



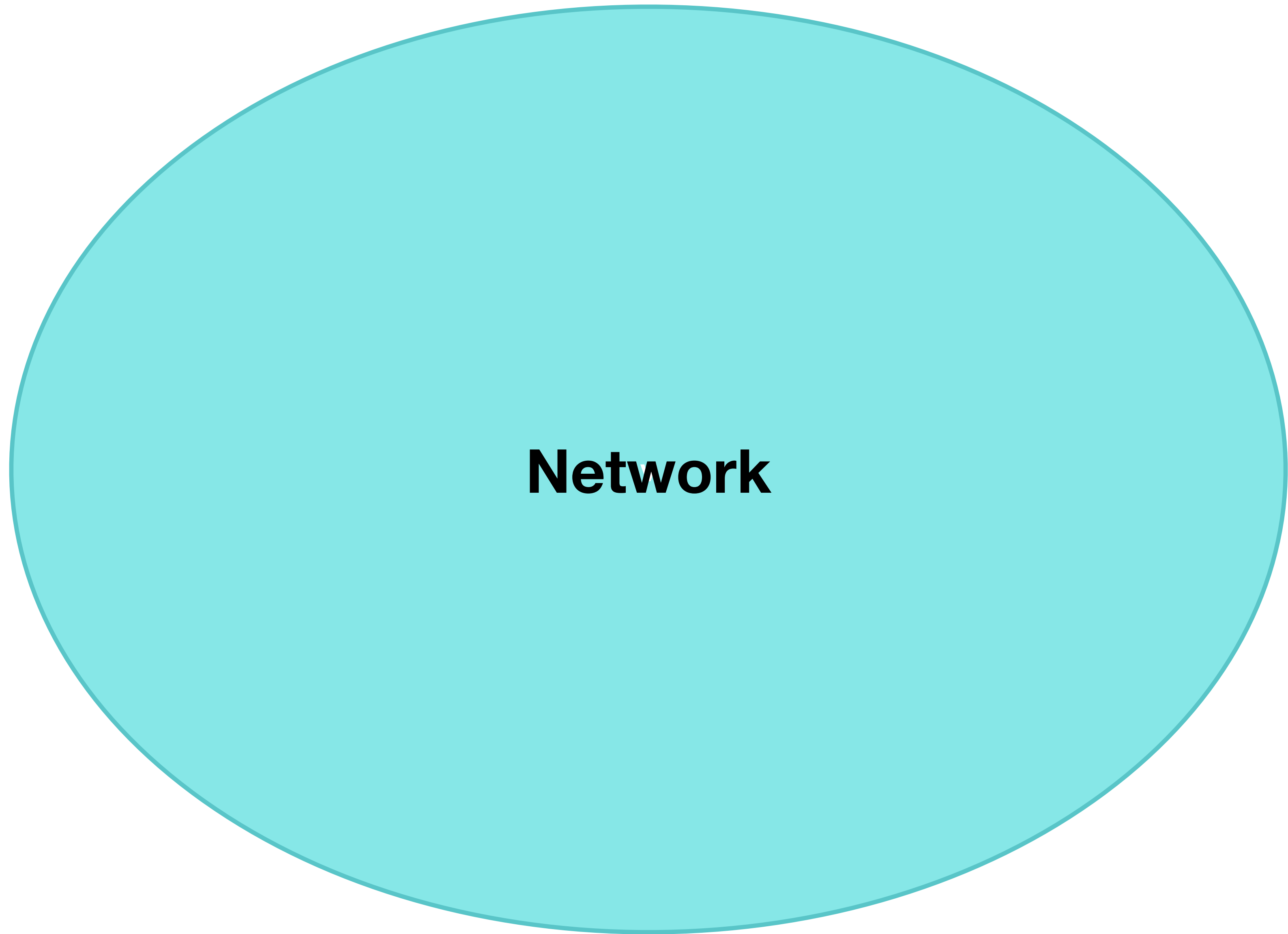
HUMAN COLOSSUS
FOUNDATION

Active and Passive Identifiers

Elements, objects and characteristics
of a decentralized network

Paul Knowles

October 20th, 2020

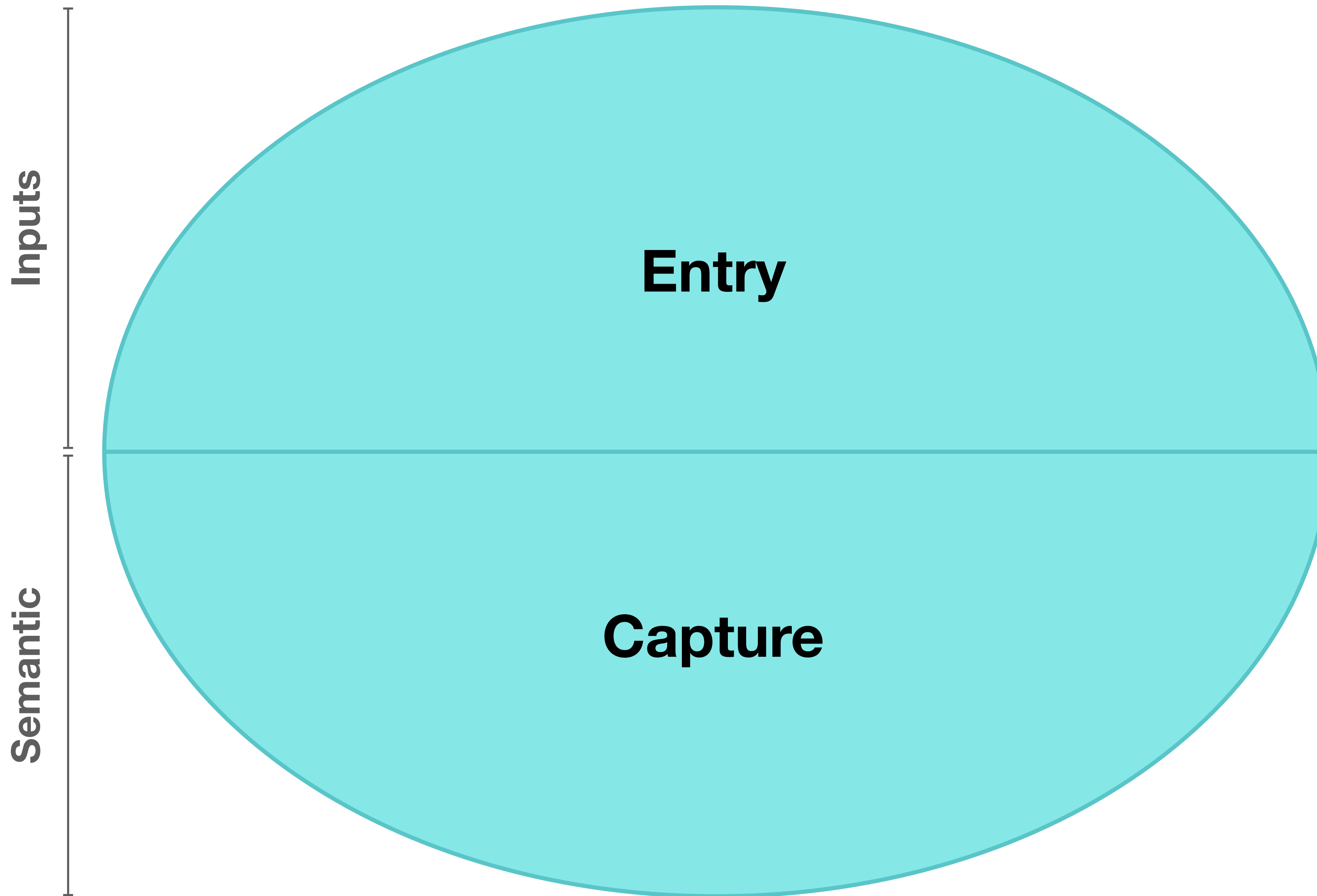


Network characteristics ...

A digital network must contain authenticable data entry and immutable data capture elements in order to maintain balance and integrity.

