EXCALIBUR

Google for the Internet of Things

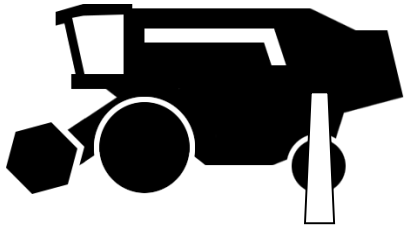
Seamless discovery and authentication

How do we search in IoT?

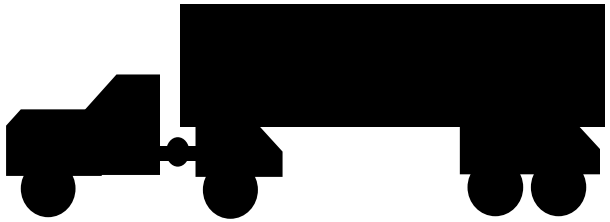
Current Internet status-quo is using search engines to navigate the Internet. But do we really want go give them all our data to just to be able to “turn on the light” or “open the door” at home?

Excalibur addresses this problem in a way that is able to provide context based naming and resolving purely inside of the network with no external/cloud participation required thus enabling “Google like” user experience even on the most resource constrained IoT devices without any data ever leaving local network.

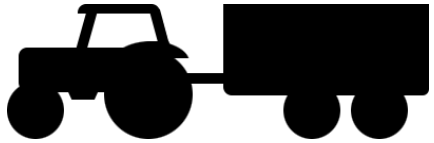
Internet of Things – Use cases



serial no. e.g. #234.36635.234

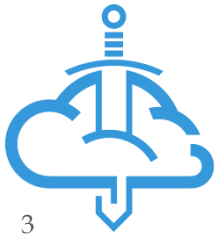


License plate e.g. “B-BA 1254”



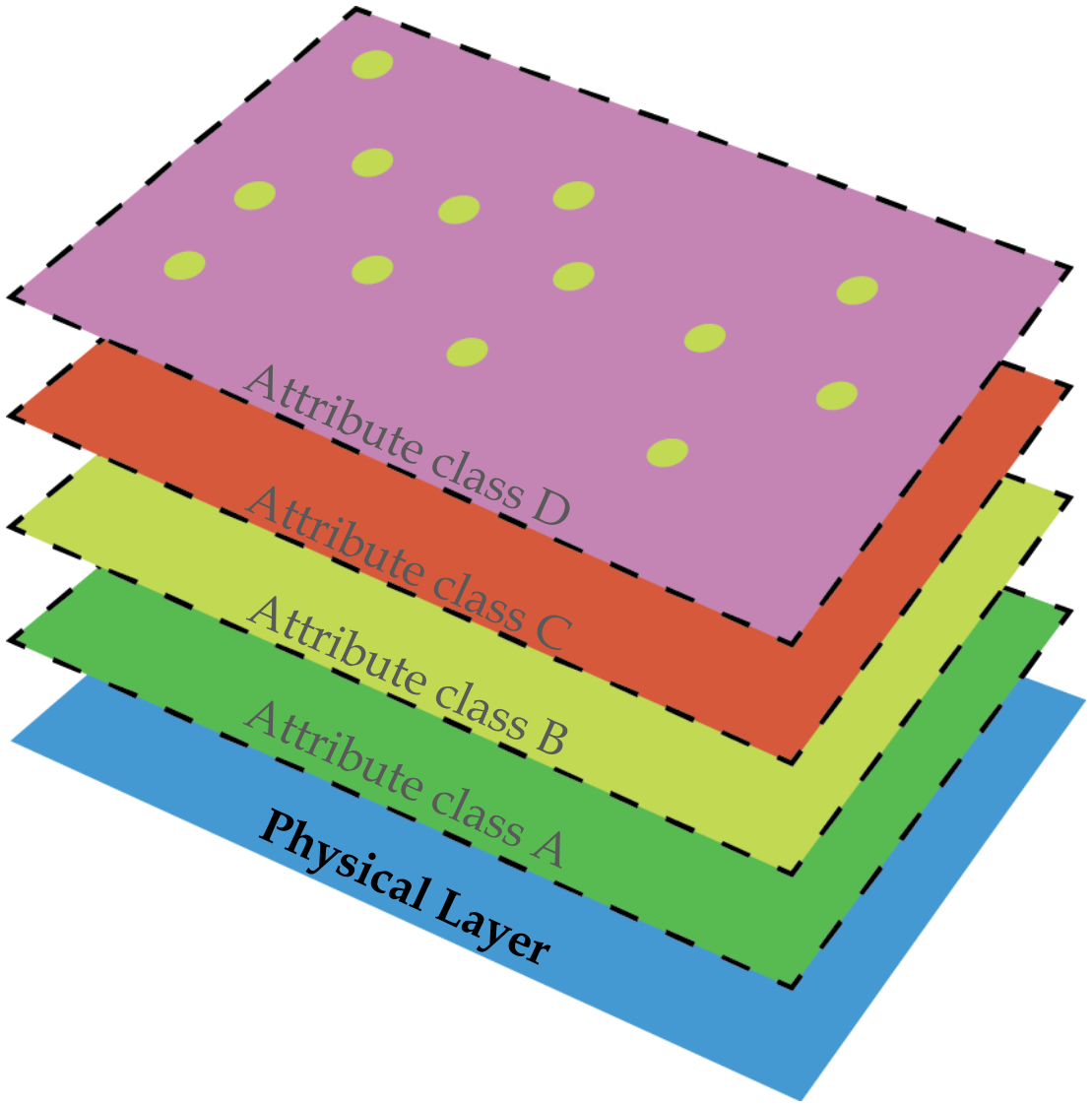
CAN-Bus Id ”11011001110”

Example:
The harvester needs to communicate with the truck in order to tell him when and where to take over the crop. The truck might ask asks:



