Monas

Decentralized Personal Data Store providing flexible access control.

2024

Ishikawa Yudai

CONTENTS

About Monas

Monas enables a privacy layer and flexible access control in cyberspace by building a cryptographic data structure called Cryptree and a P2P Network.

Unlike traditional data management systems,
we put the user at the center and build a data infrastructure that is interoperable between different applications and across different contexts.

Problem

“Our Personal Data is controlled by companies and platforms.”

Personal Data is becoming increasingly siloed due to application and enterprise fragmentation.

We cannot reflect our will on Personal Data and our privacy is being invaded.

Our Personal Data cannot be moved to other platforms or applications.

Problem

These problems hinder the original characteristics of the data.

Data maximizes value when it is aggregated in large numbers and in diversity.
And because of this characteristic,
many companies add value by collecting and storing data in their own closed worlds.

↓

Semantic Web and Blockchain are trying to create an Open world.

Proble
m

What is Semantic Web ?

The purpose of the Semantic Web is to add the communication of meaning to the act of browsing a web page, in addition to the data exchange aspect.

⇒ Linked Data, Open Data

Proble
m

Linked Data

Increase data interoperability by linking data from different data sources.

1

+

→ Linked Open Data

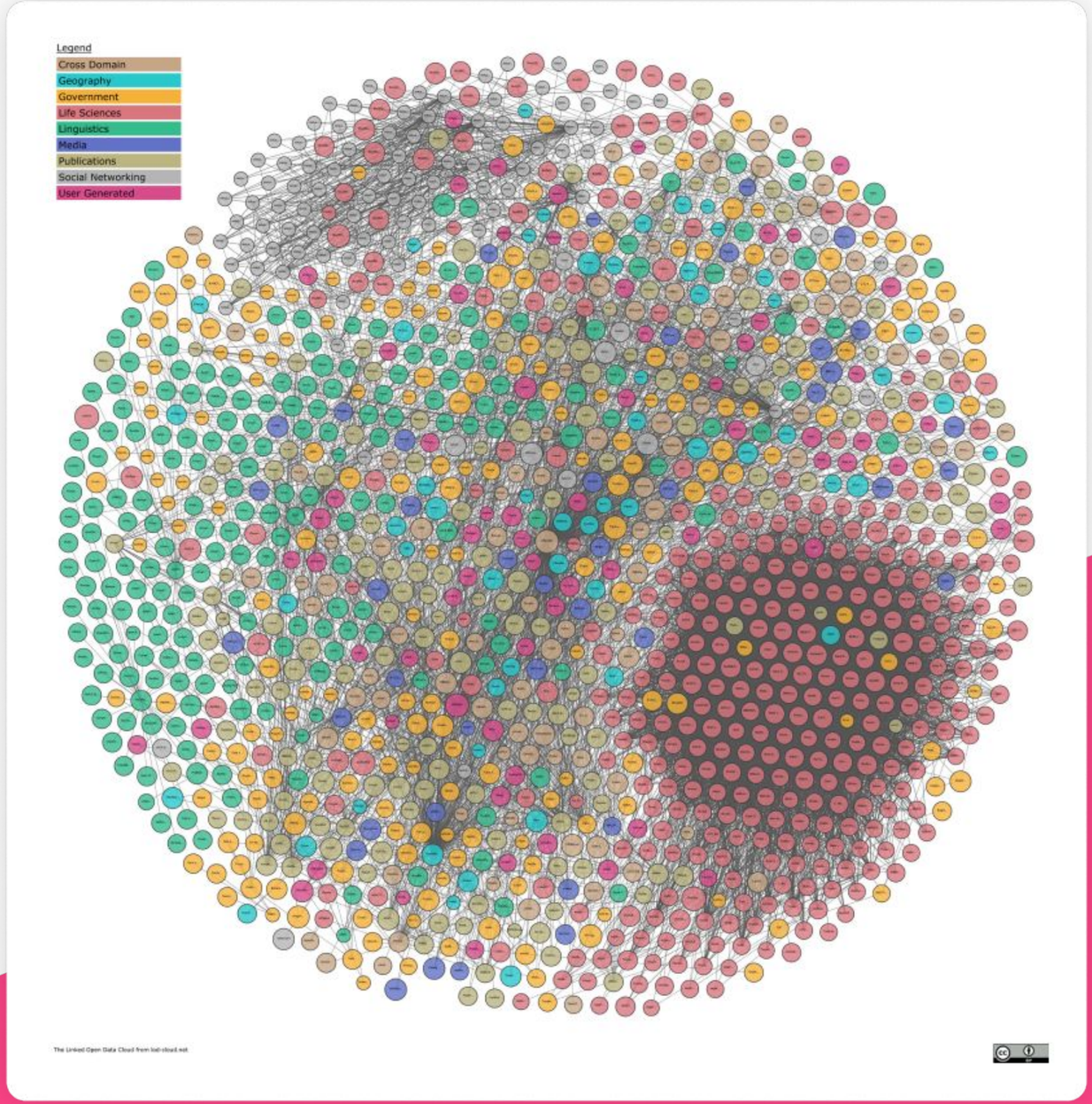
Open Data

Data can be freely used and distributed by anyone.

2

Problem

Data can be linked to realize an Open Data Cloud.



Problem

However, Linked Open Data and Semantic Web lack privacy and data integrity components.

Data are linked by solid lines,
so human space does not exist.

Verifiability of where the data was generated,
by whom, and whether it has been edited
or tampered with.