Within the context of a decentralized network, these fundamentals enable a self-regulating system where ...

- (1) data inputs can be trusted as having come from an assured source under the control of a governing entity; and*
- (2) semantic items ensure that the meaning and use of inputted data remains unaltered for all interacting actors.*

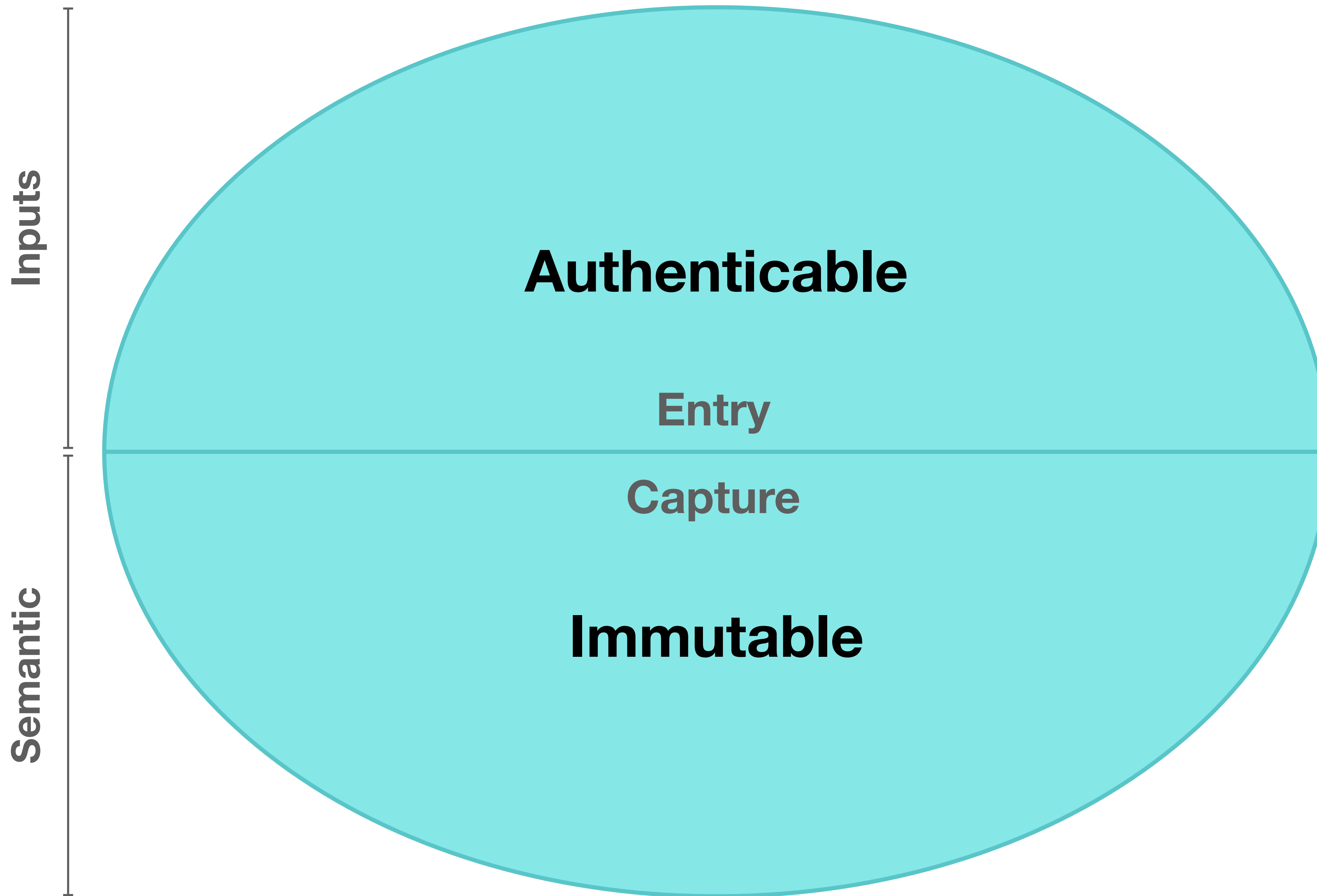


Identifier characteristics ...

