

ABOUT ME

もみやま しょうだい
樫山翔大

所属

九州大学工学部地球資源システム工学科 B4

専攻・研究

地球熱システム学研究室

地熱貯留層・坑井間の連成流動シミュレータの開発

趣味

サッカー、バックパッカー、サウナ、筋トレ、アニメ

2023 経産省AKATSUKI事業 Osaka web3

2024 経産省AKATSUKI事業 福岡未踏

2025 NICT SecHack365

2025 サイボウズラボユース

2025 EF core program



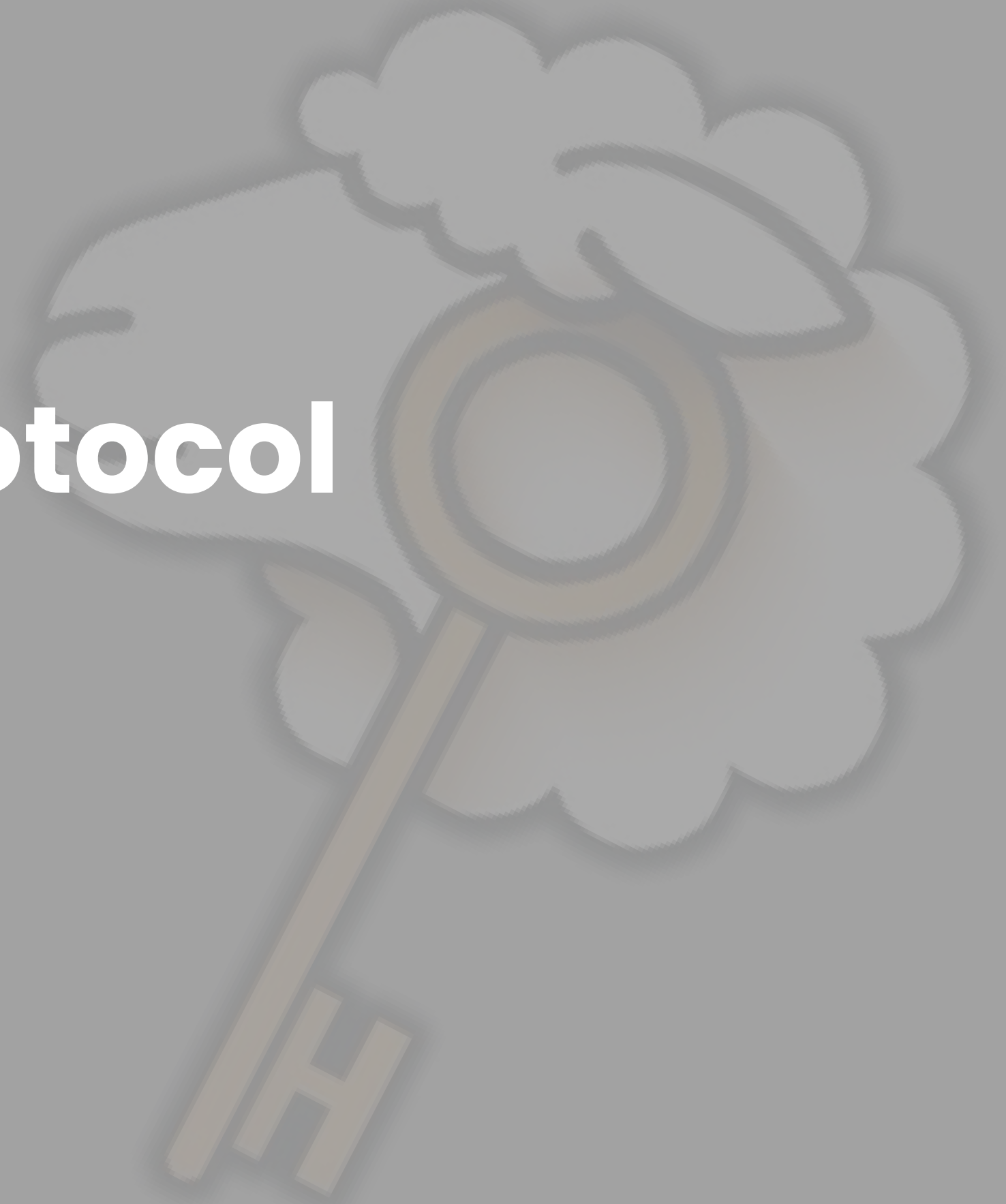
@shodaimomiyama



@ShdMmym



- **Crypto Shepherds Protocol**
- **D-TPRES**



ABOUT CRYPTO SHEPHERDS

分散型ストレージにおける
暗号化キーの共有不要なフォルダ共有ミドルウェア

ライブラリをインストールして
フォルダ構造とアクセス制御条件を設定するだけで
永続的に分散型アクセス制御付きのデータの保管を実現

