# Blockchain For Identity Verification

## Blockchain Case Study Report

## Group: 2

## Presented By:

| Team Member Name | Regd No. |
|---|---|
| Muskan Bharti | 21020031 |
| Syed Faizan Ali | 21020032 |
| Tapoban Acharya | 21020033 |
| Sushmita Singh | 21020034 |
| Pallavi Kumari | 21020035 |

## Under the Guidance of:

**Ms. Swati Sipra Das**

# CONTENT

# ABSTRACT

In the era of digital advancement, our lives are increasingly intertwined with the internet and computers. However, this digital age brings with it a growing concern—identity theft, a perilous act where malicious individuals attempt to steal our personal information for harmful purposes. The report starts by highlighting the limitations of traditional registration processes. *Traditional methods* of confirming our identity, often relying on central databases and paperwork, have proven to be inadequate in ensuring the security, accuracy, and privacy of our personal data. It emphasizes that requiring physical documents can be inconvenient, prone to loss, and a security risk if unauthorized individuals gain access to them. These challenges underscore the need for a more secure and efficient solution. The central objective of the paper is to introduce the concept of using *blockchain technology* to address these challenges.

This study highlights the urgent need for a more robust and efficient system to tackle the rising threat of identity theft. We are going to discuss is on leveraging blockchain technology for identity verification, specifically using Aadhaar as a real-world example. Aadhaar is a 12-digit unique identification number issued to residents of India.

The proposed solution advocates for leveraging blockchain technology—a secure, immutable, and decentralized digital ledger—to enhance the security and privacy of personal information. By employing a user-centric approach, this system aims to empower individuals with control over their data, allowing them to authorize access selectively. Furthermore, integration with government-issued ID systems, like Aadhar, enhances the credibility and trustworthiness of the verification process. It explains how blockchain technology can be used to securely store and verify Aadhaar information. When a user needs to verify their identity, they can request access to their Aadhaar data stored on the blockchain. The system would then check whether the requested details match the information on the blockchain. If they do, the system would return a *"true"* response, confirming the user's identity. Otherwise, it would return *"false."* Aadhaar is a widely recognized and used identification system in India. Using it as a real-world example helps illustrate the practicality and relevance of the proposed blockchain-based identity verification system. The aim is to propose a blockchain-based solution for identity verification.

# INTRODUCTION

The crime of identity theft, an unauthorized access to a person’s personal information, has impacted many people especially in the recent years and the numbers increase yearly. In the digital age, where our lives are increasingly intertwined with online interactions and transactions, the security of our personal information has become a paramount concern. Identity theft, the malicious act of unauthorized access to and misuse of our private data, has emerged as a grave threat. The conventional methods of *identity verification*, relying heavily on centralized databases and traditional paperwork, have demonstrated their limitations in ensuring the security, accuracy, and privacy of our personal data. This necessitates a fundamental shift in how we approach identity verification. This study focuses on the urgency of fortifying our systems against the rising threat of identity theft. It underscores the vulnerabilities posed by centralized data storage, which becomes an attractive target for malicious actors seeking unauthorized access. Moreover, the lack of visibility and control individuals have over their personal data within these centralized systems has led to a deficit of trust and transparency. In response to these challenges, we propose an innovative approach— a Blockchain-Based Identity Verification System. The rapid advancement of technology has digitized our lives, from financial transactions to social interactions. This digitization has exposed individuals to the risks associated with cybercrimes, particularly identity theft. Malicious actors seek unauthorized access to sensitive personal data, leading to financial fraud, reputational damage, and emotional distress.

The Blockchain-Based Identity Verification System we envision aims to reimagine how individuals' identities are verified and managed. Through this system, individuals will have control over their identity data, authorizing access only to trusted entities. *Decentralized Identifiers (DIDs) linked to Ethereum addresses* will establish a robust connection between an individual's digital identity and their blockchain address, bolstering security and privacy. Additionally, we aspire to integrate with government-issued IDs, like Aadhar, to further enhance the accuracy and credibility of the verification process. Moreover, this system addresses the limitations of traditional identity verification by incorporating a transparent verification process, offering users visibility into data access and utilization. Additionally, the integration with government-issued IDs, such as Aadhar, further enhances the credibility and accuracy of the verification process.

# PROBLEM STATEMENT

In recent years, the rapid digitization of personal and financial transactions has led to an alarming rise in identity theft and misuse of personal information. Identity theft, involving unauthorized access to a person's private data for malicious purposes, has become a pressing issue, causing significant financial and emotional distress to individuals. Traditional identity verification methods, relying heavily on centralized databases and paper-based documentation, have proven to be inadequate in ensuring data security, privacy, and accuracy.

