2 The Cardano blockchain and its relationship with the airwaves (1-b)

In the previous year (2023), verification with broadcast signals was conducted in the Symbol blockchain environment. The Symbol blockchain uses an account-based model, which differs from the UTXO model used by the Cardano blockchain. Therefore, this project has significant implications for next-generation cross-chain technology by conducting prototype verification using the Cardano blockchain.

2.1 Differences between Carudano (UTXO) and Symbol (account-based)

2.1.1 UTXO（Unspent Transaction Output）Model

The UTXO model is a system that is particularly useful for tracking and managing transactions, and it stands for ”Unspent Transaction Output.” Specifically, it refers to the balance of tokens or coins that have not yet been spent after a transaction has occurred on the blockchain.

・Input and Output of Transactions:

Each transaction has one or more ”inputs” and ”outputs.” The input refers to the UTXO generated by a previous transaction, and the output is the newly created UTXO.

・Consumption and Generation of Transactions:

UTXOs are consumed as inputs in transactions and are newly generated as outputs. For example, when Person A sends 1 ADA to Person B, the UTXO used for that transfer is consumed, and a new UTXO is generated in Person B’s wallet.

・Transparency and Ease of Tracking:
Each transaction can be clearly traced back to the UTXO it is based on, making the flow of transactions highly transparent.

・Scalability:
In the UTXO model, there is no need to track account balances; it simply manages unspent transaction outputs, making the verification of specific transactions straightforward.

・Security:
Since UTXOs can only be used once, the model prevents double-spending (the issue of using the same asset more than once). This enhances the consistency and security of the blockchain.

・Parallel Processing Capability:
The UTXO model allows for easier parallel processing of transactions, which contributes to improved scalability and performance of the system.

2.1.2 ExUTXO（Extended Unspent Transaction Output）Model

Cardano adopts an improved version of the Bitcoin UTXO model called the **ExUTXO (Extended Unspent Transaction Output)** model. This results in the following features:

・Integration with Smart Contracts:
In the EUTXO model, transaction logic can be integrated with smart contracts, and it is combined with Cardano's smart contract functionality (Plutus). This allows for more complex logic and conditional transactions.

・Deterministic Transactions:
In EUTXO, it is predetermined which UTXO each transaction will consume, making the transaction results predictable and easier to maintain the overall integrity of the blockchain.

・Low Cost and High Efficiency:
The EUTXO model is designed to reduce unnecessary gas fees and improve transaction processing efficiency. As a result, it provides a cost-effective system for both developers and users.

2.1.3 Account-based Model

The account-based model directly manages the balance of each user's account (wallet). Ethereum, among others, adopts this model. It has the following three characteristics:

・Balance Management:
Balances are recorded for each account, and transactions cause these balances to increase or decrease.

・Simple Design:
The balance of each account is recorded as is for every transaction.

・Compatibility with Smart Contracts:
It is well-suited for executing smart contracts and modifying their states, making it highly compatible with smart contract operations.

2.1.4 Differences between the UTXO model and the account-based model

The difference between the UTXO (Unspent Transaction Output) model and the Account-Based model primarily lies in the structure of transactions and the way account balances are managed. Below is a detailed explanation of the characteristics of each model and their differences.

Differences in basic structure

<UTXO Model>

Each transaction uses "Unspent Transaction Outputs (UTXO)" as inputs and generates new outputs. With each transaction, the previously unspent funds (UTXO) are used in the next transaction. Bitcoin and Cardano adopt this model.

<Account-Based Model>

Each account has a balance, and when a transaction occurs, the balance of that account is directly increased or decreased. With each transaction, the new account state is updated, and instead of using UTXO as the input/output of the transaction, the account balance is modified. Ethereum and Symbol adopt this model.

How to process transactions

<UTXO Model>

Each transaction uses multiple UTXOs as "inputs" and generates multiple "outputs." All UTXOs can only be used once, and once used, they are consumed. Payments can be made by combining multiple UTXOs, and if change is needed, a new UTXO is generated. Since each UTXO is associated with a fixed amount of cryptocurrency, transactions are highly transparent, and the risk of double-spending

is reduced.

<Account-Based Model>

In a transaction, the balance of the sender's account decreases, and the balance is added to the receiver's account. Since the balance is directly updated on the blockchain, there is no need to track transaction outputs like in UTXO. Transactions are simple and only require consideration of the amount sent and the fees.