The characteristics of the identifier types required for data entry and data capture differ.

- In the case of data entry, items are identified by active identifiers, a type of identifier that requires a signing key to authenticate the identity of an active governing entity.

- In the case of data capture, items are identified by passive identifiers, a type of identifier that has an association with a cryptographic hash of digital content which acts as an immutable fingerprint to identify a passive non-governing entity, an inanimate object or a static data input.



“Authenticable” vs “Immutable”

A hash grid table describing the different identifier states:

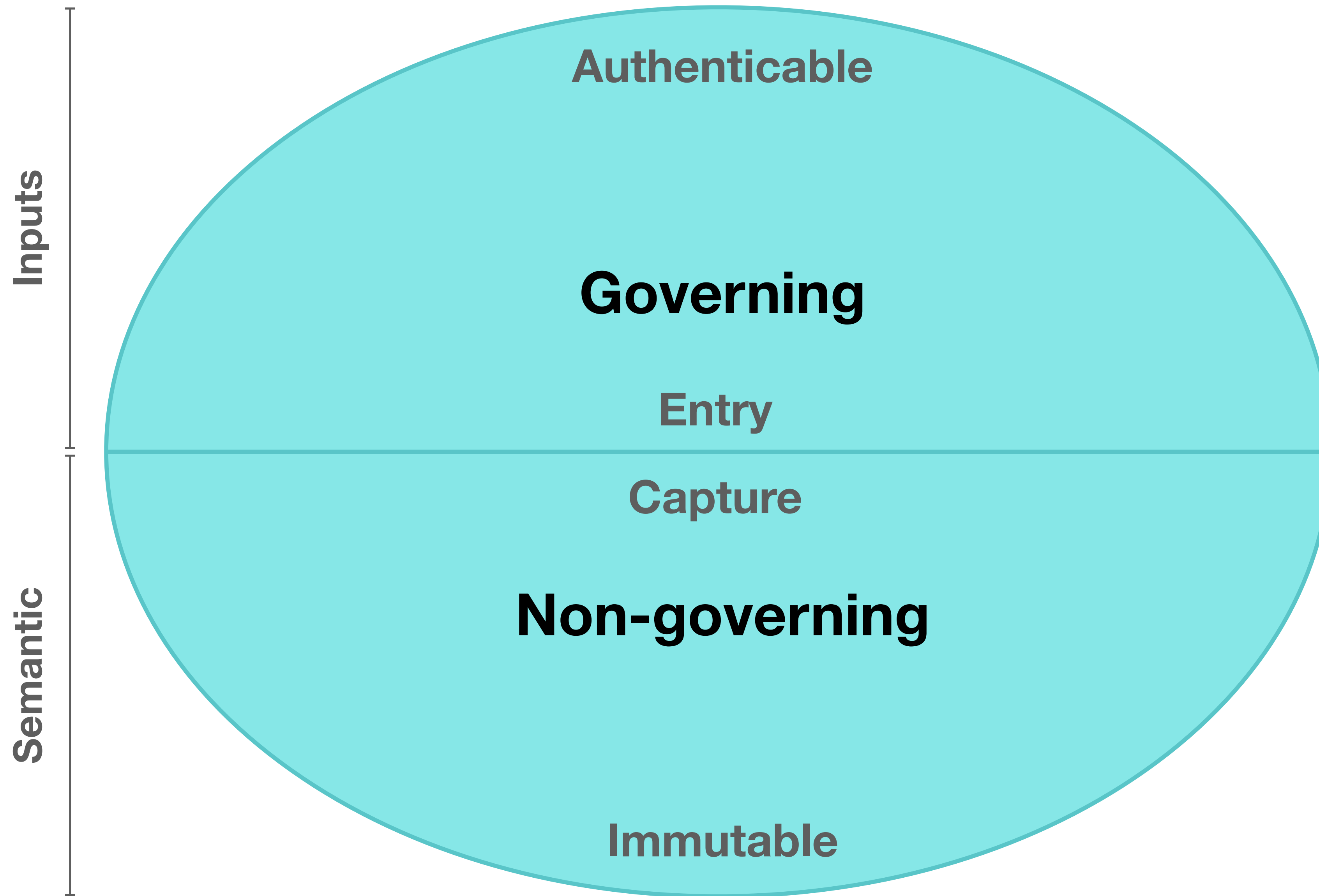
State	Governing	Non-governing
Authenticable	Active	Passive controlled by active
Immutable	Active controlled by passive <i>(This state cannot exist)</i>	Passive

Authenticable

The identifier requires a signing key for identity authentication.

Immutable

The identifier has an association with a cryptographic hash of digital content. Any change to the binary state of a single byte of the digital content will invalidate the hash. A hash value is an immutable fingerprint for digital content.



