sezoo

Towards a model for Governance in Trust over IP and **ALL** digital trust systems

A slowly slowly approach...

This deck will attempt a “first principles” approach to Governance, considering the questions and answers we need in order to understand how Governance might be understood in a Trust over IP context.

Each step is intended to build on the previous and only add one new concept at a time.

sezoo

…aim to be humble…

My hypothesis is that any instance of “governance” shares some qualities with all other instances and that there are an infinite number of specific instances possible.

I do not believe that it is our role to define what is “right” in governance, beyond some very simple primitives. Rather than be **prescriptive** I suggest we aim to be **descriptive**, to enable “what is” to be described in a way that allows trustworthiness to be assessed by the viewer.

I think there is a very significant risk that alternative approaches either try to create a governance “Borges Map” [https://en.wikipedia.org/wiki/On_Exactitude_in_Science] or they try to impose a narrow view of governance made with imperfect knowledge.

sezoo

… but with very grand ambition

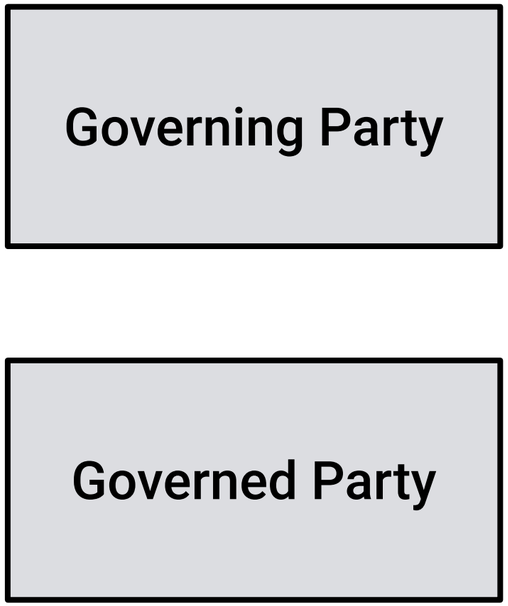
So for me, there is **no single solution** and “solving” for all is not possible. Use cases have value only in testing not defining. We need to identify the building materials that might be used in an trustworthy ecosystem, not the buildings and street layout themselves.

So rather than try and define or dictate **specifically** what governance **is** in ToIP, I want to try and identify what general “type of” qualities it ALWAYS has, no matter the specific context.

Here goes…

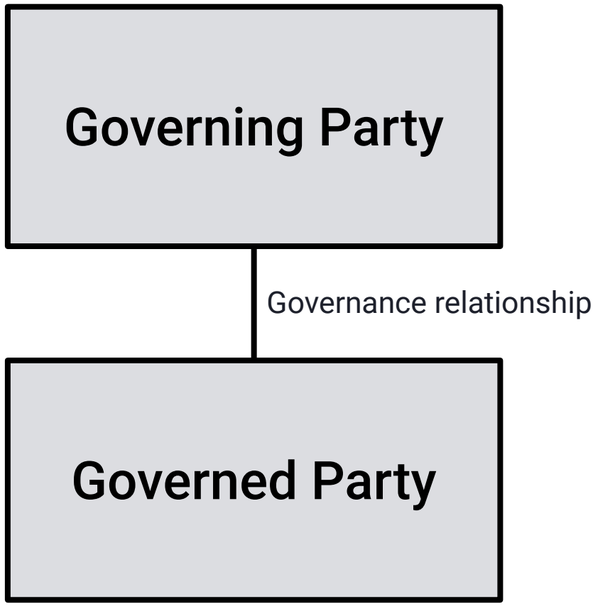
sezoo

At its simplest, we might consider governance as involving two parties: the **governed** and the **governing**



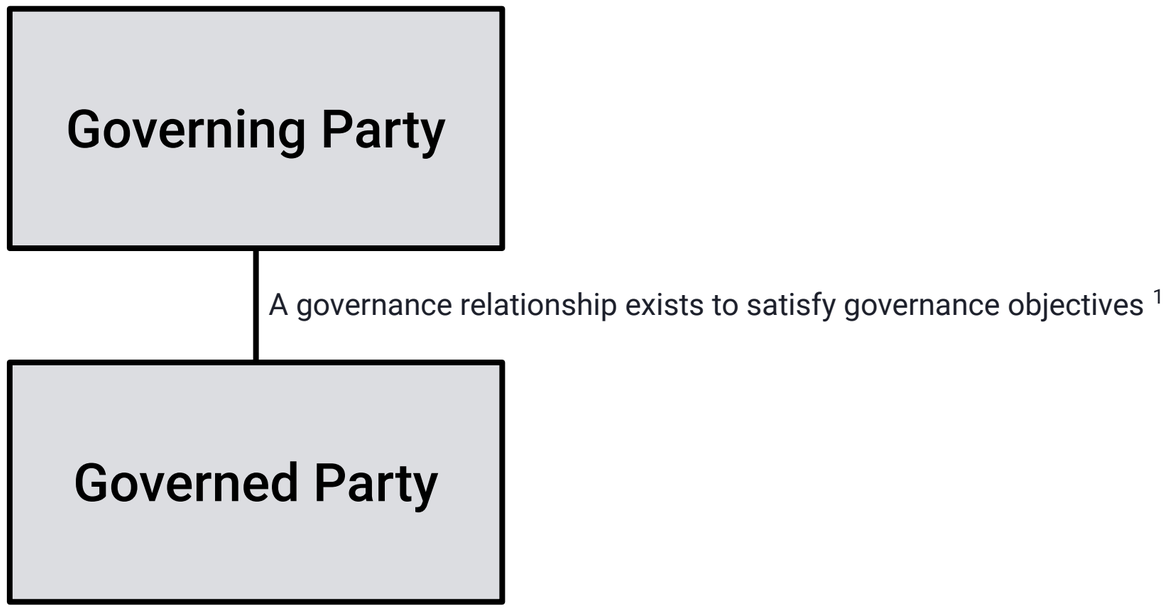
sezoo

We can think of an instance of *governance* as a relationship between these two parties



sezoo

We can assume that a governance relationship exists for a purpose - it exists to achieve one or more [governance] **objectives**

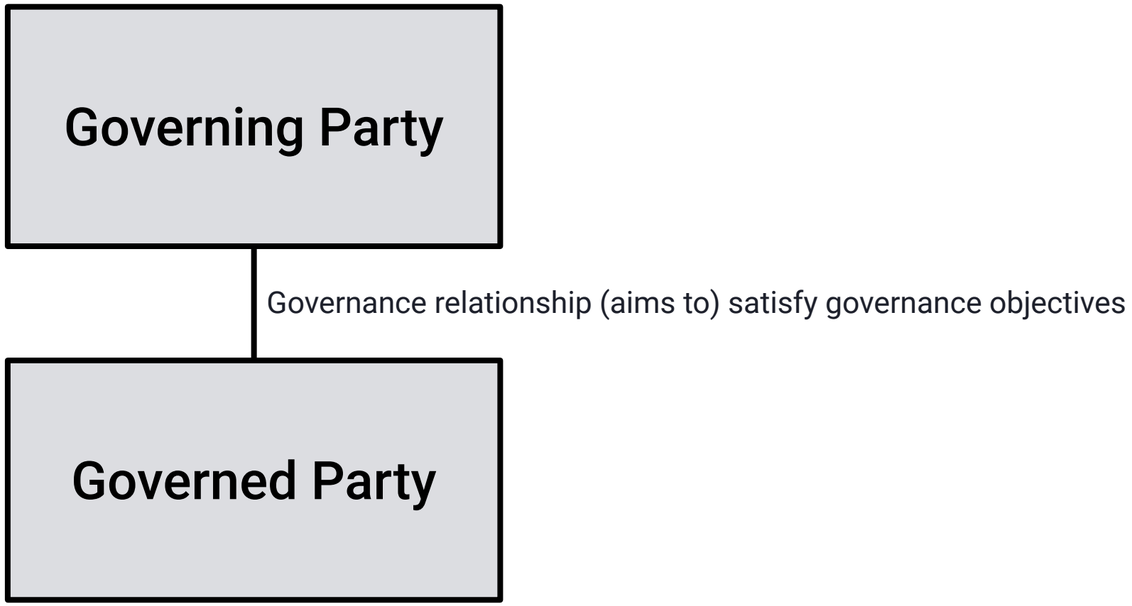


[1] The objectives could be anything, from proving that you meet certain requirements for licences, ESG obligations, carbon neutral, financial licences, safety regulations or whatever. They might be focused on risk, compliance, or other governance concerns.

We/I don't want to worry about "what" the objectives are, the point is there MUST be some otherwise why bother with the relationship?

sezoo

Each party might have **implicit** objectives as well as **explicit** objectives.
For now, we are only concerned with the explicit, documented, objectives

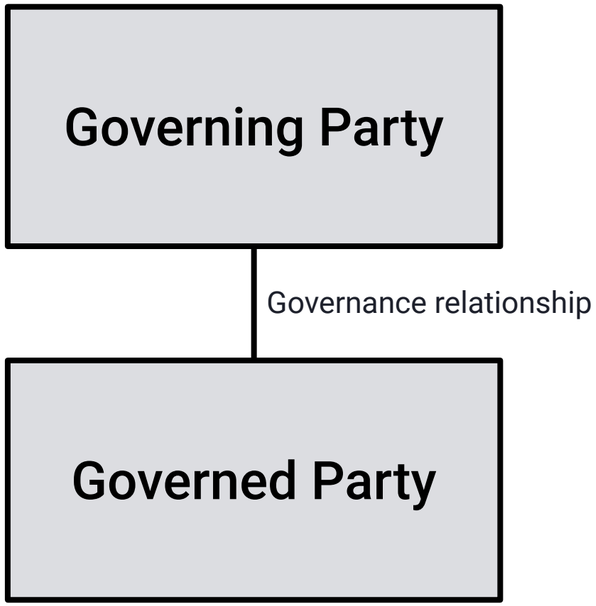


For examples, think of things like “Know Your Customer” (KYC) regulations [1] in the financial sector, age restrictions for access to adult goods and services, data protection, protection of civil liberties, compliance with licence requirements etc. Each of these are objectives that the governance relationship might seek to assure. “Implicit” objectives might be that organisations seek to “look good” through a social lens or provide evidence to others of their good intentions.