Problem

Linked Open Data + Privacy

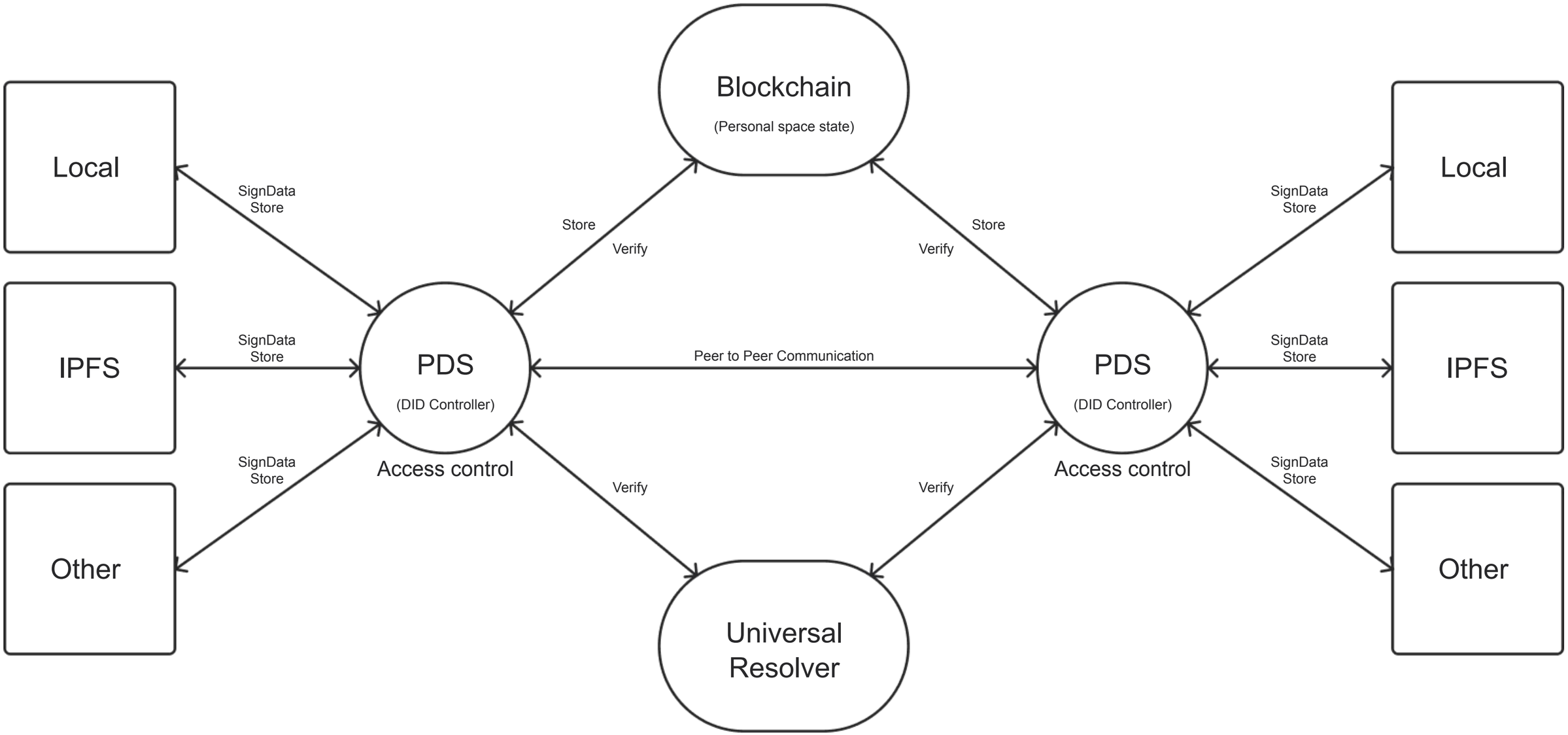
=

Web connected by a dotted line

The data are always connected by dotted lines, but can be made into solid lines by human will and can be returned to dotted lines by human will.

Combining cryptography and blockchain technology to store data state, Monas proves integrity by making it verifiable.

Architecture



Core function

- Decentralized Identifier(DID)
- Cryptree
- Peer to Peer Network
- Storing state

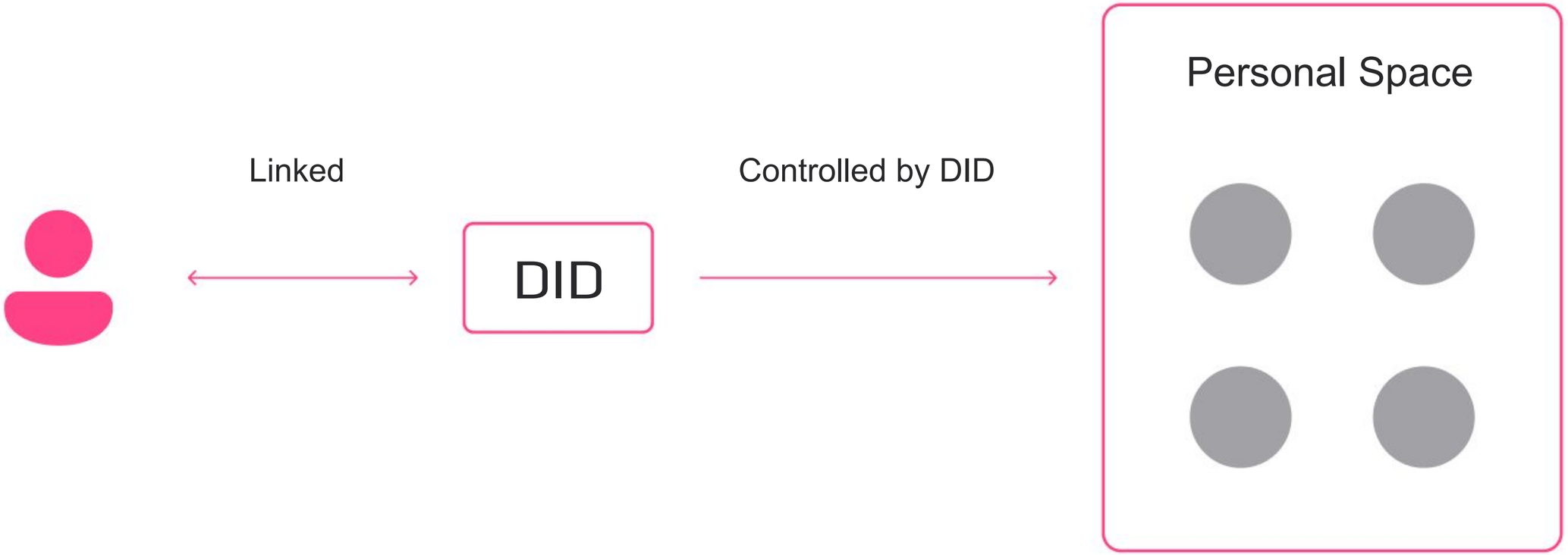
Core function - Decentralized Identifier (DID)

Decentralized Identifier

- A DID refers to any subject as determined by the controller of the DID
- DIDs have been designed so that they may be decoupled from centralized registries, identity providers, and certificate authorities
- The controller of a DID can prove control over the DID without requiring permission from other parties

