E-CERTIFY: EDUCATIONAL CREDENTIAL VERIFICATION

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

Use Case Report

submitted by

KAILA BHAVANA

(22501A0571)

Under the guidance of

Mr. A. Prashant, Asst. Prof.

Department of Computer Science and Engineering

Prasad V Potluri Siddhartha Institute of Technology

(Permanently affiliated to JNTU-Kakinada, Approved by AICTE)

(An NBA & NAAC accredited and ISO 9001:2015 certified institute)

Kanuru, Vijayawada-520 007

2024-25

Prasad V Potluri Siddhartha Institute of Technology

(Permanently affiliated to JNTU-Kakinada, Approved by AICTE)

(An NBA & NAAC accredited and ISO 9001:2015 certified institute)

Kanuru, Vijayawada-520 007

CERTIFICATE

This is to certify that the Use Case report entitled **"E-Certify: Educational Credential Verification"** that is being submitted by **Kaila Bhavana(22501A0571)**, as part of Assignment-1 and Assignment-2 for the **Blockchain Technology**(**20CS4601C)** course in **3-2** during the academic year **2024-25**.

Course Coordinator
Mr. A. Prashant
Assistant Professor,
Department of CSE,
PVPSIT, Vijayawada

Head of the Department
Dr. A. Jayalakshmi,
Professor and Head,
Department of CSE,
PVPSIT, Vijayawada

MARKS

ASSIGNMENT-1: ____/5

ASSIGNMENT-2: ____/5

INDEX

1. INTRODUCTION

Blockchain technology is transforming industries by providing a decentralized, immutable, and transparent method for storing and verifying information [1]. Originally developed for Bitcoin, blockchain has expanded into finance, healthcare, supply chains, and education, offering innovative solutions to long-standing challenges [3].

Academic credential verification remains a critical issue due to fraud, inefficiency, and reliance on centralized authorities [2]. Traditional verification methods require manual validation, making the process slow and prone to errors. The rise of fake degrees has further undermined trust among employers and universities, necessitating a secure and efficient verification system [4].

Blockchain provides a tamper-proof solution by storing academic credentials as cryptographic hashes, ensuring authenticity and preventing unauthorized alterations . Institutions, employers, and students can verify credentials instantly without intermediaries, significantly reducing verification time and administrative burdens. Additionally, smart contracts automate certificate issuance and validation, eliminating paperwork and minimizing human errors [6].

Despite its advantages, blockchain adoption in education faces challenges such as scalability, integration with existing systems, and regulatory compliance [6]. Public blockchains like Ethereum may have high transaction costs and slower processing times, limiting widespread use. Moreover, institutions must navigate data privacy concerns when implementing blockchain-based record management.

Emerging technologies like self-sovereign identity (SSI) systems further enhance credential verification by allowing students to store and manage their academic records in digital wallets, enabling seamless and direct sharing with employers and universities [1].

As blockchain continues to evolve, its application in academic credential verification is expected to grow, fostering a secure and efficient education system.

2. BACKGROUND

2.1 Fake Certificates

The proliferation of fraudulent degrees and certificates has become a critical issue in academic verification. Advancements in digital tools have made it easier for individuals to forge certificates that closely resemble authentic ones. The rise in fake credentials undermines trust in educational qualifications and creates challenges for employers and institutions relying on these documents. Studies indicate that many university administrative staff struggle to differentiate between genuine and counterfeit diplomas [5].

2.2 Slow Verification Process

Traditional verification methods rely on manual processes, which are often slow and inefficient. Employers and universities may take days or even weeks to validate a single document, causing delays in hiring and admissions. The inefficiency is further exacerbated by the lack of standardized procedures across different institutions, leading to inconsistent verification timelines [2].

2.3 Lack of Transparency

The current certificate verification process is often controlled by centralized authorities, leading to inefficiencies and trust issues. Without a standardized system, verification criteria can vary significantly, making the process opaque and unreliable. Additionally, reliance on intermediaries introduces delays and potential human errors in verification [4].

2.4 Security Vulnerabilities

Traditional systems often store credentials in centralized databases, making them vulnerable to cyberattacks and data breaches. Unauthorized access or tampering can lead to fraudulent use of academic records. Previous incidents have shown that compromised certificate authorities have issued fake credentials, further diminishing trust in conventional verification systems [3].