[1] See https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html for example

sezoo

Governance may be **optional** or **mandatory** for the governed party

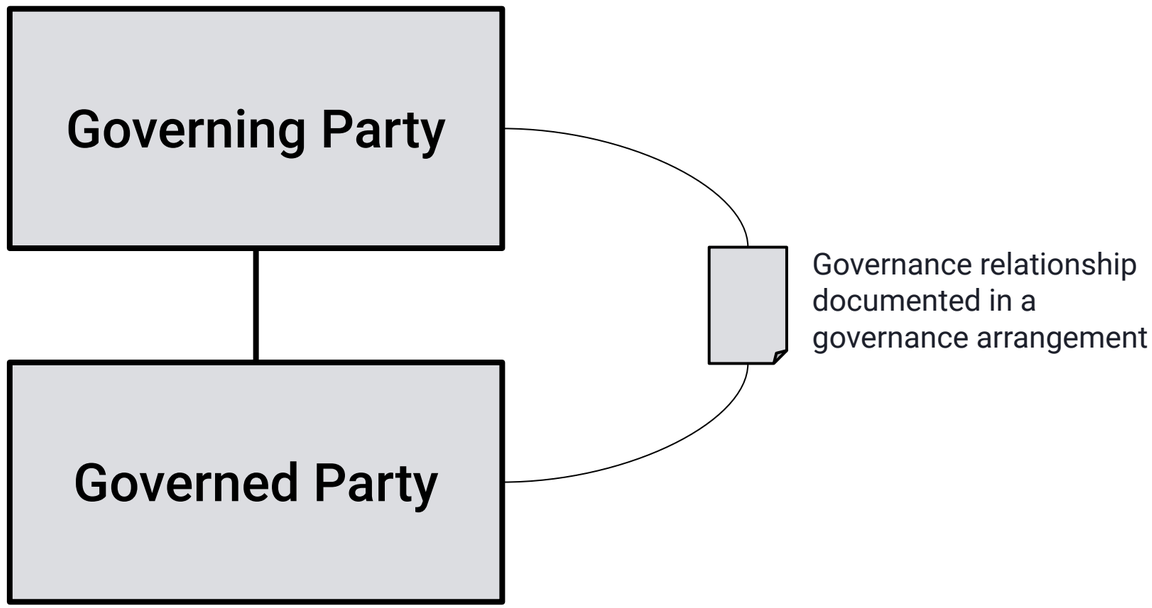


Optional: the Governed Party chooses (“opts-in”) to be governed under a framework. Things like ISO quality systems, Corporation B recognition, ESG, Zero Carbon etc. can be like this.

Mandatory: governance is a condition for legal operation of the party. Liquor Sellers, Education, Health, Finance organisations for example being required to meet the regulatory requirements of their licence in order to be allowed to operate.

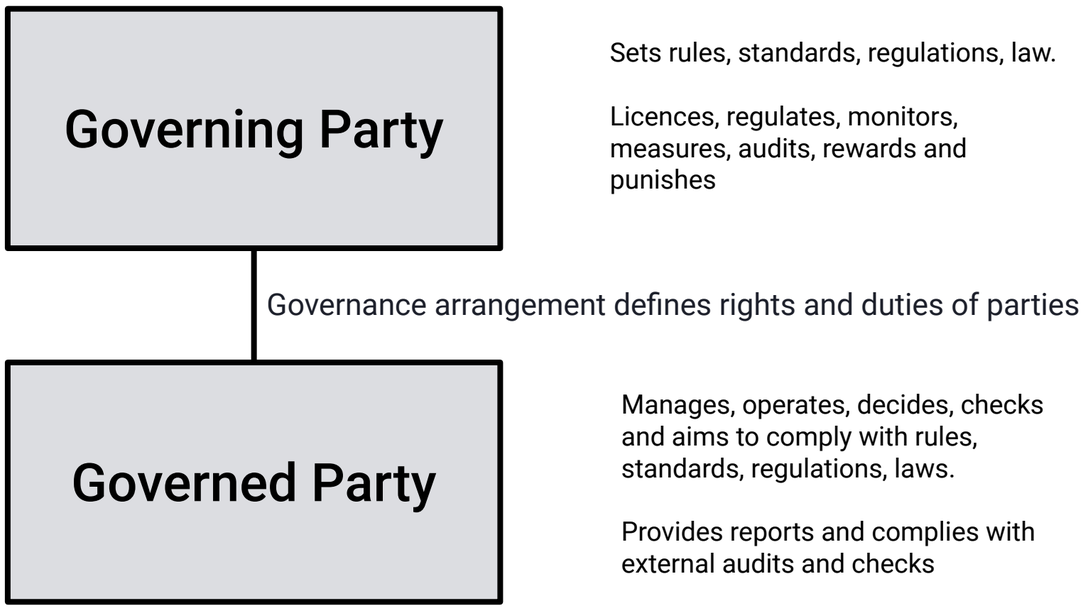
sezoo

An explicit governance relationship is defined by a **governance arrangement** between the two parties



sezoo

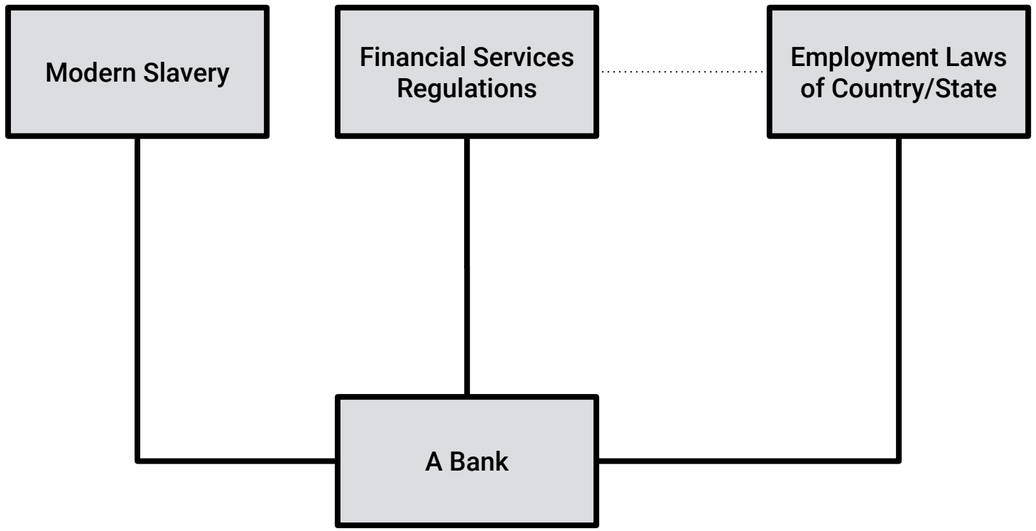
Each party commits to their **rights and duties** as defined in the governance arrangement to allow them to achieve the governance **objective(s)**



sezoo

A Governed Party may be governed by more than one governing arrangement

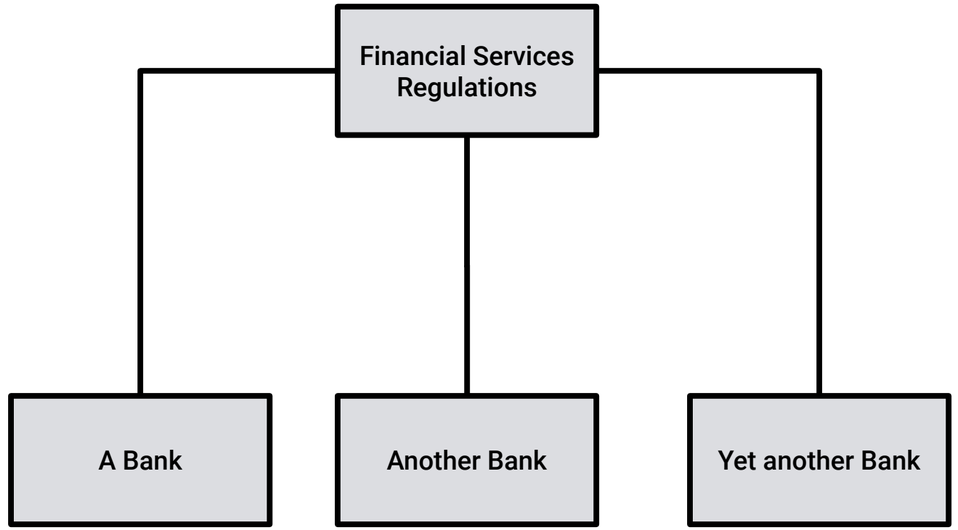
For example, a financial organisation is required to meet employment laws, sector regulations, and international regulations (amongst others). Each arrangement instance has specific governance objectives and a specific governing party. **Each is independent of the other.**



sezoo

A governing party may have many governance arrangements with many governed parties

For example, a financial services regulator may govern many financial services organisations.



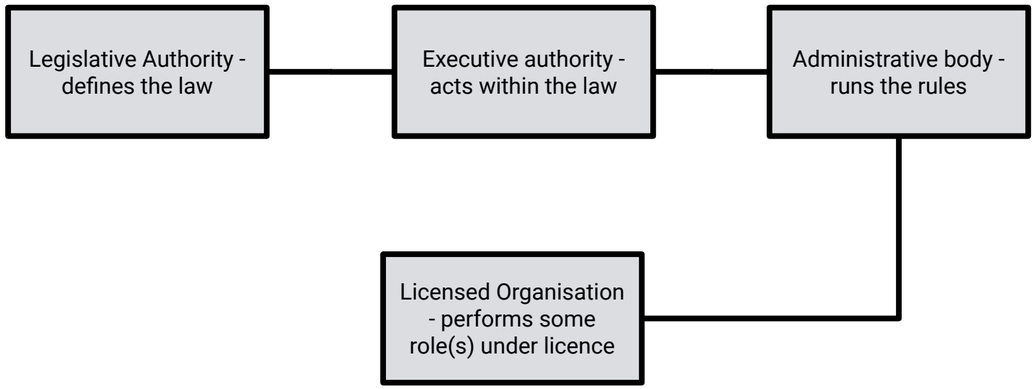
sezoo

But who governs the governing party?

