# Project Report Format

1. **INTRODUCTION**
    1.1 Project Overview
    1.2 Purpose
2. **LITERATURE SURVEY**
    2.1 Existing problem
    2.2 References
    2.3 Problem Statement Definition
3. **IDEATION & PROPOSED SOLUTION**
    3.1 Empathy Map Canvas
    3.2 Ideation & Brainstorming
4. **REQUIREMENT ANALYSIS**
    4.1 Functional requirement
    4.2 Non-Functional requirements
5. **PROJECT DESIGN**
    5.1 Data Flow Diagrams & User Stories
    5.2 Solution Architecture
6. **PROJECT PLANNING & SCHEDULING**
    6.1 Technical Architecture
    6.2 Sprint Planning & Estimation
    6.3 Sprint Delivery Schedule
7. **CODING & SOLUTIONING (Explain the features added in the project along with code)**
    7.1 Feature 1
    7.2 Feature 2
    7.3 Database Schema (if Applicable)
8. **PERFORMANCE TESTING**
    8.1 Performace Metrics
9. **RESULTS**
    9.1 Output Screenshots
10. **ADVANTAGES & DISADVANTAGES**
11. **CONCLUSION**
12. **FUTURE SCOPE**
13. **APPENDIX**

# 1. INTRODUCTION

## 1.1 Project Overview

Designing a complete smart contract system for tracking national and state highways, toll collection, and public infrastructure on the Ethereum blockchain is a complex task that requires careful consideration of various aspects such as contract architecture, data storage, user roles, and more. Below is a simplified outline of how you could structure such a system. Please note that this is a high-level conceptual design, and you would need to work with blockchain developers and experts to implement the actual code.
Using blockchain technology, particularly the Ethereum platform, for toll payments is a concept that has been explored to enhance the efficiency and transparency of toll collection systems.

## 1.2 Purpose

### Highway Registry Contract:

This contract maintains a list of registered highways. Each highway is represented by a unique identifier and includes details like the state it's located in, its length, and any other relevant information.

### Toll Collection Contract:

This contract handles toll collection for each registered highway. It stores toll data associated with each vehicle's passage, including the vehicle's license plate and the amount paid.

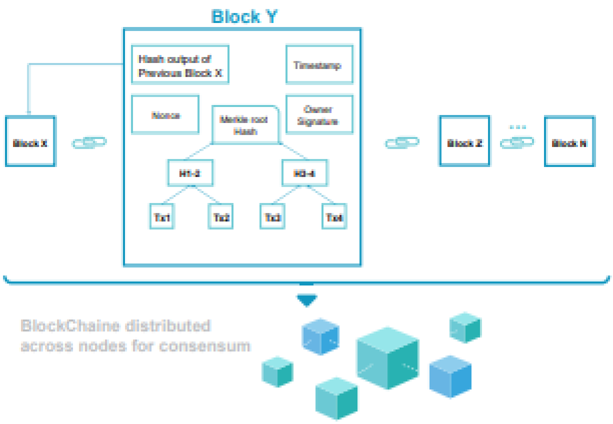
### Public Infrastructure Contract:

This contract maintains information about public infrastructure projects associated with each highway. It can track projects like road repairs, maintenance, and construction.

# 2. LITERATURE SURVEY

The use of Blockchain technology has recently become widespread. It has emerged as an essential tool in various academic and industrial fields, such as healthcare, transportation, finance, cybersecurity, and supply chain management. It is regarded as a decentralized, trustworthy, secure, transparent, and immutable solution that innovates data sharing and management. This survey aims to provide a systematic review of Blockchain application to intelligent transportation systems in general and the Internet of Vehicles (IoV) in particular.

## 2.1 Existing Problem




Asymmetric cryptography, also known as public key cryptography, is a data encryption–decryption technique that provides an extremely high level of security, information protection, authenticity, and confidentiality. The technique allows a user to sign a transaction in the public register of the Blockchain, therefore certifying that the user is the author.

## 2.2 References

- **Public Infrastructure and Toll Systems**: Identification of challenges in traditional infrastructure tracking and toll payment methods, such as manual record-keeping, fraud, lack of transparency, etc.

- **Blockchain Applications in Public Infrastructure**: Exploration of how blockchain technology can be applied to public infrastructure management. For example, tracking maintenance records, construction updates, and other relevant data on a blockchain.

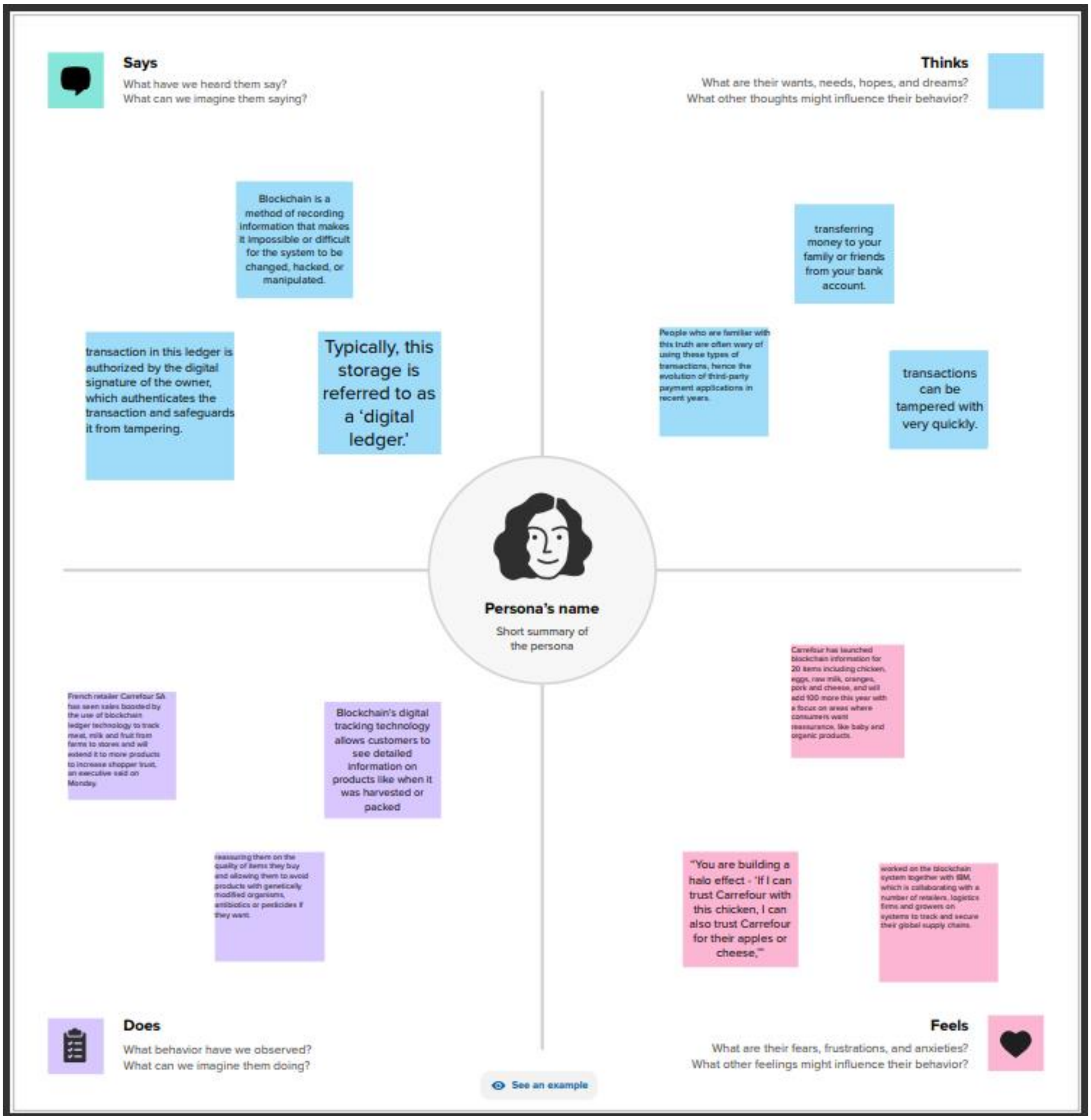
- **Blockchain Applications in Toll Payments:** Discussion of how blockchain, particularly Ethereum, can revolutionize toll payment systems. This might involve the use of smart contracts to automate toll collection, reduce transaction costs, and enhance efficiency.