2.5 Scalability Issues

As the number of certificates issued and requiring verification increases, traditional systems struggle to scale efficiently. Manual verification processes create bottlenecks, leading to delays and increased administrative workloads. This issue is particularly significant for institutions handling large volumes of academic records [6].

2.6 Inconsistent Verification Standards

Different universities and organizations employ varying criteria and processes for certificate verification, leading to inconsistencies. The absence of a universal verification framework can cause confusion and mistrust among stakeholders who rely on verified credentials for academic and professional purposes [6].

2.7 High Operational Costs

Maintaining traditional verification systems is expensive due to labor-intensive processes, physical storage requirements, and the need for secure handling of documents. Institutions must allocate significant resources to administrative tasks, diverting funds from other critical areas such as education and research [5].

2.8 Environmental Impact

The reliance on paper-based certificates has environmental consequences, contributing to deforestation and increased carbon emissions from printing and transportation. Digital credentialing methods, such as blockchain-based solutions, can mitigate these environmental concerns by eliminating the need for physical documents [1].

Addressing these challenges requires adopting secure, efficient, and standardized verification systems. Blockchain technology presents a viable solution to enhance the integrity, security, and reliability of academic credential verification .

3. BLOCKCHAIN BASICS

Blockchain is a decentralized, distributed ledger technology designed to securely record and verify transactions across multiple nodes. It ensures data integrity, transparency, and security by eliminating the need for a central authority. This technology has transformed industries such as finance, supply chain management, and education, making it an ideal solution for academic certificate verification.

3.1 Decentralization

Decentralization is a fundamental principle of blockchain technology. Unlike traditional centralized systems where a single entity (such as universities or government bodies) controls data, blockchain distributes data across multiple network nodes.

- **No Central Authority**: No single institution has full control over the blockchain network. Instead, all participants (nodes) maintain a copy of the ledger, ensuring transparency and reducing the risk of data manipulation.
- **Enhanced Security**: Since blockchain data is distributed across multiple nodes, it is highly resistant to hacking or data breaches. Any unauthorized alteration would require changes in more than 50% of the nodes, which is computationally impractical in large-scale networks.
- **Reliability & Availability**: Even if some nodes fail or go offline, the blockchain remains operational, ensuring continuous access to certificate records.

Example in Certificate Verification: In traditional systems, universities store certificate records in centralized databases, making them vulnerable to hacking or fraud. With blockchain, certificates are stored across multiple nodes, preventing unauthorized modifications and ensuring long-term security [4].

3.2 Immutability

Immutability refers to the property of blockchain where once data is recorded, it cannot be changed or deleted. Every transaction is time-stamped and cryptographically secured, making the ledger tamper-proof.

- **Hashing & Cryptographic Security**: Each transaction is assigned a unique cryptographic hash. If any modification is attempted, the hash changes, alerting the network to tampering.

- **Linked Blocks**: Transactions are grouped into blocks, which are cryptographically linked. Any attempt to alter a previous block invalidates all subsequent blocks, ensuring the integrity of data.
- **Trust & Transparency**: Since blockchain transactions are immutable, all stakeholders can trust the recorded data without the need for third-party verification.

Example in Certificate Verification: A university issues a degree certificate on a blockchain. The certificate's details (student name, course, date, etc.) are stored as a transaction with a unique hash. Any attempt to alter the certificate would be detected by the network, ensuring authenticity and fraud prevention [3].

3.3 Smart Contracts

Smart contracts are self-executing programs stored on the blockchain that automatically execute predefined actions when specific conditions are met.

- **No Middlemen**: Smart contracts remove the need for intermediaries (e.g., universities, government agencies) by executing transactions based on agreed-upon conditions.
- **Efficiency & Cost Savings**: Automating verification processes reduces paperwork, administrative delays, and costs associated with manual credential validation.
- **Trust & Security**: Smart contracts operate based on pre-programmed logic, ensuring secure and unbiased execution of transactions.

Example in Certificate Verification: A university deploys a smart contract that automatically issues a digital certificate when a student fulfills their academic requirements. The contract verifies grades, generates the certificate, and records it on the blockchain, ensuring a transparent and automated verification process [4].

