

# Authentic Chained Data Containers

## ToIP Technical Working Group Task Force

Wiki: <https://wiki.trustoverip.org/display/HOME/ACDC+%28Authentic+Chained+Data+Container%29+Task+Force>

Slack: tswg-acdc-tf

White Paper: <https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/ACDC.web.pdf>

*Samuel M. Smith Ph.D.*  
*[sam@samuelsmith.org](mailto:sam@samuelsmith.org)*

v1.03

2021-01-15

# Its all about Automated Reasoning

Automated Business Process Workflows as Automated Decision Processes

*Secure Attribution* is essential to cross entity decision processes and cross entity data supporting those decision processes.

*Decentralized Automated Decision Making* depends on securely attributable decision process data flows.

Secure Attribution provided by a portable decentralized identity system security overlay for data in motion and at rest.

Automated Reasoning with *Authentic Data*

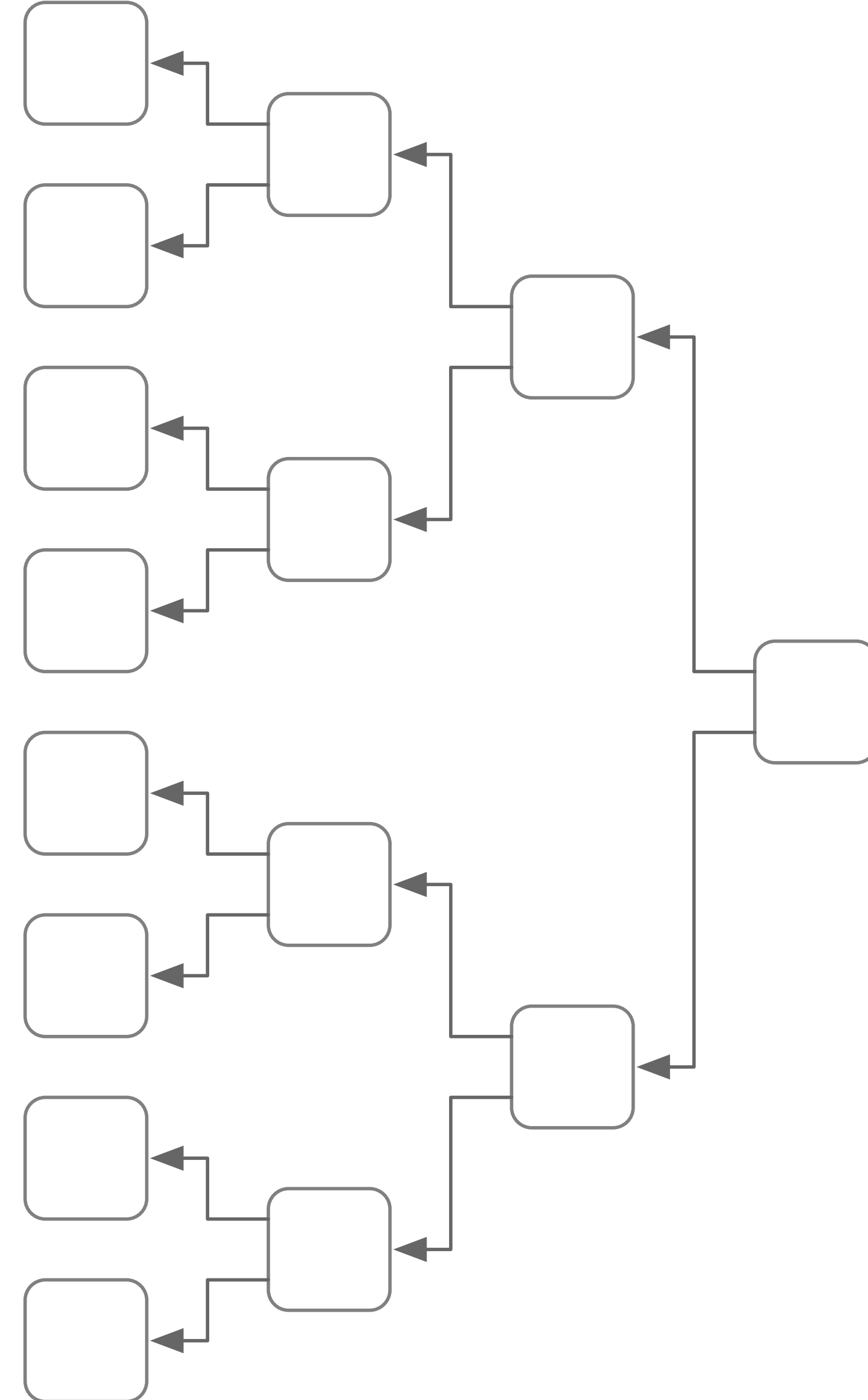
*Decision Making: finding actions that best satisfy goals and constraints*

# Authentic = Provenanced = Securely Attributed

Securely Attributed = Nonrepudiably Authenticated

Secure Attribution (Authentic Provenance):

Chain, Tree, or Graph



# Authenticity Verification

Digital Signatures for Verifiable Authenticity

Verifiable Authenticity = Authenticatable

Securely Attributable via Verifiable Non-repudiable Digital Signatures

Authenticity Verification Models (for VCs)

# Terminology

**credential:** evidence of authority, status, rights, entitlement to privileges, or the like.

**license:** formal permission from a constituted authority to do something, as to carry on some business or profession.

a certificate, tag, plate, etc., giving proof of such permission; official permit: a driver's license.

**authorization:** permission or power granted by an authority; sanction.

In decision making context, **authentic credential** = proof of satisfaction of authority constraint

# Authenticity Verification (Attribution/Provenance) Model Properties

Bipartite vs. Tripartite vs. Multipartite

Open Loop vs. Closed Loop

Chained vs. Unchained

Aggregative vs. Unaggregative

Weighted vs. Unweighted (Qualified vs Unqualified)