If we follow this logic as far as we can, we typically end up with some idea of a “sovereign entity” that defines some rules or regulations. This might be a state or country or the peak body of a sporting code (for example).

Hence governance arrangements can be be many layered structures AND any one party might be part of many such structures.

THERE IS NO ONE SINGLE “HIERARCHY” of governance.

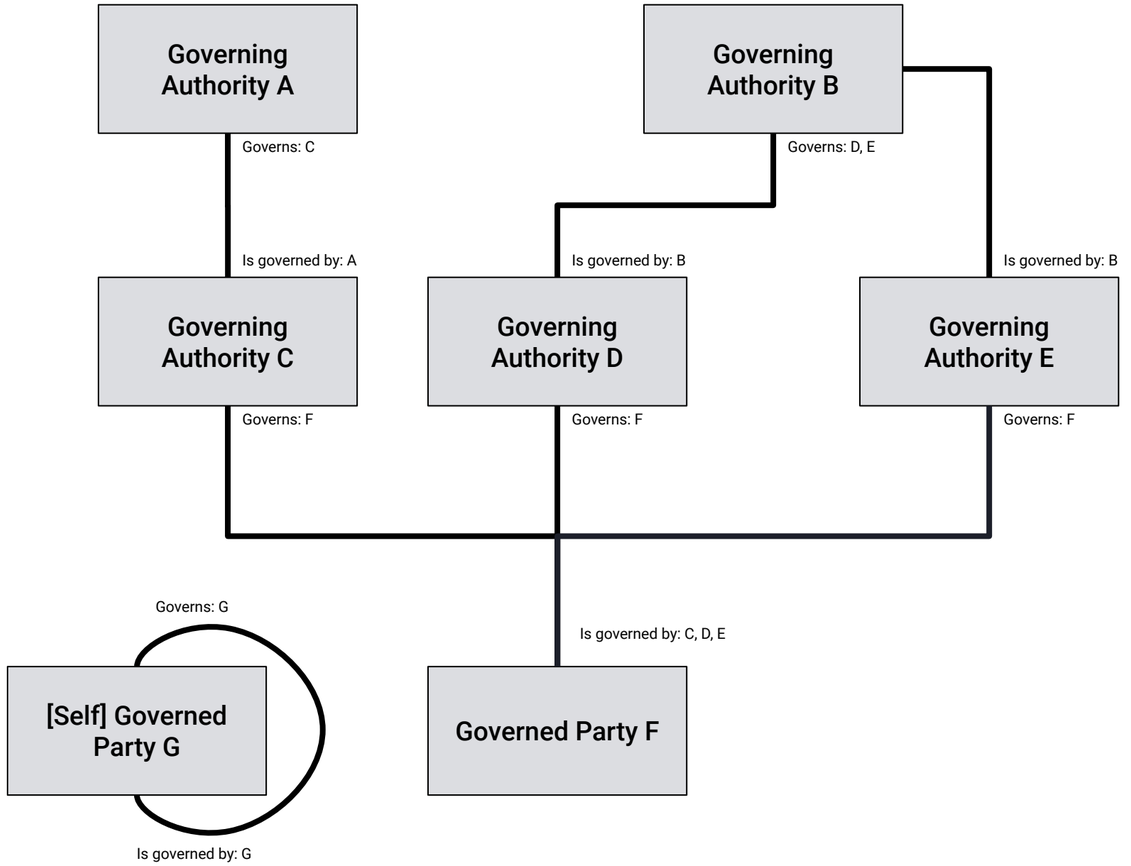


We can think of the executive and legislative branches of government as examples, and the licences they can provide to other bodies to provide authorised services (for example, “Registered Training Organisations” in Australia, licenced test labs for legalised gaming jurisdictions, and peak sporting bodies for national and international sports)

sezoo

Hence… Governing relationships form a governance network or **graph**

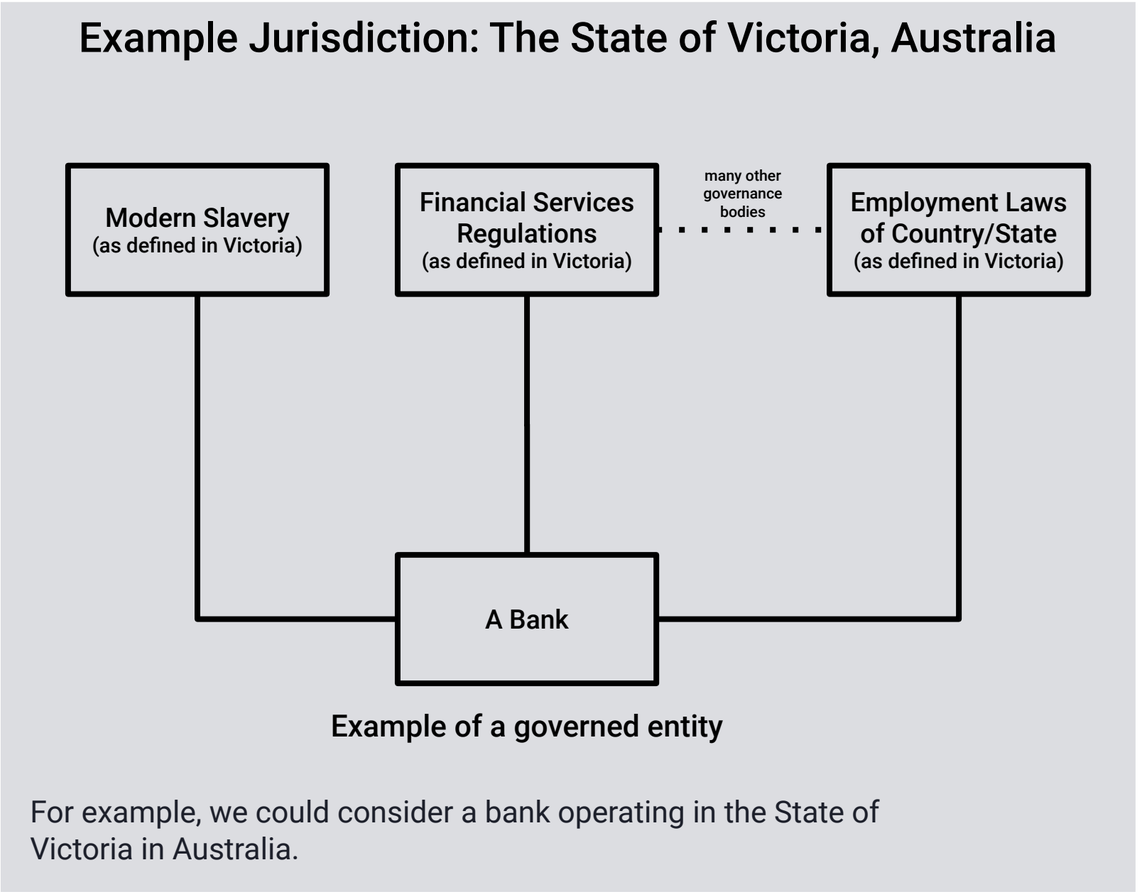
Observation: every Governed Party is a node on a governance graph. The simplest possible graph has only one node (they explicitly or implicitly declare themselves as “self-governed”)



sezoo

Observation / Assertion:

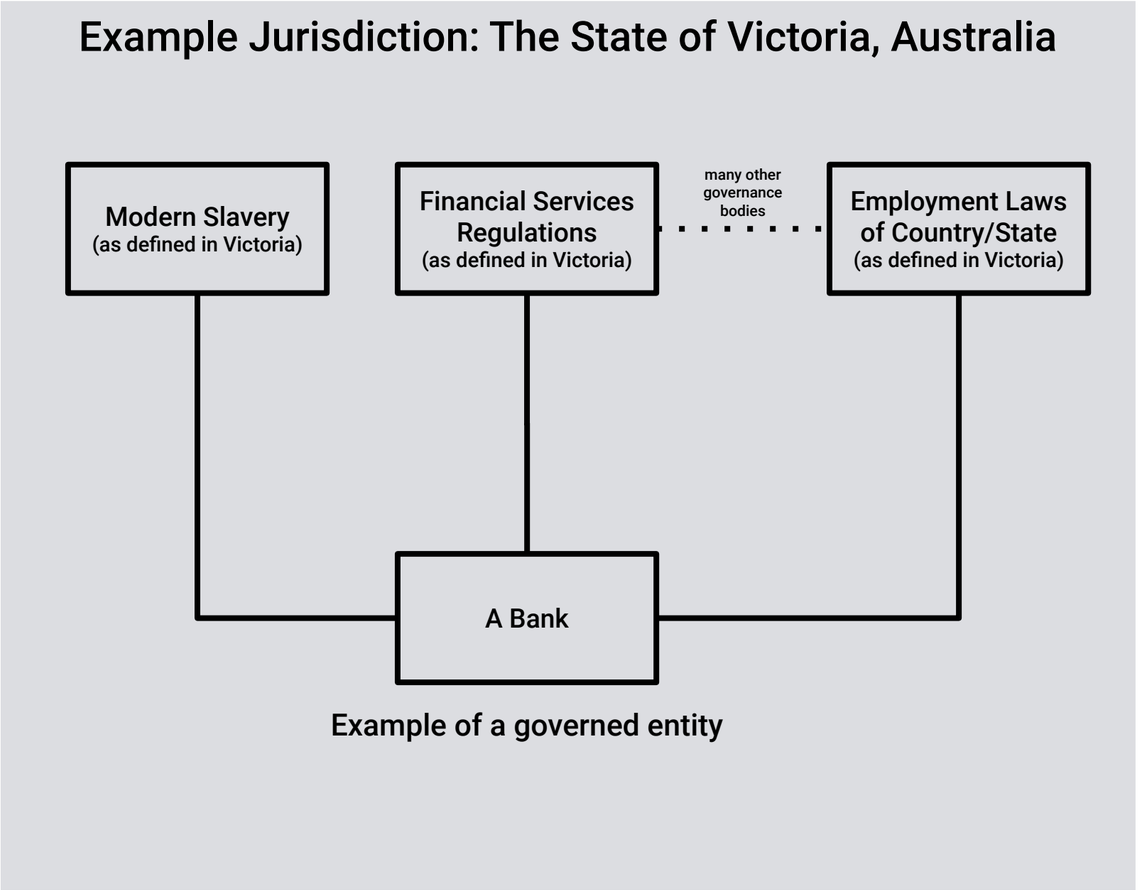
Governance Arrangements take place in a **Jurisdiction**