3.4 Why Blockchain is Ideal for Academic Certificate Verification?

- **Prevents Fraud**: Certificates stored on a blockchain cannot be forged or altered.
- **Instant Verification**: Employers and institutions can verify credentials within seconds, reducing processing time.
- **No Dependency on Third Parties**: Eliminates reliance on universities or external agencies for manual verification.
- **Global Accessibility**: Blockchain-based certificates can be accessed and verified anywhere in the world.
- **Student Ownership**: Graduates can store and share their certificates without needing to request copies from their institutions [5].

4.USE CASE OVERVIEW

4.1 Objectives of E-Certify

The primary objectives of the E-Certify system are:

- **Fraud Prevention:** Ensure certificates cannot be forged or altered.
- **Decentralization**: Remove reliance on a single authority for verification.
- **Instant Verification:** Enable employers and institutions to verify credentials in real-time.
- **Data Security**: Protect academic records using cryptographic encryption.
- **Automation**: Reduce administrative workload using smart contracts.
- **Global Accessibility**: Allow worldwide access to certificates without dependency on universities.

4.2 Scope of E-Certify

E-Certify is designed for:

- **Educational Institutions**: Universities and colleges can issue certificates digitally on the blockchain.
- **Students & Alumni**: Individuals can store and share their verified credentials.
- **Employers & Organizations**: Companies can instantly validate candidate credentials before hiring.
- **Government & Accreditation Bodies:** Regulating agencies can ensure certificate authenticity.

4.3 System Architecture

The E-Certify architecture consists of multiple components working together to ensure secure and efficient certificate issuance and verification.

4.3.1 Ethereum Blockchain

- Acts as the decentralized ledger for storing academic credentials.
- Ensures immutability, preventing data tampering or unauthorized modifications.
- Uses cryptographic hashing to secure student certificates.

4.3.2 MetaMask Wallet

- A browser-based crypto wallet for interacting with the Ethereum blockchain.
- Used to sign transactions and pay for gas fees when deploying smart contracts.

4.3.3 Ganache

- A local blockchain development environment used for testing.
- Allows developers to simulate Ethereum transactions without real costs.

4.3.4 Smart Contracts (Solidity-based)

- Automates certificate issuance, verification, and revocation.
- Defines the rules and conditions for academic credentials.
- Ensures that only authorized institutions can issue valid certificates.

4.3.5 Frontend (React-based UI)

A user-friendly interface for interacting with the E-Certify system.

Features:

- Issue Certificates: Institutions can generate and register certificates.
- Verify Certificates: Users can check the authenticity of credentials.
- View Records: Students can access and share their certificates securely.

4.3.6 Backend (Node.js & Web3.js)

- The backend connects the frontend with the blockchain.
- Uses Node.js for handling API requests and processing data.
- Uses Web3.js to interact with Ethereum smart contracts.

4.4 System Workflow (How E-Certify Works)

- Institution Registration: Universities register on the blockchain and deploy smart contracts.
- Issuance: Institutions issue certificates, which are hashed and recorded on the blockchain. Security: The certificate is linked to a blockchain transaction ID for verification.
- Verification Process: Employers or institutions can verify a certificate by entering its unique hash.
- Revocation (if needed): If a certificate is invalid, institutions can revoke it through the smart contra

4.5 Architecture Diagram

The E-Certify system follows a decentralized approach to issuing, storing, and verifying academic certificates using blockchain and IPFS. It ensures tamper-proof digital credentials, allowing students, employers, and institutions to validate documents instantly.