Attenuable vs. Unattenuable

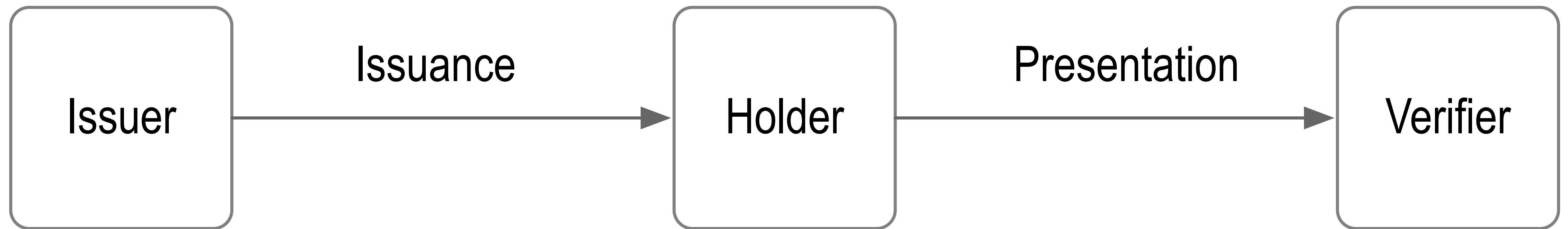
Persistent vs. Ephemeral

Implicit vs. Explicit

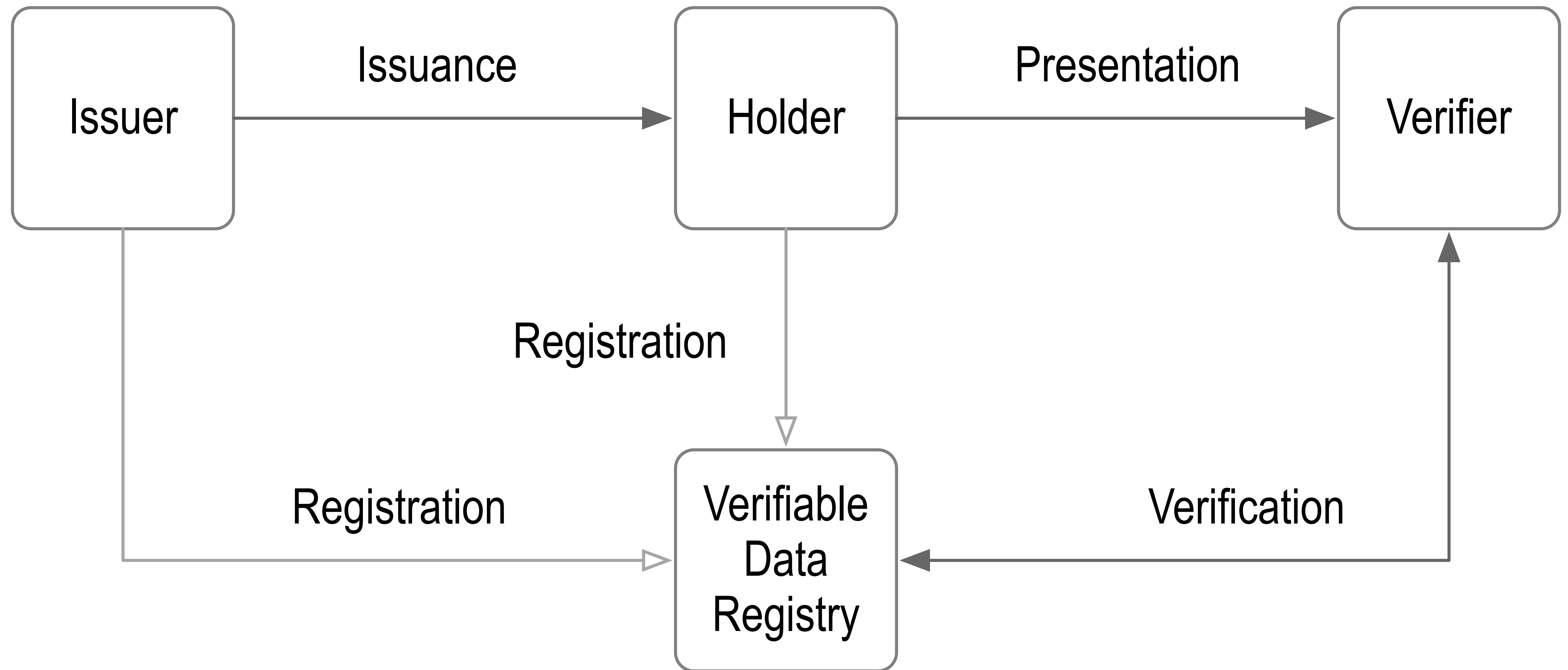
Cooperative vs. Uncooperative (Unilateral vs. Bilateral vs. Multilateral)