Virtual Layers

Multi-layers structure

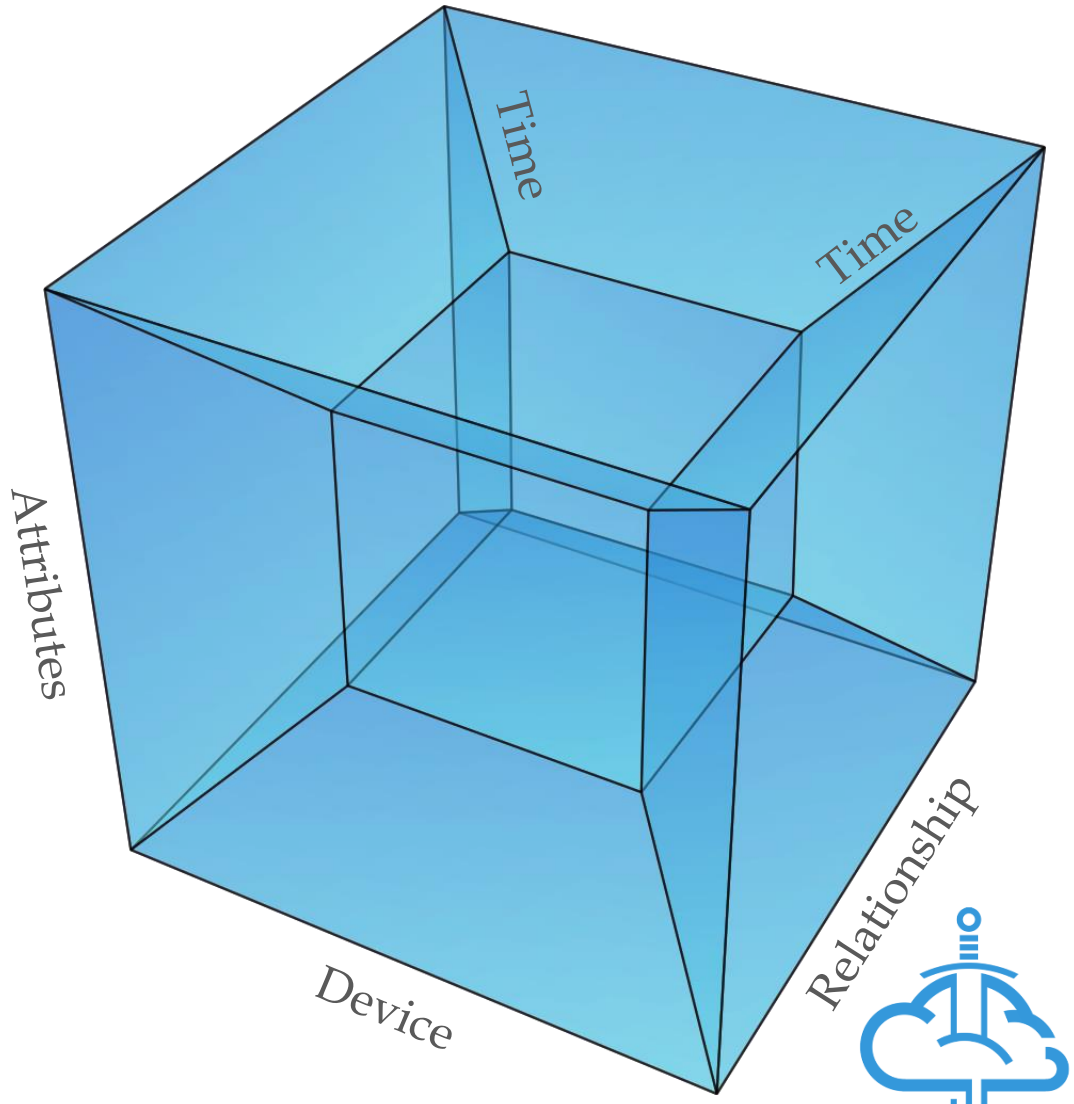


The physical layer is the only layer used for communication between devices.

On top of the physical layer other "virtual layers" can be defined to provide device attributes.

Tunable number of dimensions

Relationships between layers can be defined as needed thus creating new dimensions.



