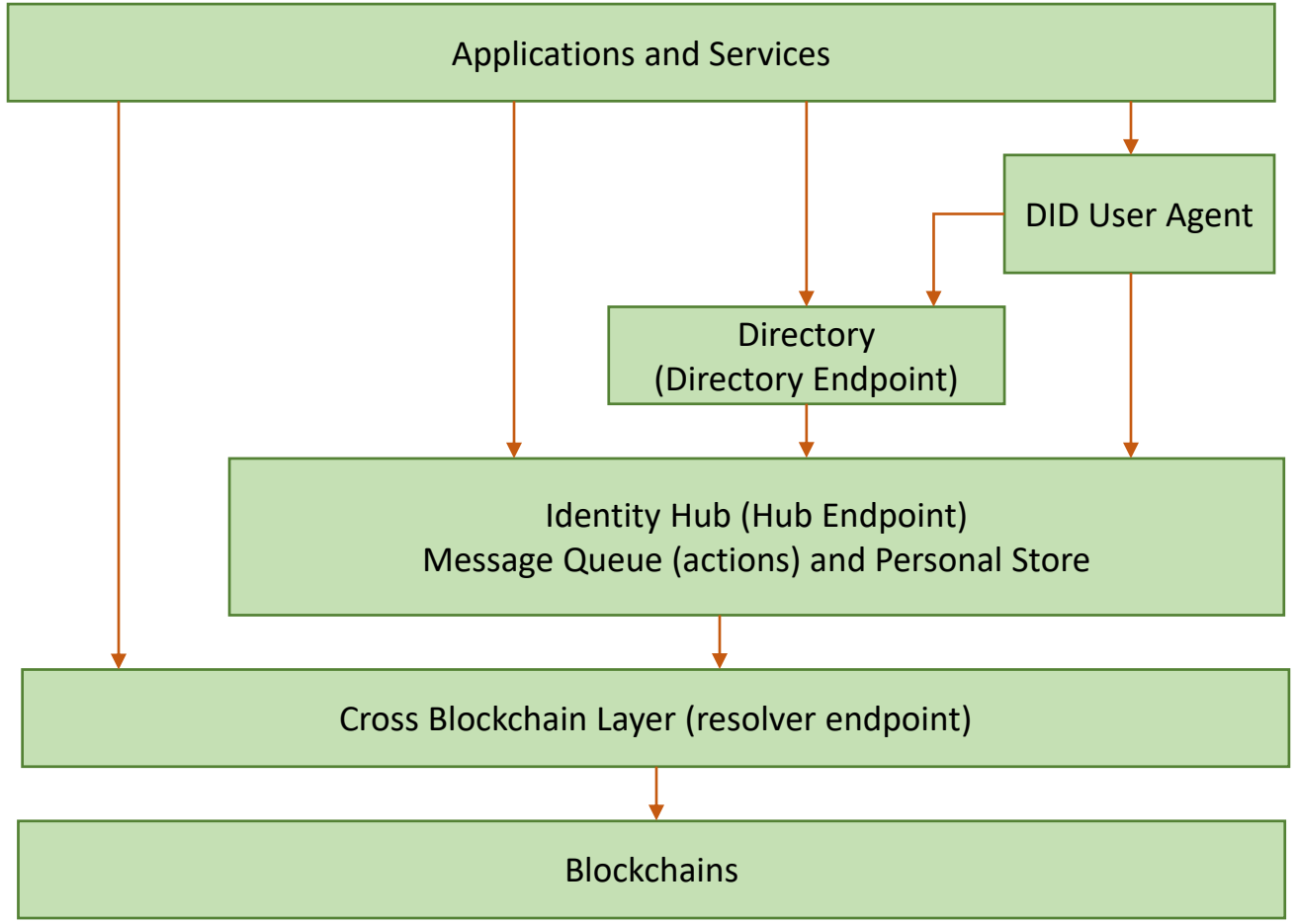
Decentralized Identity

Architecture Highlights



About the layers

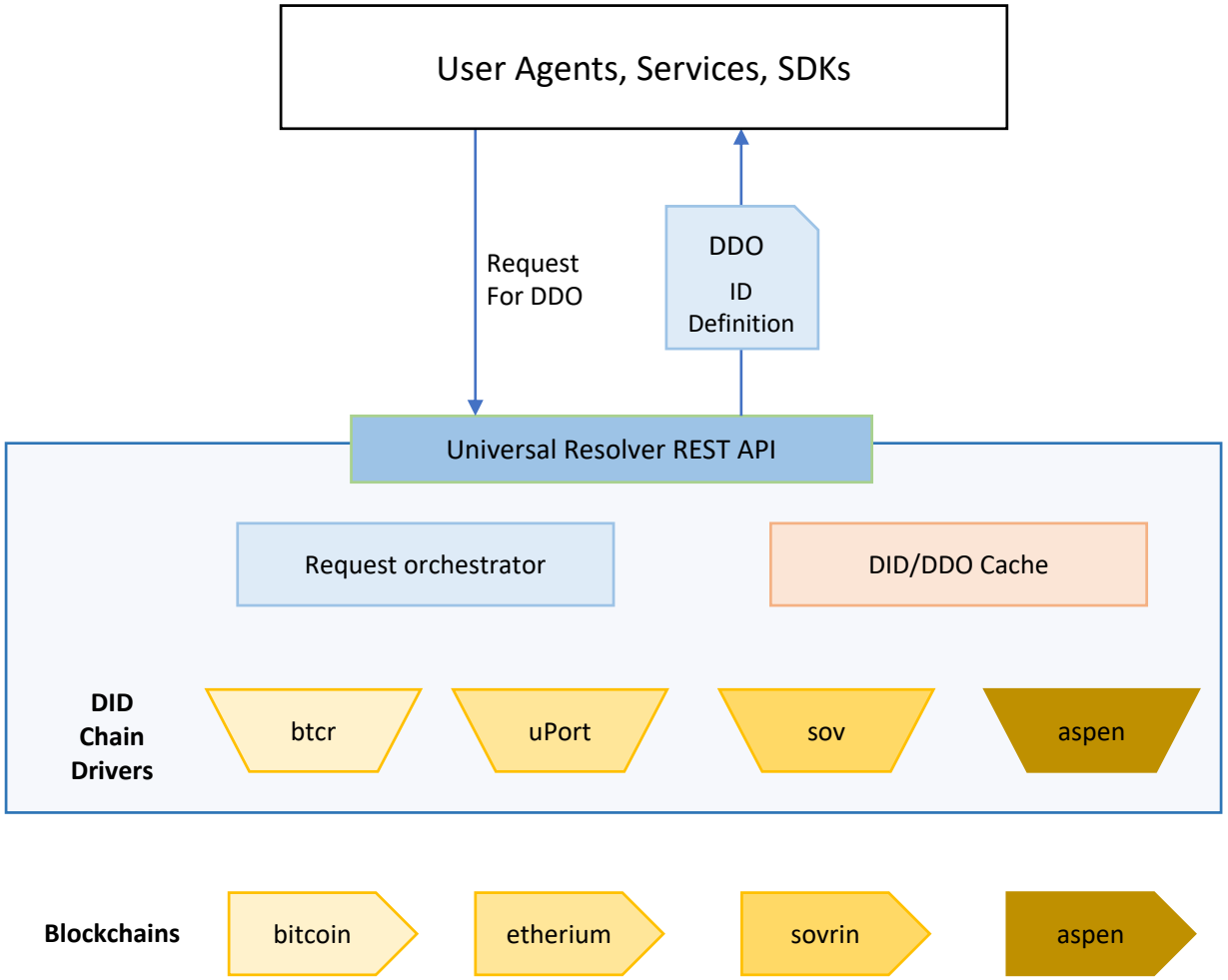
6	**Application and Service Layer**	All the higher level Decentralized services and applications based on identity, enabling the first wave of serverless apps.
5	**User Agent**	The presentation layer which manages the user's secret keys and allows them to be used to access private data
4	**Directory Services**	Provides discovery of identifiers based on public information that users want to be searchable.
3	**Identity Hub**	Stores PII and personal content, manages the message queue conveying requests for actions to a user, synchronizes across hubs and notifies apps.
2	**Cross-blockchain layer**	Allows other layers to use a single interface to manage identifiers on all the underlying blockchains.
1	**Blockchain layer**	Guarantees unique identifiers and stores a base document describing how the owner of an identifier authenticates and how she and others get to the associated Identity Hub (Layer 3) and services.

What does Decentralized Identity Bring?

Give individuals complete control over their digital identifiers	Empower people to create their own secure digital identifiers (DIDs) and fully control the personal information they present and receive without depending on or being profiled by corporations or governments
Provide identifiers and personal data stores that outlive the people who use them	Provide future-proof identities and data stores that will not be affected by changing corporate business goals, the viability of technology companies or changes in government.
Provide long term availability and provable integrity	Eliminate single points of failure and mitigate targeted attacks through multiparty redundancy and decentralized consensus.
Provide superior privacy and GDPR compliance	Empower individuals to fully control the privacy of their information, including minimal, selective, and progressive disclosure of attributes or other data.
Provide increased security for parties relying on identifiers and data	Provide sufficient security for relying parties to depend on DID Documents for their required level of assurance.
Provide search	Offer a directory/search engine allowing entities to authenticate and interact with other entities using phone numbers, email, etc.
Interoperability	DID architecture uses open interoperable standards.
Provide Portability and Interoperability	Provide a system and network-independent solution and enables people to transfer their identity to another DID system.