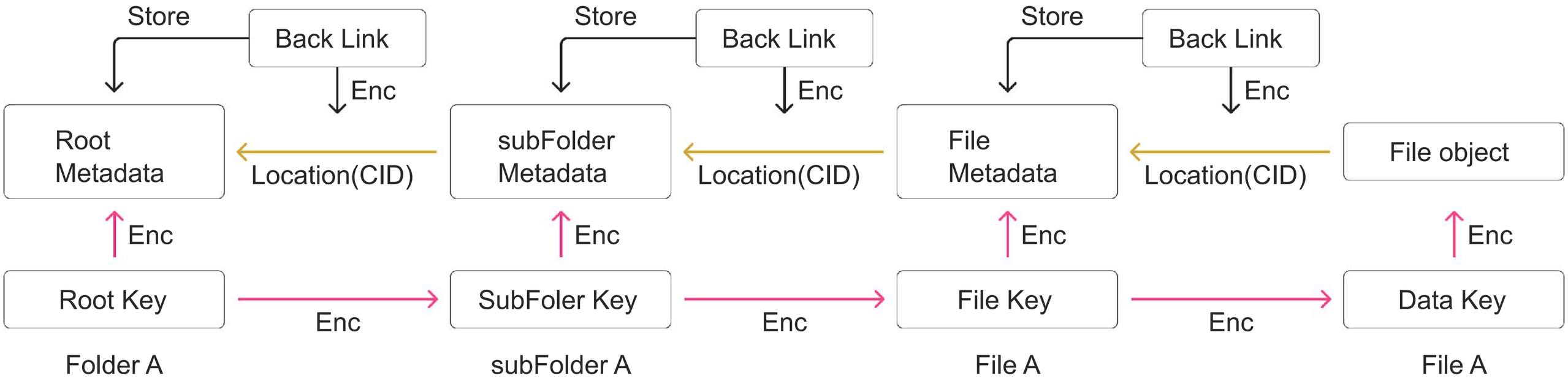
Core function - Decentralized Identifier (DID)

Personal space control by DID



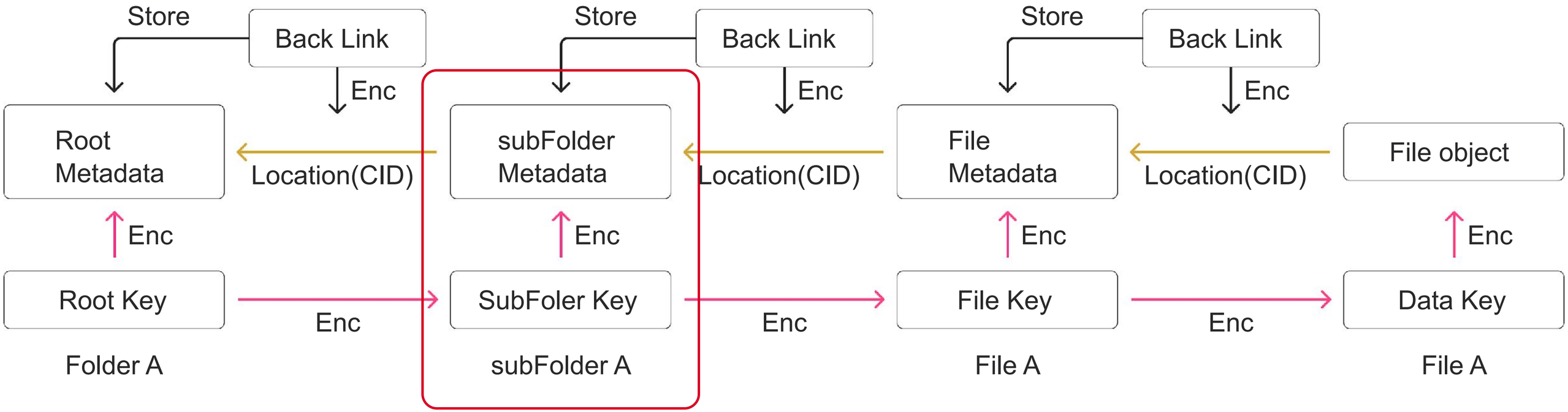
Core function - Cryptree

Directory structure : FolderA/subFolderB/FileA



Core function - Cryptree

Directory structure : FolderA/subFolderB/FileA



⇒ The entire lower layer is shared by sharing the FolderB key.

