NGI TRUST CHAIN

# D1. ‘STATE OF THE ART OVERVIEW, USE CASE ANALYSIS AND PRELIMINARY TECHNICAL SPECIFICATION OF THE SOLUTION’

>DECAST.LIVE<

10/01/2025

Funded by the European Union

TrustChain Project. Funded by the European Union under CA No 101093274. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.

| | |
|---|---|
| Due date | 10/01/2025 |
| Submission date | 10/01/2025 |
| Team | Decast |
| Version | 1.0 |
| Authors | Shivam Dhawan, Mohammed Yasrab, Ajmal Azad, Peyman Pourjafar |

## Disclaimer



## Copyright notice

The TrustChain Consortium is the following:

| Participant number | Role | Participant organisation name | Short name | Country |
|---|---|---|---|---|
| 1 | COO | EUROPEAN DYNAMICS LUXEMBOURG SA | ED | LX |
| 2 | BEN | F6S NETWORK LIMITED | F6S | IE |
| 3 | BEN | UNIVERZA V LJUBLJANI | UL | SI |
| 4 | BEN | ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS - RESEARCH CENTER | AUEB | EL |
| 5 | BEN | FUNDACION CIBERVOLUNTARIOS | CIB | SP |
| 6 | BEN | CONSORCIO RED ALASTRIA | ALA | SP |
| 7 | BEN | TIMELEX | TLX | BE |
| 8 | BEN | ETHNIKO KAI KAPODISTRIAKO PANEPISTIMIO ATHINON | NKUA | EL |
| 9 | AP | CITY UNIVERSITY OF LONDON | ICS | UK |



Funded by the European Union

# TABLE OF CONTENTS





Funded by the European Union

Funded by the European Union

# LIST OF FIGURES





Funded by the European Union

# LIST OF TABLES





Funded by the European Union

## ABBREVIATIONS

| | |
|---|---|
| DC | Dissemination and Communication |
| DID | Decentralised Identifiers |
| DIH | Digital Innovation Hub |
| DLT | Distributed Ledger Technology |
| EDIH | European Digital Innovation Hub |
| EEN | European Enterprise Network |
| EIC | European Innovation Council |
| EU | European Union |
| GA | Grant Agreement |
| GDPR | General Data Protection Regulation |
| NCP | National Contact Point |
| NGI | Next Generation Internet |
| NGO | Non-Governmental Organisations |
| OC | Open Call |
| OC#4 | Open Call #4 |
| SEO | Search Engine Optimization |
| SME | Small and Medium-sized Enterprises |
| SSI | Self-Sovereign Identities |
| WP | Work Package |
| DEPIN | Decentralized Physical Infrastructure Network |
| eKYC | Electronic Know Your Customer |



Funded by the European Union

# 1. INTRODUCTION

This project is a collaboration between Birmingham City University (BCU) and Leren Leren, with Leren Leren leading the initiative.

We have developed other projects that demonstrate our expertise in decentralized technologies and AI:

Video.Wiki: A platform that transforms text into immersive, AI-assisted video content. It was launched during the COVID-19 pandemic to help educators quickly convert text into videos, bridging the gap in remote learning. VideoWiki has since evolved into an open content editing and monetization platform, emphasizing collaborative authoring and IP protection.

Recap App: A generative AI tool designed to help students retain knowledge through personalized revision content and assist educators with automated assignment grading. It was being accelerated by organizations like HP Life and UNESCO, under the BeChangeMaker programme.

Decast.live is a decentralized live casting platform that makes it easier and safer to stream live events and telecalls. Our project focuses on integrating Decentralized Identifiers (DIDs) to manage access, ensuring that only authorized users can join a cast or view its content.

In short, our goal is to build a more secure, user-friendly way to access live video content by leveraging decentralized technology and robust identity management.

# 2. STATE OF THE ART ANALYSIS, BACKGROUND, AND INNOVATION

In this section, we examine current solutions for live streaming and decentralized access control, including our own work with Decast.live.

## 2.1 DESCRIPTION OF BACKGROUND

Before the TRUSTCHAIN project, we had already developed the core infrastructure of Decast.live, a live casting platform designed to support live events and telecalls. The platform integrates decentralized storage solutions like ethSwarm and Sia, ensuring secure, resilient content storage without reliance on centralized servers.



Funded by the European Union

Our existing components include:

Live Casting Platform: A video infrastructure that allows users to host and participate in live events using optimized load balancing principles, reducing latency and improving privacy.

Content Storage Integration: Seamless connection with decentralized storage networks to ensure secure, tamper-proof archival of live streams and related data.

For this NGI TRUSTCHAIN call, we will build on this foundation by integrating Decentralized Identifiers (DIDs) to manage user access and content authorization, enhancing both the security and user control aspects of the platform.

## 2.2 STATE OF THE ART ANALYSIS

Decentralized Identifiers (DIDs) [1] offer a novel approach to digital identity by allowing individuals and organizations to manage their own identifiers without reliance on centralized authorities. By storing identity data on distributed ledgers, DIDs ensure verifiability, privacy, and resilience [2]. Complementing this, DIDs also establish immutable chains of trust, enabling secure auditing of interactions without a central intermediary [3]. Together, these innovations form the foundation of self-sovereign identity systems.

Traditional identity models, such as single sign-on solutions from major tech providers, often compromise user privacy and control. Recent decentralized frameworks like U-Port [8], Serto [9], and Hyperledger Indy [10] have shifted the focus towards empowering users with self-sovereign identity. Although advanced cryptographic methods (e.g., zero-knowledge proofs and threshold signatures) have been developed, few solutions incorporate dynamic, context-aware authentication for live streaming. Our work extends these foundational efforts by integrating DIDs directly into a modular authentication framework, optimized for real-time identity verification and secure access control [11].

These projects also align with emerging standards and regulatory guidelines, such as the W3C Credentials Verification Data Model [2], which emphasizes privacy through techniques like zero-knowledge proofs, and various blockchain-based regulatory frameworks that ensure transparency, security, and user autonomy. This landscape provides both competitive and



Funded by the European Union

complementary foundations that can be leveraged to extend and enhance the Decast.live platform.

*Table 1: COMPARISON OF DECENTRALIZED SYSTEMS*

| System | Architecture | Identity Management | Access Management | Use of Blockchain | Network Used | SSO | Verifiability | Privacy Features | Interoperable | Data storage | Cost of Use | Scalability | Governance Model |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **uPort** | Decentralized-Self-Sovereign | User-controlled | Permission-based user control | Hashes stored for verification | Ethereum | Yes | YES | Selective disclosure, cryptographic proofs, user consent. | Limited to Ethereum ecosystem | Hashes on Ethereum | Gas fees for Ethereum transactions | Limited by Ethereum throughput | Open-source, community-driven |
| **Sovrin** | Decentralized | Self-sovereign identity | Decentralized permission enforcement | Identity recorded on ledger | Hyperledger Indy | Yes | YES | ZKPs, selective data disclosure. | W3C-compliant credentials | Hashes on Indy ledger | Free for users, fees for network ops | Permissioned ledger allows scaling | Decentralized governance |
| **Civic** | Decentralized | Identity stored on user device | User consent through app-based flows | Identity hashes stored for verification | Ethereum | Yes | YES | full user consent, no centralized storage. | Limited to Civic apps | Identity data on user device | Free for basic users | Scalable for Civic app ecosystem | Propertiary |
| **ShoCard** | Blockchain-Based | Identity stored on device, issued via app | hashes for access | Identity hashes stored for proof | Bitcoin | No | NA | Immutable identity proof, minimal data sharing, multi-factor authentication. | Limited to ShoCard ecosystem | Identity data on user device | Free for end-users | Scalable for ShoCard ecosystem | Propertiary |
| **Microsoft DID** | Decentralized | Decentralized identity | DID-linked permission management | Anchors DIDs on blockchain | Bitcoin | Yes | NO | W3C DID standards, user control. | Cross-platform, W3C DID standards | DID documents linked to storage hubs | Free for user, enterprise use based on fee | Scalable on ION | Open governance |
| **W3C DID** | Decentralized | Interoperable DID framework | Independent of specific implementations | Blockchain-agnostic | Varies (agnostic) | No | YES | Open standard, user-centric identity | Cross-platform interoperability | Decentralized storage framework | Free | Depends on blockchain | Open governance via W3C |
| **Blockstack** | Decentralized, Blockchain-Based | Identity linked to blockchain-based ID | DIDs for dApp access control | Blockchain verifies DIDs | Stacks Blockchain | Yes | YES | End-to-end encryption, off-chain data storage, user-controlled identity sharing. | Decentralized app ecosystem | decentralized storage | depending on Stacks fees | Scalable on Stacks | Decentralized community |