## 2.3 Problem Statement Definition

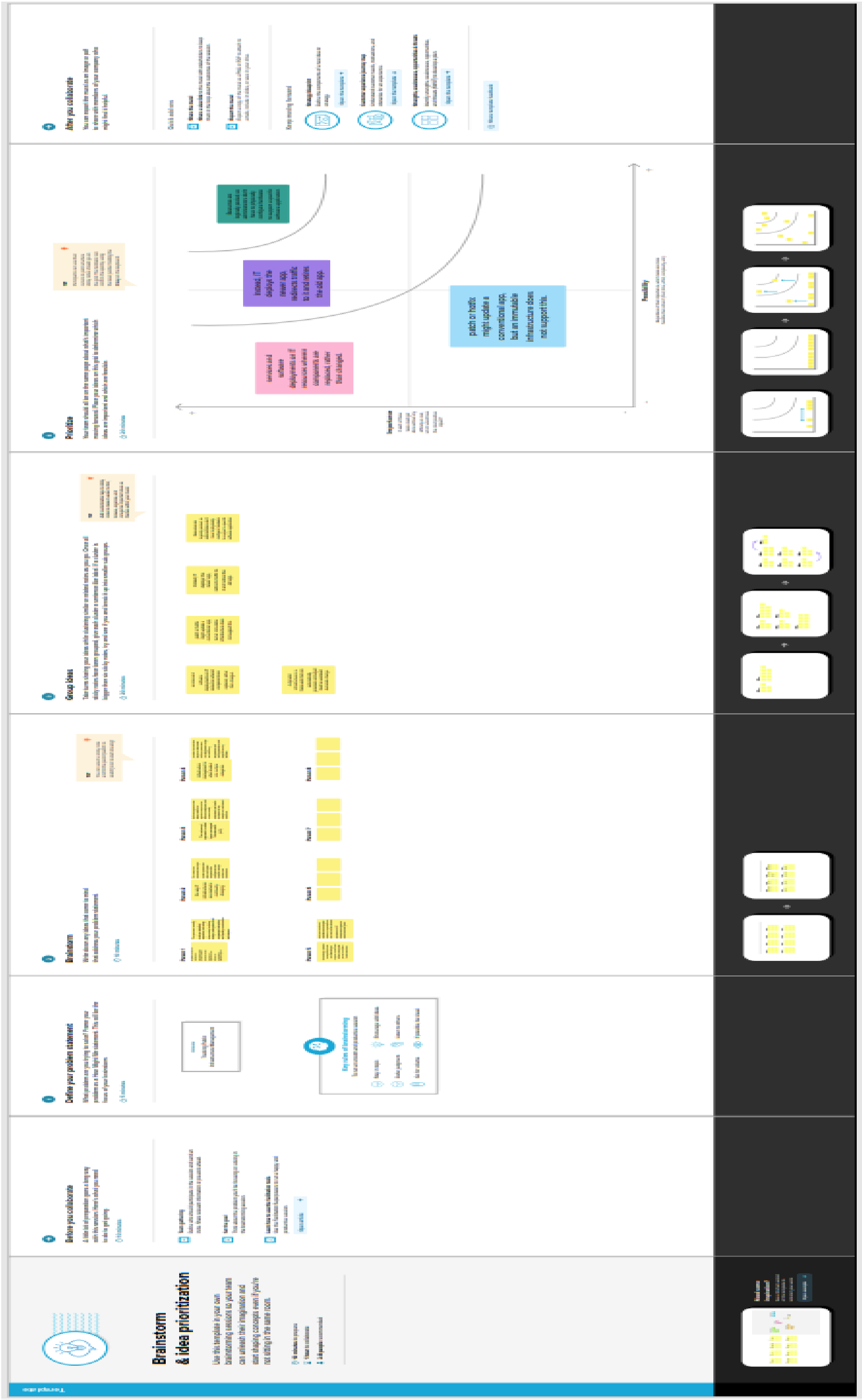
A literature survey on tracking public infrastructure and toll payments using the Ethereum blockchain would likely cover research, articles, and papers that explore the potential benefits, challenges, and applications of utilizing blockchain technology, specifically Ethereum, in the domain of public infrastructure management and toll payment systems. As of my last knowledge update in September 2021, I can provide you with a general overview of what such a literature survey might encompass

# 3. IDEATION & PROPOSED SOLUTION

## 3.1 Empathy Map Canvas



## 3.2 Ideation & Brainstorming



# 4. REQUIREMENT ANALYSIS

### Scalability

The scalability of a TM system refers to its capability to expand and adapt easily to the increasing number of IoT devices or participating nodes in the IoT network without affecting its performance. The growing number of connected devices and sensors require the TM system capacity to be able to adapt to growing amounts of trust data [78].

### Adaptability

The adaptability of a TM refers to its ability to adapt to changes in a dynamic environment. A Blockchain-based TM system should be adaptive and Flexible in IoT environments. To accommodate dynamic trust relationships and evolutionary policies, TM systems are required to frequently update themselves.

### Security And Privacy

The security of TM systems refers to the protection of trust-related information from malicious manipulation and corruption while allowing it to be accessible and productive for the other participating IoT objects. Although Blockchain technology can guarantee the integrity of data when IoT is integrated with Blockchain, a serious issue arises related to data reliability from IoT devices in cases where malicious data is received from IoT devices. Data can be corrupted due to the failure of IoT devices, such as fake devices or hacked IoT networks and devices.

## 4.1 Functional Requirements

### 1. Trust

Blockchain creates trust between different entities where trust is either nonexistent or unproven. As a result, these entities are willing to engage in business dealings that involve transactions or data sharing they may not have otherwise done or would have required an intermediary.