Attribute class definition

Attribute class D

Manufactured by

Attribute class C

Driven by

Attribute class B

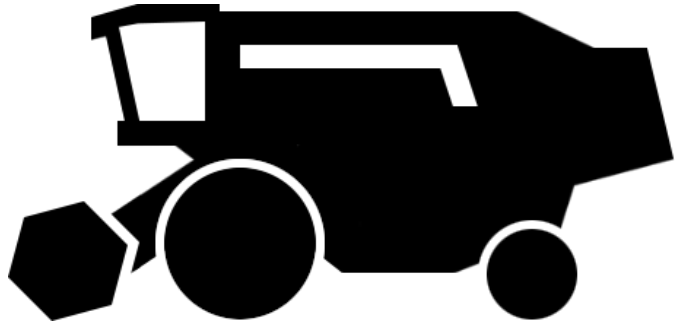
Owned by

Attribute class A

Located at

Physical Layer

Truck XYZ



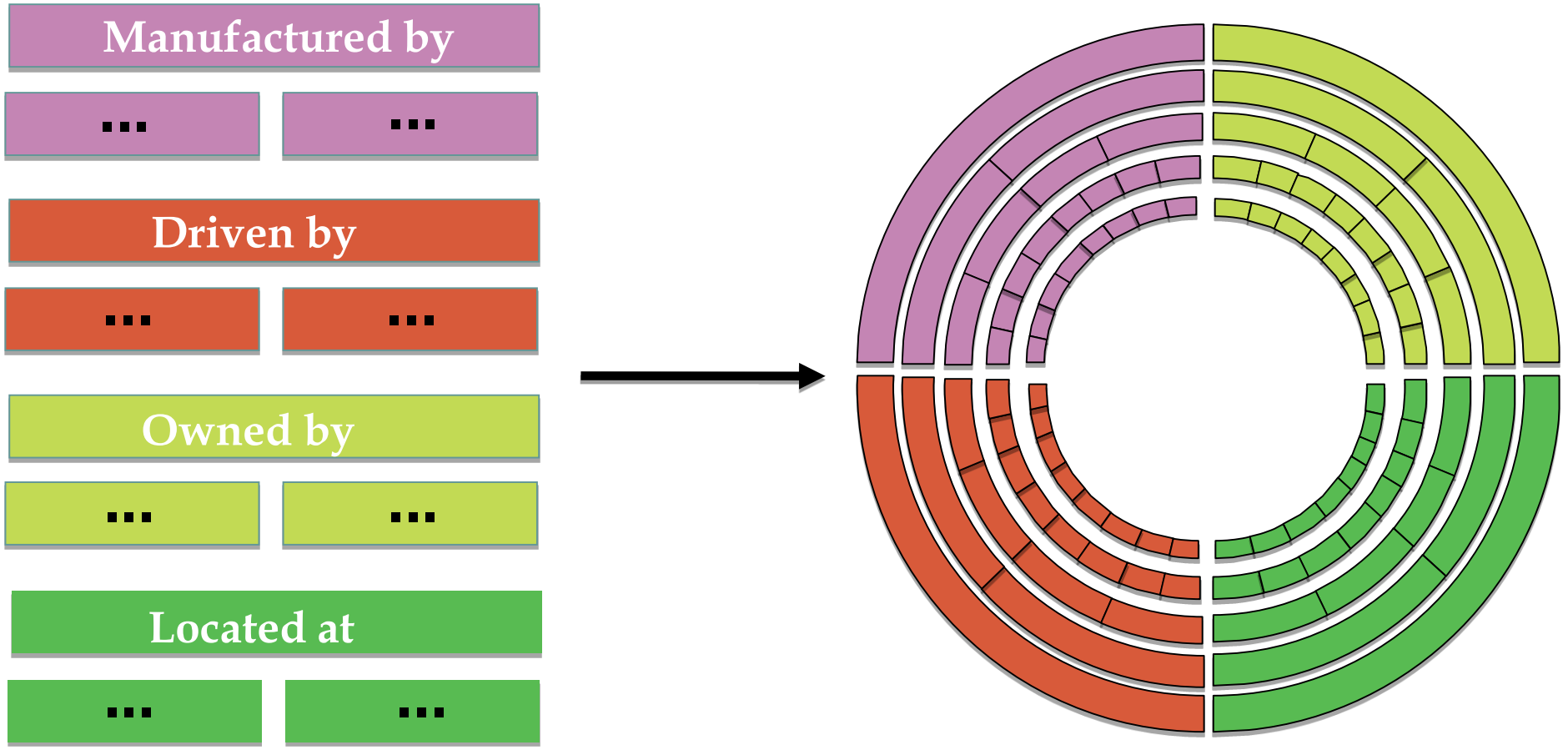
Claas

Ivan

Farmer Tom