For example, we could consider a bank operating in the State of Victoria in Australia.

sezoo

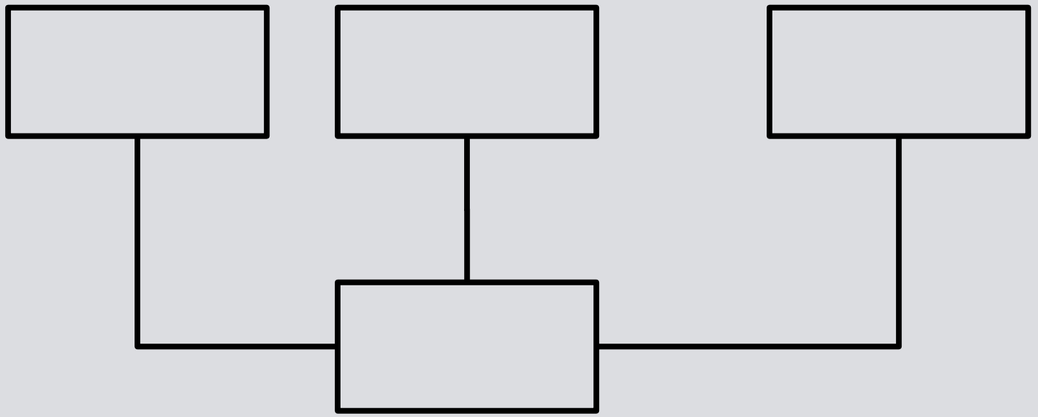
The **Jurisdiction** defines the overarching legal framework in which the governance arrangement, and each party, operates.



sezoo

In addition to any specific governance arrangements, Organisations registered and/or operating within a **Jurisdiction** must meet the laws and regulations that apply within the jurisdiction

Example Jurisdiction: The State of Victoria, Australia



For example, all businesses operating in Victoria must meet a number of regulatory requirements, such as:

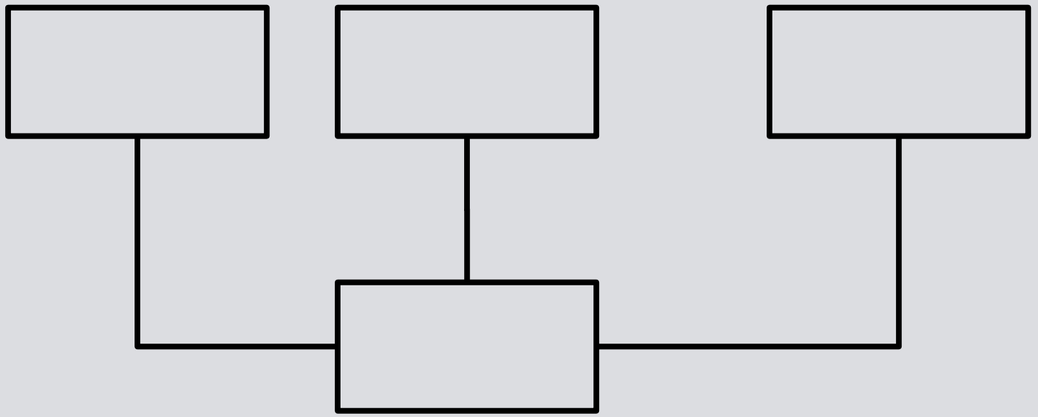
- Fair Trading Laws
- Fair Contracts
- Receipts and Itemised Bills
- Refunds and Exchanges
- Privacy and Data Protection Act

sezoo

Jurisdictional governance gives us another branch to our governance graph.

Each Party should declare the Jurisdiction in which they operate and identify where the Jurisdiction legislation relevant to their operation can be found.

Example Jurisdiction: The State of Victoria, Australia



For example, all businesses operating in Victoria must meet a number of regulatory requirements, such as:

- Fair Trading Laws
- Fair Contracts
- Receipts and Itemised Bills
- Refunds and Exchanges
- Privacy and Data Protection Act

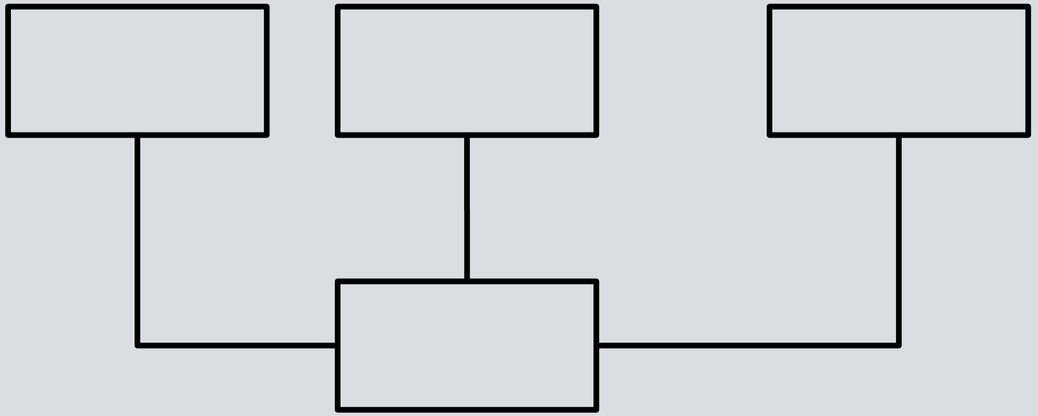
sezoo

Jurisdiction governance is different.

Explicit, ‘active’, governance arrangements are defined by each party, but the overarching governance provided by the Jurisdiction may provide other protections and provisions that aren’t made explicit in the governance arrangements.

We can say that we “inherit” additional qualities of governance from a Jurisdiction.

Example Jurisdiction: The State of Victoria, Australia



For example, all businesses operating in Victoria must meet a number of regulatory requirements, such as:

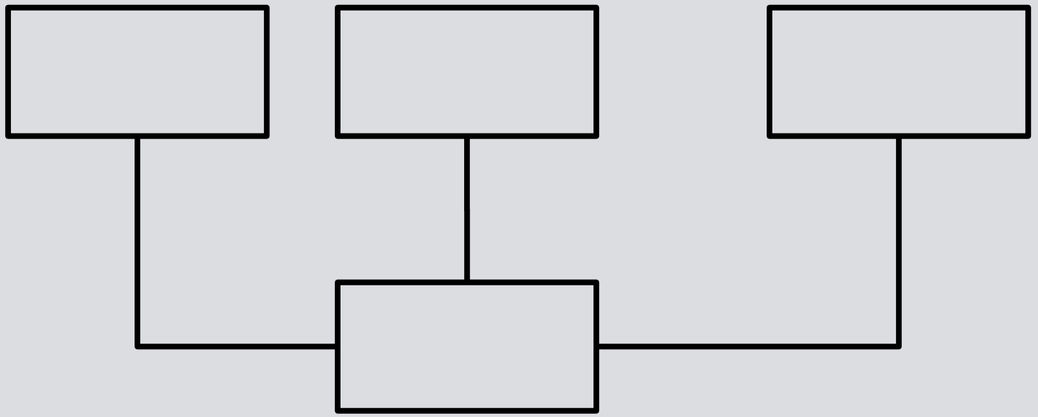
- Fair Trading Laws
- Fair Contracts
- Receipts and Itemised Bills
- Refunds and Exchanges
- Privacy and Data Protection Act

sezoo

Sanity check: I **don't** propose that we try to "encode" Jurisdictional governance.

I think we just need to accept (for the moment at least) that exploring this part of the graph takes human (legal) expertise.

Example Jurisdiction: The State of Victoria, Australia



For example, all businesses operating in Victoria must meet a number of regulatory requirements, such as:

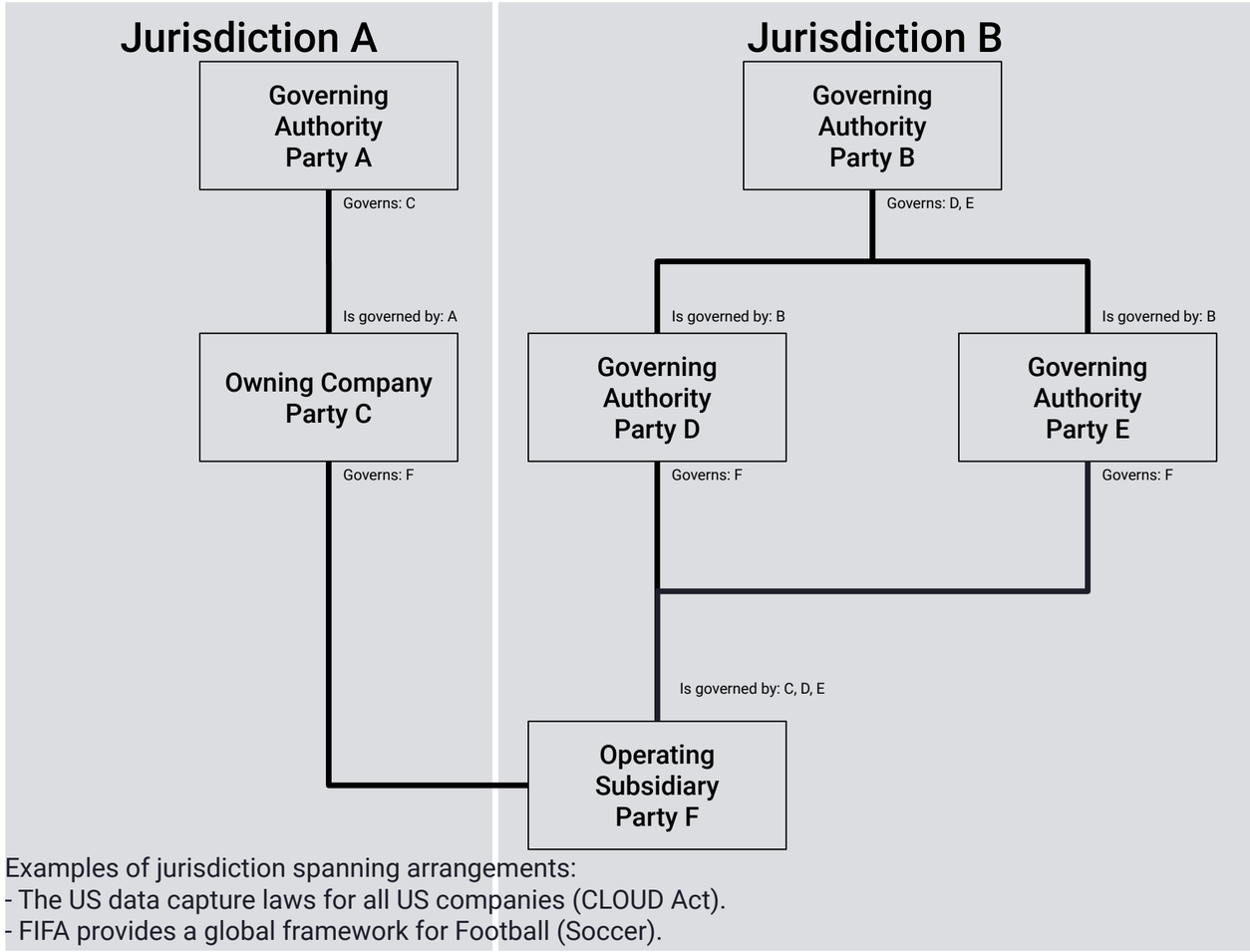
- Fair Trading Laws
- Fair Contracts
- Receipts and Itemised Bills
- Refunds and Exchanges
- Privacy and Data Protection Act

