UCLID Hub : Sensitive Information Management on Global Scalable Blockchain with on-chain Governance

UCLID Hub Labs

Abstract

As the cost of genetic testing declines and AI adoption increases, genetic information is becoming crucial in digital healthcare. However, managing this sensitive data securely is a significant challenge. UCLID Hub addresses this by leveraging blockchain technology to prioritize individual data sovereignty. It ensures that only individuals can access and control their genetic data, providing a secure and private solution.

This white paper outlines UCLID Hub's governance framework that enhances security through proposing, voting on, and executing updates. The governance process involves the Labs Wallet, Governance Module, Validator Wallets, and Nodes, ensuring robust system security and efficient updates.

To improve user accessibility, UCLID Hub incorporates a gas fee control module, allowing Fee Granters to provide gas fees to Fee Grantees, ensuring users can send transactions without incurring gas costs directly.

In managing genomic information securely, UCLID Hub uses blockchain technology and asymmetric encryption to protect sensitive genetic data. This ensures that only authorized individuals can access and control their genomic information.

For sharing genomic analysis results with third parties, UCLID Hub maintains data confidentiality and integrity through secure processes, giving users control over their information.

UCLID Hub also enhances interoperability through multi-chain communication and native tokens via the IBC protocol, facilitating seamless interactions between the UCLID Hub and regional chains.

Finally, UCLID Hub ensures the isolation of regional data and the sharing of global data, adhering to regional legal requirements and enabling global collaboration.

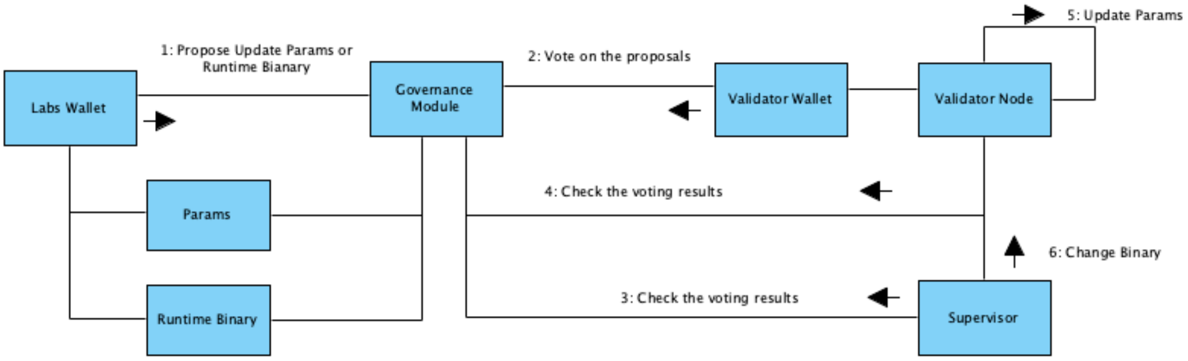
Our goal is to realize "a world where people can live healthier and more prosperous lives." UCLID Hub aims to redefine the future of healthcare through technological innovation, creating a world where everyone can safely utilize their genetic information.

Contents

1. Introduction

With the decline in the cost of genetic testing and the adoption of AI, genetic information is expected to play a crucial role in future digital healthcare. However, genetic information is highly sensitive data, and managing and utilizing it securely is one of the key challenges of the genomic era. To address this issue, UCLID Hub was created.

2. Enhanced security through governance-based deployment and operation



In the evolving landscape of blockchain technology, ensuring robust system security and efficient implementation of updates are paramount. This document outlines a structured governance framework that enhances security through a systematic process of proposing, voting on, and executing updates within our blockchain ecosystem.

Proposal Phase

Labs Wallet:

- The governance process is initiated by the **Labs Wallet**, which is tasked with proposing updates. These updates can include parameter changes or modifications to the runtime binary. Once formulated, the proposal is submitted to the **Governance Module** for evaluation.

Governance Phase

Governance Module:

- The **Governance Module** is central to managing the proposal lifecycle. It disseminates received proposals to network participants for voting, thereby involving multiple stakeholders in the decision-making process. This decentralized approach enhances the system's security by ensuring broad-based consensus.

Validator Wallets:

- Validator Wallets play a critical role in this phase. They participate in voting on proposals, helping to establish the necessary consensus for any update. This collective decision-making process adds an additional layer of security and integrity to the system.