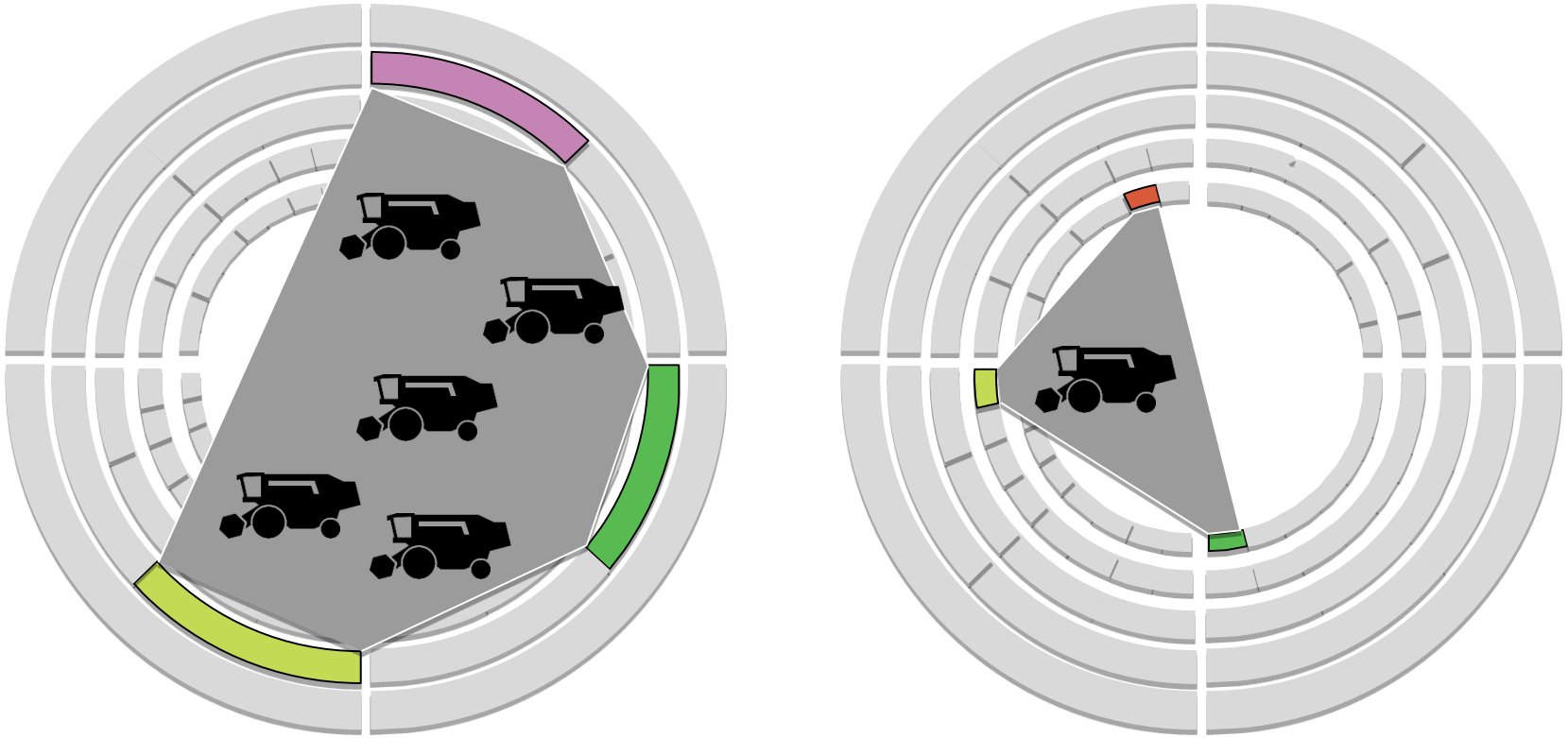
GPS position 34’23“ / 45’77“

Attribute Hierarchy



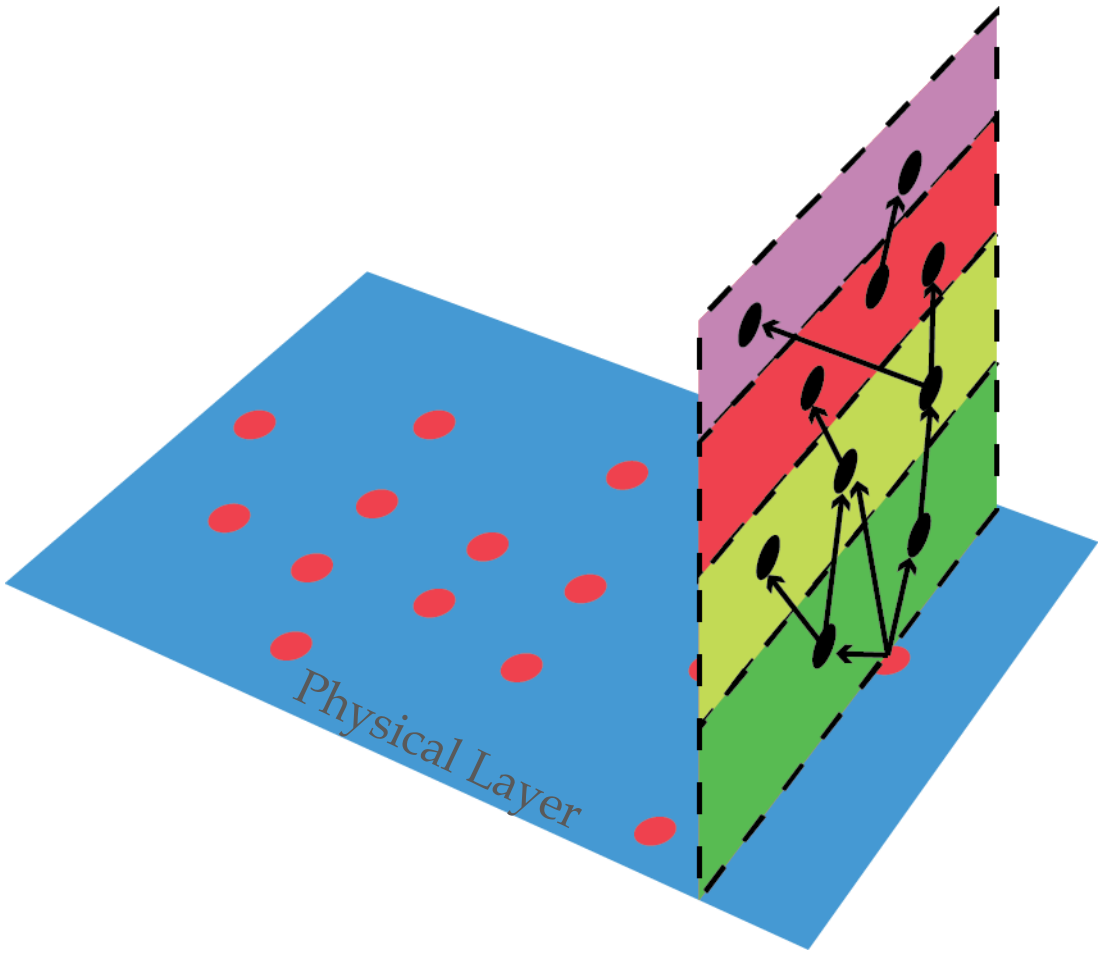
Circular tree structure of properties.

Attribute-based device discovery



The more accurate is the definition of an attribute, the more precise the result of the discovery process.

