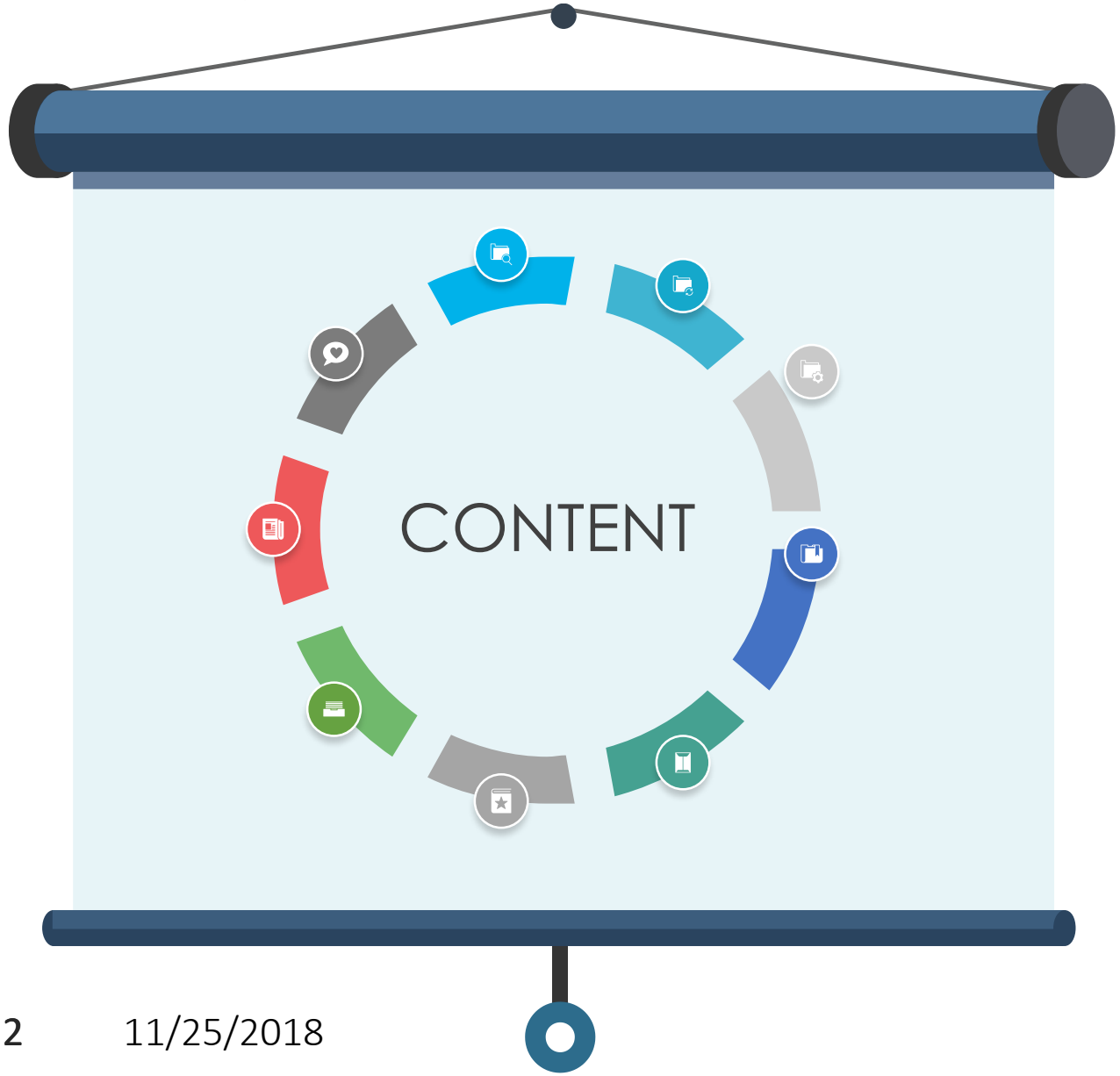
DKMS

Decentralized, zero-knowledge Key Management Service for securing user data in modern distributed applications built on top of Elastos

2018

PRESENTATION

Agenda



01 INTRODUCTION TO DKMS

02 USE CASES OF THE TECHNOLOGY

03 DKMS NETWORK AS A DAPP ON ELASTOS

04 USING DKMS TO POWER VIEWCHAIN

1. INTRODUCTION TO DKMS: DECENTRALIZED KMS SOLUTION

Problem 1- Compromised Privacy in Blockchain

Problem

Blockchain platforms are built on "ANYONE-CAN-SEE-ANYTHING" principle.

Either for competitive or legal reasons, business applications need more privacy and security over who can see what data on the public blockchain.

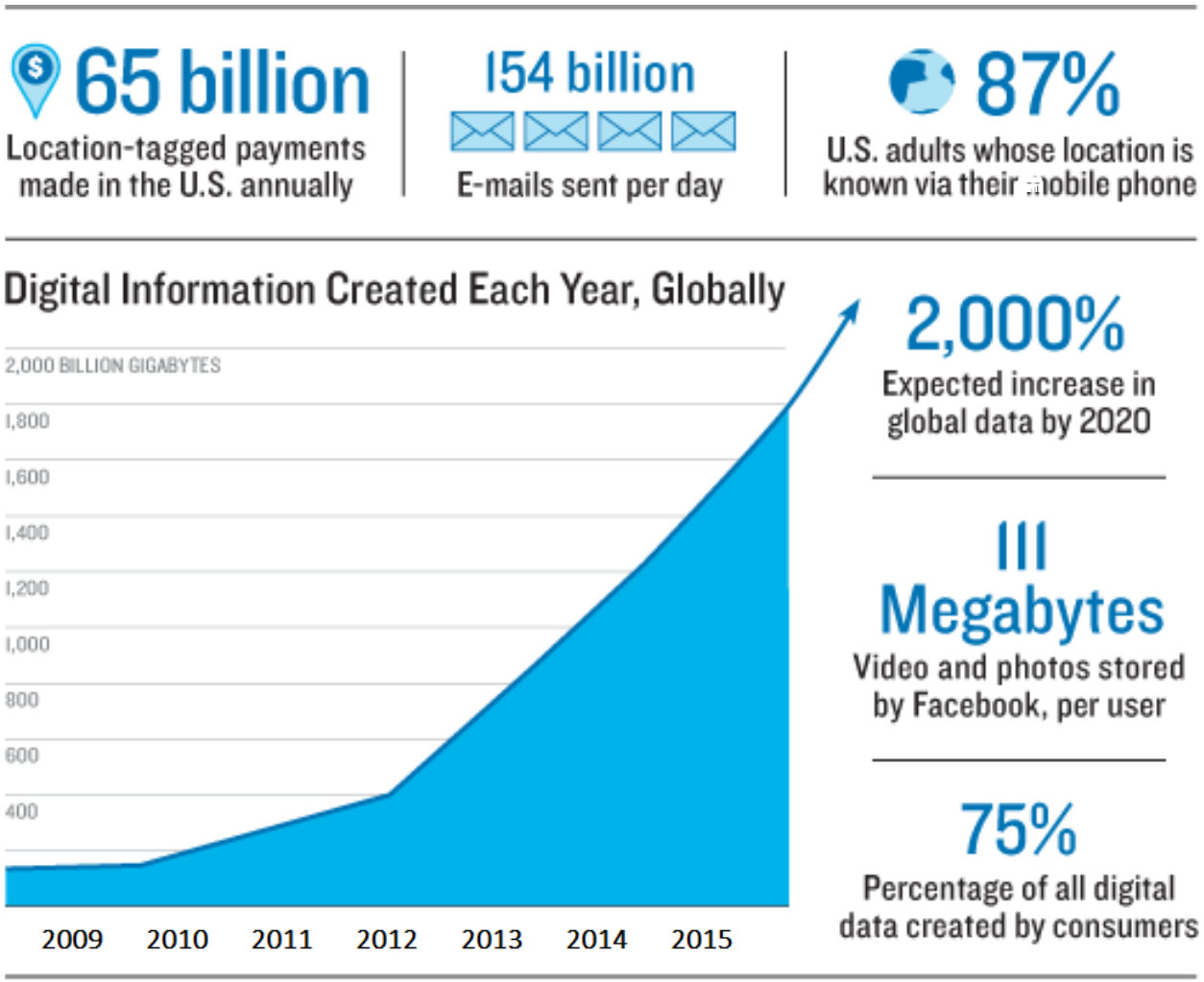
Our Solution

DKMS provide data privacy infrastructure and easy-to-use development tools to secure sensitive business and customer data on blockchain.

With our SDKs and APIS users can add end-to-end data encryption, cryptographic access control and trust management on blockchain without limiting how the data can be shared or accessed.

Data is a Core Resource

We live in a data-centric world, where data is the cornerstone of business infrastructures and driving force of social-economic relationships. Most of this data is highly sensitive and needs infrastructure for protection.



2.5 quintillion bytes of data is created per day

90% of data have been created in last two years

Emergence of audit and compliance requirements (GDPR, HIPAA, CJIS, FERPA, PCI, ITAR, etc.)

Encryption as a way to Protect Data

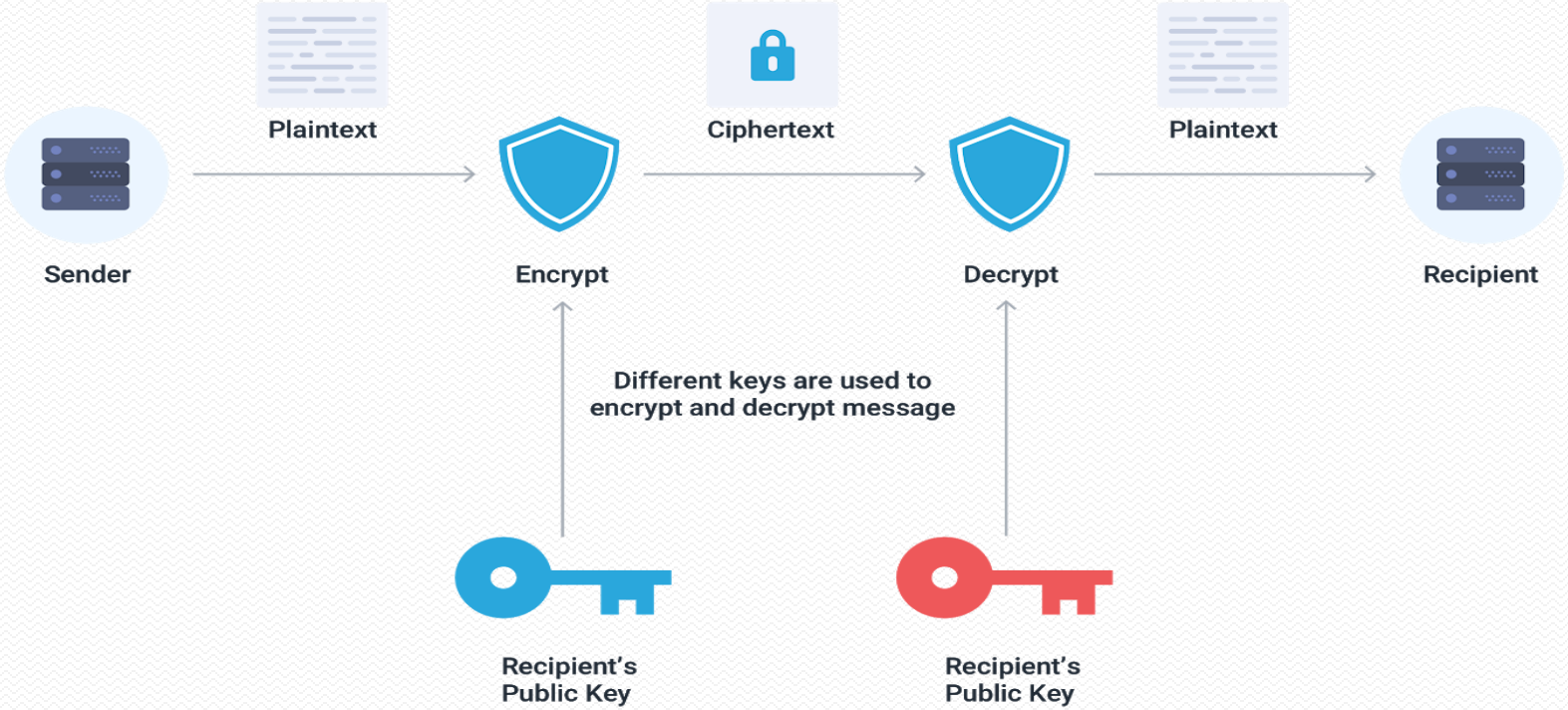
Encryption is a robust approach of protecting data from breaches and leaks. However public key cryptography has several limitations, which makes it hard to create

Plain Text

Hello World!

