ROAX: Rod of Asclepius eXchange (Draft)

Kenneth Goh Zhen Hao
zhenhao.goh@comp.nus.edu.sg

June 20, 2024

Abstract

ROAX is a universal healthcare system build on top of blockchain technology, a platform designed to empower both doctors and patients by providing a secure, compliant, and privacy preserving system for storing verifiable proofs and signatures of medical records. Utilizing blockchain technology, ROAX ensures the integrity, security, and interoperability of medical data, transferring data ownership directly to the record owner. For the first time, the platform incentivizes doctors to collaborate, fostering a cooperative medical ecosystem.

By decentralizing verifiable data, ROAX significantly enhances data security, protecting against breaches and unauthorized alterations. This immutable and verifiable record system not only safeguards patient information but also assures the credibility of medical records.

ROAX introduces a universal interoperable framework, the idea was inspired from the end-to-end encryption from WhatsApp and incorporates blockchain technologies as well as recent trends of cryptography to complete an entire infrastructure that can facilitate the development of Decentralized Medical (DeMed) applications, thereby broadening the scope and accessibility of healthcare services. The platform supports a new economy for medical data, promoting efficient data availability and utilization across the medical industry.

This document provides a comprehensive overview of ROAX, detailing its technical architecture, economic and governance models, and potential applications. Through ROAX, the medical industry can achieve a secure, efficient, and collaborative future, benefiting all stakeholders involved.

1 Acknowledgements

Also, I'd like to take this opportunity to thank my dear friend, Ansel, a super stacked individual, a medical doctor, a post-graduate in computing and a post-graduate in analytics. Thank you for the encouragements and excitement to contribute to this project.

This is also for a dear uncle Alex, a well known doctor in his field. Thank you for the extended helping hand to a stranger when the silence was really loud. There are still noble and respectable doctors out there, it makes this place alot easier to live in. This project is for all the doctors and medical professionals out there!

Contents

2 Introduction

The healthcare industry faces significant challenges related to data security, record credibility, and a lack of incentives for medical professionals to cooperate. ROAX aims to address these challenges by providing a decentralized, immutable, and universally interoperable medical record system. This document outlines the vision, technical architecture, economic model, and potential applications of ROAX.

In the wake of previous medical system hacks, such as ransomware attacks[23] and the SingHealth data breach [24], it has become evident that centralized storage of information presents significant security vulnerabilities. ROAX enhances security by ensuring that information is not only stored on a centralized authority but remains with the data owner. This decentralized approach significantly mitigates the risks associated with data breaches.

Furthermore, the credibility of medical records is crucial. Instances like a Singapore doctor who altered medical records for personal gain highlight the dangers of tampering with medical data[5]. ROAX provides a secure and safer alternative through its immutable decentralized medical record system, ensuring that records cannot be altered without detection.

Another critical issue is the lack of sufficient incentives for doctors and medical professionals to actively contribute to the healthcare ecosystem. ROAX proposes a solution by creating an economic model that incentivizes medical stakeholders. By enabling a universally interoperable protocol, ROAX fosters cooperation and connectivity among various medical entities, promoting a more collaborative and efficient healthcare system.

ROAX is being built as a Layer 1 blockchain system[4] focused on establishing a universal interoperable privacy preserving medical record framework. This innovative approach offers numerous benefits:

- **Universal Interoperability:** ROAX provides a framework that allows Decentralized Medical (DeMed) applications, such as insurance services, to be built on top of the core blockchain layer, promoting widespread adoption and integration.
- **Immutable, Privacy-Preserving, and Verifiable Records:** The system ensures that medical records are immutable and verifiable while preserving patient privacy. Only a verifiable proof is submitted onchain, while the raw data is securely stored in the patient's hardware device / mobile device. (Inspiration from WhatsApp End-To-End Encryption). Anyone, that receives the shared record, by the patient or the authorised entitiy can easily verify the medical record onchain. The current way of storing medical data in healthcare system is preserved.
- **Patient Data Ownership:** Patients maintain ownership of their medical records in a secure manner, giving them control over their personal health information. In the case of a ransomware attack, patients can easily re-share their records and medical entities can verify them on chain. They can, without fees, locally share their medical records and any receiving entity can actually verify the records on chain.
- **Cooperative Incentives:** For the first time in many years, ROAX gives doctors and medical professionals a voice and a stake in the system, providing incentives to cooperate and contribute to a universal healthcare network. Medical professionals are incentivised to keep the network secure, anyone requesting information will have to pay a transaction fee. In comparison to most national healthcare record system that face difficulties to rally private medical practitioners to share patient's medical record. A entity submitting data to a requesting entity, can make use of the receiver's public key, encrypt the data into a trusted temporary data availability service, emit an event, the receiver can locally decrypt the medical record.
- **New Economy:** In face of monopolistic organisations that have rights over medical data in an AI driven world, this creates an economy that allows individuals to contribute and monetise their own data to projects, possibly allowing more healthy competition in the market. A new insurance economy (a large portion of finance) can also be spun off from the foundations of this network.

ROAX is not a disruptive technology; rather, it catapults the existing healthcare system into a universal interoperable network, evolving the current system into humanity's next healthcare system. This transformative approach aims to enhance the security, credibility, and efficiency of medical records, ultimately benefiting patients, healthcare providers, and the entire medical ecosystem for humanity. It is capable of spinning new economies driven by patient participation and secured by medical professionals.

3 Background

Blockchain technology, pioneered by platforms like Bitcoin[13], Ethereum [17] and Polkadot[21], has shown immense potential to revolutionize various industries. However, these platforms are not specifically tailored to address the unique challenges faced by the healthcare sector. ROAX aims to be the first universal, interoperable medical record system, offering a secure and efficient solution for storing and sharing medical data. Unlike disruptive technologies, ROAX enhances the existing healthcare infrastructure, transforming it into a universal inter-operable network. This evolution propels the current system into a comprehensive healthcare system for humanity.

3.1 Blockchain Technology Structure

A blockchain is a distributed ledger that records transactions in a secure and immutable manner. Each block contains a list of transactions, and each block contains the cryptographic hash of the previous block, forming a chain. This structure ensures the integrity and security of the data.

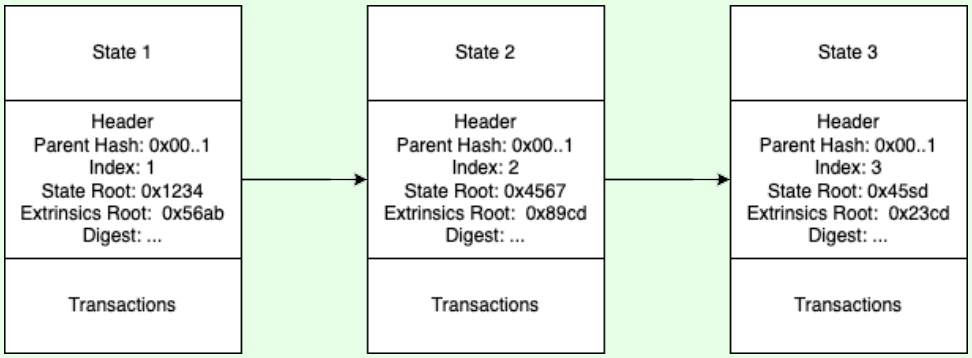

Figure 1: Blockchain Structure

Parent hash: A 32-byte Blake2b[12] hash of the Parity SCALE Codec [11] encoded parent block header.