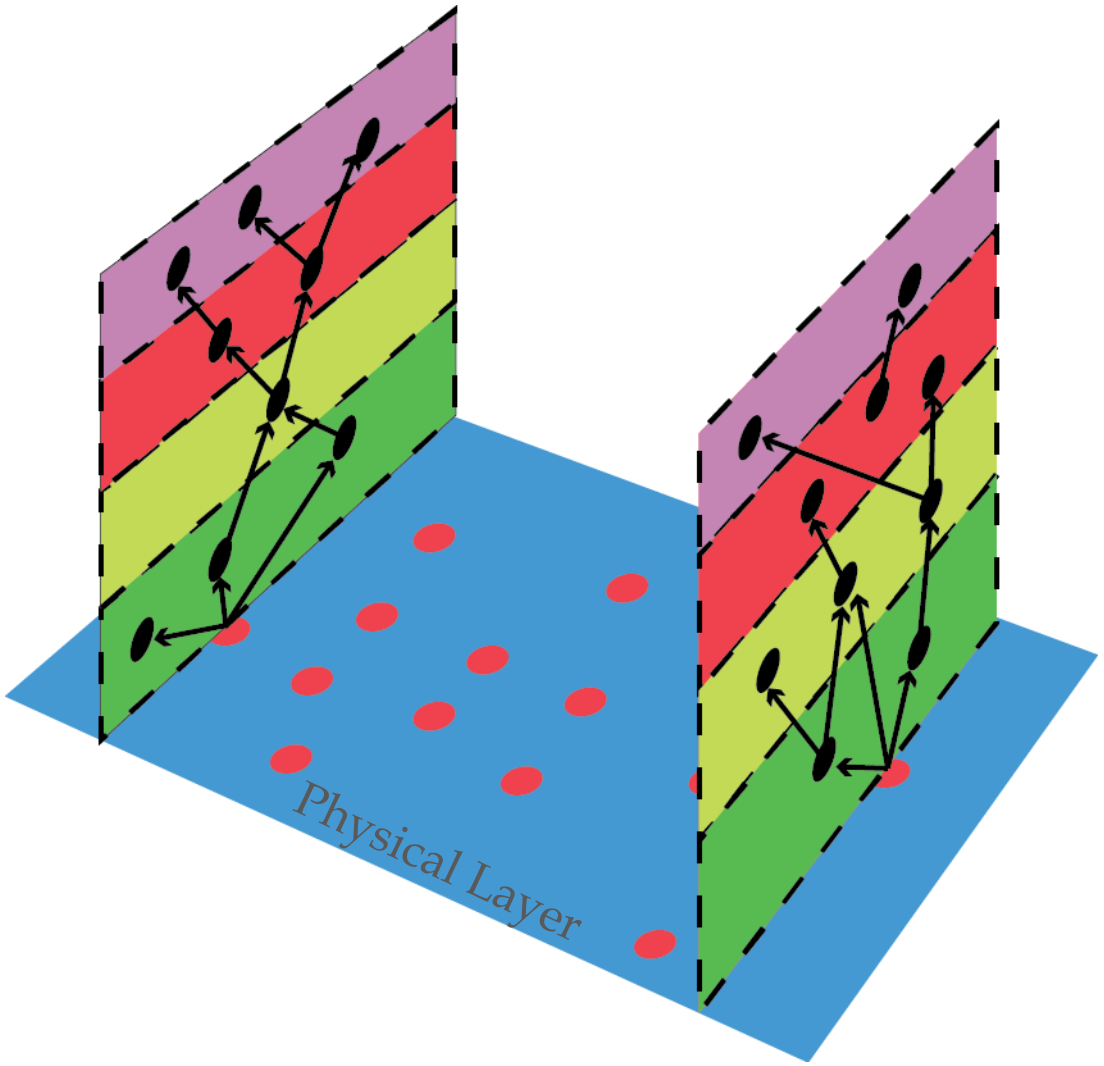
Inter-Layers Communications



Device attributes (also known as virtual nodes) are stored in a database within the device itself.

Resource constrained devices that cannot manage their own database can rely on more powerfull devices in the same local context.

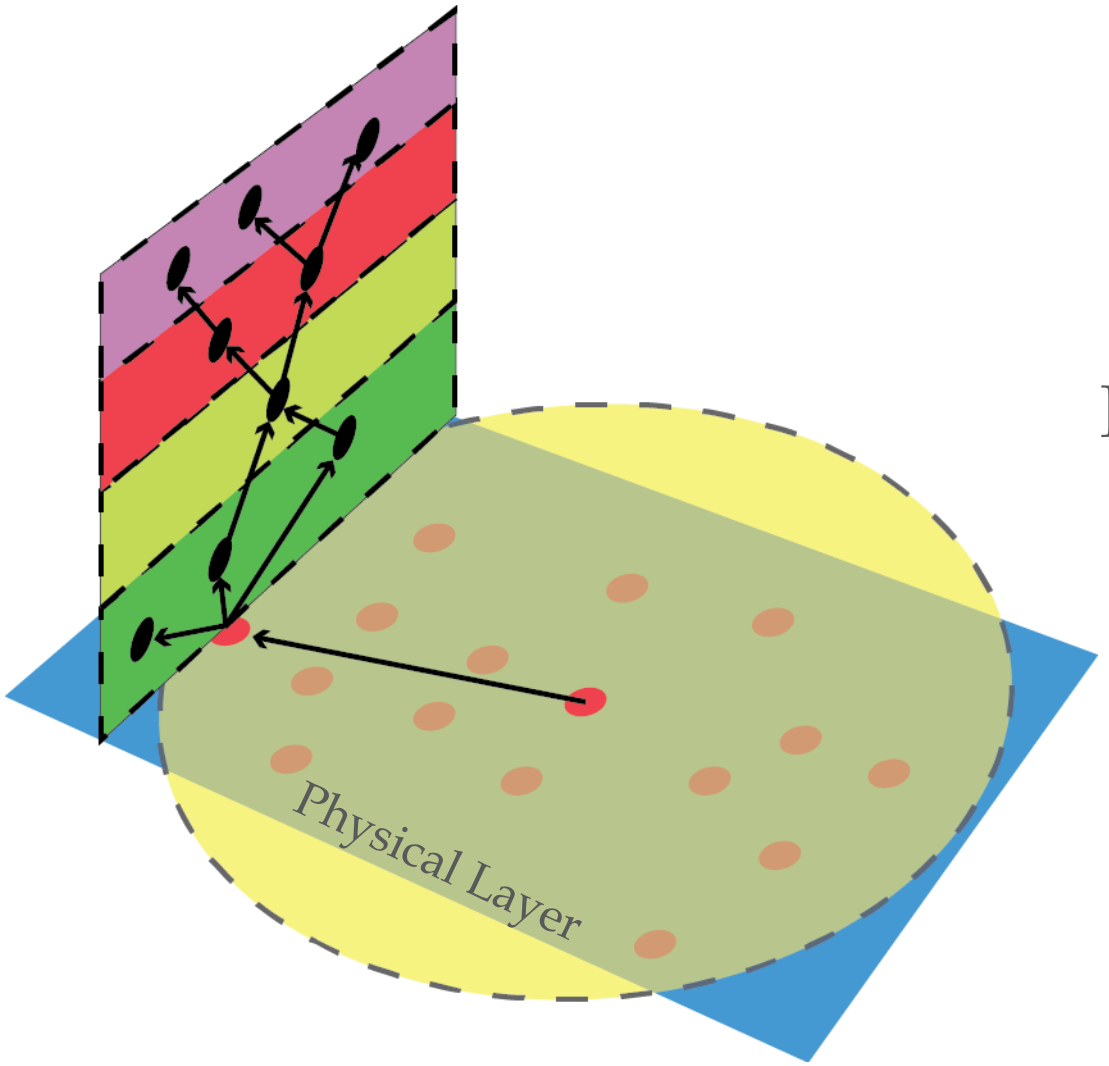
Inter-Devices Communications



Devices that have enough storage can keep track of attributes belong to other devices, thus being able to directly contact them.