Encrypted Gibberish

EnCt2ac4bfa13c762664d5352dee620
2eeb360a029d3dac4bfa13c762664d5
352dee60v1+mjP5fAF



Problem 2 – Limitation of Standard PKC

Problem

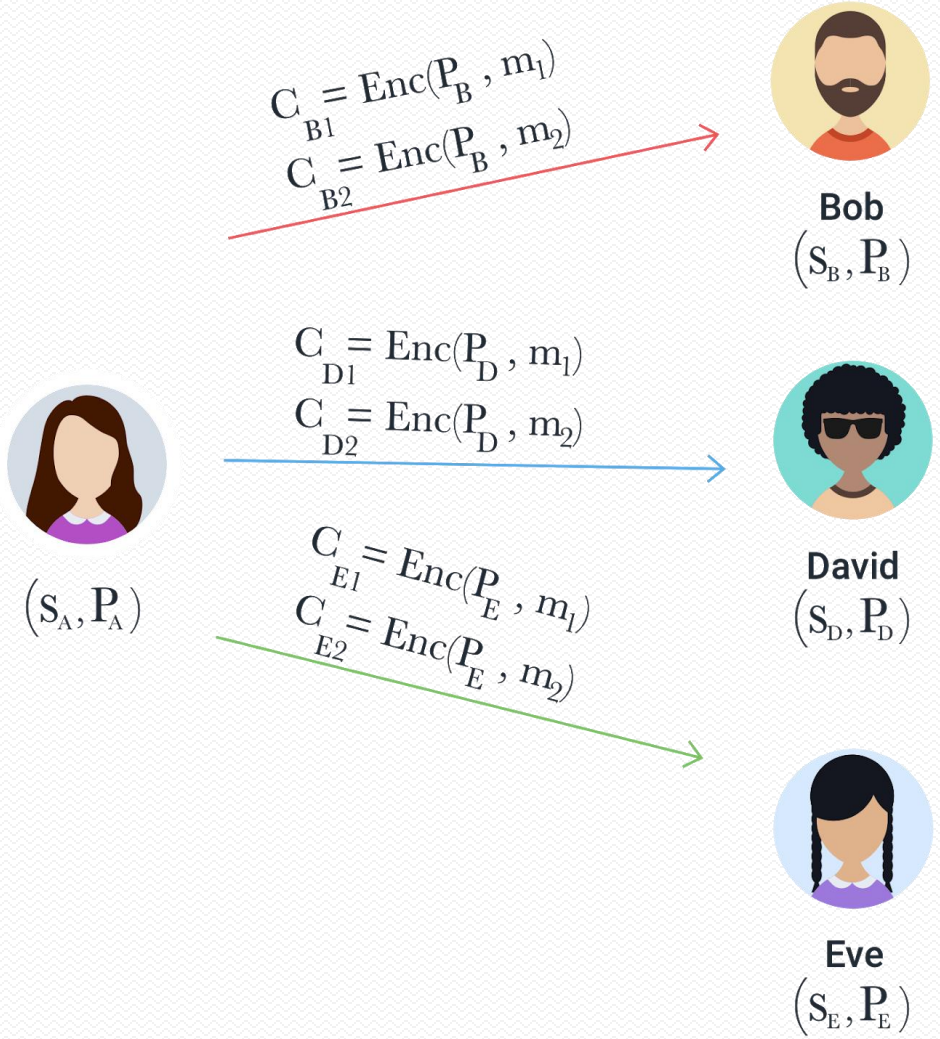
Standard public key cryptography has been invented in pre-cloud, pre-blockchain and pre-IoT era. It significantly limits how encrypted data can be easily shared, accessed or manipulated in distributed apps, where the business logic implies many-to-many, dynamic collaboration is implied.

Our Solution

DKMS leverages cutting-edge proxy re-encryption science to enable scalable, zero-knowledge key management, data encryption and cryptographic trust management toolsets for modern web 3.0 (blockchain, cloud and IoT) applications. Proxy re-encryption eliminates most functional constraints associated with standard public key crypto and can empower dynamic, scalable, many-to-many secure communication over different kind of applications

Management of Encrypted Data is a Challenge

As a cryptographic access control mechanism Public Key Encryption is limited in several ways

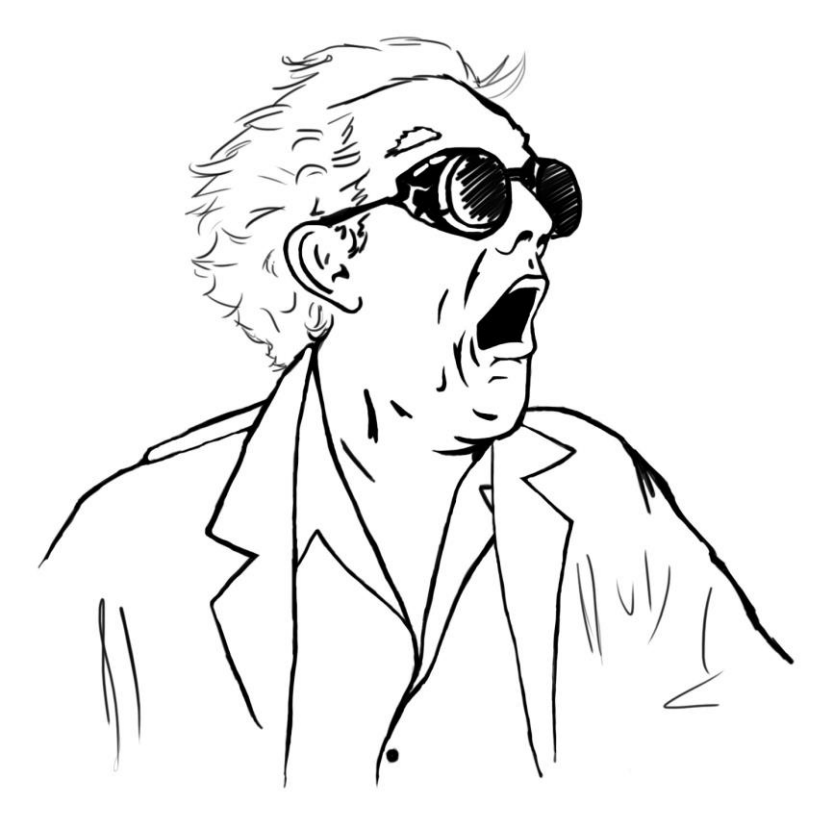


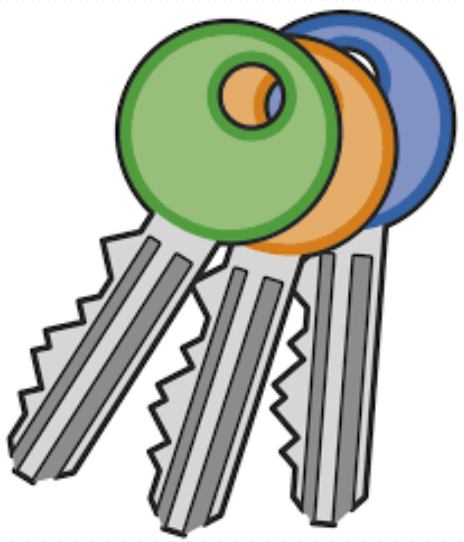
Limitations of Standard Public Key Cryptography

- Requires advanced knowledge of recipient
- Does not scale well in case of many to many messaging and multiple intended recipients
- Access can not be revoked after the encrypted message has been shared.

Key Management Process is a Challenge

Despite being essential, efficient data encryption cycle is a challenging process, where the main complexity is Key Management rather than the encryption itself.





What are Alternatives of Key Management?

Amazon, Google, Microsoft, Alibaba provide Key Management as a Service for addressing this technical challenge.

But these services can not serve dApps, are

1. **Service providers get access and manage all user keys.**

2. **Centralized Services with an undue trust put on the service provider can not serve decentralized applications**

Comparison with Alternative Solution

None of the existing methods enables safe, scalable and decentralized key management service for modern distributed applications and other data critical use cases.

	User Exclusive Control Over the Encryption Keys	Cost Efficient Solution	Simple User Experience, Scalable, Flexible Data Sharing	Easy-to-deploy and maintain	Distributed KMS, No Single Point of Failure
Federated Key Management (FKM)	**No**	**Yes**	**Yes**	**Yes**	**No**
Deploying On-Premise KSM/HSM	**Yes**	**No**	**Yes**	**No**	**No**
Legacy Encryption Methods (LEM)	**Yes**	**Yes**	**No**	**No**	**No**
DKMS	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**

How Proxy Re-encryption Works

The proxy can transform a ciphertext encrypted under Alice's public-key into ciphertext encrypted under Bob's public key.

