# BLOCKCHAIN CRYPTOGRAPHY IN COMMUNICATION SYSTEMS (22MPD048)

**A PROJECT REPORT**

***Submitted by***

**KOUSTUBH SAXENA [Reg No: RA1811003030185]**
**SATWIK SRIVASTAVA [Reg No: RA18110030390202]**
**RACHIT GUPTA [Reg No: RA1811003030204]**
**DEEPTANSHU YADAV [Reg No: RA1811003030237]**

*Under the guidance of*

**Dr. PREMANANAD SAHU, Ph.D**
(Professor, Department of Computer Sciene & Engineering)

***in partial fulfillment for the award of the degree***

***of***

**BACHELOR OF TECHNOLOGY**

in

**COMPUTER SCIENCE & ENGINEERING**

of

**FACULTY OF ENGINEERING AND TECHNOLOGY**

SRM
INSTITUTE OF SCIENCE & TECHNOLOGY
Deemed to be University u/s 3 of UGC Act, 1956

S.R.M. Nagar, Kattankulathur, Kancheepuram District

**JUNE 2022**

# SRM INSTITUTE OF SCIENCE & TECHNOLOGY

(Under Section 3 of UGC Act, 1956)

## BONAFIDE CERTIFICATE

Certified that this project report titled “**BLOCKCHAIN CRYPTOGRAPHY IN COMMUNICATION SYSTEMS (22MPD048)**” is the bonafide work of “ **KOUSTUBH SAXENA [Reg No: RA1811003030185], SATWIK SRIVASTAVA [Reg No: RA18110030390202], RACHIT GUPTA [Reg No: RA1811003030204], DEEPTANSHU YADAV [Reg No: RA1811003030237],** ”, who carried out the project work under my supervision. Certified further, that to the best of my knowledge the work reported herein does not form any other project report or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate.

| | |
|---|---|
| **SIGNATURE** | **SIGNATURE** |
| Dr. PREMANANAD SAHU, Ph.D<br>**GUIDE**<br>Professor<br>Dept. of Computer Sciene & Engineering | Dr. R.P.Mahapatra<br>**HEAD OF THE DEPARTMENT**<br>Dept. of Computer Science & Engineering |
| Signature of the Internal Examiner | Signature of the External Examiner |

# ABSTRACT

The blockchain is an innovative technology that overcomes these threats and allows decentralisation of sensitive operations while preserving a high level of security. It eliminates the need for trusted intermediaries. The blockchain is accessible to all network nodes and keeps track of all transactions already made. The goal of our work is to propose a secure messaging solution based on blockchain technology. In this project, we explain why blockchain would make communications more secure, and we propose a model design for blockchain-based messaging main- taining the performance and security of data recorded on the blockchain, using a smart contract to verify the identities and their associated public keys, and validate the users certificate. The system is entirely decentralized and allows users to exchange messages securely.

# ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to my guide, DR. PREMANANAD SAHU, Ph.D his valuable guidance, consistent encouragement, personal caring, timely help and providing me with an excellent atmosphere for doing research. All through the work, in spite of his busy schedule, he has extended cheerful and cordial support to me for completing this research work.

**Author**

# TABLE OF CONTENTS

# CHAPTER 1

# INTRODUCTION

## 1.1 OBJECTIVE

Modern communication system have problems dealing with identities as in it is difficult to verify that a user is who it claims to be. And not someone impersonating another user. We rovide a noel solution using inspiration from modern distributed systems, so called Web3. We use Blockchain to store identities of all the user of a communication platform. With the added benefit of complying with future privacy laws like PARLIAMENT (2022b).

## 1.2 IMPLEMENTATION

We propose to use unique quality of BlockChains to be used as an append-only ledger and use it as a record of every user public key that can be verified. One of the implementation of this technique is given in certificate transparency log (B. Laurie, 2021).

## 1.3 Terminolgy

**Blockchain** is a peer-to-peer network; the word ‘blockchain‘ is made up of two separate terms, ‘block’ and ‘chain’. A block being referred to a collection of data, alias data records, and chain being referred to a public database of these blocks, stored as a list.

These are implemented using Linked list using pretty novel cryptography techniques. These lists are linked using cryptography, making it the most essential and fundamental requirement for creating a blockchain. Blockchain is a growing list of records, and the blocks get appended to the list with time.

**Cryptography** is a method of developing techniques and protocols to prevent a third party from accessing and gaining knowledge of the data from the private messages during a communication process. Cryptography is also made up of two ancient Greek terms, Kryptos and Graphein, the former meaning “hidden” and latter being “to write”. There are several terms related to cryptography;

**Encryption** It is a process of plaintext (normal text) to a ciphertext (random sequence of bits), such that it’s impossible to know what was the original text without knowing the algorithm used, and the key used to create it. It differs from hashing in only one sense that it is reversible.

**Decryption** The inverse process of encryption, conversion of ciphertext to plaintext.

# CHAPTER 2

# BLOCKCHAIN

## 2.1 INTRODUCTION

Blockchain is a distributed database with decentralized, traceable, non-tamperable, secure and reliable features. It integrates P2P (Peer-to-Peer) protocol, digital encryption technology, consensus mechanism, smart contract and other technologies together. Abandoning the maintenance mode of the traditional central node and adopting the method of mutual maintenance by multiple users to realize the information supervision among multiple parties, thereby ensuring the credibility and integrity of the data. The blockchain platform can be divided into public chain, private chain and alliance chain. All nodes in the public chain can join or withdraw freely; the private chain strictly limits the qualification of participating nodes; the alliance chain is jointly managed by several participating institutions. Bitcoin was proposed Nakamoto (2014), which is the most successful case of digital currency, and is also the most typical application of blockchain. In addition, the blockchain has expanded its unique application value in many aspects and has shown its potential to reshape society.