sezoo

A governance graph may span more than one Jurisdiction and may even include relationships like “ownership”

Observation: Governed Parties may be party to international governance agreements and/or be a subsidiary operating in a different jurisdiction to the parent organisation.

Where an arrangement spans more than one jurisdiction it should make clear how jurisdictional authority is recognised.



Examples of jurisdiction spanning arrangements:
- The US data capture laws for all US companies (CLOUD Act).
- FIFA provides a global framework for Football (Soccer).

sezoo

In order to be understood, the “governance graph” needs to be **discoverable** and **traversable**

If all the elements of a system declare how they are governed (who by and to what objective(s), and where), and **if** we can discover and traverse the governance graph as far as we choose (in all/any directions), **then** we can gather governance information about a Party until we have enough confidence to make a context/risk based decision), or until we exhaust the graph.

Either way, we can make a decision based on what we’ve learnt given the context/risk.

sezoo

Summing a few of these observations…

- We can consider Governance to be either explicit or implicit, internal (self) or external.
- We can assume that governance is **always** there in one of these forms.
- Governance relationships between governing authorities and governed organisations form a graph or network
- Parties operate within Jurisdictions, which provide another form of governance
- To enable a verifying party to gain supporting information about others we need we each party in a ToIP system to state how it is governed: who by, to what purpose(s), where, and how.
- We need a protocol to enable searching and exploring a governance graph.

sezoo

So we might propose **a few** (as few as possible) canonical requirements for Governance in ToIP…

1. A Governing Party MUST declare what Jurisdiction they are in and list the governance arrangements that they govern and the Parties that are governed by those arrangements
2. A Governed Party MUST declare what Jurisdiction they are in and list the governing arrangements and the governing authorities that they declare themselves to be governed by
3. Each Governance Arrangement MUST declare sufficient information about the arrangement such as the Parties, Objectives, Process/Procedures, Outcomes, Jurisdiction, Version and Status
4. All Parties in a ToIP Governance Framework MUST support the <<protocol [1]>> that allows searching and traversing their governance graph.

[1] Insert name of protocol here

sezoo

Item 3 of this list is very much like the ToIP Governance Metamodel Specification - that's a good thing!

[https://wiki.trustoverip.org/display/HOME/ToIP+Governance+Metamodel+Specification]

1. A governing party MUST declare what Jurisdiction they are in and list the governance arrangements that they govern and the Parties that are governed by those arrangements
2. A governed party MUST declare what Jurisdiction they are in and list the governing arrangements (and the governing authorities) that they declare themselves to be governed by
3. Each Governance arrangement MUST declare sufficient information about the arrangement such as the Parties, Objectives, Process/Procedures, Outcomes, Jurisdiction, Version and Status
4. All Parties in a ToIP Governance Framework MUST support the <<protocol [1]>> that allows us to search and traverse the governance graph that they are a part of.

[1] Insert name of protocol here

sezoo

Governance in the context of Trust over IP

sezoo

Trust over IP's mission is to provide a robust, common standard and complete architecture for Internet-scale digital trust

This mission is being realised by exploring a framework that consists of 4 layers (each layer using the services of the layer below and providing services to the layer above) and two stacks: a technology stack and a governance stack.

The thing(s) that ToIP enable are evidence or proof of reasons to trust some person, organisation or thing.

The transactions are "trust decisions".

sezoo

Stepping back…
What is a “trust decision”, and what role does governance play in making one?

We might consider any decision to take action based on data a “trust decision”.

While we may know who published the data and that it hasn’t been tampered with, can we be certain of the “trustworthiness” of the issuer and the outcome of our action?

We only need “trust” in the presence of uncertainty, and there is **always** some uncertainty (see Rachel Botsman etc.)

sezoo

Context, Sufficiency, and Trustworthiness

In order to decide to take an action with another party, we need to gain **sufficient** evidence to meet our **contextual** needs.

We need to find that the party is (or is not) **sufficiently trustworthy** given the context of the decision (its risk/value and the choices we have available to us).

sezoo

So when does governance come into play in the “classic” Issuer | Holder | Verifier model?

Let’s approach our answer by considering the situation at a well known point to ToIP thinkers: where the holder is providing a verifiable presentation in response to a proof request from a verifier.

From here we’ll explore what had to happen beforehand, and what might happen next…

sezoo

Let’s use a story that may be familiar to some…

Setting the scene

In our story, Jackie, a happily working adult, wants to buy a bottle of wine to celebrate with one of their friends who has just got a new job.

We have the following cast list and roles:

- Jackie: Wine buyer (“Holder”)
- Pino the Wine Seller: Organisation (“Verifier”)
- Licensor (“Issuer”)
- Age Verification Issuer (“Issuer”)

sezoo

At the point of sale

Jackie goes to Pino, a wine seller, finds a bottle they like, and asks to buy the bottle of wine. Before selling the wine to Jackie, Pino needs to know if Jackie is old enough to buy alcohol in the jurisdiction in which Pino is licensed.

HOW DOES PINO KNOW THAT THIS NEEDS TO BE ASKED? BECAUSE THE REGULATIONS OF THE JURISDICTION UNDER WHICH PINO IS OPERATING REQUIRE IT.

sezoo

Business inform thyself

How did Pino learn all this? Pino (or their business) had to inform themselves since operating **within** the law is a requirement of their business licence. This happened sometime BEFORE the interaction with Jackie.

In Victoria (Australia), these regulations are described here: https://www.vic.gov.au/acceptable-forms-identification-for-licensed-premises

sezoo

So we know that Pino knows what to ask, and what will be sufficient and acceptable proof in their jurisdiction

Given that we know that Pino knows what they need, we can either assume that they ask for explicit types of proof, “have you got one of the following proofs of age…”, or that they ask for a “proof of age”, or “ID”, and then check whether what Jackie offers meets their requirements.

sezoo

And Pino can ask for something else if the first proof doesn’t work…

IF Jackie’s first proof doesn’t meet their requirements, Pino can ask Jackie if Jackie has something else they could use (and that might satisfy the regulations as understood by Pino). This can repeat until Jackie doesn’t have something else in which Jackie exits (no sale).

IF a proof from Jackie does meet Pino’s requirements, then Pino goes on with the sale.

sezoo

Jackie can be pre-informed too

Jackie is also able to inform themself of the law in terms of what proof(s) they need to provide.

Importantly, Jackie can know what is legally acceptable to be asked by the store before selling a bottle of wine. Jackie might want to protect themselves from overreach of the store or of Pino in terms of personal details.

Generally this is self-directed rather than public notice, but for online systems we can imagine this information being made available.

sezoo

Maybe we can provide Jackie with additional protections?

The physical world doesn't have easy ways to provide buyer protections (it's hard to "see" fakes and identify scammers), but a ToIP model might let us consider some additional capabilities such as Jackie being able to check in real time that the store is currently licenced and that they are allowed to ask the question(s) that they are asking.

sezoo

Towards a mental model…

sezoo

I have argued for a need for **objectives**, **jurisdictions**, **governance**, **roles**, and the **rights** and **duties** of participants to each other.

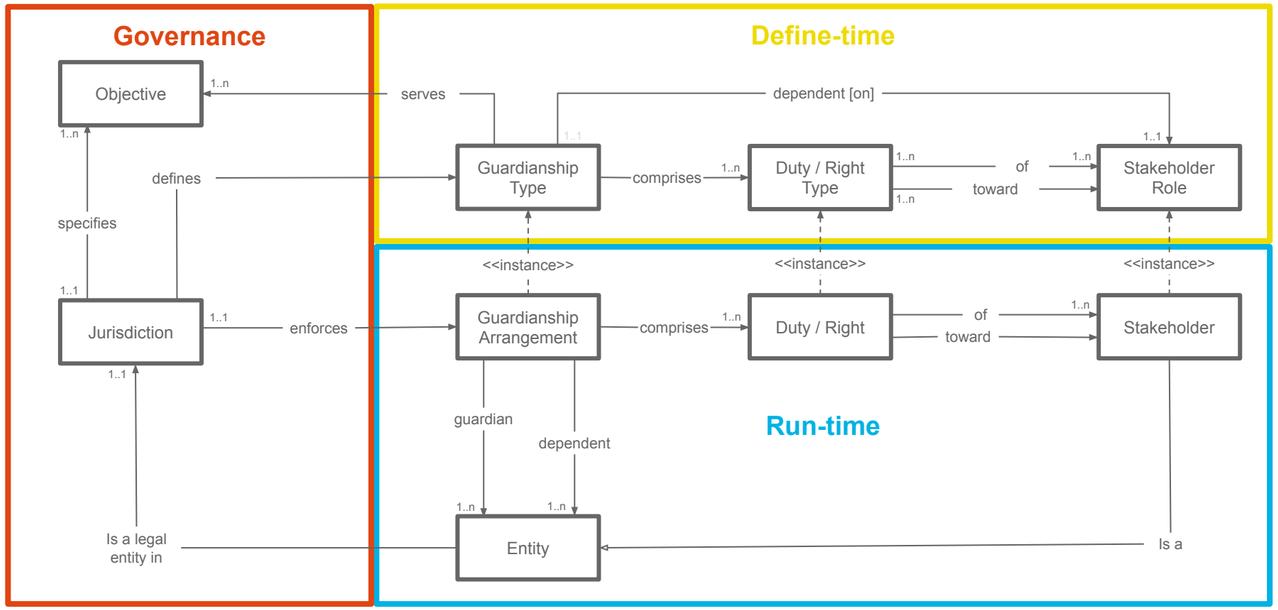
These elements are similar to a mental model that was developed for another purpose, guardianship…

https://drive.google.com/file/d/1vBePVx8n3MRDWcePkwVDya9ab4BHEyU_/view

sezoo

This is what the guardianship mental model looks like.