“Governing” vs “Non-governing”

A hash grid table describing the different identifier states:

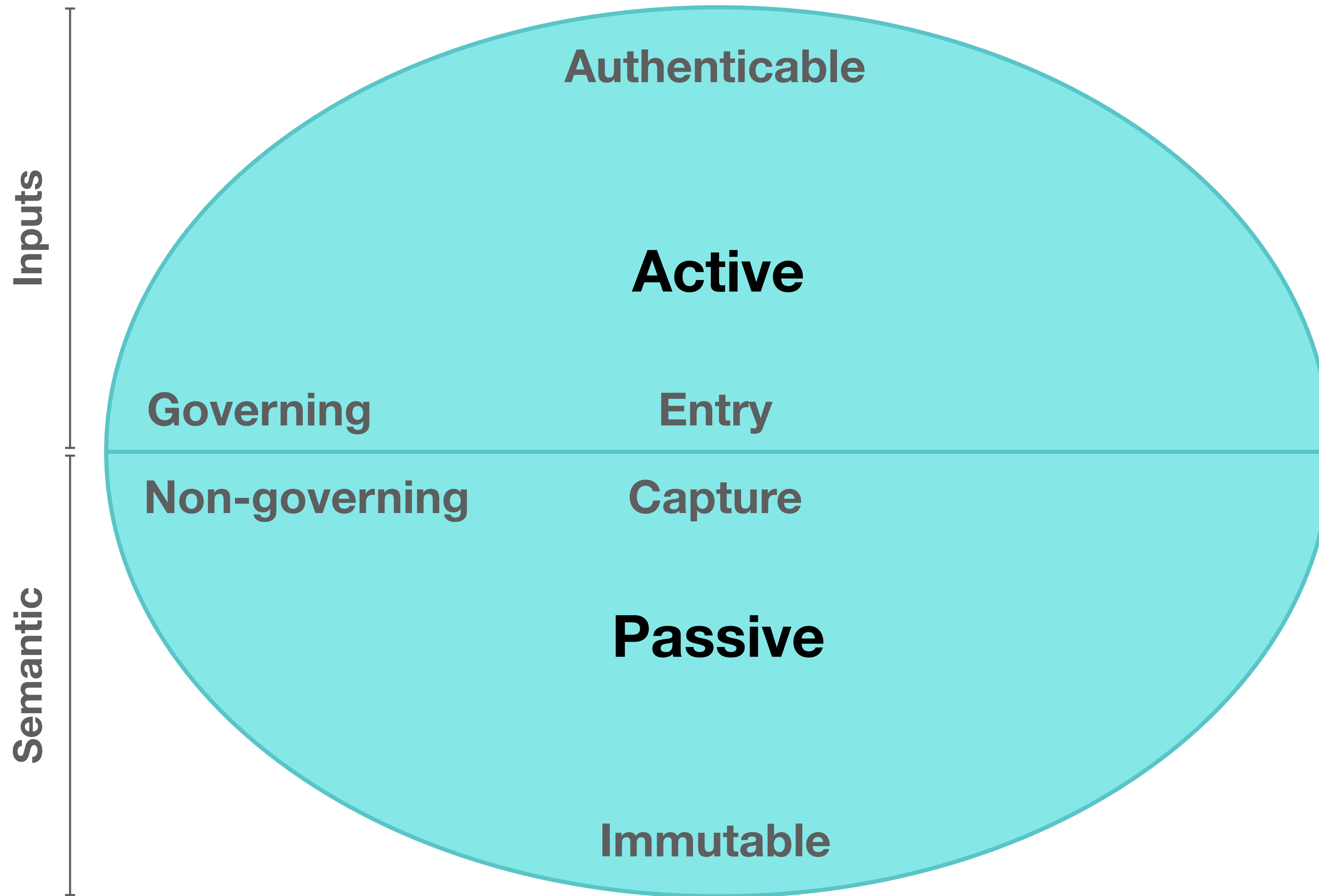
State	Governing	Non-governing
Authenticable	Active	Passive controlled by active
Immutable	Active controlled by passive <i>(This state cannot exist)</i>	Passive

Governing

The identifier identifies an entity that has the capacity to govern.

Non-governing

The identifier identifies a non-governing entity, an inanimate object or a static data input.



“Active” vs “Passive”

A hash grid table describing the different identifier states:

State	Governing	Non-governing
Authenticable	Active	Passive controlled by active
Immutable	Active controlled by passive <i>(This state cannot exist)</i>	Passive