As a representative of distributed databases, blockchain stores all user transaction information on the blockchain, which has high requirements for the security performance of blockchain. Blockchain is a decentralized peer-to-peer network. Nodes do not need to trust each other and there is no central node. Therefore, transactions on the blockchain also need to ensure the security of transaction information on unsecured channels and to maintain the integrity of transactions. It can be seen that cryptography technology occupies the most central position in the blockchain. In blockchain, cryptography technology is mainly used to protect user privacy and transaction information, and ensure data consistency, etc.

This paper briefly introduces the cryptographic techniques such as hash algorithm, asymmetric encryption algorithm and digital signature, also elaborates the blockchain infrastructure, the blockchain structure, bitcoin address, digital currency trading and other technologies of blockchain, and also explains how cryptography technology protects privacy and transaction maintenance in the blockchain in detail.

## 2.2 Blockchain Infrastructure

According to Melanie Swan, founder of the Blockchain Science Institute, blockchain technology has experienced two phases, the first one is the blockchain 1.0 phase of multi-technology portfolio innovation represented by Bitcoin, the second one is the blockchain 2.0 phase represented by Ethereum, which is transferred by digital assets. Typical applications of blockchain technology mainly include Bitcoin, Ethereum, Hyper Ledgers, etc. Although the implementations are different, there are many commonalities in the overall architecture. As shown in Table 1, the blockchain platform can be divided into five levels: network layer, consensus layer, data layer, contract layer and application layer.

The data layer mainly uses the block data structure to ensure the integrity of data storage. Each node in the network encapsulates the data transactions received over a period of time into a time-stamped data block and links the block to the current longest main blockchain for storage. This layer involves the main techniques of block storage, chain structure, hash algorithm, Merkle tree, time stamp and so on.

The consensus layer mainly includes a consensus mechanism, which enables each node to reach a consensus on the validity of block data in the decentralized system. The consensus mechanism mainly has PoW, PoS, PBFT and SBFT. The consensus layer mainly includes a consensus mechanism, which enables each node to reach a consensus on the validity of block data in the decentralized system. The consensus mechanism mainly has PoW, PoS, PBFT and SBFT.

The blockchain is a typical P2P network. All nodes are connected through a planar topology and have no central nodes. Any two nodes can be freely traded, and any node can join or leave the network at any time. The P2P protocol in the blockchain is mainly used for information transmission between nodes. The application layer mainly includes Bitcoin, Ethereum and Hyperledger and so on. Bitcoin is mainly for digital currency transactions. Ethereum adds decentralized applications based on digital currency. Hyperledger does not support digital currency transactions, mainly enterprise-level blockchain applications.

## 2.3 Hash and block structure

The hash algorithm is a function that maps a sequence of messages of any length to a shorter fixed-length value, and is characterized by susceptibility, non-omnidirectionality, collision resistance, and high sensitivity. Hash is usually used to ensure data integrity, that is, to verify the data has been illegally tampered with. When the data tested changes, its hash value also changes correspondingly. Therefore, even if the data is in an unsafe environment, the integrity of the data can be detected based on the hash value of the data. SHA is a type of cryptographic hash function issued by the National Institute of Standards and Technology (NIST) with the general characteristics of a cryptographic hash function. The SHA256 algorithm is a class of the SHA-2 algorithm cluster, which generates a 256-bit message digest. The algorithm's calculation process includes two stages: message preprocessing and main loop. In the message preprocessing stage, binary bit filling and message length filling are performed on the information of any length, and the filled message is divided into several 512-bit message blocks. In the main loop phase, each message block is processed by a compression function. The input of the current compression function is the output of the previous compression function, and the output of the last compression function is the hash value of the original message.

RIEPEMD, a summary of the RACE original integrity check message, is a hash function algorithm developed by the COSI research team of the University in Leuven, Belgium. RIPEMD-160 is the most common version of RIPEMD. As the SHA series functions, the first step of the algorithm is message complement, and the complement method is identical to the SHA series algorithm. The core of the processing algorithm is the compression function, which is a loop, where each loop consists of 16 step functions. Using different original logic functions in each loop, the processing of the algorithm is divided into two different cases, with five of the two original logic functions running in reverse order. After all 512-bit packet processing is completed, the resulting 160-bit output is the hash value of the original message.

For blockchain, hash functions can be used to perform block and transaction integrity verification. In the blockchain, the hash value of the information of the previous block is stored in the header of each block, and any user can compare the calculated hash value with the stored hash value. In turn, the integrity of the information of the previous block is detected. Similarly, the hash function can be used to generate public-private key pairs.

The hash pointer is a data structure that contains, in addition to the usual pointers, some data information and password hashes associated with the information. A normal pointer is used to retrieve information, and a hash pointer is used to verify that the information has been tampered. The blockchain is a list of hash pointers, each of which is connected by using a hash value. It is verified according to the hash value whether the data contained in the block is changed, thereby ensuring the integrity of the block information.

## 2.4 Types of blockchains

Blockchains can be categories dependent upon there consensus mechanism used in them. And which protocol they used to distribute themselves and last but not least. Who can participate in that blockchain.

### 2.4.1 Public Blockchain

A blockchain that anyone in the world can read, can send transactions to and expect to see them included if they are valid. This means anyone can become part of the network and participate in the consensus process making them permissionless. There is no way to censor transactions on the network nor change transactions retrospectively. The content of the blockchain can be trusted to be correct. Public blockchains are, however, very inefficient. The more com- puting power is required to support trust. So, an attacker would need to acquire 51

### 2.4.2 Consortium Blockchain

It is a blockchain where a pre-selected set of nodes control the consensus process.

### 2.4.3 Private Blockchain

A blockchain where access permissions are more lightly controlled, where rights to modify or even read the blockchain state are restricted to a few users, where only known nodes are allowed to participate in the network. Ideally, it is internal for an organization. The writes permissions are kept centralized to one organization. Private blockchain reduces counterparty risk by enabling the exchange of data without the intermediation of third parties.

