

# Hi WCHL

We are pleased to present our project to you...



Proof prove whether this content is original or cleverly fabricated and at the same time will be the strongest proof of identity without revealing privacy

## ● The problem and the idea:

In a world full of content, it can be difficult to distinguish between what is real and what is fake.

# ProofMe

It is a protocol built on [Web3](#) and [Blockchain technologies \(using ICP\)](#) whose primary goal is to prove the authenticity of digital content, whether it is:

- Social media posts.
- Educational certificates.
- Scientific articles.
- Photos, videos, or artwork.

All of this is done by linking content to an encrypted and trusted digital identity, so anyone can know [who posted the content, when, and whether it is real or generated by AI.](#)

## • Project goal:

- Combating misinformation and fake content.
- Enabling content creators to prove ownership.
- Giving users confidence in everything they watch.
- Utilizing decentralized identity (DID) to verify or proving credentials and educational experience.



**Building a safer and more transparent digital community.**

## ● Implementation method:



### 1 - Digital Identity Issuance (DID):

- When a new user registers in the system, a decentralized digital identity (DID) is created using Web3 technologies.
- This identity is linked to verified information about the user, such as university degrees, training courses, employment, and professional history.
- This data is verified by reviewing official documents and confirming its authenticity through the issuing authorities.



### 2 - Upload and document content:

- The user uploads content (such as a photo or video) to the platform.
- As part of the verification process, the user is asked to take a selfie directly from within the app through integrated platforms (such as Facebook or Twitter) while uploading the content. This is to ensure that the person appearing in the content is the same person who uploaded it.
- After this verification, a unique hash value is generated for the content.
- This value (hash) is recorded on a blockchain (ICP) and linked to the publisher's digital identity.
- When someone attempts to repost this content, the hash value is checked to confirm the following:
- If the hash value already exists on the blockchain, the content is authentic.
- If the hash value is not found, this indicates that the content may be fake or generated using artificial intelligence.

## ● Implementation method:



### 3 -Proof System:

Any user or entity can check content for authenticity through the system, which indicates:

- Whether the content was posted by a real, identified person.
- Whether the content has been modified after posting.
- Identifying the original source of the content and the exact date and time of posting.



### Where's the real innovation?











Most systems try to "detect" fraud after

**But ProofMe**

enables you to prove your "integrity" before anyone even thinks of forging it.

This content is yours...and no one else can fake it.

- Comparison points between the Proofme system and other systems:

Comparison points	Traditional systems	proofMe
Detect fake content	 sometimes	 Yes – via unique fingerprint
Ensure originality of content	 No	 Yes
Personal digital signature	 No	 Yes
Proof of ownership of a certificate or identity	 No	 Yes
Authentication as a legal document	 No	 Yes – Blockchain

## ● Technologies Stack:

Layer	Technology
Frontend	Next.js, Tailwind CSS
Blockchain Layer	ICP + Motoko Smart Contract
Identity Layer	ICP Identity, Web3 Wallet
Hashing	ICP Identity, Web3 Wallet
Integration	Contract API, Internet Identity SDK

- Tools and techniques used:

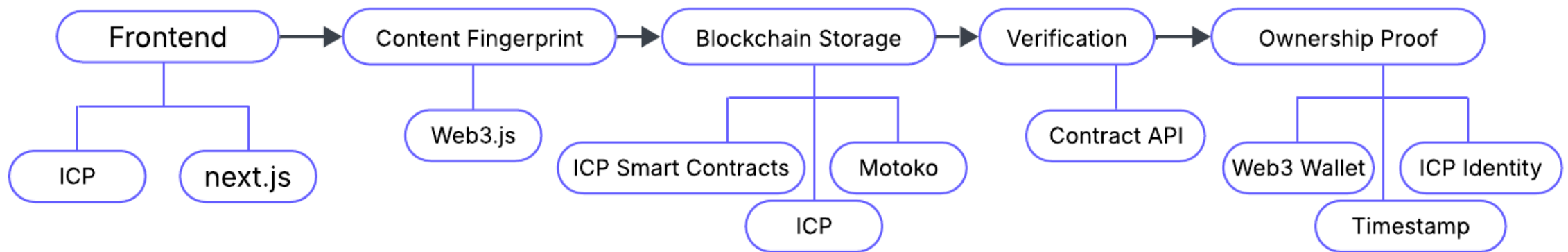
Technology	Use
Motoko	Smart Contract Programming on ICP
Internet Identity (ICP)	To create decentralized and secure digital identities
NFT Standard	To generate unique digital fingerprints for content
IPFS	To store original content in a decentralized manner
Plug Wallet	Linking the user to the personal wallet
JavaScript + React	Front end design
Node.js	Backend and integration with ICP
ICP Candid UI	To test APIs and smart contracts