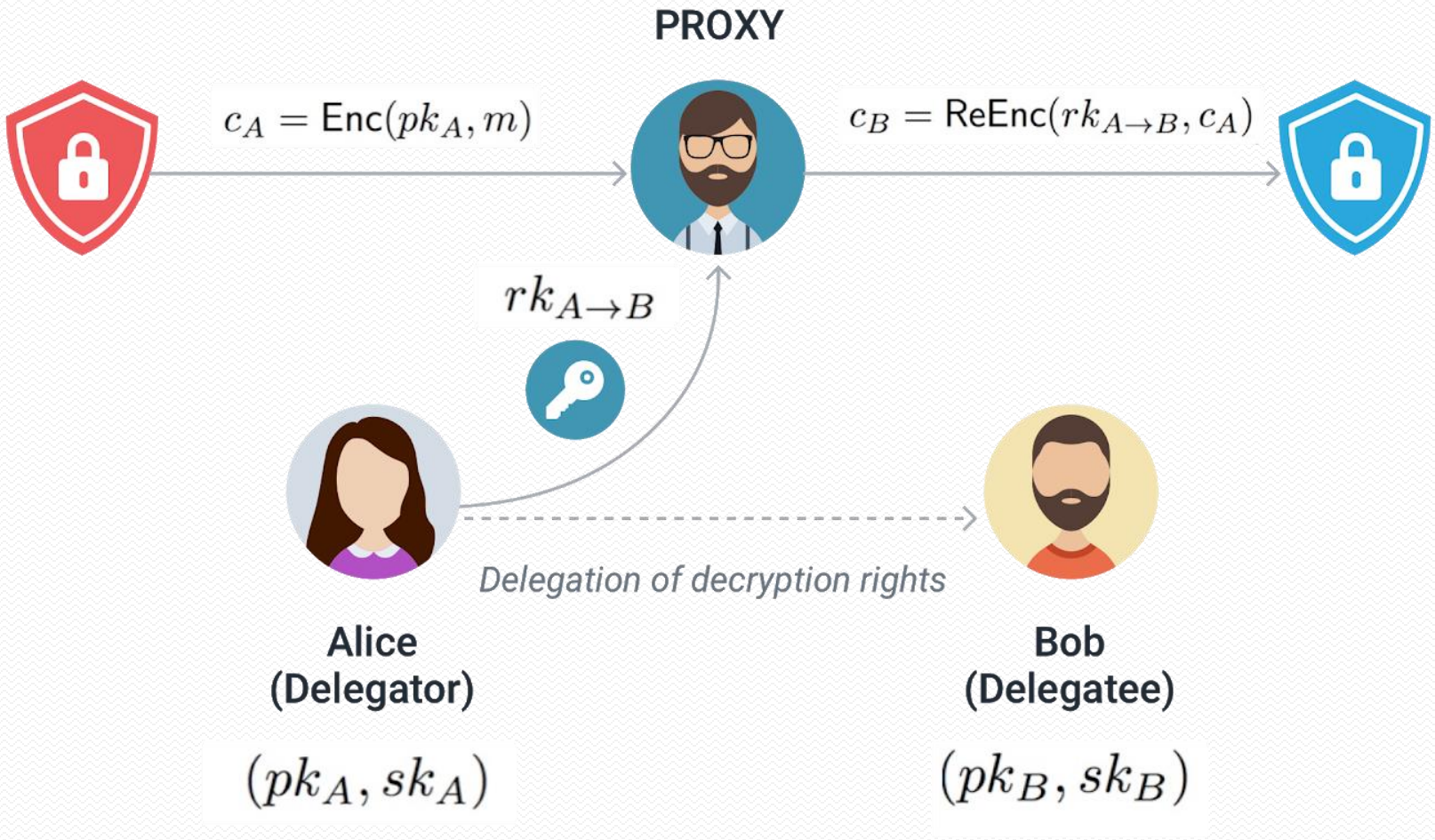
01 Alice encrypts information with her public key and puts it in decentralized storage

02 Alice generates re-encryption key using her private key and Bob's public key

03 Alice delegates the re-encryption key to an always online proxy (service provider)

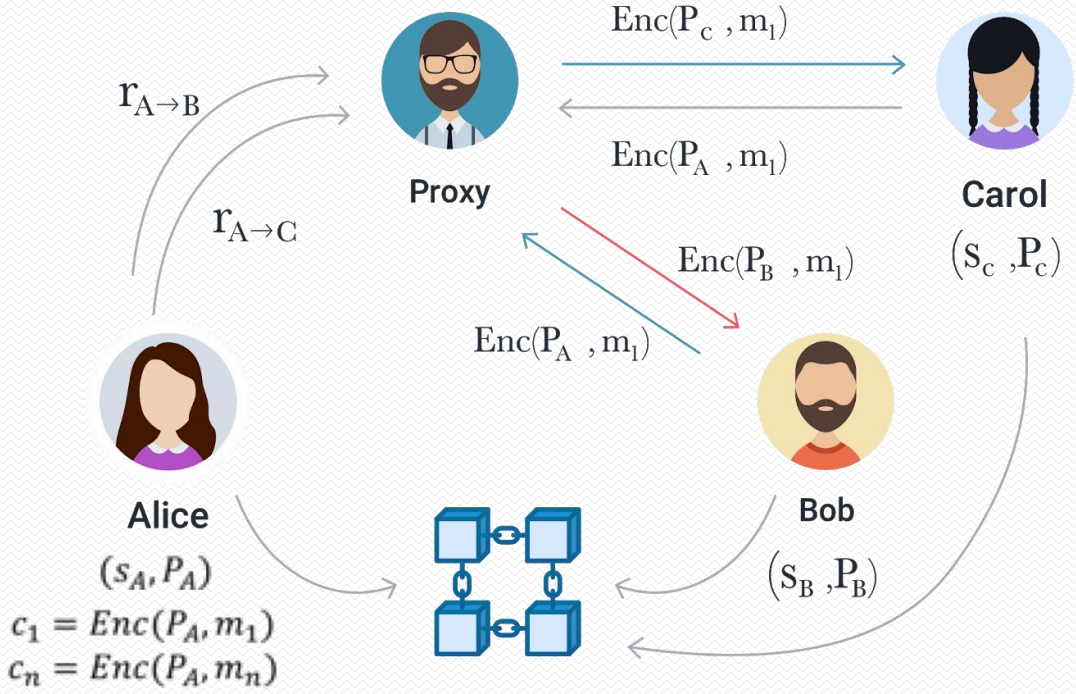
04 Proxy re-encrypts encrypted data from Alice's public key to Bob's public key

05 After re-encryption Bob can go and decrypt the information with his private key



Advantages of Our Technology

Proxy re-encryption allows DKMS to split document access management from cryptographic operations without the need to always-trusted, centralized entity



DKMS enables flexible and secure key management in distributed environments.

Enables encryption of already encrypted data and access delegation without decrypting data as an intermediate step.

Information confidentiality is maintained even if the PRE server is captured or compromised.

Problem 3 – Absences of Decentralized KMS

Problem

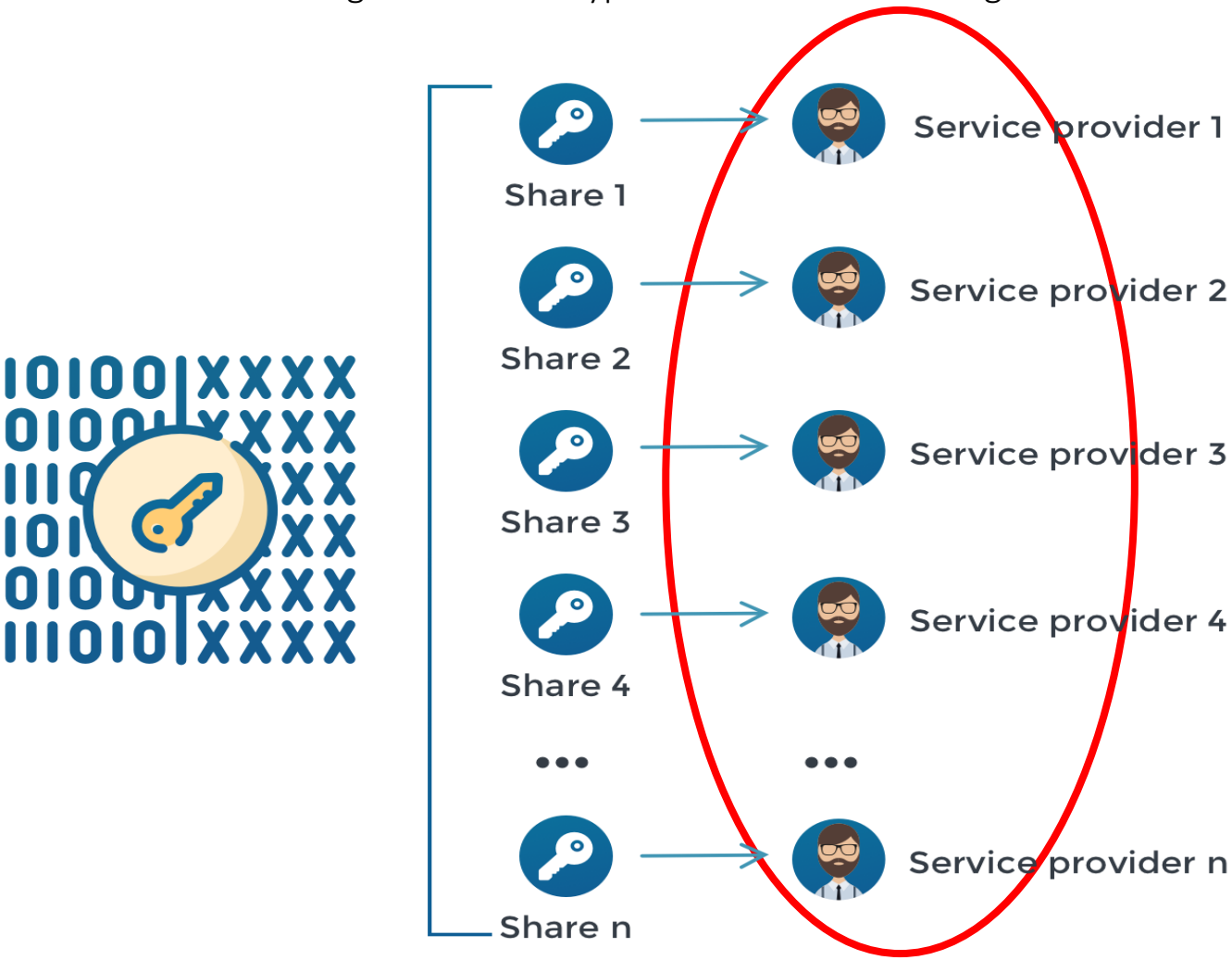
If any building block of decentralized (blockchain) application is based on centralized service provider, it significantly undermines DApps main value proposition, decentralization. All existing KMS services in the market provided by Google, Amazon, Microsoft and others are centralized services.

Our Solution

DKMS enables to build decentralized, zero-knowledge Key Management Services to solve a significant market need enabling DApps to integrate data encryption and KMS technologies without compromising decentralization.

Decentralized Privacy Layer for Decentralized Web

DKMS enables to build decentralized, zero-knowledge Key Management Services to solve a significant market need enabling DApps to integrate data encryption and KMS technologies without compromising decentralization.