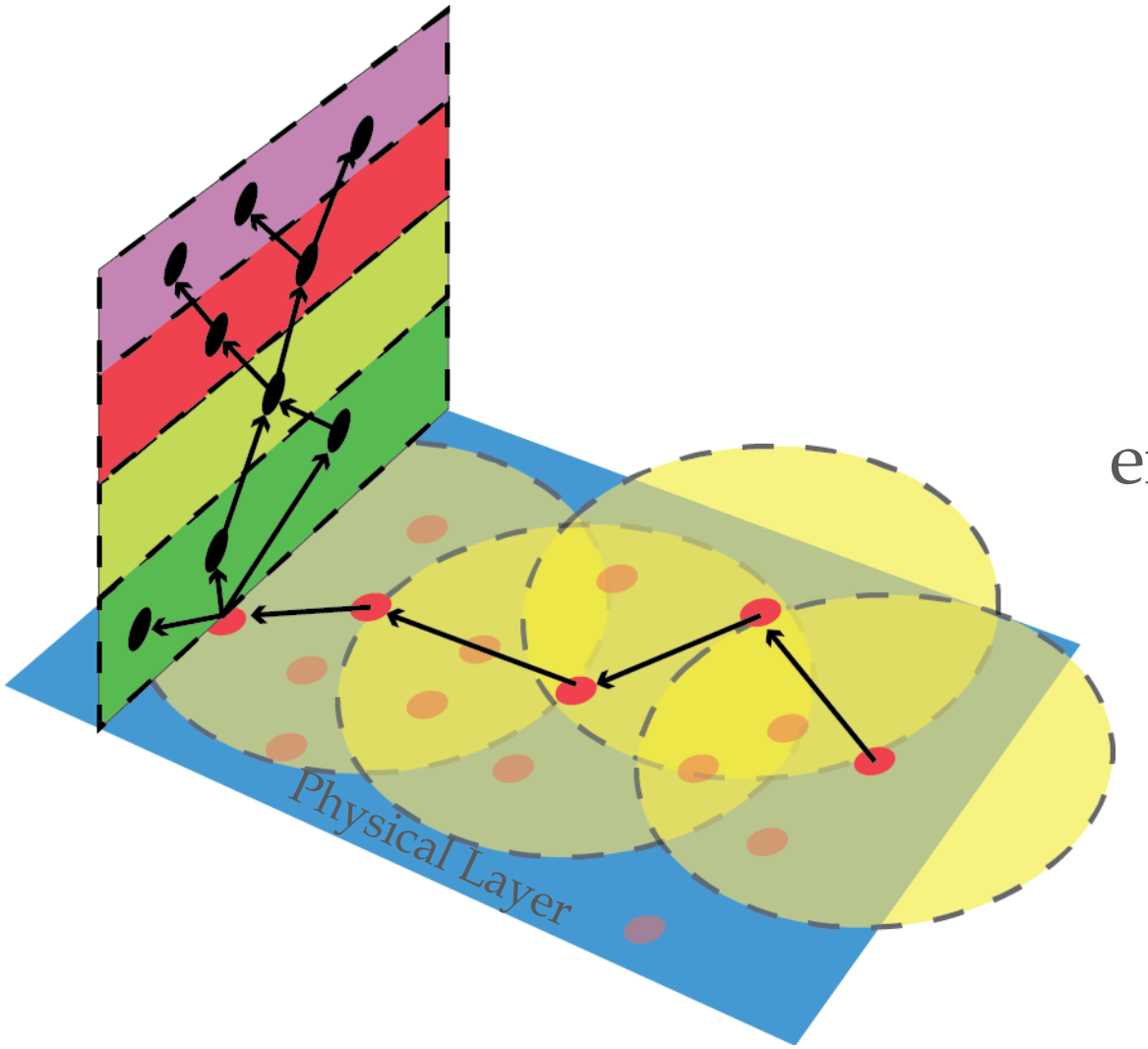
The communication between devices strictly depend on their resource constraints.

Direct Request



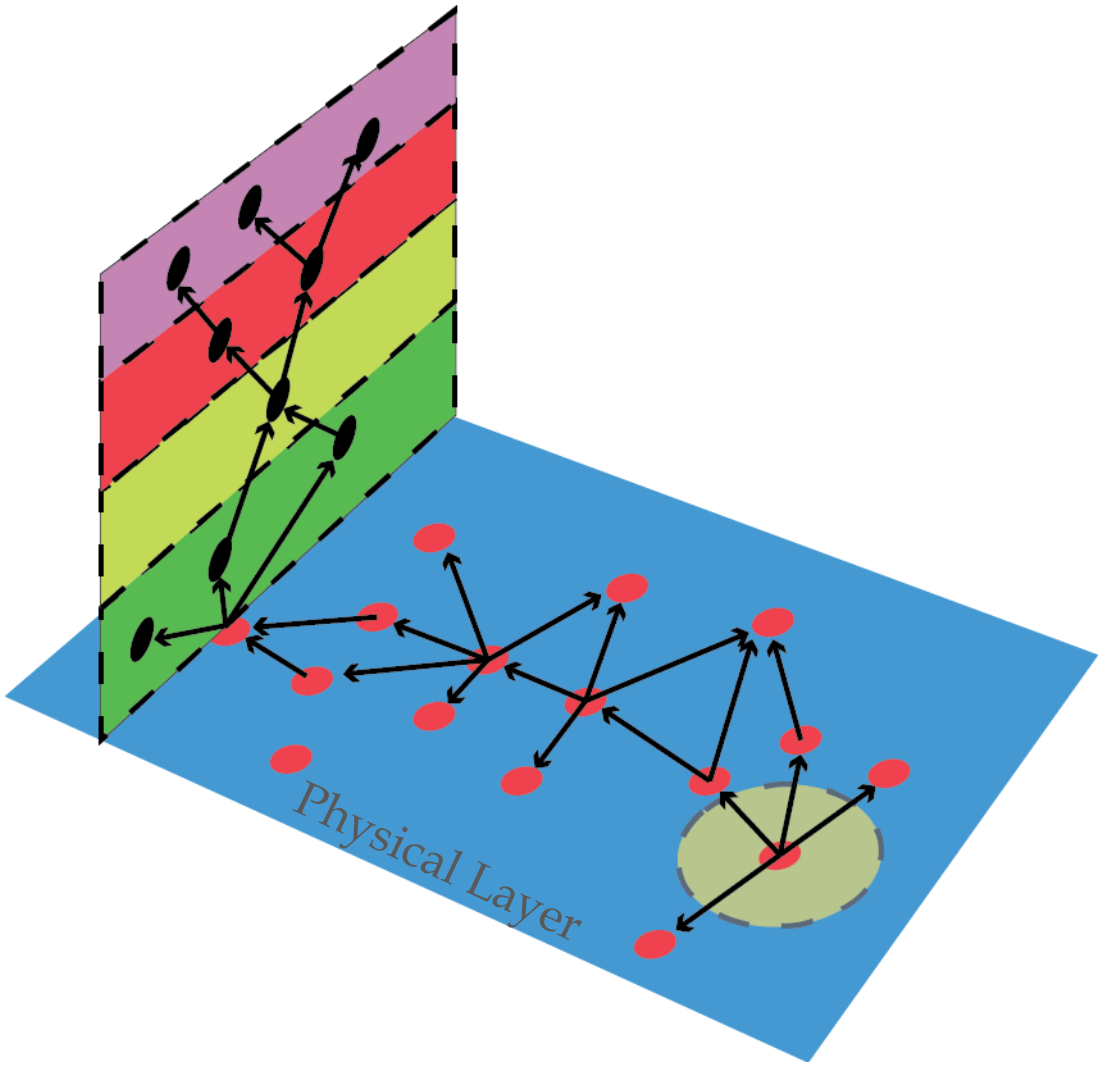
Known targets within the scope of the source node are directly queried.