### 2. Decentralized Structure

Blockchain proves its value when there's no central actor who enables trust, said Daniel Field, director of innovation and global head of blockchain at UST, a provider of digital technology and services. In addition to enabling trust among participants who are unknown to each other, blockchain enables data sharing within an ecosystem of businesses where no single entity is exclusively in charge.

### 3. Improved Security And Privacy

The security of blockchain-enabled systems is another leading benefit of the technology. Blockchain creates an unalterable record of transactions with end-to-end encryption to shut out fraud and unauthorized activity. Additionally, data on the blockchain is stored across a network of computers, making it nearly impossible to hack, unlike conventional systems that store one copy of the data on servers.

### 4. Reduced Costs

Blockchain's inherent design can also cut costs for organizations. It brings certain efficiencies to transaction processing, reduces manual tasks such as aggregating and amending data, and eases reporting and auditing processes.

## 4.2 Non-Functional Requirements

### 1. Visibility And Traceability

Walmart's use of blockchain isn't just about speed. It's also about the ability to trace the origin of mangoes and other products. Blockchain visibility and traceability applications also help retailers manage inventory, respond to problems or questions, and confirm the origin of merchandise.

## 2. Immutability

Immutability simply means that transactions, once recorded on a blockchain, can't be changed or deleted. All transactions are time- and date-stamped, so there's a permanent record that can be used to track information over time, enabling secure, reliable auditing of information. Paper-based filing and older computer systems, in contrast, are error prone, and they can be more easily corrupted or retired.

## 3. Individual Control Of Data

Blockchain gives individuals unprecedented control over their digital data. "In a world where data is a very valuable commodity, the technology inherently protects the data that belongs to you while allowing you to control it," said Michela Menting, senior research director at ABI Research. Individuals and organizations can decide what pieces of their digital data they want to share and with whom and for how long, with limits enforced by blockchain-based smart contracts.

## 4. Tokenization

Tokenization is the process whereby the value of a physical or digital asset is converted into a digital token that is then recorded and shared on a blockchain. Tokenization has caught on with digital art and other virtual assets, but it has broader applications that could smooth business transactions, said Joe Davey, a partner at the technology consulting firm West Monroe. Utilities, for example, could use tokenization to trade carbon emission allowances under carbon cap-and-trade programs.

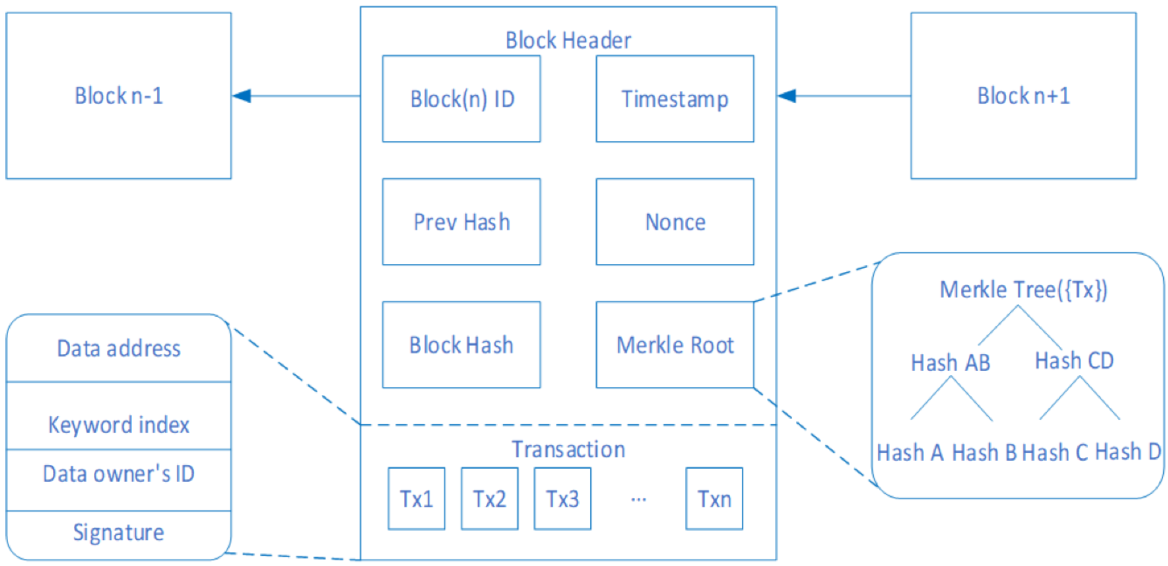
# 5.PROJECT DESIGN

To differentiate between different groupings of data, a conceptual framework of multiple data levels has been developed with which data can be logically sorted into characters, fields, records, files, and databases. (O'Brien & Marakas, 2010.) A character can be a single alphabetic, numeric, or other symbol. It is the most fundamental data element. This is the logical view as opposed to the physical or hardware view of data, according to which the bit or byte is the most basic element. So, from the user's viewpoint, a character is the most basic data element to be manipulated and observed. (O'Brien & Marakas, 2010.) A field, or data item, is the next higher level of data, and it is a collection of related characters. As an example, the characters in a person's name can constitute a name field, and the grouping of numbers in a person's salary amount forms a salary field. A data field usually represents an attribute (a characteristic) of an entity (a person, an object, a place, or an event). (O'Brien & Marakas, 2010.)

## 5.1 Data Flow Diagrams & User Stories

### Block Structure Reconstruction Diagram

The blockchain system consists of Block Header, Block Body, and Policy Header, which form a chain structure with the sequence in the form of a "series connection". The block header encapsulates the version number, timestamp, hash value of the previous block, Merkle root, and random value of the solution. The block body records the number of transactions. In addition to the Genesis block, each block in the blockchain contains the hash value of the previous block [6].