Entrained vs. Unentrained

## Issuer-Holder-Verifier Model

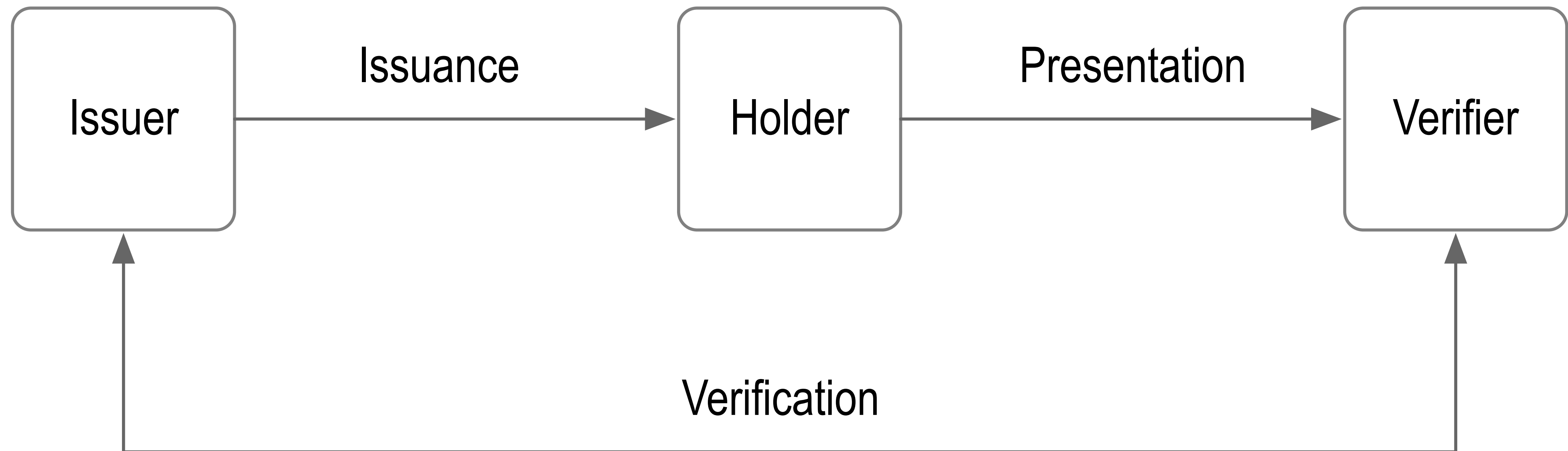


# Issuer-Holder-Verifier Model with Verification at Verifiable Data Registry

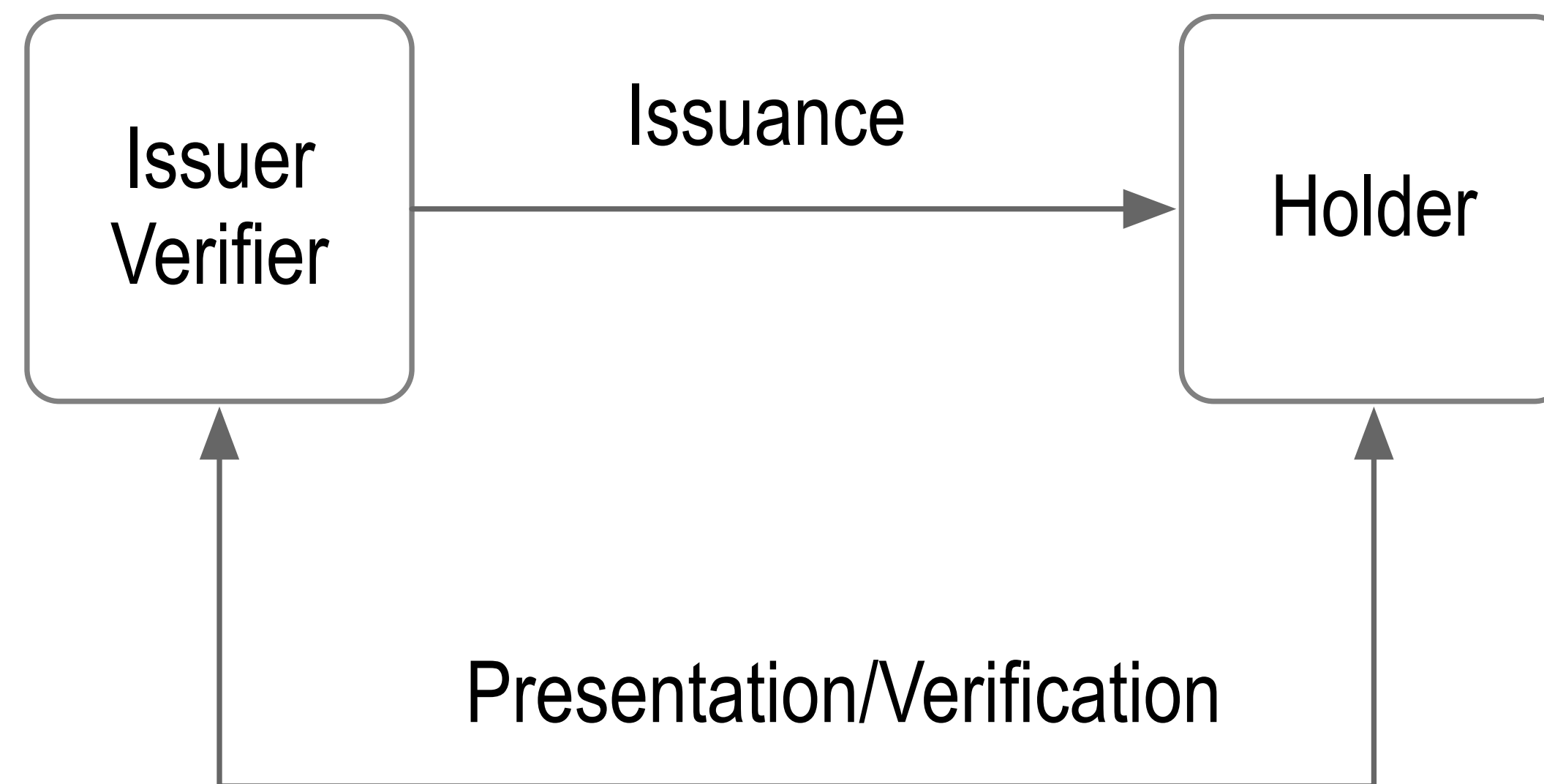




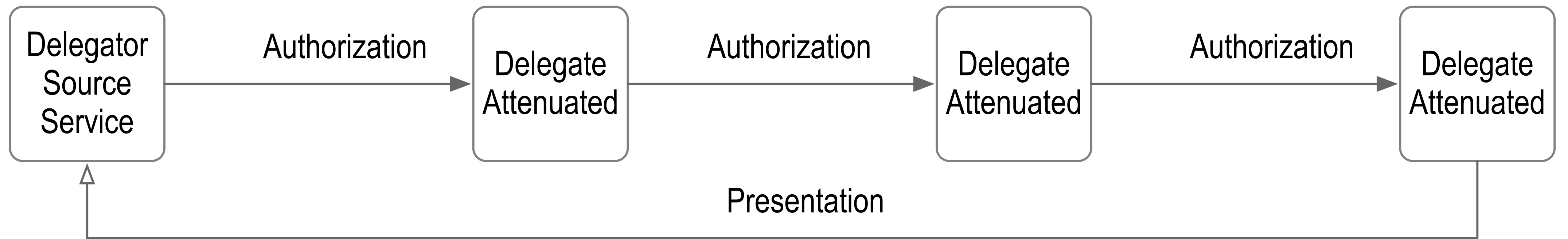
## Issuer-Holder-Verifier Model with Verification at Issuer



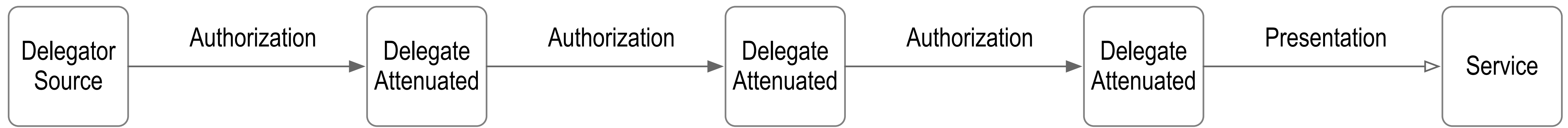
## Issuer-Holder Model with Verification at Issuer