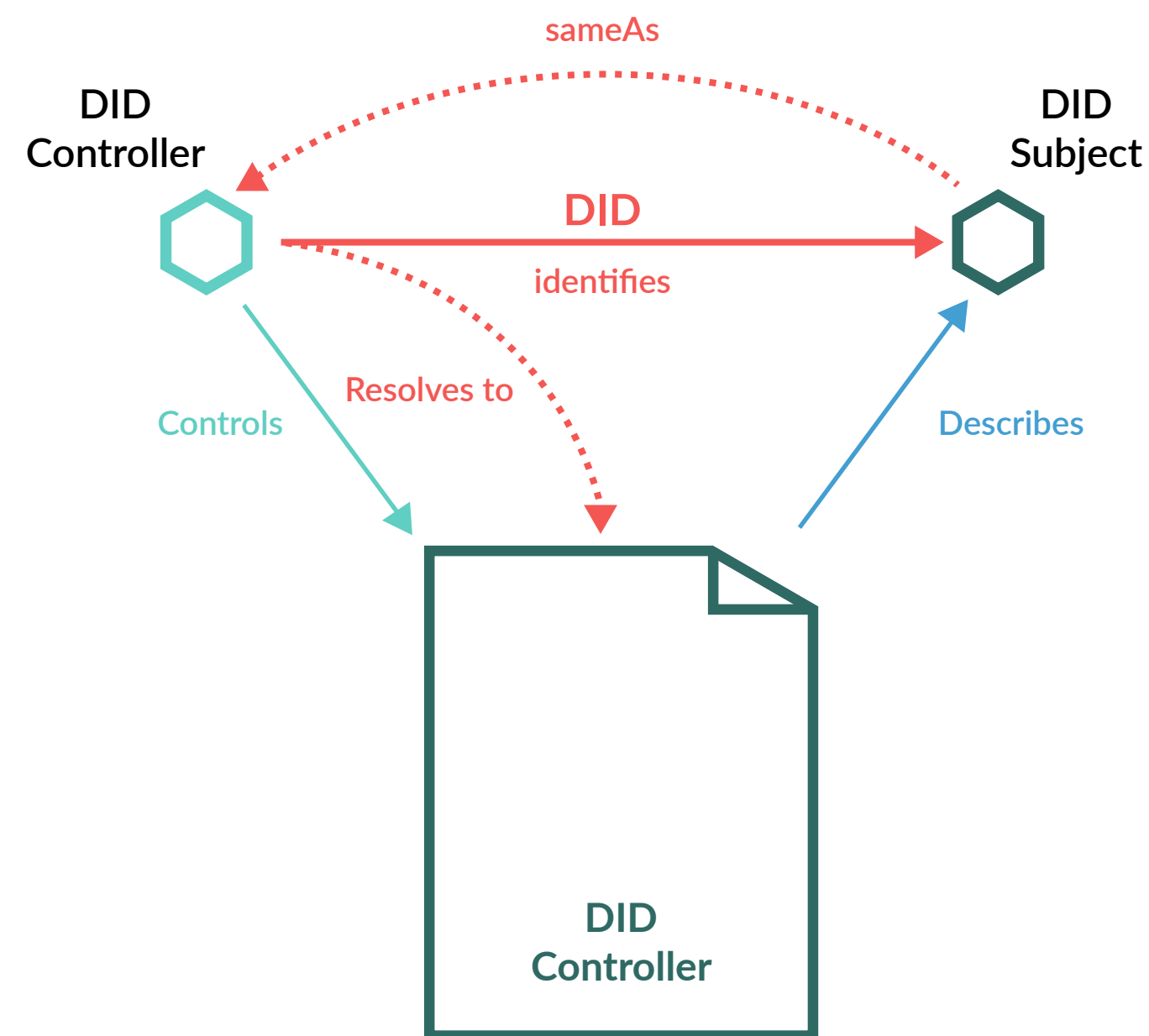
Active

An identifier that requires a signing key to authenticate the identity of an active governing entity. An active identifier cannot be controlled by a passive identifier.

Passive

An identifier that has an association with a cryptographic hash of digital content which acts as an immutable fingerprint to identify a passive non-governing entity, an inanimate object or a static data input. A passive identifier can either be (1) controlled by an active identifier or (2) not controlled.