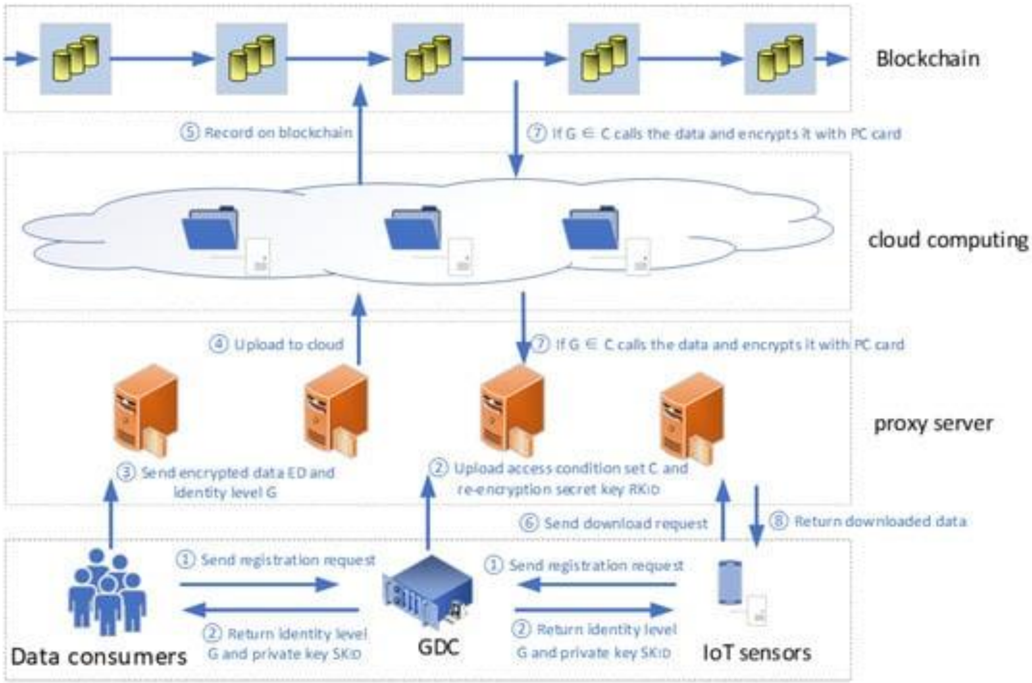


## Division Of Iot Data Flow Module

The Internet of Things is a new technology paradigm derived from the Internet era, which uses the network to intelligently control various terminal devices [9,10]. A global or specific local area network can be formed according to specific needs to achieve the interoperability of people and things [11]. The Internet of Things technology can be used in various fields, such as medical care [12,13], agricultural science and technology [14], and the ecological environment [15].


## Agent Re-Encryption Technology Based On Blockchain

Proxy re-encryption technology eliminates the dependence on third parties and decrypts data by transferring different keys to different users instead of using shared public keys as an intermediate link, which not only increases the security of information, but also reduces the complexity of operations [16,17,18,19,20,21,22,23]. Gao [16] proposed a combination of blockchain and proxy re-encryption technology for device communication and data sharing in the IoT community. Chen [17] proposed a threshold-based proxy re-encryption algorithm combined with the blockchain consensus algorithm, which eliminates the restrictions on the secure storage and distribution of private data in a distributed network and meets a wide range of data access needs.




## 5.2 Solution Architecture

### Main Advantages Of Blockchain Technology :

- Since there’s no central authority to oversee operations, the blockchain is an ideal register for joint business ventures.
- The digital signature and verification process used in blockchains helps prevent fraudulent activity.
- Information isn’t centralized, preventing it from being lost.

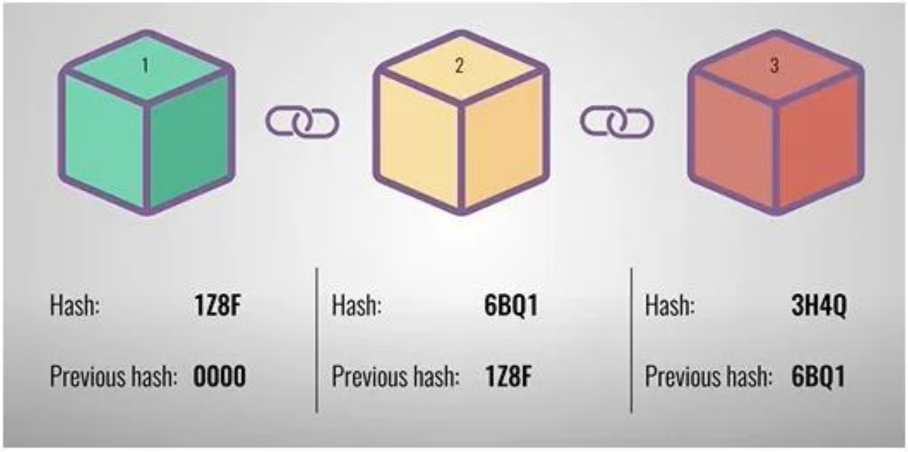
### What The Blockchain Is And How It Works :

This technology was originally described in 1991 by a group of researchers and was originally intended to timestamp digital documents so it wouldn’t be possible to backdate or tamper with them.

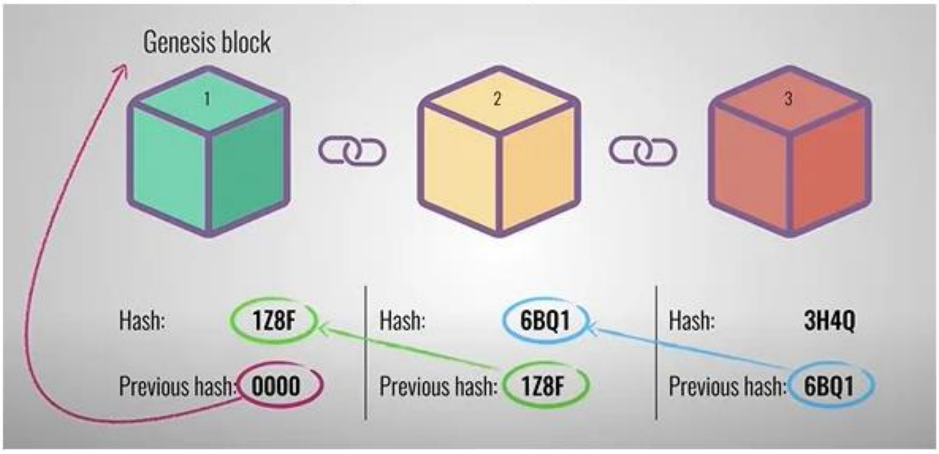
Each block in a blockchain contains some data, the hash of the block itself, and the hash of the previous block. The data stored inside a block depends on the type of blockchain.

## How To Write Acceptance Criteria: Examples And Best Practices

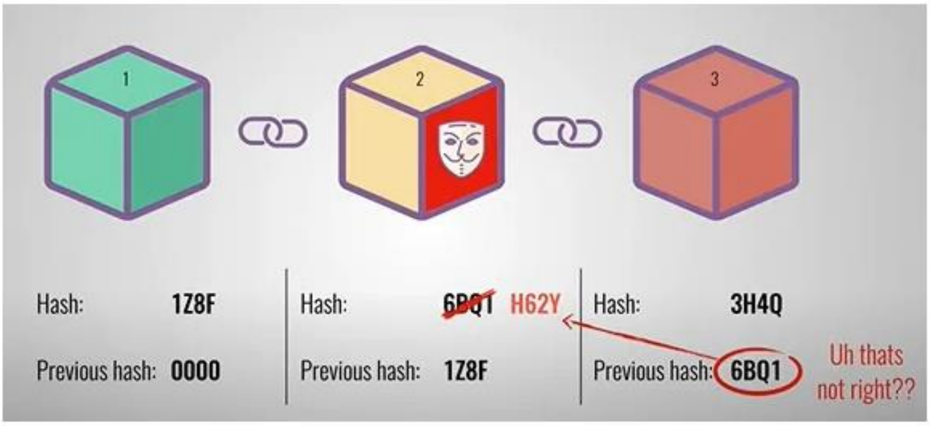
The third element inside each block is the hash of the previous block. This effectively creates a chain of blocks, and it's this technique that makes a blockchain so secure. Let's look at an example.




Block number 3 points to block number 2, and block number 2 points to block number 1. Now, the first block is a bit special, as it cannot point to previous blocks because it's the first. This block is called the genesis block.




This causes the hash of that block to change. In turn, that will make block 3 and all following blocks invalidbecause block 3 will no longer store a valid hash of the previous block.