### 2.4.4 Permissioned Blockchain

It is a blockchain where we can allow specific actions to be performed only by specific addresses. The participants in the network can restrict who can participate in the consensus mechanism and who can create a smart contract and give the authority for some participants to provide the validation of blocks of transactions. A control access layer into the blockchain nodes is used. However, raise their questions, Who has the authority to grant permission? A permission blockchain may make its owners feel more secure, giving the database rigorous secu- rity and privacy capabilities but can be seen as violating the idea of blockchain because only some participants have more control, which means they can make changes whether or not other network participants agree.

## 2.5 Digital Content Protection

Blockchain technology is used extensively in digital content protection and privacy advocates. Because of it's append only and tamper-proof nature. It's very useful in protecting digital documents from tamper. Nowadays, you can find calculate a checksum of any documents using numerous cryptographic hashing algorithms, and if we store those ashes in a public blockchain then we can verify that it isn't tamperproof and as an added bonus the unique public key of the sender make it, so it is verifiable who was the original author.

In order to preserve the privacy for traceable encryption in blockchain, Wu et al. proposed a system in which authenticity and non-repudiation of digital content is guaranteed. The problem tackled by authors is the secret key of the user, which when shared with other entities does not hold the specific information of the user. In case the shared key is corrupted or abused, it makes it difficult to analyze the source of the secret key. Moreover, leakage of confidential information in access control is a bottleneck for existing systems. Therefore, authors have integrated the privacy protection algorithm such as attribute based encryption (ABE) to secure the secret keys. However, the decryption mechanism does not show improved efficiency.

Management of digital data rights is a fundamental requirement to achieve protection of digital data. Existing techniques for data rights lack transparency, decentralization, and trust. In response to above mentioned problems, Zhang and Zhao proposed blockchain-based decentralized solutions. Information regarding the use of digital content, such as transaction and license information is transparent to everyone. Smart contract is designed for the automatic assignment of license. In this mechanism, the owner can set the prices for selling the license to other customers. However, peers of the network have to possess high computational power to perform key acquisition.

Ma et al. focus on digital rights management using blockchain to avoid the use of sensitive digital content for illegal purposes. For such concerns, a solution is proposed which is called DRMchain. This solution ensures the usage of digital content in the right way by authenticated users. Two separate blockchains are designed: one is to store the original content with its cipher summary, and the other stores the cipher summary of protected digital content. DRMchain provides the traceability record of a violation and high level trusted protection. From the proposed solution, protection of digital content, secure authorization of users, and use of multi signatures for usage control is achieved. However, the use of Ethereum coins could be a new research direction for protection of digital content.

Data sharing is a crucial step to gain maximum benefit from the strengths of research. A lot of data sharing mechanisms are proposed and discussed in literature. There is no sufficient work available that focuses on the incentive mechanism to promote data sharing. To cover these limitations, authors conducted a review on medical and health data to uncover the incentive mechanisms with the pre- and post- results after empirical analysis. According to a survey, a single incentive is tested for medical and health data to analyse the rate of data sharing. Therefore, it is concluded that more incentive based research needs to be performed to encourage data sharing.

## 2.6 The Significance of Security for Blockchain

Before we dive right into understanding the role of cryptography in blockchain, let us reflect briefly on the blockchain itself. It basically refers to a distributed database that offers the features of decentralization, security, traceability, reliability, and immutability. Blockchain takes away the need for traditional approaches for maintaining central nodes and introduces the new approach for mutual maintenance of nodes by multiple users.

As a result, it can entrust information supervision to multiple parties and ensure desired levels of credibility and data integrity. Another important aspect pertaining to blockchain refers to the three distinct types of blockchain platforms. The types of blockchain platforms include public chain, private chain, and alliance chain. All the nodes in a public chain could easily participate or withdraw from the blockchain according to their preferences.

On the other hand, private blockchains impose specific conditions to determine the eligibility of the participating nodes. The alliance chain operates under the joint management of different participating organizations. Over the years, blockchain has been largely associated with the financial industry. However, it has showcased the promising potential for adding value to different sectors alongside reshaping the fundamental tenets of our society. So, what is the relationship between blockchain and cryptography? The blockchain serves as a representative of distributed databases by storing all the transaction information of users on the blockchain. Therefore, it is reasonable to identify a profoundly higher demand for security performance in the blockchain.

Since blockchain operates with a decentralized, peer-to-peer network model, there is no single node, and nodes don't have to trust one another. So, blockchain must also ensure appropriate safeguards for transaction information on unsecured channels while maintaining transaction integrity. Therefore, cryptography becomes an essential requirement for blockchain to safeguard user transaction information and privacy alongside ensuring data consistency.

## 2.7 Mining

Mining, in the context of blockchain technology, is the process of adding transactions to the large distributed public ledger of existing transactions, known as the blockchain. The term is best known for its association with bitcoin, though other technologies using the blockcahin employ mining. Bitcoin mining rewards people who run mining operations with more bitcoins.

Blockchain mining involves adding transactions to the existing blockchain ledger of transactions distributed among all users of a blockchain. While mining is mostly associated with bitcoin, other technologies using a blockchain employ mining as well. Mining involves creating a hash of a block of transactions that cannot be easily forged, protecting the integrity of the entire blockchain without the need for a central system.

Mining is typically done on a dedicated computer, as it requires a fast CPU, as well as higher electricity usage and more heat generated than typical computer operations. The main incentive for mining is that users who choose to use a computer for mining are rewarded for doing so. In the case of bitcoin, it is 25 bitcoins per hash. That is why some hackers use machines they break into to mine bitcoins, getting an unwitting victim to pay for the costs of mining while reaping none of the benefits.

### 2.7.1 Steps

Specialized computers perform the calculations required to verify and record every new bitcoin transaction and ensure that the blockchain is secure. Verifying the blockchain requires a vast amount of computing power, which is voluntarily contributed by miners.