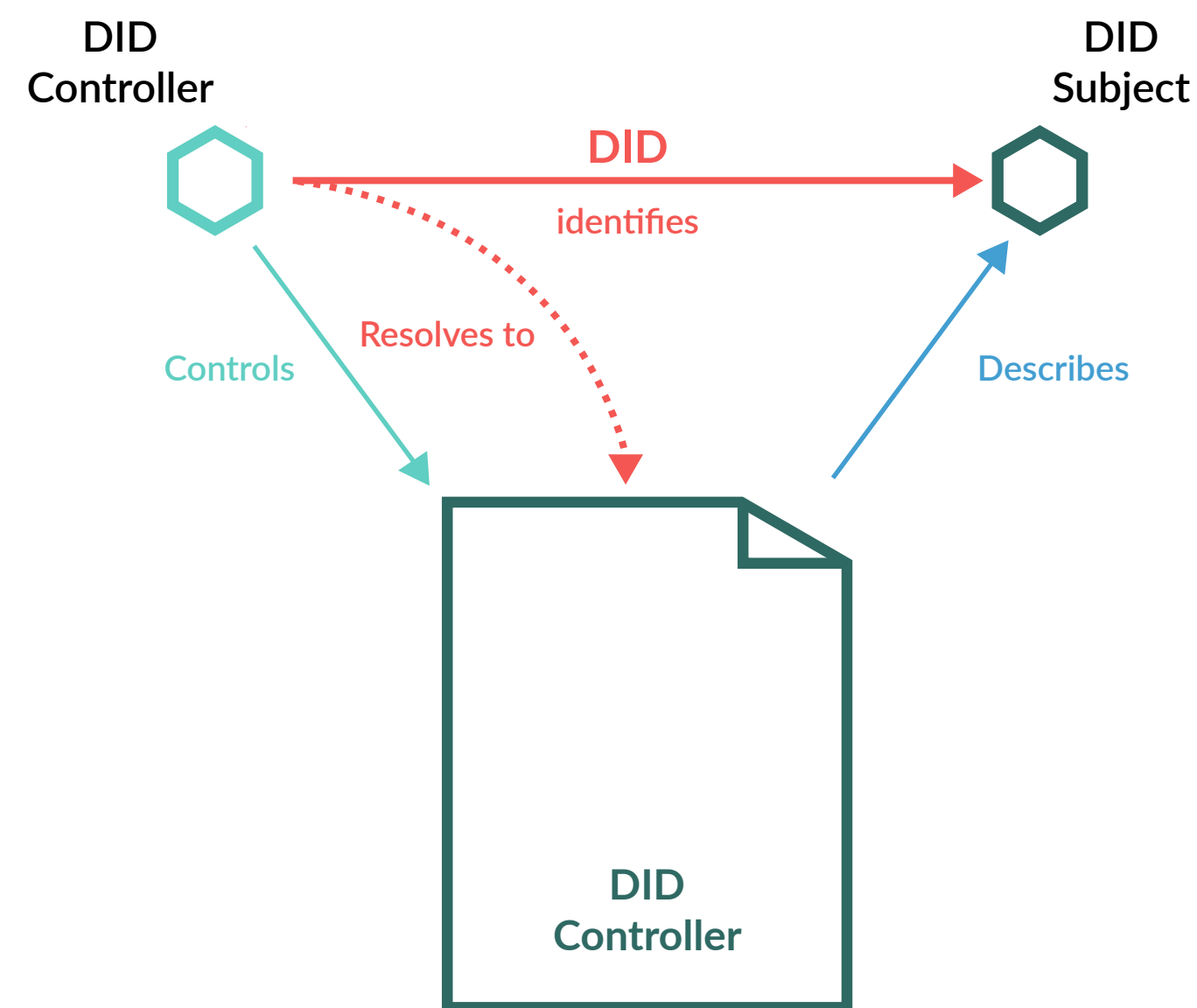
Active state



Example of an active identifier

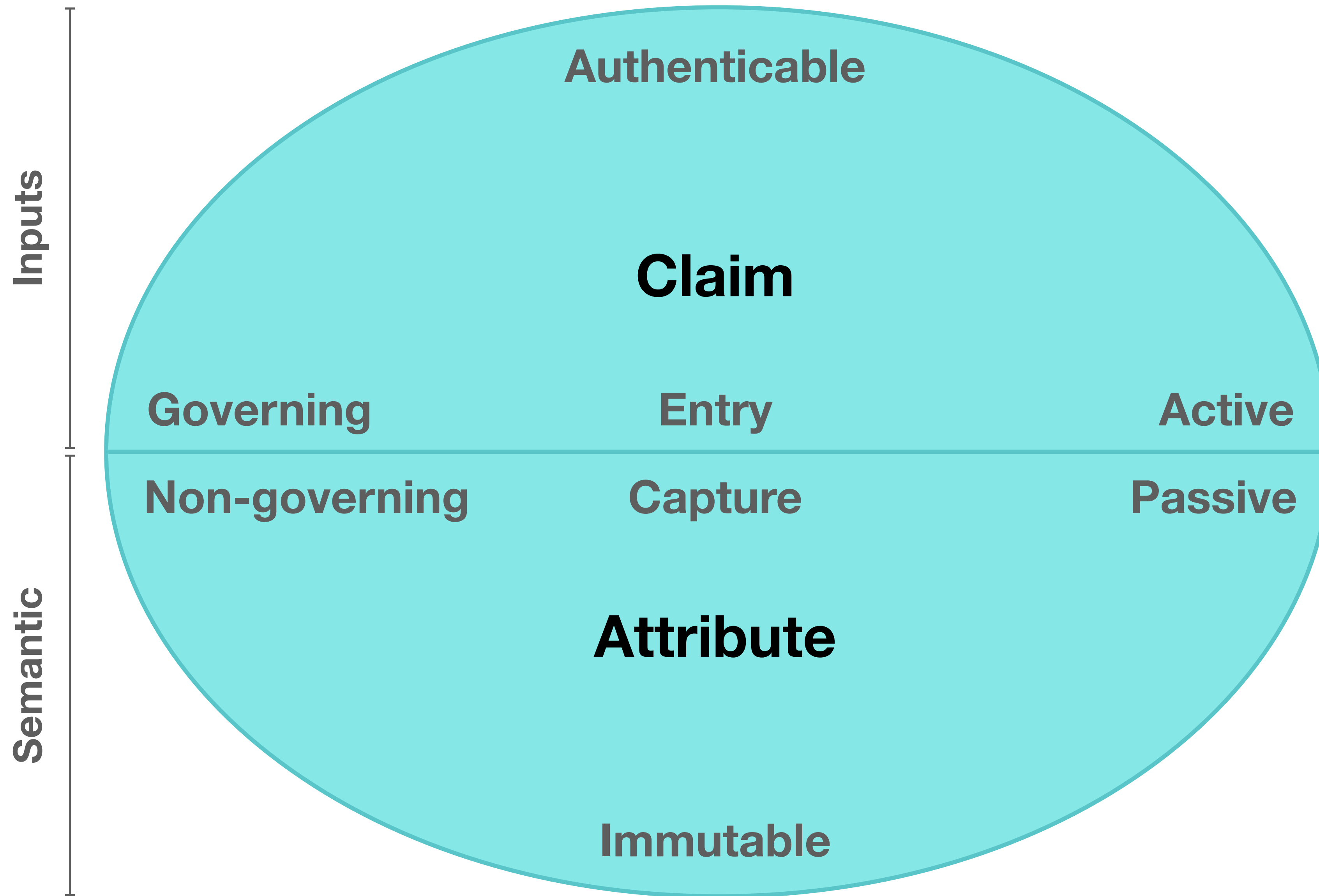
The figure shows an instance when the DID subject is the same as the DID controller. In this scenario, the controller represents itself, an active entity that requires a signing key for identity authentication. Through the authentication process, the controller is able to establish full rights of control over the active identifier.