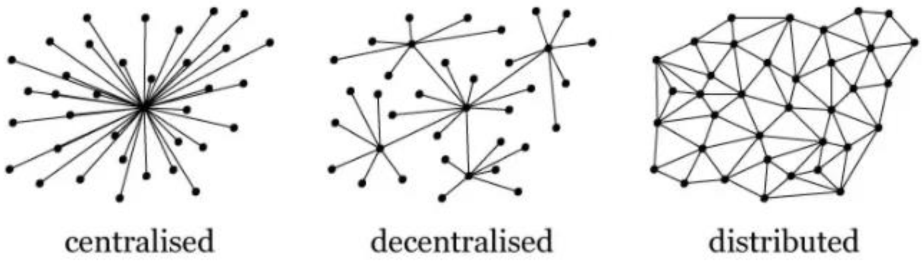



## Key Characteristics Of The Blockchain Architecture :

- **Cryptography** — Blockchain transactions are verified and trustworthy because of complex computations and cryptographic proof between the parties.
- **Immutability** — Records in a blockchain can’t be modified or deleted.
- **Provenance** — It’s possible to trace the origin of each transaction in the blockchain ledger.
- **Decentralization** — Every member of the blockchain structure is able to access the entire distributed database. Unlike in a centralized system, a consensus algorithm is responsible for network management.
- **Anonymity** — Every member of the blockchain network has a generated address, not a user ID. This preserves the anonymity of users, especially in a public blockchain.
- **Transparency** — The blockchain system is unlikely to be damaged as it takes enormous computing power to completely rewrite the blockchain network.

## Blockchain Architecture Explained :

A blockchain is an open financial ledger or record in which every transaction is authenticated and authorized. A blockchain is designed as a decentralized network of millions of computers, commonly referred to as nodes.




## Creating a Blockchain Network :

- Gold mining companies
- Government institutions
- Gold transporters
- Gold sellers
- Goldsmiths

# 6. PROJECT PLANNING & SCHEDULING

- Inclusivity: Eliminate or reduce economic, technical, or social barriers to enable inclusion, empowerment of end-users, last-mile access, and avoid erroneous algorithmic bias.

- Interoperability: Enable interoperability by using and building on open standards and specifications with a technology neutral approach, wherever possible, while accounting for appropriate safeguards and keeping in view the legal considerations and technical constraints.

- Modularity and Extensibility: Extensible approach implies a building block or modular architecture to accommodate changes/modifications without undue disruption.

- Scalability: Use flexible design to easily accommodate any unexpected increase in demand and/or to meet expansion requirements without changing existing systems.

- Security and Privacy: Adopt an approach that embeds key privacy enhancing technologies and security features within the core design to ensure individual privacy, data protection, and resilience based on standards offering appropriate levels of protection.

- Collaboration: Encourage the participation of community actors at different stages of planning, designing, building, and operating to facilitate and promote a culture of openness and collaboration. Enable the development of user-centric solutions and facilitate widespread and sustained adoption and allow innovators to develop new services.

- Governance for Public Benefit, Trust and Transparency: Maximise public benefit, trust and transparency while respecting applicable legal frameworks. This means that laws, regulations, policies and capabilities should seek to ensure that these systems are safe, secure, trusted and transparently governed, and also promote competition and inclusion, and adhere to principles of data protection and privacy.

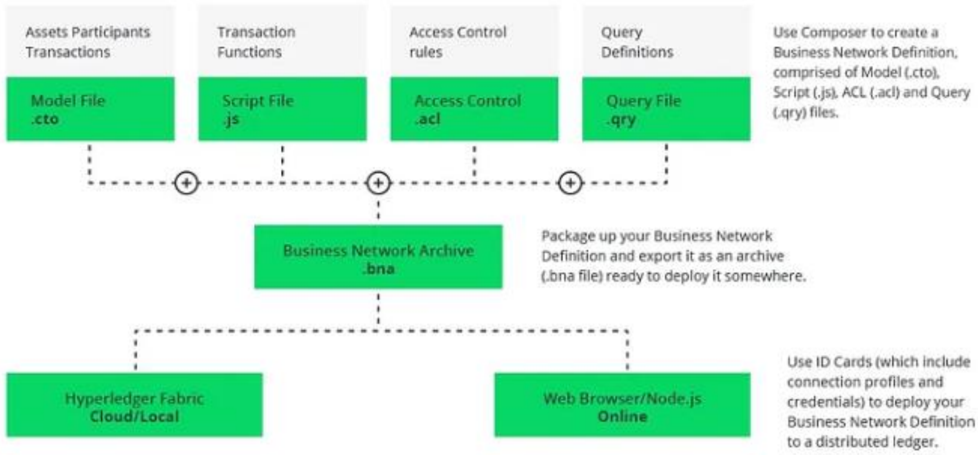
- Grievance redress: Define accessible and transparent mechanisms for grievance redress, i.e., user touchpoints, processes, responsible entities, with a strong focus on actions for resolution.

- Sustainability: Ensure sustainability through adequate financing and technological support and enhancements to facilitate uninterrupted operations and seamless userfocused service delivery.

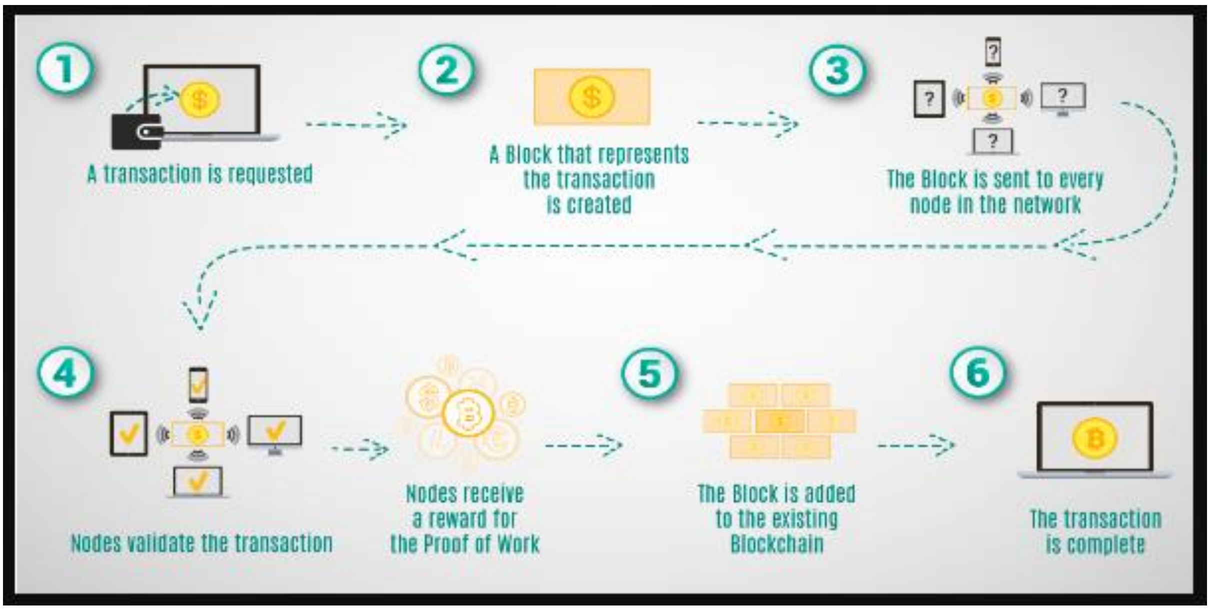
- Human rights: Adopt an approach that respects human rights at every stage of the planning, designing, building, and operating.