<u>Verification Phase</u>

Check Voting Results:

- Following the voting process, both the **Supervisor** and **Validator Wallets** are responsible for verifying the outcomes. This step ensures transparency and accuracy, which are essential for maintaining trust in the governance mechanism.

Validator Node:

- The **Validator Node** independently verifies the voting results to confirm the consensus. Once validated, the node proceeds with the necessary actions as dictated by the voting outcome. This independent verification further fortifies the security of the system.

<u>Execution Phase</u>

Update Parameters:

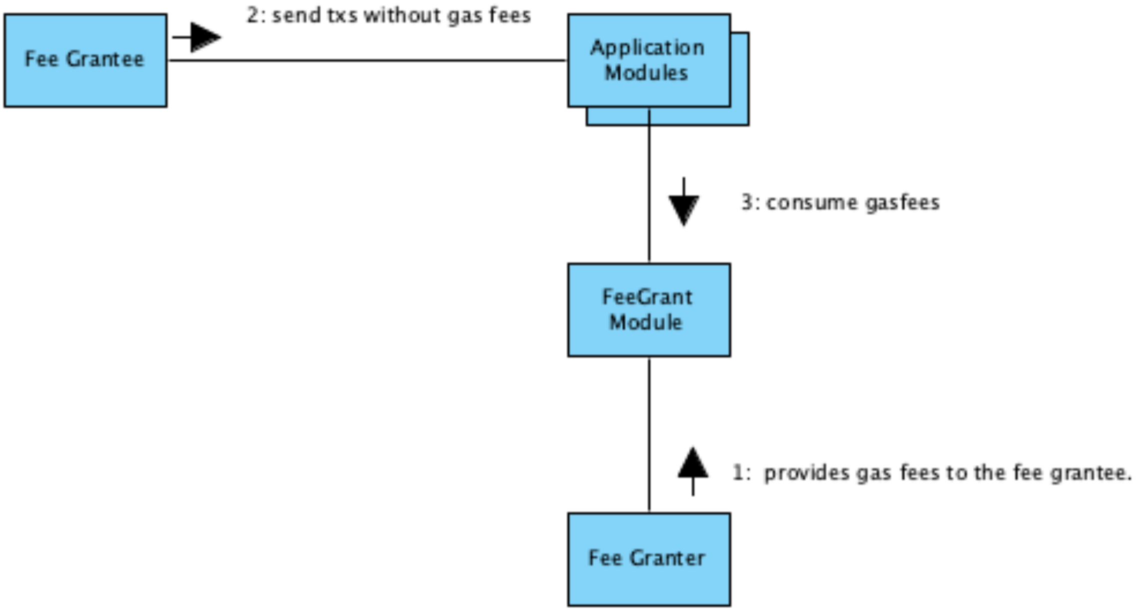
- For proposals involving parameter updates, the **Validator Node** directly implements the changes. This ensures that the blockchain operates with the most current and agreed-upon parameters, maintaining system stability and security.

Change Runtime Binary:

- In cases where the proposal involves changes to the runtime binary, the **Supervisor** manages the update process. The new binary is then deployed to the **Validator Node**, ensuring seamless operation of the system with the updated binary. This managed deployment process minimizes risks and potential vulnerabilities.

This governance and update framework significantly enhances the security of our blockchain system. By leveraging governance-based deployment and operation, involving multiple stakeholders, and ensuring thorough verification processes, we maintain the integrity and robustness of our blockchain ecosystem. This structured approach ensures that all changes are handled with the highest level of security and efficiency, reinforcing the resilience of our system.

3. Improved user accessibility with gas fee control module



In the rapidly evolving blockchain landscape, user accessibility and transaction efficiency are critical factors for widespread adoption. To address these needs, our blockchain ecosystem incorporates a sophisticated gas fee control module, enhancing user experience and operational efficiency.

The gas fee control module is designed to streamline transactions by allowing designated Fee Granters to provide gas fees to Fee Grantees. This mechanism ensures that users can send transactions without directly incurring gas costs, thereby improving accessibility and usability.

<u>Step 1: Fee Granter Provision</u>

- The process initiates with the **Fee Granter**. This entity is responsible for supplying gas fees to the **Fee Grantee**. The provision of gas fees is managed through the **FeeGrant Module**.