Index: An integer representing the index of the current block in the chain. It is equal to the number of the ancestor blocks. The genesis state / initial state has number 0.

State root: The root of a Merkle tree, used as storage for the system.

Extrinsics root: A field reserved for the Runtime, a configuration and API service by the Parity Technology FRAME framework, to validate the integrity of the extrinsics composing the block body. The extrinsics_root is set by the runtime and its value is opaque to the Polkadot Host.

Digest: A field used to store any chain-specific data, which could help the light clients interact with the block without the need of accessing the full storage as well as consensus-related data including the block signature.

3.2 Merkle Trees

Merkle trees are a fundamental component of blockchain technology. They allow for efficient and secure verification of data integrity. A Merkle tree is a binary tree where each leaf node represents a hash of a data block, and each non-leaf node represents the hash of its children. The root of the Merkle tree, called the Merkle root, is a compact representation of all the data in the tree.

The benefits of Merkle trees include:

- Efficient data verification: The time complexity for verifying data is $O(\log n)$.
- Data integrity: Any change in the data would result in a different Merkle root, making tampering easily detectable.

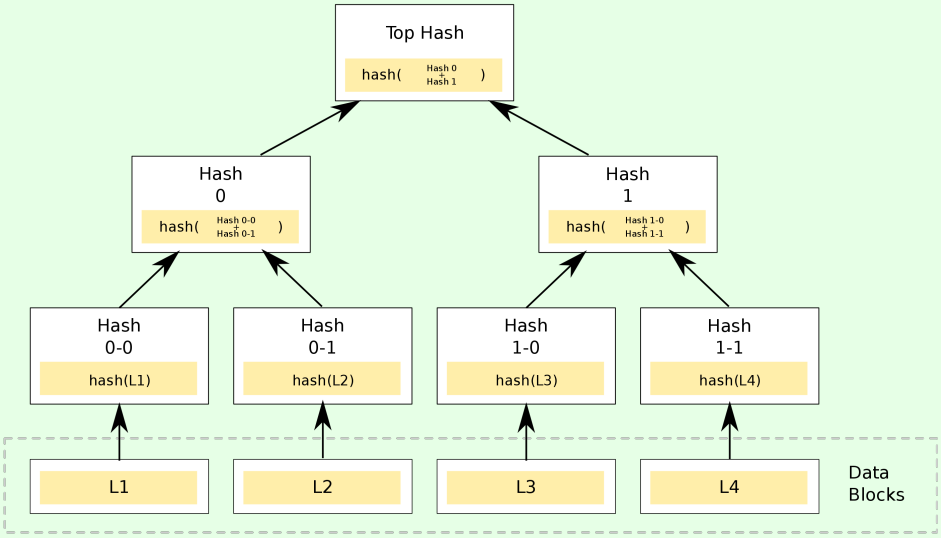

Figure 2: Merkle Tree Structure ([19])

3.3 Patricia Trees and Radix Trees

Patricia trees and radix trees are data structures used to store the state of the blockchain. These trees provide efficient methods for updating and querying the state, making them ideal for handling the dynamic nature of blockchain applications.

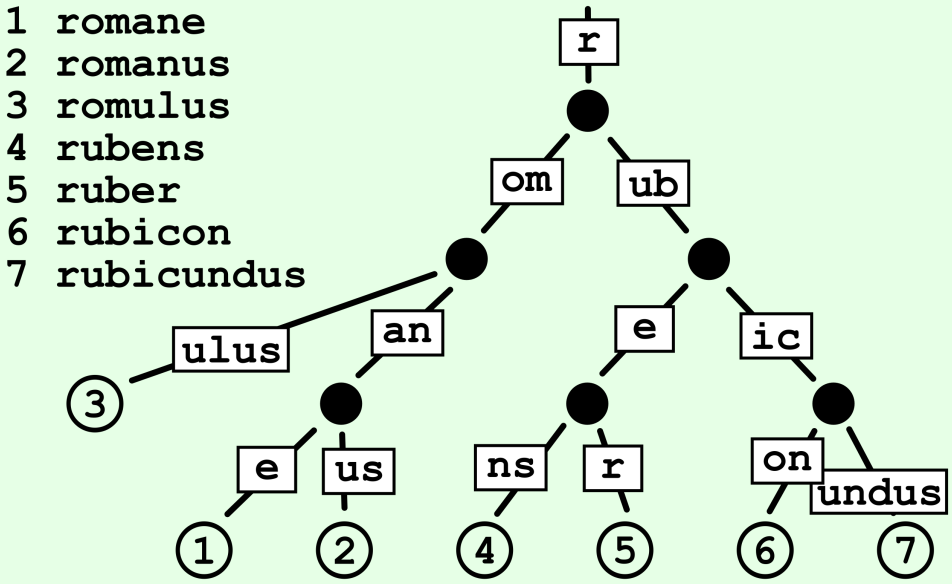

Figure 3: Patricia / Radix Tree Structure [22]

3.4 Cryptography

The end-to-end solution will incorporate three primary cryptography schemes:

- Digital Signatures[15]: Used to sign and verify transactions, ensuring data authenticity and integrity.

- Hashing Algorithms[18]: Employed for address checksum and proof generation, providing data integrity and verification when chaining blocks.
- Encryption [16]: Used to secure data temporarily shared across various entities, ensuring confidentiality and privacy.

There will be a detailed coverage on the chain specifications on another resource. But it would be good to have some coverage on Multi-Party Computation here.

3.5 Multi-Party Computation Cryptography

3.5.1 Overview

Multi-party computation (MPC) [20] is a subfield of cryptography that enables multiple parties to jointly compute a function over their inputs while keeping those inputs private. MPC allows participants to collaboratively compute a result without revealing their individual data to one another. This technique is particularly useful in scenarios where medical professionals can jointly sign a transaction.

3.5.2 MPC Protocols

MPC protocols are designed to ensure the correctness and privacy of the computation. There are several types of MPC protocols, including:

Informally, a multi-party computation (MPC) protocol aims to have two properties:

- **Input privacy:** No information about the private data held by the parties can be inferred from the messages exchanged during the protocol execution. The only information that can be deduced about the private data is what could be inferred from the function's output alone.
- **Correctness:** Any subset of adversarial colluding parties, even if they share information or deviate from the protocol, should not be able to force honest parties to produce an incorrect result. This correctness goal comes in two forms: either the honest parties are guaranteed to compute the correct output (a "robust" protocol), or they abort the computation if they detect an error (an MPC protocol "with abort").
- **Secret Sharing:** Each participant's input is split into multiple shares, which are distributed among the participants. No single participant can deduce the original input from their share alone.
- **Homomorphic Encryption:** A form of encryption that allows computations to be performed on ciphertexts, generating an encrypted result that, when decrypted, matches the result of operations performed on the plaintext.