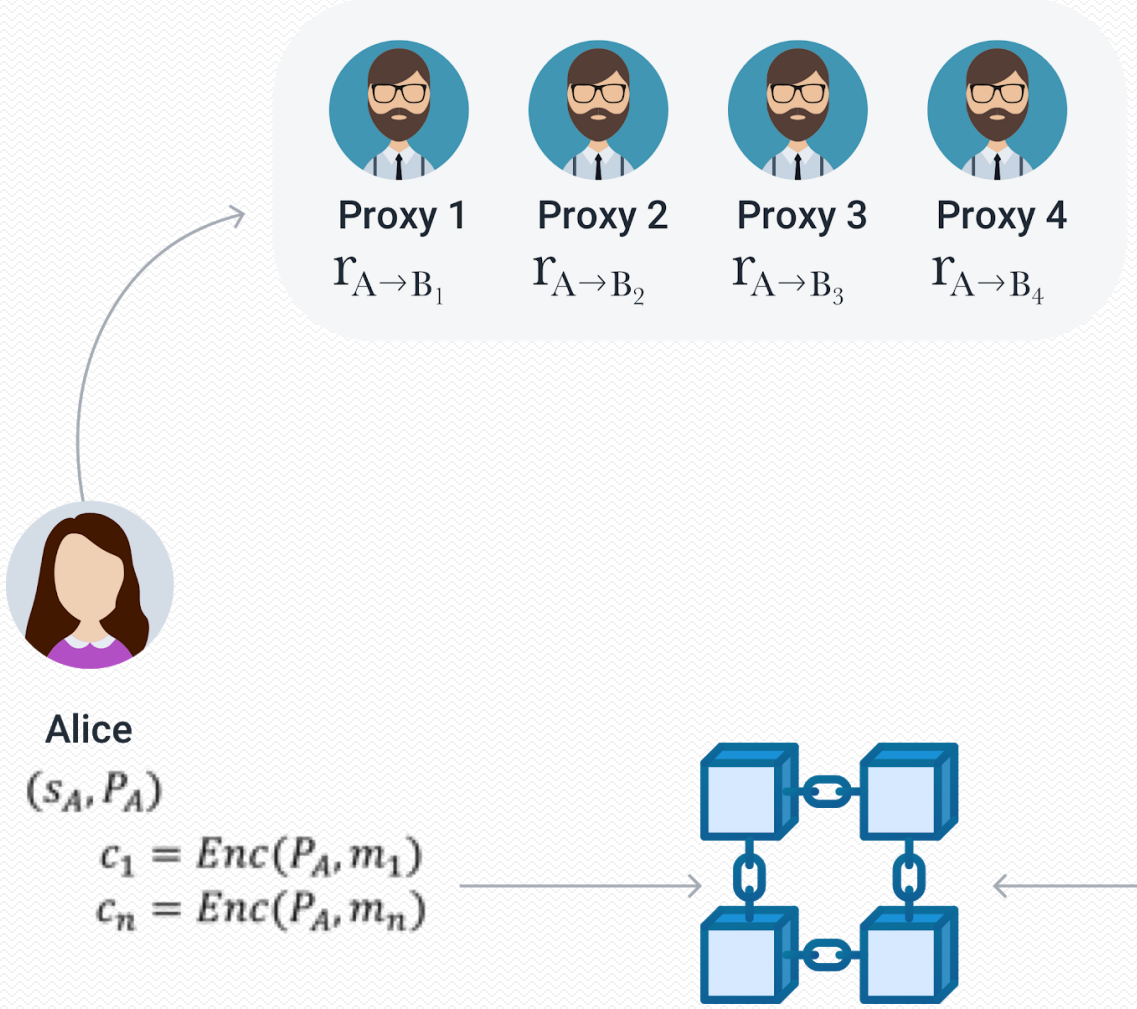


Re-encryption key are split into multiple re-encryption shares.

We leverage cutting-edge cryptography techniques and blockchain technology to decentralize our service into multiple standalone KMS Services (nodes)

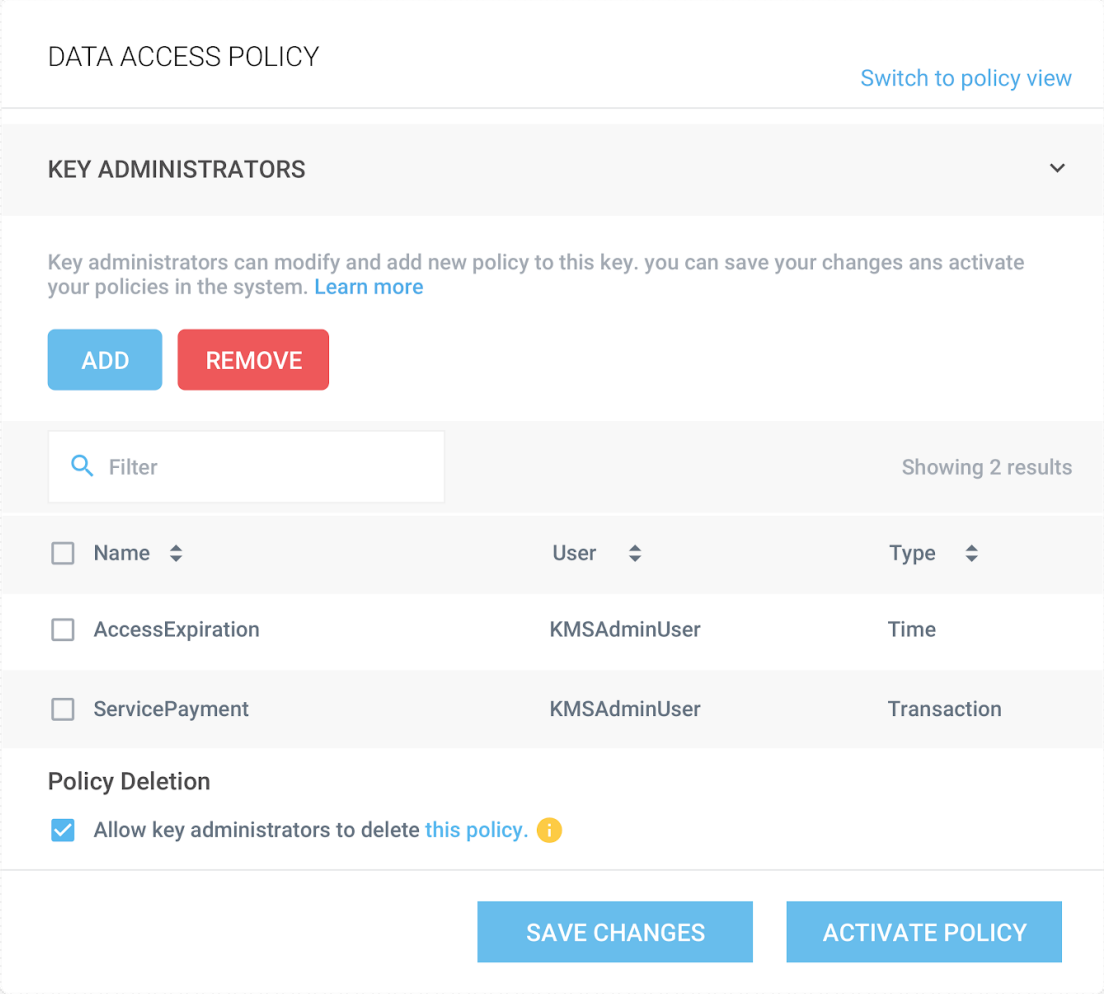
Decentralized Proxy Re-Encryption Network

Our DKMS network will be a DApp based on Elastos blockchain. The blockchain technology will applied to enable decentralized internal economy, and interaction between KMS service providers and clients.



Blockchain Technology

Data Access Policies for Automatic KMS, Integration to Smart Contracts



Conditional Data Access Delegation

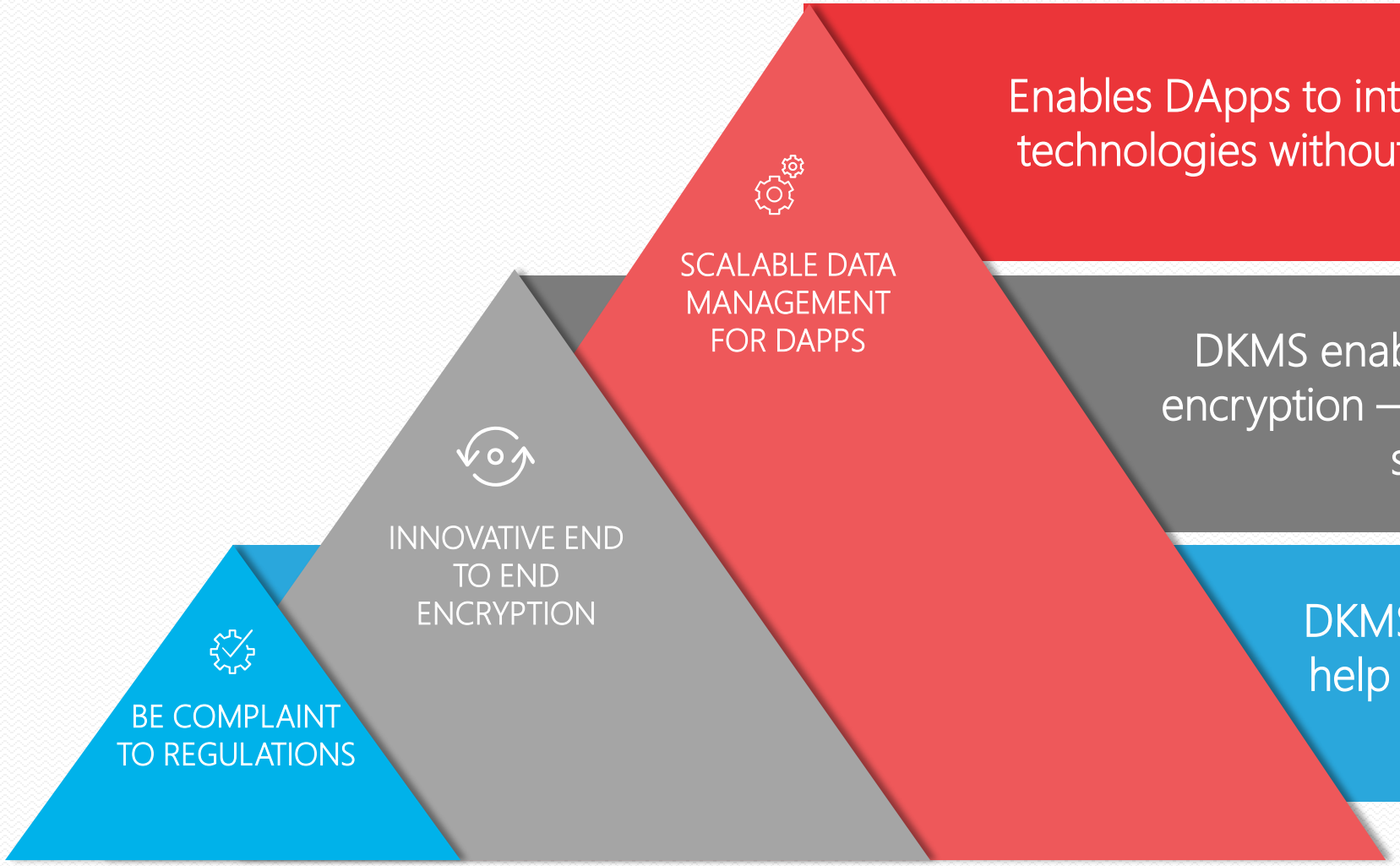
Time: enabling or disabling user to get data access after a certain point of time,

Transaction value: enabling users to get access to data when a amount is sent to an address

Other Events: other easily verifiable, blockchain based events.

Value added for DApps and Enterprises

Store, share and manage private data on public blockchains. Apply our end-to-end encryption and scalable KMS.