Multi-hop request



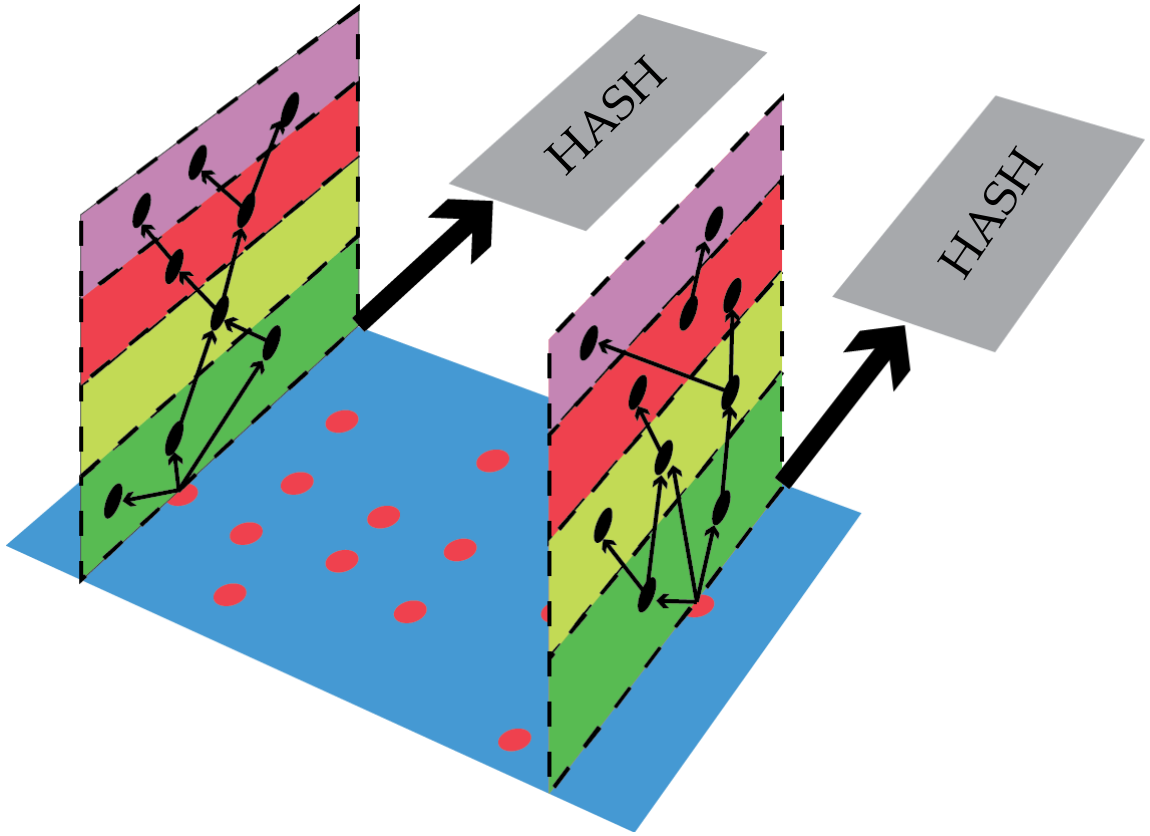
Known targets that are not close enough to the source node are queried with a multi-hop protocol

Broadcasted Request



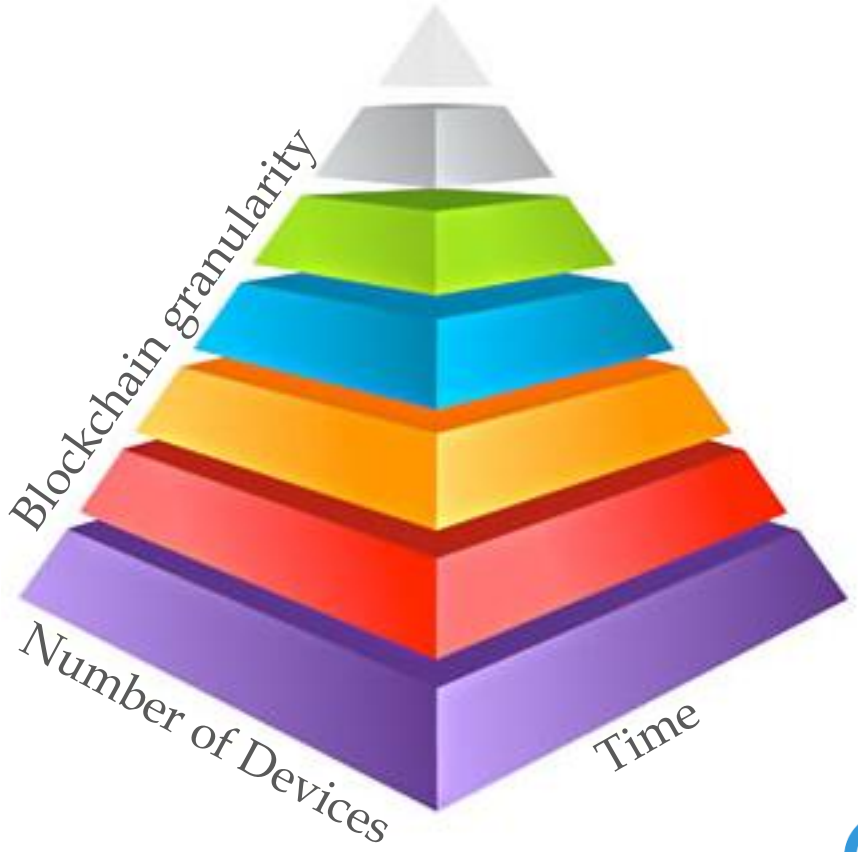
Unknown devices are discovered by a broadcast protocol.