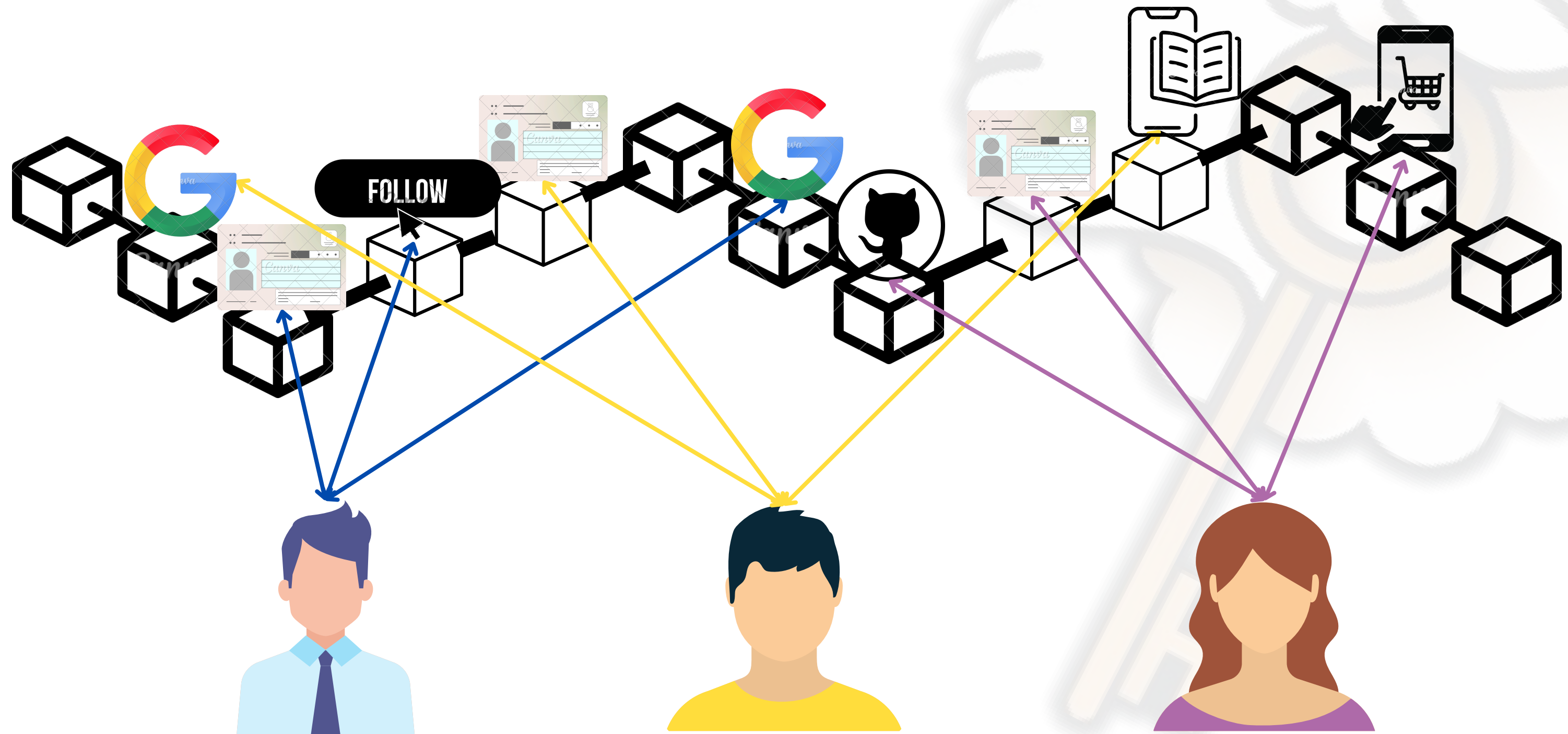


アカウントのいらないデータ共有

分散型のGoogle Drive

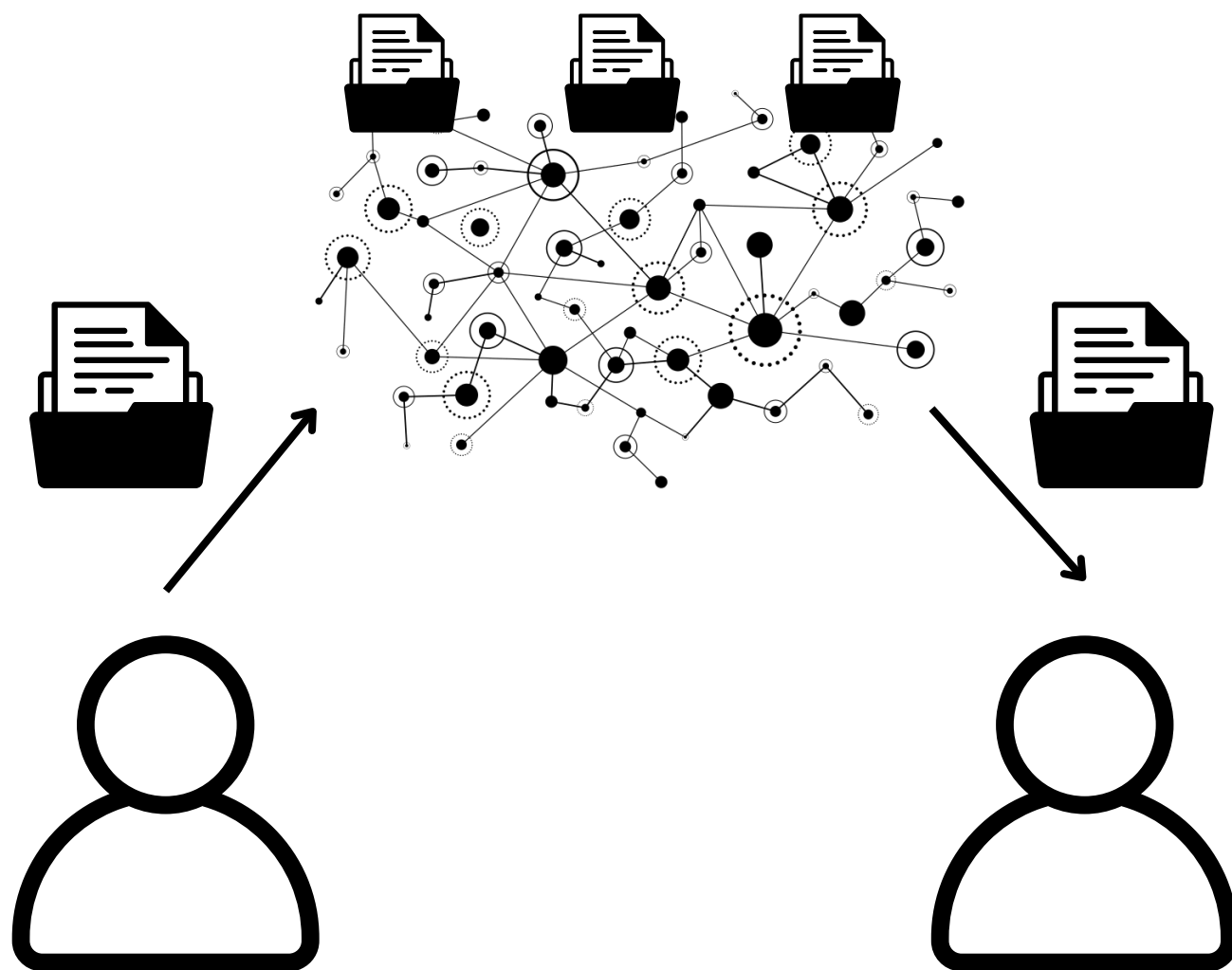
CryptoShepherdsが変える価値観

すべての出来事がオンチェーンで検証できる近い未来。
私たちのデジタル活動にプラットフォームの壁はもうない。

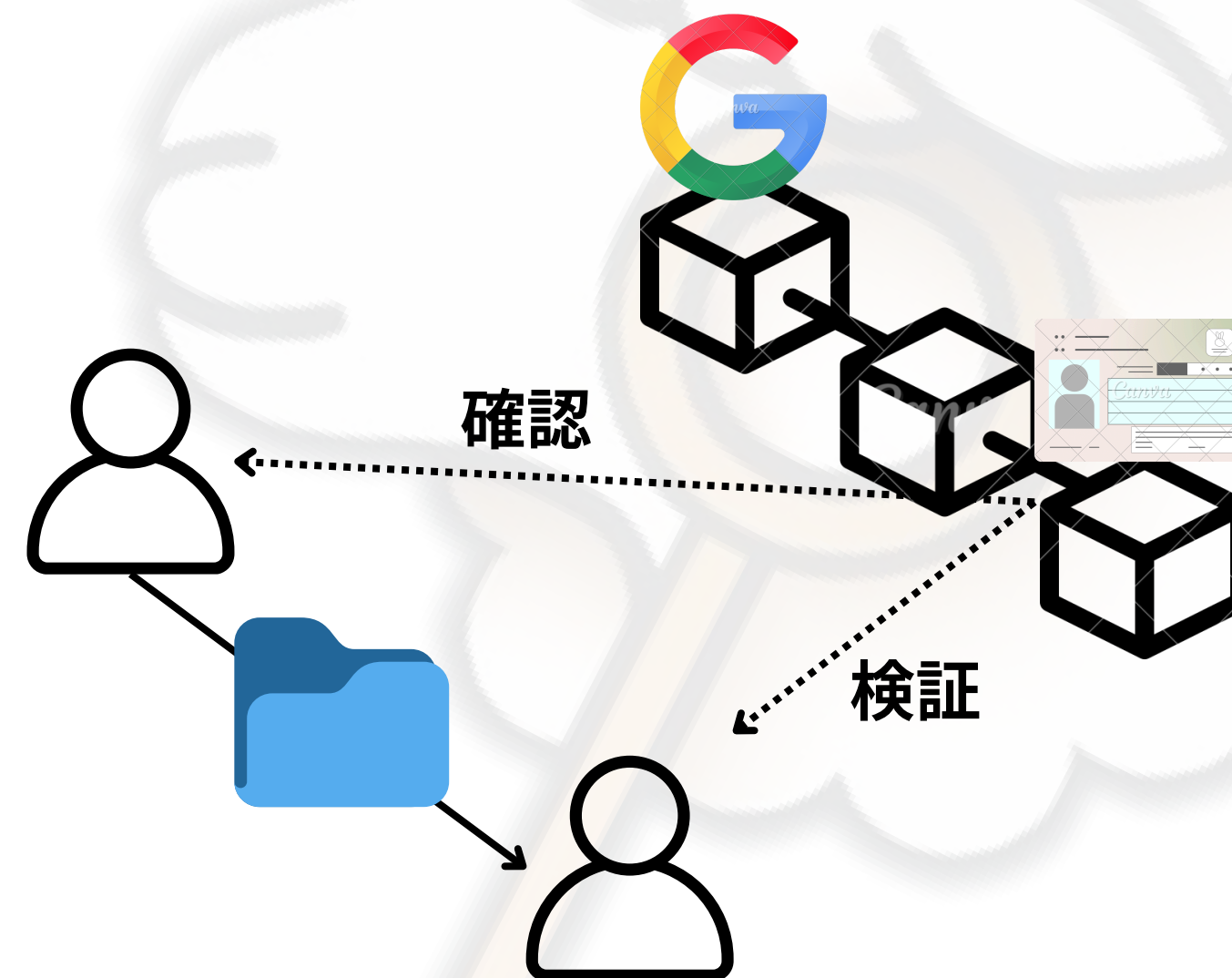


CryptoShepherdsが変える価値観

アカウントがいないデータ共有。分散型のGoogleDrive。



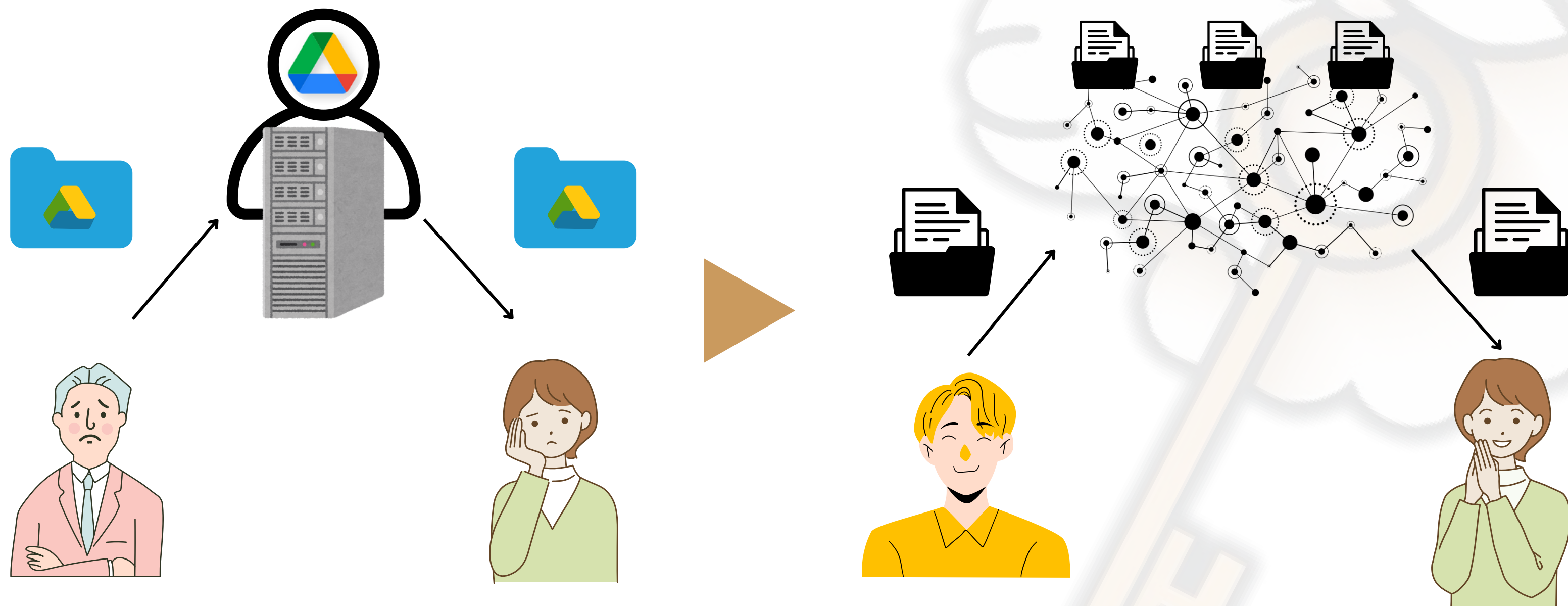
事前セットアップがなく共有できる



異なるアイデンティティやイベントの
検証をもとに共有できる

CryptoShepherdsが変える価値観

プロバイダーを介さない、渡したい人と欲しい人の二者間で行うデータのやりとり



CryptoShepherdsのユースケース

分散型のデータ制御で生まれる新しい経済活動

Balance

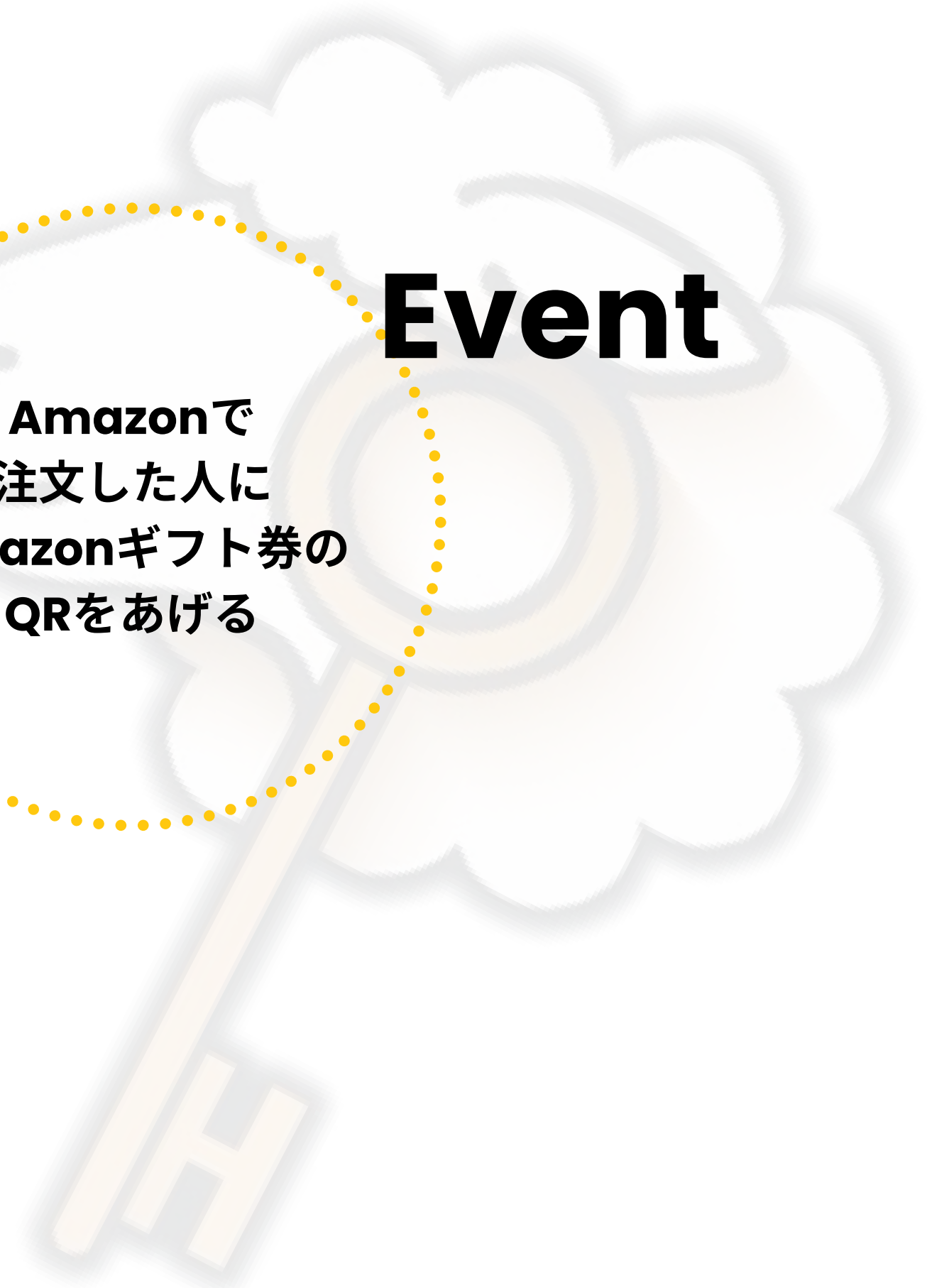