Core function - Cryptree - Accessibility

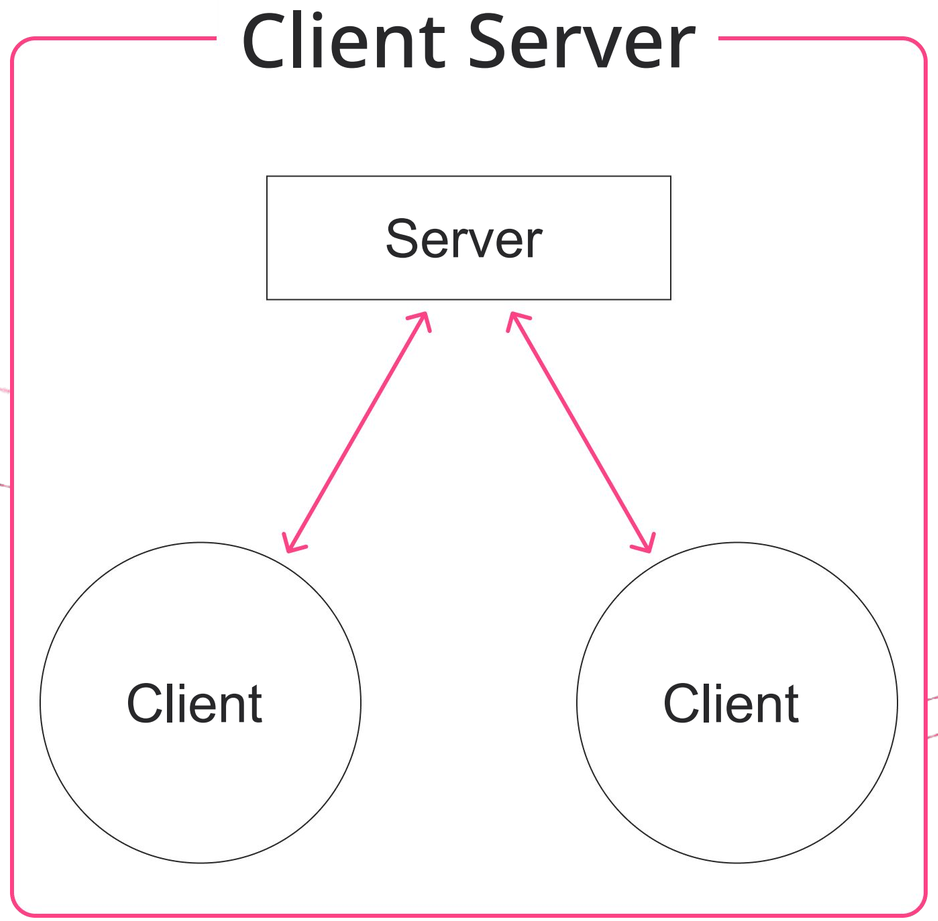
Each key is linked on the Tree
so that multiple data can be shared
with a single key.