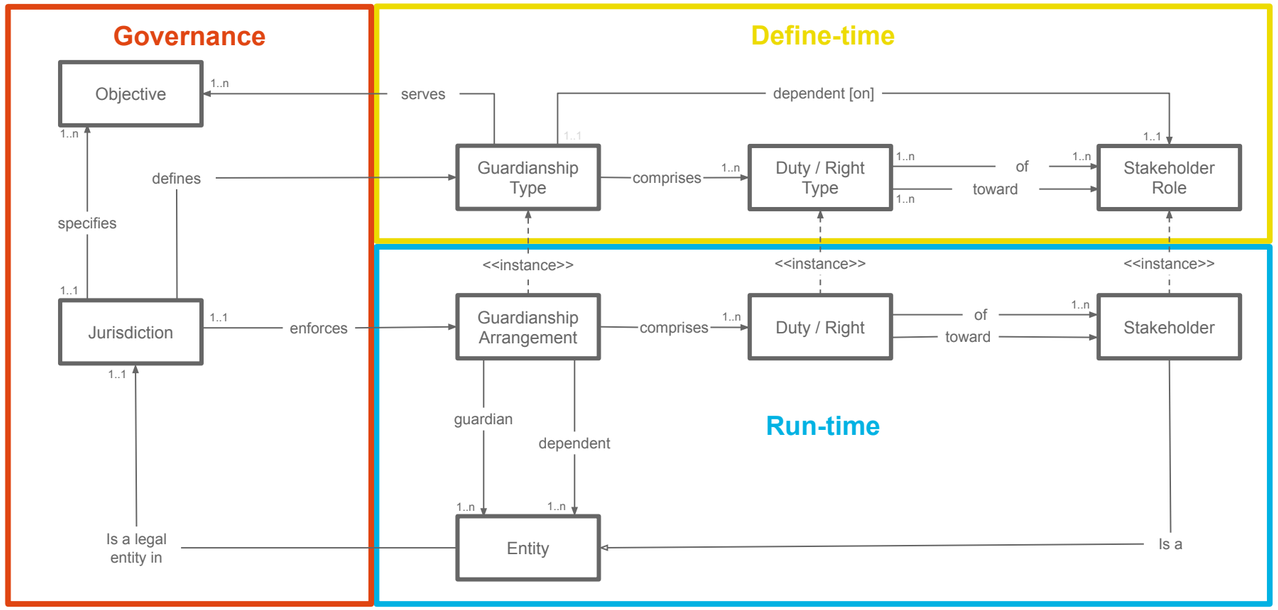
This model, developed by Rieks Joosten of TNO, gave meaning for the terms and concepts used and provided a powerful simplification of a complex subject.



sezoo

“Guardianship” involves defining how parties can be issued with credential(s) proving their responsibilities to each other.

Could we repurpose this model to create a mental model for governance?...

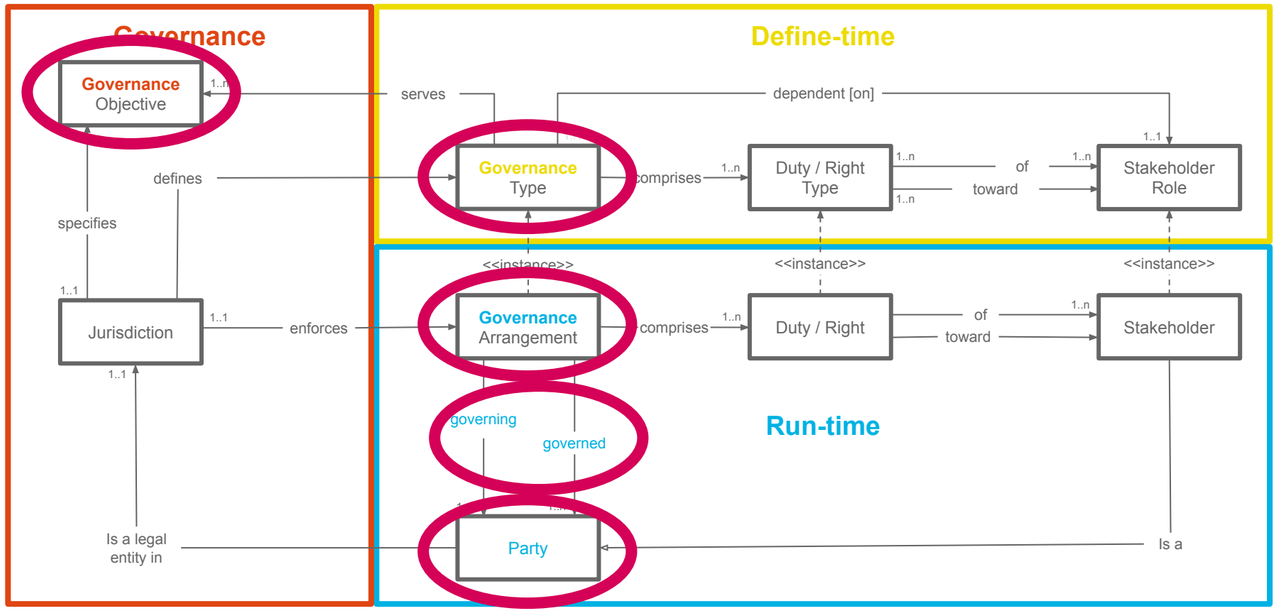


sezoo

Let’s try a few simple changes:

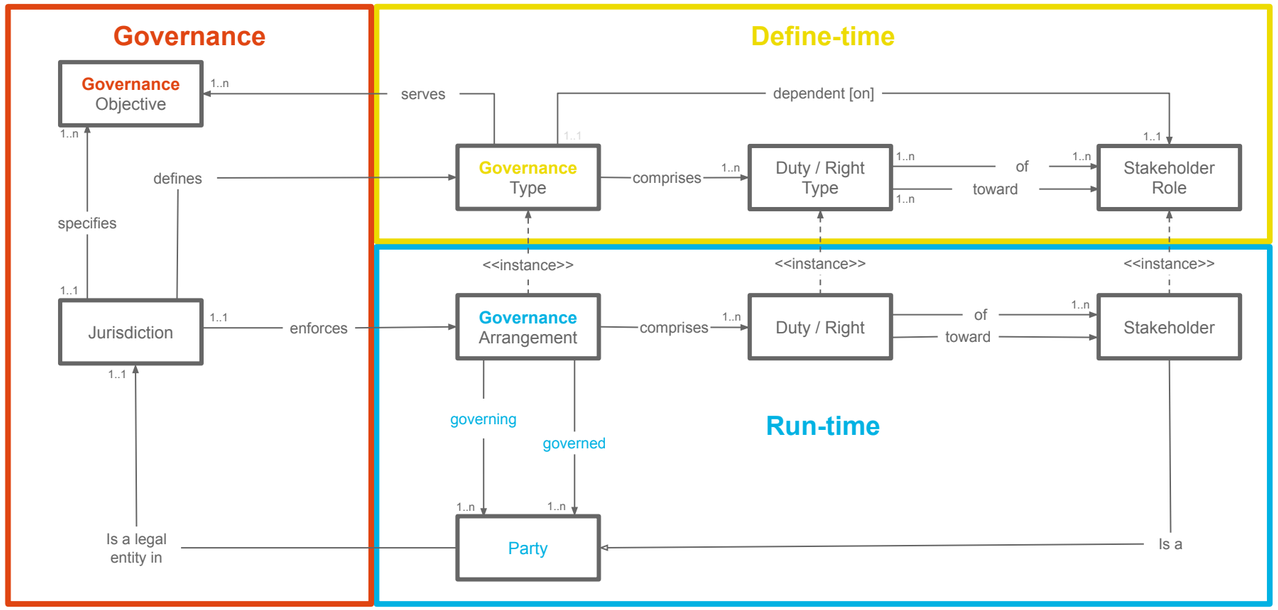
- *Objective → Governance objective*
- *Guardianship Type → Governance Type*
- *Guardianship Arrangement → Governance Arrangement*
- *Guardian → Governing*
- *Dependent → Governed*
- *Entity → Party*