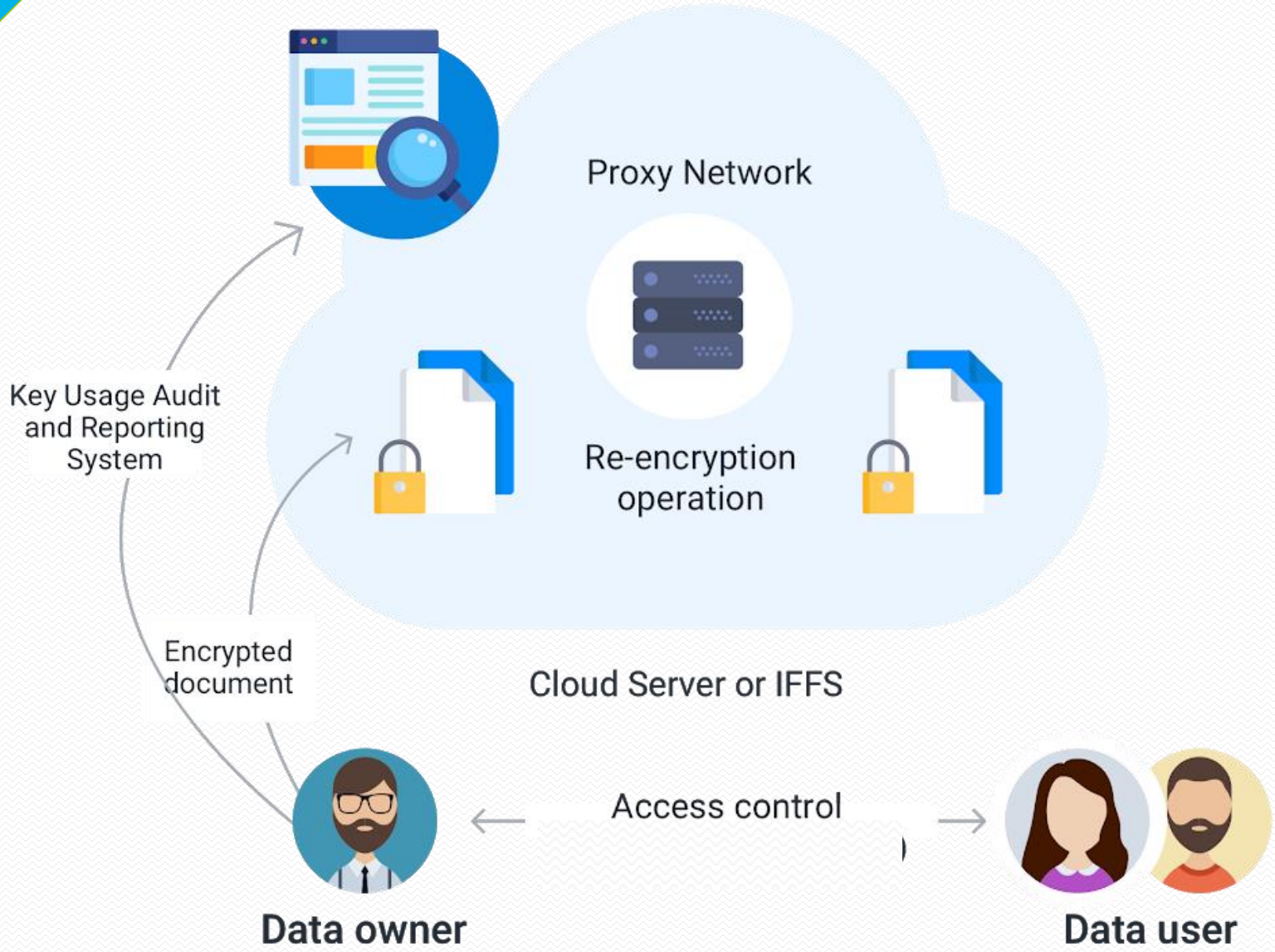
Enables DApps to integrate data encryption and KMS technologies without compromising decentralization

DKMS enables to implement Data-centric encryption — pervasive and seamless client-side data encryption

DKMS Key management platform can help to secure user data to meet the regulatory requirements

2. USE CASES OF THE TECHNOLOGY

Decentralized File Storage



DKMS provides an out-of-band mechanism of decentralized KMS to mitigate the data breach risks and increase the efficiency of data management. Overall, secure file sharing is one of the most natural applications of the proxy re-encryption schemes making sure that centralized clouds and untrusted data storages do not get access to shared information.

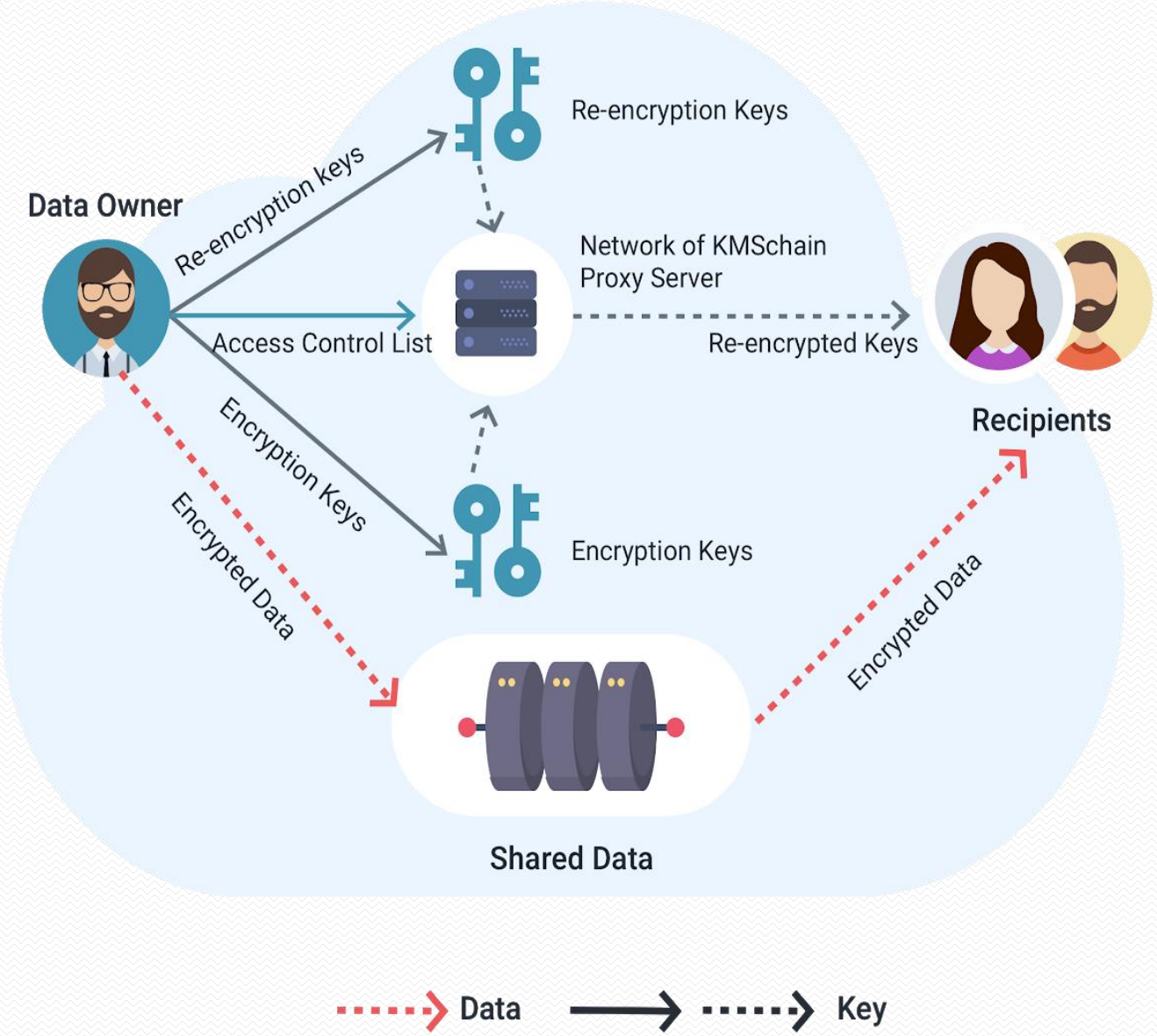
High security and data protection can be achieved by encrypting the data before storing it with untrusted servers. Our decentralized reencryption scheme can be applied to easily manage the data access, enabling scalable access control.

Digital Identity Management

Digital identities allow individuals to own, control, and carry their data wherever they go. Imagine if your health records, bank accounts, and citizenship could all be accessed through a single entry point – your private key.

Through Proxy re-encryption powered key management users no longer need to decrypt and encrypt their data every time new access should be granted or revoked. The DKMS will enable digital IDs to securely transcend industries and geographies flexibly, streamlining travel, KYC, insurance claims, and more.

Decentralized Data Marketplaces



DKMS provides the security infrastructure for media producers to create, distribute, and monetize their content securely through any distribution channel. End-to-end encryption and flexible key management allow media to float securely through the decentralized internet from creators to paying consumers without leaving the piracy a chance.

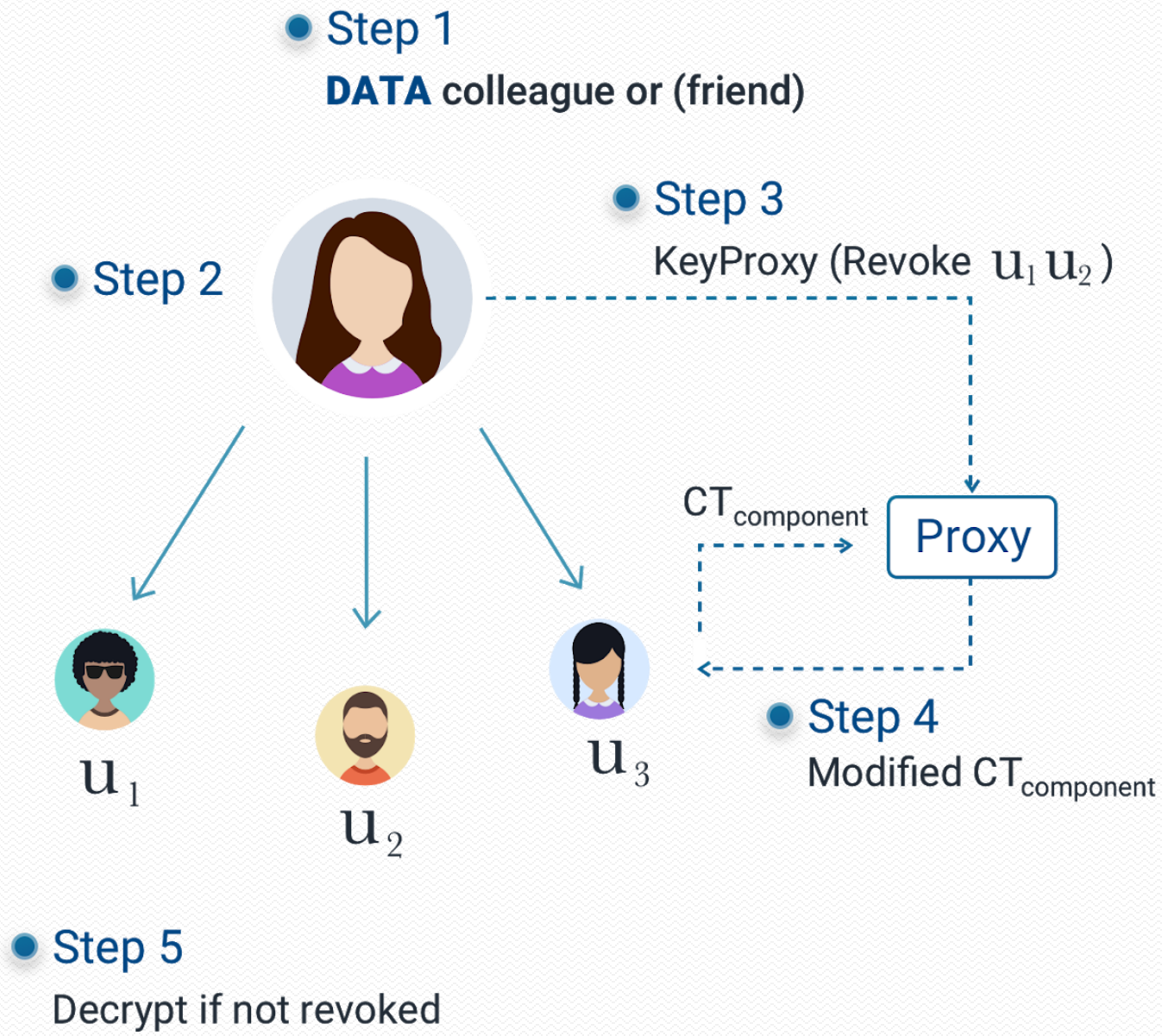
The technology enables to craete marketplaces with all following characteristics which a unique value proposition in the market

- ✓ Anonymity and Privacy protection
- ✓ Decentralization
- ✓ Transparency
- ✓ Control

Supply Chains

Supply chains are complicated, often inefficient, and ideal for blockchain. DKMS can be used to streamline secure and safe supply chains so that goods can be tracked from provenance to product, creating a more transparent, safe, and efficient system without compromising the business data privacy or enable trade secret leaks.