Funded by the European Union

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Serto** | Decentralized, consortium based | DID integration | App-level user-controlled permissions | Verification layer using blockchain | Ethereum, Polygon | Yes | YES | Interoperability, selective disclosure, cryptographic proofs. | Interoperable across networks | Off-chain storage with blockchain proofs | Free for basic use | Scalable with Ethereum/Polygon layer | Decentralized with open standards |
| **Indy Ledger** | Decentralized, Permissioned Ledger | Self-sovereign identity | Decentralized network enforces permissions | Verifiable credential registry | Hyperledger Indy | Yes | YES | ZKPs, selective sharing, no reliance on centralized systems, persistence of identity. | W3C DID standards | On-ledger claims and ZKPs | Free for users, operational costs for nodes | Scalable within the Sovrin network | Decentralized, Sovrin Foundation |

## Table 2: Comparison of Decentralized Identity Systems for Human Integration and Data Disclosure

| System Name | Required Trusted Users or Consortium | Working Mechanism | Human Integration | Disclosure |
|---|---|---|---|---|
| **uPort** | No | Privacy is user controlled. | Mobile-friendly app, simple user experience for creating and managing identities. | Full user control with selective disclosure of credentials and cryptographic proofs. |
| **Sovrin** | Yes | Operates as a permissioned ledger managed by a consortium of trusted nodes (stewards) to ensure privacy and consensus. | Focus on usability for end-users with verifiable credentials accessible via wallets. | Zero-Knowledge Proofs (ZKPs) ensure users only disclose necessary data. |
| **Civic** | No | Privacy is managed by the user with information stored locally on their device and hashes on Ethereum. | Mobile app for identity verification and sharing. | users fully control what data to share with whom. |
| **ShoCard** | No | Privacy is managed by users through app-based QR codes and hashes. | QR code-based system with a simple app for managing identity. | Users disclose only hashes for verification, ensuring minimal data exposure. |
| **Microsoft DID** | No | User privacy is managed with decentralized identifiers and identity hubs. No consortium is required, though enterprises may participate. | Enterprise-ready system with integration into apps like Microsoft 365. | Data-sharing transparency with DID documents and user consent for disclosures. |
| **W3C DID** | No | Privacy depends on specific implementations, and no consortium is inherently required. | Standard-based, requiring integration into other platforms for user-friendly access. | Interoperable and user-centric; users control which parts of their identity are shared. |



Funded by the European Union

| | | | | |
|---|---|---|---|---|
| **Blockstack** | No | Uses a decentralized architecture where users control their data. No consortium is required for privacy management. | Easy-to-use identity management via dApps | End-to-end encryption and off-chain data storage ensure users only share necessary identity data. |
| **Serto** | No | Privacy is user-controlled and based on cryptographic proofs. | User-friendly interfaces for managing DIDs and verifiable credentials. | Interoperability and selective disclosure; users retain full control over shared credentials. |
| **Indy Ledger** | Yes | Relies on a consortium of trusted stewards to operate the permissioned Hyperledger Indy ledger, ensuring privacy and trust | Wallets provide a straightforward way for users to manage self-sovereign identities. | ZKPs and verifiable credentials ensure only essential data is disclosed during interactions. |

## 2.3 INNOVATION COMPARED TO THE STATE OF THE ART

Decast.live pushes the boundaries of current technologies by integrating Decentralized Identifiers (DIDs) directly into a live streaming environment. While many existing identity solutions focus on static credentials or document verification, our approach ties dynamic, real-time identity management to the very act of streaming.

This means that users can control who accesses their live content with fine-grained, on-the-fly permissions—without relying on centralized authorities. By merging decentralized live streaming with self-sovereign identity principles, we provide a secure and flexible access control system that stands apart from conventional offerings.

Additionally, our solution will leverage techniques such as zero-knowledge proofs and threshold signature schemes to further enhance privacy and security. This not only ensures that user data remains confidential and under individual control, but also builds trust by preventing unauthorized access in a fully decentralized setup.

In short, Decast.live represents a novel convergence of live decentralized video delivery and next-generation identity management, offering a user-centric, secure, and highly adaptable platform that addresses the limitations of current research and market solutions.



Funded by the European Union

# 3. MOTIVATION AND PLANNED FUNCTIONALITIES

Decast is designed to address the challenges of centralized identity platforms by considering decentralized technologies such as blockchain to empower users to have full control on their credentials while ensuring security and scalability. In this section, we detail the planned features our solution is offering while considering user needs and market demands.

## 3.1 DIDs - DECENTRALIZED ID BASED (AUTHENTICATION)

**Motivation**: Centralized identity management systems often suffer from data breaches and lack user control, which can compromise user's security and privacy. DIDs provide self-sovereign identity management, enabling users to authenticate themselves without relying on centralized authorities.

**Functionality**: In DECAST, DIDs will be implemented using the privacy-preserving architecture, which supports multi-chain interoperability. Users can control their digital identities and data associated with the identity, which are securely stored on a decentralized ledger. These identities are used to authenticate and authorize users on the platform, ensuring privacy and security during live casting sessions.

*Figure 1: Authentication Functionality*

## 3.2 VERIFYABILITY (AUTHORIZATION)

**Motivation**: Establishing trust in user identities is crucial for secure interactions and preventing fraudulent activities.

**Functionality**: The platform uses JWT Strategies and ZKP to verify the authenticity of user identities without exposing sensitive information. Verification logs are maintained, providing transparency and enabling audits by authorized entities. This ensures that all interactions are trusted and secure.



Funded by the European Union

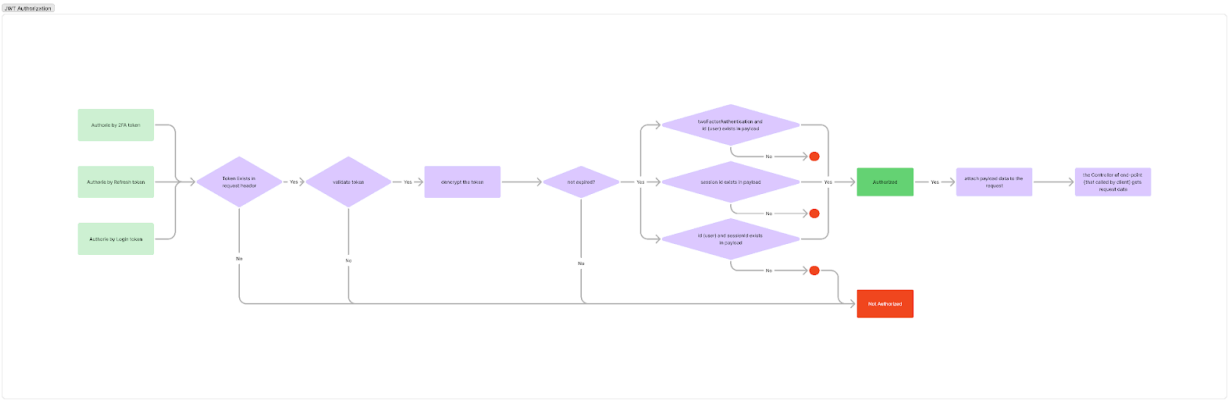

*Figure 2: Verifiability Function*

## 3.3 ACCESS CONTROL (ACCESSIBILITY)

**Motivation**: Fine-grained access control is essential for managing permissions and protecting sensitive resources.

**Functionality**: The platform will use DID's to enforce access control policies. Organizers can allow grant or restrict users from specific resources such as Moderation and Recording access. Role-based access control (RBAC) and Fine-grained permissions (ABAC) strategies will be used to determine accesses.