- Intellectual Property Protection: Provide adequate and effective protection and enforcement of intellectual property rights for the rights-holders of technologies and other materials used based on existing legal frameworks.

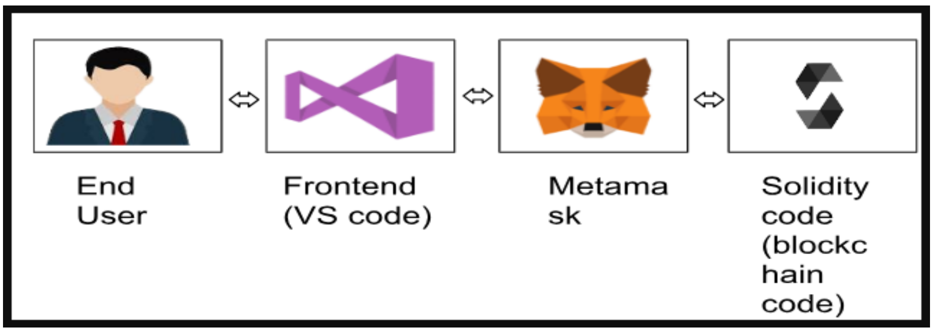
- Sustainable Development: Seek to develop and deploy these systems that contribute to the implementation of the 2030 Agenda for Sustainable Development and achievement of Sustainable Development Goals.




## 6.1 Technical Architecture




## Technical Stack:



## 6.2 Sprint Planning & Estimation

Introduction to Computer Network, Types- LAN,MAN & WAN, Data Transmission Modes- Serial & Parallel, Simplex, Half Duplex & Full Duplex, Synchronous & Asynchronous Transmission, Transmission Medium- Guided & Unguided, Cables- Twisted Pair, Coaxial Cable & Optical Fibre, Networking Devices-Repeaters, Hub, Switch, Bridge, Router, Gateway and Modem, Performance Criteria- Bandwidth, Throughput, Propagation Time & Transmission Time.

Switching- Circuit Switching, Message Switching & Packet Switching Multiplexing: FDM – Frequency Division Multiplexing, WDM – Wavelength Division Multiplexing & TDM – Time Division Multiplexing.

Data Link Layer: Introduction, Design Issues, Services, Framing, Error Control, Flow Control, ARQ Strategies, Error Detection and Correction, Parity Bits, Cyclic Redundant Code (CRC), Hamming Codes.

Network Layer & Transport Layer: Introduction, Design Issues, Services, RoutingDistance Vector Routing, Hierarchical Routing & Link State Routing, Shortest Path Algorithm- Dijkstra's Algorithm

## 6.3 Sprint Delivery Schedule

Supply chain management involves overseeing the flow of goods and services, such as tracking the movement and storage of raw materials, inventory, and finished goods. It has been identified as one area that can benefit from blockchain technology, a shared database maintained by a network of computers connected to the internet.

The new blockchain network is called Trust Your Supplier and alongside IBM, the other founding participants were Anheuser-Busch InBev, Cisco, GlaxoSmithKline, Lenovo, Nokia, Schneider Electric and Vodafone.

Chainyard, a blockchain specialist firm, is providing the technology and building the network using IBM’s blockchain platform. The other companies, meanwhile, are putting their supplier data onto the network and contributing their expertise to expand the network.

Traditional methods of managing suppliers often involve cumbersome manual processes, which make it difficult to verify identities and track documents such as ISO certifications, bank account information, tax certifications, and certificates of insurance, IBM said.

# 7. CODING & SOLUTIONING (Explain the features added in the project along with code)

```
AWSTemplateFormatVersion: "2010-09-09"
Resources:
WebInstance:
Type: AWS::EC2::Instance
Properties:
InstanceType: t3.small
ImageId: ami-0123456
KeyName: web_server_test_key
SecurityGroupIds:
- sg-dfdd00011
SubnetId: subnet-a000111x
Tags:
-
Key: Name
Value: Web_Server
```

## 7.1 Feature 1

```
terraform {
required_providers {
aws = {
source  = "hashicorp/aws"
version = "~> 3.27"
}
}
}
provider "aws" {
access_key = "aws_access_key"
secret_key = "aws_secret_key"
// shared_credentials_file = "/Users/.aws/creds"
region = "us-west-1"
}
resource "aws_instance" "web_server" {
ami                        = "ami-0123456"
instance_type              = "t3.small"
subnet_id                  = "subnet-a000111x"
vpc_security_group_ids = "sg-dfdd00011"
key_name                   = "web_server_test_key"
tags = {
Name = "Web_Server"
}
}
```

## 7.2 Feature 2

```
- hosts: localhost
gather_facts: False
vars_files:
- credentials.yml
tasks:
- name: Provision EC2 Instance
ec2:
aws_access_key: "{{aws_access_key}}"
aws_secret_key: "{{aws_secret_key}}"
key_name: web_server_test_key
group: test
instance_type: t3.small
image: "ami-0123456"
wait: true
count: 1
region: us-west-1
instance_tags:
Name: Web_Server
register: ec2
```

## 7.3 Database Schema (If Applicable)

### Private Blockchain Networks

Private blockchains operate on closed networks, and tend to work well for private businesses and organizations. Companies can use private blockchains to customize their accessibility and authorization preferences, parameters to the network, and other important security options. Only one authority manages a private blockchain network.

### Public Blockchain Networks

Bitcoin and other cryptocurrencies originated from public blockchains, which also played a role in popularizing distributed ledger technology (DLT). Public blockchains also help to eliminate certain challenges and issues, such as security flaws and centralization. With DLT, data is distributed across a peer-to-peer network, rather than being stored in a single location. A consensus algorithm is used for verifying information authenticity; proof of stake (PoS) and proof of work (PoW) are two frequently used consensus methods.

### Permissioned Blockchain Networks

Also sometimes known as hybrid blockchains, permissioned blockchain networks are private blockchains that allow special access for authorized individuals. Organizations typically set up these types of blockchains to get the best of both worlds, and it enables better structure when assigning who can participate in the network and in what transactions.

## 8.PERFORMANCE TESTING

### Why Do You Need Performance Testing in a Blockchain Network

- To monitor the health of connected peers (disk i/o, CPU usage, and memory utilization)
- To ensure scalability to support increasing the number of nodes
- To maintain data integrity without any packet loss
- To ensure a seamless transaction
- To track the number of failed/delayed transactions due to timeouts

## The KPIs To Be Monitored

- **Transaction-level:** At the transaction level, it is recommended to monitor the throughput, transaction failures, response time, etc.

- **Network-level:** At this level, the number of transactions per second, disk I/O, transactions per CPU, etc. are evaluated.