Bitcoin mining is a lot like running a big data center. Companies purchase the mining hardware and pay for the electricity required to keep it running (and cool). For this to be profitable, the value of the earned coins has to be higher than the cost to mine those coins.

What motivates miners? The network holds a lottery. Every computer on the network races to be the first to guess a 64-digit hexadecimal number known as a “hash.” The faster a computer can spit out guesses, the more likely the miner is to earn the reward.

The winner updates the blockchain ledger with all the newly verified transactions – thereby adding a newly verified “block” containing all of those transactions to the chain – and is granted a predetermined amount of newly minted bitcoin. (On average, this happens every ten minutes.) As of late 2020, the reward was 6.25 bitcoin – but it will be reduced by half in 2024, and every four years after. In fact, as the difficulty of mining increases, the reward will keep decreasing until there are no more bitcoin left to be mined.

## 2.8 Proof of Work (PoW)

Proof of work (PoW) is a form of cryptographic proof in which one party (the prover) proves to others (the verifiers) that a certain amount of a specific computational effort has been expended. Verifier can subsequently confirm this expenditure with minimal effort on their part. The concept was invented by Cynthia Dwork and Moni Naor in 1993 as a way to deter denial-of-service attacks and other service abuses such as spam on a network by requiring some work from a service requester, usually meaning processing time by a computer. The term "proof of work" was first coined and formalized in a

1999 paper by Markus Jakobsson and Ari Juels. Proof of work was later popularized by Bitcoin as a foundation for consensus in permissionless decentralized network, in which miners compete to append blocks and mint new currency, each miner experiencing a success probability proportional to the computational effort expended. PoW and PoS (proof of stake) are the two best known Sybil deterrence mechanisms. In the context of cryptocurrencies they are the most common mechanisms. PARLIAMENT (2022a)

A key feature of proof-of-work schemes is their asymmetry: the work – the computation – must be moderately hard (yet feasible) on the prover or requester side but easy to check for the verifier or service provider. This idea is also known as a CPU cost function, client puzzle, computational puzzle, or CPU pricing function. Another common feature are built-in incentive-structures that reward allocating computational capacity to the network with value in the form of money

The purpose of proof-of-work algorithms is not proving that certain work was carried out or that a computational puzzle was "solved", but deterring manipulation of data by establishing large energy and hardware-control requirements to be able to do so.[citation needed] Proof-of-work systems have been criticized by environmentalists for their energy consumption.

### 2.8.1 Environment Impact

We can't talk about PoW with mentioning its huge environment impact as mentioned there use very high compute heavy task to do the "work" but that means that a huge amount of compute resource are used essentially to increase the amount of time that it took to mine a block. And that can be huge waste of power which can be used for more priority task instead of this. As to have mining incentives it's return should be greater than the price of electricity and equipment used to mine it.

Since the creation of Bitcoin, proof-of-work has been the predominant design of peer-to-peer cryptocurrency. Studies have estimated the total energy consumption of cryptocurrency mining.[22] The PoW mechanism requires a vast amount of computing resources, which consume a significant amount of electricity. Recent estimates from the University of Cambridge put Bitcoin's energy consumption as equal to that of Switzerland.

In January 2022 Vice-Chair of the European Securities and Markets Authority Erik Thedéen called on the EU to ban the proof of work model in favor of the proof of stake model due its lower energy emissions. Bateman (2022)

## 2.9 Proof of Stake(PoS)

Proof of stake (PoS) Y (2022) protocols are a class of consensus mechanisms for blockchains that work by selecting validators in proportion to their quantity of holdings in the associated cryptocurrency. This is done to avoid the computational cost of proof of work schemes. The first functioning use of PoS for cryptocurrency was Peercoin in 2012.

For a blockchain transaction to be recognized, it must be appended to the blockchain. Validators carry out this appending; in most protocols, they receive a reward for doing so. For the blockchain to remain secure, it must have a mechanism to prevent a malicious user or group from taking over a majority of validation. PoS accomplishes this by requiring that validators have some quantity of blockchain tokens, requiring potential attackers to acquire a large fraction of the tokens on the blockchain to mount an attack. Proof of work, another commonly used consensus mechanism, uses a validation of computational prowess to verify transactions, requiring a potential attacker to acquire a large fraction of the computational power of the validator network.[2] This incentivizes consuming huge quantities of energy. PoS is more energy-efficient.

Critics have argued that the proof of stake will likely lead cryptocurrency blockchains being more centralized in comparison to proof of work as the system favors users who have a large amount of cryptocurrency, which in turn could lead to users who have a large amount of cryptocurrency could have major influence on the management and direction for a crypto blockchain.

In 2021 a study by the University of London Platt et al. (2021) found that in general the energy consumption of the Proof-of Work based Bitcoin was about 1,000 times higher than that of the highest consuming proof of stake system that was studied even under the most favorable conditions and that most proof of stake systems cause less energy consumption in most configurations. The researchers also noted that the energy consumption of different Proof of stake systems was divergent with permissioned systems that used less validators being more energy efficient then permission-less systems that don't. They also couldn't find the energy consumption of a proof of stake system on a large scale as such a system does not exist at the time of the report.

# CHAPTER 3

# CRYPTOGAPHY

## 3.1 Introduction

Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents. The term is derived from the Greek word kryptos, which means hidden.

By concept, it is a method of developing techniques and protocols to prevent a third party from accessing and gaining knowledge of the data from the private messages during a communication process.

The word Cryptography is made up of two ancient greek terms, Kryptoshaving meaning “hidden” and Graphein having meaning “to write”.