Note 1: The “Entity → Party” change is for consistency of terms used in this pack



sezoo

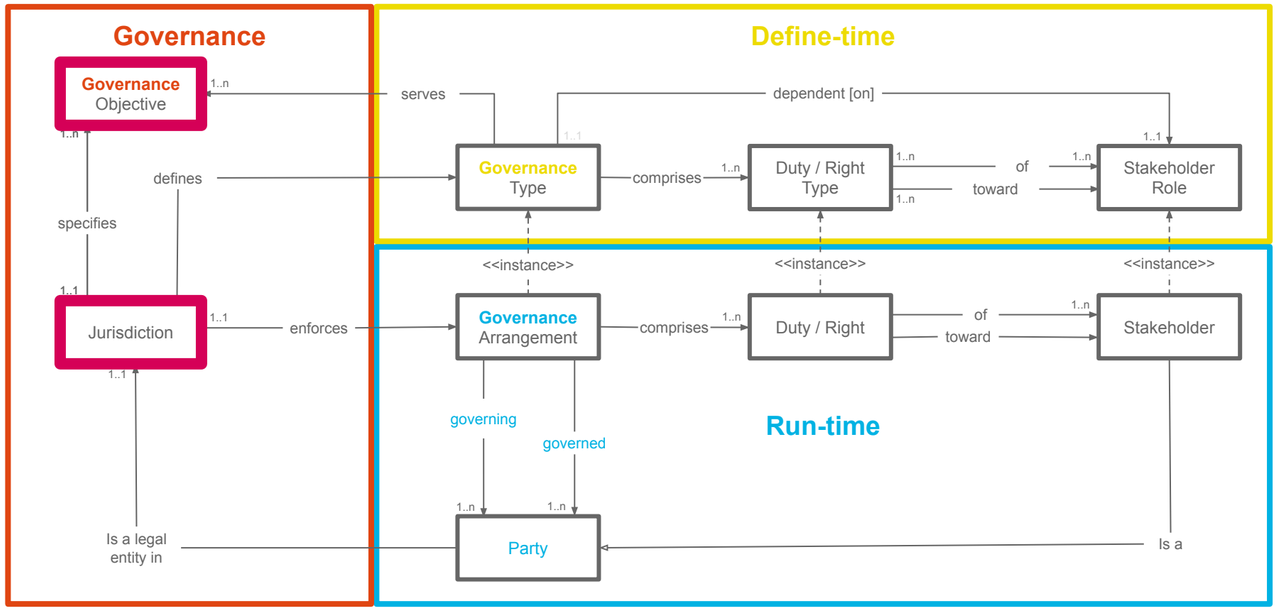
Now let's explore the revised model and see if it works…



sezoo

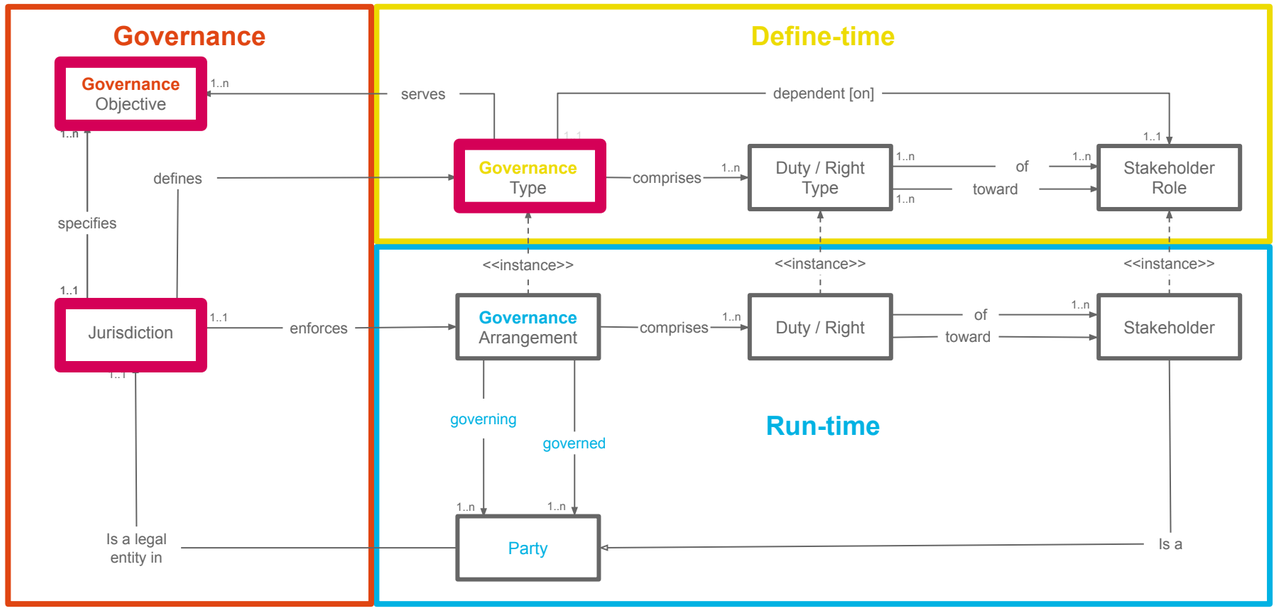
It tells us that “governance” starts with *Governance Objectives* specified by a *Jurisdiction*.

For example, a Jurisdiction might want to restrict the sale of alcohol to licensed organisations and to people who are considered an adult (over 18 or 21 say)



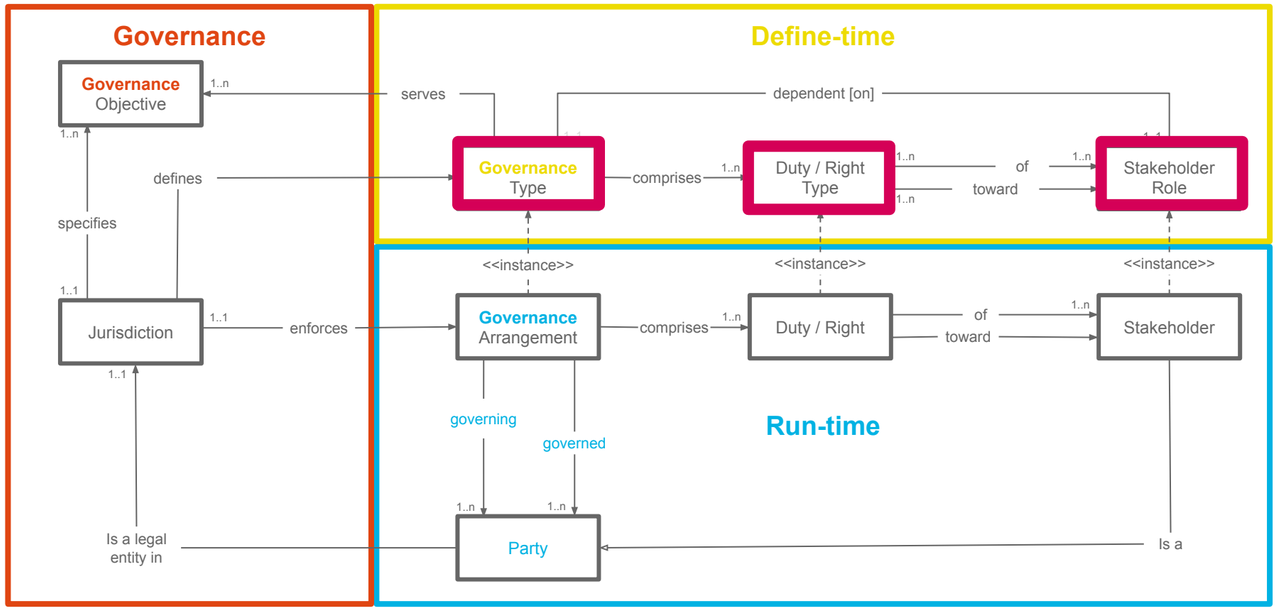
sezoo

It tells us that a "*Governance Type*" serves one or more *governance objectives* and these objectives are defined by a *jurisdiction*.



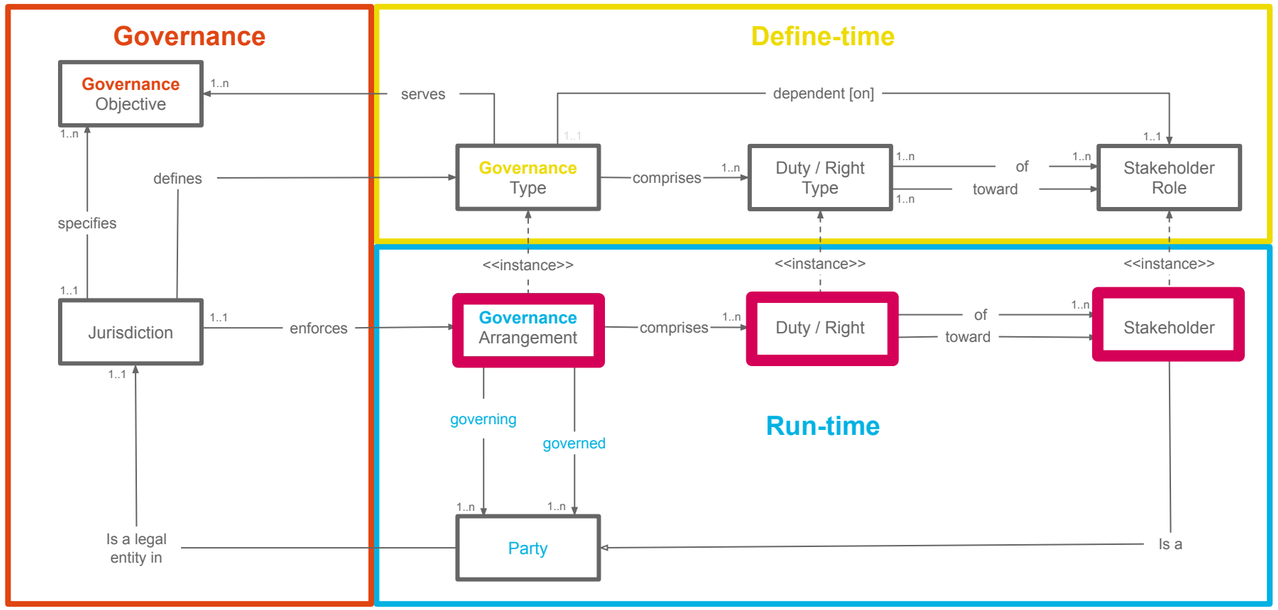
sezoo

And that each "define-time" *Governance Type* includes the governance *duties and rights type* for each *stakeholder role* in the governance type.



