1 Overall structure and overview（1-a）

This structure uses a platform called Narrowcast as an advanced means of information transmission, utilizing conventional television signals to deliver block information for blockchain authentication as public data. It aims to enable public authentication in environments without internet access.

- **Issuance of certificates via the Cardano blockchain and retrieval of generated block information**
- **Information distribution and reception via television signals using Narrowcast (IPDC)**
- **Reconstruction of block information and verification of certificates**

In this demonstration, we will implement reliability verification using broadcast waves in environments where the internet is unavailable. Normally, certificates created with electronic signatures in an internet environment can be verified by utilizing information from a third party, known as a "Certificate Authority (CA)."

However, when a disaster occurs, it becomes difficult to query information from the "Certificate Authority" due to factors such as the collapse of base stations. In this demonstration, we will utilize IPDC technology to superimpose foundational information onto broadcast waves, enabling the verification of data reliability in disaster-affected areas.

Furthermore, unlike regular electronic signatures, the use of blockchain ensures that the proof of existence for verified data will persist into the future. This can serve as a basis for maintaining economic activities even in situations where access to various databases is cut off during disasters.

1.1 Overall Configuration

The system developed in this demonstration will consist of a ”Certificate Generation Subsystem” and a ”Certificate Verification Subsystem.”

In the Certificate Generation Subsystem, transactions that make up the components of the certificate will be created and registered on the blockchain, and the block header that approves these transactions will be broadcasted via IPDC.

In the Certificate Verification Subsystem, the reliability of the transactions that make up the components of the certificate will be verified based on the block header received through IPDC.

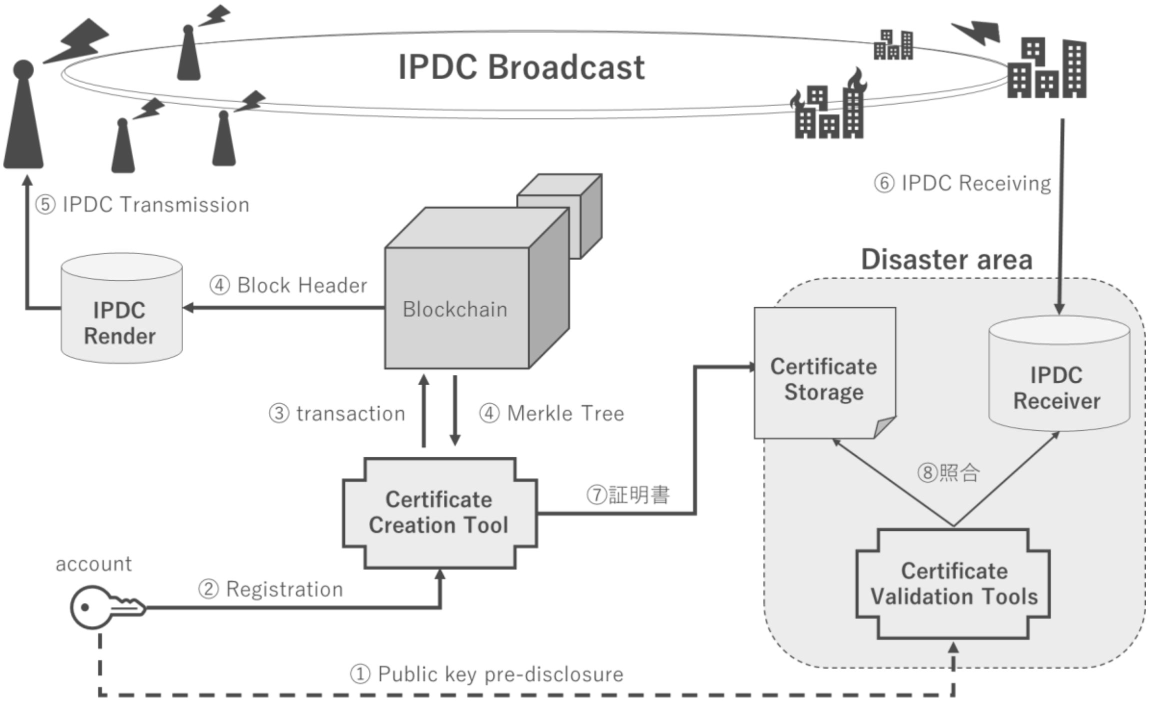


FIGURE: OVERALL CONFIGURATION

In this configuration, disaster areas are assumed as environments without internet access. During large-scale disasters, communication infrastructure used in daily life (such as 4G/5G mobile, free Wi-Fi, and home Wi-Fi) may become unusable due to various reasons. The recovery time after disaster victims lose access to mobile communication can range from several days to weeks (as seen in the case of the Noto Peninsula earthquake in Japan on January 1, 2024). During this period, smartphones such as Android and iPhone may become unusable. Currently, most mobile communication relies on terrestrial stations, wired connections like fiber optic cables, or terrestrial wireless systems, making it vulnerable to large-scale disasters. In this situation, if public authentication using the Cardano blockchain becomes possible, it could help prevent crimes.