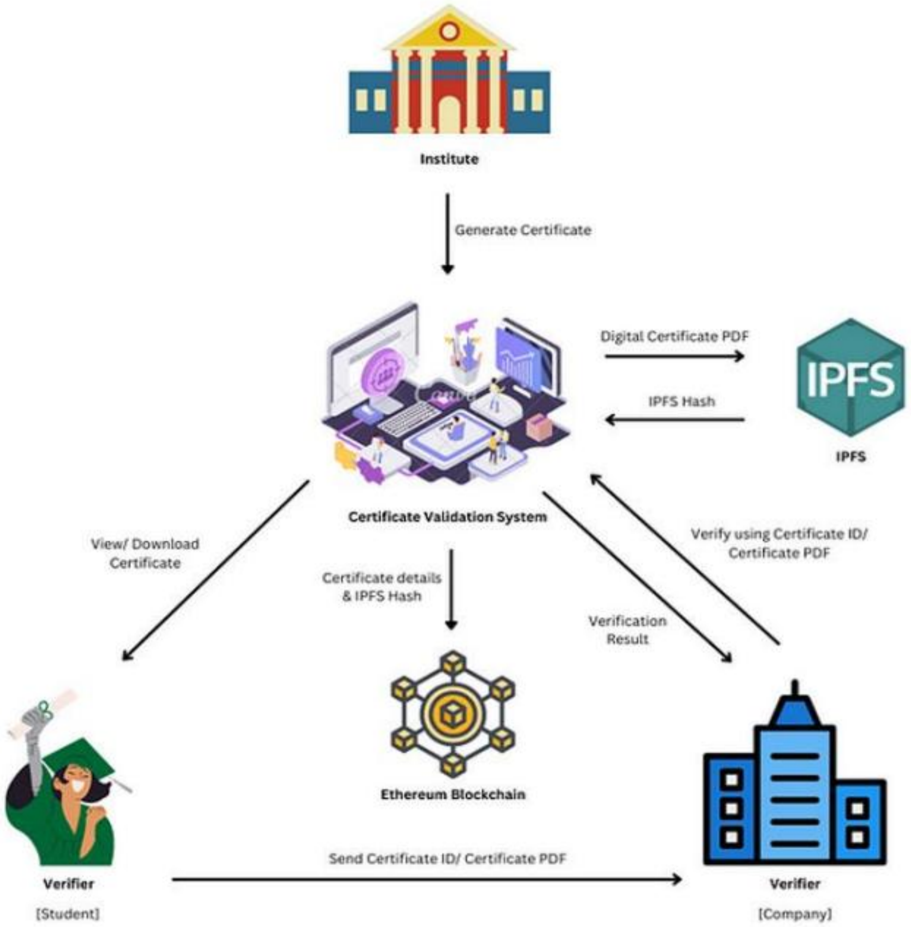
Institute
Generate Certificate
Digital Certificate PDF
IPFS
IPFS Hash
IPFS
Certificate Validation System
View/ Download Certificate
Certificate details & IPFS Hash
Verify using Certificate ID/ Certificate PDF
Verification Result
Ethereum Blockchain
Send Certificate ID/ Certificate PDF
Verifier
[Student]
Verifier
[Company]

Fig. 4.5.1: System architecture of E-Certify (Source: [*International Journal of Innovative Science and Research Technology*, *9*(11)**)**

Fig 4.5.1 Workflow Explanation

1. **Certificate Issuance**
    - The institution generates a digital certificate and uploads it to IPFS, which returns a unique hash (CID).
    - The certificate details and its IPFS hash are recorded on the Ethereum blockchain via a smart contract.

2. **Certificate Storage**
    - On-Chain (Blockchain): Stores only the certificate hash and metadata to ensure security and immutability.
    - Off-Chain (IPFS): Stores the full certificate document (PDF) to reduce blockchain storage costs.
3. **Verification Process**
    - Employers and other verifiers can use the certificate ID or PDF to check authenticity.
    - The system retrieves the certificate’s hash from the blockchain and cross-checks it with the IPFS-stored file.
    - If the hashes match, the certificate is valid; otherwise, it is flagged as tampered or invalid.
4. **Student Access & Sharing**
    - Students can download, view, and share their certificates securely using the validation platform.

4.6 Where certificates are stored?

4.6.1 On-Chain Storage (Blockchain) – Stores Certificate Hash & Metadata

The blockchain stores only a cryptographic hash of the certificate.

Metadata such as student name, institution, course name, and issue date are stored as immutable transactions on the blockchain.

4.6.2 Off-Chain Storage (IPFS) – Stores Full Certificate Data

Full certificate documents (PDFs, images) are stored off-chain using IPFS to reduce costs.

IPFS generates a Content Identifier (CID), which is stored on the blockchain for verification.

Why IPFS?

- Reduces Ethereum gas fees by keeping large files off-chain.
- Ensures decentralized, permanent access to academic records.
- Prevents data loss, unlike traditional cloud storage

5.IMPLEMENTATION

5.1 Smart Contract Development

Technology Used:

- Solidity (Smart contract programming language)
- Ethereum Blockchain (Decentralized ledger for verification)
- Remix IDE (For writing and deploying smart contracts)
- MetaMask Wallet (For executing blockchain transactions)
- IPFS (InterPlanetary File System) (For off-chain certificate storage)

How It Works?