3.5.3 An Overly Simplified Example: Secure Sum Computation

Consider a scenario where three hospitals want to determine the total number of patients they have treated for a specific condition without revealing their individual patient counts. This problem can be solved using an MPC protocol for secure sum computation.

3.5.4 Step-by-Step Process

1. **Input Sharing:** Each hospital splits its patient count into three shares using a secret sharing scheme. For example, if Hospital A has 50 patients, it generates three random shares a_1, a_2, a_3 such that $a_1 + a_2 + a_3 = 50$. The same process is followed by Hospitals B and C with their patient counts.
2. **Share Distribution:** Each hospital securely distributes its shares to the other hospitals. Hospital A sends a_2 to Hospital B and a_3 to Hospital C, keeping a_1 for itself. Similarly, Hospitals B and C distribute their shares.
3. **Local Computation:** Each hospital computes the sum of the shares it has received, including its own. For example:
    - Hospital A computes $a_1 + b_1 + c_1$

- Hospital B computes $a_2 + b_2 + c_2$
- Hospital C computes $a_3 + b_3 + c_3$

4. **Final Computation:** The hospitals collectively add the results of their local computations to obtain the total sum. Since the shares were constructed such that the sum of each participant's shares equals the original input, the final sum is the total number of patients treated by all hospitals. Specifically:

$$(a_1 + b_1 + c_1) + (a_2 + b_2 + c_2) + (a_3 + b_3 + c_3) = \text{Total Patient Count}$$

3.6 Accounts and Addresses

Accounts are generally tied to an professional identity, they are publicly known. Whilst for any individual they are free to create an address [1], consisting of a public key along with some additional context information.

3.7 Proof of Staked Authority (PoSA)

Proof of Staked Authority (PoSA) [3] is a consensus mechanism that combines elements of Proof of Stake (PoS) and Proof of Authority (PoA) to achieve network consensus. It leverages the benefits of both systems to provide a secure, efficient, and scalable solution for blockchain networks.

3.7.1 Principles of PoSA

The key principles of PoSA include:

- **Stake-Based Selection:** Validators are chosen based on the amount of stake they hold in the network. This aligns their interests with the security and stability of the blockchain.
- **Authority-Based Validation:** Validators must be pre-approved and identified, ensuring accountability and trustworthiness. This reduces the risk of malicious behavior.
- **Hybrid Consensus:** By combining staking and authority, PoSA achieves a balance between decentralization and efficiency. Staking ensures validators have a financial incentive to act honestly, while authority ensures they are accountable for their actions.

3.7.2 Operation of PoSA

- **Validator Selection:** Participants in the network can become validators by staking a significant amount of the network's native token. Validators are periodically selected based on their stake and reputation.
- **Block Production:** Selected validators take turns producing new blocks. Each block producer is responsible for verifying transactions and adding them to the blockchain.
- **Consensus Process:** Validators reach consensus on the validity of transactions and blocks through a combination of staking power and their established authority within the network.
- **Incentives and Penalties:** Validators receive rewards for producing valid blocks and ensuring network security. Conversely, misbehavior such as double-signing or producing invalid blocks results in penalties, including the loss of staked tokens.

3.7.3 Advantages of PoSA

- **Security:** The requirement for validators to stake tokens provides a strong financial disincentive against malicious behavior.
- **Scalability:** PoSA can handle a high transaction throughput due to the efficient block production process.
- **Accountability:** Validators are known entities within the network, which enhances trust and accountability.
- **Energy Efficiency:** Unlike Proof of Work (PoW), PoSA does not require intensive computational resources, making it more environmentally friendly.

3.7.4 Use Cases of PoSA

Proof of Staked Authority is particularly well-suited for blockchain applications that require a high degree of trust and efficiency. These include:

- **Enterprise Blockchain Solutions:** Enterprises can use PoSA to create private or consortium blockchains where validators are known and trusted entities.
- **Supply Chain Management:** PoSA can ensure the integrity and traceability of goods in supply chain networks by leveraging trusted validators.
- **Healthcare Systems:** Secure and efficient sharing of medical records can be facilitated through a PoSA-based blockchain, where validators are authorized healthcare institutions.

3.8 Tech Risk Management Policies in the Medical Industry

3.8.1 United States

Regulatory Framework:

- **Health Insurance Portability and Accountability Act (HIPAA):**
  - Enforces data privacy and security provisions for safeguarding medical information.
  - Requires covered entities to implement physical, administrative, and technical safeguards to ensure data confidentiality, integrity, and availability.
- **Food and Drug Administration (FDA):**
  - Regulates medical devices, including software and digital health technologies, ensuring they meet safety and efficacy standards.
  - Mandates cybersecurity measures for connected medical devices to protect against unauthorized access and data breaches.

Key Policies:

- **Data Encryption:** All electronic protected health information (ePHI) must be encrypted both in transit and at rest.
- **Access Control:** Strict access control mechanisms to ensure only authorized personnel can access sensitive medical data.
- **Incident Response Plan:** Comprehensive incident response plans to quickly identify, contain, and mitigate security breaches.
- **Vendor Management:** Assess and monitor third-party vendors to ensure they comply with HIPAA and other regulatory requirements.

3.8.2 Europe

Regulatory Framework:

- **General Data Protection Regulation (GDPR):**
  - Provides a comprehensive framework for data protection and privacy for all individuals within the European Union (EU).
  - Requires organizations to implement appropriate technical and organizational measures to secure personal data.
- **Medical Device Regulation (MDR):**
  - Sets requirements for the safety and performance of medical devices, including software, ensuring they are safe to use and function as intended.

Key Policies:

- **Data Minimization:** Only collect and process the minimum amount of personal data necessary for the intended purpose.
- **Data Protection Impact Assessment (DPIA):** Conduct DPIAs for high-risk processing activities to identify and mitigate potential risks.
- **Right to Erasure:** Implement procedures to honor individuals' rights to have their personal data erased.
- **Data Breach Notification:** Notify supervisory authorities and affected individuals of data breaches within 72 hours.

3.8.3 Australia

Regulatory Framework:

- **Privacy Act 1988 and the Australian Privacy Principles (APPs):**
  - Governs the handling of personal information, including health information, by Australian government agencies and private sector organizations.
  - Requires organizations to take reasonable steps to protect personal information from misuse, interference, loss, unauthorized access, modification, or disclosure.
- **Therapeutic Goods Administration (TGA):**
  - Regulates medical devices and ensures they meet quality, safety, and performance standards.

Key Policies:

- **Data Security Measures:** Implement robust security measures, such as encryption and secure access controls, to protect health data.
- **Privacy by Design:** Integrate privacy considerations into the design and development of health technologies.
- **Regular Audits:** Conduct regular audits and assessments of security measures and practices.
- **Patient Consent:** Obtain explicit consent from patients before collecting, using, or disclosing their health information.

3.8.4 New Zealand

Regulatory Framework:

- **Privacy Act 2020:**
  - Provides comprehensive data protection and privacy rules for handling personal information.
  - Emphasizes the need for data security, transparency, and accountability in processing personal information.
- **Health Information Privacy Code 2020 (HIPC):**
  - Specifically addresses the privacy of health information and imposes additional obligations on health agencies.