In disaster areas, people who have evacuated because their homes have been damaged take refuge in evacuation centers. When a disaster lasts for a long time, fatigue from communal living can lead to distrust, increased crime, and the spread of infectious diseases. In such chaotic situations, blockchain demonstrates its power in terms of reliability. Trust eases the mind of evacuees, prevents crime, and gives evacuees peace of mind and safety. This is important as it also concerns human lives.

Overall flow

As shown in the diagram, at the current stage, the ”certificate” issued through signature registration on the Cardano blockchain is crucial, and authentication processing can be carried out as usual if the internet environment is available. However, our assumption is that even when the internet environment is lost after a large-scale disaster, it should still be possible to conduct ”public authentication” and, consequently, ”protect the lives of disaster victims.” In other words, even if a large-scale disaster occurs, the Cardano blockchain can be utilized to enable authentication under more severe conditions, thus achieving social contributions.

・Assumption 1: Public Key is Announced in Advance (1)
It is assumed that the public key has been announced in advance.

・Register the Certificate by Signing with the Private Key (2)(3)(4)
Information signed with the private key is registered on the Cardano blockchain. The block header and Merkle tree are retrieved from the generated transaction.

・Issue the Certificate (7) (2)
The certificate is issued and handed over to the registrant.

・Broadcast & Receive via IPDC Waves (5)(6) (3)
Block header information is continuously broadcasted via waves and received using a dedicated device.

・Verification at Disaster Base (8)
The certificate is verified and checked based on (1), (2), and (3).

Basic explanation 1: Difference between cryptography and digital signatures

In the blockchain, we mainly utilize the mechanism of electronic signatures. The private key is strictly managed by the sender and is used for generating the signature. On the other hand, the public key is accessible to anyone and is used for verifying the signature. This mechanism does not encrypt the data itself.

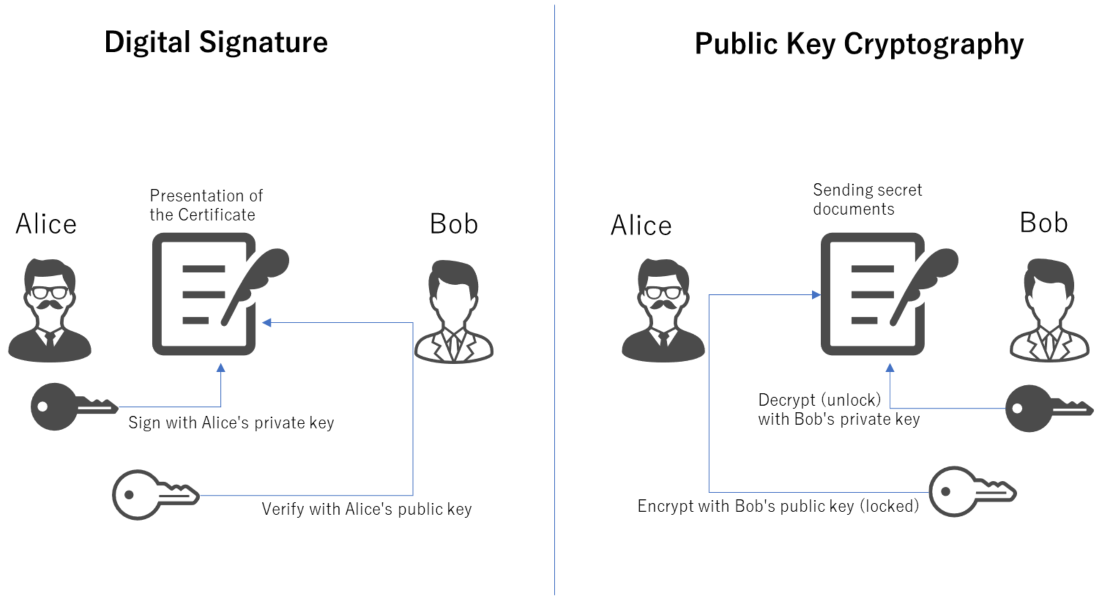
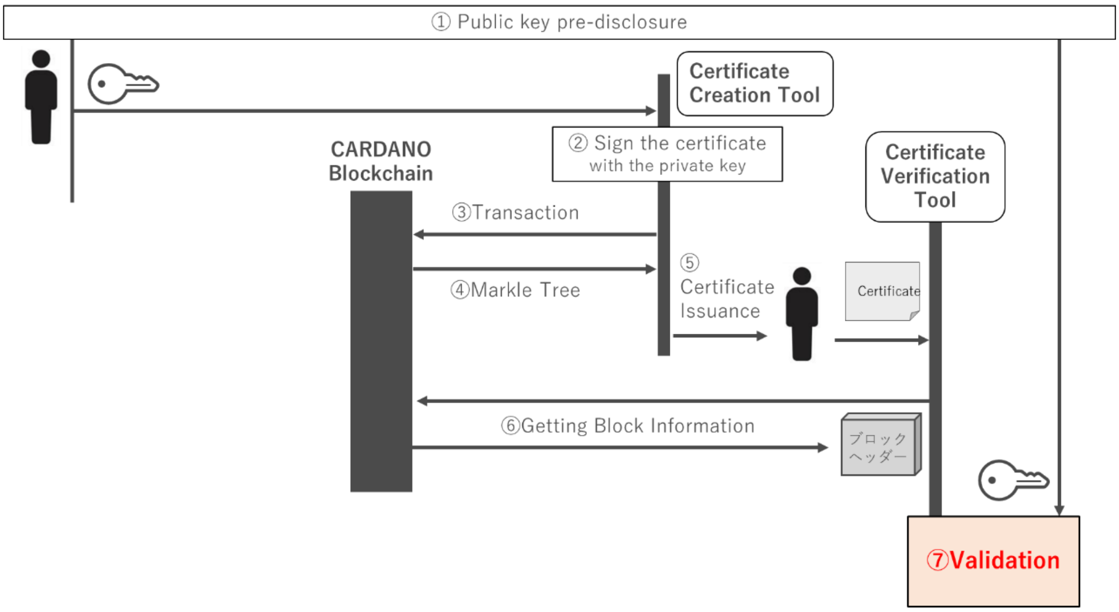