<u>Step 2: Transaction Submission</u>

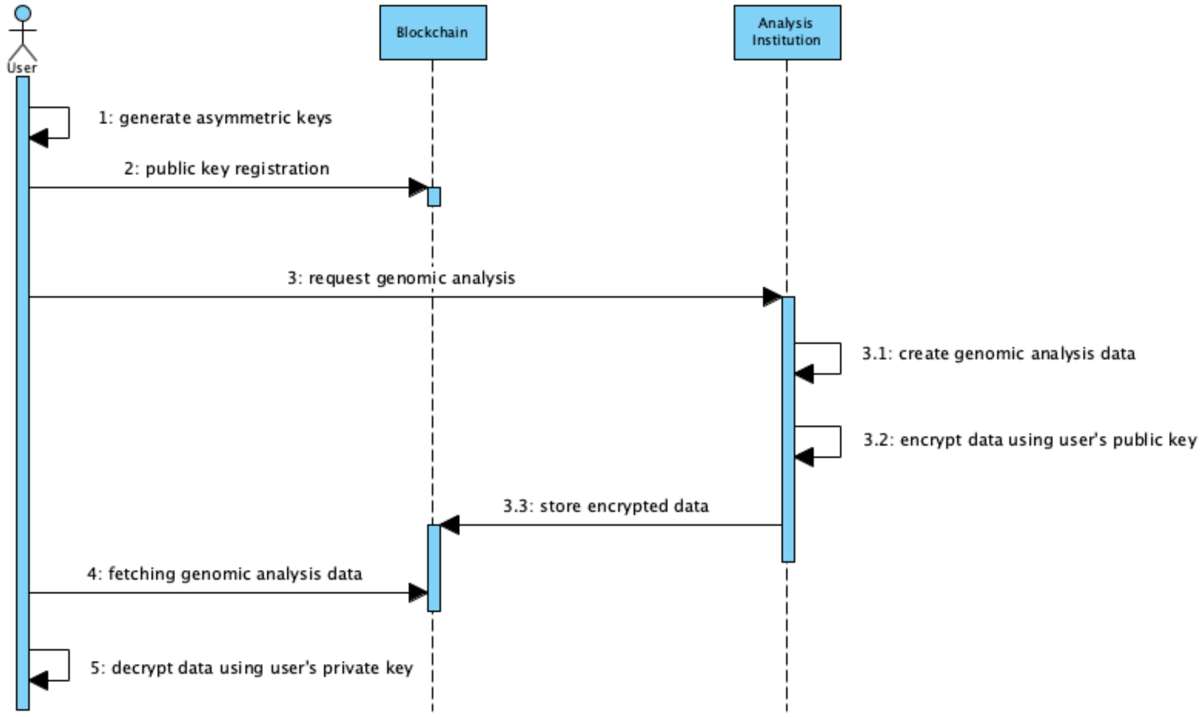
- Once the gas fees are provided, the **Fee Grantee** can submit transactions. These transactions are sent without the need for the Fee Grantee to cover the gas fees directly. The transactions are processed through the **Application Modules**, which handle the core application logic.

Step 3: Gas Fee Consumption

- As the transactions are processed, the associated gas fees are consumed. The **FeeGrant Module** ensures that these fees are appropriately accounted for and deducted from the allocation provided by the Fee Granter.

The integration of a gas fee control module significantly enhances user accessibility within our blockchain ecosystem. By allowing transactions to be executed without direct gas fee payments from users, this system fosters a more inclusive and efficient environment. The structured and transparent management of gas fees through the Fee Granter and FeeGrant Module underscores our commitment to improving the user experience and promoting the widespread adoption of blockchain technology.

4. Registration and review of genomic analysis results securely


User
Blockchain
Analysis Institution
1: generate asymmetric keys
2: public key registration
3: request genomic analysis
3.1: create genomic analysis data
3.2: encrypt data using user's public key
3.3: store encrypted data
4: fetching genomic analysis data
5: decrypt data using user's private key

In the era of personalized service, the secure management of genomic information is critical. This section of our white paper outlines the secure process for registering and reviewing genomic analysis results using blockchain technology and asymmetric encryption. This approach ensures that sensitive genetic data is protected and accessible only to authorized individuals.

User Key Generation

Generate Asymmetric Keys:

- Users initiate the process by generating a pair of asymmetric keys (public and private keys). This cryptographic step is fundamental for ensuring the security and privacy of the genomic data.

Public Key Registration

Register Public Key on Blockchain:

- Users register their public key on the blockchain. This registration step securely associates the user's identity with their public key, enabling trusted interactions within the ecosystem.