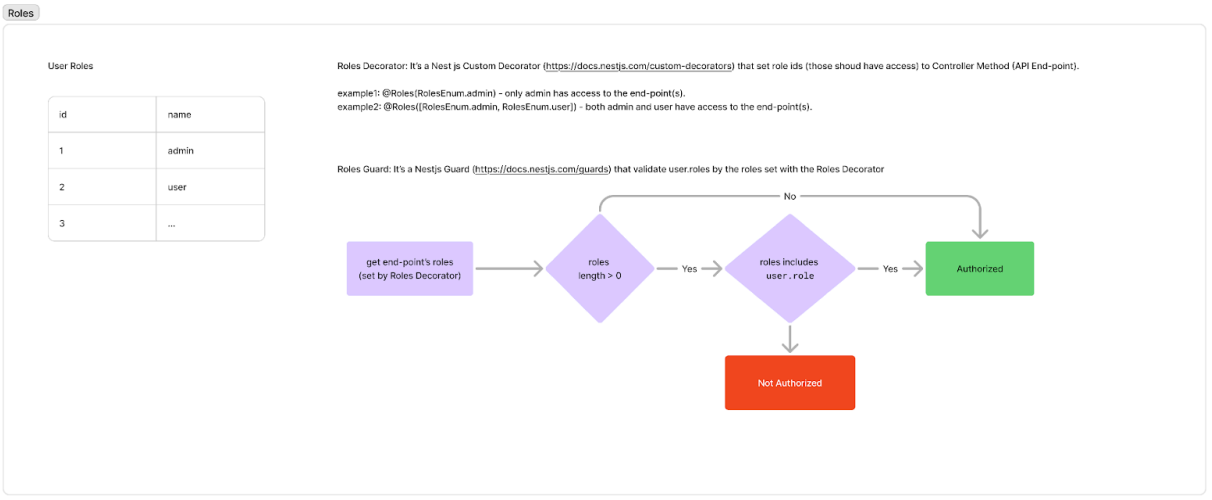


*Figure 3: Access Control*



Funded by the European Union

## 3.4 ROOM, CAST AND DECAST

**Motivation**: There is a requirement for decentralized, secure environments for hosting live sessions, meetings, and events. This would avoid the risks and limitations associated with centralized systems.

**Functionality**: DECAST allows users to create Virtual Rooms for hosting live sessions. Decast leverages blockchain technology to decentralize video stream distribution, minimizing risks like data breaches and ensuring secure, transparent access. Participants authenticate using Decentralized Identifiers, that helps manage permissions and participation seamlessly, creating a tamper-proof record of actions. This innovative approach enhances security, transparency, and reliability, offering users a seamless and trustworthy platform for their live sessions.

## 3.5 LIVE STREAMING

**Motivation**: Live Streaming feature ensures secure, real-time communication by addressing risks like tampering, unauthorized access, and data breaches. It provides a reliable infrastructure to maintain privacy and trust in live broadcasts.

**Functionality**: Live Streaming transmits video and audio data securely. By distributing streams across a network of trusted nodes, it eliminates single points of failure, ensuring consistent service availability even in high-demand scenarios. The infrastructure integrates adaptive bitrate streaming, which optimizes video delivery based on varying network conditions, maintaining high-quality playback for users regardless of their internet speed. This combination of decentralization, encryption, and adaptive streaming guarantees a secure, resilient, and seamless live-streaming experience.

## 3.6 RECORDING AND STORAGE

**Motivation:** Secure storage of a session recordings is essential for future reference, especially in sensitive fields like education and healthcare where privacy, integrity, and accessibility are critical.

**Functionality:** The Recording storage feature offers users the flexibility to store session recordings either in traditional cloud storage or decentralized solutions such as **Sia** or **Swarm**. Both options provide robust, tamper-proof storage for recordings and associated metadata. The platform includes user-controlled, ensuring that only authorized individuals can access the stored data. Additionally, versioning is



Funded by the European Union

supported, enabling users to track and manage edits or updates to recordings, maintaining a complete and secure history of changes.

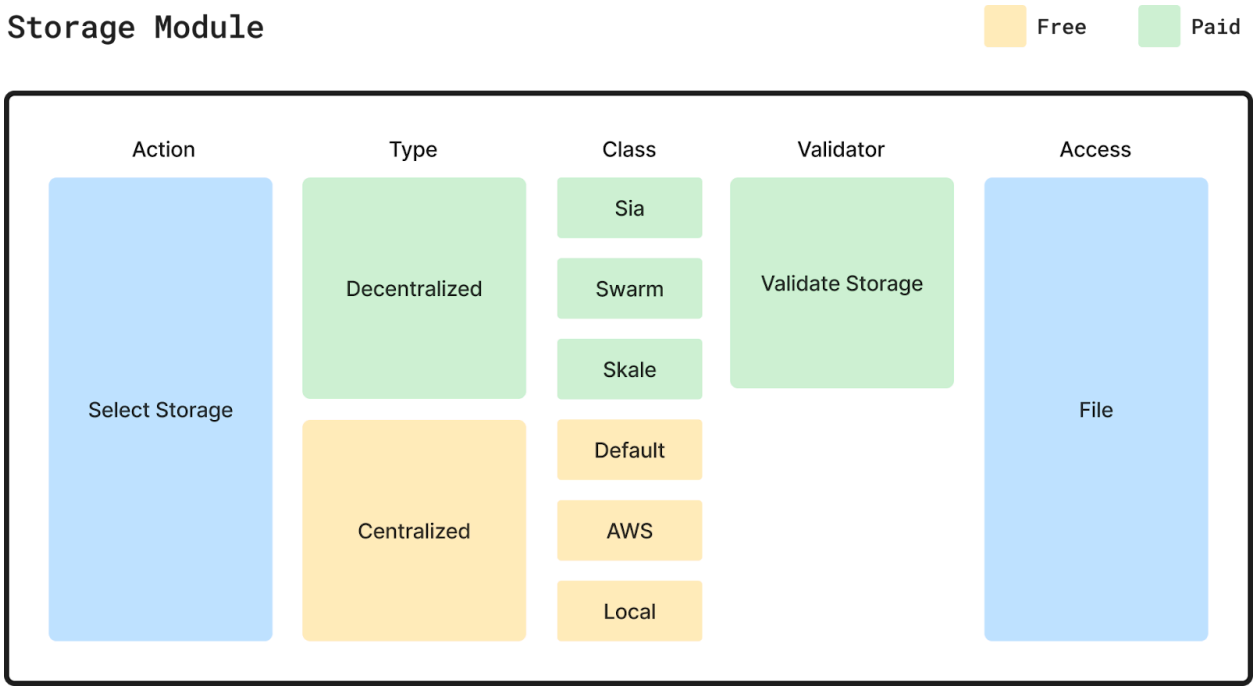


*Figure 4: Storage Module*

## 4. USER NEEDS ASSESSMENT

Our research has focused on understanding the distinct requirements of different communities using live casting. We've engaged with users across legal, corporate, anonymous, and educational settings to ensure our solution is both secure and user-friendly. Key insights include:

**Use Cases for Live Casting Solution**

1. **Witness Testimony in Legal Proceedings**:
    - **Strict Authentication:** Verify identity using government-issued IDs, biometric facial recognition, and liveness detection.
    - **Continuous Monitoring:** Ensure the witness remains authenticated throughout the session.