Key Policies:

- **Secure Storage:** Ensure health information is stored securely, both electronically and physically.
- **Access Rights:** Patients have the right to access their health information and request corrections.
- **Data Breach Protocols:** Develop and implement protocols for responding to data breaches, including notifying affected individuals and authorities.
- **Information Sharing:** Establish clear guidelines and safeguards for sharing health information with other entities.

3.8.5 Singapore

Regulatory Framework:

- **Personal Data Protection Act (PDPA):**
  - Regulates the collection, use, disclosure, and care of personal data, including health information, in Singapore.
  - Requires organizations to implement reasonable security arrangements to protect personal data.
- **Ministry of Health (MOH) Guidelines:**
  - Provides specific guidelines and standards for the management and protection of health information.

Key Policies:

- **Data Protection Officer (DPO):** Appoint a DPO to ensure compliance with PDPA and other relevant regulations.
- **Security Measures:** Implement strong security measures, such as encryption and multi-factor authentication, to safeguard health data.
- **Data Retention:** Establish data retention policies to ensure health information is retained only for as long as necessary.
- **Training and Awareness:** Conduct regular training programs for employees on data protection and cybersecurity best practices.
- **HIPAA Compliance:** For organizations dealing with US patients, ensure compliance with HIPAA requirements.

3.8.6 China

Regulatory Framework:

- **Cybersecurity Law:**
  - Imposes stringent requirements on the protection of personal data and critical information infrastructure.
  - Requires network operators to implement security measures to safeguard personal data.
- **Personal Information Protection Law (PIPL):**
  - Provides comprehensive data protection and privacy rules for handling personal information.
  - Emphasizes data minimization, informed consent, and data security.

Key Policies:

- **Data Localization:** Store health data within China unless specific conditions for cross-border transfer are met.
- **Consent Mechanisms:** Obtain explicit consent from patients before collecting and processing their health information.
- **Security Assessments:** Conduct regular security assessments and audits to ensure compliance with cybersecurity and data protection laws.
- **Incident Reporting:** Develop protocols for reporting data breaches and cybersecurity incidents to regulatory authorities.

3.8.7 Dubai

Regulatory Framework:

- **Dubai Healthcare City (DHCC) Regulations:**
  - Provides specific guidelines and standards for the management and protection of health information within the DHCC.
  - Emphasizes the importance of data security, patient confidentiality, and information governance.
- **Dubai Data Law:**
  - Regulates the collection, use, and sharing of data, including health data, within Dubai.

Key Policies:

- **Data Encryption:** Implement encryption for health data both in transit and at rest.
- **Access Controls:** Ensure that access to health data is restricted to authorized personnel only.
- **Data Sharing Agreements:** Establish clear data sharing agreements and protocols when sharing health information with third parties.
- **Patient Rights:** Protect patient rights to access, correct, and control their health information.

3.8.8 India

Regulatory Framework:

- **Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011:**
  - Imposes obligations on businesses to implement reasonable security practices to protect sensitive personal data, including health information.
  - Requires businesses to obtain consent from individuals before collecting and processing sensitive personal data.
- **Personal Data Protection Bill (PDPB):**
  - Provides a comprehensive framework for data protection and privacy in India.
  - Emphasizes data localization, transparency, and accountability in handling personal data.

Key Policies:

- **Data Security:** Implement strong security measures, such as encryption and secure access controls, to protect health data.
- **Consent Mechanisms:** Obtain explicit consent from patients before collecting and processing their health information.
- **Data Breach Protocols:** Develop and implement protocols for responding to data breaches, including notifying affected individuals and authorities.
- **Data Retention:** Establish data retention policies to ensure health information is retained only for as long as necessary.
- **Data Localization:** Store health data within India unless specific conditions for cross-border transfer are met.

A side note that the purpose of the technical risk management of various countries in this section are to understand what are the regulated areas. Here, We'd like to emphasize that ROAX does not disrupt the current healthcare system. In fact, there is business continuity for existing healthcare system. ROAX will be an attached enhancement.

4 System Architecture Overview

4.1 Overview

The diagram illustrates an abstract end-to-end information process within the ROAX platform. ROAX leverages a decentralized network where various validators collaborate to secure the network. This collaborative effort ensures the integrity, security, and availability of medical data across the platform.

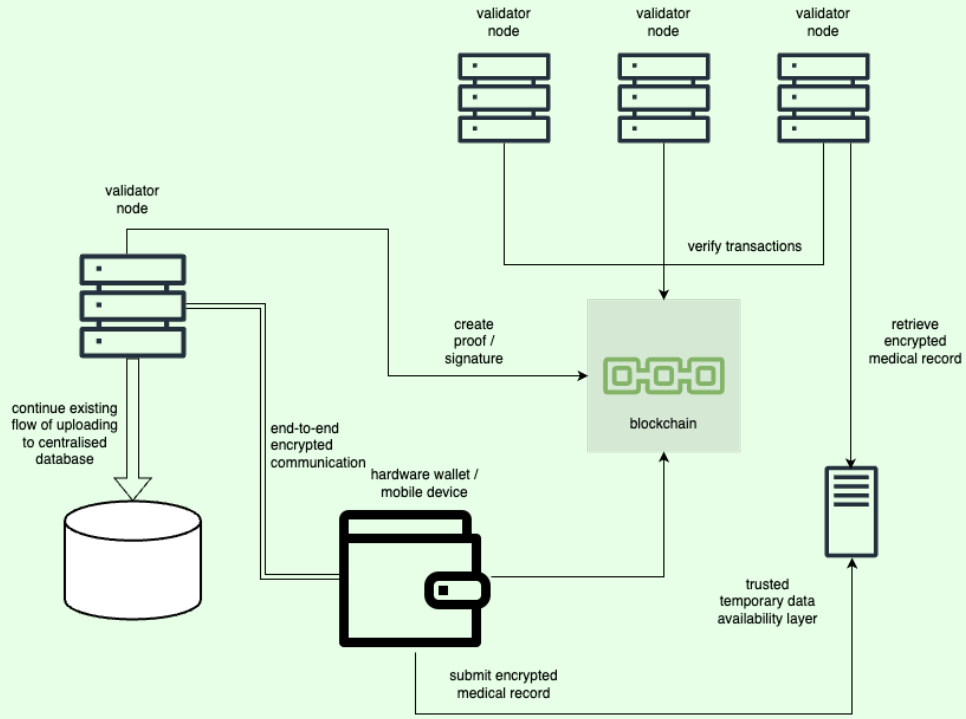

Figure 4: ROAX System Architecture

4.2 Medical Professionals (Validators)

Medical Professionals (Validators)[10] are crucial components of the ROAX network. They perform various functions to maintain the network's security and operational efficiency. Validators participate in consensus mechanisms to validate transactions and maintain the blockchain's integrity. These entities can be medical institutions, healthcare providers, or independent organizations with the required computational resources and credibility.