Traditional identity verification systems often store sensitive personal data in centralized databases, making them lucrative targets for cyber-attacks and data breaches, risking the privacy and security of individuals.

Centralized systems can be susceptible to manipulation or unauthorized alterations of stored data, leading to inaccuracies and fraudulent activities.

Individuals lack visibility into how their personal data is accessed, utilized, and shared within centralized systems, contributing to a lack of trust and transparency.

***Objective:***

- Explore integration options with government-issued IDs to validate and augment the credibility of the identity verification process.
- Develop a system that securely manages and store’s identity information using blockchain technology, ensuring immutability and resistance against unauthorized alterations.

# MODEL

Here's a description of each function is provided of smart contract, "*IdentityVerification*":

- **submitIdentity` Function**: This function allows a user to submit their identity information and Aadhar details for verification.

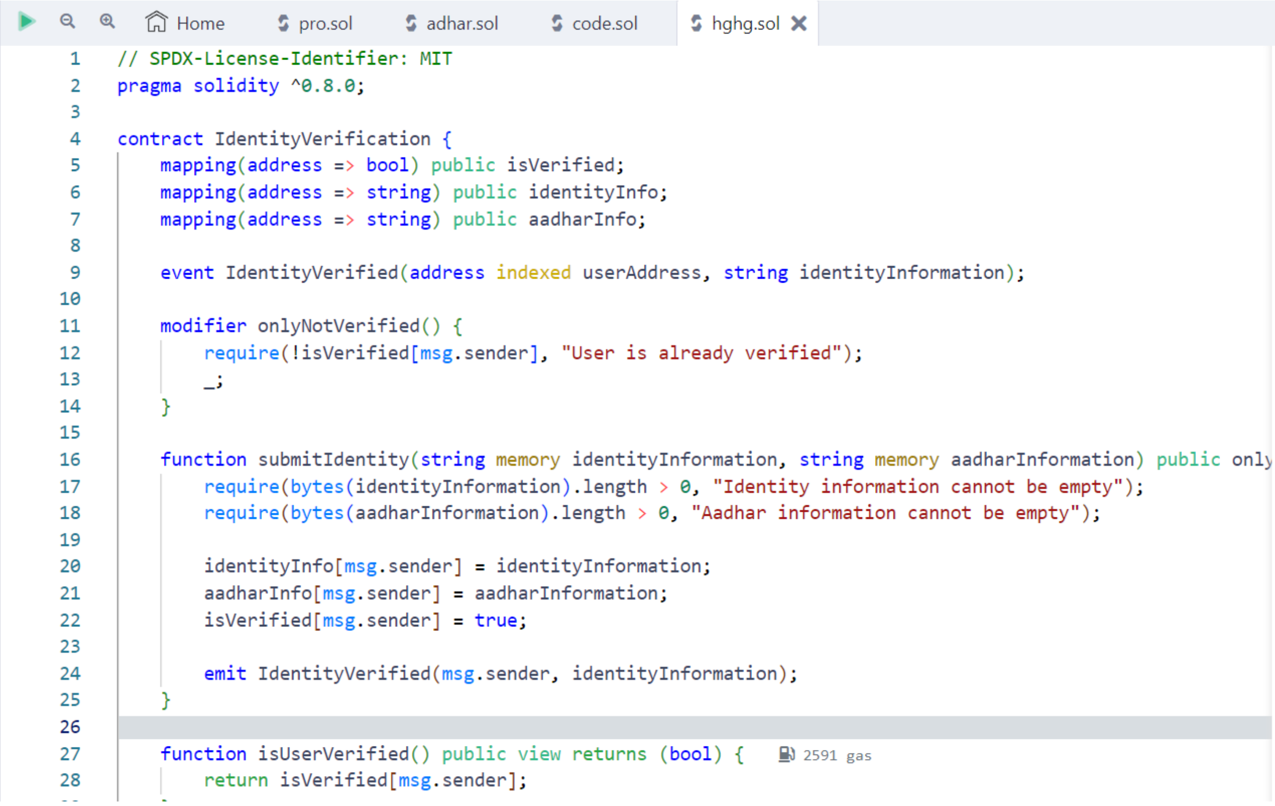
  ***Parameters***:
  - **identityInformation**: A string containing the user's identity information.
  - `**aadharInformation**`: A string containing the user's Aadhar information.