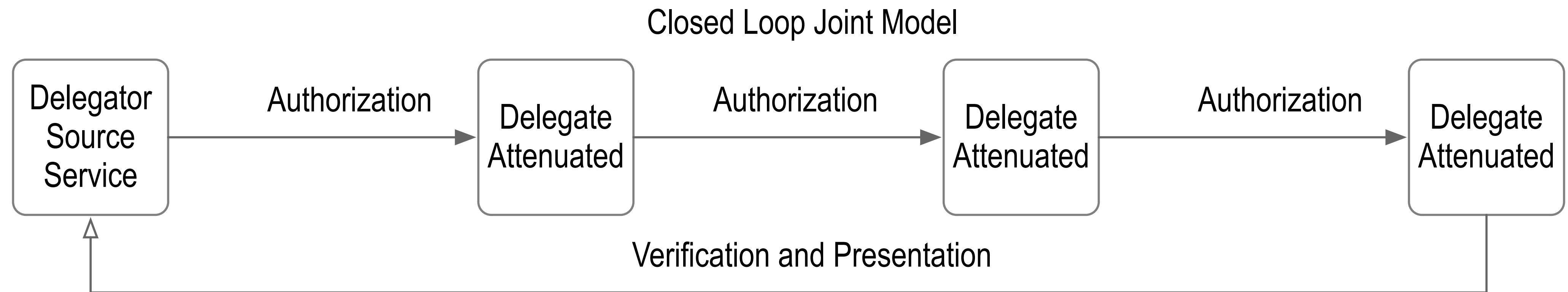


# Joint Delegator-Service Model

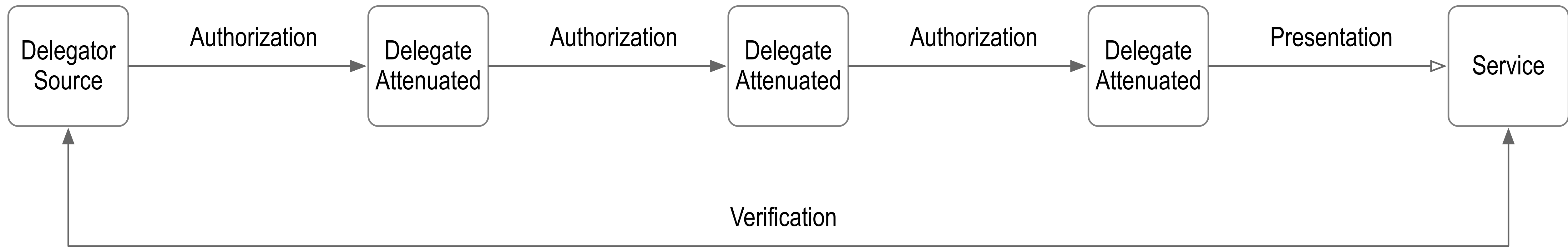


# Split Delegator-Service Model

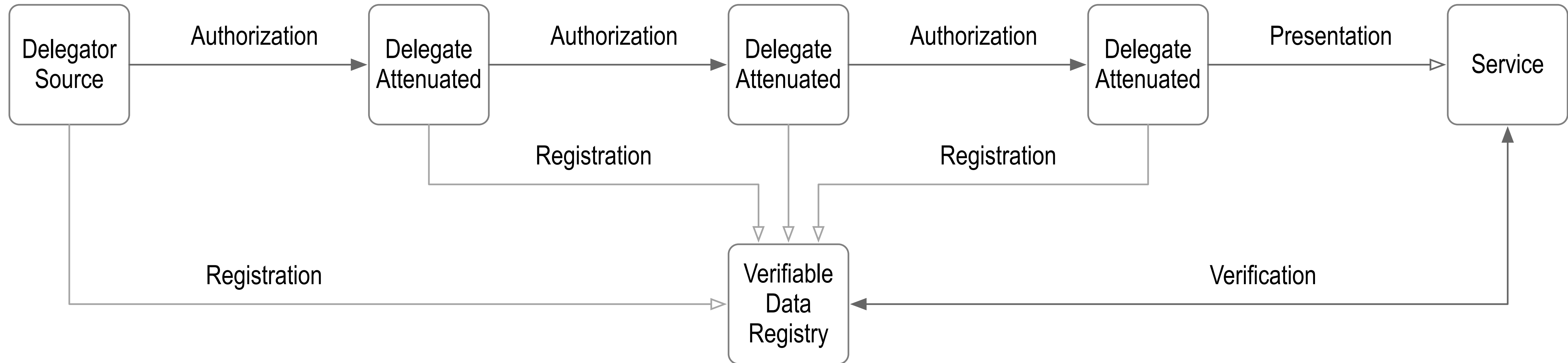




# Closed Loop Split Model



# Open Loop Split Model



# References

- Buchner, D., Zundel, B. and Riedel, M., “Presentation Exchange,” Decentralized Identity Foundation (DIF), <https://identity.foundation/presentation-exchange/>
- Conway, S., Hughes, A., Ma, M. et al., “A DID for Everything,” Rebooting the Web of Trust RWOT 7, 2018/09/26 [https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/A\\_DID\\_for\\_everything.pdf](https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/A_DID_for_everything.pdf)
- Ellison, C., Frantz, B., Lampson, B. et al., “RFC 2693 SPKI Certificate Theory,” IETF, 1999/09/01 <https://www.rfc-editor.org/rfc/rfc2693.txt>
- Evernym, “Simple Grant Language (SGL),” <https://github.com/evernym/sgl>
- Hardman, D., “Aries RFC 0103: Indirect Identity Control,” HyperLedger Aries, 2019-06-04 <https://github.com/hyperledger/aries-rfcs/blob/master/concepts/0103-indirect-identity-control/README.md>
- Hardman, D. and Harchandani, L., “Aries RFC 0104: Chained Credentials,” 2019-11-04 <https://github.com/hyperledger/aries-rfcs/blob/master/concepts/0104-chained-credentials/README.md>
- Hartzog, W., “Chain Link Confidentiality,” Georgia Law Review, vol. 46 :657, pp. 48, 2012/04/24 [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2045818](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2045818)
- “IDESG Consent to Create Binding,” IDESG IDENTIRAMA, [https://wiki.idesg.org/wiki/index.php/Consent\\_to\\_Create\\_Binding](https://wiki.idesg.org/wiki/index.php/Consent_to_Create_Binding)
- “ISO 27560 Consent record information structure (Draft),” ISO, <https://www.iso27001security.com/html/27560.html>
- Kathrein, A., Lizar, M. and Turner, D., “Consent Receipt Specification 1.1.0,” Kantara Initiative, 2019/12/30 <https://kantarainitiative.org/download/7902/>
- “Object-capbility model,” Wikipedia, [https://en.wikipedia.org/wiki/Object-capability\\_model](https://en.wikipedia.org/wiki/Object-capability_model)
- Ruff, T., “Verifiable Credentials Aren’t Credentials. They’re Containers.,” Medium, 2020-07-14 <https://rufftimo.medium.com/verifiable-credentials-arent-credentials-they-re-containers-fab5b3ae5c0>
- Ruff, T., “Like Shipping Containers, Verifiable Credentials Will Economically Transform the World,” Medium, 2020-07-14 <https://rufftimo.medium.com/like-shipping-containers-verifiable-credentials-will-economically-transform-the-world-fece2b9da14a>
- Ruff, T., “How Verifiable Credentials Bridge Trust Domains,” Medium, 2020-07-14 <https://rufftimo.medium.com/how-verifiable-credentials-bridge-trust-domains-97155dof3c17>
- Smith, S. M., “Universal Identifier Theory,” 2020-10-23 [https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/IdentifierTheory\\_web.pdf](https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/IdentifierTheory_web.pdf)
- Smith, S. M., “Decentralized Autonomic Data (DAD) and the three R’s of Key Management,” Rebooting the Web of Trust RWOT 6, Spring 2018 <https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/DecentralizedAutonomicData.pdf>
- “w3c-ccg Traceability Vocabulary Specification,” w3c-ccg, <https://github.com/w3c-ccg/traceability-vocab>
- Webber, C. L., Sporny, M. and Miller, M. S., “Authorization Capabilities for Linked Data v0.3 (ZCAP-LD):An object capability framework for linked data systems,” W3C, 2020/October/22 <https://w3c-ccg.github.io/zcap-ld/>



# Object Capabilities vs VC Authorizations

ObjCap:

Most useful for computer OS security, does not translate easily to many real world use cases

Not VC Native

explicit, ephemeral, attenuable, chained, unaggregative, unweighted, uncooperative, closed-loop

VC:

No standard model for authorization, chaining, delegation etc.