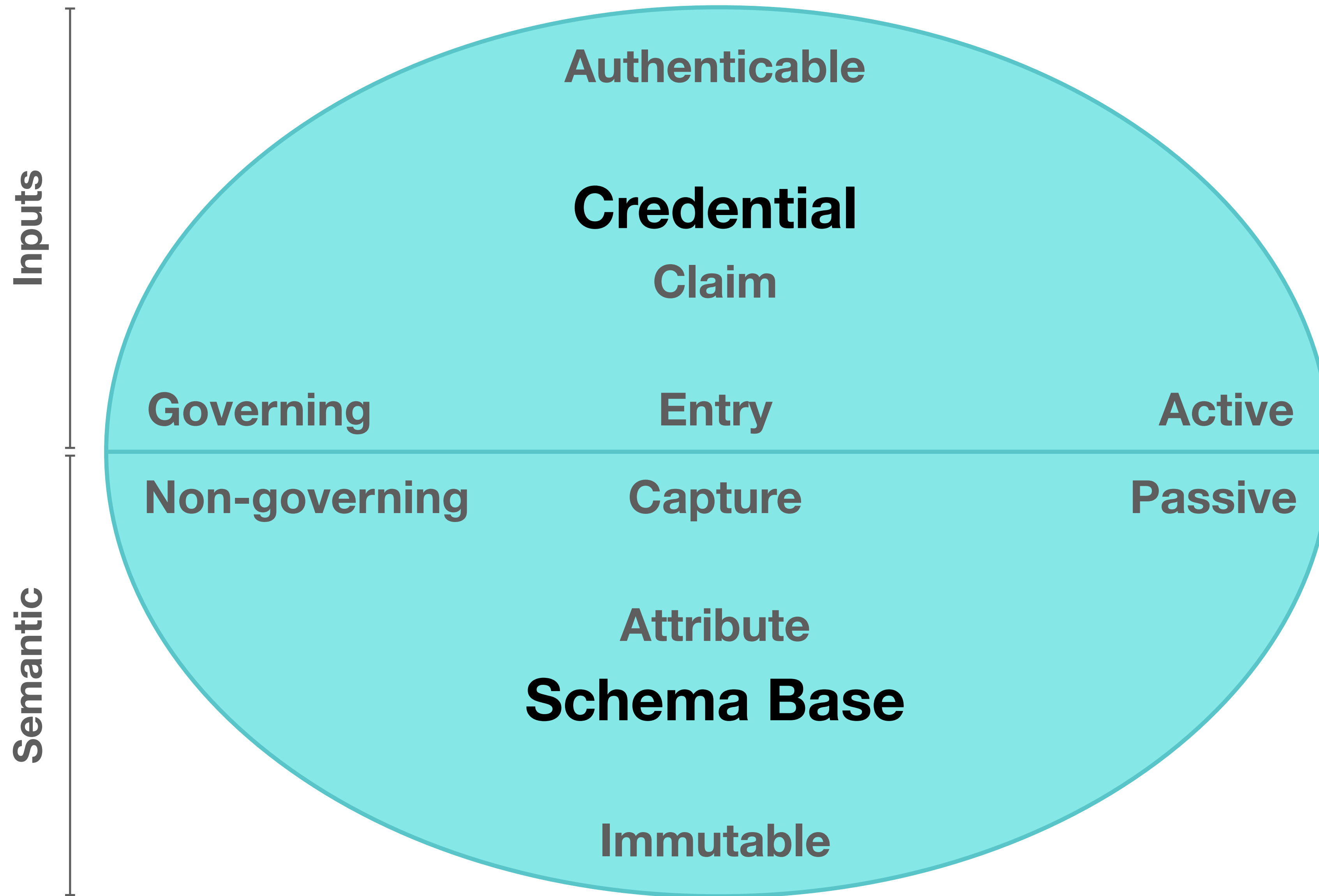
Passive state



Example of a controlled passive identifier

The figure shows an instance when the DID subject may not be the same as the DID controller. In this scenario, the subject may represent a passive non-governing entity, an inanimate object or a static data input with the controller's DIDs being active, requiring a signing key for identity authentication. Through the authentication process, the controller is able to express ownership, control, or management of the passive resource.