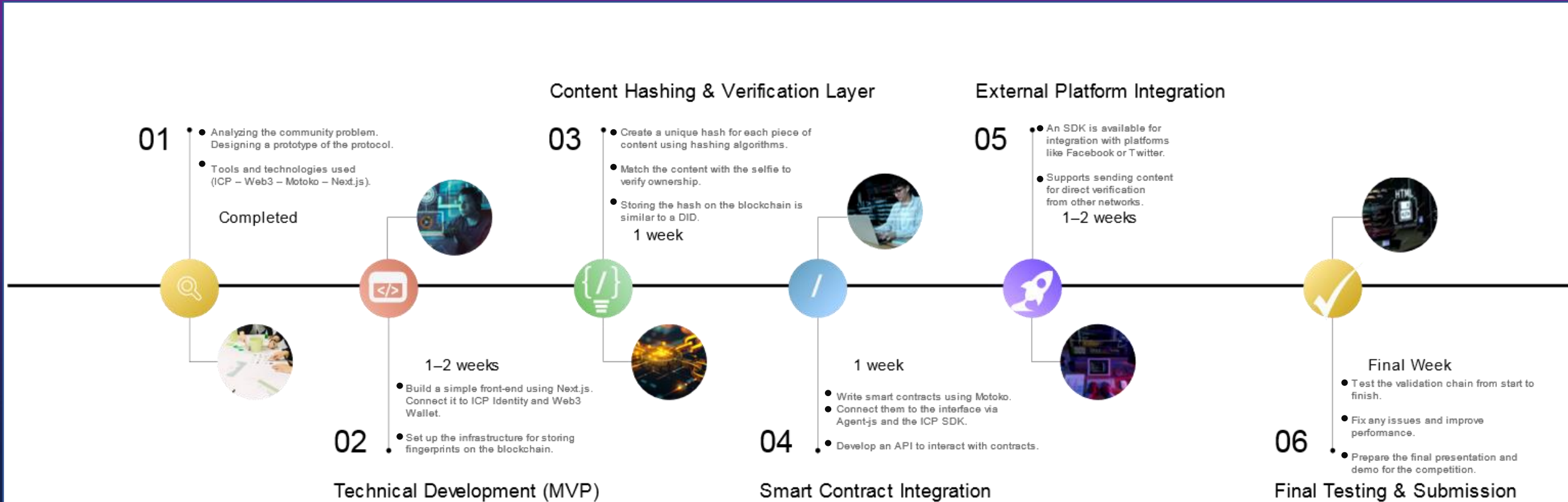
## •workplan:

### System architecture design:

- We create a user interface using Next.js to upload content and prove ownership. We then connect the interface to smart contracts on the ICP platform.
- We use hash algorithms to create a fingerprint of the content and store it on the blockchain using ICP smart contracts, written in Motoko.
- Next, we proceed to the verification phase, which compares the fingerprint generated from the new content with the fingerprint stored on the blockchain by calling the smart contract API.
- Finally, we link the user's signature to the stored fingerprint using ICP Identity and Web3 Wallet to securely ensure ownership of the content.



## • Project Timeline (Execution Phase):



## • Sample Code Snippets:

```
import crypto from 'crypto';

export function generateContentHash(contentBuffer) {
  const hash = crypto.createHash('sha256');
  hash.update(contentBuffer);
  return hash.digest('hex');
}
```

Generate a Hash for a Fingerprint (with JavaScript in Next.js)

```
import { AuthClient } from "@dfinity/auth-client";

const authClient = await AuthClient.create();
await authClient.login({
  identityProvider: "https://identity.ic0.app",
  onSuccess: async () => {
    const identity = await authClient.getIdentity();
    const principal = identity.getPrincipal().toText();
    console.log("User logged in as:", principal);
  }
});
```

Log in and link identity with ICP Identity + Web3

## • Sample Code Snippets:

```
actor ProofRegistry {  
  
    stable var registry : Trie.Trie<Text, Text> = Trie.empty();  
  
    public func registerHash(userId : Text, contentHash : Text) : async Text {  
        registry := Trie.put(registry, userId # contentHash, contentHash);  
        return "Hash registered successfully.";  
    };  
  
    public query func verifyHash(userId : Text, contentHash : Text) : async Bool {  
        let result = Trie.get(registry, userId # contentHash);  
        return switch result {  
            case (?storedHash) storedHash == contentHash;  
            case null false;  
        };  
    };  
}
```

Smart Contract for Fingerprint Storage – Motoko (ICP Canister)

## ● Future Development & Scalability:

### 1-ProofMe for Creators & Designers:

- Famous designers and artists receive a unique stamp for their artwork (logos, graphics, social media designs) before publishing it.