## 3.2 Terminologgy

**Encryption** It is a process of plaintext (normal text) to a ciphertext (random sequence of bits).

**Key** A small amount of information is required to induce the output of the cryptographic algorithm.

**Decryption** The inverse process of encryption, conversion of ciphertext to plaintext.

**Cipher** The mathematical function, i.e. a cryptographic algorithm which is used to convert plaintext to ciphertext.

## 3.3 Types of Cryptgraphy

Fundamentally, there are mainly three different ways one can perform cryptographic algorithms,

### 3.3.1 Symmetric-Key Cryptography

In this encryption method, we take a single key into the application.

This common key is used for both the encryption as well as the decryption process.

Using a common single key creates a problem of securely transferring the key between the sender and the receiver.

It is also called Secret-Key Cryptography.

### 3.3.2 Asymmetric-Key Cryptography

This encryption method uses a pair of keys, an encryption key, and a decryption key, named public key and private key respectively.

The key pair generated by this algorithm consists of a private key and a unique public key that is generated using the same algorithm.

It is also called Public-Key Cryptography.

### 3.3.3 Hash Functions

It doesn't make use of keys.

It uses a cipher to generate a hash value of a fixed length from the plaintext.

It is nearly impossible for the contents of plain text to be recovered from the ciphertext.

Blockchains mainly make use of two types of cryptographic algorithms, Asymmetric-key algorithms 1. Asymmetric-key algorithms 2. Hash Functions

## 3.4 Hash Function

Hash functions are used to provide the functionality of a single view of blockchain to every participant. And generally, blockchains use the SHA-256 and RIPEMD-160 hashing algorithm as their hash function.

### 3.4.1 Why Use Cryptographic Hash Functions?

Well, cryptographic hash functions provide the following benefits to the blockchain,

Further, hash functions have a major role in linking the blocks to one another and also in maintaining the integrity of the data stored inside each block. Any alteration in the block data can lead to inconsistency and break the blockchain, making it INVALID. This requirement is achieved by the property of the hash functions, called the 'avalanche effect'.

It's this feature that makes the data reliable and secure on the blockchain. And any changes in the block data will lead to this difference in hash value and make the blockchain invalid, making it immutable.

**Avalanche effect** i.e., a slight change in the data can result in a significantly different output.

**Uniqueness** i.e., very input has a unique output.

**Deterministic** i.e., any input will always have the same output if passed through the same hash function.

**Quickness** he output can be generated in a very small amount of time.

Reverse engineering is not possible, i.e. we cannot generate the input by having the output and the hash function.

## 3.5 Asymmetric-Key Cryptography

It is where the private key generally needs to be produced by a random number algorithm, and the public key is calculated by executing an irreversible algorithm.

The asymmetric encryption algorithm has the advantage of having separate public and private keys, which can be transferred over unsecured channels.

Likely, it also has several disadvantages, some of them being low processing speed and unsatisfactory encryption strength. Also, It is very much necessary to ensure the security of the asymmetric encryption algorithm during the transmission of data on the blockchain.

## 3.6 Digital Signatures

One of the major parts of asymmetric-key cryptography is digital signatures. And for those who don't know, Digital signatures provide integrity to the process; as they are easily verifiable and cannot be corrupted.

They also hold the quality of non-repudiation, making them similar to the signatures in the real world. Further, It is these digital signatures, which ensure that the blockchain is valid and the data is verified and correct.

### 3.6.1 A Perspective

Hashing, public-private key pairs, and the digital signatures together constitute the foundation for the blockchain. These cryptographic features make it possible for blocks to get securely linked by other blocks, and also ensure the reliability and immutability of the data stored on the blockchain.

There are a huge number of applications of blockchain technology, and it is cryptography that makes all of them possible. One of the major real-world applications is cryptocurrencies.

Cryptocurrencies are one of the major applications of blockchains, and they use public-private key pairs to maintain the addresses of the users on the blockchain. For cryptography in blockchain, the public key is used as the address of the person.

Take note that the public key is visible globally, i.e. it is visible to any participant. Whereas the private key is a secret value and is used to access that address data and authorize any of the actions for the ‘address’, which are generally regarded as transactions.

Digital signatures are widely used for cryptocurrencies as well. They are used to approve transactions by signing them securely (i.e. offline) and are also used for multi-signature contracts and digital wallets on the blockchain.

This further helps to perform any action from these multi-signature contracts and digital wallets, but do account for the fact that the digital signatures from multiple (i.e. different) private keys are required before any action to be executed.

## 3.7 Understanding Blockchain Cryptography with Examples

Blockchain cryptography is definitely a complicated topic. However, you can achieve a better and simpler understanding of cryptography by reflecting on the fundamentals of its working. Take the example of radio signals that help you listen to broadcasts on your vehicle’s radio. The broadcast is publicly available to everyone, and other people could also listen to the broadcast.

On the other hand, take the example of radio communications between two soldiers on a military mission. Such type of defense-level communications will be highly secure and encrypted, and only the intended participants can receive and know the information. You can find the applications of cryptography in blockchain in the exact same manner.

Basically, cryptography serves as a technique for the transmission of secure messages among two or more participants. The sender leverages a specific type of key and algorithm for encryption of a message before sending it to the receiver. Then, the receiver employs decryption for obtaining the original message. So, what is the important aspect in the operations of cryptography? The answer directly points out encryption keys.

Encryption keys ensure that unauthorized recipients or readers cannot read a message, data value, or transaction. They are the right tools for making sure that the intended recipients only are capable of reading and processing a specific message, data value, or transaction. Therefore, keys are able to bring 'crypto' traits to information.

The majority of blockchain applications don't involve explicit use of sending secret, encrypted messages, especially in the public blockchain. On the other hand, a new generation of blockchain applications utilizes different variants of cryptography encryption for ensuring security and complete anonymity of transaction details. Many new tools related to applications of cryptography in blockchain have emerged over the years with diverse functionalities. Some notable examples of the tools include hashing and digital signatures.