4.3 Trusted Data Availability Service

In ROAX, trusted data availability[6] refers to the ability of authorized entities to securely access and share medical data. While any participant can act as a trusted data provider, specific entities are typically assigned this role based on trust and reliability criteria. These entities ensure that the data is available when needed, facilitating seamless information flow across the network.

4.4 Patient Interaction

Patients play a vital role in the ROAX ecosystem. They own their medical data and have control over its access and distribution. Entities, such as healthcare providers or medical professionals, can connect to the patient's hardware security module (HSM) or hard wallet to request and make data transfers. This interaction is secure and ensures that the patient's data is only accessible to authorized parties.

4.5 Cryptographic Schemes

The ROAX platform employs various cryptographic schemes to secure interactions and data transfers. Different relationships and interactions within the network may require different cryptographic techniques. For instance:

- **Encryption:** Used to protect data during transmission, ensuring that only authorized recipients can decrypt and access the information.
- **Digital Signatures:** Ensure the authenticity and integrity of the data, allowing recipients to verify that the data has not been tampered with and originates from a trusted source.
- **Hashing:** Used in address checksums and proof generation to verify data integrity and create secure, immutable records.

4.6 Hardware Security Modules (HSM) for Mobile

4.6.1 Introduction

Hardware Security Modules (HSMs) are dedicated devices designed to provide secure key management and cryptographic processing. When applied to mobile devices, HSMs enhance security by protecting sensitive data, cryptographic keys, and operations from various threats.

4.6.2 Security Mechanisms

- **Secure Enclave Technology:** Mobile devices often incorporate a secure enclave or trusted execution environment (TEE) as an HSM. These are isolated processors within the main processor, ensuring secure execution of sensitive tasks. Example: Apple's Secure Enclave and Google's Titan M chip
- **Key Management:** HSMs securely generate, store, and manage cryptographic keys. Keys are generated within the secure enclave and never leave the protected environment. Hardware-backed key storage prevents extraction even if the main OS is compromised.
- **Cryptographic Operations:** HSMs perform cryptographic operations such as encryption, decryption, digital signing, and verification within the secure environment, ensuring that sensitive data and keys are not exposed to the main operating system.
- **Tamper Resistance:** HSMs in mobile devices are designed to resist physical and logical tampering. They include mechanisms to detect and respond to attempts to breach security, such as erasing keys upon detection of tampering.
- **Secure Boot:** HSMs ensure that the mobile device boots securely by verifying the integrity of the operating system and other critical components before they are loaded. This prevents unauthorized modifications and malware infections.
- **Biometric Security:** Integration with biometric authentication methods (e.g., fingerprint, face recognition) enhances security by ensuring that only the authorized user can access sensitive operations and data.

4.6.3 Existing Applications

- **Secure Mobile Payments:** HSMs are integral to secure mobile payment systems such as Apple Pay and Google Wallet. They store sensitive payment information and cryptographic keys securely, ensuring that payment data cannot be intercepted or tampered with. HSMs generate one-time-use tokens for each transaction, enhancing security by ensuring that the actual payment data is never exposed.
- **Secure Communication:** Encrypted messaging apps like WhatsApp and Signal use HSMs to protect encryption keys and user credentials. HSMs ensure that the keys used for end-to-end encryption are securely generated, stored, and managed, preventing unauthorized access and ensuring the confidentiality of messages.

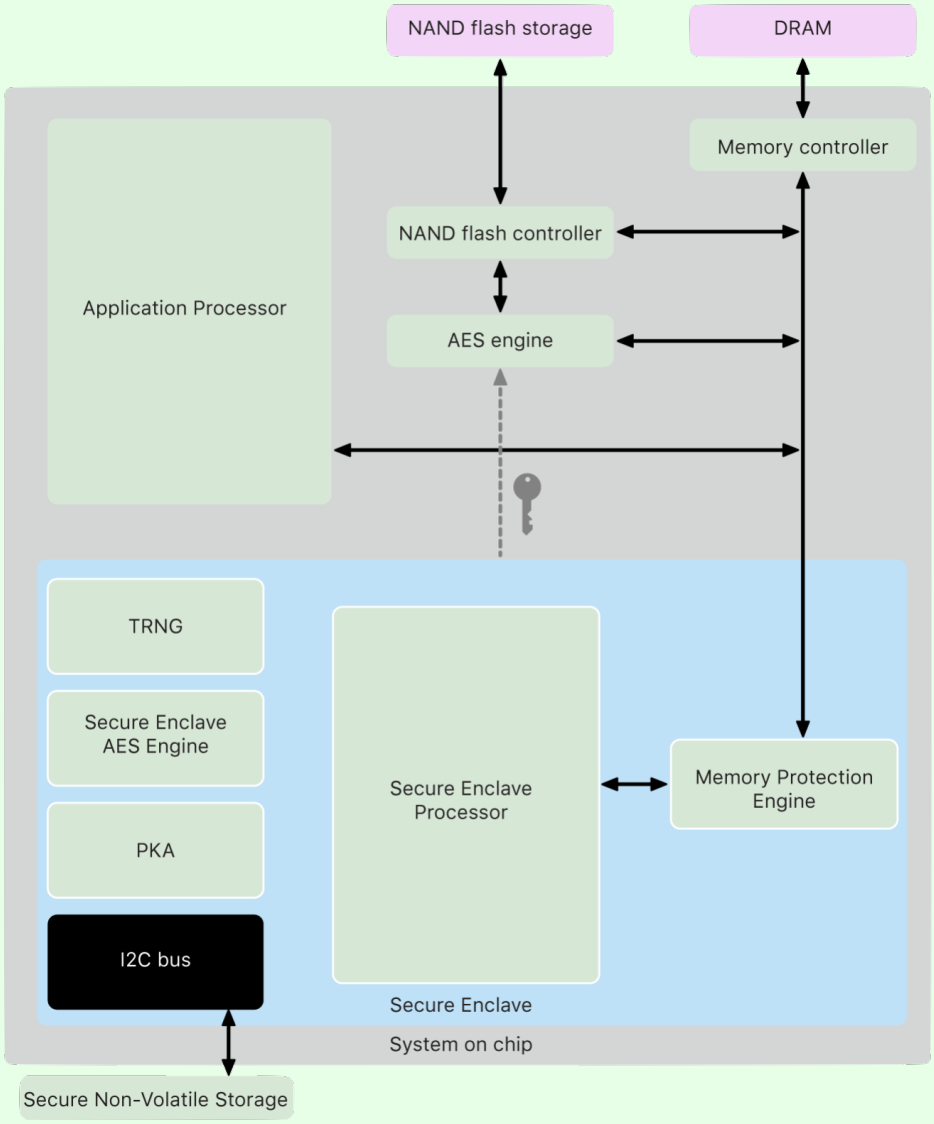

Figure 5: Secure Enclave Technology [2]

- **Mobile Banking and Financial Services:** HSMs are used in mobile banking applications to secure transactions, authenticate users, and protect sensitive financial data. They manage cryptographic keys and perform secure operations such as digital signatures and encryption, ensuring that user data and transactions are secure from fraud and unauthorized access.
- **Secure Access to Corporate Resources:** HSMs enable secure access to corporate resources by managing authentication keys and certificates. They support multi-factor authentication (MFA) solutions, ensuring that only authorized users can access sensitive corporate data and applications. This is crucial for protecting against unauthorized access and ensuring data security in corporate environments.