Genomic Analysis Request

Request Genomic Analysis:

- Users submit a request for genomic analysis to an accredited genomic information analysis institution. The request includes the user's public key, facilitating secure data handling and communication.

Data Creation and Encryption

Genomic Data Generation:

- The analysis institution conducts the genomic analysis and produces the corresponding data, tailored to the user's specific genetic profile.

Encrypt Data Using User's Public Key:

- The genomic data is encrypted using the user’s public key. This encryption ensures that the data remains confidential and can only be decrypted by the user who holds the corresponding private key.

Secure Data Storage

Store Encrypted Data on Blockchain:

- The encrypted genomic data is stored on the blockchain. This immutable storage solution ensures that the data is securely preserved and can be accessed by authorized parties without risk of tampering or unauthorized access.

Data Retrieval and Decryption

Fetch Encrypted Data:

- Users can retrieve their encrypted genomic analysis data from the blockchain using their authenticated credentials. This step ensures that only the rightful owner can access their genomic information.

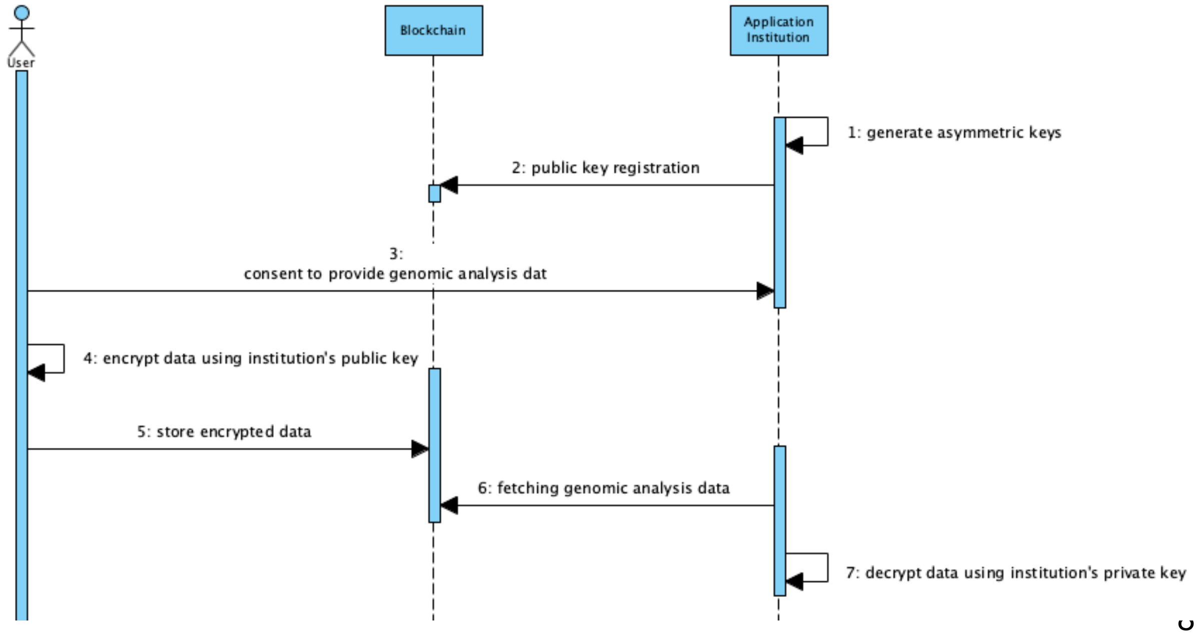
Decrypt Data Using Private Key:

- Finally, users decrypt the retrieved genomic data using their private key. This ensures that the sensitive information contained within the genomic analysis results is accessible only to the user, maintaining confidentiality and data integrity.

This secure workflow for the registration and review of genomic analysis results demonstrates our commitment to data privacy and security in the genomic era. By integrating blockchain technology and asymmetric encryption, we provide a robust framework that safeguards sensitive genetic information. This approach not only protects user data but also empowers individuals by giving them control over their genomic information.

Our methodology ensures that the management of genomic data is both secure and efficient, fostering trust in the digital healthcare ecosystem. As we continue to advance in personalized service, these security measures will be crucial in maintaining the integrity and confidentiality of genetic information, ultimately contributing to improved healthcare outcomes and patient trust.