Digital Signature
Alice
Presentation of the Certificate
Bob
Sign with Alice's private key
Verify with Alice's public key
Public Key Cryptography
Alice
Sending secret documents
Bob
Decrypt (unlock) with Bob's private key
Encrypt with Bob's public key (locked)

FIGURE: ENCRYPTION AND SIGNATURES

1.2 Overall processing flow

Normal processing (Internet connection available)

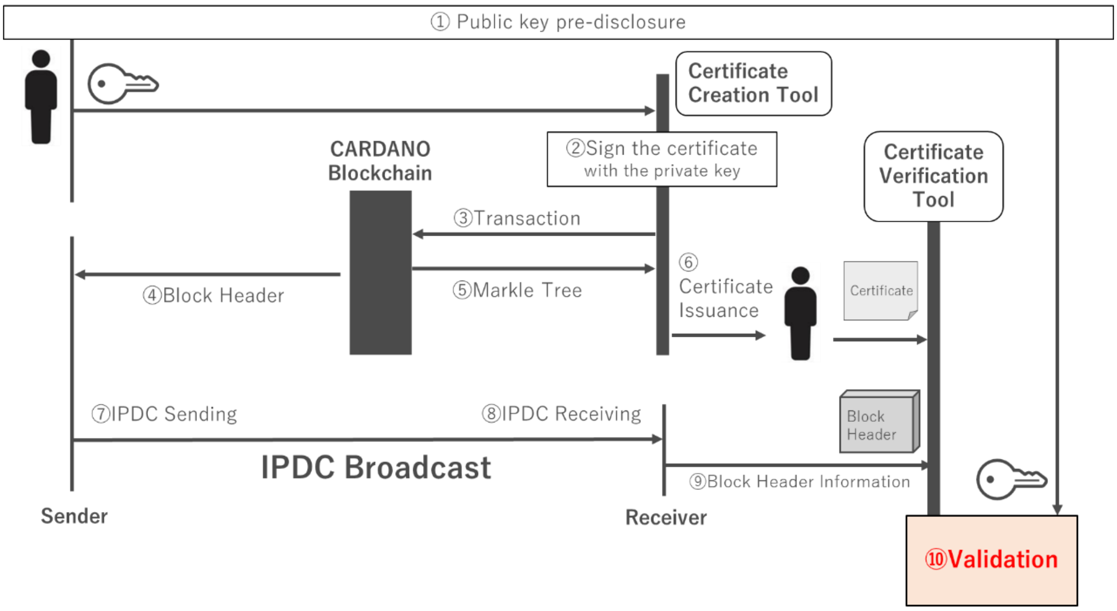
Using a certificate creation tool with a unique account, a certificate is issued via the Cardano blockchain. Even in disaster areas, if the internet environment remains available, the block information can be retrieved from the Cardano blockchain for verification.