Parallel Processing

<UTXO Model>

In the UTXO model, transactions are independent, making parallel processing easier. Since multiple UTXOs can be processed simultaneously, it offers excellent scalability. Each transaction specifies which UTXO it consumes, and this does not affect other transactions.

<Account-Based Model>

In the account-based model, since the balance of each account is continuously updated, parallel processing can be difficult. If multiple transactions attempt to process the same account simultaneously, conflicts may occur.

Gas charges and fees

<UTXO Model>

Each transaction is calculated based on which UTXO it uses. The gas fee is usually determined by the complexity of the transaction and the number of UTXOs used.

<Account-Based Model>

Transaction fees may either be fixed per transaction or vary depending on the transaction's content (such as data size or computational load). When there are complex operations, such as executing smart contracts, the fees tend to increase.

Transparency and Security

<UTXO Model>

Since all UTXOs are tracked as inputs and outputs of transactions, the flow of transactions is highly transparent. The entire transaction history is clearly visible, preventing double-spending.

<Account-Based Model>

Since the account balance is directly modified, the transaction history appears simple at first glance, but it does not have the same level of transparency as the UTXO model when it comes to tracking balances. In the account-based model, additional measures may be necessary to enhance security.

Compatibility with smart contracts

<UTXO Model>

Integration with smart contracts is somewhat complex. Since UTXOs are consumed once used, it becomes difficult to manage the state of smart contracts. However, Cardano adopts the "EUTXO" model, an improved version of the UTXO model, which allows for integration with smart contracts.

<Account-Based Model>

Integration with smart contracts is somewhat complex. Since UTXOs are consumed once used, it becomes difficult to manage the state of smart contracts. However, Cardano adopts the "EUTXO" model, an improved version of the UTXO model, which allows for integration with

smart contracts.

Comparison Table

Feature	UTXO Model	Account-Based Model
Transaction Structure	Processed using unspent transaction outputs	Directly manages account balances
Transparency	High (easy to track transactions)	Balances are easy to understand, but transaction flow is complex
Parallel Processing	Easy (multiple transactions can be processed simultaneously)	Difficult (account conflicts may occur)
Smart Contracts	Somewhat complex (improved with EUTXO)	Highly compatible with smart contracts
Use Case	Ideal for simple transactions and high scalability	Primarily for smart contracts and account management

2.2 Integration of IPDC and Blockchain Technology and the Significance of This Demonstration

2.2.1 Method for Reliability Verification by Integrating IPDC and Blockchain

IPDC (IP Data Cast) is a technology that enables efficient data transfer in a unidirectional transmission environment via broadcasting, allowing information to be transmitted over a wide area even in situations where internet connectivity is difficult. This technology is an effective means of ensuring that critical information is delivered reliably to recipients during widespread communication failures or localized cloud outages, such as in disaster scenarios.

However, due to the unidirectional nature of the transmission, there is a challenge in how to verify the reliability of the received data. In particular, with the increasing prevalence of data tampering and forgery using artificial intelligence in modern times, if the reliability of the received information is not guaranteed, decisions and economic activities based on that information may involve significant risks.

One important factor in verifying reliability is the presence of a ”trust anchor.” In traditional Public Key Infrastructure (PKI), third-party certification authorities (CAs) function as trust anchors, ensuring the reliability of information. In environments where bidirectional communication over the network is possible, queries can be made to the certification authority to verify trustworthiness, reducing the likelihood of problems. However, in unidirectional transmission environments such as IPDC, it is difficult for the receiver to scrutinize the contents of the information, and additional methods are required to ensure reliability.

2.2.2 Method for New Reliability Verification Using Blockchain Technology

One promising method to solve the challenges of reliability verification in a unidirectional transmission environment is the use of blockchain technology. Blockchain has a chain structure where each block is linked by a hash, making it highly reliable and difficult to tamper with. Furthermore, by verifying that the received data is recorded in a specific block, blockchain ensures that the data has not been tampered with.

Additionally, since broadcasting is publicly available as a social infrastructure, it is continuously monitored by viewers, making it practically impossible to deliver different information only to specific users. Therefore, using blockchain as a system to prove the existence of data can be a safer and more reliable approach. By leveraging smart contracts, it is also possible to control the recording of only electronically signed data that meets certain conditions, enabling more flexible reliability verification.