With a basic outline of details in blockchain cryptography explained properly, it is evident that cryptography refers to the practice of creating protocols for preventing third parties from accessing and viewing data. The modern applications of cryptography bring a combination of different disciplines such as physics, math, computer science, engineering, and others.

However, the focus of applications of blockchain cryptography primarily emphasizes terms such as encryption, decryption, cipher, and keys. Readers must have already come to terms with the applications of encryption and decryption in cryptography. Cipher is the algorithm that helps in performing the processes of encryption and decryption, generally by following a series of well-defined steps.

Keys refer to the trivial amount of information required to obtain output from the cryptography algorithm. Now, let us take a look at digital signatures and hashing, the two components that establish the significant role of cryptography in the blockchain.

## 3.8 Implications of blockchain and cryptography with Digital Signatures

Digital signature basically refers to a mathematical approach for creating digital codes that are utilized for verifying whether digital messages and documents are legible or not. Public-key encryption is suitable for producing and substantiating the codes. In addition, attaching digital signatures to an electronically disseminated document ensures verification of specifications of the content and the sender.

Before diving further into the implications of blockchain and cryptography with digital signatures, let us reflect back on security fundamentals. It is important to address the requirements of four significant traits in the online transmission of valuable data. The four important traits include confidentiality, non-repudiation, authentication, and integrity.

Generally, encryption algorithms such as AES can address the need for confidentiality. However, digital signatures are preferable alternatives for addressing the requirement of the other three traits of non-repudiation, integrity, and authentication. The effectiveness of blockchain cryptography with digital signatures depends a lot on two prominent methods of encryption.

## 3.9 Symmetric-Key Encryption

he first type of encryption refers to symmetric-key encryption. Symmetric-key encryption focuses on using similar keys for encryption as well as decryption of data. Most important of all, the symmetric-key encryption method is applicable in various information security use cases such as encryption of your hard drive or security of the connection to an HTTPS website. The use of a similar key for encryption and decryption creates issues in the safe transfer of the key between the receiver and the sender. Symmetric-key encryption is also referred to as secret-key cryptography.

## 3.10 Asymmetric-Key Encryption

The second encryption method that has a profound role in the applications of cryptography in the blockchain is asymmetric-key encryption. Asymmetric-key encryption is also known as public-key cryptography and involves the use of different keys for encryption and decryption processes.

The public key and private key can serve the roles of the encryption key and decryption key, respectively. Asymmetric-key cryptography algorithms generate the key-pair, and the public key is shared openly while the private key is maintained in secret. Public-key cryptography, as it is also called, can help two completely unknown parties for exchanging information securely.

Digital signatures leverage public-key cryptography and help individuals to prove ownership of their private keys. Interestingly, users don't have to reveal their private keys to the other parties as they can prove it by decrypting messages. So, the applications of cryptography in blockchain with digital signatures focus on the transaction process for ownership verification.

## 3.11 Use of Cryptographic Hashing in Blockchain Cryptography

The use of cryptographic hashing is also one of the notable highlights in blockchain cryptography explained properly. As a matter of fact, cryptographic hashing presents a basic component of blockchain technology. Hashing enables immutability in blockchain, the most significant feature in the blockchain. The encryption through cryptographic hashing does not involve the use of keys.

On the contrary, hashing in cryptographic leverages a cipher or an algorithm for obtaining a hash value of a particular length from the input. Hashing involves taking a string of any length as input and producing an output with a fixed length. The most common applications of hashing in blockchain are evident in the use of the SHA-256 cryptographic hash function.

### 3.11.1 Cryptographic hash functions

It offer various unique traits which establish their productivity for blockchain cryptography. Here is an outline of the characteristics that make cryptographic hash functions suitable for blockchain use cases.

Cryptographic hash functions are deterministic. Therefore, no matter how many times you enter a specific input, the hash function delivers the output of the same length. So, whether you enter a string with 3 characters or 200 characters, you would receive the output of the same length, i.e., 32 characters in a fixed string with a combination of numbers and letters.

The second important trait that is evident in the case of cryptographic hash functions refers to the uniqueness of output. You don't have to worry about two different inputs having the same output with cryptographic hash functions. Therefore, they can also offer unique functionalities for avoiding any collisions.

Cryptographic hash functions are also associated profoundly with the trait of irreversibility. It is basically impossible to derive the original input from the output by using existing technology and techniques.

Another profound characteristic that establishes the significance of hash functions in blockchain and cryptography is the faster computation of hashes. Hash functions can generate outputs faster, thereby ensuring better prospects for faster transaction completion.

The avalanche effect is also a prominent highlight in the traits of cryptographic hash algorithms. The avalanche effect basically implies that a small change in the input results could lead to a completely different output.

### 3.11.2 Secure hash algorithm

SHA or Secure Hash Algorithm is the most widely used cryptographic hash function with many variants such as SHA1, SHA256, MD5, and SHA512 being used commonly. Every cryptographic hash function has its unique function as follows,

1. MD5 or the Message-Digest algorithm helps in generating a 128-bit hash value

2. SHA1 is the upgraded version of SHA tailored by NIST and published in accordance with FIPS or Federal Information Processing Standard

3. SHA256 function involves hash value computing with 32-bit words and message digest amounts to 256 bits

4. SHA512 function involves hash value computing with 64-bit words and message digest amounts to 512 bits.

Therefore, it is clearly evident that cryptographic hash functions offer unique benefits of mathematics with various appealing properties. So, how are the properties of cryptographic hash algorithms relevant for the role of cryptography in blockchain? Basically, the characteristics of hash functions ensure the following benefits,

Access to proof of ownership of specific information without revealing the information

Prevention of unauthorized modifications in transactions

Verification of transaction confirmation without complete knowledge of the block

Reduction of transaction bandwidth

Development of cryptographic puzzles for transactions

## 3.12 Blockchain networks

One of the main aims of a blockchain is to create a decentralized system that can verify itself without the need for third parties. This is generally achieved via a peer-to-peer verification process, where the network offers financial incentives for honestly validating transaction data. Many blockchains refer to this process as mining.