Enable next-generation personal apps that cross all boundaries

The DID and DDO – The base of the system



DDO: Minimal, stable, PII-free information needed to authenticate the owner and point to her identity system services

Request

resolve('did:btcr:xyz123def')

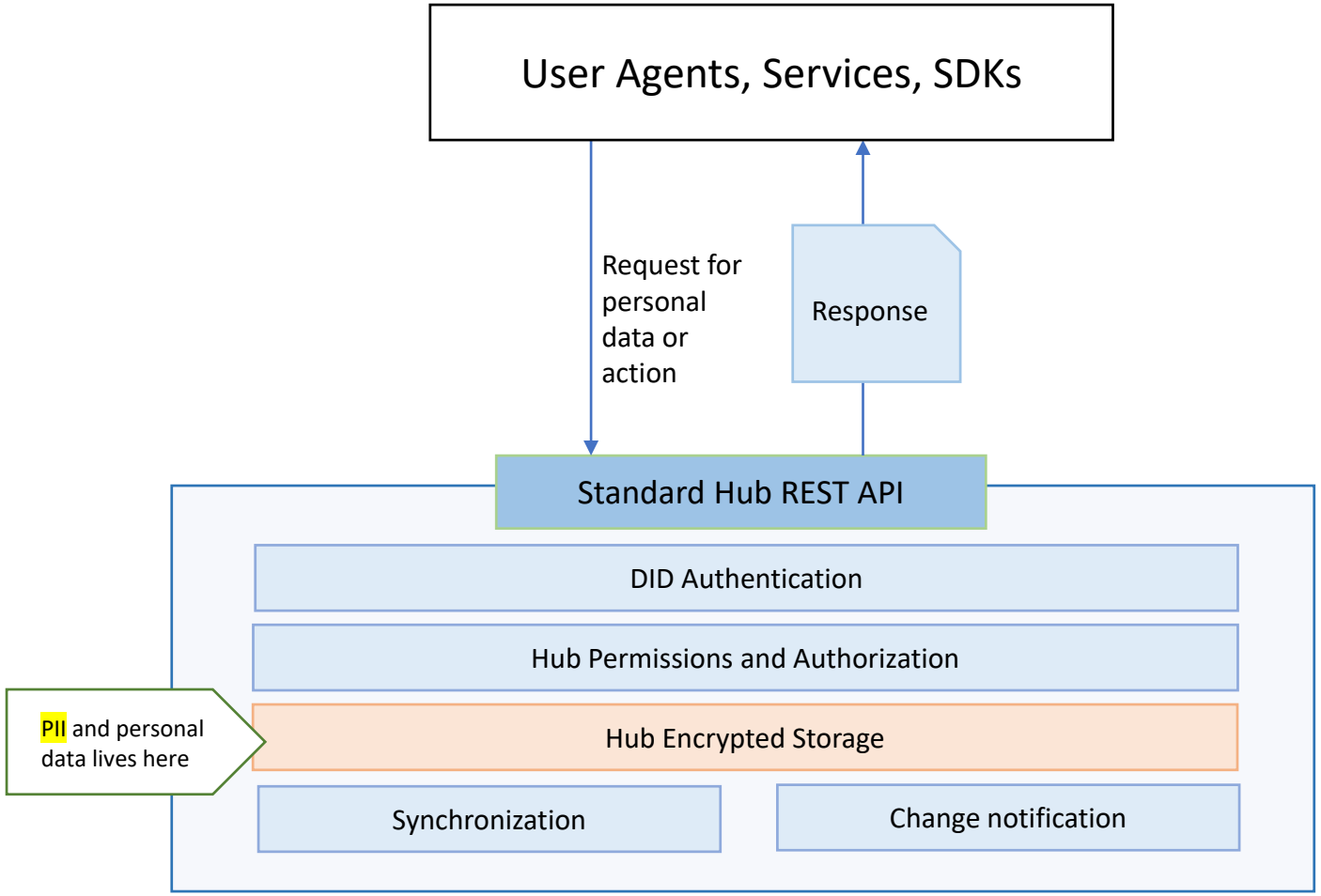
Response

```
{
 "id":did:btcr:xyz123def",
 "publicKey": [
   {...},
   {...},
 ],
"service": [
 {
    "type": "HubService",
    "endpoint": "https://foo123"
 },
 {
    "type": "DirectoryService",
    "endpoint": "https://bar456"
 }],
   "proof": {....}
}
```

PII and personal data lives here

Public searchable info released by user lives here

Identity Hub



* With unencrypted searchable metadata tags

By default the hub only has visibility onto metadata, permissions, and public information. As a DID in its own right it can be granted further visibility,

Standard Hub Interfaces	
Profile	Owning entity's primary identity attributes
Permissions	Access control document for interfaces
Actions	Endpoint for relay of actions to the identity owner
Stores	Pairwise storage space for specific DIDs
Collections	Owning entity's queryable collections
Extensions	Custom service-based functionality the entity maintains

The Directory