Funded by the European Union

2. **Corporate Meetings and Webinars**:
    - **Moderate Authentication:** Use facial recognition and liveness detection for secure access.
    - **Behavioral Biometrics:** Monitor user behavior to detect anomalies.
3. **Anonymous Group Meetings**:
    - **Anonymous Tokens:** Allow users to join anonymously with tokens while ensuring they are real participants using liveness detection.
    - **Minimal Data Storage:** No personal data is stored beyond the session.
4. **Educational Live Streams**:
    - **Student Authentication**: Verify student identity at the beginning of the session using facial recognition.
    - **Continuous Engagement Monitoring**: Use behavioural biometrics to ensure students are actively participating.

## 4.1 PROVIDE A DETAILED ACCOUNT ON THE RESEARCH CONDUCTED FOR YOUR COMMUNITY OF USER'S NEEDS.

**Actions Taken:**

- **Research:**
  We began by reviewing current literature, industry reports, and regulations related to virtual events, remote education, and legal proceedings.
- **User Interviews and Virtual Focus Groups:**
  Through one-on-one interviews and structured virtual focus groups, participants shared experiences with current systems to share pain points.
- **Security & Privacy Assessments:**
  This phase involved collaboration with cybersecurity professionals who provided insights into safeguarding user credentials and ensuring the integrity of live streams.
- **Feature Requirement Analysis:**
  In collaboration with our target users, we prioritized essential features such as Decentralized Identifiers (DIDs), NFT-based gating, and advanced tools for



Funded by the European Union

recording post-processing.

- **Iterative Prototyping and Feedback:**
  After gathering initial feedback, we developed early prototypes of our interface and system functionalities.

**General Trends Identified:**

- **Usability Needs:**
  - An intuitive, user-friendly interface that minimizes the learning curve for new users.
  - Accessibility features such as screen-reader support and customizable UI elements, ensuring that the platform is inclusive for all users.

- **Functionality Needs:**
  - Identity Verification: Users consistently emphasized the need for reliable identity verification, specifically through DIDs, to ensure secure and authenticated access.
  - High-Quality Live Streaming: There was a strong demand for adaptive bitrate streaming that can handle varying network conditions without compromising quality.
  - Secure Storage Solutions: Users want a combination of cloud and decentralized storage options to ensure data integrity and privacy.
  - Exclusive Access Control: The use of NFT-based gating was seen as a promising method for monetization and securing exclusive content.

Through the insights gathered from our user community, we have directly influenced the development of Decast.live, ensuring that it not only meets but exceeds the expectations of its users.



Funded by the European Union

## 4.2 USER STORIES

*Grouped by Functionalities and Scenarios:*

**Scenario 1:** *Virtual Conference Experience (Secure & Authenticated)*

DIDs (Decentralized Identifiers):

- As an event organizer, I want to verify participant identities securely so that only authorized users can access my events. (Critical)
- As a viewer, I want to authenticate using DIDs so that my personal information remains private. (High Priority)

Access Control: As an admin, I want to assign roles dynamically so that I can manage participation effectively. (High Priority)

**Scenario 2:** *Digital Education Transformation (Virtual Classroom)*

Live Streaming:

- As a teacher, I want to stream live lessons securely so that my students can access content without interruptions. (Critical)
- As a student, I want to access high-quality streaming so that I can engage in real time. (High Priority)

Recording Storage (Cloud + Web3):

- As a teacher, I want to save my lectures securely so that students can review them later. (Critical)
- As a developer, I want decentralized storage for IP integrity. (High Priority)

Recording post-processing: As an educator, I want to edit recordings so that I can provide concise and relevant content. (Moderate Priority)

**Scenario 3:** *Legal Consultation Innovation (Remote Legal Services)*

DIDs (Decentralized Identifiers):

- As a lawyer, I want to authenticate clients securely so that confidential sessions are protected. (Critical)



Funded by the European Union

- As a client, I want to use a private and secure identity system so that my personal information is safe. (High Priority)

Verifiability: As a legal professional, I want audit logs for client interactions so that I can ensure compliance and accountability. (High Priority)

Access Control: As a lawyer, I want to control session permissions dynamically so that only authorized individuals participate. (Moderate Priority)

**Scenario 4:** *Digital Legal Testimony (Secure Court Proceedings)*

DIDs (Decentralized Identifiers): As a court official, I want to verify witness identities securely so that testimonies are credible. (Critical)

Recording Storage (Cloud + Web3): As a administrator, I want tamper-proof storage for session recordings so that legal proceedings are preserved securely. (High Priority)

Version Control: As a legal team member, I want to track recording changes so that I maintain an accurate history. (Moderate Priority)

## 4.3 PROVIDE WITH A PLAN FOR THE UPCOMING PILOTS

**Users Involved:**

- **Educators**: From schools, universities, and online training platforms.
- **Legal Professionals**: Lawyers, paralegals, and court officials.
- **Corporate Trainers and Event Organizers**: From diverse industries.
- **Blockchain Developers**: To test and provide feedback on functionalities.
- **General Users**: Representing a wide range of demographics.

**Channels Employed to Reach Users:**

- Professional Networks: Leveraging platforms like LinkedIn.
- Educational and Industry Collaborations: Working with schools, universities, and online communities.
- Direct Outreach: Email campaigns and targeted social media initiatives.
- Ambassador Partnerships: Engaging domain experts to recruit participants.



Funded by the European Union

**Methodological Approach:**

1. Preparation Phase:
    - Define pilot scenarios based on research focus areas (e.g., virtual classrooms, secure legal consultations).
    - Develop user guides, FAQs, and walkthroughs for participants.
2. Execution Phase:
    - Conduct separate pilot sessions for each focus area, emphasizing specific functionalities (e.g., DIDs for authentication, NFT gating).
    - Gather real-time feedback through interviews.
3. Analysis Phase:
    - Analyse user feedback to identify pain points and areas for improvement.
    - Validate pilot outcomes against research focus areas and user stories.

**Pilots' Results (Preliminary):**

- **User Experience & Functional Performance:** Detailed insights into how key features (like live streaming quality and NFT-based access control) perform in real scenarios.
- **Authentication Validation:** Early confirmation of DIDs' effectiveness for secure authentication across various use cases.
- **Scalability Insights:** Identification of performance challenges during high-demand events, guiding necessary refinements in the infrastructure.

**Design Specifications Drawn from the Pilots:**

1. **User-Validated Feature Roadmap**:
    - Identify critical functionalities and prioritize their development.
    - Use Fider at fider.decast.live to manage feedback efficiently.
2. **Security Requirement Specifications**:
    - Develop comprehensive security protocols for streaming, decentralized storage, and user authentication.



Funded by the European Union

- Define DID-based workflows for different use cases (e.g., event organizers, legal professionals).

3. **Implementation Priorities**:
   - Conduct an Effort vs. Return analysis to focus on high-impact features.
   - Maintain a CR (Change Request) sheet for tracking technical and operational updates.
4. **Adoption Strategy Insights**:
   - Create sector-specific onboarding guides and video walkthroughs.
   - Optimize website to highlight key value propositions for user groups.
5. **Platform Enhancement Recommendations**:
   - Categorize user inputs into BR (Bug Reports), CR (Change Requests), DR (Data Requests), and ER (Enhancement Requests).
   - Focus on improving usability, accessibility, and cross-platform functionality based on categorized feedback.

# 5. SOFTWARE DESIGN AND ANALYSIS, COMPONENT SPECIFICATION (PRELIMINARY)

This section outlines the architecture of DECAST.LIVE, highlighting its core modules and the integration of decentralized components.

## 5.1 HIGH-LEVEL ARCHITECTURE OVERVIEW

The application follows a microservices architecture implemented using the NestJS framework and a mono-repo structure for the Authentication module (Foreground). The system includes the following key components:

**Foreground:**

1. **Authentication Module** – Handles authentication, including login via wallet, social etc. authentications.



Funded by the European Union

2. **Shared Library** – Contains reusable utilities, common types, and shared business logic.