Implicit, persistent or not, unattenuable, unchained, unaggregative, unweighted, uncooperative, open-loop

# Verifiable Chains

Verifiable Credential *Native*:

*Chaining Semantics*:

Provenance

Credence (Trust)

Confidence

Data Custody

Authorization

Consent

Custodian Governance

TADA<sup>3</sup>!

*Samuel M. Smith Ph.D.*

*sam@samuelsmith.org*

# Verifiable C...

Verifiable (integrity & attribution) Container of ?

Verifiable Chain (Tree) of Containers of ?

Authenticity verification and Veracity verification

...

Data Source Provenance

Data Source Credence (Reputation, Trust)

Data Source Weighting Confidence

Data Source Aggregation

...

Authority Source Authorization

Authority Source Consent

Authority Source Custodian

Authority Source Aggregation

*Samuel M. Smith Ph.D.*

*sam@samuelsmith.org*

# Verifiable ... *Credential*?

*credential*:

evidence of authority, status, rights, entitlement to privileges, or the like.

*authorization*:

permission or power granted by an *authority*; sanction.

*claim*:

an assertion of something as a fact, an assertion of a right or an alleged right.

*container*:

anything that *contains* or can *contain* something, ... factual data container.

# What is verifiable?

## Verifiable Signature:

- Provides proof of data integrity and non-repudiable commitment to data syntax.

- Verifiable attribution

- Does not by itself provide verifiable veracity/truthfulness of facts/data semantics.

A signature imbues no veracity of any kind to the data semantics.

Verifies authenticity of signed statement = attribution to author/signer, not veracity of signed statement.

IF the operative semantics of the data are under the control of the signer, then a signature conveys a verifiable non-repudiable commitment to those operative semantics.

= *authorization*.

# Authorization Properties

Implicit vs. Explicit

Persistent vs. Ephemeral (revocation policy)

Chained vs. Unchained

Attenuable vs. Unattenuable

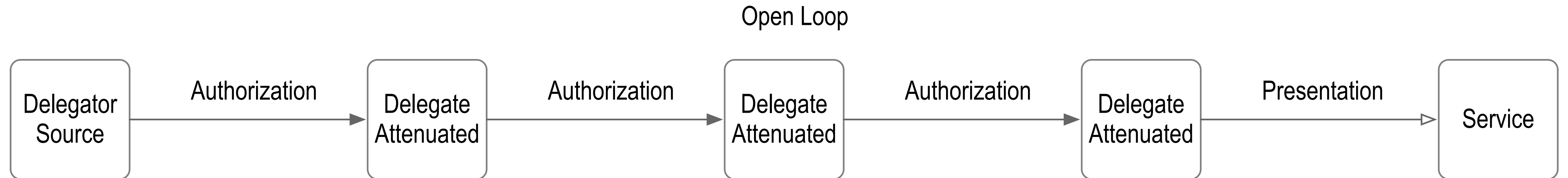
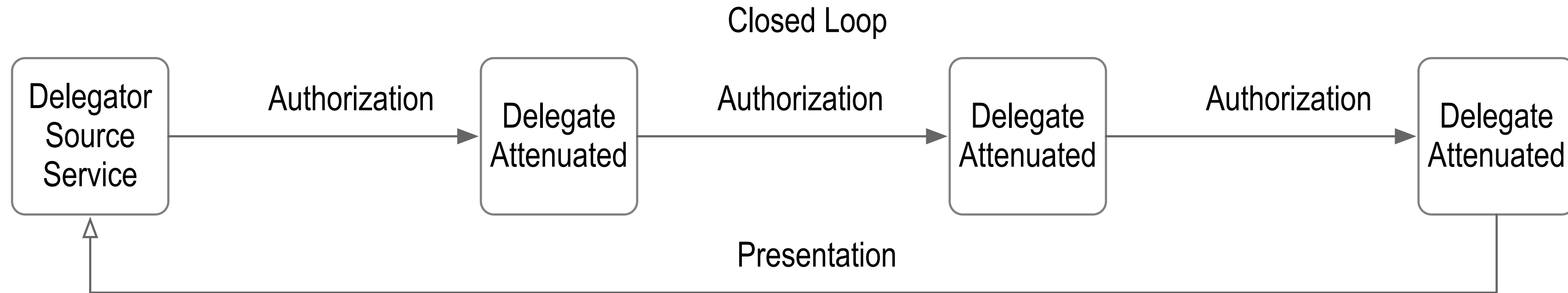
Aggregative vs. Unaggregative (Tree vs linear Chain)

Weighted vs. Unweighted

Closed Loop vs. Open Loop

Cooperative vs. Uncooperative

# Closed vs Open Loop



# Weighted Aggregation of Authorizations

Analogous to thresholded multi-signature

$$\hat{C}_l = [C_l^1, \dots, C_l^{L_l}]_l \quad \hat{K}_l = [U_l^1, \dots, U_l^{L_l}]_l \quad 0 < U_l^j \leq 1 \quad \bar{U}_l = \sum_{i=s_0}^{s_{S_k-1}} U_l^i \geq 1 \quad \hat{s}_k^l = [s_0, \dots, s_{S_k^l-1}]_k^l$$

$$\hat{C} = [C^1, C^2, C^3] \quad U_l^j = 1/K_l \quad \hat{K} = [1/2, 1/2, 1/2]$$

$$\hat{K}_l = [1/2, 1/2, 1/4, 1/4, 1/4, 1/4]_l$$

$$\hat{K}_l = \left[ [1/2, 1/2, 1/4, 1/4, 1/4, 1/4], [1/2, 1/2, 1/2, 1/2], [1, 1, 1, 1] \right]$$



# Cooperative Delegation Relationship

Authority flows source to sink (down or left to right)

Credence (trust) flows sink to source (up or right to left)

Provenance requires tracing relationships both ways

Cooperative delegation flows both ways.

Delegator sends authority to Delegate.

Delegate sends credence to Delegator.

# Cooperative Verification Relationship

Delegator has rules (constraints)

Delegate has rules (objectives)

Verifier has rules (constraints and objectives)

Authorization success upon the conjoint satisfaction of the three sets of rules

Authorization success upon the satisfaction of rule chain

# Decision Making Model

is-a has-a knowledge graph: decision making based on querying knowledge graph, indirect decision making process

decision making graph: decision making based on evaluating decision making graph, direct decision making process

JSON = Data

Just JSON = Just Data

Subject is-a, has-a data

Metadata about is-a has-a data

Limiting case, data item is the subject of its own data = Just Data

# Attribution Chain

Super semantic is an attribution chaining semantic.