① Public key pre-disclosure
Certificate Creation Tool
CARDANO Blockchain
② Sign the certificate with the private key
Certificate Verification Tool
③Transaction
④Markle Tree
⑤ Certificate Issuance
Certificate
⑥Getting Block Information
ブロック ヘッダー
⑦Validation

① Public Key Pre-Announcement
② Register Certificate by Signing with the Private Key
③ Transaction (CARDANO)
④ Merkle Tree Structure
⑤ Issuance by the Certifier
⑥ Block Information Retrieval (CARDANO)
⑦ Validation

Processing with IPDC Broadcast

Using a certificate creation tool with a unique account, a certificate is issued via the Cardano blockchain. In disaster areas where there is no internet access, it is not possible to access the Cardano blockchain. Therefore, after receiving the IPDC broadcast, the block information is retrieved for verification.



① Pre-announcement of Public Key
② Sign the Certificate with the Private Key and Register
③ Transaction (CARDANO)
④ Retrieve Block Header
⑤ Construct Merkle Tree
⑥ Issuance by the Certifier
⑦ IPDC Sender
⑧ IPDC Receiver
⑨ Retrieve Block Header Information
⑩ Validation

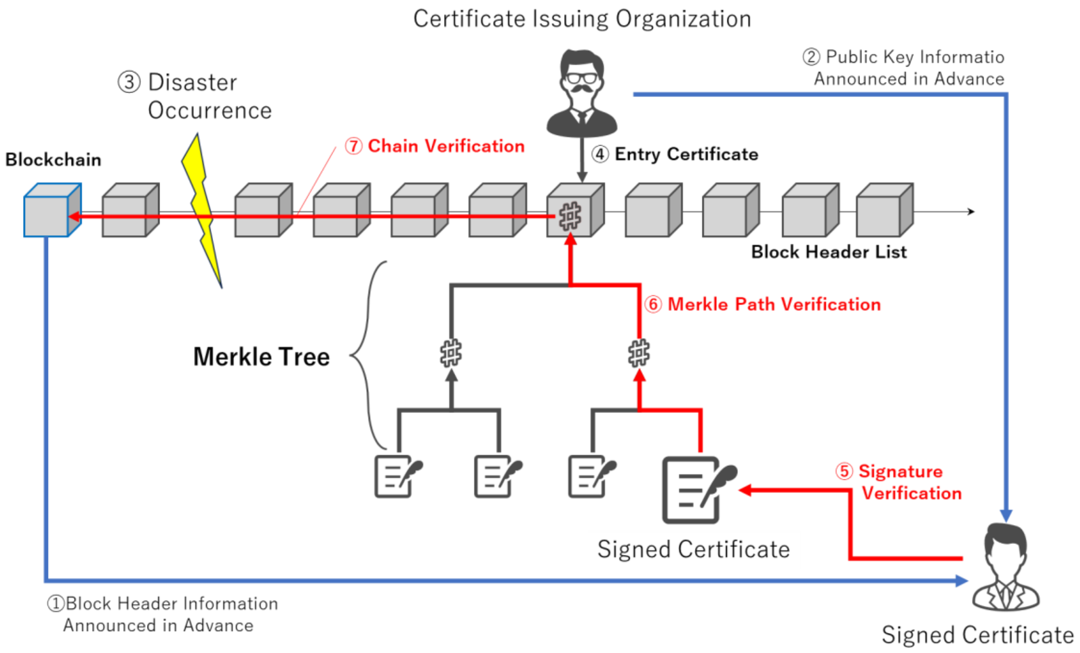
1.3 Certificate Issuance Subsystem

After the transaction is signed by the account of the organization issuing the certificate, it is recorded on the blockchain. When recorded on the blockchain, the Merkle tree information can be calculated from the recorded block height and other transactions recorded in the same block.

These transaction details, Merkle tree information, and block height information are collectively used as a certificate, which is assigned to personnel or equipment that may need identity verification or contract status confirmation during disasters.

Additionally, to verify the existence of the transaction information, it is assumed that block headers generated by the blockchain at regular intervals will be continuously broadcast via IPDC.

Basic explanation: Certificate Issuance Steps



① First, the verifier obtains in advance the block header information, which is well-known and difficult to tamper with on the network, as "information serving as the basis for reliability verification."