  ***Modifiers***:
  - ***onlyNotVerified***`: Ensures that the user initiating the function is not already verified.

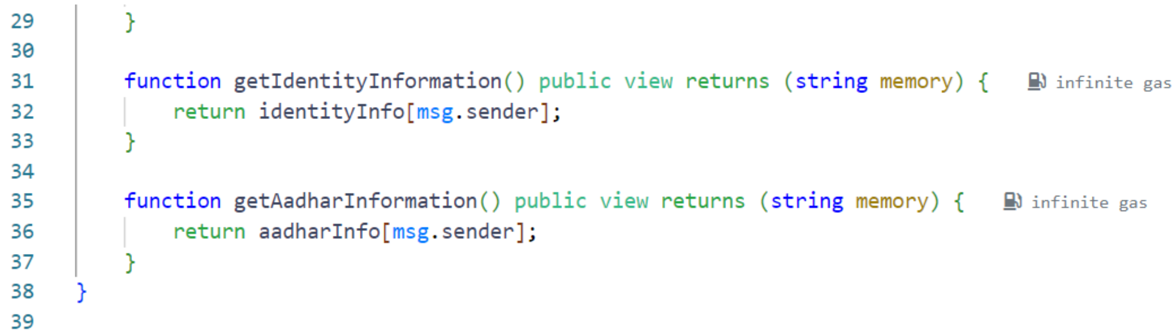
  ***Actions***:
  - Verifies that both identity and Aadhar information are provided.
  - Stores the provided identity and Aadhar information for the sender (the user) in the contract.
  - Marks the sender as verified.
  - Emits an `IdentityVerified` event containing the user's address and identity information.
- **isUserVerified Function**: This function allows anyone to check if a particular user is verified.
  - ***Returns***: A boolean indicating whether the sender (caller) is verified or not.

- **getIdentityInformation Function**: This function allows anyone to retrieve the identity information of a particular user.
  - ***Returns***: A string containing the identity information of the sender (caller).
- **getAadharInformation Function**: This function allows anyone to retrieve the Aadhar information of a particular user.
  - ***Returns***: A string containing the Aadhar information of the sender (caller).
- **onlyNotVerified Modifier:** This modifier ensures that a function can only be executed if the sender is not already verified.
  - Checks if the sender's address is not in the `isVerified` mapping, indicating the sender is not verified.
  - The provided contract facilitates the submission of identity and Aadhar information, verification status checking, and retrieval of identity and Aadhar information for verified users.

# SCREENSHOTS OF CODING

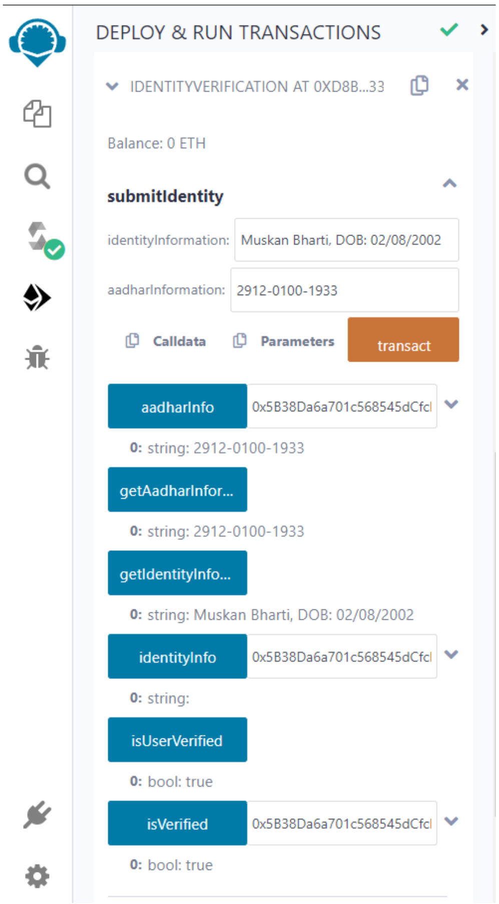


```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract IdentityVerification {
    mapping(address => bool) public isVerified;
    mapping(address => string) public identityInfo;
    mapping(address => string) public aadharInfo;

    event IdentityVerified(address indexed userAddress, string identityInformation);

    modifier onlyNotVerified() {
        require(!isVerified[msg.sender], "User is already verified");
        _;
    }

    function submitIdentity(string memory identityInformation, string memory aadharInformation) public only
        require(bytes(identityInformation).length > 0, "Identity information cannot be empty");
        require(bytes(aadharInformation).length > 0, "Aadhar information cannot be empty");

        identityInfo[msg.sender] = identityInformation;
        aadharInfo[msg.sender] = aadharInformation;
        isVerified[msg.sender] = true;

        emit IdentityVerified(msg.sender, identityInformation);
    }

    function isUserVerified() public view returns (bool) {    2591 gas
        return isVerified[msg.sender];
```



```
    }

    function getIdentityInformation() public view returns (string memory) {    infinite gas
        return identityInfo[msg.sender];
    }

    function getAadharInformation() public view returns (string memory) {    infinite gas
        return aadharInfo[msg.sender];
    }
}
```

# RESULTS



DEPLOY & RUN TRANSACTIONS

IDENTITYVERIFICATION AT 0XD8B...33

Balance: 0 ETH

submitIdentity

identityInformation: Muskan Bharti, DOB: 02/08/2002

aadharInformation: 2912-0100-1933

Calldata Parameters transact

aadharInfo 0x5B38Da6a701c568545dCfcl

0: string: 2912-0100-1933

getAadharInfor...