Need first make secure attribution of source of information = issuers of ADC

Attribution tree (aggregation)

Then once we have made secure attribution to issuers (AID KERI etc)

Then we can color the edges of the attribution tree with layered semantic

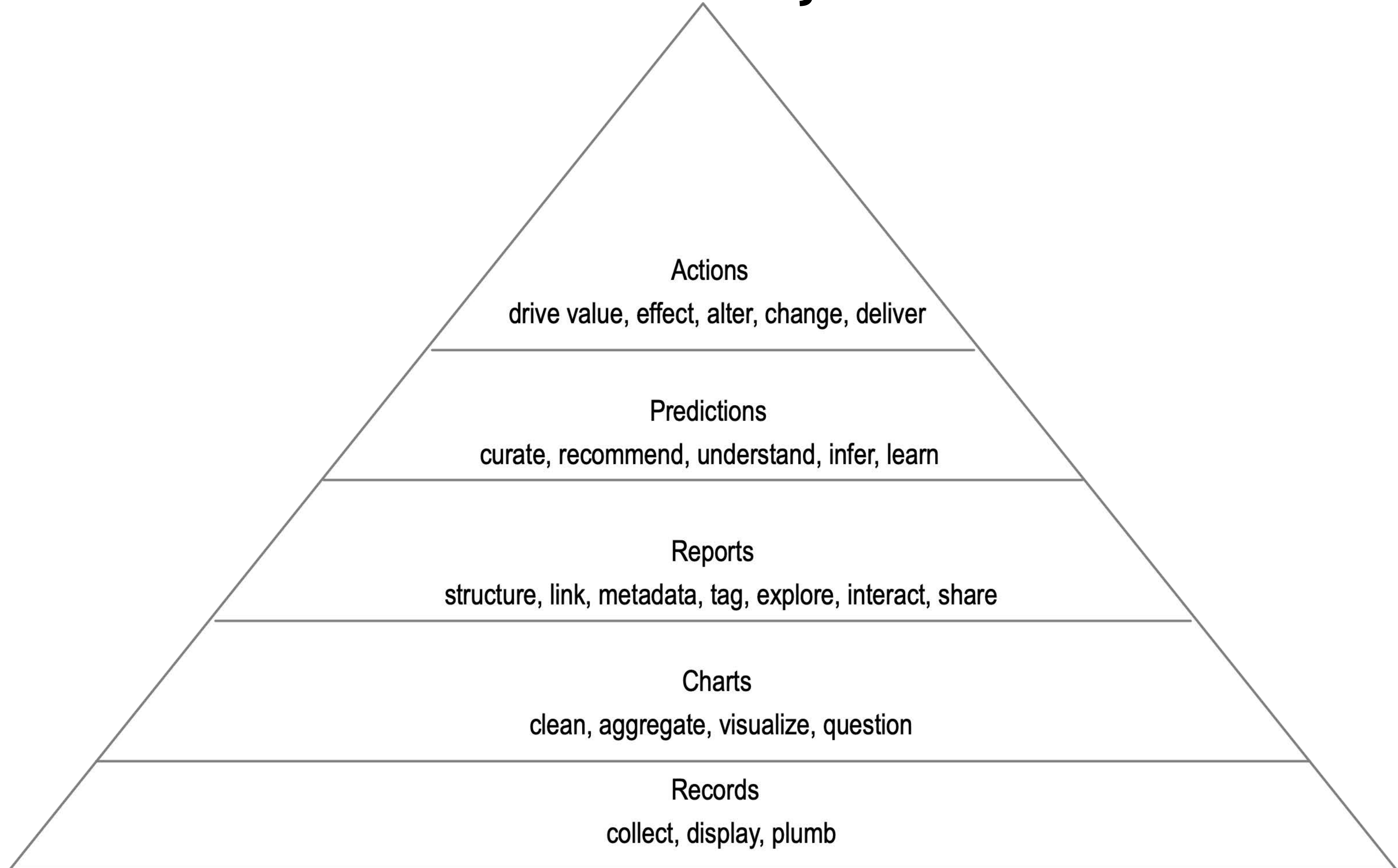
Provenance Tree/Chain

Delegation Tree/Chain

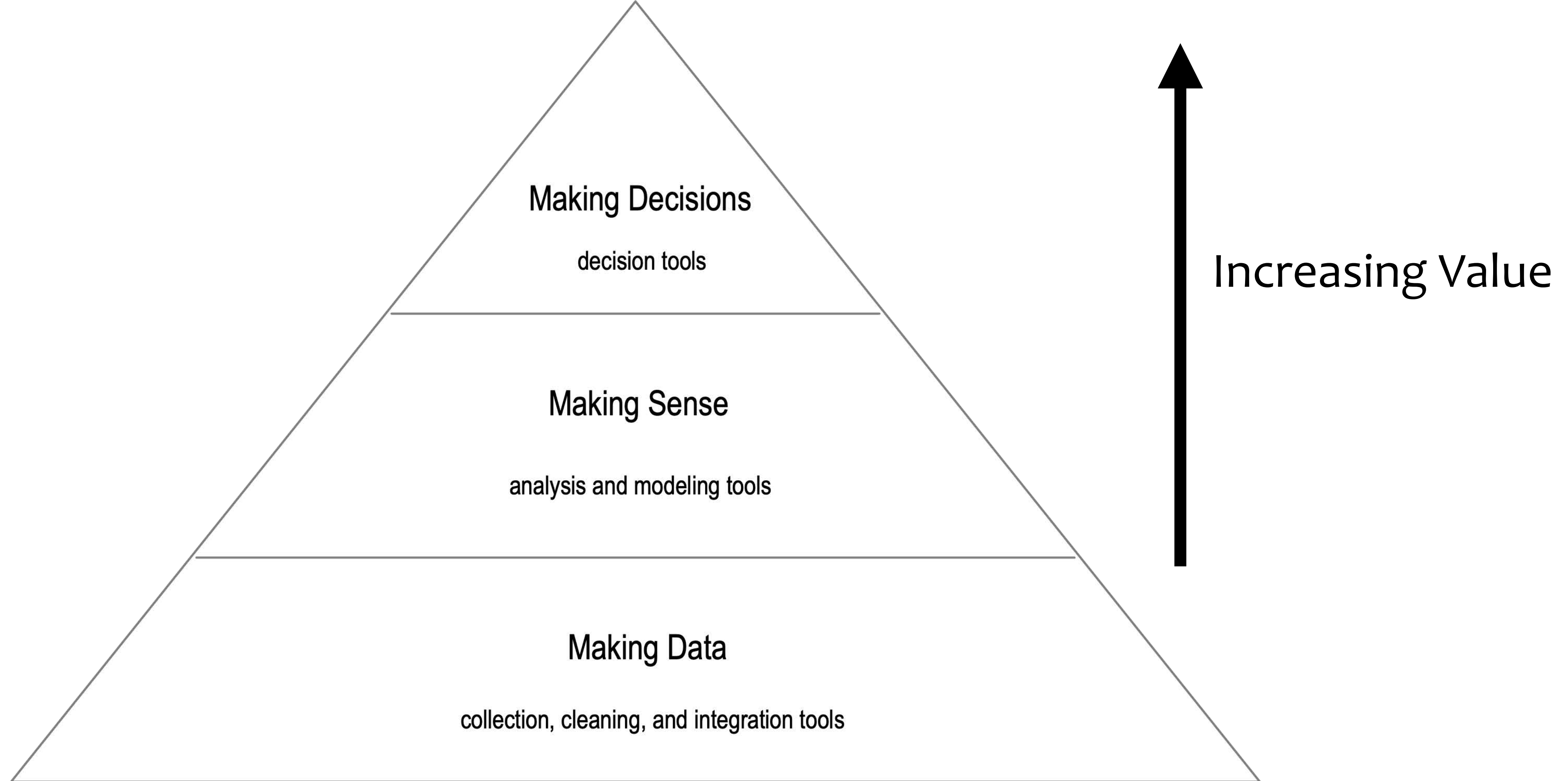
Attestation Tree/Chain

Etc.

