 do

**for** j = 0 to 256 **do**

1. **procedure** blowfish\_encrypt(&l, &r);

                                          S[i][j] = l;

                                          S[i][j+1] = r

**End for**

1. **End for**

**Tools-**

Node js - Node.js is an open-supply server surroundings. Node.js is move-platform and runs on Windows, Linux, Unix, Mac OS, etc. Node.js is a returned-cease JavaScript runtime surroundings. Node.js runs on a JavaScript Engine and executes JavaScript code out of doors an internet browser.

As a report-focused database application, MongoDB is open-source and accessible on the Go platform. MongoDB, which is categorized as a NoSQL database application, employs documents that are similar to JSON and have optional schemas. MongoDB Inc. is responsible for creating MongoDB. And it's licensed under the restrictive Server-Side Public License, which isn't included in many free software packages.

Ganache - Ganache is used to build up a personal Ethereum Blockchain to test your Solidity contracts. When put next to Remix, it has greater features. While working out with Ganache, you'll be learning about the many features. If you want to utilize Ganache, you have to first acquire the Blockchain app for your local device and install it.

Kali Linux is an open-source Linux distribution created specifically for doing information security-related activities including pen testing, security analysis, digital forensics, and reverse engineering.

Microsoft's Visual Studio Code (VS Code) is a cross-platform source-code editor that runs on Windows, Linux, and macOS and was built using the Electron framework. Debugging, syntax highlighting, intelligent code crowning splendor, snippets, code restructuring, and integrated Git are just some of the features.

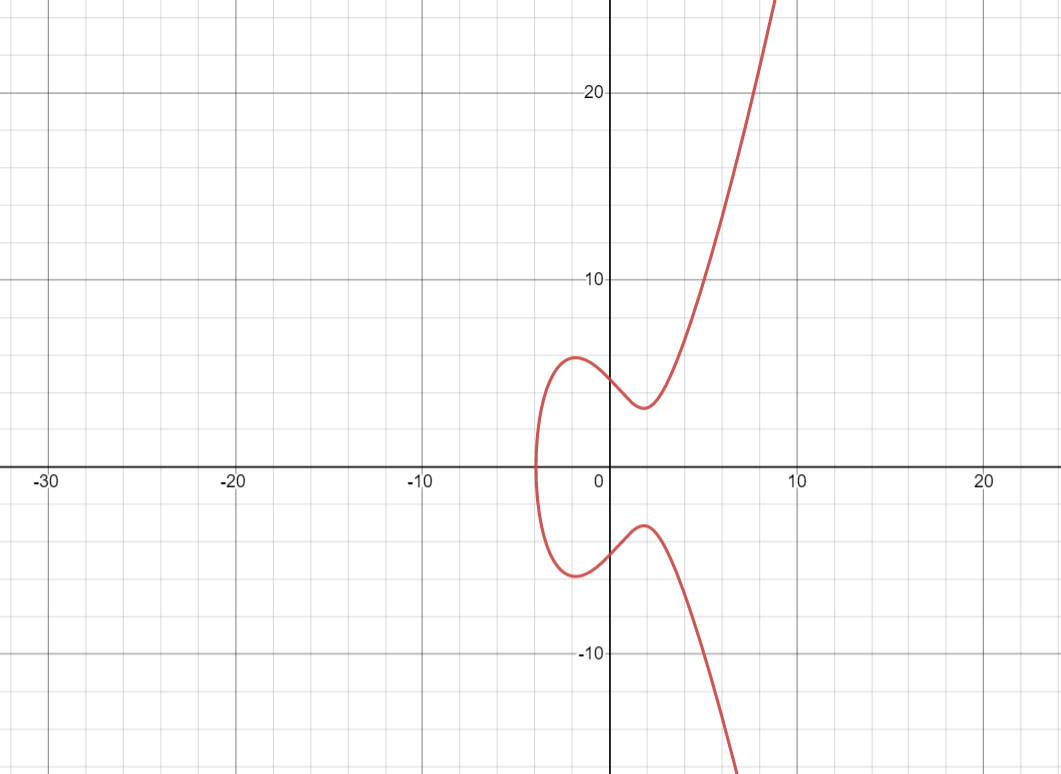
Git- Git is free and open source software for distributed version manipulate: monitoring alterations in any group of files, and is often used for coordinating work amongst programmers working together to develop source code during software development.