Decentralized Social Networks



The decentralized proxy re-encryption solution can provide fine-grained access control, ensuring that users can securely communicate in the network by applying attribute-based encryption and very flexible access delegation. The user can apply end to end encryption for the direct messaging with the contacts; as the information is re-encrypted for a particular private key it makes sure that only friends get access to the message regardless where ciphered message has been stored.

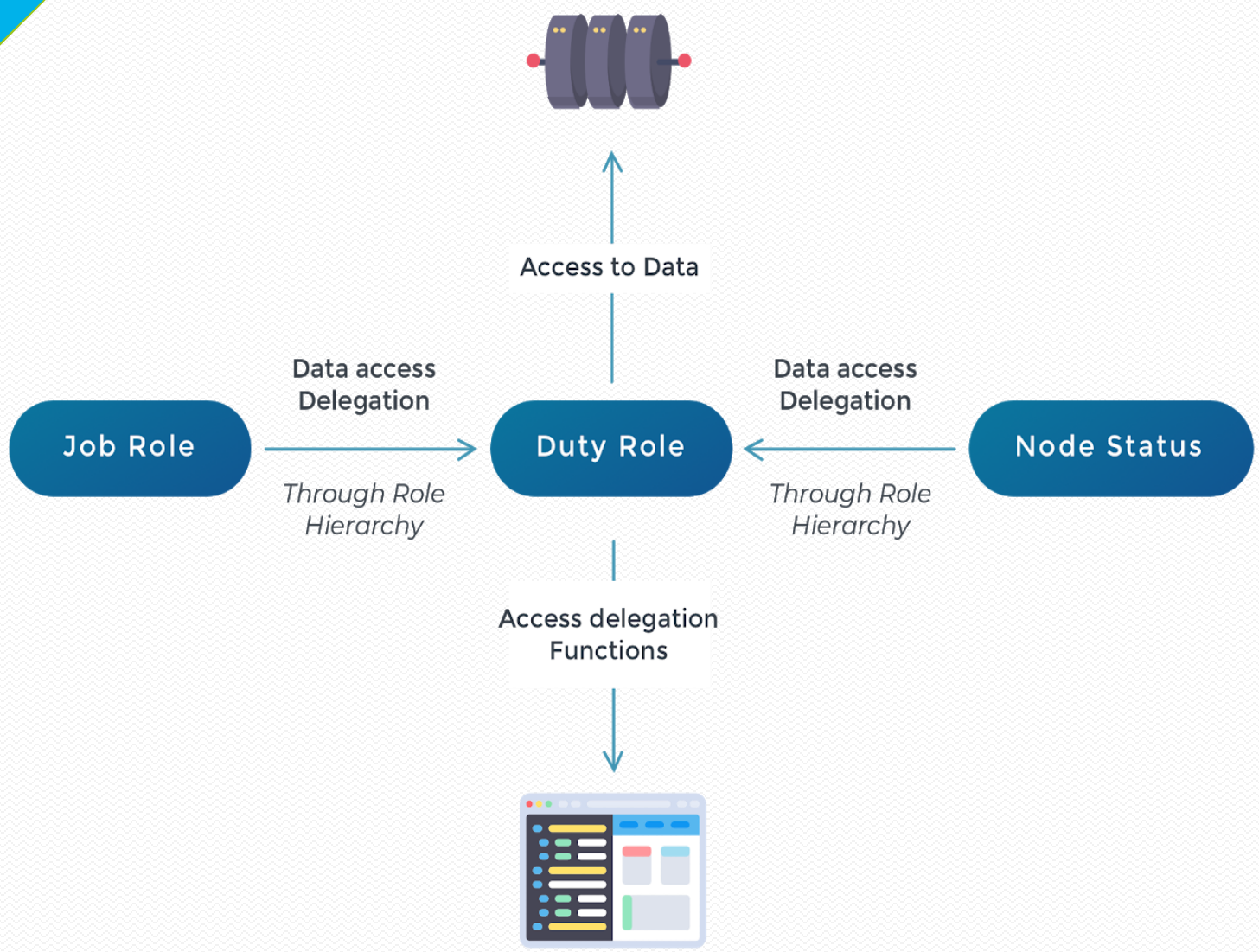
The user can create very secure social groups by assigning different attributes and keys to their social contacts, and then encrypt data such that only particular users with desired set of attributes can decrypt it. Overall, the social networks which are built on top of DKMS provide protectionof information from the unauthorized users and at the same time enable highly efficient, dynamic social network management (social group management, contact addition, revocation, etc) functionality.

Medical Health Record’s Transfer

In health information management the patient-centric approach is getting more acceptance considering that it allows higher control of personal health records (PHR). However, currently, the information storage and access delegation are mostly handled by the cloud providers, which introduces several risks in terms of breach of health information and privacy.

To make sure that the data does not get used without the permission of the patients (full controlled by patients), it is a more viable approach to encrypt the data before storing it with cloud provider. However, application of encryption brings problems in term of scalability, privacy concerns, the flexibility of access and the efficiency of the user revocation (decided by the patient). To solve those problems, DKMS can be applied for the development of fine-grained, cryptographically enforced data access control systems.

Role based Data Management



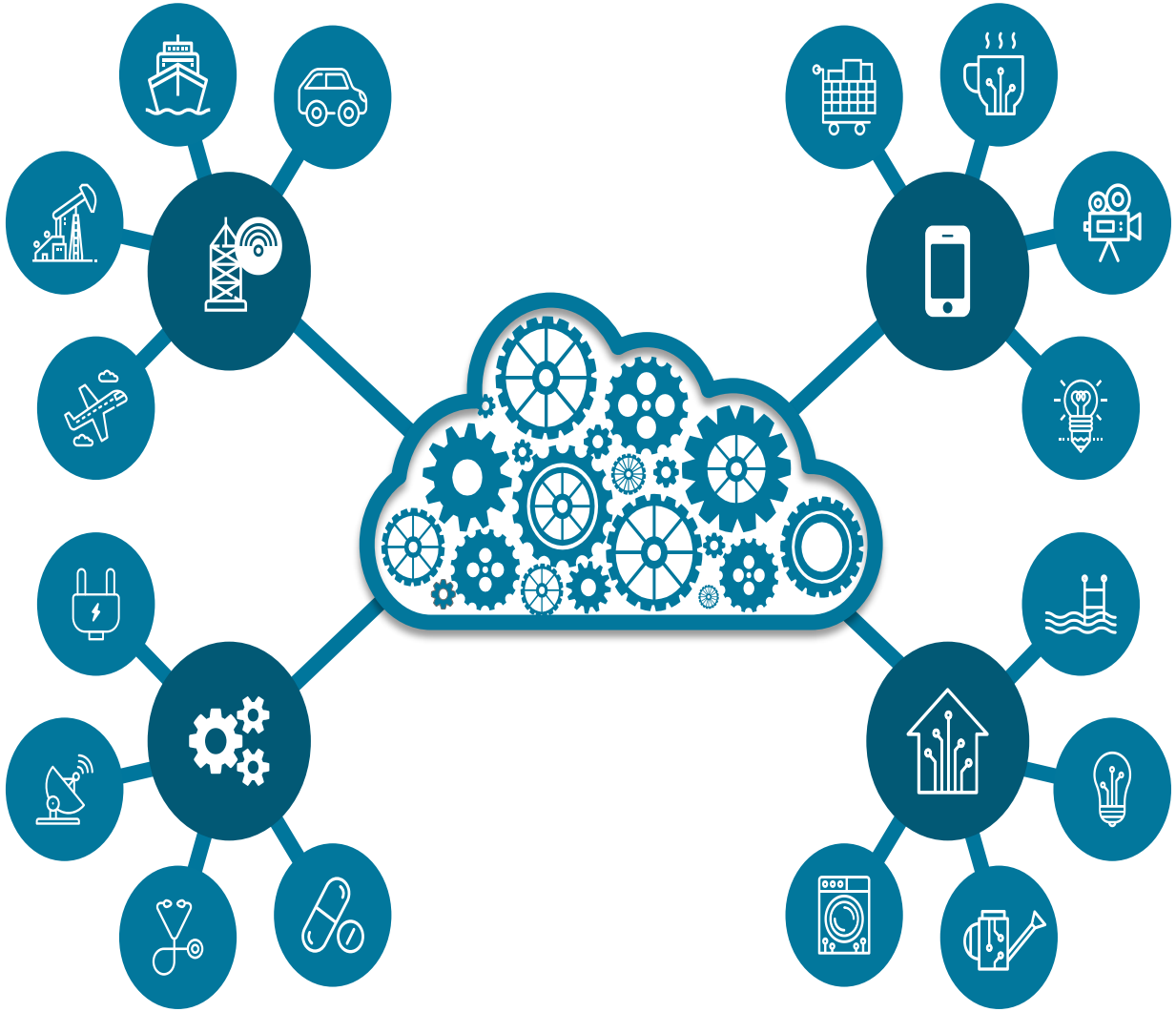
The role-based approach is widely accepted as a very robust and efficient way of data permission management. The distributed role-based access control (DRBAC) mechanism offered by DKMS is an excellent way for the optimal data security administration. Our technology has a wide application both for the traditional companies (as internal infrastructure) as well as for blockchain powered decentralized organizations (DAOs).

For example if there are different classes of nodes in the network (master nodes, service providers, Oracles, etc.) our technology can be applied to segregate the permission levels of this users, also enabling dynamic self-management (such as nodes get access to certain information if they change their class from normal to master or other conditions).

Digital Rights Management

We provide fine-grained, cryptographically enforced data access control tools for development of efficient digital rights management systems. Our technology makes sure that application of the cryptography does compromise the high scalability and efficiency of DRM.

Furthermore, the users can easily monetize their digital rights. Royalties can be tracked and distributed to their rightful owners, as content is distributed to the right users in a secure and controllable way.