ファントークンを
会員証にした
ファンコミュニティへの
限定コンテンツ

Event

Amazonで
注文した人に
Amazonギフト券の
QRをあげる

ID

マイナンバーをIDとした
重要書類の送付



CryptoShepherdsのユースケース

マイナンバー（マイナウォレット）検証による医療カルテの共有

医療カルテ共有システム

カルテ作成・共有設定

カルテデータへのアクセス

患者フォルダ作成

患者名：

例：山田太郎

フォルダパス（任意・上書き）：

例：/山田太郎/2023-08

患者ウォレットアドレス（共有条件）：

例：0xABC...123

フォルダ作成

医療カルテの保存

ファイル名：

例：record.txt

カルテ内容：

診断結果や治療内容を入力...

医療カルテを保存

より自由度の高いデータ共有

分散型のGoogle Drive

分散型のデータ制御とは？

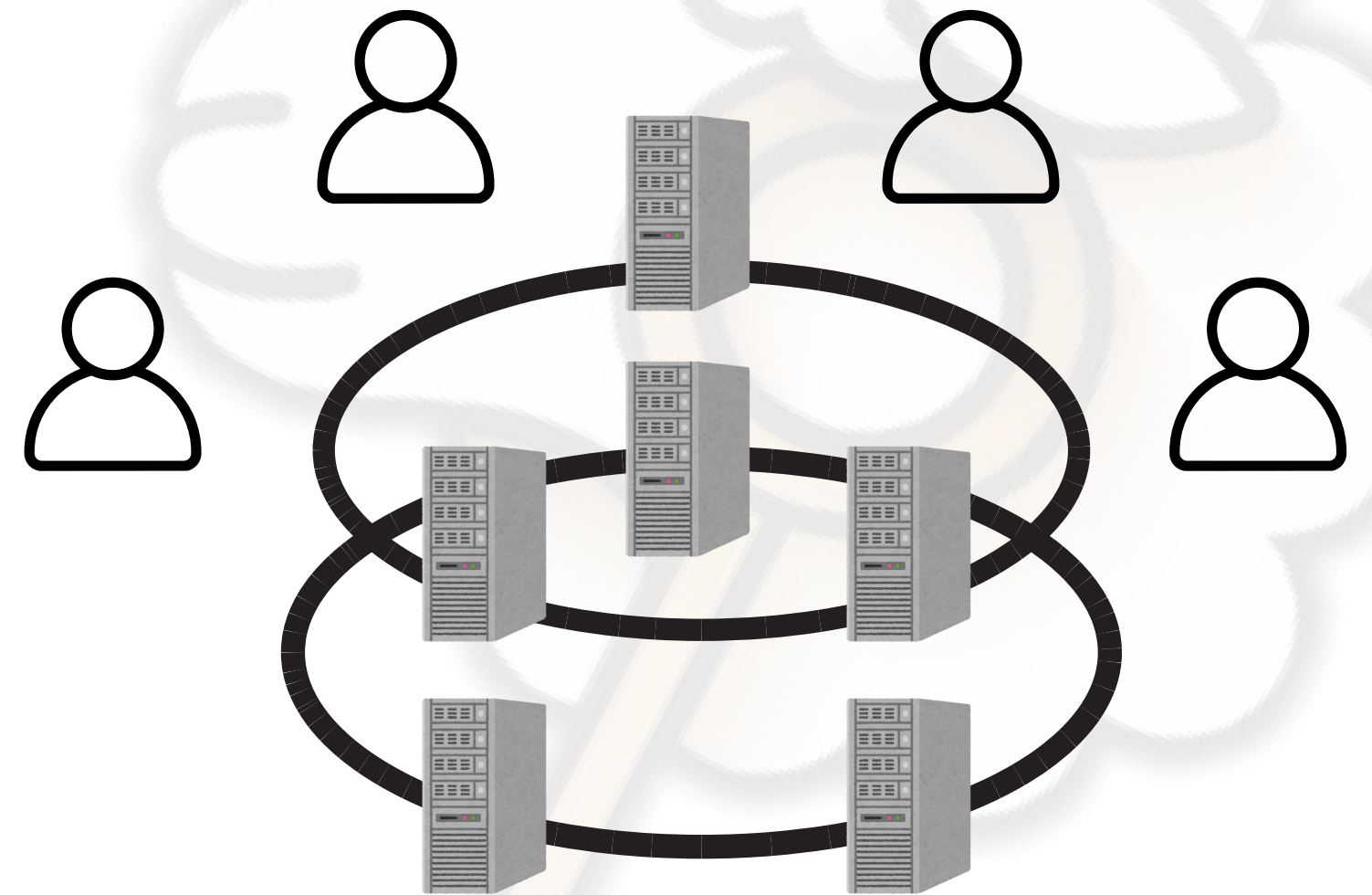
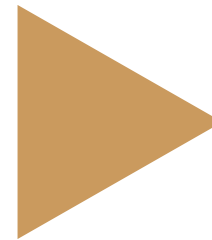