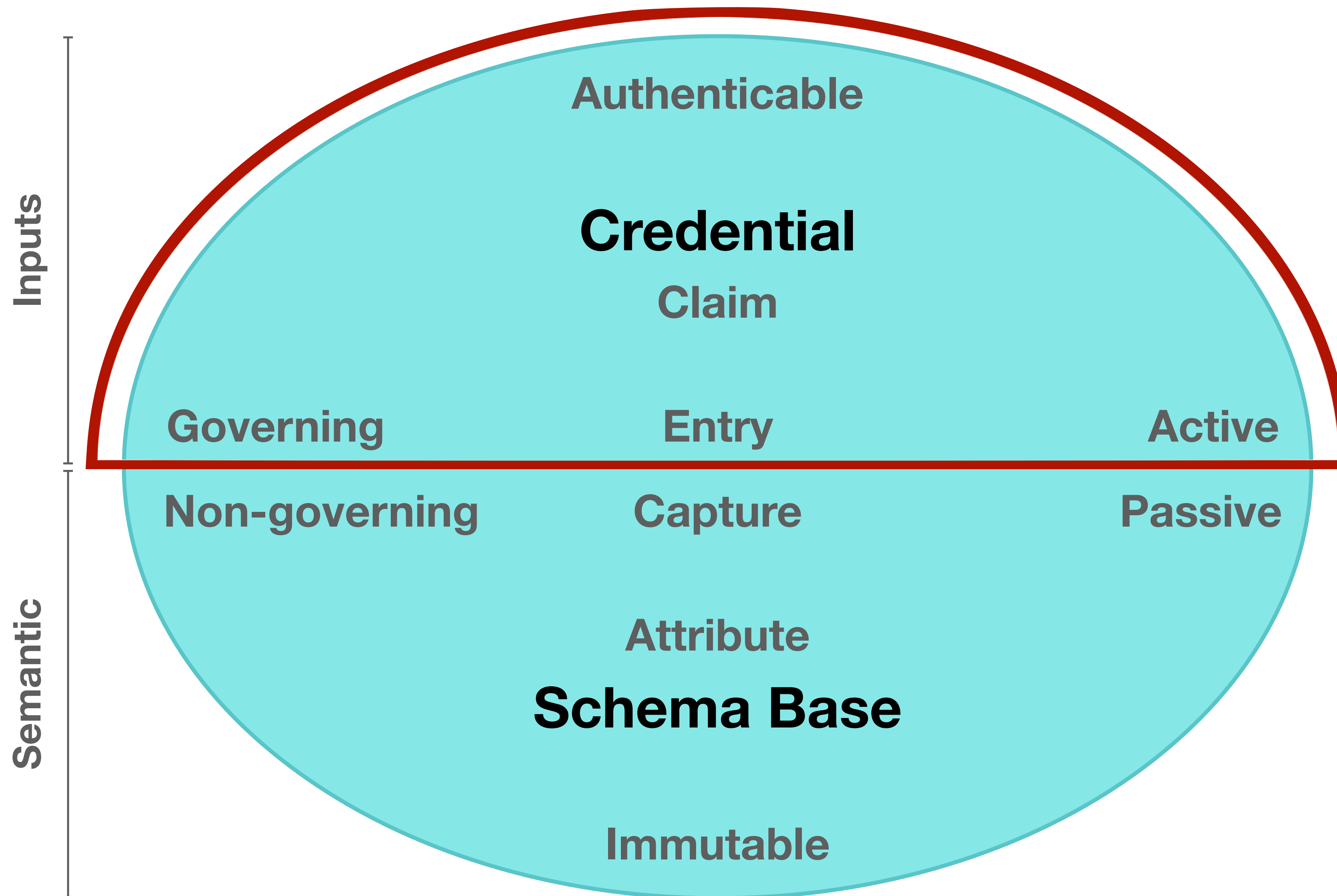




Inputs domain

["the active domain"]

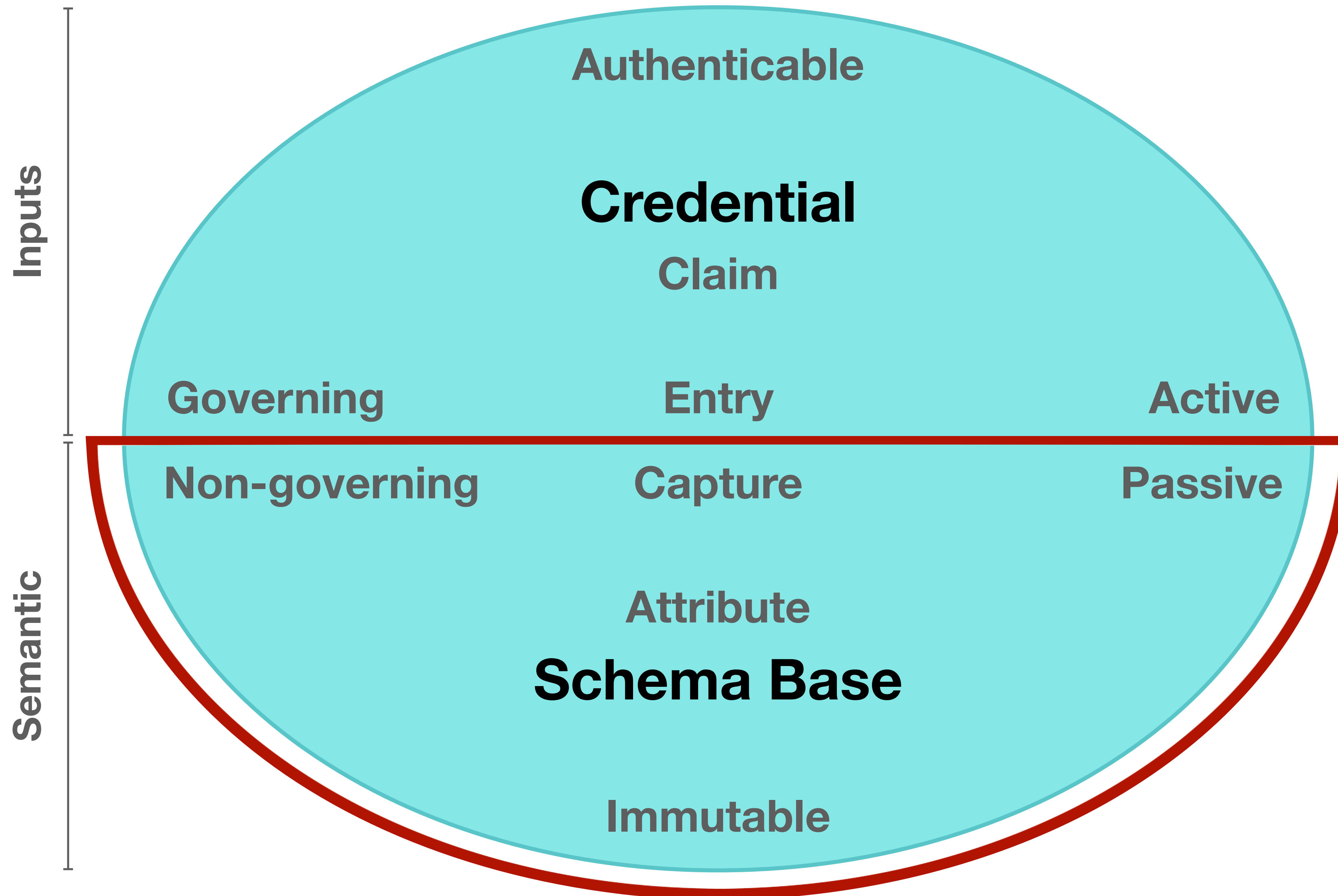
*What is put in, taken in, or operated on
by any process or system.*



Semantic domain

["the passive domain"]

*The meaning and use of what is put in, taken in,
or operated on by any process or system.*



Summary statement

Active identifiers bring authenticability and passive identifiers bring immutability to a decentralized network.



HUMAN COLOSSUS
FOUNDATION

▶ Paul Knowles paul.knowles@humancolossus.org