In the bitcoin protocol, every time a transaction is made, the details are sent through a relay of nodes until every node on the network receives the data.

The miners then collect each of these transactions and form them into a block. Each miner then tries to solve the cryptographic puzzle for the block. When a miner succeeds, it sends the block to all of the nodes on the network.

The nodes will only accept the block if all of the transactions within it are verified and haven't already been spent. When nodes accept a block, they take its hash and distribute it to miners, who then integrate it into the next block of transactions that they are trying to solve.

If two separate miners solve a block at the same time, the other miners will take the data from whichever block they received first, and incorporate it into the next block they are working on. They will also save the data from the second block, just in case they need it later on.

The entire network will be working on either one block or the other until the next block is solved. At this point, those that were working on the other block will abandon it. This is because miners will always accept the longest chain as the correct one. They focus their work towards extending the longest chain, because this is the most likely way for them to end up with the reward.

## 3.13 An introduction to encryption and cryptography

Section 3 has introduced you to the main threats to network security. Before I begin to examine the countermeasures to these threats I want to briefly introduce one of the fundamental building blocks of all network security. This is encryption – a process that transforms information (the plaintext) into a seemingly unintelligible form (the ciphertext) using a mathematical algorithm and some secret information (the encryption key). The process of decryption undoes this transformation using a mathematical algorithm, in conjunction with some secret value (the decryption key) that reverses the effects of the encryption algorithm. An encryption algorithm and all its possible keys, plaintexts and ciphertexts is known as a cryptosystem or cryptographic system.

Cryptography is the general name given to the art and science of keeping messages secret. It is not the purpose here to examine in detail any of the mathematical algorithms that are used in the cryptographic process, but instead to provide a general overview of the process and its uses.

Modern encryption systems use mathematical algorithms that are well known and have been exposed to public testing, relying for security on the keys used. For example, a well-known and very simple algorithm is the Caesar cipher, which encrypts each letter of the alphabet by shifting it forward three places. Thus A becomes D, B becomes E, C becomes F and so on. (A cipher that uses an alphabetic shift for any number of places is also commonly referred to as a Caesar cipher, although this isn't strictly correct since the Caesar cipher is technically one in which each character is replaced by one three places to the right.) I could describe this mathematically as p + 3 = c, where p is the plaintext and c the ciphertext. For a more general equation I could write p + x = c where x could take any integer value up to 25. Selecting different values for x would obviously produce different values for c, although the basic algorithm of a forward shift is unchanged. Thus, in this example the value x is the key. (The Caesar cipher is of course too simple to be used for practical security systems.)

It should be computationally infeasible to derive the plaintext from the ciphertext without knowledge of the decryption key.

It should be computationally infeasible to derive the ciphertext from the plaintext without knowledge of the encryption key.

The reason for the first condition is obvious, but probably not the second, so I shall briefly explain. In Section 3, the need to confirm authenticity was introduced. This is often also a requirement for information that is sent 'in the clear', that is, not encrypted. One method of authentication is for the sender and recipient to share a secret key. The sender uses the key to encrypt a copy of the message, or a portion of it, which is included with the data transfer and, on receipt, the recipient uses the key to decrypt the encrypted data. If the result matches the plaintext message, this provides a reasonable assurance that it was sent by the other key owner, and thus a check on its authenticity. (You will learn more about authentication in Section 8.) Of course, this assumes that the key has not been compromised in any way.

Modern encryption systems are derived from one of two basic systems: symmetric key (sometimes called shared key) systems, and asymmetric key (often called public key) systems.

## 3.14 Types of Keys

**Symmetric Key** Symmetric-key encryption are algorithms which use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext.

**Asymmetric Key** Asymmetric encryption uses 2 pairs of key for encryption. Public key is available to anyone while the secret key is only made available to the receiver of the message. This boots security.

**Public Key** Public key cryptography is an encryption system which is based on two pairs of keys. Public keys are used to encrypt messages for a receiver.

**Private Key** Private key may be part of a public/ private asymmetric key pair. It can be used in asymmetric encryption as you can use the same key to encrypt and decrypt data.

**Pre-Shared Key** In cryptography, a pre-shared key (PSK) is a shared secret which was earlier shared between the two parties using a secure channel before it is used.

## 3.15 How Does Blockchain Technology Work?

In recent years, you may have noticed many businesses around the world integrating Blockchain technology. But how exactly does Blockchain technology work? Is this a significant change or a simple addition? The advancements of Blockchain are still young and have the potential to be revolutionary in the future; so, let's begin demystifying this technology.

Cryptographic keys, A peer-to-peer network containing a shared ledger. A means of computing, to store the transactions and records of the network

Cryptography keys consist of two keys – Private key and Public key. These keys help in performing successful transactions between two parties. Each individual has these two keys, which they use to produce a secure digital identity reference. This secured identity is the most important aspect of Blockchain technology. In the world of cryptocurrency, this identity is referred to as 'digital signature' and is used for authorizing and controlling transactions.

The digital signature is merged with the peer-to-peer network; a large number of individuals who act as authorities use the digital signature in order to reach a consensus on transactions, among other issues. When they authorize a deal, it is certified by a mathematical verification, which results in a successful secured transaction between the two network-connected parties. So to sum it up, Blockchain users employ cryptography keys to perform different types of digital interactions over the peer-to-peer network.

## 3.16 The Process of Transaction

One of Blockchain technology's cardinal features is the way it confirms and authorizes transactions. For example, if two individuals wish to perform a transaction with a private and public key, respectively, the first person party would attach the transaction information to the public key of the second party. This total information is gathered together into a block.

The block contains a digital signature, a timestamp, and other important, relevant information. It should be noted that the block doesn't include the identities of the individuals involved in the transaction. This block is then transmitted across all of the network's nodes, and when the right individual uses his private key and matches it with the block, the transaction gets completed successfully.