- A smart contract is written in Solidity to handle the issuance, verification, and revocation of certificates.
- Only authorized institutions can issue certificates, preventing unauthorized access.
- The certificate (PDF, image, etc.) is stored on IPFS, generating a unique Content Identifier (CID).
- The CID and certificate metadata (student name, course, issue date) are stored on the blockchain for immutable verification.

5.2 Institution Registration

Technology Used:

- Web3.js & Node.js (For blockchain interactions)
- MetaMask (For authentication and transactions)

How It Works?

- Institutions fill out a registration form with details like name, accreditation, and institution ID.
- A smart contract is deployed, linking the institution’s details to the blockchain.
- The institution receives a unique blockchain identifier, ensuring that only verified institutions can issue certificates.
- The registration record is stored immutably on the blockchain.

Key Benefit: Ensures only trusted institutions can issue certificates, reducing the risk of fraud.

5.3 Certificate Issuance

Technology Used:

- Solidity (Smart Contracts) (Handles issuance logic)
- IPFS (Decentralized File Storage) (Stores full certificates)
- Cryptographic Hashing (SHA-256) (Generates unique certificate IDs)

How It Works?

- The institution uploads the certificate (PDF, image, etc.) to IPFS, which generates a CID (unique file identifier).
- A cryptographic hash (SHA-256) is generated for the certificate to ensure integrity.
- The smart contract records the CID and metadata (student name, course, issue date) on the blockchain.
- The student receives a digital certificate ID, linking the CID on IPFS and metadata on the blockchain.

Key Benefit: Decentralized and tamper-proof certificate storage, ensuring long-term accessibility.

5.4 Certificate Verification

Technology Used:

- Web3.js & Smart Contracts (Fetches stored certificate metadata)
- IPFS Gateway (Retrieves full certificate file)

How It Works?

- The verifier enters the certificate ID into the verification portal.
- The system retrieves the CID from the blockchain.
- Using IPFS, the system fetches the full certificate.
- The system compares the cryptographic hash stored on the blockchain with the fetched file.
- If the hashes match, the certificate is authentic; otherwise, it is tampered with.

Key Benefit: Employers and institutions can instantly verify credentials without contacting the issuing authority.

5.5 Revocation Mechanism

Technology Used:

- Solidity (Smart Contracts) (Handles revocation logic)
- Blockchain Transactions (Records revocation status)

How It Works?

- The institution identifies a fraudulent or incorrect certificate.
- A revocation request is submitted to the smart contract.
- The certificate status is updated to "revoked" on the blockchain.
- If someone attempts to verify a revoked certificate, the system marks it as invalid.

Key Benefit: Prevents misuse of revoked, expired, or fraudulent certificates.

6. BENEFITS

The E-Certify system leverages blockchain technology to offer secure, transparent, and tamper-proof certificate issuance and verification. Below are the key benefits of using blockchain in this use case:

6.1 Enhanced Data Security

Certificates are stored on a decentralized blockchain ledger, preventing unauthorized modifications.

6.2 Transparency & Trust

All stakeholders (students, institutions, employers) can access real-time verification of certificates.

Blockchain ensures that no single authority can alter the data, enhancing credibility.

6.3 Fraud Prevention

Each certificate is assigned a unique cryptographic hash, making it impossible to counterfeit.

Employers and institutions can verify the authenticity of credentials instantly.

6.4 Instant Verification

Eliminates manual verification delays, allowing real-time validation. Reduces dependency on issuing institutions, simplifying the hiring and admission process.

6.5 Cost Efficiency

Automates certificate issuance and verification using smart contracts. Eliminates the need for third-party verification agencies, reducing administrative costs.

6.6 Student Ownership & Control

Students can store and manage their certificates in digital wallets. Allows secure sharing of credentials with employers or universities without physical copies.

6.7 Scalability & Global Accessibility

Employers and institutions worldwide can access and verify credentials without contacting the issuing authority.

Supports cross-border recognition of academic qualifications.