**Performance Evaluation and graphs**

**Fig.8** Distribution of Security attacks on daily basis

**Fig. 9** A comparison of cryptographic algorithms for Attack preventions

Elliptic Curve Cryptography (ECC) is a key-based method for encrypting facts. ECC (Fig. 9) focuses on pairs of public and private keys for decryption and encryption of web site visitors. ECC is regularly mentioned inside the context of the Rivest–Shamir–Adleman (RSA) cryptographic set of rules. RSA achieves one-manner encryption of factors like emails, records, and software program the usage of top factorization.



**Fig. 10** Elliptic curve cryptography (public key cryptography)

As a viable substitute to RSA, ECC is a strong cryptographic tool. Using the mathematics of elliptic curves, it creates a secure environment for key pairs in public key encryption.

While RSA does a similar task using prime numbers in lieu of elliptic curves, elliptic curve cryptography (ECC) has been gaining popularity as of late due to its reduced key size and ability to maintain security. Due to the increasing size of keys and the corresponding increase in demand for devices to maintain a comfortable temperature, this trend is likely to continue at the expense of increasingly limited mobile resources. This is why a thorough comprehension of the background of elliptic curve cryptography is essential.

ECC is an alternative to RSA for public-key cryptography that takes use of the elliptic curves' algebraic dependence over finite fields. In this way, ECC generates keys that are more difficult to decipher mathematically. Because of this, ECC is more secure than RSA and is considered the next generation of public key cryptography technology.

In addition to improving speed and security, using ECC makes logical sense. This is due to the fact that ECC is becoming increasingly popular as more and more websites recognize the need to safeguard their users' personal information while also optimizing for more mobile traffic. There is a growing need for a concise introduction on elliptic curve cryptography as the number of websites using ECC to secure data increases.

In modern ECC contexts, an elliptic curve is an airplane curve over a finite discipline that is constructed from the points satisfying the equation.

y²=x³ + ax + b.

In this elliptic curve cryptography instance, any factor on the curve may be reflected over the x-axis and the curve will stay the identical. Any non-vertical line will intersect the curve in 3 locations or fewer.

**Mathematical equations-**

**F(XL) = ((S1,a + S2,b mod232)XOR S3,c) + S4,d mod232**

The characters that comprise the resultant hash are:

./ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789$.

Resultant hashes will be 60 characters long and they will include the salt among other parameters, as follows:

$[algorithm]$[cost]$[salt][hash]

 2 chars hash algorithm identifier prefix. "$2a$" or "$2b$" indicates BCrypt

Cost-factor (n). Represents the exponent used to determine how many iterations 2^n

16-byte (128-bit) salt, base64 encoded to 22 characters

24-byte (192-bit) hash, base64 encoded to 31 characters

Example:

 $2b$10$nOUIs5kJ7naTuTFkBy1veuK0kSxUFXfuaOKdOKf9xYT0KKIGSJwFa

**hash-value=** = K0kSxUFXfuaOKdOKf9xYT0KKIGSJwFa

 salt = nOUIs5kJ7naTuTFkBy1veu

 cost-factor => 10 = 2^10 rounds

 hash-algorithm identifier => 2b = BCrypt

**Proposed system vs existing system-**

**Fig.11** It can be noticed from the table (Fig. 9) that not all the modes have been tried for all the algorithms. Nonetheless, these results (Table 1) are good to have an indication about what the presented comparison results should look like.

Also, it is shown that Blowfish and AES have the best performance among others. And both are known to have better encryption (i.e., stronger against data attacks) than the other two.

**Fig. 12** Comparative execution times (in seconds) of encryption algorithms in ECB mode the results (Fig. 10) showed that Blowfish has a very good performance compared to other algorithms. Also, it showed that AES has a better performance than 3DES and DES. Amazingly it shows also that 3DES has almost 1/3 throughput of DES, or in other words it needs 3 times than DES to process the same amount of data. Table 2 shows the corresponding graph data.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Input Size (bytes) | DES | 3DES | AES | BF |
| 20527(1) | 2 | 7 | 4 | 2 |
| 36002(2) | 4 | 13 | 6 | 3 |
| 45911(3) | 5 | 17 | 8 | 4 |
| 59852(4) | 7 | 23 | 11 | 6 |
| 69545(5) | 9 | 26 | 13 | 7 |
| 137325(6) | 17 | 51 | 26 | 14 |
| 158959(7) | 20 | 60 | 30 | 16 |
| 166364(8) | 21 | 62 | 31 | 17 |
| 191383(9) | 24 | 72 | 36 | 19 |
| 232398(10) | 30 | 87 | 44 | 24 |