- **Node-level:** Node-level monitoring includes analyzing block time, block size, transaction latency, etc.

## Challenges of Running Performance Tests On a Blockchain Network

1) Transaction Validation in the Test Environment
   Transaction validation can take several minutes or even longer for a single piece of data to be stored.

2) Block and Chain Size Monitoring
   Without sufficient block and chain size validation, blockchain applications could fail.

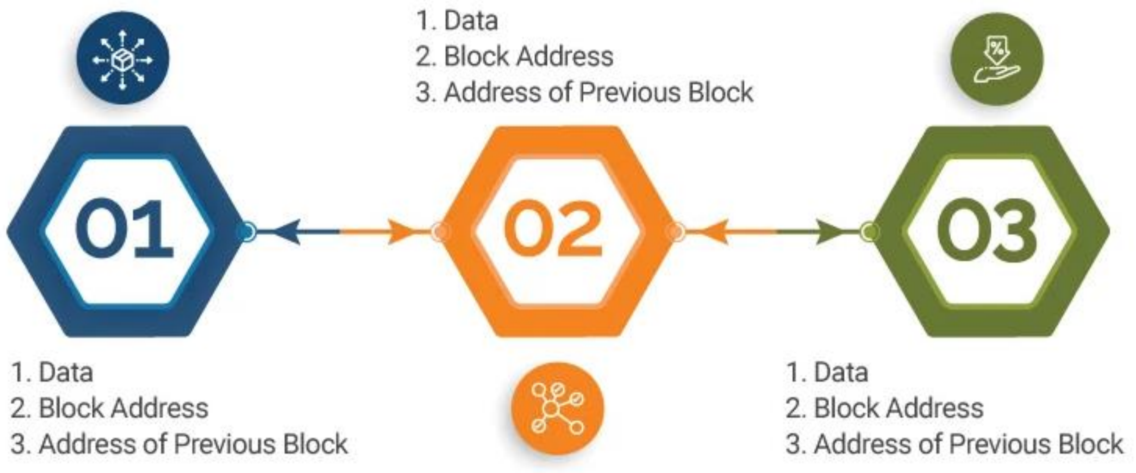
3) Lack of Standardization in Blockchain Testing
   Lack of technical, standardization, operational, and legal competence is another important factor in the implementation of blockchain testing.

4) Lack of Skills
   Engineers need to be knowledgeable in a variety of fields in order to create and test blockchain-based systems.

## 8.1 Performance Matrics

### Know About Blockchain Technology

**Blockchain:** A chain of connected blocks using cryptography and spread over distributed ledger in the cloud.




### Blockchain Types

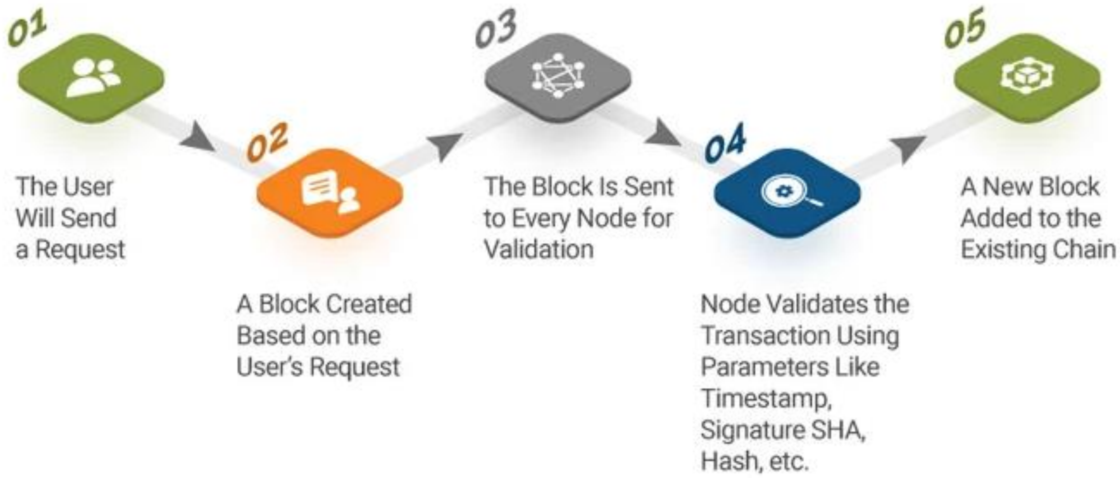
**Public Blockchain:** Anyone can access it without any permission. They are open to following the idea of decentralization.

**Private Blockchain:** Only known users of a single organization can access the network. These are not decentralized and only selected nodes can participate in the process.

**Consortium Blockchain:** Only known users of multiple organizations can access the network. One of its main benefits is that it can validate, and also initiate or receive transactions.

## How Does the Request Cycle for Blockchain Work in the Backend

The following diagram represents the backend request cycle for blockchain-based application:



# 9. RESULTS

## 9.1 Output screenshots

```
AWSTemplateFormatVersion: "2010-09-09"
Resources:
WebInstance:
Type: AWS::EC2::Instance
Properties:
InstanceType: t3.small
ImageId: ami-0123456
KeyName: web_server_test_key
SecurityGroupIds:
- sg-dfdd00011
SubnetId: subnet-a000111x
Tags:
-
Key: Name
Value: Web_Server
```

```
- hosts: localhost
gather_facts: False
vars_files:
- credentials.yml
tasks:
- name: Provision EC2 Instance
ec2:
aws_access_key: "{{aws_access_key}}"
aws_secret_key: "{{aws_secret_key}}"
key_name: web_server_test_key
group: test
instance_type: t3.small
image: "ami-0123456"
wait: true
count: 1
region: us-west-1
instance_tags:
Name: Web_Server
```

# 10. ADVANTAGES & DISADVANTAGES

## Advantages

One major advantage of blockchains is the level of security it can provide, and this also means that blockchains can protect and secure sensitive data from online transactions. For anyone looking for speedy and convenient transactions, blockchain technology offers this as well. In fact, it only takes a few minutes, whereas other transaction methods can take several days to complete. There is also no third-party interference from financial institutions or government organizations, which many users look at as an advantage.

## Disadvantages

Blockchain and cryptography involves the use of public and private keys, and reportedly, there have been problems with private keys. If a user loses their private key, they face numerous challenges, making this one disadvantage of blockchains. Another disadvantage is the scalability restrictions, as the number of transactions per node is limited. Because of this, it can take several hours to finish multiple transactions and other tasks. It can also be difficult to change or add information after it is recorded, which is another significant disadvantage of blockchain.

# 11.CONCLUSION

Although we just skimmed the industry-wide potential of blockchain applications in this article, the career potential in this field is growing exponentially. Getting ahead of the game is always a good strategy for any professional. At Simplilearn, our latest and most up-to-date course on this emerging field is the Professional Blockchain Certificate Program in Blockchain. In partnership with the world-renowned university, IIT Kanpur, this program will help you get on track.

In this blockchain program, you will learn how to master blockchain concepts, techniques, and tools like Truffle, Hyperledger, and Ethereum to build blockchain applications and networks.