3. **API Gateway** – Routes requests and provides a unified interface for clients.

## Background

1. **Storage Service** – Manages file storage, retrieval, and access control.
2. **Video Infrastructure** – Works as the interaction layer for all events and casts.

Decast will follow a Hexagonal Architecture. The main reason for using it is to **separate the business logic** from the infrastructure. This separation allows us to easily change the database, the way of uploading files, or any other infrastructure without changing the business logic.

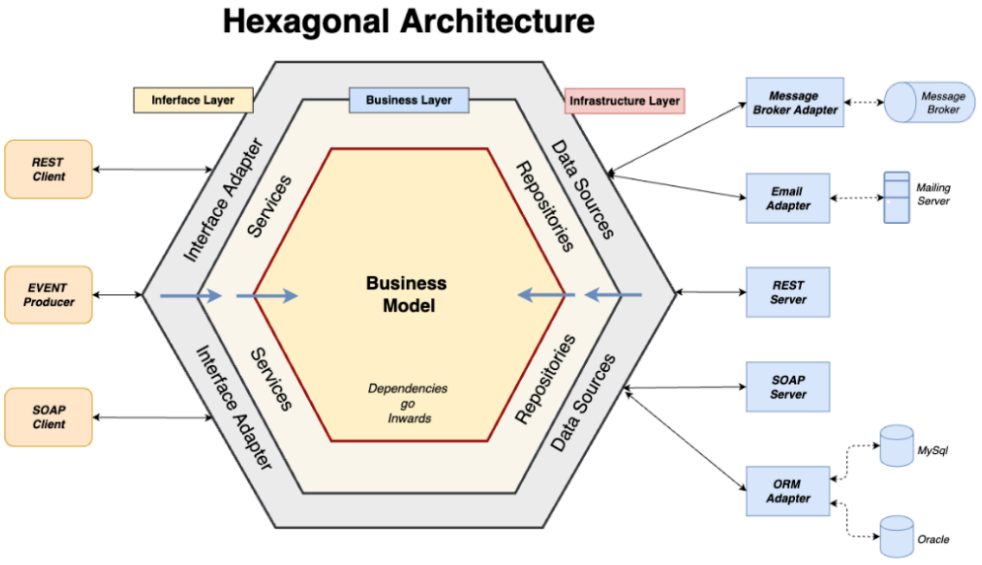


*Figure 5: High Level Architecture*



Funded by the European Union

This further integrates into Decast's vision of developing a Decentralized Physical Infrastructure (DePIN).

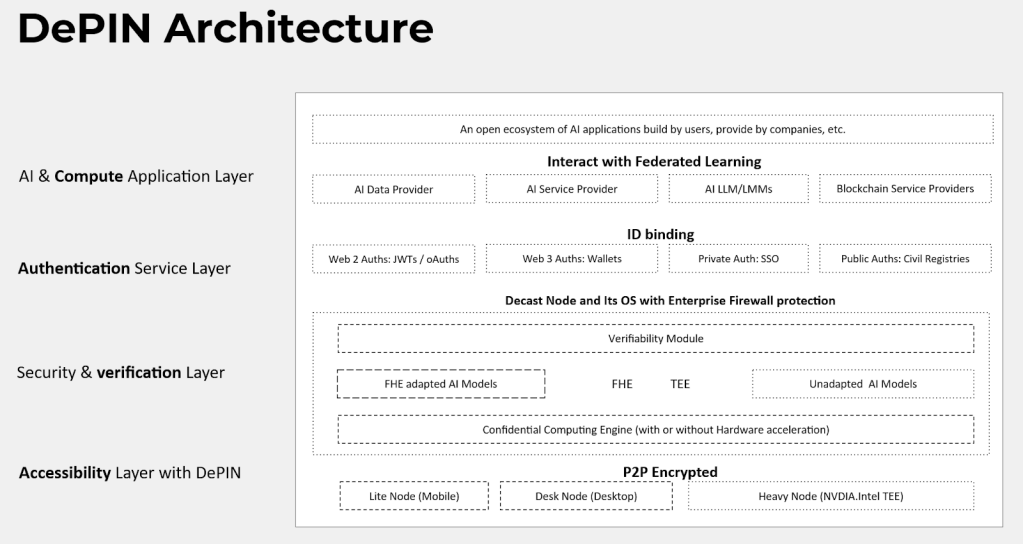


*Figure 6: DePIN Architecture*

## 5.2 MODULES AND COMPONENTS

### Authentication Module (Foreground)

The **Authentication Module** is responsible for handling user authentication using decentralized identifiers (DIDs), social login, and traditional email/password methods. It eliminates the need for traditional username/password authentication by enabling users to log in with their wallets while still supporting conventional authentication methods.



Funded by the European Union

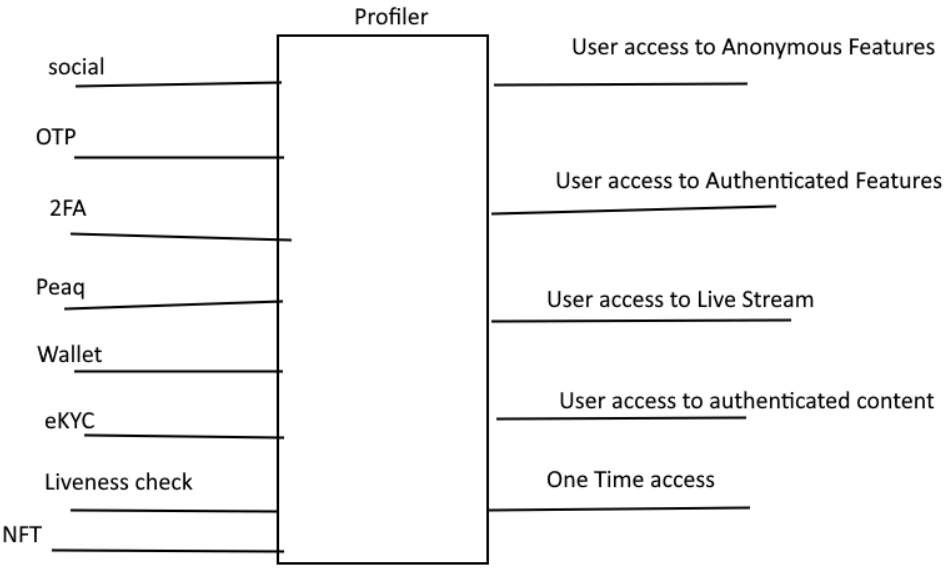


*Figure 7: Authentication Profiler*

**Authorization Strategies (Passportjs.org)**

Our authentication system utilizes various JWT-based strategies to manage user authorization and session handling effectively.

- **JWT (DID-JWT) Access Token**: Used to verify user authentication. It stores the userId, role, and sessionId.
- **JWT (DID-JWT) Refresh Token**: Used to obtain a new access token while checking for any user changes in storage. It stores the sessionId and userId.
- **JWT (DID-JWT) 2FA Token**: Used for two-factor authentication (2FA) during login or sensitive actions. It stores the userId.
- **Anonymous Token**: Used for anonymous sessions with predefined, limited permissions. It stores the sessionId.