4.7 Hardware Wallets Integrations(e.g., Ledger)

4.7.1 Introduction

Hardware wallets [9] are specialized devices designed to securely store cryptocurrency private keys and facilitate secure transactions. Ledger is a popular example of such hardware wallets. For any hardware wallets to integrate with ROAX it will require additional features and mechanisms to securely save the patient's medical record. (References: https://www.ledger.com/academy/basic-basics/ledgers-ecosystem/why-is-ledger-nano-so-secure)

4.7.2 Security Mechanisms

- **Secure Element:** Ledger devices incorporate a secure element, a dedicated chip designed to protect cryptographic secrets. It provides a high level of security by isolating private keys from the main device firmware. The secure element is certified to meet stringent security standards (e.g., Common Criteria, EAL5+).
- **Offline Storage:** Private keys are stored offline within the secure element, preventing exposure to online threats such as malware and hackers. Transactions are signed within the device, and only the signed transaction is broadcasted to the network.
- **Pin Protection:** Access to the hardware wallet is protected by a PIN code. Multiple incorrect attempts to enter the PIN can trigger a security mechanism that wipes the device.
- **Firmware Integrity:** Ledger devices employ secure boot mechanisms to ensure that only authenticated firmware can run on the device. Firmware updates are cryptographically signed by the manufacturer, preventing unauthorized modifications.
- **Physical Security:** Ledger wallets are designed to be tamper-evident and tamper-resistant. Any physical attempt to breach the device triggers protective measures, such as erasing sensitive data.
- **Recovery Seed:** In case the hardware wallet is lost or damaged, a recovery seed (a set of words) is provided during setup. This seed allows the user to recover their private keys and access their funds on a new device.

4.7.3 Existing Applications

- **Secure Storage and Management of Cryptocurrency:** Hard wallets provide a secure environment for storing private keys that are used to access and manage cryptocurrency holdings. Unlike software wallets, hard wallets keep these keys offline, significantly reducing the risk of them being compromised by malware or hackers. Examples include devices like Ledger and Trezor, which use secure hardware components to safeguard keys.
- **Signing Cryptocurrency Transactions:** Hard wallets are used to securely sign cryptocurrency transactions. When a user initiates a transaction, the transaction details are sent to the hard wallet, which then signs the transaction with the private key stored in the device. This ensures that the private key never leaves the hard wallet, providing a secure way to authorize transactions without exposing the key to potential threats.
- **Authentication for Cryptocurrency Exchanges and Services:** Hard wallets can be used as a second factor for authentication when accessing cryptocurrency exchanges and other related services. By integrating with exchange platforms, users can authenticate their identity by confirming access through their hard wallet, adding an additional layer of security to prevent unauthorized access to their accounts.

4.7.4 Comparison of HSM for Mobile and Hardware Wallets

4.8 Encryption and Data Privacy (Zero Knowledge Protocol)

Advance features of privacy preserving data collection can be unlock through a particular group of cryptography implementations, known as Zero-Knowledge Protocols [27]. These are possible techniques that could be managed by the protocol to allow easy integration of insurance DApps. One example of such a technique is the Schnorr Idenfication Scheme.

4.8.1 Schnorr Cryptographic Idenfication Scheme

The Schnorr Identification Scheme[8], developed by Claus-Peter Schnorr, is a cryptographic protocol, where there's a group G of order q in which the discrete logarithm problem holds for the generator g. The scheme establishes a secure interactive process between two parties — a Prover and a Verifier. The Schnorr Identification Scheme is designed to enable the Prover to demonstrate knowledge of a secret value x without revealing it. The Verifier, on the other hand, is aware of g^x, which is a public value derived from x:

Feature	HSM for Mobile Devices	Hardware Wallets (e.g., Ledger)
Primary Use	Secure key management and cryptographic operations on mobile devices	Secure storage and transaction of cryptocurrency
Secure Element	Integrated within mobile processors (e.g., Secure Enclave, Titan M)	Dedicated secure element chip
Key Storage	Hardware-backed, within the secure enclave	Offline, within the secure element
Cryptographic Operations	Performed within the secure enclave	Performed within the secure element
Tamper Resistance	Yes, with tamper detection and response	Yes, with tamper-evident and tamper-resistant design
PIN Protection	Integrated with device PIN and biometric authentication	Device PIN protection with data wipe on multiple failed attempts
Firmware Security	Secure boot and authenticated updates	Secure boot and authenticated firmware updates
Data Recovery	Integrated with mobile device's backup mechanisms	Recovery seed for private key recovery
Primary Applications	Secure mobile payments, communication, banking	Cryptocurrency storage and transactions

Table 1: Comparison of HSM for Mobile and Hardware Wallets

- Both the Prover and the Verifier operate through polynomial-time algorithms.
- The Prover knows some x that is randomly chosen from q, while the Verifier knows g^x.
- The Prover wants to prove to the Verifier that it knows x.

Prover (x)	**Verifier** (g^x)
$k \leftarrow [q]$	
$\xrightarrow{g^k}$	
	$r \leftarrow [q]$
	$\xleftarrow{r}$
$s \leftarrow r \cdot x + k \mod q$	
$\xrightarrow{s}$	
	Check $g^s \cdot (g^x)^{-r} = g^k$

Table 2: The Schnorr Identification Scheme

$g^s.(g^x)^{-r} = g^{r.x+k}.g^{-rk} = g^k \implies$ Prover Knows x, Verifier accepts

Claim

The Schnorr Identification Scheme is secure. And if the Prover does know x, this will always be correct.

Proof

Suppose the Prover does not know x, but somehow makes the Verifier accept. This implies that for a random r_1, r_2, the Prover can find s_1, s_2 such that:

$$g^{s_1} \cdot (g^x)^{-r_1} = g^k = g^{s_2} \cdot (g^x)^{-r_2}$$

This implies:

$$x = (s_1 - s_2) \cdot (r_1 - r_2)^{-1} \mod q$$

And we can use such a Prover to solve the Discrete Log Problem, which is a contradiction and thus such a Prover cannot exist.

4.9 Public Key Encryption

You might have heard of the Ralph Merkle Secure Communications over insecure channels [Mer78] or the Diffie Hellman Key Exchange for establishing a shared secret. However, in the real world, it may not be feasible for every sender and receiver pair to establish a shared private key before communication. In particular, for our case when a patient wants to share data across different entities. Under a public key encryption scheme, anyone may encrypt messages using a publicly available key, but only those with the corresponding hidden secret key may decrypt the resultant ciphertexts. One such example is the ElGamal encryption Scheme.

4.9.1 ELGamal Encryption

ElGamal encryption[7] is a public-key cryptosystem that is widely recognized for its strong security properties and versatility. Developed by Taher Elgamal in 1985, it represents a significant advancement in the field of cryptography, offering an alternative to the RSA cryptosystem. The ElGamal encryption scheme comprises three fundamental components (KeyGen, Enc, Dec).