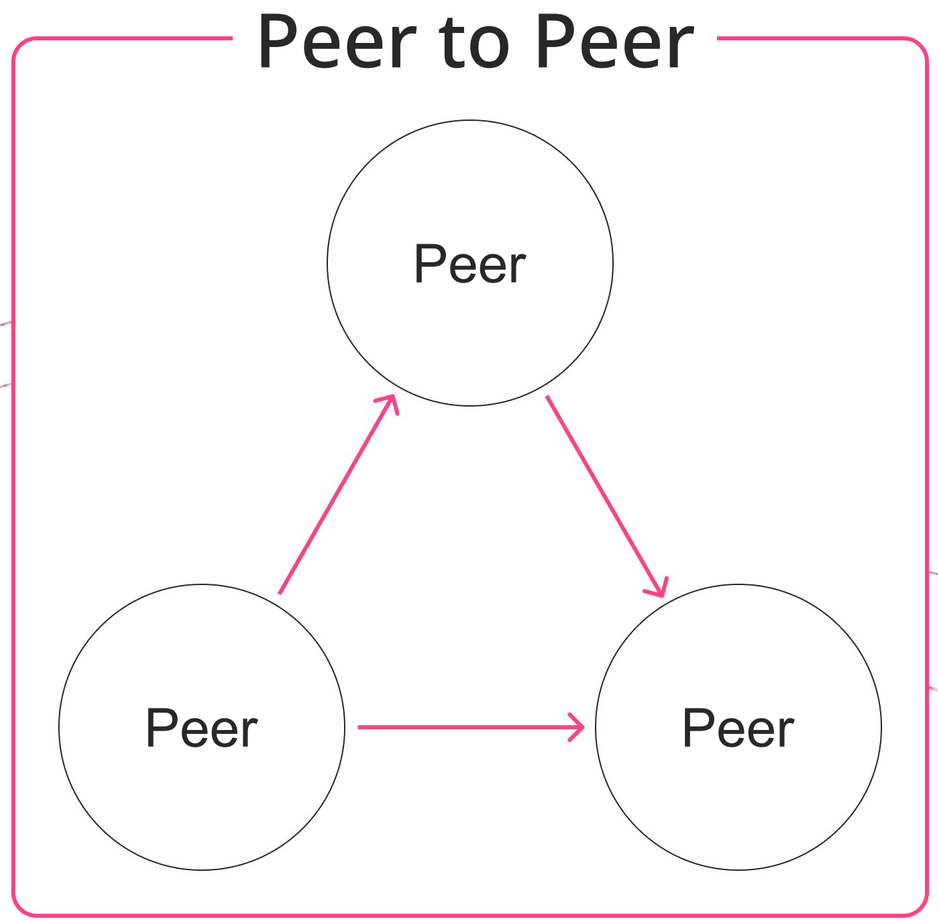
= Cryptographic Data Structures

↓

Monas implements Cryptree as a core functionality, enabling
access control to multiple data with a single key.
This allows users to intuitively control access to personal data.