# Data Value Pyramid



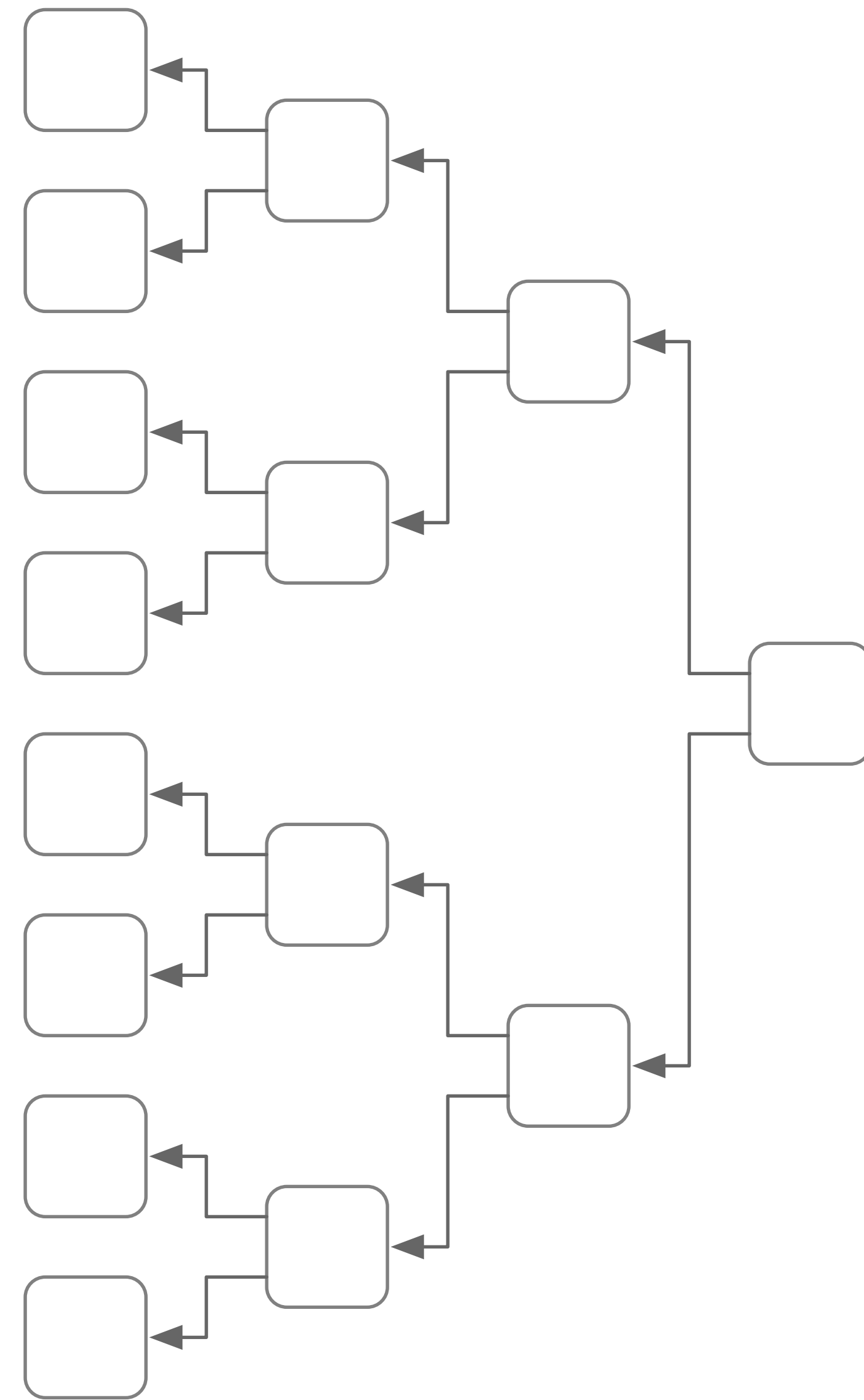
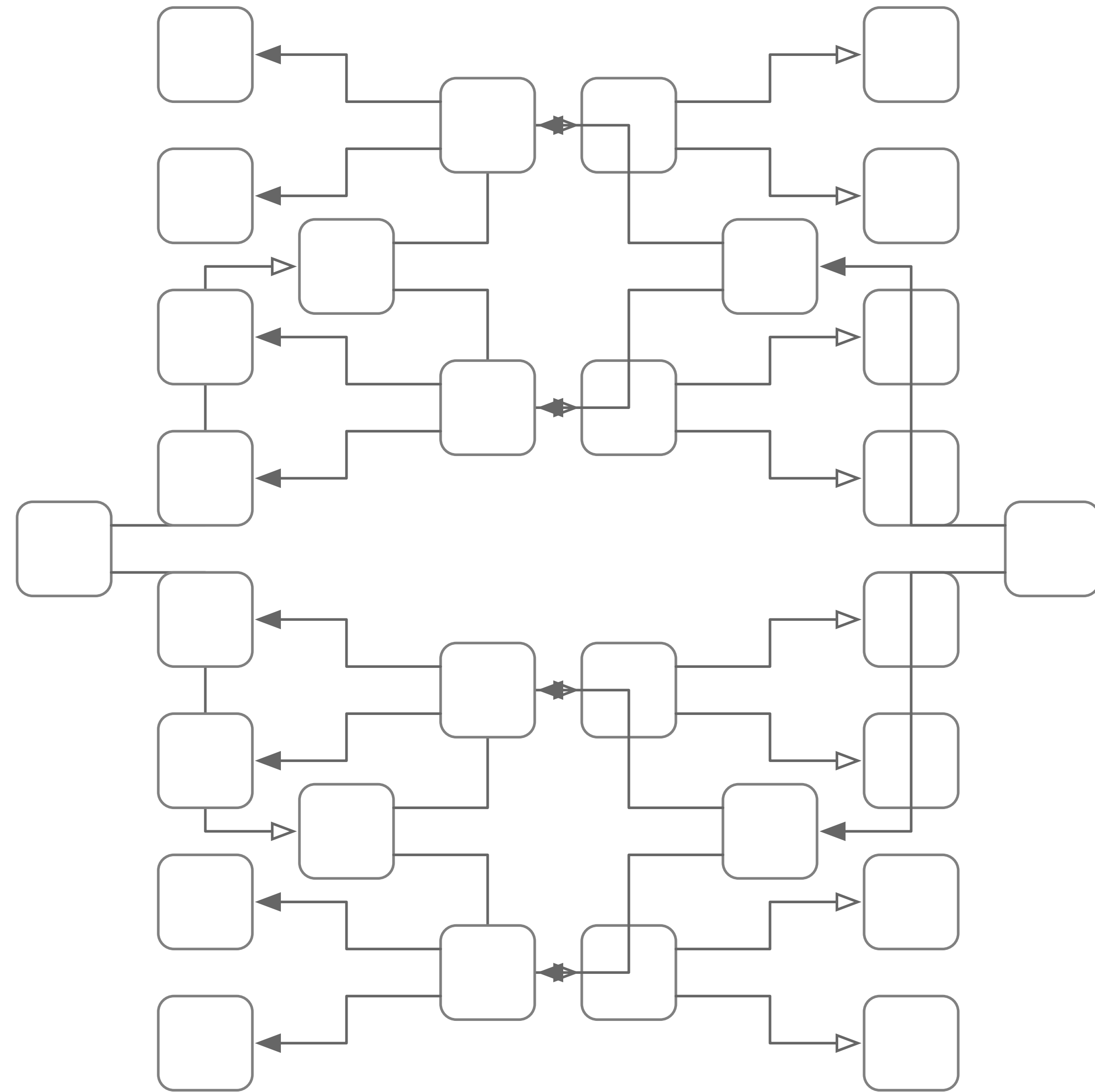
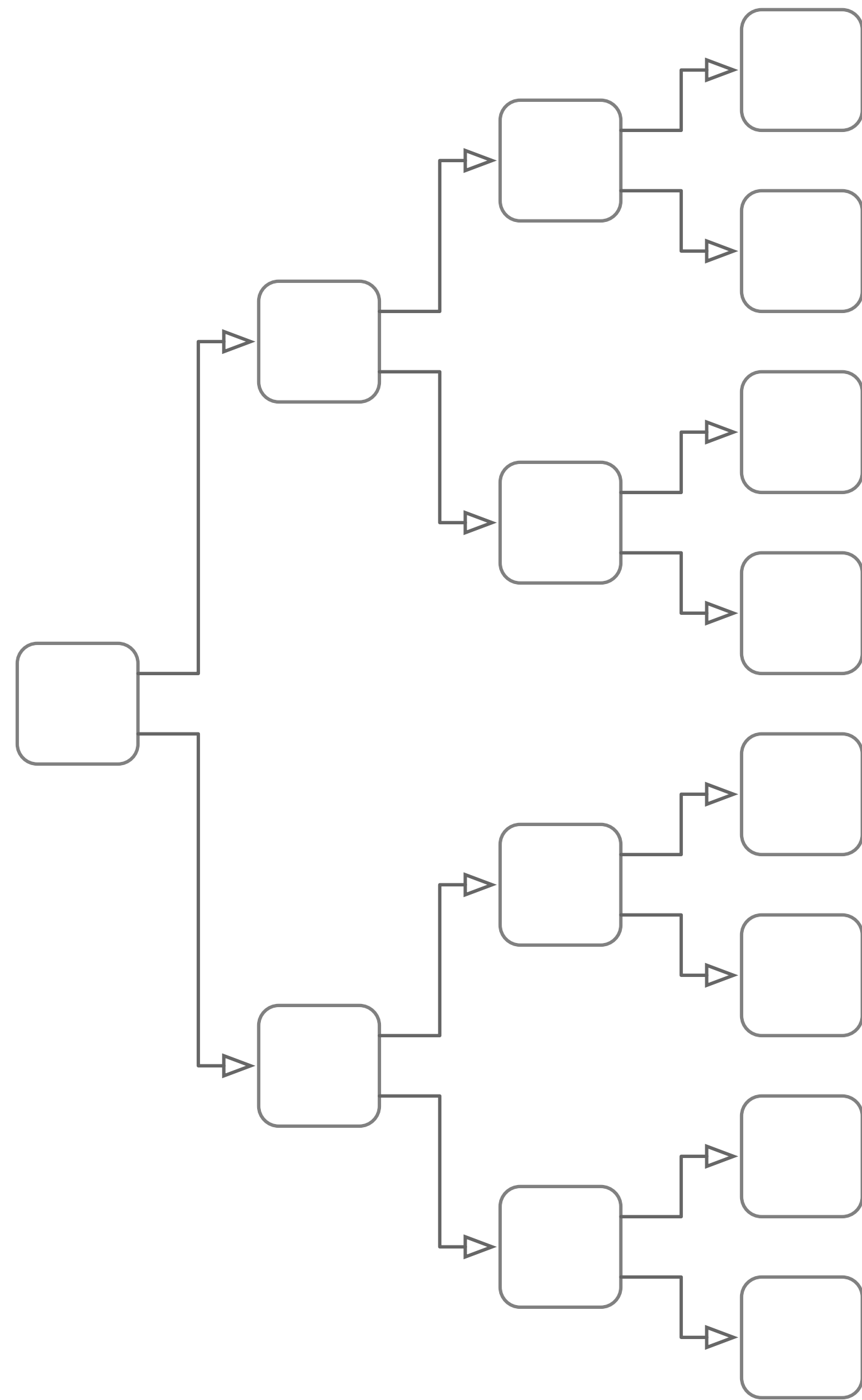
# Activity Value Pyramid



Automated Reasoning = High Leverage Decision Making

# Data Supply Chains

# Cooperative Delegation





# Provenance Semantics: Chaining and Rules

Provenance Chains (Credence or Authorization)

```
{
  priors:
  {
    {source: id, rules: { ...}, weight: value, ...},
    {source: id, rules: { ...}, weight: value, ...},
    ...
  },
  destination: id,
  rules: { ... },
  weight: value,
  sink: id,
  ...
}
```

# TADA<sup>3</sup> Mnemonic

T ail

A uthenticated

D elegatable

A ttenuable

A ggregatable

A uthorization