**Table 1** Comparative execution times (in seconds) of encryption algorithms in ECB mode on machine 1(a P-4 2.4 GHz machine)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Input Size (bytes) | DES | 3DES | AES | BF |
| 20527(1) | 24 | 72 | 39 | 19 |
| 36002(2) | 48 | 123 | 74 | 35 |
| 45911(3) | 57 | 158 | 94 | 46 |
| 59852(4) | 74 | 202 | 125 | 58 |
| 69545(5) | 83 | 243 | 143 | 67 |
| 137325(6) | 160 | 461 | 285 | 136 |
| 158959(7) | 190 | 543 | 324 | 158 |
| 166364(8) | 198 | 569 | 355 | 162 |
| 191383(9) | 227 | 655 | 378 | 176 |
| 232398(10) | 276 | 799 | 460 | 219 |

**Table 2** Comparative execution times (in seconds) of encryption algorithms in ECB mode in machine 2(P-II 266 MHz machine)

**Fig. 13** The results (Fig. 11) showed that Blowfish has a very good performance compared to other algorithms. Also, it showed that AES has a better performance than 3DES and DES. Amazingly it shows also that 3DES has almost 1/3 throughput of DES, or in other words it needs 3 times than DES to process the same amount of data.

**Fig 14.** The above diagram gives a clear picture about the irregularities or the shortcomings of the existing system and the scope where the proposed system can establish an impact.

**Conclusion and Future Work-**

Blockchain business is becoming more popular as a result of its built-in record security and robust privacy protection in the modern day. It's important to note, however, that as its usefulness grows, so do the quantity and variety of blockchain-specific security concerns. Undeniably, further study is required to determine how to best fortify the blockchain's security measures.

Blockchain is a significant improvement in online safety and might help guarantee that the CIA triads of cybersecurity are followed. Utilitarian challenges may arise from the intricacy of its execution.

Once the ruleset has been executed and a block has been supplied to the chain, it cannot be changed or withdrawn. To create an unbreakable chain of records capturing transactions, all changes to previously entered data may be structured as a new block and added to the chain without affecting the initial blocks.

Blockchains' secure, decentralized, and verifiable transaction records and data representations have inspired new approaches to cyber defense. The blocks' decentralized structure makes them more resistant to corruption than other types of concealed information. In contrast to conventional database architectures, there is no single point of failure or statistical disaster that may be exploited by hackers.

The immutability of blockchain generation's openness is analogous. As opposed to storing this information in a central repository, the blocks of facts are shared throughout all nodes. Accountability and performance are fostered by the openness and ease of use of these blocks by all stakeholders.

Blockchain technology has begun to spread across the corporate world, with companies like REMME disseminating blockchain technology with unique SSL certificates to do away with passwords and the possibility of human error. The REMME team isn't the only one working on blockchain identity products; other companies like Civic Technology have entered the market as well..

Consistent with Moody's forecast, scientists are working on quantum-secure encryption to thwart attempts to decrypt data using quantum computers. Most notably, in 2016, NIST sponsored a Post-Quantum Cryptography Standardization challenge to help future-proof information against quantum computers. According to Vadim Lyubashevsky, a cryptographer at the Security institute at IBM Research - Europe in Zurich, after 69 applicants and many rounds of evaluation, IBM has emerged as a frontrunner, with 4 of the 7 finalist bids, all based fully on lattice cryptography.

Using the so-called "knapsack difficulty," lattice cryptography conceals data inside intricate algebraic structures called lattices. If today's encryption were to be replaced with lattices, Lyubashevsky says, "in most circumstances, the user would not notice any changes," save from maybe a boost in performance.

**References-**

[1] Vitalik Buterin. A next generation smart contract and decentralized application platform, 2013.

[2] S. Paavolainen and C. Carr, "Security Properties of Light Clients on the Ethereum Blockchain," in IEEE Access, vol. 8, pp. 124339-124358, 2020, doi: 10.1109/ACCESS.2020.3006113.

[3] Y. N. Aung and T. Tantidham, "Review of Ethereum: Smart home case study," 2017 2nd International Conference on Information Technology (INCIT), 2017, pp. 1-4, doi: 10.1109/INCIT.2017.8257877.