Funded by the European Union

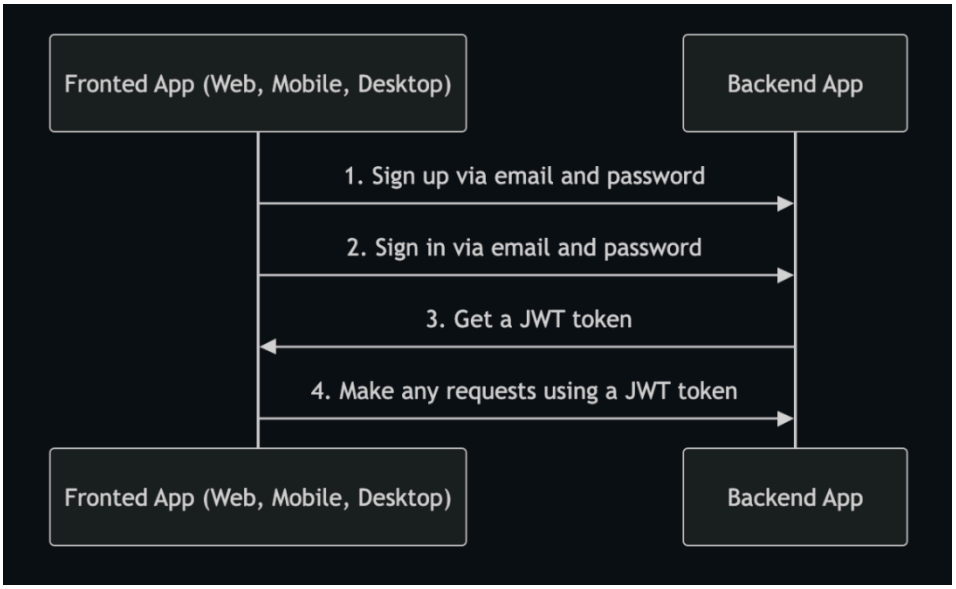


*Figure 8: Simple JWT Login sequence*

**Components**

- **Wallet Authentication**: Allows users to sign authentication requests with their wallets.



Funded by the European Union

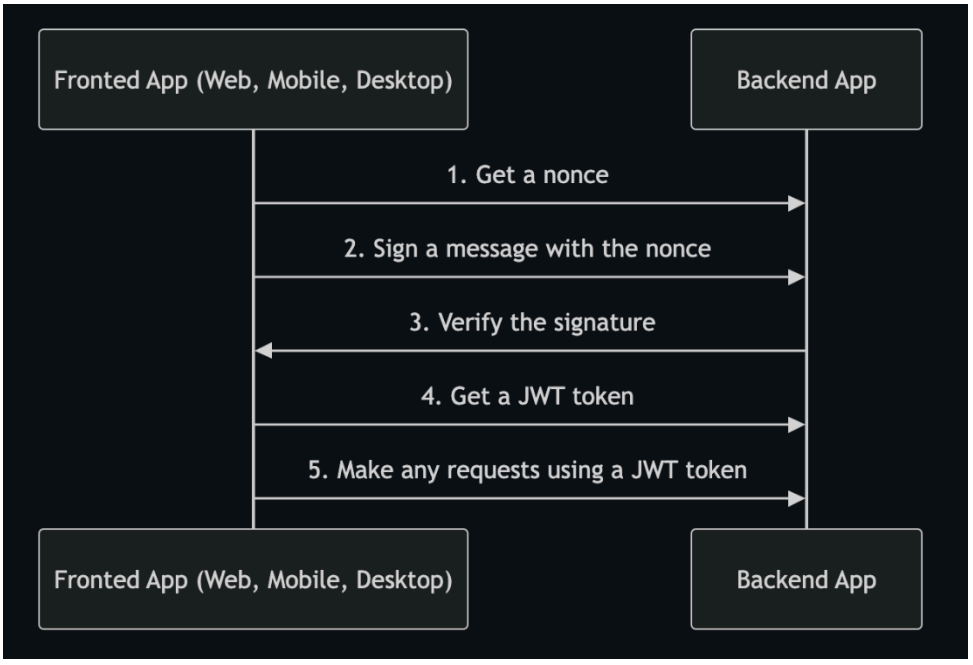


*Figure 9: Wallet JWT Login sequence*

- **DID Verification**: Ensures the validity of the user's decentralized identity using ethr-did.
- **JWT Issuance**: Generates and signs JSON Web Tokens (JWTs) for authenticated sessions.
- **Session Management**: Manages user sessions, token refresh mechanisms, and expiration policies.
- **Two-Factor Authentication (2FA)**: Provides an additional layer of security using OTP.
- **Social Login**: Supports OAuth 2.0 authentication for Google, Facebook, and other providers.



Funded by the European Union

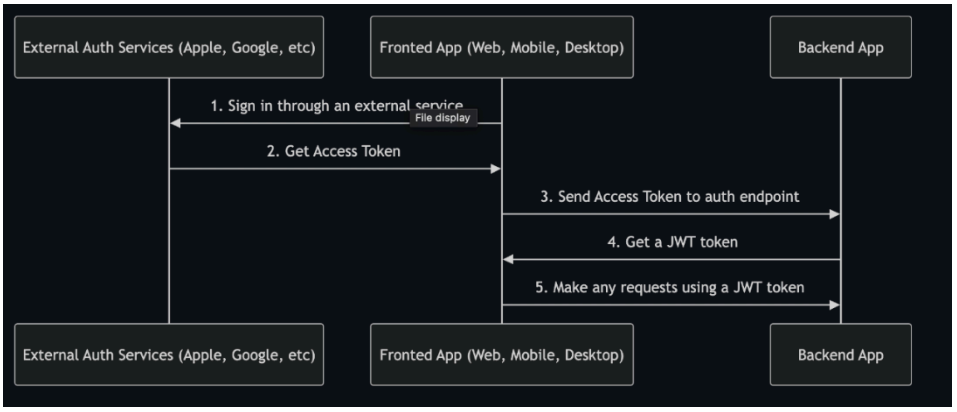


*Figure 10: Social JWT Login sequence*

- **Email/Password Authentication**: Allows users to register and authenticate using email and passwords.

## 5.3 COMPONENT INTEGRATION AND DEPLOYMENT



Funded by the European Union

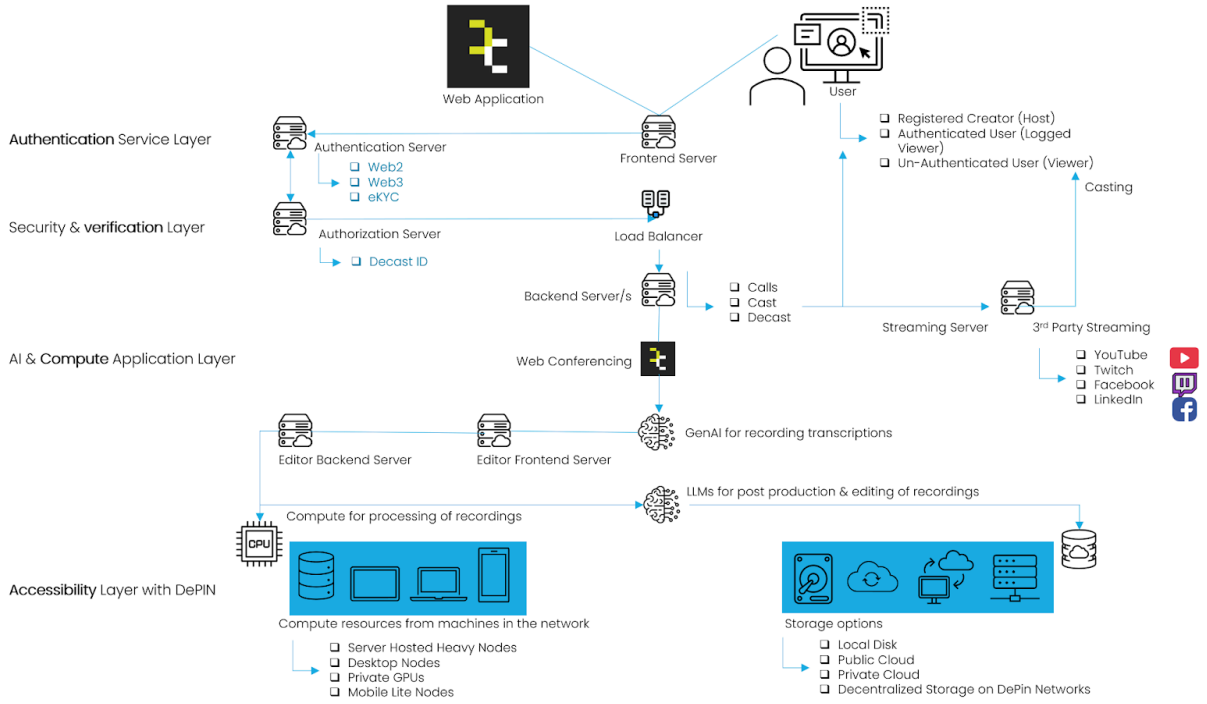


*Figure 11: Platform Architecture*

The architecture of the video infrastructure integrates multiple interconnected components to deliver a seamless and secure solution.