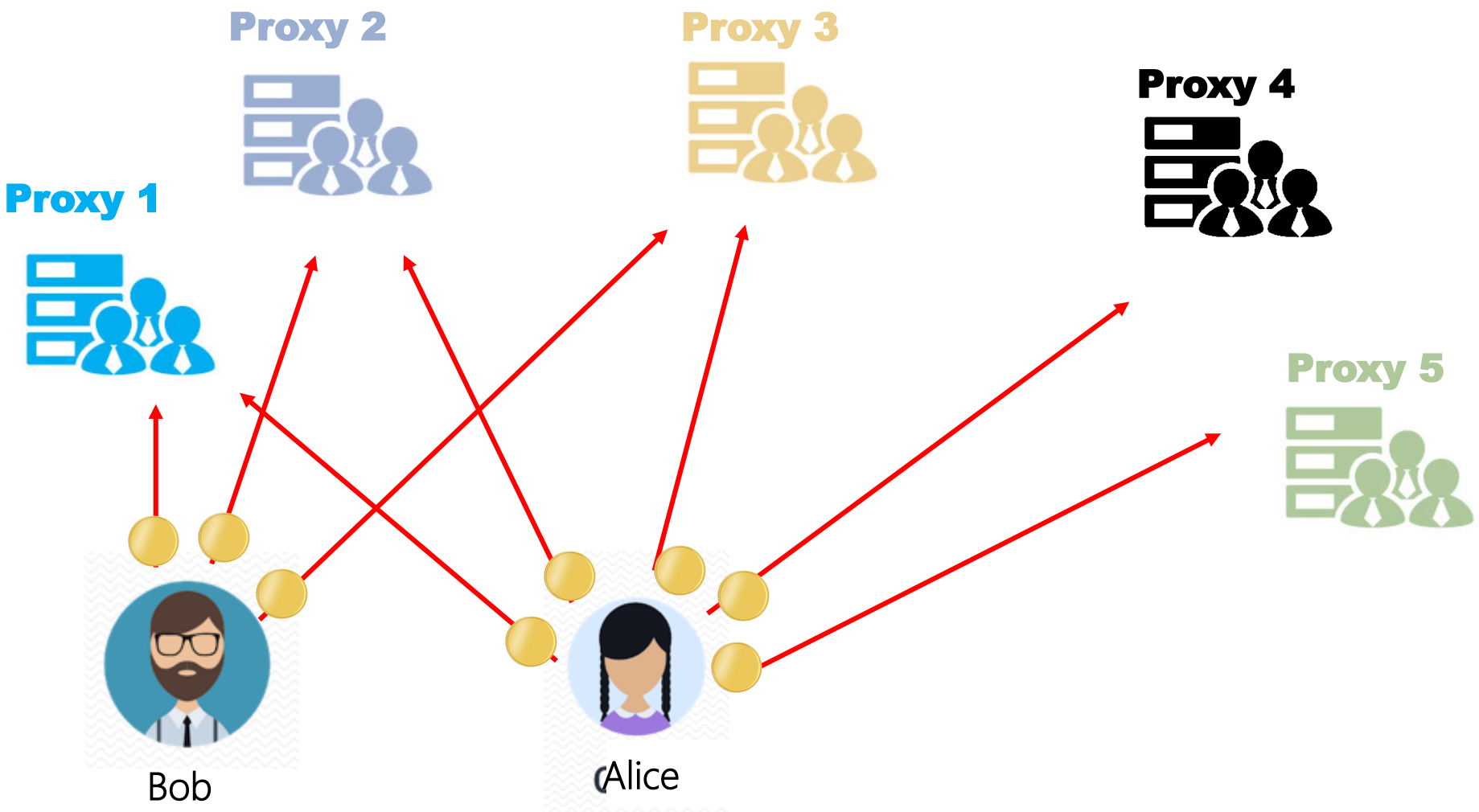
Internet of Things

Autonomous vehicles, smart grids, urban infrastructure, and more will communicate and transact on blockchain-based networks. DKMS data security infrastructure will empower secure bridges between devices & different blockchains ensuring the data will never get into the wrong hands.

3. DKMS NETWORK AS A DAPP ON TOP OF ELASTOS

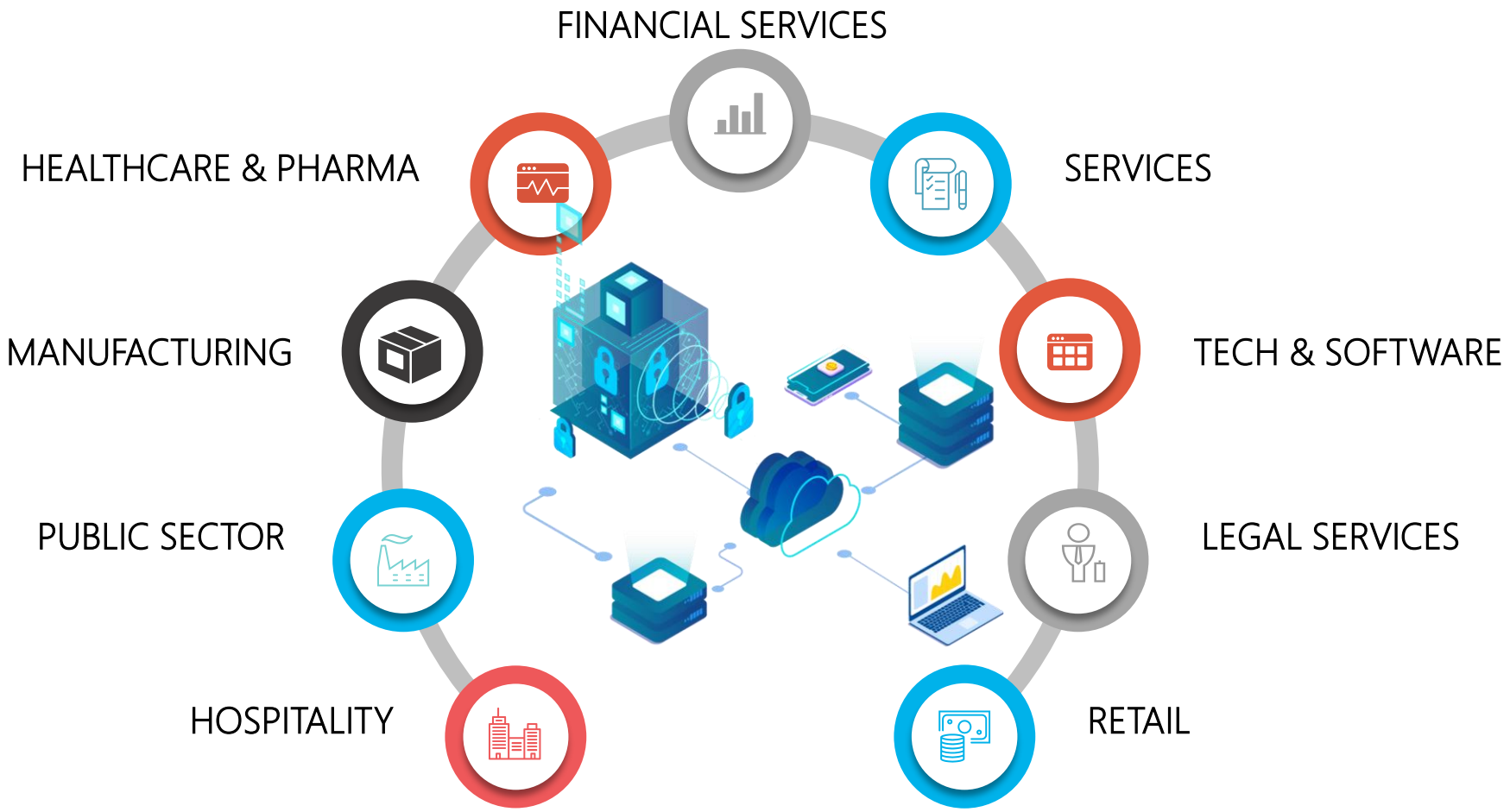
Key Management Service Providers in DKMS Network

Proxies (KMS service providers) earn service fees from clients for their re-encryption service. So, they are well incentivized to join to the network and offer their services to users of DKMS.



Decentralized Proxy Re-Encryption Network

We expect that not only DApps but also enterprises from different segments can host nodes in DKMS network on one hand to service their own needs and on the other hand to provide KMS services to their clients, blockchain applications and beyond



Why to Host DKMS Nodes

Create Value Added for your customers providing encryption and KMS service as add-on to main offerings

Position themselves in the blockchain space, providing decentralized KMS services to DApps

Assist clients to secure their private data without need to put undue level of trust on third party vendors

Acquire new blockchain clients and build relationship with blockchain applications

Help their clients to meet regulatory and compliance needs.

Develop partnerships (KMS clusters) for robust data security via becoming nodes for each other

Application of Elastos Blockchain

DKMS is effectively a DApp enabling the trustless integration of new nodes in the system and interaction with clients without involving any intermediary. We will use the blockchain technology offered by Elastos to power all key aspects of the system. The smart contract run on top of Elatsos will make sure that the transaction for clients to service providers, service provider's performance registration and decision making on proxies are done in a decentralized way without involvement of any intermediary.

Payment Infrastructure

The Elastos Smart Contracts will be applied to allow distribution of service fee from clients to service provider in a decentralized way.

Decentralized Reputation System

Our system will offer decentralized and immutable proxy reputation system (of service providers) powered by Elastos blockchain .

Voting Based Service Selection

The voting smart contract on top of Elastos will enable community of DApps at will to choose the proxies via decentralized voting

Internal Economy of DKMS

The Elastos Token (ELA) will be applied as native currency of the platform to enable decentralized transactional interaction between clients and service providers (proxies)

ELA

Payment in ELA guarantees that no service provider can get any clue about origin of re-encryption keys under their custody

ELA cryptocurrency enables P2P transactions with no involvement of any master server.