Blockchain architecture



Blockchain construction

Blockchain structure



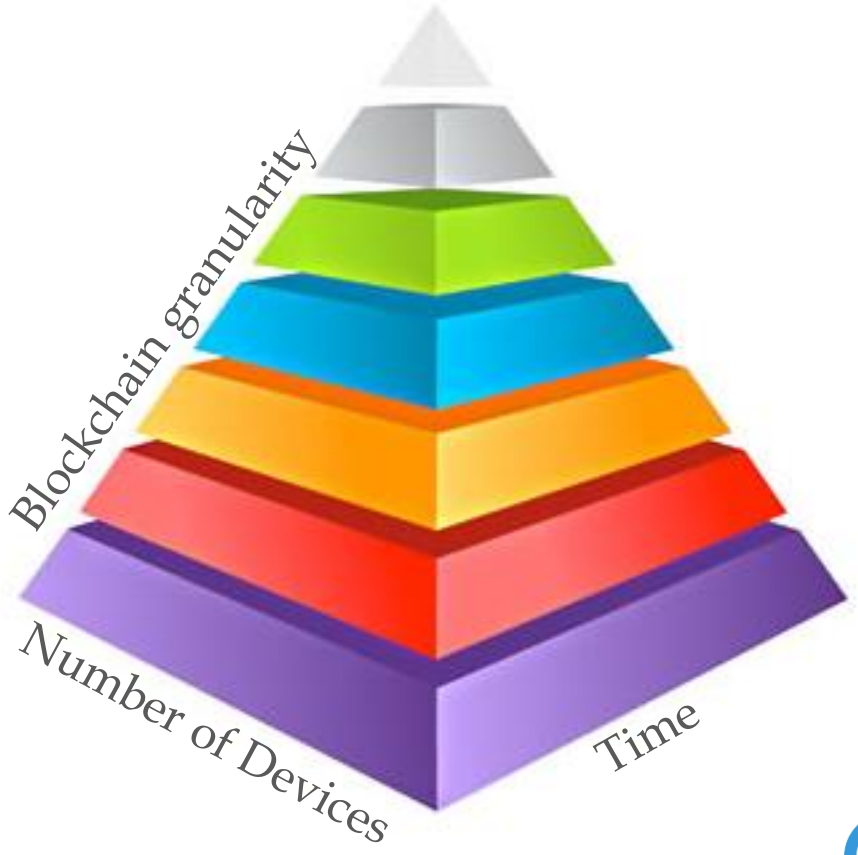
Blockchain security factor

The private blockchain provides a twofold security factor depending on the available resources:

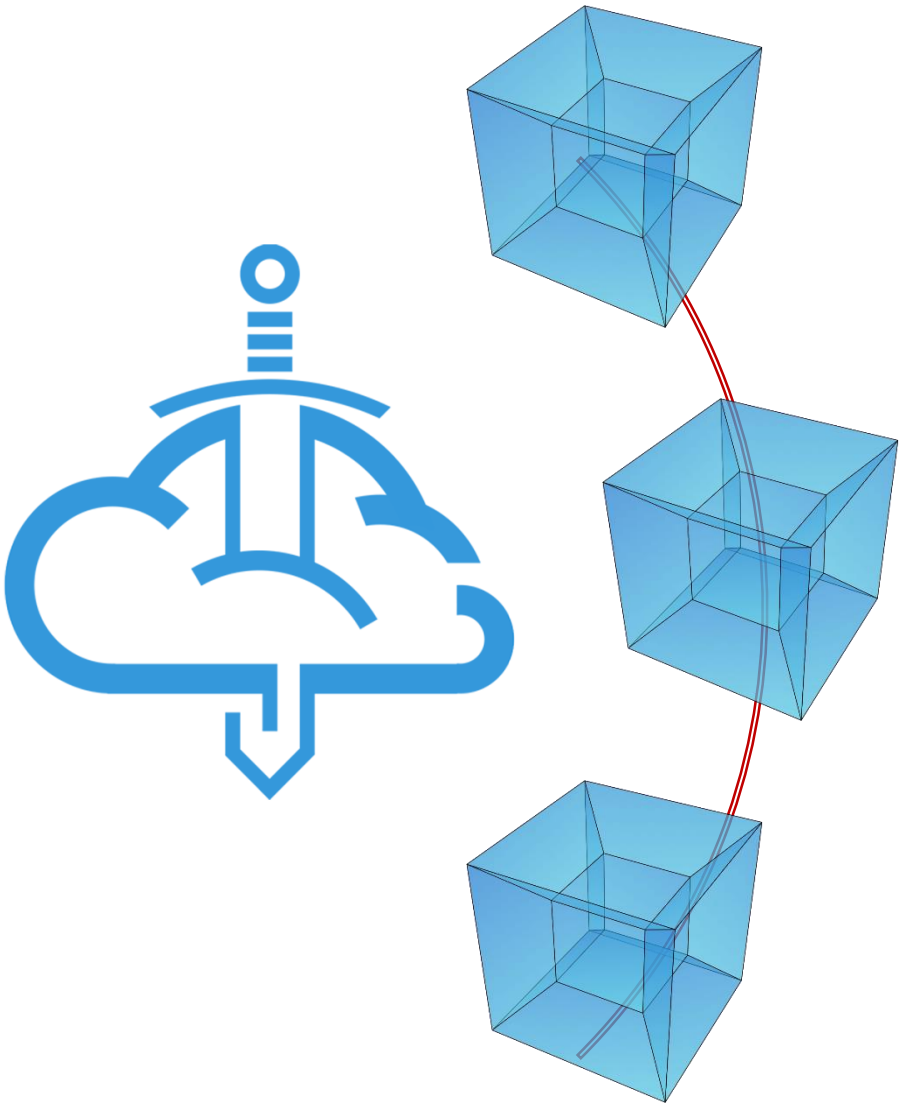
1)Allows a basic authentication approach based on past operations

2)Allows an advanced authentication approach based on the interaction continuity and behaviour analysis

Blockchain structure



Inter-blockchain communications



Excalibur is used as trusted anchor to provide cooperation and interaction between local contexts

Query are not processed at any time by Excalibur that only has the burden to provide secure and private interactions between different blockchains