HISTO BIT

Roadmap Histo Bit

1) Problem Definition

Currently, hospitals, health insurance companies, health insurance funds, and clinics manage patients' medical information and records. This setup leads to issues with portability, security, data breaches, and a heavy dependence on centralized systems that are vulnerable. Additionally, patients lack the freedom to choose who can access their data for medical opinions, while still maintaining confidentiality about their medical conditions.

2) Value Proposition

Our solution aims to empower patients to manage and control their own medical records, allowing for portability between different healthcare providers and giving patients the authority to decide who can view their medical data and for how long. We propose a model that combines cryptographic security with a user-friendly interface, built on a private (L1) encrypted blockchain. This approach ensures the privacy and security of documents.

The goal for this competition is to demonstrate the solution through an MVP, with insurers and physicians as the entities and patients as the end users, including auditors for blockchain security. The MVP will be capable of managing role and action creation, handling encrypted data (creating, modifying, and setting permissions), and providing navigation flow for both web and mobile applications.

Likewise, since the patient is the owner of the data, they will be given the ability to monetize their profile statistics through encrypted tokens. This way, they can benefit from sharing them with various healthcare entities that require this

information for various purposes, such as medical and pharmacological research, hospital management, market research, health policies, etc.

Actors and Roles

Histo Bit contemplates four main types of users:

· Patients: will be the true owners of their data, managing their read and write permissions and deciding with whom to share it.

· Doctors: will have the power to read and validate clinical information, generating records that will then be stored on the blockchain.

· Insurers: will manage the list of their insured users and act as part of the network's validators.

· Auditors: will have a monitoring role over user transactions, actions, and activities.

3) Technical Complexity

Access and Permissions

Initial access management will utilize a digital wallet that links verified identities to access credentials. Future integration with biometric recognition is planned. A dynamic permissions system, governed by smart contracts, will enable patients to grant or revoke access in real time.

Security, Data, and Cryptography

The system will process various types of information, including medical records, identity data, audit logs, and usage statistics. All sensitive data will be encrypted and stored on the private Layer 1 (L1) blockchain. Large files, such as medical images or lengthy certificates, will be encrypted and stored in an external repository linked to the L1 blockchain.

Monetary transactions between users and entities, including those for granting permissions or accessing statistical data, will be conducted in isolation and encrypted using the enhanced ERC20 (eERC20) protocol. Additional confidentiality will be provided through encryption algorithms such as Baby Jubjub and Partial Homomorphic Encryption. Zero Knowledge Proofs will be employed to validate transactions without disclosing sensitive information, ensuring end-to-end security.

Key management and account generation will be based on biometric human identification or proof of human presence for each individual or entity. This approach is intended to enhance overall system security.

Smart Contracts and Logic

The core of the application will be based on specific smart contracts. One will control access and roles, defining differentiated permissions for patients, physicians, insurers, and auditors. Another will store medical records, which will store only hashes and encrypted references, maintaining complete information in IPFS.

There will also be a transactional contract that records all access and modifications, functioning as a fully auditable record. Consent management will be resolved through an additional action, allowing each patient to decide what information to share and for how long. Finally, an encrypted token is being considered for managing identities and digital assets linked to users.

4) Avalanche Components

Avalanche Architecture

The project will be built on Avalanche through a private (L1) permissioned blockchain. The validators will be participating insurers and medical entities, ensuring a mixed consortium structure. Snowman++ will be used as the consensus protocol, enabling low latency and near-instant transaction finality, a key factor for medical environments.

The virtual machine will be compatible with the EVM, opening the door to developing smart contracts in Solidity and leveraging ecosystems already known by the industry. Gas will be managed with a native token of the network, designed solely for internal operations. The possibility of integrating bridges to public networks is anticipated from the outset, but the first phase will operate in isolation to ensure simplicity and control during the initial deployment.

5) Feasibility

Applications and Integration

The user experience will be delivered through web and mobile apps. Each profile will feature an interface designed for their role: patients can view their data and control permissions; physicians can validate clinical records; insurers can access administrative dashboards; and auditors can monitor user activities.

For the demonstration phase, a user-friendly, intuitive interface focusing on patients will be developed.

6) Development Phases

The development will be structured into four key stages.

Stage One:

Deploy fundamental smart contracts, encryption logic, and security tests using Hardhat. Then, integrate simulated data with IPFS and develop the user interface, emphasizing permission workflows and clinical records.

Stage Two:

Set up the initial infrastructure: the private blockchain on Avalanche, validator nodes, RPC nodes in the cloud, and establish a closed testing environment.

Stage Three:

Integrate the audit layer, permission control panels, and privacy tests using Zero Knowledge Proofs.

Stage Four:

Perform network stress testing, simulate multi-user environments with different roles, and prepare technical and executive documentation for the public presentation.

5) Deliverables

Upon completion of all stages, this project will have a functioning private blockchain, deployed and verified smart contracts, an application with a prominent interface, simulated medical data managed with advanced encryption, and an audited technical metrics report.

6) Attached Documents

- Roadmap

- Github repository

- Application flows

- Slide presentation

- Demo video

- Website

- Corporate image