5. Provision of sovereign genomic analysis results to third parties


User
Blockchain
Application Institution
1: generate asymmetric keys
2: public key registration
3:
consent to provide genomic analysis dat
4: encrypt data using institution's public key
5: store encrypted data
6: fetching genomic analysis data
7: decrypt data using institution's private key

In the context of advancing personalized healthcare services, the secure and efficient provision of genomic analysis results to third-party institutions is paramount. This section outlines the process by which genomic analysis data is securely shared with application institutions, ensuring the integrity and confidentiality of sensitive genetic information.

Application Institution Actions:

Generate Asymmetric Keys:

- The process begins with the application institution generating a pair of asymmetric keys (public and private keys). This step is essential for ensuring secure communication and data transfer.

Public Key Registration:

- The application institution registers their public key on the blockchain. This registration links the institution's identity to their public key, enabling secure interactions within the ecosystem.

User Actions:

Consent to Provide Genomic Analysis Data:

- The user provides consent to share their genomic analysis data with the application institution. This consent is a critical step in maintaining ethical standards and respecting user autonomy.

Encrypt Data Using Institution's Public Key:

- Upon receiving the genomic analysis data, the user encrypts the data using the institution’s public key. This encryption ensures that only the institution can decrypt and access the data.

Store Encrypted Data:

- The encrypted genomic analysis data is then securely transmitted and stored on the blockchain. This ensures that the data is preserved in a tamper-proof manner and is only accessible to authorized parties.

Application Institution Actions:

Fetching Genomic Analysis Data:

- The application institution retrieves the encrypted genomic analysis data from the blockchain using their authenticated credentials. This step ensures that only the authorized institution can access the genomic information.

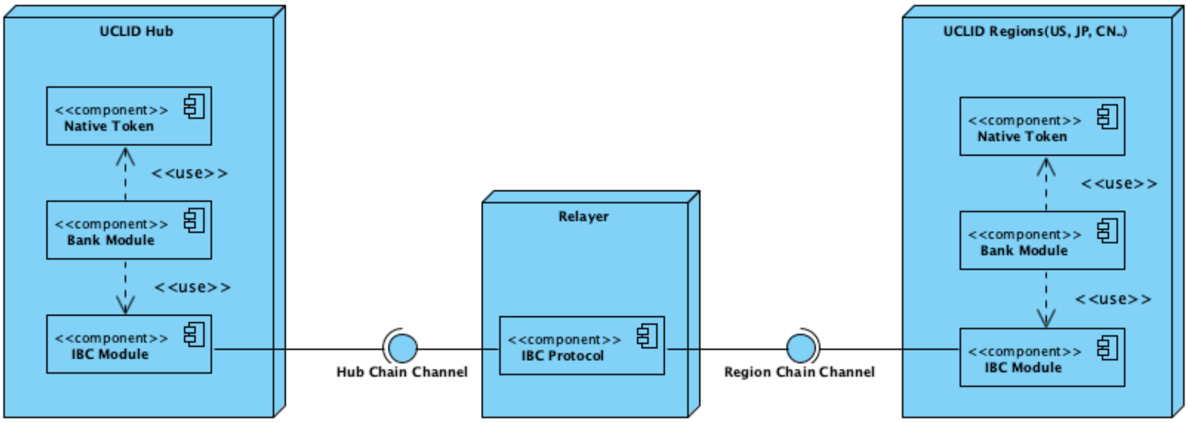
Decrypt Data Using Private Key:

- Finally, the application institution decrypts the genomic analysis data using their private key. This ensures that the sensitive information contained within the genomic analysis results is accessible only to the authorized institution, safeguarding against unauthorized access and ensuring data integrity.

The outlined workflow provides a robust framework for the secure provision of genomic analysis results to third parties. By leveraging blockchain technology and asymmetric encryption, we ensure that sensitive genetic data is protected throughout the entire process. This method not only preserves the confidentiality and integrity of the data but also empowers users by maintaining their control over how their genetic information is shared and utilized.

This approach aligns with our commitment to security, privacy, and ethical standards, reinforcing trust in our digital healthcare ecosystem. As we continue to advance in personalized healthcare services, these measures will be crucial in fostering a secure and efficient environment for managing and sharing genomic information.