However, there are several challenges when using blockchain technology in a unidirectional transmission environment. Typically, blockchain requires bidirectional communication to maintain data consistency between nodes and needs to constantly verify the synchronization of the entire network. Therefore, when using IPDC to transmit information to terminals outside the network, the challenge lies in how to verify the reliability of the received information. In other words, while IPDC ensures the reliability of the transmission path through broadcasting, the key issue is whether the reliability of the received information can also be guaranteed. If this can be achieved, a platform that ensures trustworthiness can be established.

2.2.3 Conditions necessary for realization

To implement this reliability verification model, several important conditions must be met.

・The trust anchor and the information of the transaction issuer must remain unchanged.

In unidirectional transmission, there is no way to detect changes in the source information. Therefore, to ensure the reliability of the received information, it is essential that critical information, such as the trust anchor and the public key of the transaction issuer, has not been tampered with. Additionally, to prevent data tampering, strict security measures, such as regular rotation of private keys, are necessary.

・All information required for verification must be provided to the receiver.

In a unidirectional communication environment, all data required for verification must be provided to the receiver. For example, while transaction data and trust anchor information are connected through Merkle trees and block headers, all of this information must be provided. To meet these conditions, it is essential to select and implement appropriate blockchain technology.

2.2.4 Previous Cases Using the Symbol Blockchain and Their Outcomes

In our previous research, we confirmed that these issues can be resolved by utilizing the Symbol blockchain. First, in blockchain systems, the genesis block or widely-known block hashes can be used as trust anchors, and the risk of these being tampered with is low. Additionally, the security of the transaction issuer's key information can be maintained by regularly rotating private keys. Furthermore,

with Symbol's flexible multisig (multi-signature) functionality, the configuration of signatories can be easily modified, enabling secure operation.

Symbol also implements a decentralized API (REST API), allowing verification of blockchain information while checking the synchronization status of multiple nodes without the need to maintain your own node. This mechanism is particularly effective for broadcasters who need to provide information during disasters, and it is also advantageous for building a multi-chain broadcast system.

2.2.5 Challenges in the Cardano Blockchain and Considerations for Disaster Operations

Although multi-signature is available on the Cardano blockchain, changing the key configuration is difficult, and it seems unlikely that operations can be performed where the public key remains fixed while rotating the private key. Additionally, the public APIs of Cardano (e.g., blockfrost) do not provide sufficient information to verify blocks and transactions, which may limit the reliability verification in disaster situations.

For this reason, a new approach called "Trusted Web" has been proposed in Japan. Unlike Web3, which verifies all information, the Trusted Web adopts a system where trusted companies ensure part of the reliability, aiming for more flexible and efficient data circulation. Based on this concept, it is possible to build a highly reliable information provision and verification environment by leveraging the public auditability of broadcasting.

About blockfrost (reference)

An API platform that functions as infrastructure for accessing data on the Cardano blockchain. Blockfrost enables developers to easily access Cardano blockchain data and functions, supporting the rapid

development of applications and services. The following are its features:

・Easy API Access

It provides a mechanism to easily access Cardano's blockchain data through a REST API. This allows programs to access block information, transactions, addresses, assets (such as tokens), and stake pool information.

・Cardano Blockchain Integration

It connects to the Cardano blockchain nodes, allowing users to utilize Cardano's data without managing the nodes themselves. This eliminates the need for developers to build and maintain their own infrastructure, allowing them to focus on application development.

・Transaction submission

Using Blockfrost, it is possible to send transactions directly to the Cardano blockchain. This simplifies the development of services such as wallet apps and payment apps that require interactions on the blockchain.

・Multiple Network Support

It supports both the Cardano mainnet and testnet, allowing developers to smoothly test and deploy in both production and development environments.

・IPFS Support

In addition to Cardano, it also supports the decentralized file system IPFS (InterPlanetary File System). This allows developers to build DApps (decentralized applications) and services using decentralized file storage.

・Scalability and Stability

It provides scalable infrastructure, enabling reliable access even for large-scale applications. Developers can efficiently handle a large number of requests, with a focus on the reliability and response speed of the API.