### *Foreground*

**Modular Authentication Layer:** We designed a plug-and-play authentication module that interfaces directly with the live streaming engine. This module is responsible for dynamically selecting authentication mechanisms—such as social logins, OTPs, biometric checks, and wallet-based verifications—based on the event context and user role.

**DID Management and Profiler Package:** At the core of our approach is the integration of Decentralized Identifiers (DIDs). We developed a dedicated DID management system that leverages self-sovereign identity principles, enabling users to control their credentials via a distributed ledger.



Funded by the European Union

***Background***

**Web Application** serves as the user interface, connecting to **Backend Servers** that handle core functionalities like calls, casting, and streaming.

**Streaming Server** supports live casting to platforms like YouTube and Twitch, enabling broad content distribution. Together, these layers ensure scalability, decentralized infrastructure, and secure interactions, providing a robust alternative to centralized solutions.

***Foreground + Background***

**Storage module** leverages decentralized storage options like Sia, ethSwarm etc. to ensure data privacy, tamper-proof storage, and autonomy for its users while also providing traditional storage options.

***Future Work***

Advanced features, such as real-time transcription and post-production editing, are powered by the **AI & Compute Application Layer**, leveraging decentralized compute resources from the **Accessibility Layer with DePIN**, which utilizes server nodes, GPUs, and decentralized storage networks.



Funded by the European Union

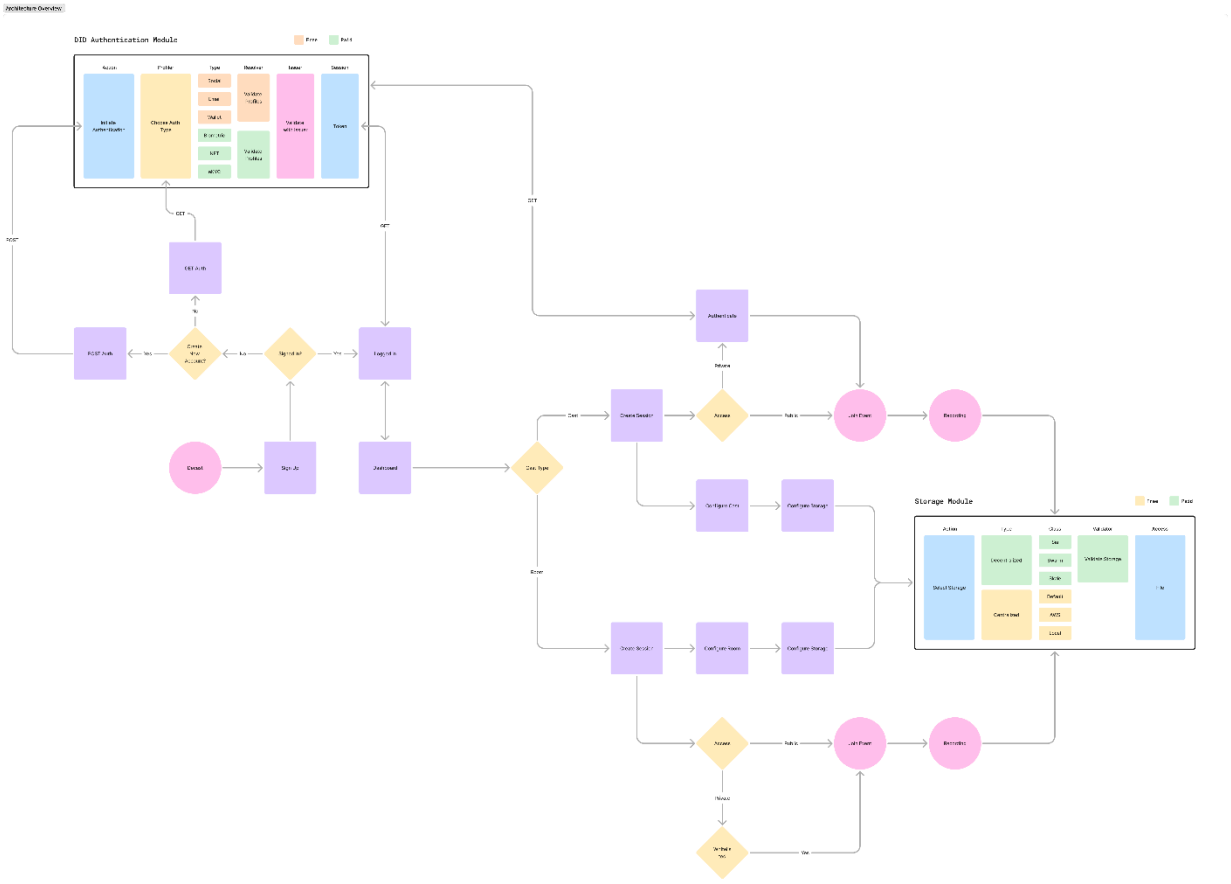


*Figure 12: Module Integration Map*

# 6. PLAN FOR IMPLEMENTATION AND DEPLOYMENT (PRELIMINARY)

This section defines the implementation and deployment strategy for DECAST.LIVE, focusing on the phased approach to integrating decentralized technologies and ensuring scalability.

## 6.1 IMPLEMENTATION PLAN

Key milestones, tasks, and timelines are outlined below:



Funded by the European Union

*Table 2: WORK PLAN TASKS AND TIMELINE*

| **Work plan tasks** | **Description** | **Starting Month** | **Ending Month** |
|---|---|---|---|
| Project Initiation and Research | Requirement Gathering, Market Analysis, Technical Feasibility Analysis, Team Formulation | Nov 2024 | Jan 2025 |
| Prototyping and Development | Development of the Prototype, Blockchain Integration, DID Implementation and Testing, Security Testing, User Interface Design and Integration | Jan 2025 | March 2025 |
| Testing and Iterative Refinement | Beta Release<br>Usability Testing<br>Scalability Assessment, Identity Integration, Video Integration<br>Security Audit | March 2025 | April 2025 |
| Deployment and Marketing | Full Release<br>Marketing Campaigns<br>User Acquisition and Promotion<br>Documentation and Support | May 2025 | June 2025 |
| Ongoing Optimization and Future Planning | Continuous Improvement<br>Future Roadmap<br>User Training and Deployment | June 2025 | July 2025 |