6. Multi-chain communication and native tokens via IBC protocol


UCLID Hub
<<component>> Native Token
<<use>>
<<component>> Bank Module
<<use>>
<<component>> IBC Module
Hub Chain Channel
Relayer
<<component>> IBC Protocol
Region Chain Channel
UCLID Regions(US, JP, CN..)
<<component>> Native Token
<<use>>
<<component>> Bank Module
<<use>>
<<component>> IBC Module

In the context of enhancing interoperability and efficiency within our blockchain ecosystem, the implementation of multi-chain communication and native tokens via the Inter-Blockchain Communication (IBC) protocol is paramount. This section details the architecture and operational dynamics that facilitate seamless interaction between the UCLID Hub and various regional chains, ensuring robust and secure transactions.

Architecture Overview

UCLID Hub:

- The UCLID Hub serves as the central nexus of the ecosystem, orchestrating core operations and maintaining connectivity with multiple regional chains. It is equipped with several critical components:
  - **Native Token:** This digital asset is used consistently across both the UCLID Hub and UCLID Regions, providing a standardized medium of exchange and value throughout the entire ecosystem.
  - **Bank Module:** This module handles all financial transactions, managing transfers, balances, and accounts to ensure smooth financial operations.
  - **IBC Module:** A pivotal component that enables interoperability with regional chains via the IBC protocol, facilitating secure and efficient multi-chain communication.
  -

UCLID Regions (e.g., US, JP, CN):

- The UCLID Regions operate autonomously within the UCLID framework, delivering localized services while ensuring synchronized connectivity with the UCLID Hub.
  - **Native Token:** The same native token used in the UCLID Hub is also utilized in all UCLID Regions, ensuring currency uniformity and seamless value transfer across the entire ecosystem.
  - **Bank Module:** Responsible for managing the region-specific financial transactions, including transfers and account management.
  - **IBC Module:** This component ensures each region can interact seamlessly with the UCLID Hub and other regions through the IBC protocol.

Multi-Chain Communication Process

- Initiation of Communication:
  - Communication between the UCLID Hub and regional chains is initiated via the IBC protocol. The IBC modules within the Hub and regional chains establish a secure channel, referred to as the Hub Chain Channel and Region Chain Channel, respectively.
- Transaction Execution:
  - Transactions involving the native token are managed by the Bank Module of the respective chains. When a transaction is

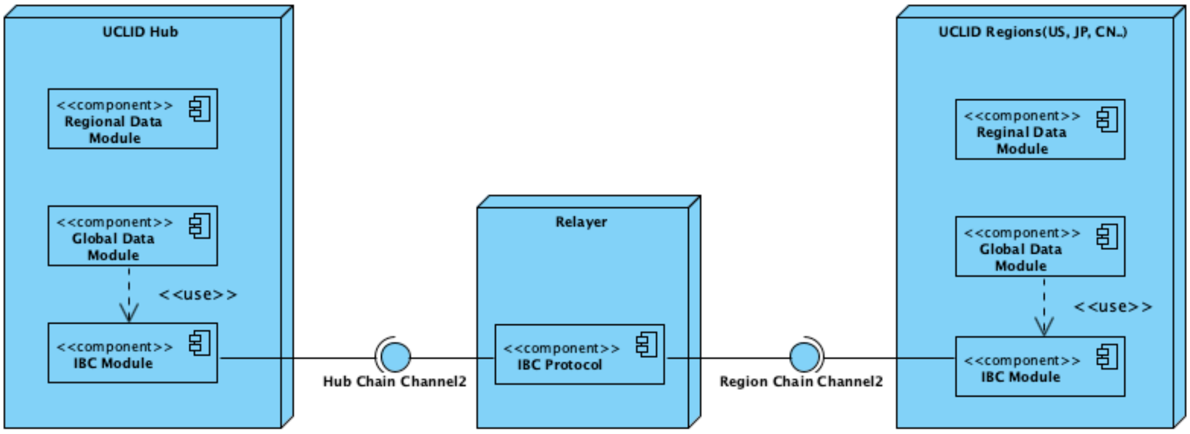
initiated, the Bank Module processes it and invokes the IBC Module to handle the cross-chain communication.

- Interoperability via IBC Protocol:
  - The IBC protocol ensures that transactions and data transfers are carried out securely and efficiently. The Relayer component facilitates the communication, ensuring data integrity and transaction consistency across chains.
- Finalization and Validation:
  - Once the transaction data is relayed, the receiving chain's IBC Module processes it, and the Bank Module finalizes the transaction. This ensures that all operations are synchronized and validated across the ecosystem.