Key Generation

$$\text{KeyGen}(\lambda):$$
$$(G, g) \leftarrow \text{GroupGen}(\lambda)$$
$$a \leftarrow \mathbb{Z}_{|G|}$$
$$pk = (G, g, g^a), \quad sk = a$$

Output (pk, sk)

Encryption

$$\text{Enc}(\lambda, pk, m):$$
$$b \leftarrow \mathbb{Z}_{|G|}$$

Output $(g^b, (g^a)^b \cdot m)$

Decryption

$$\text{Dec}(\lambda, sk, c):$$

Output $((g^b)^{sk})^{-1} \cdot (g^a)^b \cdot m$ or $((g^b)^a)^{-1} \cdot (g^a)^b \cdot m)$

EGE-DDH-IND-CPA(λ) Security Game

Challenger	**Adversary**
$(pk, sk) \leftarrow \text{KeyGen}(\lambda)$	
$b \leftarrow \{0, 1\}$	
$\xrightarrow{pk}$	
	m_0, m_1
	$\xleftarrow{m_0, m_1}$
$c \leftarrow \text{Enc}(pk, m_b)$	
$\xrightarrow{c}$	
Output b'	
Wins if $b' = b$	

Table 3: EGE-DDH-IND-CPA(λ) Security Game

Public Key Encryption Scheme is CPA-Secure

$$\forall \text{ PPT } A \; \exists \text{ negl. } \nu : \Pr[A \text{ wins EGE-DDH-IND-CPA}(\lambda)] < \frac{1}{2} + \nu(\lambda)$$

5 Transactions and State Transition

Transactions in ROAX contain the following fields:

- Recipient
- Signature
- Amount of ROAX tokens
- Optional data field
- Optional medical record field
- STARTWEIGHT and WEIGHTPRICE values

The state transition function $APPLY(S, TX) -> S'$ involves checking transaction validity, calculating fees, and updating account balances.

5.1 ROAX State Transition Function

The ROAX state transition function, $APPLY(S, TX) -> S'$, can be defined as follows:

1. Check if the transaction is well-formed (i.e., has the right number of values), the signature is valid, and the nonce matches the nonce in the sender's account. If not, return an error.
2. Calculate the transaction fee as STARTWEIGHT * WEIGHTPRICE, and determine the sending address from the signature. Subtract the fee from the sender's account balance and increment the sender's nonce. If there is not enough balance to spend, return an error.
3. Initialize WEIGHT = STARTWEIGHT, and take off a certain quantity of gas per byte to pay for the bytes in the transaction.
4. Transfer the transaction value from the sender's account to the receiving account. If the receiving account does not yet exist, create it. If the receiving account is a contract, run the contract's code either to completion or until the execution runs out of gas.
5. If the value transfer failed because the sender did not have enough money, or the code execution ran out of gas, revert all state changes except the payment of the fees, and add the fees to the miner's account.
6. Otherwise, refund the fees for all remaining gas to the sender, and send the fees paid for gas consumed to the miner.

6 Smart Contracts

ROAX supports smart contracts[25] with additional functionalities tailored for medical purposes, enabling the development of various decentralized medical (DeMed) applications on the platform. These smart contracts facilitate automated, secure, and transparent interactions between different entities within the healthcare ecosystem.

6.1 How Smart Contracts Work

Smart contracts on ROAX can be self-executing contracts with the terms of the agreement directly written into code. These contracts run on the blockchain and are triggered by specific conditions, ensuring that the contract terms are automatically enforced without the need for intermediaries.

6.1.1 Deployment and Execution

Smart contracts are deployed on the ROAX blockchain by submitting a transaction containing the contract's code. Once deployed, each contract is assigned a unique address and becomes immutable. Users interact with smart contracts by sending transactions to these addresses, triggering the contract's functions.

6.1.2 Virtual Machine

The execution of smart contracts is handled by a virtual machine (VM) integrated into the ROAX blockchain. This VM interprets and executes the contract code, ensuring that all computations are deterministic and verifiable by all network participants. The VM's design ensures compatibility with existing smart contract languages, allowing developers to leverage familiar tools and frameworks.

6.1.3 Gas and Fees

To prevent abuse and ensure fair resource usage, executing smart contracts requires paying gas fees. Gas is a unit that measures the amount of computational work required to execute a contract function. Users specify the gas limit they are willing to pay for each transaction, and if the execution exceeds this limit, the transaction fails, ensuring that only well-defined operations are processed.

6.1.4 Interoperability and Extensions

ROAX's smart contracts are designed with interoperability in mind, allowing seamless integration with various healthcare systems and applications. This is achieved through standardized interfaces and protocols that enable different contracts and services to communicate and interact securely. Additionally, ROAX provides specialized libraries and extensions for medical applications, facilitating the development of DeMed services such as patient data sharing, insurance claims processing, and clinical trial management.

6.2 Medical and Insurance DApps [14]

Smart contracts on ROAX offer functionalities specifically designed for the healthcare industry, including:

- **Patient Data Sharing:** Secure and controlled sharing of medical records between patients, healthcare providers, and other authorized entities.
- **Insurance Claims Processing:** Automated verification and processing of insurance claims, reducing administrative overhead and fraud.
- **Clinical Trials Management:** Transparent and efficient management of clinical trial data, ensuring data integrity and compliance with regulatory requirements.
- **Supply Chain Management:** Tracking and verification of medical supplies and pharmaceuticals to ensure authenticity and traceability.
- **Pandemic Detection:** Allowing organizations to contribute sufficient verifiable data seamlessly within the network.
- **Medical Data Marketplace:** Enabling the buying and selling of medical data through decentralized applications (DApps).
- **Blood Banks Management:** Facilitating the management and distribution of blood donations using DApps.
- **Organ Auction Platforms:** Providing a secure platform for organ donation and transplantation.

7 Economic Model

The ROAX economic model is designed to ensure a sustainable and incentivized ecosystem for medical data storage and sharing. This model draws inspiration from existing blockchain networks while introducing unique features tailored to the healthcare and insurance sector.

7.1 Tokenomics [26]

ROAX utilizes its native utility token, ROAX, which serves multiple purposes within the ecosystem, including transaction fees, staking, and incentivizing participants.

7.1.1 Token Supply and Inflation

- **Initial Supply:** The initial supply of ROAX tokens is set at 1 billion tokens.
- **Inflation Rate:** To ensure long-term sustainability and incentivize network participation, ROAX will have a controlled inflation rate of 3% per annum. This lower inflation rate is designed to balance token supply growth with the demand driven by network usage.

7.1.2 Token Distribution

- **Founding Team and Development:** 20% of the initial supply is allocated to the founding team and development efforts. These tokens will be vested over a 4-year period to align incentives.
- **Ecosystem Fund:** 15% of the initial supply is reserved for an ecosystem fund to support the development of applications and integrations on the ROAX platform.
- **Staking and Rewards:** 40% of the initial supply is allocated for staking rewards to incentivize validators and participants who contribute to network security.
- **Public Sale:** We are considering 25% of the initial supply will be made available through a public token sale to distribute tokens to a wide range of participants and bootstrap network adoption.