About the Trusted Web (reference)

The Trusted Web is a new internet concept and technical framework promoted by the Japanese government, certain companies, and research institutions. This initiative is designed to enhance the reliability and transparency of the digital society, ensuring the authenticity of information, preventing tampering, and protecting privacy. Unlike traditional centralized web systems, it aims to create a decentralized system for sharing trustworthy information, with the goal of building an internet that everyone can use with confidence.

・Ensuring reliability

The Trusted Web aims to ensure the reliability of information exchanged in the digital space. It addresses issues such as false information, fake news, and data tampering. By verifying the source and authenticity of each piece of data, it provides a system that ensures the proper circulation of trustworthy information.

・Utilization of Decentralized Technology

It is based on technologies such as blockchain and Distributed Ledger Technology (DLT). These technologies prevent data tampering and enable transparent and secure information sharing among multiple parties. By eliminating reliance on a central authority, trust is autonomously maintained.

・Data Privacy Protection

Protecting user privacy is also an important element of the Trusted Web. It ensures the exchange of trustworthy data while preventing unnecessary leakage of personal data and its misuse by third parties.

・Transparent and tamper-proof

In the Trusted Web, information transparency and the ability to track change histories are possible. By using decentralized databases like blockchain, it records who updated the information, when, and how, making data tampering impossible.

・Increased trust in online transactions

By utilizing this technology, it provides an environment where all parties involved in online transactions, contracts, and other exchanges can trust the information. As a result, it allows for safer transactions in B2B and B2C commercial activities.

2.3 Utilization of the Cardano Blockchain on IPDC and Future Prospects

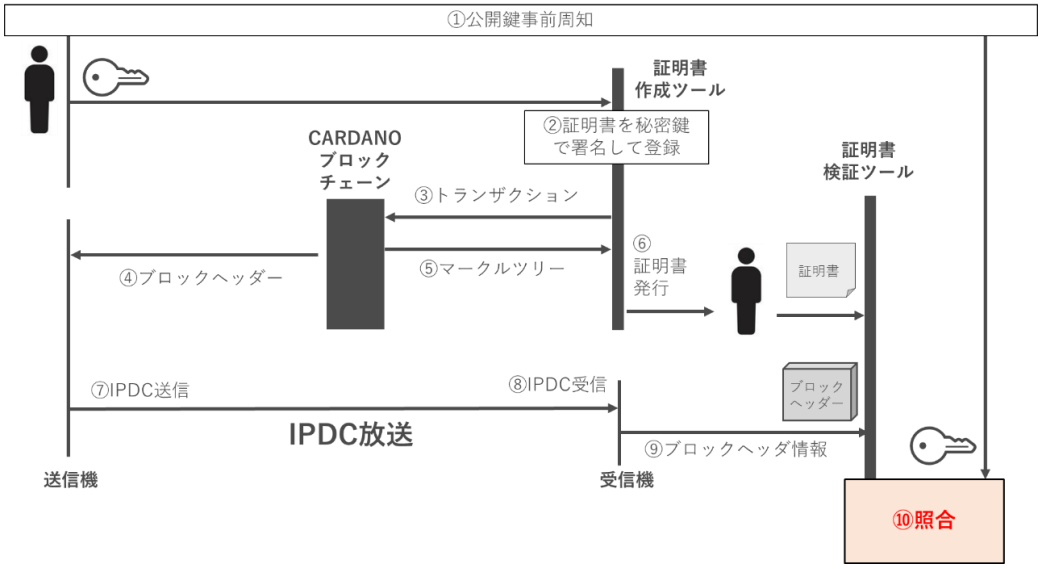
To implement a reliability verification system that integrates IPDC technology with the Cardano blockchain, the following elements are essential:

2.3.1 Ensuring the reliability of the certificate issuer through broadcasting.

The broadcaster guarantees reliability by authenticating the document issuer. Additionally, a system should be established that excludes transactions that do not meet authentication requirements from broadcasting, thereby preventing the transmission of fraudulent information.

2.3.2 Broadcasting supplements information necessary for verification

Provide the necessary information for verification (such as block headers and transaction verification data) to the receiver via broadcasting. This allows the receiver to trust the broadcast content and perform reliability verification smoothly. It is essential that the transmission and reception of block information via IPDC broadcast, as illustrated in steps ⑦ and ⑧, maintain the highest level of reliability.



With such a system, it is believed that a new mechanism can be established that ensures the reliability of received information while enabling efficient data distribution, even in environments or situations where the internet is unavailable.