従来型のデータ制御と比較した分散型のデータ制御

アクセス制御と保存をどちらも分散型で行うことで、よりデータの制御を主権的に。



単一のプロバイダーが行っていた
データのアクセス制御と保存を



「アクセス制御」と「保存」の
2つのレイヤーの複数ノードで分散型で行う

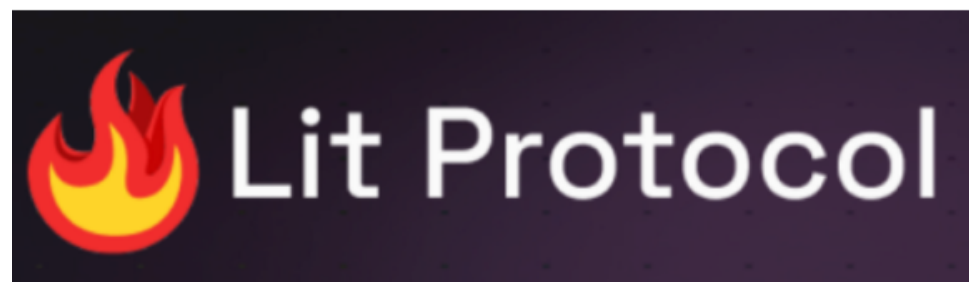
データの制御を分散型で行う

複数のプロトコルを横断的に使用する必要がある

デジタルコンテンツ



分散型アクセス制御



分散型ストレージ

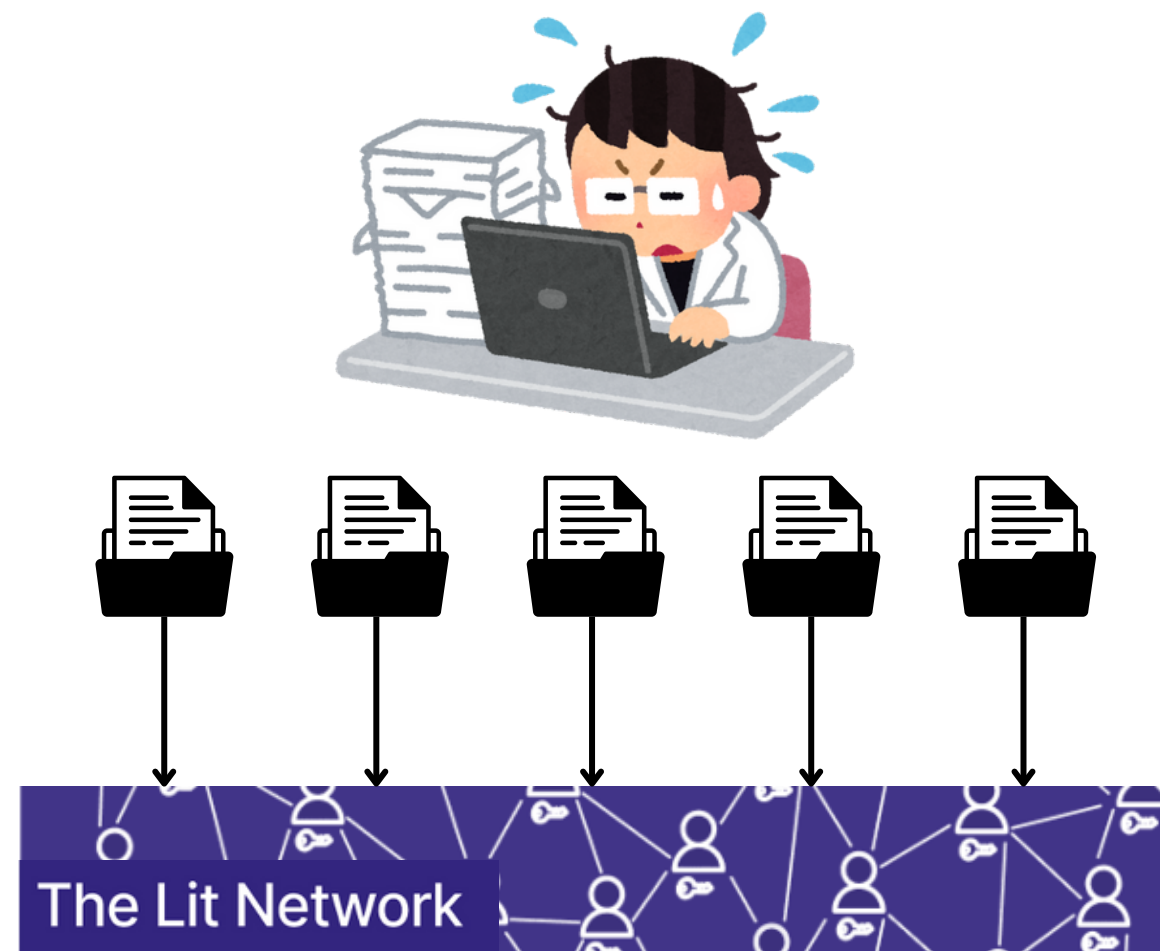


まず分散型アクセス制御を提供する
プロトコルでアクセス制御を設定

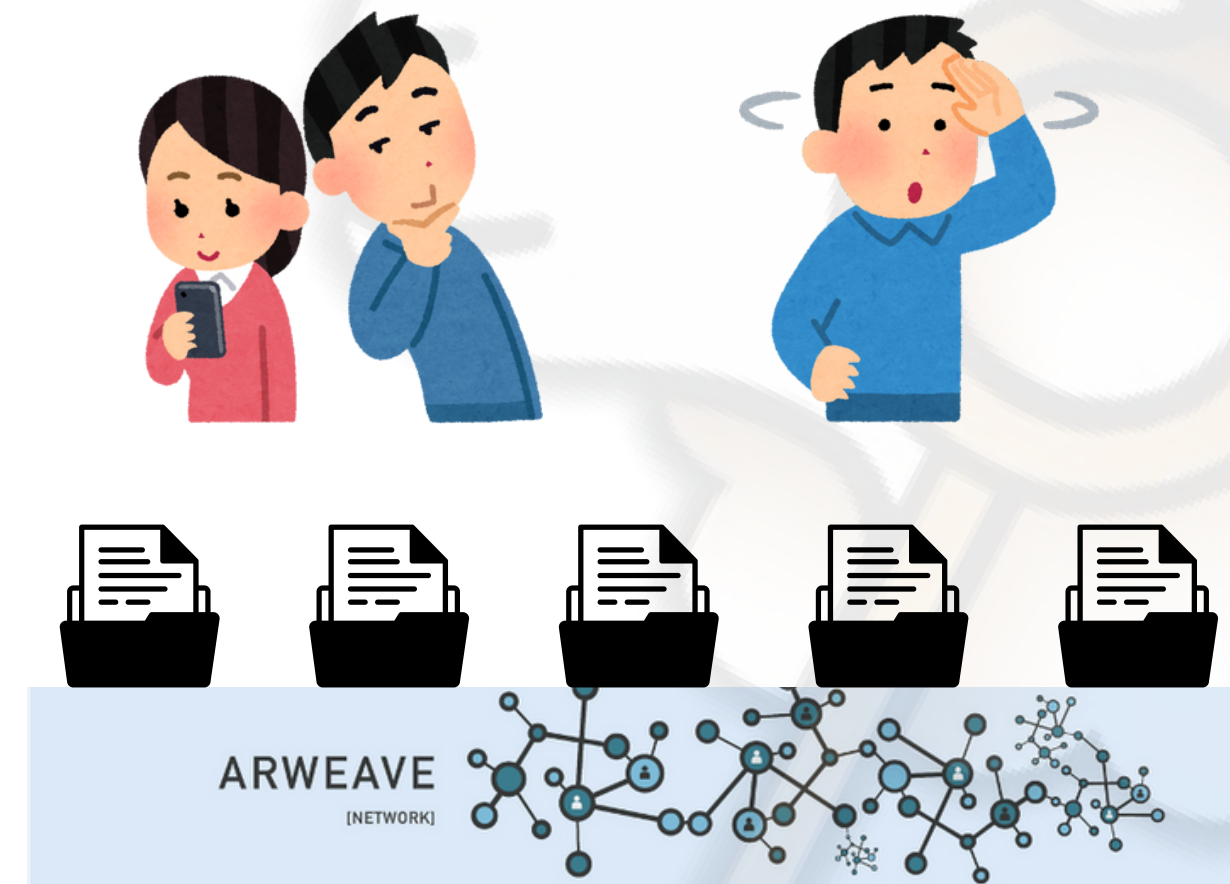
その後、分散型のストレージに
暗号化したデータを保存

データの制御を分散型で行う

現状の分散型データ制御を提供するプロトコルの課題

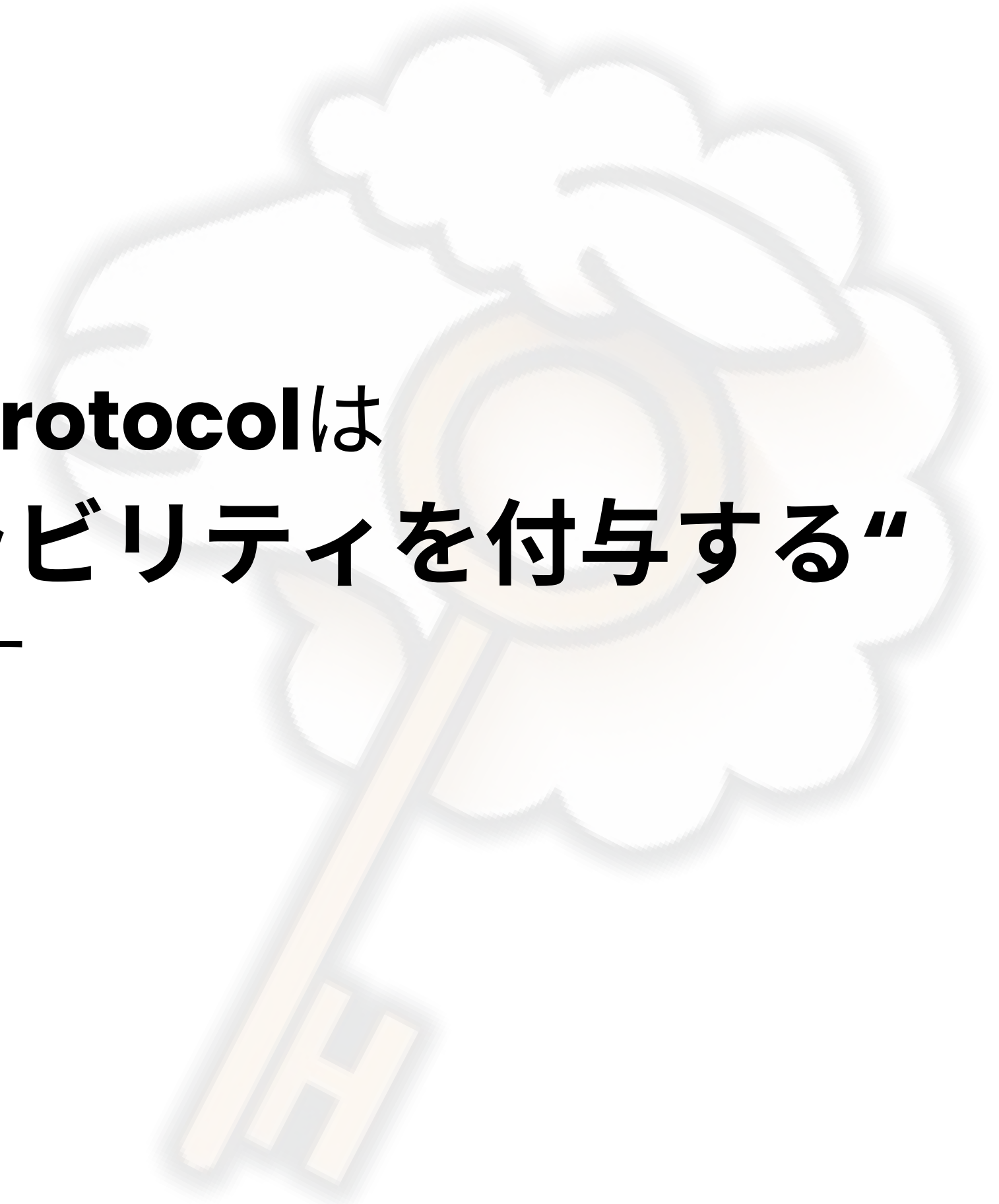


「単一データ」や「個別ファイル」
ごとに対してのアクセス制御



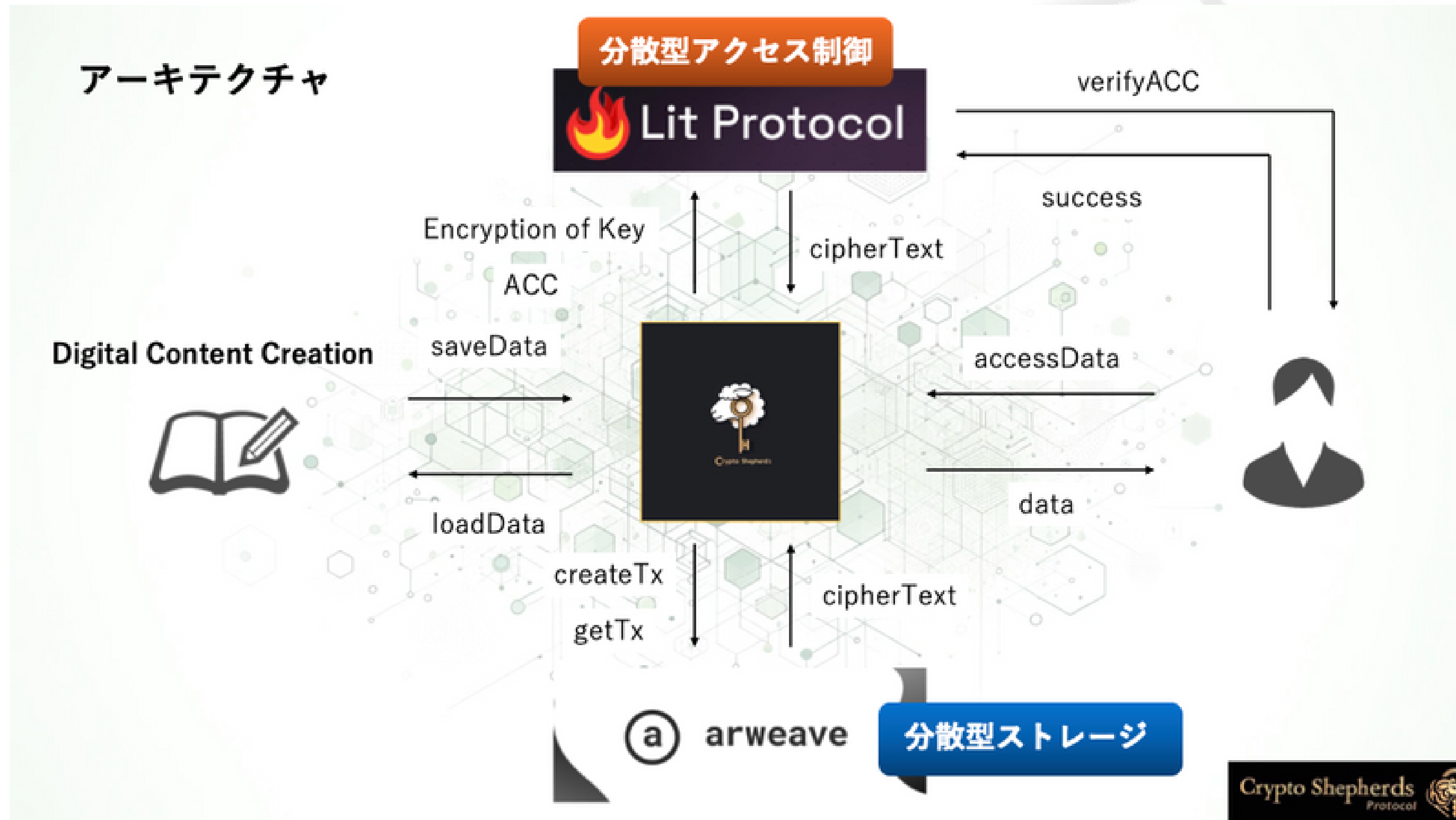
デフォルト公開性やネイティブで
データを構造的に保存できない性質

CryptoShepherds Protocolは