The integration of multi-chain communication and the use of a single native token across the UCLID Hub and UCLID Regions via the IBC protocol represents a significant advancement in our blockchain ecosystem. By leveraging the IBC protocol, we ensure robust, secure, and efficient interoperability between the UCLID Hub and its regional chains. This architecture not only enhances the scalability and functionality of our ecosystem but also ensures a seamless user experience, facilitating broader adoption and utilization of blockchain technology.

This approach aligns with our commitment to creating a decentralized, interoperable, and scalable blockchain infrastructure. As we continue to innovate and expand, the IBC protocol will remain a cornerstone of our strategy, driving the future of multi-chain blockchain ecosystems.

7. Isolation of regional data and sharing of global data



In the decentralized framework of UCLID's blockchain ecosystem, managing data efficiently while adhering to regional legal requirements and facilitating global data sharing is essential. This section elaborates on how UCLID achieves the isolation of regional data and the sharing of global data, ensuring compliance and enhancing interoperability.

Architecture Overview

UCLID Hub:

- The central hub of the UCLID ecosystem, responsible for managing both regional and global data through its integrated modules:
    - **Regional Data Module:** Handles data specific to individual regions, ensuring that sensitive and legally constrained information remains within the appropriate jurisdiction.
    - **Global Data Module:** Manages data intended for global sharing, facilitating broader access and collaboration across different regions.
    - **IBC Module:** Facilitates communication and data transfer between the UCLID Hub and regional chains via the IBC protocol.

UCLID Regions (e.g., US, JP, CN):

- These regional entities operate under the UCLID framework, focusing on localized data management and integration with the global network:
    - **Regional Data Module:** Ensures that region-specific data, especially sensitive information subject to legal constraints, is stored and processed within the region.
    - **Global Data Module:** Manages data that can be shared globally, supporting collaborative efforts and data exchange.
    - **IBC Module:** Enables seamless communication and interoperability with the UCLID Hub and other regions using the IBC protocol.

Data Management Process

Regional Data Isolation:

- Data Handling:
    - Regional Data Modules in both the UCLID Hub and UCLID Regions handle data that is specific to a particular region. This ensures compliance with local regulations and legal requirements.
- Access Control:

    - Only entities within the same region can access regional data, maintaining the privacy and security of sensitive information.

Global Data Sharing:

- Data Handling:
    - Global Data Modules manage data intended for sharing across different regions. This facilitates collaboration and innovation by making non-sensitive information widely accessible.
- Interoperability:
    - The IBC Modules ensure that global data can be seamlessly transferred and accessed between the UCLID Hub and various regional chains. The IBC protocol guarantees secure and efficient data exchange.

Legal Compliance and Data Security:

- Regional Legal Compliance:
    - The architecture ensures that sensitive data subject to regional legal constraints remains within the regional chain, addressing potential legal issues and compliance requirements.
- Data Encryption and Access Control:
    - Both regional and global data are encrypted and managed with stringent access controls to ensure security and integrity.

The isolation of regional data and the sharing of global data within the UCLID blockchain ecosystem are crucial for balancing legal compliance with the need for global collaboration. By leveraging specialized modules and the IBC protocol, UCLID ensures that sensitive regional data is protected while enabling the efficient sharing of global data. This approach not only adheres to regional legal requirements but also promotes innovation and cooperation across different regions.

This section underscores our commitment to secure and compliant data management, ensuring that our blockchain ecosystem remains robust, interoperable, and adaptable to varying legal landscapes. As we continue to expand and refine our services, these measures will be integral to maintaining the trust and efficiency of the UCLID ecosystem.

8. Conclusion

UCLID Hub leverages blockchain technology to build an infrastructure that prioritizes individual data sovereignty. This infrastructure ensures that only individuals have access to their genetic data, providing complete control over it. Through this, users can securely store their genetic data, protect their privacy, and receive optimized health solutions.

Our goal is to realize "a world where people can live healthier and more prosperous lives." **UCLID Hub** aims to redefine the future of healthcare through technological innovation and create a world where everyone can safely utilize their genetic information

References

1. *Cosmos SDK Governance Module, https://docs.cosmos.network/v0.50/build/modules/gov*
2. *Cosmos SDK Feegrant Module, https://docs.cosmos.network/main/build/modules/feegrant*
3. *Asymmetric Algorithm, https://en.wikipedia.org/wiki/Public-key_cryptography*
4. *IBC Protocol, https://www.ibcprotocol.dev/*