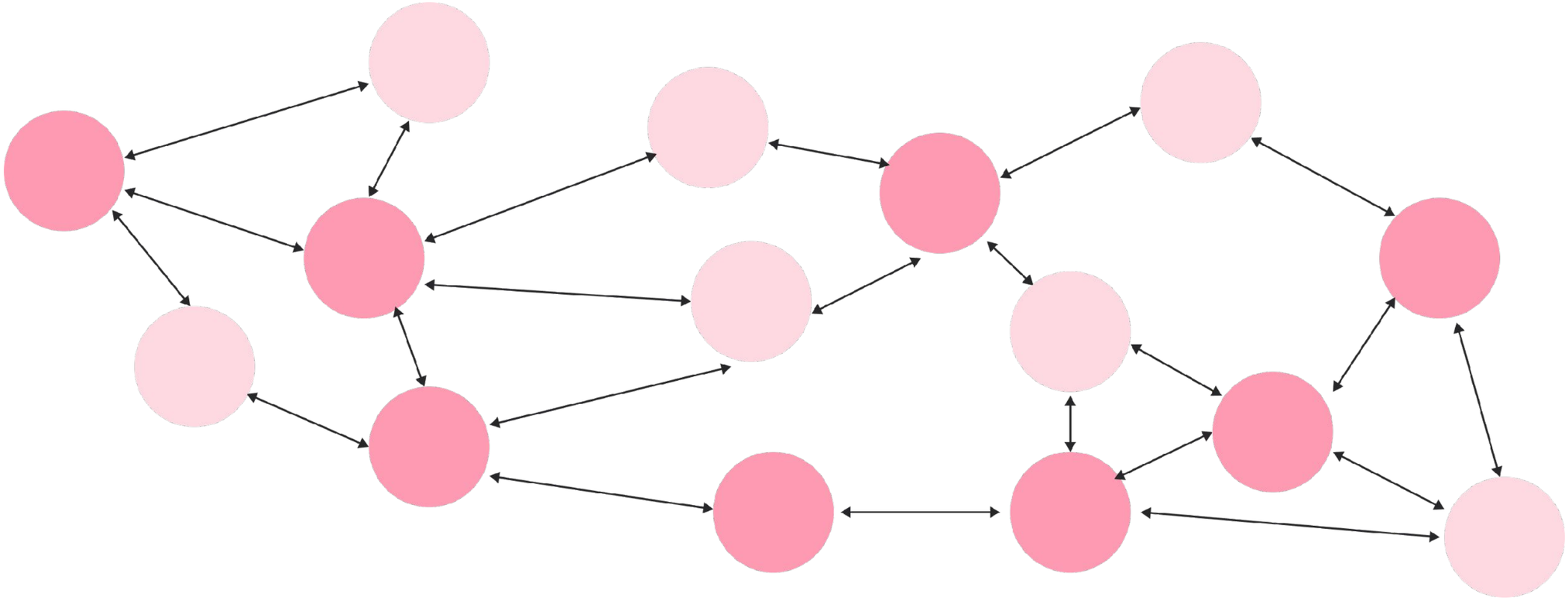
Core function - Peer to Peer Network





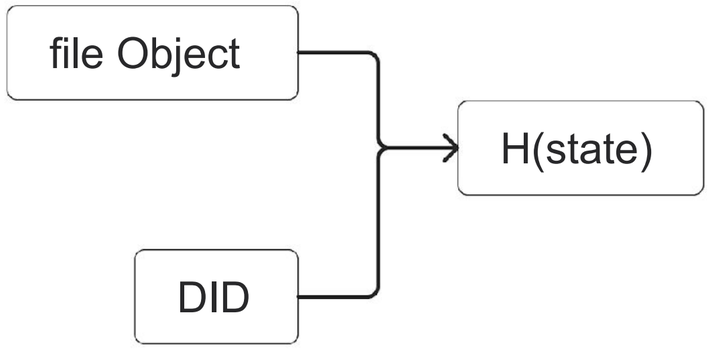
Core function - Peer to Peer Network

Each Peer on the network has its own Personal Data Store functionality. By building a Peer to