“分散型のデータ制御にスケーラビリティを付与する”
システムです



データの制御をCryptoShepherdsで分散型で行う

ローカルでの暗号化・復号制御、対称鍵ベースのフォルダ構造の作成、
暗号化キーを共有しない特定のフォルダに対応する対称鍵の共有



CryptoShepherds Protocolの データ制御ロジック

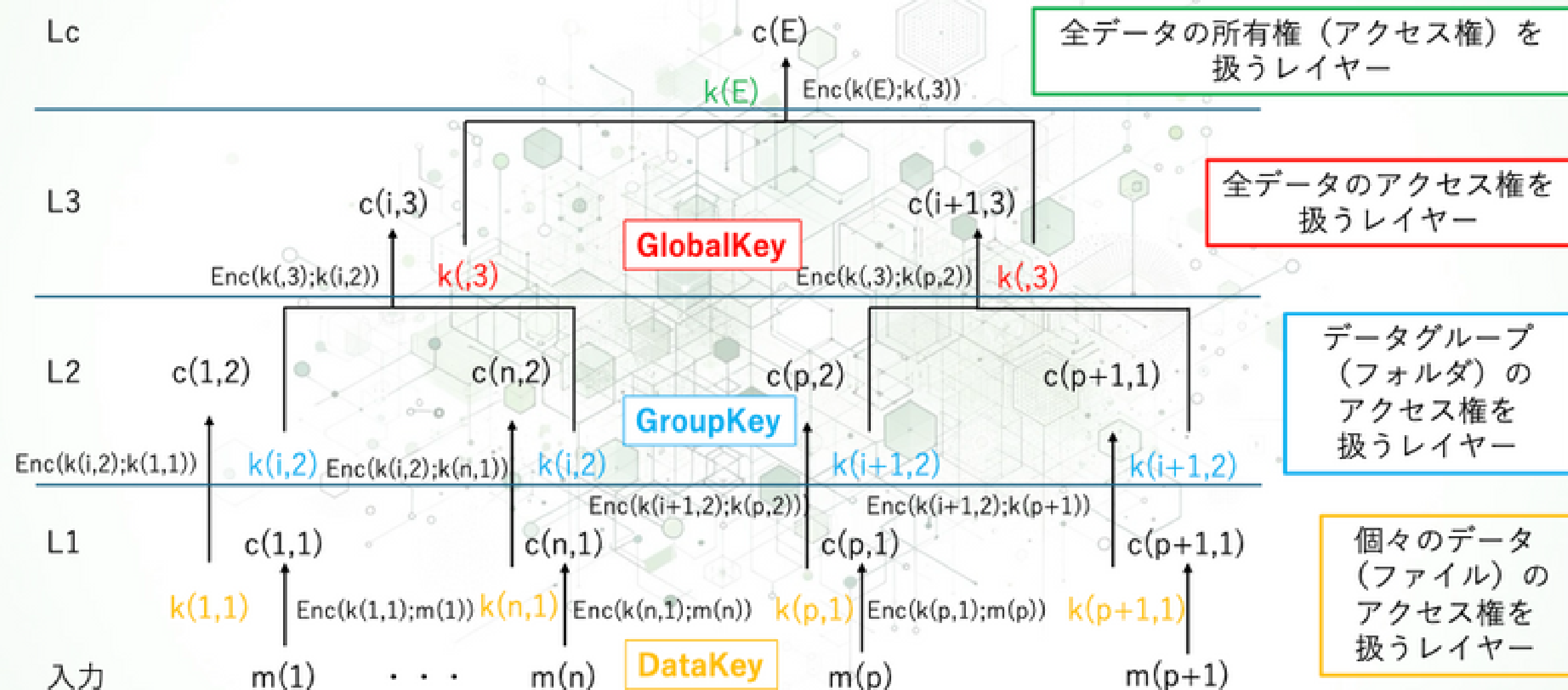


CryptoShepherdsはデータを構造的に分散型で保存する

対称鍵をベースとした階層的暗号化構造により分散型ストレージにフォルダ構造を構築

対称鍵ベースの階層的暗号化構造によるフォルダ構造の作成

階層的な暗号化アルゴリズムとアクセス粒度

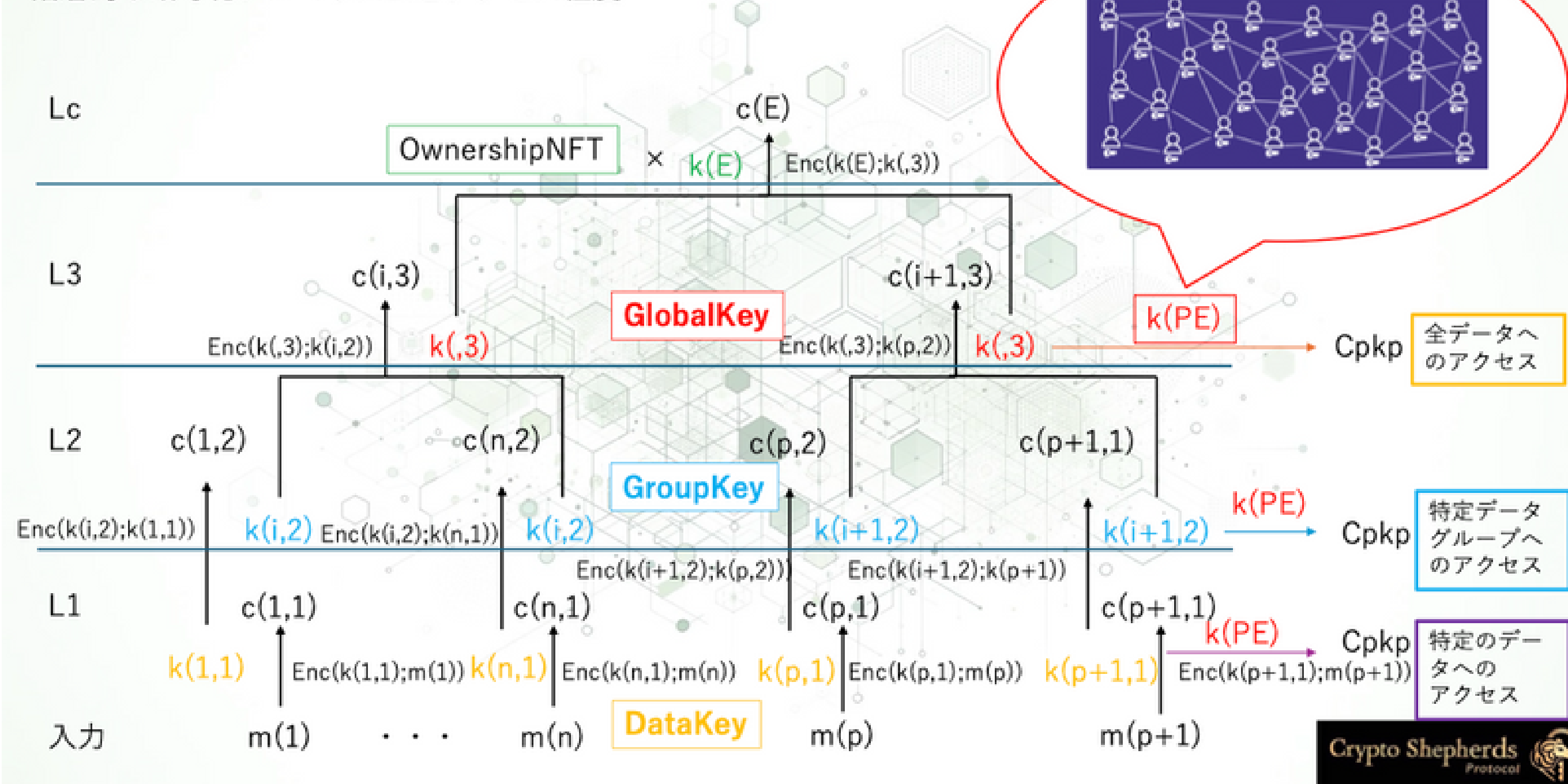


CryptoShepherdsはフォルダを分散型で共有する

単一のデータのアクセス制御だけでそれに紐づくすべてのデータを共有

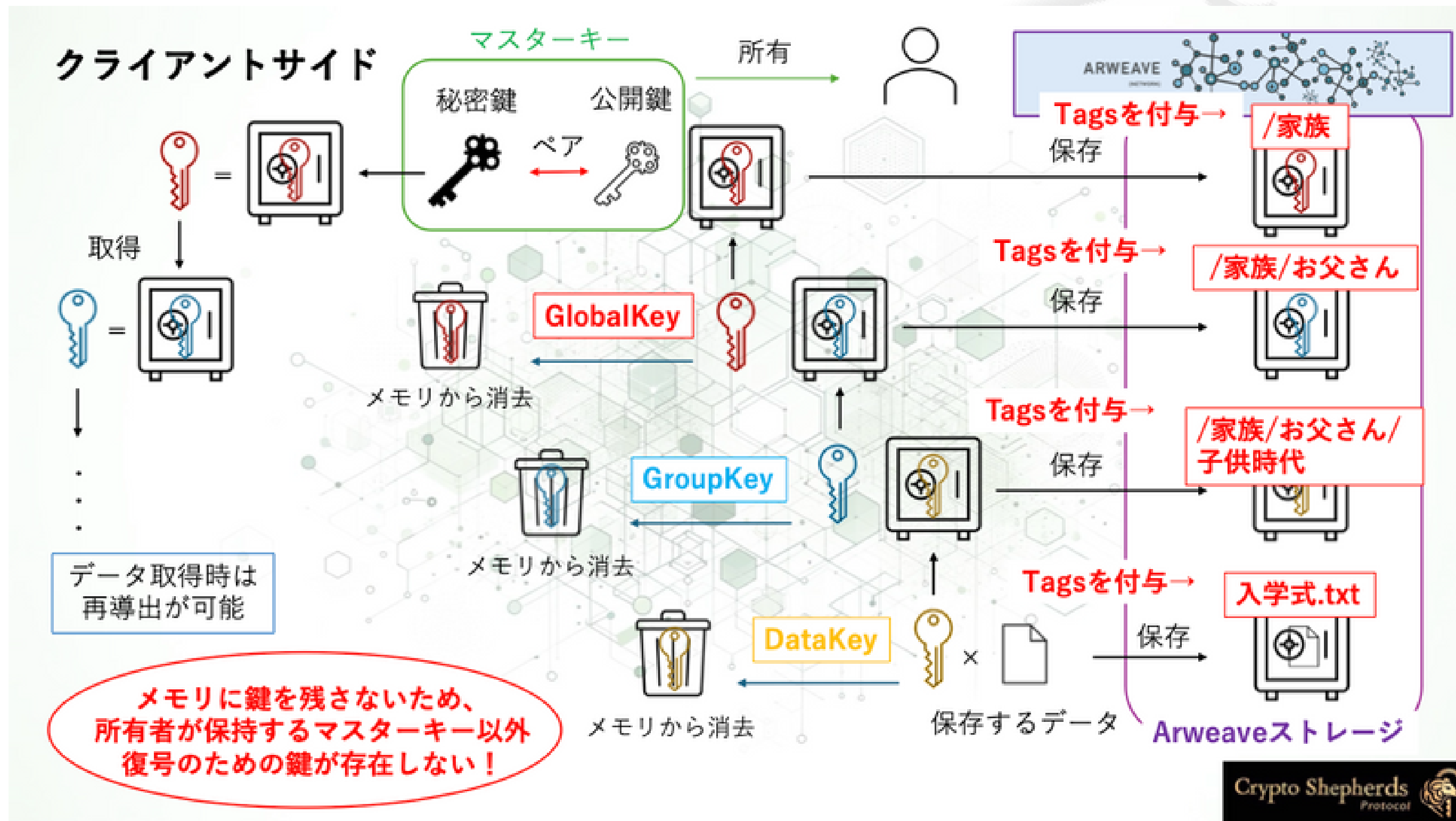
暗号化キーの共有不要なフォルダ共有

階層的な暗号化アルゴリズムとアクセス粒度



The CryptoShepherds Algorithm

順次暗号化・順次取得・順次復号



開発者体験



シンプルな6つの基本関数

学習コストゼロで、今日から分散型のデータ制御を実現