② At the same time, the verifier also obtains the public key of the "certificate issuing organization," which will be needed for verification after a disaster occurs.

③ Block headers from the blockchain are broadcasted via IPDC to receivers throughout the broadcast area every time they are generated. Even after a disaster, the robustness of the broadcast facilities, including resistance to earthquakes and wind pressure, ensures that block headers can continue to be distributed via IPDC each time they are generated.

④ After the disaster occurs, the certificate issuing organization creates the necessary certificates for disaster response and recovery support at any given time, recording them as transactions

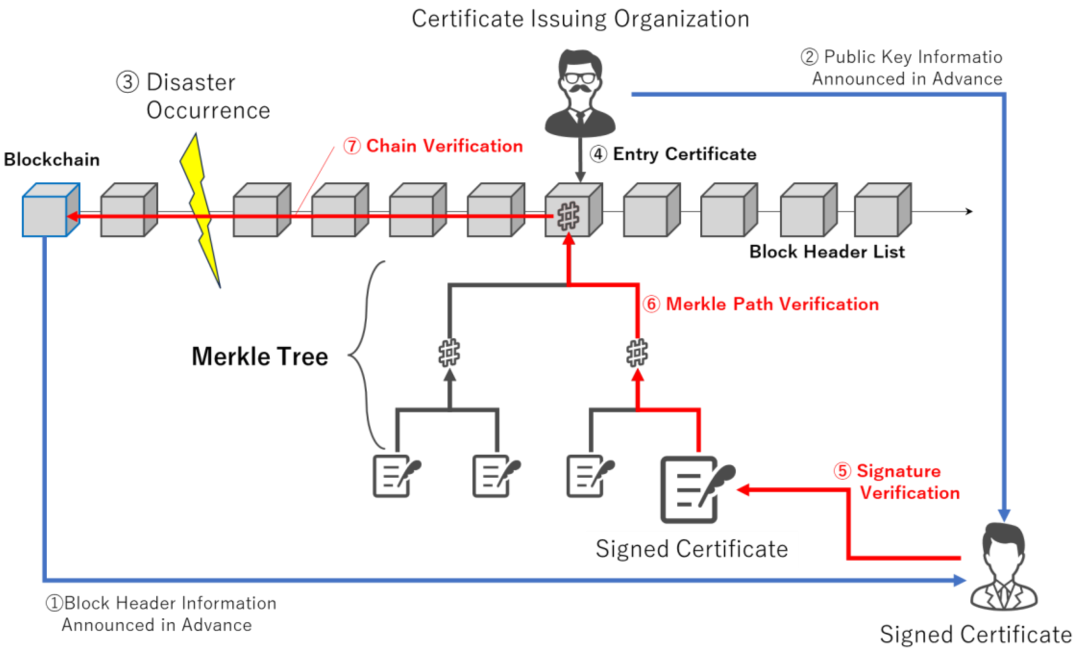
1.4 Certificate Validation Subsystem

The reliability is verified by matching the block header information received via IPDC with the certificate brought into the disaster area. First, the IPDC receiver constantly receives block headers from the broadcast and regularly monitors the integrity of the blockchain. If a rollback occurs, the receiver updates the saved block header list by receiving the broadcast again. The verifier extracts the block header information from the IPDC receiver and first verifies that it traces back to a known block height.

The verifier extracts the block header information from the IPDC receiver and verifies that it traces back to a known block height. Then, they receive the certificate from the presenter and verify the signature on the certificate content. Furthermore, the verifier calculates the transaction root information using the transaction information recorded in the certificate's critical parts and the Merkle tree information attached to the certificate.

If this transaction root information matches the transaction root value within the block header at the specified block height, it proves that the transaction is recorded on the blockchain.

Basic Description: Certificate Verification Steps



⑤ If a staff member providing support on-site needs to prove their identity, they present the "verifiable certificate" to the local verifier. The local verifier first checks whether the presented certificate has been tampered with by verifying it using the public key of the certificate-issuing organization.

⑥ Next, after confirming the integrity of the certificate, the verifier calculates the transaction root using the Merkle path and verifies whether it matches the transaction root of a specific block header received from the IPDC receiver. If these values match, it means that the block header could not have been generated without the transaction being present, confirming that the transaction meets the various constraints that occur when the block is generated.

⑦ If the transaction root matches the block header of block "n," the information contained within that block header proves the existence of the "previous block hash" for block n-1. By sequentially verifying this backwards and confirming that the block header obtained in step

(1) exists, the chain information sent via broadcast is verified to be an integrity-maintained chain, starting from the ”block header information that serves as the basis of reliability.”