Peer network, data interoperability between different platforms is realized via Peers.

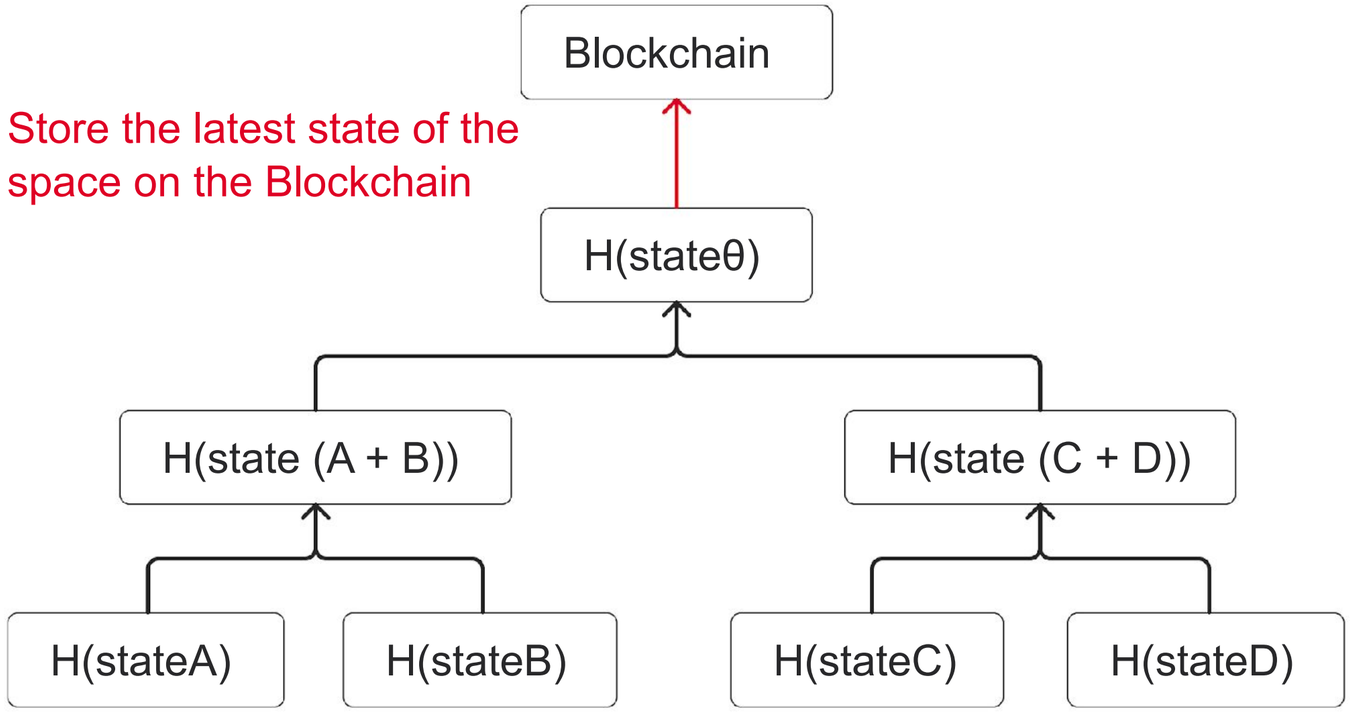


Core function - Storing state

Monas stores PDS state on the Blockchain for authenticity and consistency on the Monas network.