Functions for Data Owners

Creating a Folder

JavaScript

```
cs.createFolder('/path/to/folder');
```

Saving Data

JavaScript

```
cs.saveData('/path/to/folder', 'filename', data);
```



Retrieving Data

JavaScript

```
cs.loadData('/path/to/folder', 'filename');
```

Functions for Data Sharers

Sharing a Folder

JavaScript

```
cs.setShareFolder('/path/to/folder', decryptionCondition);
```

Sharing a File

JavaScript

```
cs.setShareData('/path/to/folder', 'filename', decryptionCondition);
```

Accessing Shared Data

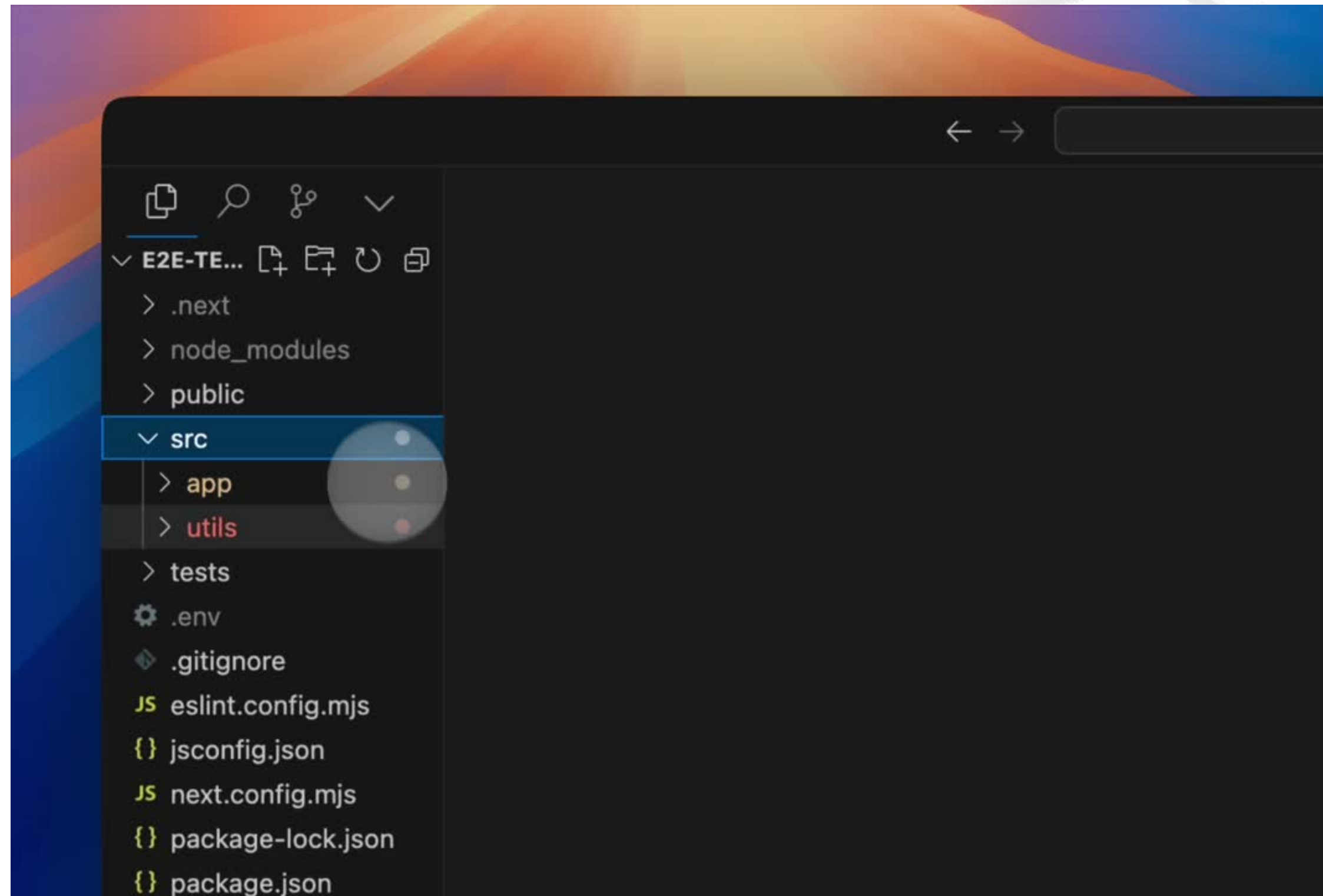
JavaScript

```
cs.accessData('/path/to/folder', 'filename');
```