**(This stamp can serve as legal evidence in criminal or intellectual property cases.)**

### 2-Verified Market Integration:

- Create a digital marketplace to sell designed content (artwork and videos) provided it is verified through ProofMe.

**(Stolen content is strictly prohibited)**

### 3-Proof for Audio, Voice & 3D Content:

- Expand the system to include sounds, music, 3D models, and more.

**(Suitable for digital artists, distributors, and developers.)**

### 4-Plugin for Design Platforms (Figma – Adobe):

- Adding a button within design software like Figma or Photoshop allows the user to document the design directly from the program.

**(Save time and integrate directly into the work environment.)**

## ● Questions & A:

### 1-Does this system really help victims or is it just theoretical talk?

ProofMe provides legal evidence, documented on the blockchain, against blackmail or forgery. If a girl's videos are hacked, you can prove they are fake and do not contain her signature. We give victims a voice, rights, and security.

### 2-What makes me trust this system more than any other site?

ProofMe doesn't claim to know the truth using artificial intelligence, but it does record it from the first moment. **We don't chase fakery... we stay one step ahead.**

### 3-Where exactly is the digital signature stored?

The signature is not stored within the video itself **(meaning it's not part of the pixels or audio)**.

This is **important to:**

Preserve the original video quality without modification.

Prevent anyone from "copying" the signature from one video and transferring it to another.

### 4-So, where exactly is it stored?

**On the blockchain (ICP):**

When a user authenticates their content, a unique hash and the user's DID are generated.

These two are recorded as a transaction on the blockchain.

Each transaction has a public link that you can access to verify its status.

## ● Questions & A:

### 1-Does this system really help victims or is it just theoretical talk?

ProofMe provides legal evidence, documented on the blockchain, against blackmail or forgery. If a girl's videos are hacked, you can prove they are fake and do not contain her signature. We give victims a voice, rights, and security.

### 2-What makes me trust this system more than any other site?

ProofMe doesn't claim to know the truth using artificial intelligence, but it does record it from the first moment. **We don't chase fakery... we stay one step ahead.**

### 3-Where exactly is the digital signature stored?

The signature is not stored within the video itself **(meaning it's not part of the pixels or audio)**.

This is **important to:**

Preserve the original video quality without modification.

Prevent anyone from "copying" the signature from one video and transferring it to another.

### 4-So, where exactly is it stored?

**On the blockchain (ICP):**

When a user authenticates their content, a unique hash and the user's DID are generated.

These two are recorded as a transaction on the blockchain.

Each transaction has a public link that you can access to verify its status.

## ● Questions & A:

### 5-How do I make sure that the certificate is original and not fake?

A copy of the manifest or document is uploaded by the user, and the verification team manually reviews it and verifies the source.

After the acknowledgement, we generate a digital fingerprint (hash) of the existing one and record it on the blockchain, preventing any future forgery attempts.

### 6-I have old paper certificates...will this work?

Of course.

Once it's photographed and uploaded for verification, the system converts it into a digital fingerprint and builds a verified record on the blockchain.

What's important is that the document is clear and its source is verifiable.

### 7-Why do I need to notarize the certificate?

Because in every job application, internship, or similar, your credibility speaks for itself.

Your certifications are validated on the blockchain, allowing any entity to immediately verify that you are truly qualified and that your accomplishments are genuine, not fake.

**In a time of uncertainty, authentication is crucial.**



- **Team Members:**

The idea and planning were created by students from the  
Swedish University of Technology:

**Nayra Ahmed**

**Abdurahman Mohamed Gaber**

**Ahmed Ehab**

- Team Lead & Contact:

**Abdurahman Mohamed**

Executive Director – ProofMe Protocol

✉ Email : [Abdurhman240101628@sut.edu.eg](mailto:Abdurhman240101628@sut.edu.eg)  
☎ Phone number: +20 1127229179

# Thanks WCHL

For your precious time



is not just a protocol — it's a statement of truth in a digital world.

ProofMe is not just a protocol... ProofMe Proof of the innocence of the oppressed