Funded by the European Union

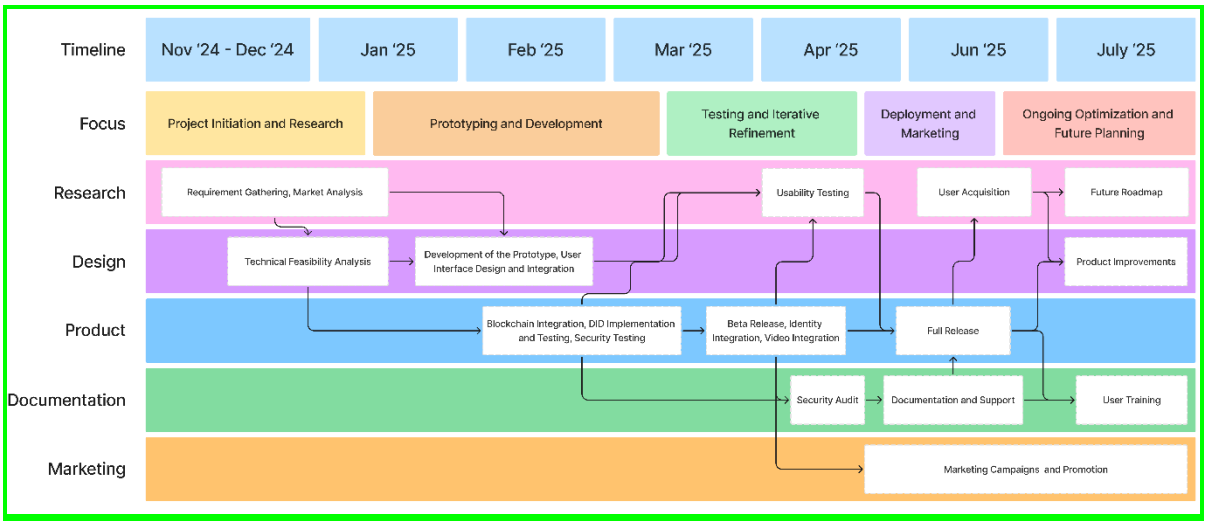


*Figure 13: Gantt Chart of Workplan*

## Resources and Role Allocation

*Table 3: RESOURCES AND ROLE ALLOCATION*

| Name | Role | Social Profile |
|---|---|---|
| Shivam Dhawan | Project Coordinator | https://www.linkedin.com/in/shivamdhawan/ |
| Aman Bishnoi | Development Lead & Backend Developer | https://www.linkedin.com/in/aman-j-bishnoi/ |
| Mohammed Yasrab | Product Manager & Designer | https://www.linkedin.com/in/mohammed-yasrab/ |
| Anish Jha | Application Developer | https://www.linkedin.com/in/anish-jha7/ |
| M. Ajmal Azad | Blockchain Researcher | https://www.linkedin.com/in/sushil-kumar-gupta/ |



Funded by the European Union

| | | |
|---|---|---|
| Sushil Gupta | Application Developer | https://www.linkedin.com/in/muhammad-ajmal-azad-25b34717/ |

## Deliverables and Milestones

*Table 4: DELIVERABLES AND MILESTONES*

| No. | Deliverable or milestone name | Description | Type | Delivery Month | TRL level delivered |
|---|---|---|---|---|---|
| 1 | Requirement Analysis | A requirement analysis and design document will be released | Document | Jan 2025 | 7 |
| 2 | Feasibility and Market Analysis | A Market analysis report will be released after studying major competitors and performing requirement and need analysis | Report | April 2025 | 7 |
| 3 | Implementation, Testing and Analysis | A detailed report will be released that will cover all functional, non-functional, and security use cases. The report will cover all implementation | Report | June 2025 | 8 |



Funded by the European Union

| | | | | | |
|---|---|---|---|---|---|
| | | and testing details/scenarios. | | | |
| 4 | Product Release | An open-source codebase will be released | Tool/code repository | June-July 2025 | 7 |
| 5 | Research paper and final report | Project documentation will be released. | Documentation | July 2025 (Document) and July-August (Research Paper) | 10 |

## 6.2 DEPLOYMENT PLAN

The deployment process of proposed DECAST will follow a complete work plan to ensure a smooth, nominally disruptive shift towards production environment. This deployment plan includes five phases: preparation, deployment, testing and validation, monitoring and maintenance.

**Preparation Phase**

Preparation phase will include several steps such as setting up the necessary infrastructure, organizing necessary resources, and deployment planning of DECAST LIVE.

**Infrastructure Setup:** Infrastructure setup for deployment will includes the establishment of technical environment such as cloud services or on-premises servers as per the requirements of the platform. It will also include the setup of blockchain nodes, configuration of databases, and organizing adequate resources.

**Resource Allocation:** In resource allocation, roles and responsibilities will be assigned to concerning team members such as, developers, administrators, quality assurance testers etc. Training session will also be conducted for the team members to make them familiar with technologies and processes related to the deployment.



Funded by the European Union

**Documentation Preparation:** System architecture, deployment guidelines and procedures will be documented comprehensively to make sure that all the team members are clear about the tasks and system requirements.

### Deployment Steps

Proposed DECAST Live platform will be released into the production environment during deployment phase involving initial deployment, integration and configuration, feature activation and user onboarding activities.

**Initial Deployment:** Firstly, core components of the DECAST Live e.g. identity Verification, Blockchain integration, Implementation of Zero Knowledge proofs and integration with online video sharing platform. Following by the setup of software on servers, integration with blockchain and correct configuration of platforms modules

**Configuration and Integration:** After this initial deployment of system components, configuration of system setting and integration of components will be performed. This involves building connection between ZK proof modules and blockchain based identity wallet and storage of Video.

**Feature Activation:** Key functionalities of the system, such as wallet management, video broadcasting, user interaction will be activated. Correct working of these functionalities and their compliance with benchmark performance will be ensured.

**User Onboarding:** Initial users will be onboard and necessary access credentials will be provided to them. After creating user's accounts, system's initial data will be imported to test the system's functionalities.

### Challenges and Solutions

**Dynamic Integration:**
Selecting the appropriate authentication method on-the-fly without disrupting the user experience will be a major challenge. We will address this by implementing a middleware profiler that will classify events and user roles using nested segmentation, ensuring seamless and context-aware authentication.

**System Interoperability:**
Integrating the new authentication layer with existing decentralized storage systems (ethSwarm, Sia) and live casting components will require careful design to avoid disruption. We will solve this by developing a well-defined API that will allow the authentication module to operate independently while interfacing smoothly with the core platform.



Funded by the European Union

**Balancing User Experience and Security:**
Implementing stringent security measures without overburdening users will be a delicate balance. Our adaptive framework will ensure that low-risk scenarios offer frictionless entry while higher-risk events trigger additional security layers, maintaining an optimal balance between usability and protection.

# 7. CONCLUSIONS

This project tackles the challenges of decentralized identity management and secure video casting by eliminating centralized vulnerabilities and enhancing privacy and user autonomy. As online interactions surge, risks like data breaches and identity theft demand innovative solutions. Our initiative leverages blockchain, decentralized identifiers (DIDs), and zero-knowledge proofs to provide robust identity verification, fine-grained access control, secure streaming, NFT gating for exclusive content, and customizable branding.

Our design is guided by extensive user feedback from educators, legal professionals, event organizers, and IT experts, ensuring an intuitive interface, adaptive streaming, and secure storage that blends decentralized networks with traditional cloud services. Technically, we have established a decentralized architecture that uses blockchain for tamper-proof data and encryption for privacy, with modular components for scalability. The system also integrates oracles to connect legacy systems and advanced cryptographic methods to guarantee interoperability and robust security.

In summary, this pioneering effort redefines identity management and video casting in a decentralized context, setting a new standard for secure, transparent, and efficient digital interactions. Decast is poised to empower users and organizations with a seamless, privacy-preserving, and highly adaptable digital solution for the modern era.



Funded by the European Union

# REFERENCES


1. Sporny, M., Longley, D., Sabadello, M., Reed, D., & Steele, O. (2022). *Decentralized Identifiers (DIDs) v1.0*. Retrieved from https://www.w3.org/TR/did-core/
2. W3C. (2022). *Credentials Verification Data Model*. Retrieved from https://www.w3.org/TR/vc-data-model/
3. Xu, J., et al. Anonymous Credential Schemes.
4. Garman, C., et al. Anonymous Credential Schemes.
5. Coconut Project. Decentralized Credential Issuance Framework.
6. PrivIdEx Project. Privacy-Preserving Identity Exchange.
7. CanDID Framework. A Blockchain-Based Framework for Decentralized Identifiers.
8. U-Port. Self-Sovereign Identity Management.
9. Serto. Decentralized Identity Solutions.
10. Hyperledger Indy. Distributed Identity.
11. Microsoft. Decentralized Identifier Solutions.




Funded by the European Union

# APPENDIX A.

Anything that is related but not core to the deliverable can go into appendix.



Funded by the European Union