柔軟なアクセス制御条件

開発者の関心ごとを「どのフォルダに」「どんな復号ロジックを付与するか」に集中



D-TPRES



サイボウズラボユースで 開発するプロダクト全体像



ABOUT

D-TPRES (Deterministic Threshold Proxy Re-Encryption System)

コントラクトで記述される公開された唯一のロジックに従った
秘密管理システム

EVMでのACC検証と、Arweave AOでの閾値プロキシ再暗号化を基盤とした秘密管理の実装により、
コンセンサスがストレージに準拠し、かつ決定論的な秘密の復元を実現するための
分散型アクセス制御ネットワーク

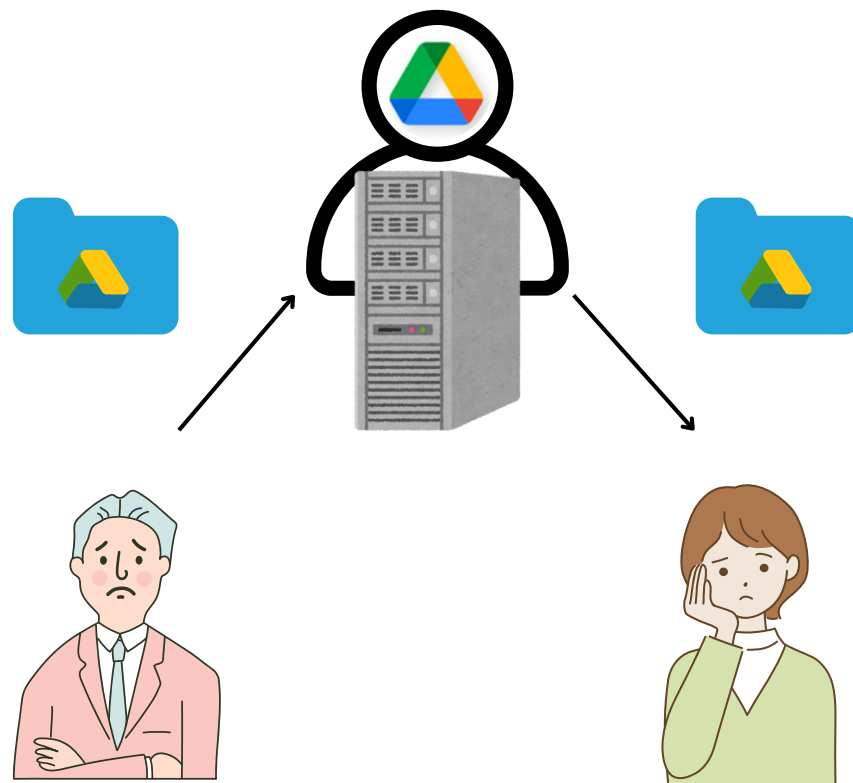


背景と課題

集中型の鍵管理のリスクと既存の分散型の鍵管理の課題

ベンダーによる鍵管理

- 各国の法令遵守によるコンテンツ削除
→ 検閲が「構造上」可能であることが社会的リスク
- 単一障害点の形成と内部の脅威
→ 攻撃の標的が定まり得ることが技術的リスク