7.CHALLENGES

7.1 Scalability Issues

- Public blockchains (e.g., Ethereum) have limited transaction speed and may incur high gas fees.
- As the number of stored certificates grows, scalability must be addressed with efficient consensus mechanisms.
- IPFS does not guarantee permanent storage**,** requiring solutions like Filecoin or Pinning Services to keep files accessible long-term**.**

7.2 Regulatory and Compliance Concerns

- Different countries have varying legal frameworks regarding digital certificates and blockchain usage.
- Compliance with data privacy laws (e.g., GDPR, FERPA) is necessary when storing student records.
- IPFS stores files publicly, meaning institutions must encrypt certificates before uploading to protect student data.

7.3 Adoption Resistance

- Universities and institutions may hesitate to replace traditional systems with blockchain.
- Institutions must understand how to manage off-chain storage, ensuring documents remain accessible even after extended periods.
- Requires training and awareness to ensure smooth adoption.

7.4 Data Privacy & Confidentiality

- While blockchain is transparent, institutions must ensure student data privacy.
- Solutions like Zero-Knowledge Proofs (ZKP) may be needed to enhance privacy.
- If a file is deleted or lost from non-pinned IPFS nodes, verification may fail, requiring redundant storage solutions.

7.5 High Initial Setup Costs

- Deploying blockchain and IPFS infrastructure requires smart contract development, IPFS node hosting, and integration with university systems.
- Institutions must invest in long-term IPFS pinning services (e.g., Filecoin, Pinata, Infura) to prevent file loss.

8.CONCLUSION

The E-Certify system leverages blockchain and IPFS to revolutionize academic credential verification, ensuring security, transparency, and efficiency. By storing certificate metadata on the blockchain and full certificate files on IPFS, the system eliminates fraud, delays, and reliance on centralized authorities.

Smart contracts automate certificate issuance, verification, and revocation, while IPFS ensures decentralized, cost-effective storage. This hybrid approach reduces on-chain storage costs, maintains tamper-proof records, and provides global accessibility.

Despite challenges such as scalability, data privacy, and long-term IPFS file availability, blockchain and IPFS together offer a secure and scalable solution for credential verification. Future enhancements like Self-Sovereign Identity (SSI), encrypted IPFS storage, and improved interoperability with institutional databases will further streamline credential management.

As blockchain and IPFS adoption grow, educational institutions must collaborate and innovate to ensure seamless implementation. With immutable credentials, automated verification, and decentralized accessibility, E-Certify is set to redefine the future of academic certification.

9. SDG’s ADDRESSED

9.1 SDG 4: Quality Education

Blockchain ensures secure, verifiable, and tamper-proof academic credentials, eliminating fake degrees and fraud. Students own and manage their records on a decentralized ledger, enabling lifelong tracking and global accessibility without reliance on institutions. This enhances trust in education and simplifies verification for students, employers, and universities.

9.2 SDG 9: Industry, Innovation, and Infrastructure

Blockchain modernizes credential verification, replacing paper-based, manual processes with a secure digital system. It reduces administrative costs, enhances data integrity, and enables scalable, decentralized access to academic records. By fostering interoperability, institutions worldwide can collaborate and innovate, driving digital transformation in education.

10.REFERENCES

1. Subramanian, C., George, A. A., Abhilash, K. A., & Karthikeyan, M. (2020). Blockchain Technology (Chapter 10: E-Certify).

2. Harika, G., Hareesh, B. H., Harshitha, B. H., Akash, G. A., & Hema, N. (2024). *Academic Credential Verification System Using Blockchain*. *International Journal of Innovative Science and Research Technology*, *9*(11).

   [Link: Academic credential verification system using blockchain| International Journal of Innovative Science and Research Technology]

3. Viswanathan, B., & Lakshmi, B. (2025). *Enhancing Educational Certificate Management and Verification with Blockchain Technology*. Journal of Computer Information Systems.

4. Parekh, R., Pillai, P., Shukla, S., & Parvatikar, S. (2020). *Digitised Academic Credential Verification Using Blockchain*. Research & Reviews: A Journal of Embedded System & Applications, 8(2), 21–29.

5. Alkhowaiter, W. A., & Prince, D. (2023). *Integrating Blockchain Technology into a University Graduation System*. Trends in Higher Education, 2(3), 514–525.

11.APPENDIX

https://drive.google.com/drive/folders/17ExGafQRzymQsusgCATwxG49uKR_e0Lu?usp=drive_link