[4] Avijit Mallik Department of Mechanical Engineering, Rajshahi University of Engineering & Technology, Rajshahi, Bangladesh. MAN-IN-THE-MIDDLE-ATTACK: UNDERSTANDING IN SIMPLE WORDS. Cyberspace: Journal Pendidikan Teknologi Informasi Volume 2, Nomor 2, Oktober 2018, (109 – 134)

[5] Ehab Zaghloul, Tongtong Li, Matt W. Mutka, Jian Ren, Bitcoin and Blockchain: Security and Privacy, Citation information: DOI 10.1109/JIOT.2020.3004273, IEEE Internet of Things Journal

[6] Parinya Ekparinya, Vincent Gramoli, Guillaume Jourjon, University of Sydney, Australia, Impact of Man-In-The-Middle Attacks on Ethereum, DOI 10.1109/SRDS.2018.00012

[7] Pouyan Razmjouei, Abdollah Kavousi-Fard1, Senior Member, IEEE, Morteza Dabbaghjamanesh, Senior Member, IEEE, Tao Jin, Senior Member, IEEE, Wencong Su, Senior Member, IEEE, Ultra-lightweight Mutual Authentication in the Vehicle Based on Smart Contract Blockchain: Case of MITM Attack, Citation information: DOI 10.1109/JSEN.2020.3022536, IEEE Sensors

[8] Joanna F. DeFranco, Bob Maley,Cyber Security In book: What Every Engineer Should Know About Cyber Security and Digital Forensics, DOI: 10.1201/9781003245223-2

[9] Mohammadreza Hazhirpasand, Arash Ale Ebrahim, Oscar Nierstrasz, Stopping DNS Rebinding Attacks in the Browser

DOI: 10.5220/0010310705960603

[10] Fran Casinov, Thomas K. Dasaklis, Constantinos Patsakis, A systematic literature review of blockchain-based applications: Current status, classification and open issues, Telematics and Informatics 36 (2019) 55–81

[11] Vitalik Buterin, Ethereum White Paper, A next generation smart contract and decentralized application platform (2013)

[12] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder, Princeton University Press, Princeton, NJ, USA, 2016.

[13] Abdelwahab, Ihab & Ramadan, Nagy & Hefny, Hesham. (2020). Cybersecurity Risks of Blockchain Technology. International Journal of Computer Applications. 177. 8-14. 10.5120/ijca2020919922.

[14] Taş, Ruhi & Tanriover, Omer. (2019). Building A Decentralized Application on the Ethereum Blockchain. 1-4. 10.1109/ISMSIT.2019.8932806.

[15] Aurelie Saglio, Julien Bourgeay, Romain Socrate, Alexis Canette, Gerard Cuvelier, Understanding the structure of ganache: Link between composition and texture, International Journal of Gastronomy and Food Science, Volume 13, 2018, Pages 29-37, ISSN 1878-450X, https://doi.org/10.1016/j.ijgfs.2018.05.003.

[16] Abdelwahab, Ihab & Ramadan, Nagy & Hefny, Hesham. (2020). Cybersecurity Risks of Blockchain Technology. International Journal of Computer Applications. 177. 8-14. 10.5120/ijca2020919922.

[17] Latif, R.M.A., Farhan, M., Rizwan, O. *et al.* Retail level Blockchain transformation for product supply chain using truffle development platform. *Cluster Comput* **24**, 1–16 (2021). https://doi.org/10.1007/s10586-020-03165-4

[18] Li, H., Pei, L., Liao, D., Wang, X., Xu, D. and Sun, J.: BDDT: use blockchain to facilitate IoT data transactions. Clust. Comput. (2020)

[19] Pilkington, M.: 11 Blockchain technology: principles and applications. In: Research Handbook on Digital Transformations, vol. 225, (2016)

[20] Lee, WM. (2019). Testing Smart Contracts Using Ganache. In: Beginning Ethereum Smart Contracts Programming. Apress, Berkeley, CA.<https://doi.org/10.1007/978-1-4842-5086-0_>7

[21] Hindawi Security and Communication Networks Volume 2022, Article ID 5307697, 11 pages<https://doi.org/10.1155/2022/5307697>

[22] Hindawi Mobile Information Systems Volume 2018, Article ID 2159082, 16 pages<https://doi.org/10.1155/2018/2159082>

[23] Security and Communication Networks Volume 2022, Article ID 3448950, 12 pages<https://doi.org/10.1155/2022/3448950>

[24] Security and Communication Networks Volume 2022, Article ID 5307697, 11 pages https://doi.org/10.1155/2022/5307697