7.2 Staking and Validation

ROAX adopts a Proof of Stake (PoS) consensus mechanism, where validators are required to stake ROAX tokens to participate in the network's transaction validation process.

7.2.1 Validator Incentives

- **Staking Rewards:** Validators earn rewards in the form of newly minted ROAX tokens and transaction fees for their efforts in securing the network.
- **Slashing Penalties:** To ensure the integrity of the network, validators who act maliciously or fail to maintain required uptime will face slashing penalties, resulting in the loss of a portion of their staked tokens.

7.2.2 Delegated Staking

- **Delegation:** Token holders who do not wish to run a validator node can delegate their ROAX tokens to trusted validators. In return, delegators receive a portion of the staking rewards earned by the validators.
- **Incentive Alignment:** This model aligns the incentives of validators and delegators, promoting active participation and network security.

7.3 Transaction Fees

To facilitate sustainable network operations, ROAX implements a fee structure for various network activities.

7.3.1 Fee Structure

- **Data Creation Fees:** A small fee is charged for creating new medical records on the blockchain. This fee compensates validators and deters spam transactions.
- **Data Retrieval Fees:** Users retrieving medical data from the blockchain pay a nominal fee to cover network resources and ensure efficient data access.

- **Smart Contract Execution Fees:** Deploying and executing smart contracts incurs fees proportional to the computational resources required, ensuring fair resource allocation and network sustainability.

7.4 Incentives for Healthcare Providers

- **Participation Rewards:** Healthcare providers earn ROAX tokens as rewards for contributing medical data, participating in clinical trials, and other beneficial activities.
- **Reduced Costs:** By using ROAX for data transactions, healthcare providers benefit from reduced administrative costs and streamlined operations compared to traditional systems.

7.5 Governance

ROAX adopts a decentralized governance model to ensure that the platform evolves according to the community's needs and priorities.

7.5.1 Governance Tokens

- **Voting Power:** ROAX token holders possess voting power proportional to their token holdings, enabling them to participate in governance decisions. At the initial stages only the curated set medical professionals whom are token holders should vote.
- **Proposals and Voting:** Any individual, whom are token holders can submit proposals for network upgrades, parameter changes, and other governance matters. Proposals are voted on by the medical community, with decisions implemented based on majority consensus.

7.6 Sustainability and Growth

The ROAX economic model is designed to support sustainable growth and long-term value creation for all participants in the ecosystem.

- **Ecosystem Development:** Continuous investment in the ecosystem fund supports the development of new applications, integrations, and partnerships, driving network adoption and utility.
- **Community Engagement:** Active engagement with the ROAX community ensures that the platform remains responsive to the needs and feedback of its users, fostering a vibrant and collaborative ecosystem.

8 Conclusion

ROAX represents an advancement in the healthcare industry by addressing critical issues related to data security, integrity, and stakeholder incentives. By leveraging the power of blockchain technology, ROAX offers a decentralized, immutable, and universally interoperable platform for medical records.

The implementation of ROAX ensures that medical data is stored securely, with the ownership of data firmly in the hands of the patients. This decentralized approach mitigates the risks associated with centralized data storage, such as hacking and unauthorized alterations, thereby enhancing the overall security and credibility of medical records.

Furthermore, ROAX introduces an innovative economic model that incentivizes doctors and medical professionals to participate actively in the ecosystem. Through staking and rewards, ROAX fosters a cooperative environment where medical professionals can contribute to and benefit from a universally interoperable healthcare system. This model not only encourages participation but also ensures the sustainability and growth of the platform.

The integration of smart contracts adds another layer of functionality, enabling the development of various decentralized medical applications (DeMed) on the ROAX platform. These applications can streamline processes such as insurance claims, clinical trials, and supply chain management, ultimately leading to a more efficient and transparent healthcare system.

In conclusion, ROAX is poised to revolutionize the healthcare industry by providing a secure, interoperable, and incentivized platform for medical records. By addressing the key challenges of data security, integrity, and stakeholder engagement, ROAX has the potential to create a more efficient, transparent,

and patient-centric healthcare ecosystem. The comprehensive technical architecture, innovative economic model, and broad range of applications outlined in this document underscore the transformative impact that ROAX can have on the future of healthcare.

References

[1] Wallet-address. https://www.coinbase.com/en-sg/learn/wallet/what-is-a-wallet-address.

[2] Apple. Apple-secure-enclave. https://support.apple.com/en-sg/guide/security/sec59b0b31ff/web.

[3] Binance. Posa. https://academy.binance.com/en/glossary/proof-of-staked-authority-posa.

[4] Binance. Layer-1-blockchain, 2022. https://academy.binance.com/en/articles/what-is-layer-1-in-blockchain.

[5] CNA. Doctor fradulent data submission. https://www.channelnewsasia.com/singapore/hiv-leak-singapore-doctor-struck-off-ler-teck-siang-brochez-584626.

[6] CoinMarketCap. Data-availability, 2022. https://coinmarketcap.com/academy/article/what-is-data-availability.

[7] GeeksForGeeks. Elgamal-encryption. https://www.geeksforgeeks.org/elgamal-encryption-algorithm/.

[8] GeeksForGeeks. Schnorr-idenfication-scheme. https://www.geeksforgeeks.org/schnorr-identification-scheme/.

[9] Ledger. Hardware-wallets, 2023. https://www.ledger.com/academy/crypto-hardware-wallet.

[10] Ledger. Validator, 2023. https://www.ledger.com/academy/what-is-a-blockchain-validator.

[11] Pairty. Scale-codec. https://docs.rs/parity-codec/latest/parity_codec/.

[12] rfc. Blake2. https://www.rfc-editor.org/rfc/rfc7693.html.

[13] Wiki. Bitcoin. https://en.wikipedia.org/wiki/Bitcoin.

[14] Wiki. Dapps. https://en.wikipedia.org/wiki/Decentralized_application.

[15] Wiki. Digital-signatures. https://en.wikipedia.org/wiki/Digital_signature.

[16] Wiki. Encryption. https://en.wikipedia.org/wiki/Encryption.

[17] Wiki. Ethereum. https://en.wikipedia.org/wiki/Ethereum.

[18] Wiki. Hashing-function. https://en.wikipedia.org/wiki/Hash_function.

[19] Wiki. Merkle-tree. https://en.wikipedia.org/wiki/Merkle_tree.

[20] Wiki. Multi-party-computation. https://en.wikipedia.org/wiki/Securemulti-partycomputation.

[21] Wiki. Polkadot. https://wiki.polkadot.network/.

[22] Wiki. Radix-tree. https://en.wikipedia.org/wiki/Radix_tree.

[23] Wiki. Ransomeware. https://en.wikipedia.org/wiki/Ransomware.

[24] Wiki. Singhealth data breach. https://en.wikipedia.org/wiki/2018_SingHealth_data_breach.

[25] Wiki. Smart-contract. https://en.wikipedia.org/wiki/Smart_contract.

[26] Wiki. Tokenomics. https://en.wikipedia.org/wiki/Tokenomics.

[27] Wiki. Zero-knowledge-proof. https://en.wikipedia.org/wiki/Zero-knowledge_proof.