Fiatless transaction handling ensures that clients can use service of the KMS providers from any geographical location,

4. SPECIFIC USE CASE OF TECHNOLOGY: USING DKMS TO POWER VIEWCHAIN

Current Design of Viewchain and How to Power it with DKMS

Decentralized Key Management Service

Add Decentralzied Key Management Service to enable encryption and secure/scalable transfer of private information

User layer in Zapya

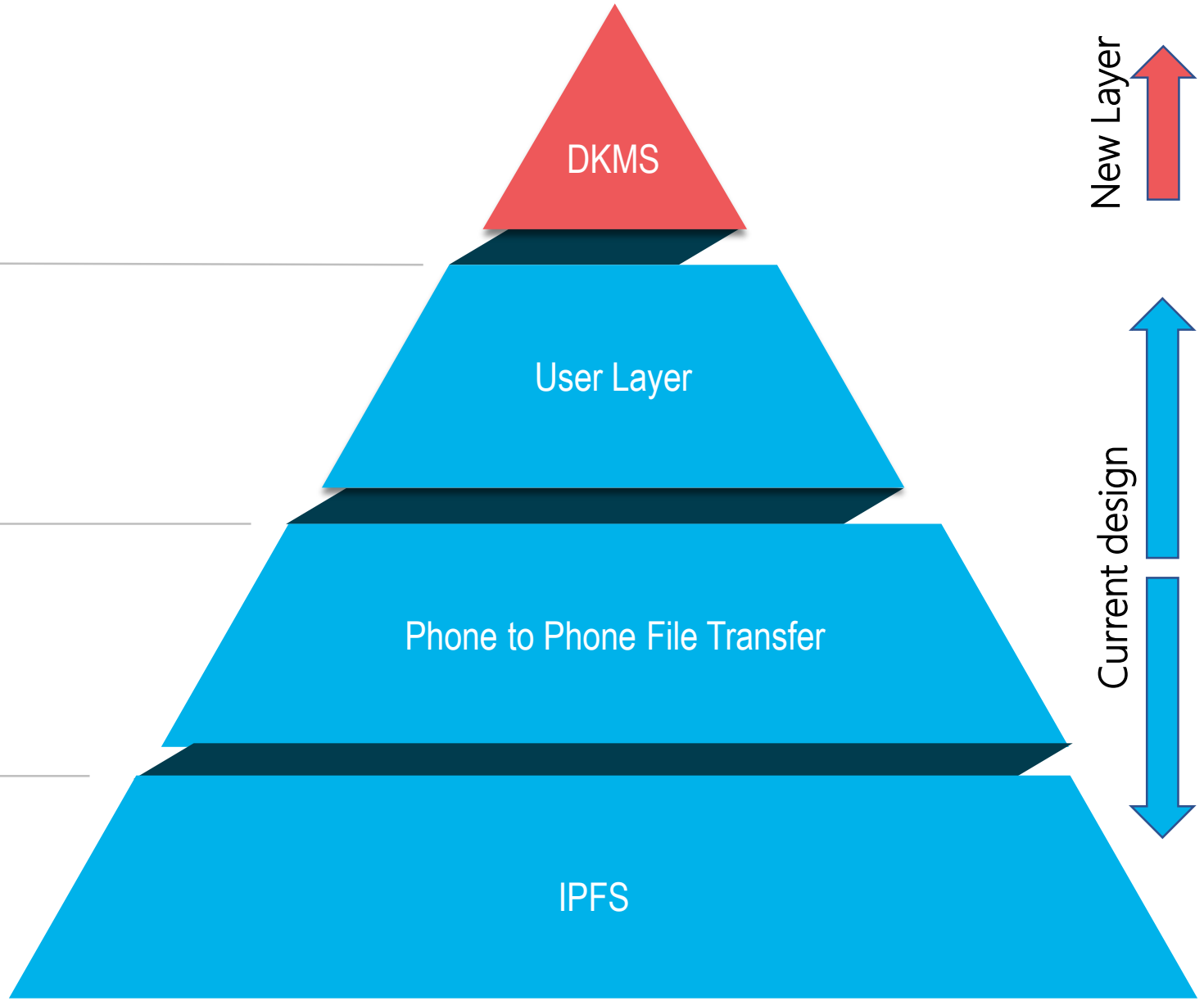
People-to-people private file sharing protocol, where people share files 1-on-1, also utilize large followings of Zapya KOLs

Zapya phone to phone file transfer protocol

Lightweight IPFS client on phones, enabling users to put up content on store shelf with just one click.

IPFS for P2P storage

IPFS serves as data layer for the technology enabling distributed data storage



Why to Power Viewchain with Our Technology

In the decentralized data storage applications, our decentralized proxy re-encryption technology will add significant value enabling scalable and trustless data access delegation.

01

Storage of Encrypted Data

High security and data protection can be achieved by encrypting the data before storing it IPFS through Viewchain system

02

Flexible Management of Encrypted Data

Our decentralized re-encryption scheme can be applied to easily manage the data access, enabling scalable and trustless access control.

03

Efficient Utilization of Data Storage

With our proxy re-encryption technology: only one encrypted file is stored in IPFS, the access management does not require any interaction with data storage layer.

04

High Uptime of the System

Delegation of re-encryption keys to always online proxies makes sure that the uptime of the data permission layer is not compromised when the data delegator goes offline.

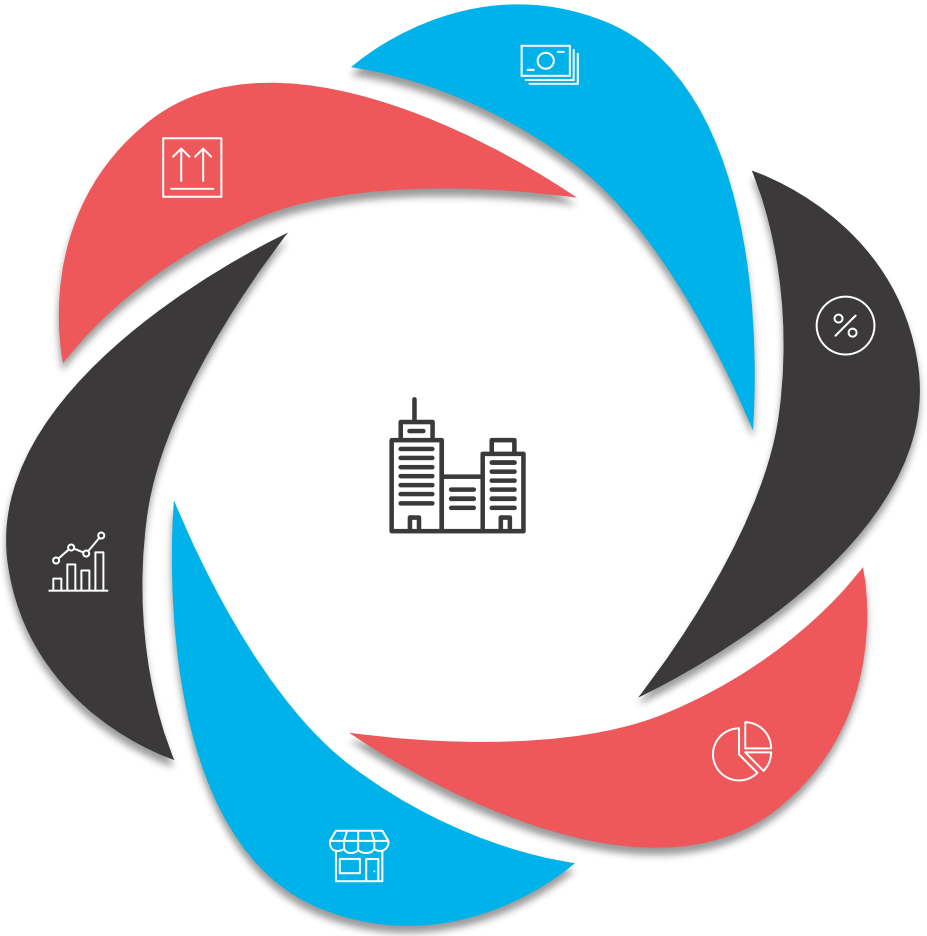
Allow Content Writers and Data Owners in Viewchain Effectively Monetize Their Data using our KMS

01 There is a big demand for decentralized and privacy-preserving data marketplaces to ensure secure, cheap and efficient monetization of user data

02 DKMS layer on top of IPFS in Viewchain network will enable the development truly decentralized and scalable decentralized data and content marketplace.

03 DKMS layer will enable the content writers to sell their works seamlessly using always online, decentralized network of KMS service providers.

04 The system can be combined smart contract technology to provide easy data monetization. The conditional and time-based policies enabled in DKMS makes sure that the data access to the consumer is delegated only after certain conditions are met

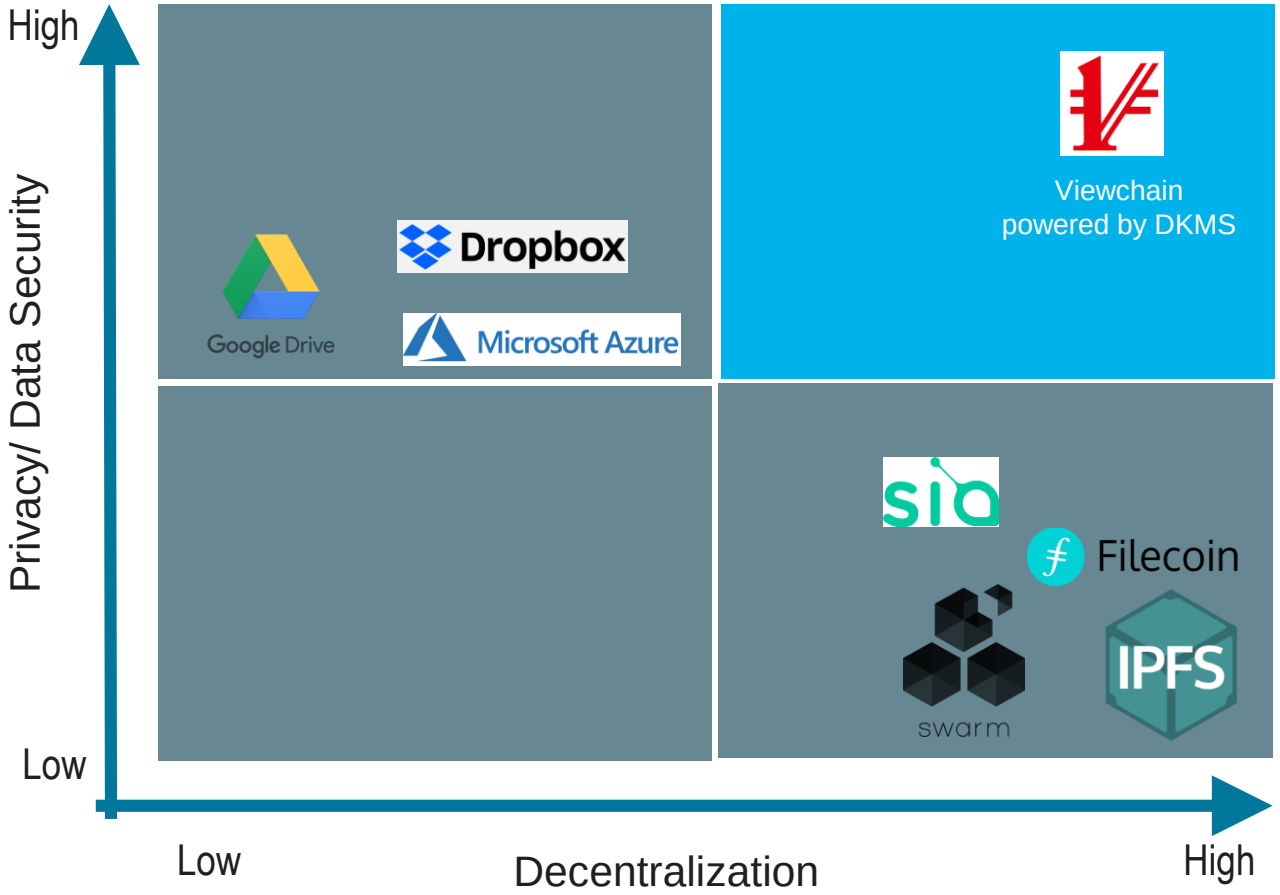


How to be Unique in the Market

Non of current decentralized storages (IPFS, FileCoin Sia, Storj & Swarm) provides an robust and scalable security layer to enable efficient private data storage and permission management. The sensitive data should not be stored on these solutions.

The cloud storage services, such as Google Drive, Dropbox, and Microsoft Azure, provide significantly increased efficiency, scalability and privacy. However these cloud providers are centralized trusted parties, who have significant control over client data.

Using DKMS as a security layer to power Viewchain, we can create truly unique, decentralized data storage proposition in the market.



THANK **YOU**

KMS CHAIN

https://DKMS.com