In addition to conducting financial transactions, th

### 3.16.1 Hash Encryptions

Blockchain technology uses hash encryption to secure the data, relying mainly on the SHA256 algorithm to secure the information. The address of the sender (public key), the receiver's address, the transaction, and his/her private key details are transmitted via the SHA256 algorithm. The encrypted information, called hash encryption, is transmitted across the world and added to the Blockchain after verification. The SHA256 algorithm makes it almost impossible to hack the hash encryption, which in turn simplifies the sender and receiver's authentication.

## 3.17 Use of Cryptographic Hashing in Blockchain Cryptography

He use of cryptographic hashing is also one of the notable highlights in blockchain cryptography explained properly. As a matter of fact, cryptographic hashing presents a basic component of blockchain technology. Hashing enables immutability in blockchain, the most significant feature in the blockchain. The encryption through cryptographic hashing does not involve the use of keys.

On the contrary, hashing in cryptographic leverages a cipher or an algorithm for obtaining a hash value of a particular length from the input. Hashing involves taking a string of any length as input and producing an output with a fixed length. The most common applications of hashing in blockchain are evident in the use of the SHA-256 cryptographic hash function.

Cryptographic hash functions offer various unique traits which establish their productivity for blockchain cryptography. Here is an outline of the characteristics that make cryptographic hash functions suitable for blockchain use cases.

Cryptographic hash functions are deterministic. Therefore, no matter how many times you enter a specific input, the hash function delivers the output of the same length. So, whether you enter a string with 3 characters or 200 characters, you would receive the output of the same length, i.e., 32 characters in a fixed string with a combination of numbers and letters.

The second important trait that is evident in the case of cryptographic hash functions refers to the uniqueness of output. You don't have to worry about two different inputs having the same output with cryptographic hash functions. Therefore, they can also offer unique functionalities for avoiding any collisions

Cryptographic hash functions are also associated profoundly with the trait of irreversibility. It is basically impossible to derive the original input from the output by using existing technology and techniques.

Cryptographic hash functions are also associated profoundly with the trait of irreversibility. It is basically impossible to derive the original input from the output by using existing technology and techniques.

Another profound characteristic that establishes the significance of hash functions in blockchain and cryptography is the faster computation of hashes. Hash functions can generate outputs faster, thereby ensuring better prospects for faster transaction completion.

The avalanche effect is also a prominent highlight in the traits of cryptographic hash algorithms. The avalanche effect basically implies that a small change in the input results could lead to a completely different output.

SHA or Secure Hash Algorithm is the most widely used cryptographic hash function with many variants such as SHA1, SHA256, MD5, and SHA512 being used commonly. Every cryptographic hash function has its unique function as follows,

MD5 or the Message-Digest algorithm helps in generating a 128-bit hash value. SHA1 is the upgraded version of SHA tailored by NIST and published in accordance with FIPS or Federal Information Processing Standard. SHA256 function involves hash value computing with 32-bit words and message digest amounts to 256 bits SHA512 function involves hash value computing with 64-bit words and message digest amounts to 512 bits

Therefore, it is clearly evident that cryptographic hash functions offer unique benefits of mathematics with various appealing properties. So, how are the properties of cryptographic hash algorithms relevant for the role of cryptography in blockchain? Basically, the characteristics of hash functions ensure the following benefits,

Access to proof of ownership of specific information without revealing the information Prevention of unauthorized modifications in transactions Verification of transaction confirmation without complete knowledge of the block Reduction of transaction bandwidth Development of cryptographic puzzles for transactions

## 3.18 Use of Cryptography in Blockchain

Blockchains make use of two types of cryptographic algorithms, asymmetric-key algorithms, and hash functions. Hash functions are used to provide the functionality of a single view of blockchain to every participant. Blockchains generally use the SHA-256 hashing algorithm as their hash function.

Our approach removes central authorities (CA) and uses the blockchain pub- lic as a distributed ledger of identity and their associated public keys. We use Blockchain to store public keys, digital signatures, and peer information.

Once published, the smart contract code works precisely as programmed. This is one of the main advantages of the platform, the code always interacts as promised, it cannot be falsified, and it never has any downtime. The system is trustworthy, transparent and traceable.

**Confidentiality** Once the communication channel between users is se- cured, peer to peer encryption between endpoints can be set and only authorized users have access to the messages exchanged.

**Message integrity and Authentication** The blockchain checks the validity of the signature, before being stored. Another person can not change/modify the signed agreement or alter exchanged messages during the network transit. Each user has a certificate stored on the blockchain. The smart contract checks the certificate and proves the identity of users. All exchanged messages are signed with private keys associated with the public key on certificates using the ECDSA algorithm.

**Reliability** It is impossible to shut down all computers participating in the blockchain simultaneously. As a result, this database is always online, and its operation never stops.

# REFERENCES

1. B. Laurie, R Stradling, E. M. (2021). “Rfc 9162.

2. Bateman, T. (2022). “Ban proof of work crypto mining to save energy, eu regulator says.” *euronews*.

3. Nakamoto, S. (2014). “Bitcoin: A peer-to-peer electronic cash system" (pdf.” *Bitcoin RFC*.

4. PARLIAMENT, E. (2022a). *Cryptography and Blockchain*. europress.

5. PARLIAMENT, E. (2022b). “Digital services act.” *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*, (52020PC0825).

6. Platt, M., Sedlmeir, J., Platt, D., Xu, J., Tasca, P., Vadgama, N., and Ibañez, J. I. (2021). “The energy footprint of blockchain consensus mechanisms beyond proof-of-work.” 1135–1144.

7. Y, X. (2022). “A survey of distributed consensus protocols for blockchain networks.” *IEEE Communications Surveys and Tutorials*, 22(14321465).