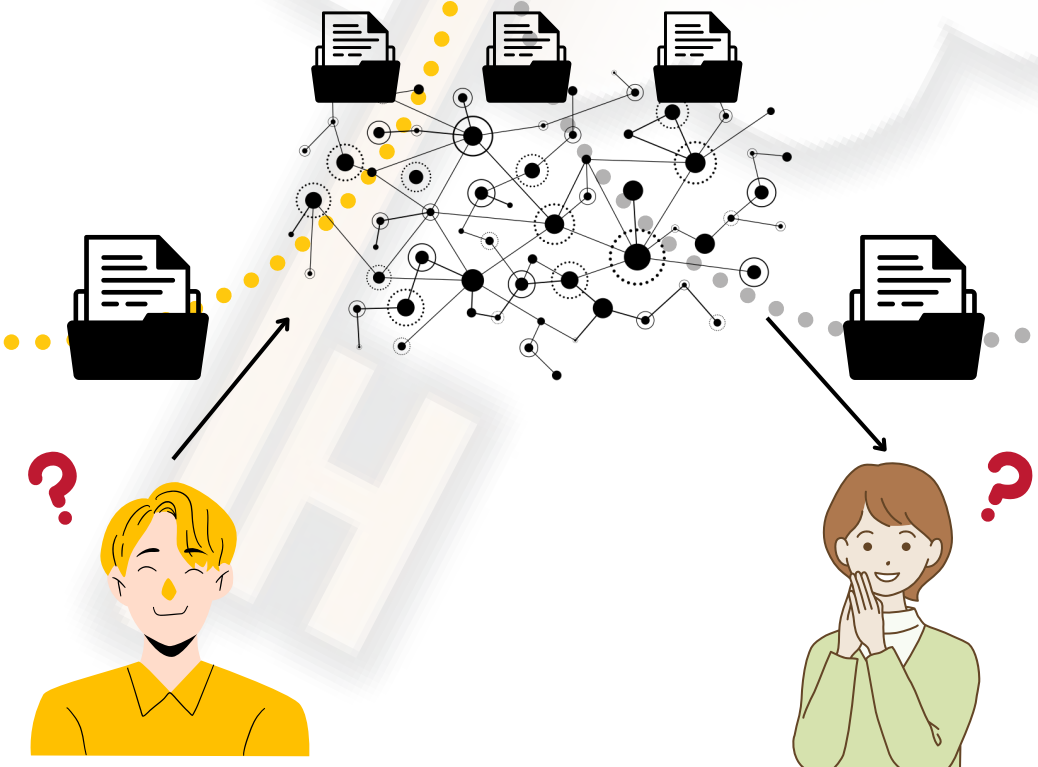
分散型鍵管理の先行事例

Lit Protocol

- TEEへの信頼依存
- 多数ノードの誠実性に基づいたJSの実行による復号の決定

NuCypher

- Ethereum上での実行コスト
- 経済的インセンティブによるビザンチン耐性の担保の困難性

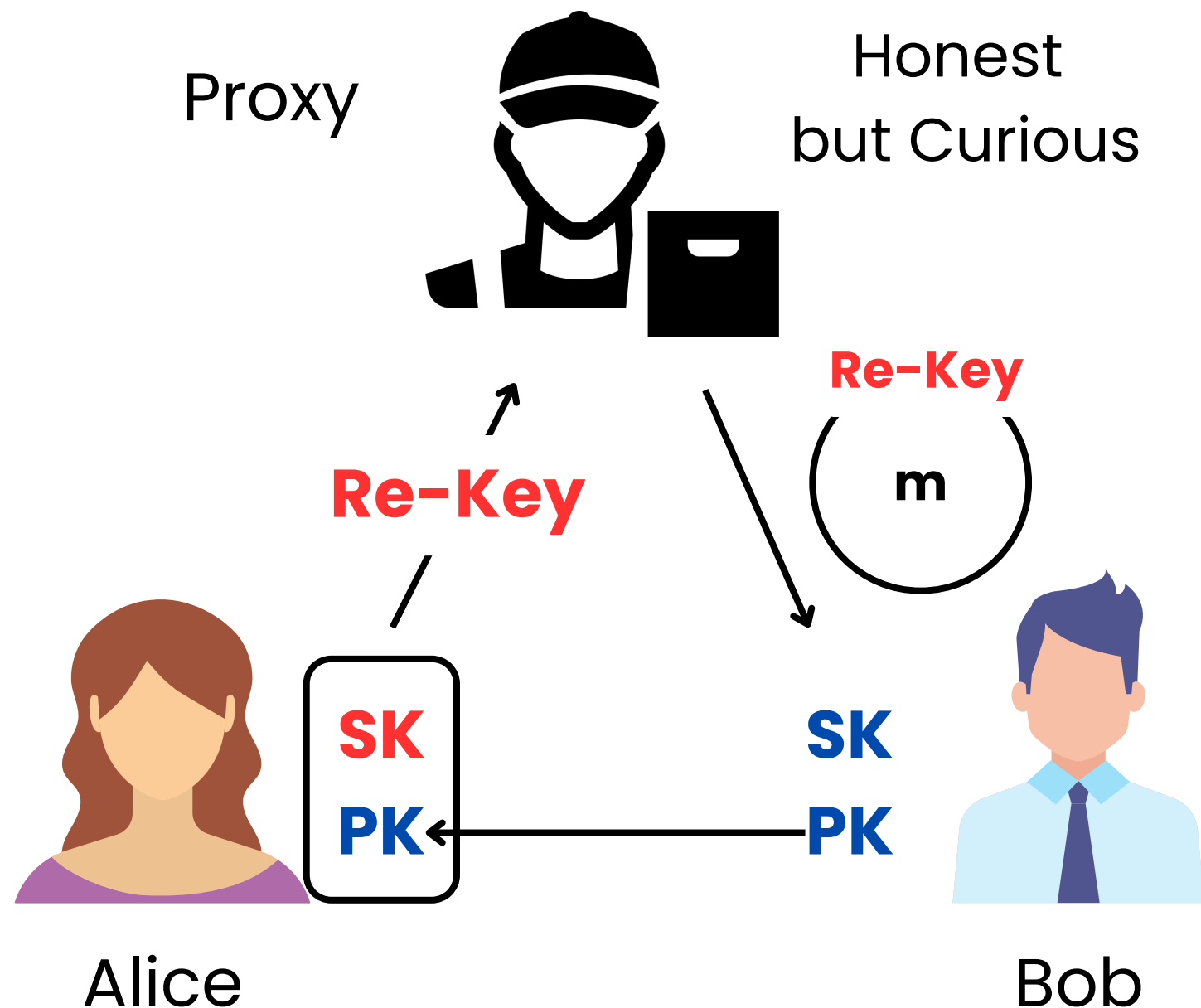


D-TPRESの基盤技術

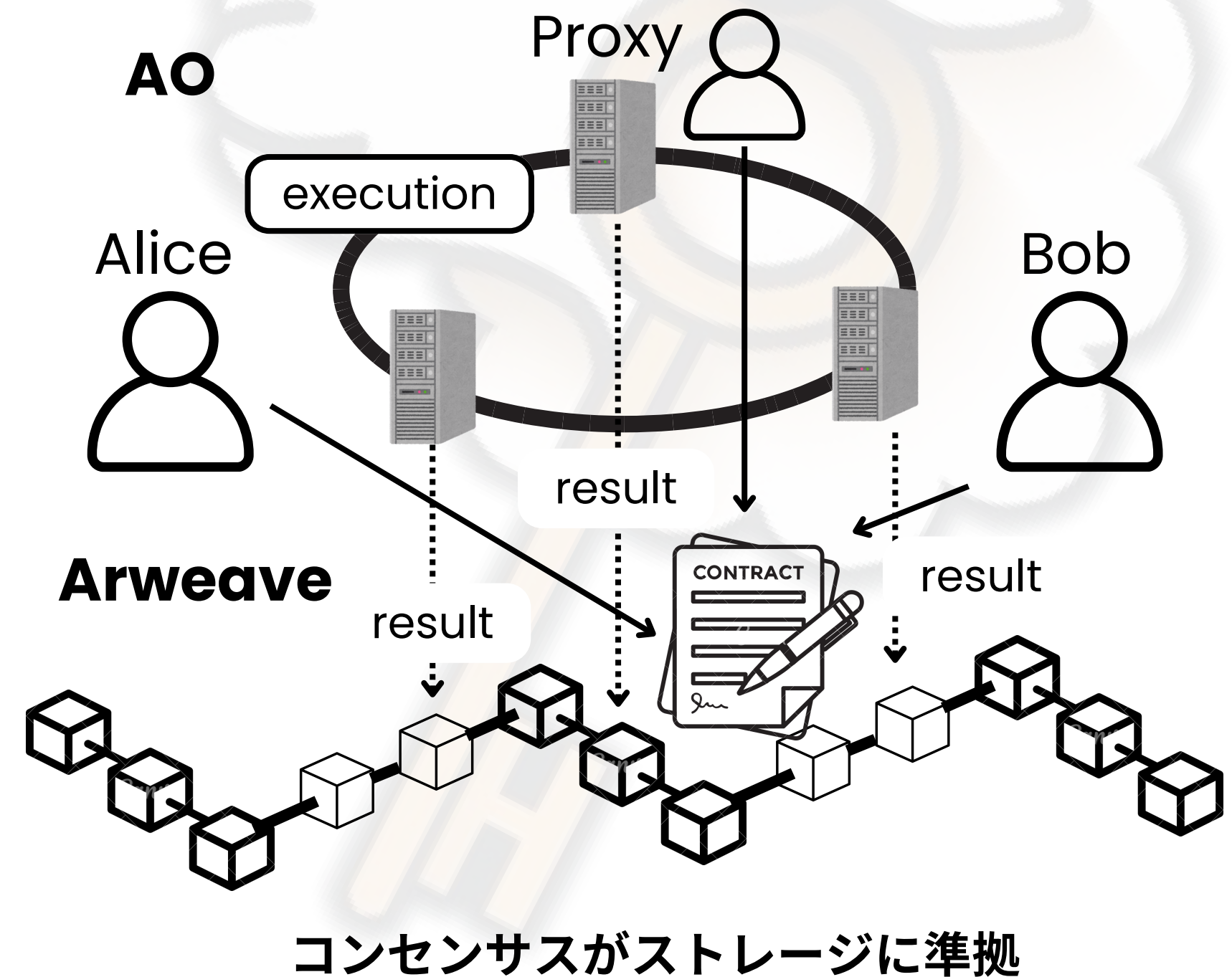
プロキシ再暗号化とArweaveとAO

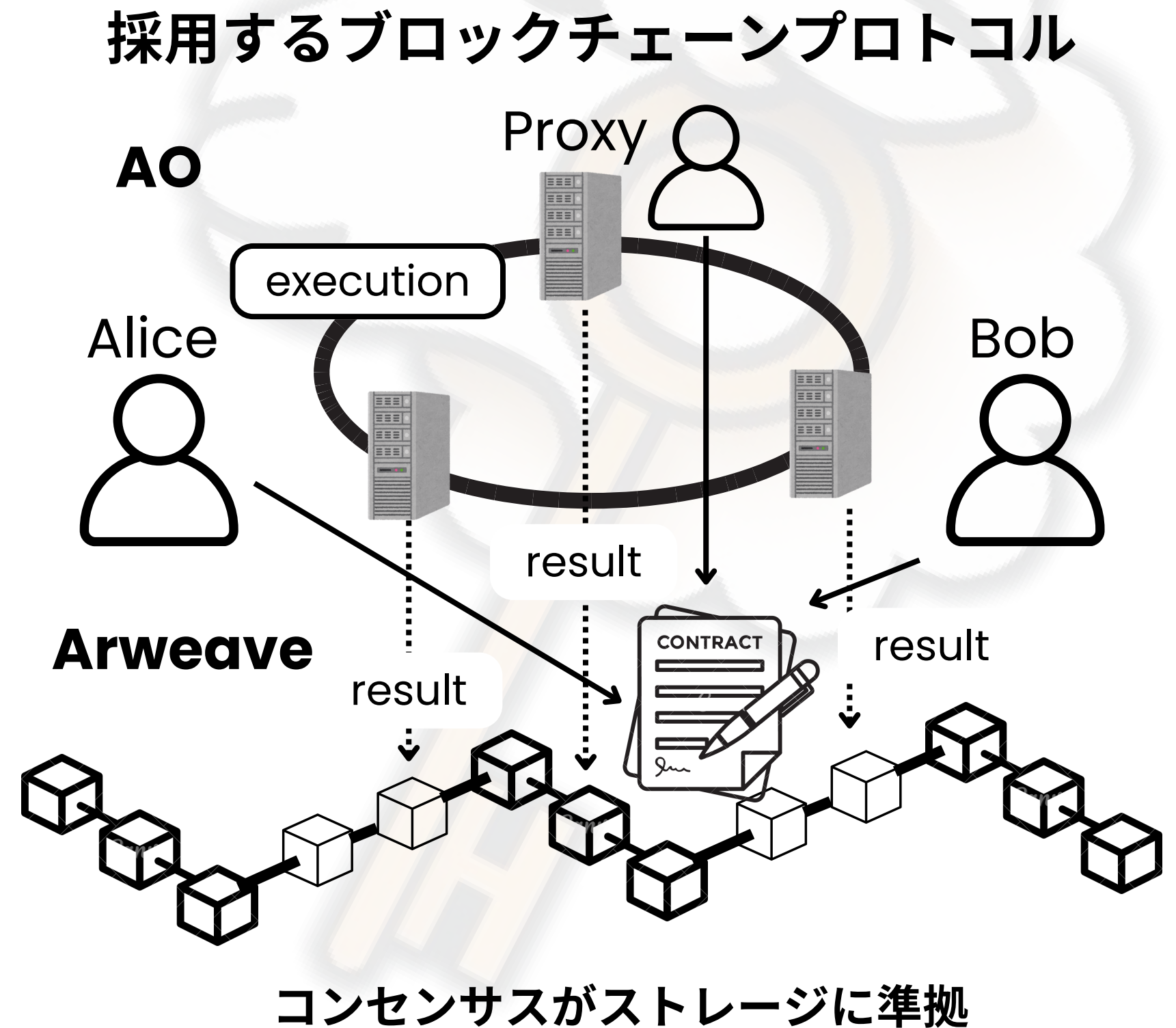
採用するプリミティブな暗号技術

Proxy Re-Encryption



採用するブロックチェーンプロトコル





Docs

 CryptoShepherds Protocol Tutorial  

CryptoShepherds Protocol

スケーラブルな分散型のデータ制御

CryptoShepherds Tutorial - 5min 



分散型のデータ制御

アクセス制御と保存を分散型で統合的に行うことができます。



柔軟な復号条件

オンチェーンでの検証から、apiを呼び出したオフチェーンコードの実行まで、あらゆる復号条件を設定できます。



シンプルなSDK

6つの基本関数からなるシンプルなSDKを提供しています。学習コストはほぼ0です。

Docs

Tutorial

Developer

X 

More

GitHub 



<https://cryptoshepherds.netlify.app>



ABOUT **CRYPTO SHEPHERDS**