# 12.FUTURE SCOPE

Bockchain has a lot of potential to be used in different areas, particularly in the field of Autonomous Vehicles, as discussed through this paper. However, before this can be deployed on a large scale, several problems surrounding the technology must be examined and repaired to ensure that it meets necessary requirements for energy consumption, resource use, and response time [24,25].

Nevertheless, the general form of Blockchain is quite inefficient in terms of consuming computation resource. Lightweight applications of Blockchain have shown a great deal of progress in reducing computational resource strain, and, even now, research is ongoing to improve on this current drawback. Blockchain technology itself also does not have an inherent flaw in computational resource consumption: this is instead linked directly to its PoW algorithm, which has been studied, with some proposals being put forth to reduce resource consumption [24,133]. As alternative algorithms to PoW are studied, Blockchain will likely be able to overcome its current high degree of resource use.

The high cost of implementation for Blockchain is the next challenge, which could be expensive in applications, such as CAVs. There are not many works discussing the expected cost for a large implementation, but examples of costs to develop other common blockchain applications are discussed across several papers [134,135]. However, as with many technologies, this cost can be expected to reduce significantly over time as more people study it, improve its efficiency, and become familiar with its structure and implementation enough to increase the number of workers who are able to work on implementing large-scale networks as needed.

Another challenge with using Blockchain in CAVs application is the fact that it requires high energy consumption. However, that depends on the exact type of blockchain type, there may be a much lower drain on energy use, as in non PoW models in use today [136]. While a good deal of blockchain applications today are fairly energy-intensive, a number of papers have also thought of how to resolve this issue, coming to a variety of possible solutions depending on the type of application desired [25]. In addition, Blockchain has shown that it provides a platform for users to interact more directly with their energy use and obtainment, as in proposed energy exchanging mechanisms between vehicles, as discussed by papers in the past, which could make up for higher rates of consumption in allowing more user control of how much energy they obtain at a time and from where they can access it [137].

Another main drawback of Blockchain is the responding time when more users are connected to the network, which makes them no suitable for safety applications. Delays are a known problem for Blockchain today, and as such, there is currently a lot of discussion on how to proceed when working to resolve the issue, as discussed in several papers [138]. Although there is not currently an agreed-upon solution to be used in all blockchain implementations, many incorporations of blockchain technology today still use their own methods to account for the issue of delay when under use by many people. For example, proposed methods like parallel proof of work [139] have shown to allow significant improvement in this area already. More lightweight blockchain applications have also been implemented, as with Block4Forensic, to improve the speeds of Blockchain when several users are in a network. With these examples, it's clear that these flaws are already noted and are currently being examined in a variety of ways to come to a resolution. In time, this flaw will most likely be mitigated, at which point blockchain technology will be closer to being ready for full use.

# 13.APPENDIX

## Appendix I: Objectives, Scope, and Methodology

We examined (1) non-financial applications of blockchain, including potential benefits and challenges, (2) financial applications of blockchain, including potential benefits and challenges, and (3) policy options that could help enhance benefits or mitigate challenges of blockchain technologies.

### Scope

We focused our research to include financial applications, shared data services, and smart contracts. Financial applications includes cryptocurrencies and decentralized finance (DeFi). Shared data services includes applications in supply chain management, public records, voting, and real estate. We did not assess all possible applications of blockchain technologies. For example, we excluded decentralized marketplaces.

# Appendix II: Expert Participation

We collaborated with the National Academies of Sciences, Engineering, and Medicine to convene a two-day meeting of experts to inform our work on blockchain technology; the meeting was held virtually on July 14–15, 2021. The experts who participated in this meeting are listed below. Many of these experts gave us additional assistance throughout our work, including 5 who reviewed our draft report for accuracy and provided technical comment.

**Kyle Burgess**
Specialist Leader
Deloitte

**Quinn DuPont**
Founder and CEO
Alumni Labs

**Tonya Evans**
Professor
Penn State Dickinson Law
Penn State Institute for Computational and Data Sciences Co-Hire

**Mark D. Fisk**
IBM Consulting – Federal
Partner - Data and Technology Transformation Services

**Stefan Gstettner**
Partner and Director
Boston Consulting Group

**Emin Gun Sirer**
Associate Professor and Co-Director, Initiative for Cryptocurrencies and Smart Contracts
Cornell University

**Stuart Levi**
Partner, Blockchains and Digital Assets; Intellectual Property and Technology; Outsourcing; Cybersecurity and Privacy
Skadden

**Anil John**
Technical Director, Silicon Valley Innovation Program
Department of Homeland Security

**Caroline Malcolm**
Head, Global Blockchain Policy Centre
Organisation for Economic Co-operation and Development

**Pramita Mitra**
Research Supervisor, IoT and Blockchain Applications
Ford Motor Company

**Dawn Song**
Professor, Computer Science
University of California, Berkeley

**Mark Treshock**
Global Blockchain Solutions Leader, Healthcare and Life Sciences
IBM

# Appendix III: Selected Definitions

- Best practices. Processes, practices, and systems identified in public and private organizations that performed exceptionally well and are widely recognized as improving an organization’s performance and efficiency in specific areas.

- Consensus protocol. The steps a blockchain takes to ensure verified blocks are added to the blockchain and unverified blocks are ignored. It is the way in which at least a majority of blockchain network members agree on the information of a proposed transaction, which is then updated to the ledger.
- Cryptocurrencies. Digital assets, credits, or units that are built on technologies like blockchain. Users can secure and authenticate cryptocurrency transactions using cryptographic techniques on the blockchain. Blockchain protocols can generate cryptocurrencies.
- Immutable. Immutable is the property of not being subject to change. In the context of data, it refers to data that can only be written, not modified or deleted.
- Node. Blockchain nodes consist of individuals systems—computers or servers—in the peerto-peer blockchain network that are operated by a single person, group, business, or organization.

  Oracles. Oracles are external sources including people, devices, or software that add information to a blockchain, such as freight shippers in a product supply chain. Decentralized protocols may rely on oracles to access off-chain information, such as cryptoasset exchange rates, in order to process transactions on the blockchain.

- Regulatory sandbox. Regulatory sandboxes are a safe space for novel products or services and define rules and requirements for eligibility and testing and may provide special authorizations, exemptions, or other relief to eligible businesses for a limited period.
- Smart contracts. Software code stored on a blockchain that contains a set of conditions, so that transactions automatically trigger when the conditions are met.
- Stablecoins. Cryptocurrencies designed to maintain a stable value compared to other types of cryptocurrency by maintaining reserve assets that could include fiat currencies, corporate and municipal bonds, cryptocurrencies, or other digital assets.

- Standards. A document, established by consensus and approved by a recognized body, which provides—for common and repeated use—rules, guidelines, or characteristics for activities or their results aimed at optimizing order.
- Tokens. Tokens are digital assets on the blockchain. The process of adding new digital assets to a blockchain is called tokenization.
- Virtual currencies. Digital representations of value, usually other than a government-issued legal tender (e.g., U.S. dollars), that function as a unit of account, a store of value, or a medium of exchange. Cryptocurrencies are a type of digital currency