0: string: 2912-0100-1933

getIdentityInfo...

0: string: Muskan Bharti, DOB: 02/08/2002

identityInfo 0x5B38Da6a701c568545dCfcl

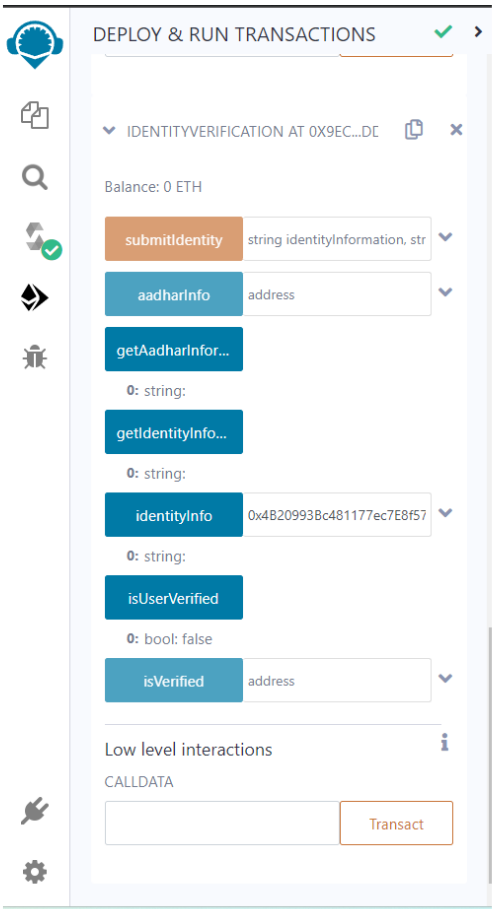
0: string:

isUserVerified

0: bool: true

isVerified 0x5B38Da6a701c568545dCfcl

0: bool: true



DEPLOY & RUN TRANSACTIONS

IDENTITYVERIFICATION AT 0X9EC...DE

Balance: 0 ETH

submitIdentity string identityInformation, str

aadharInfo address

getAadharInfor...

0: string:

getIdentityInfo...

0: string:

identityInfo 0x4B20993Bc481177ec7E8f57

0: string:

isUserVerified

0: bool: false

isVerified address

Low level interactions

CALLDATA

Transact

## True Case

## False Case

# CONCLUSION

In conclusion, this report has explored the potential of leveraging blockchain technology for identity verification, using Aadhaar as a real-world example. It has shed light on the inherent limitations of traditional registration processes, which rely on physical documents and are vulnerable to inconvenience, loss, and security risks. These shortcomings have underscored the pressing need for a more secure and efficient solution. The central objective of this paper has been to introduce the concept of blockchain technology as a feasible and robust alternative to address these challenges. Blockchain, with its distributed ledger architecture, offers unparalleled security and transparency features, making it an ideal candidate for enhancing identity verification and safeguarding personal data.

By focusing on Aadhaar verification, a system that involves the validation of individuals' Aadhaar details, which encompass a wide array of demographic and biometric information, this report has showcased the practical application of blockchain technology in a real-world scenario. It has articulated how blockchain can be harnessed to securely store and verify Aadhaar information, all while ensuring tamper resistance and data integrity.

The report has also delved into the verification process, elucidating the steps involved when users seek to confirm their identities. Through a request for access to their Aadhaar data stored on the blockchain, the system meticulously checks whether the provided details align with the information on the blockchain. This process, marked by its accuracy and transparency, culminates in either a "true" or "false" response, offering a streamlined and dependable identity verification mechanism.

Our vision encompasses a future where individuals regain control over their identities in the digital landscape. Through the integration of blockchain technology, we aim to provide a more secure, transparent, and efficient identity verification process.

# REFRENCE

- Arshad Jamal, Ampuan Siti Nurin Syahirah, Rabab Alayham Abbas Helmi, Mariam-Aisha Fatima, Blockchain-Based Identity Verification System , 2019 IEEE 9th International Conference on System Engineering and Technology (ICSET), 7 October 2019, Shah Alam, Malaysia
- Gunit Malik; Kshitij Parasrampuria; Sai Prasanth Reddy; Seema Shah Blockchain Based Identity Verification Model; 2020 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN)
- Haifa Alanzi and Mohammad Alkhatib; Towards Improving Privacy and Security of Identity Management Systems Using Blockchain Technology: A Systematic Review