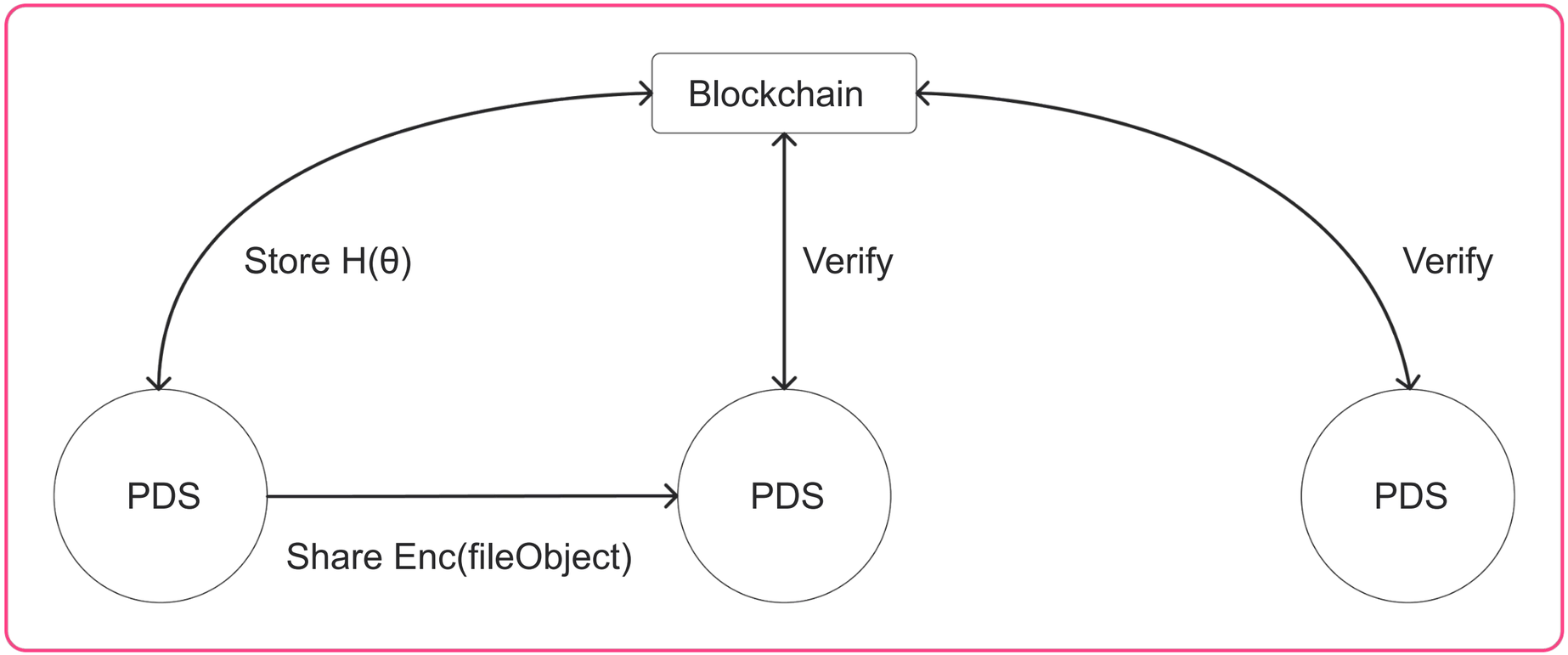
Generate hash value from fileObject and DID



Core function - Storing state

Those who are granted access to the space can verify that the space is up-to-date.

Blockchain makes it possible to verify the consistency of each space on the Monas network.



Monas facilitates the transfer of data between different services.
Developers can develop on Monas and by default have
a dotted line between different platforms and applications.
This grants all platforms or applications the potential right
to access user data, based on user consent.
Monas enables the Meta-Platform.

Currently status

Development of prototypes(Monas app)

- EOA Authentication
- Cryptree Implementation
- Smartcontract development on Filecoin

Monas is OSS.

Media

・X(Twitter)

@monas_pds

GitHub

https://github.com/Monas-project