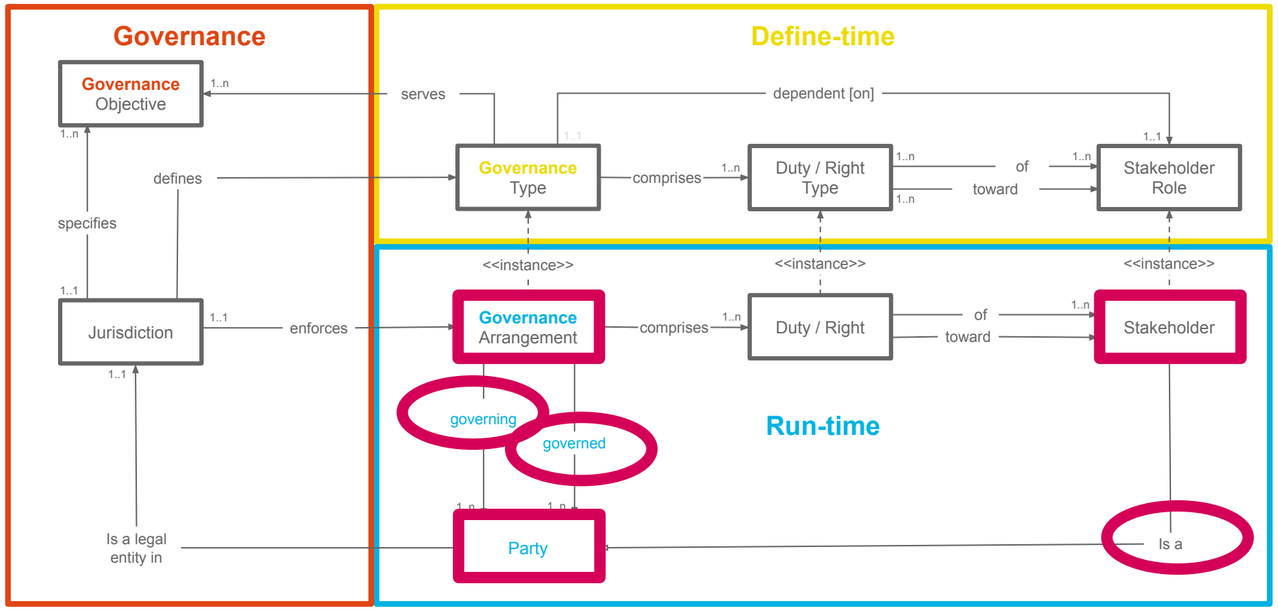
sezoo

Each “run-time” instance of a *Governance Type* is a specific *Governance Arrangement*, and this includes specific rights, duties and stakeholder identification



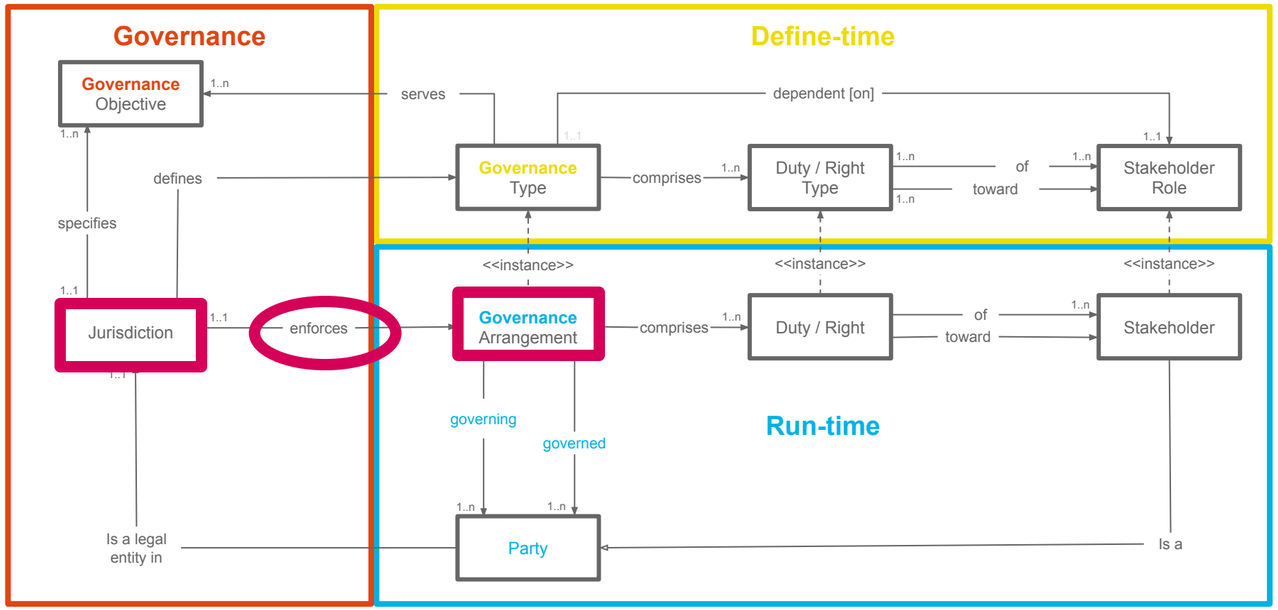
sezoo

It tells us that each *Party* in a *governance arrangement* is either *governed* or *governing*, that all are *stakeholders*, and that one or more of each may be involved in any arrangement.



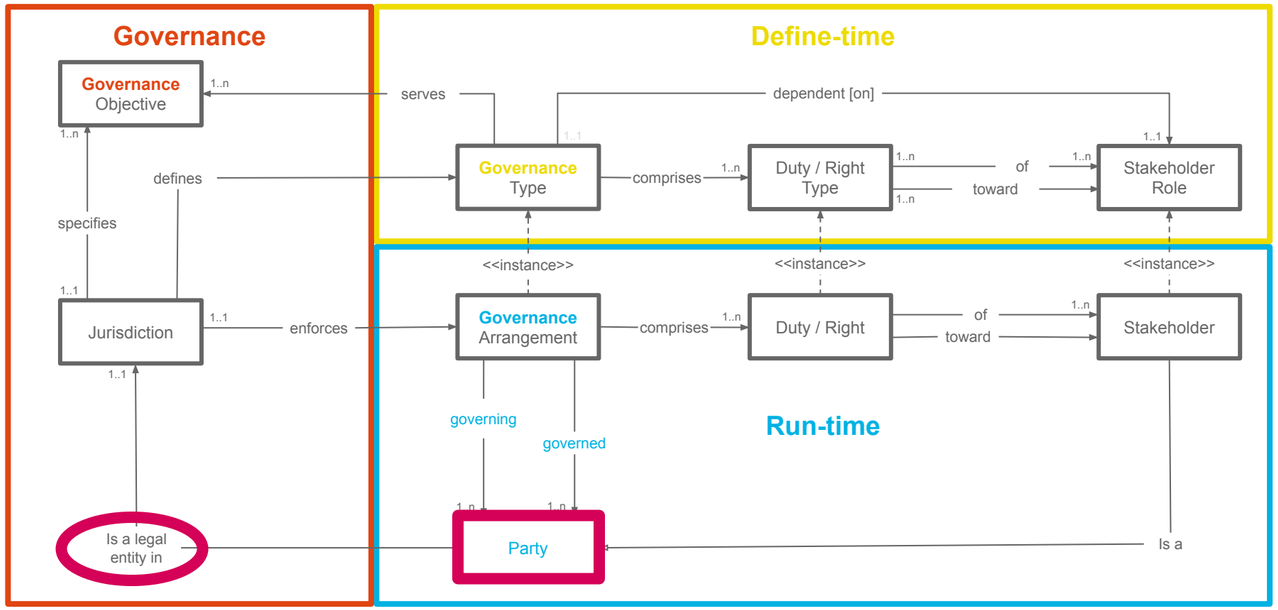
sezoo

It means that (recognises that) each *Governance Arrangement* has meaning/significance (and is enforced) by a *Jurisdiction*



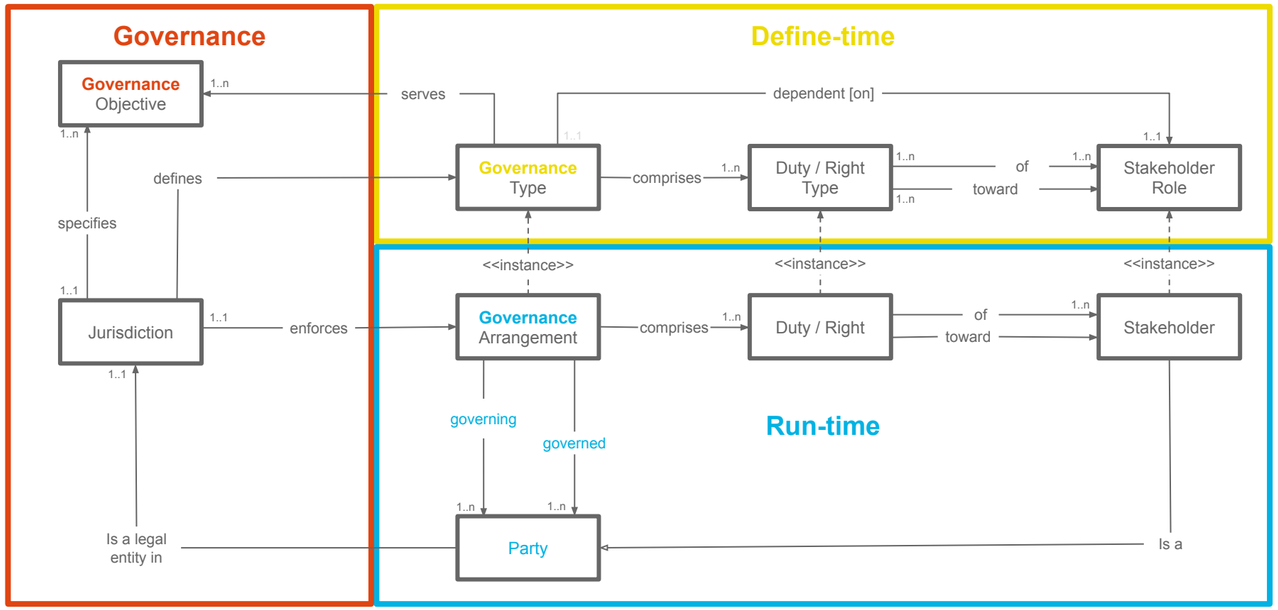
sezoo

And finally that each *Party* needs to be recognised as legal entity in the *Jurisdiction* (in order to be governed by the *Jurisdiction*).



sezoo

It seems to work.



sezoo

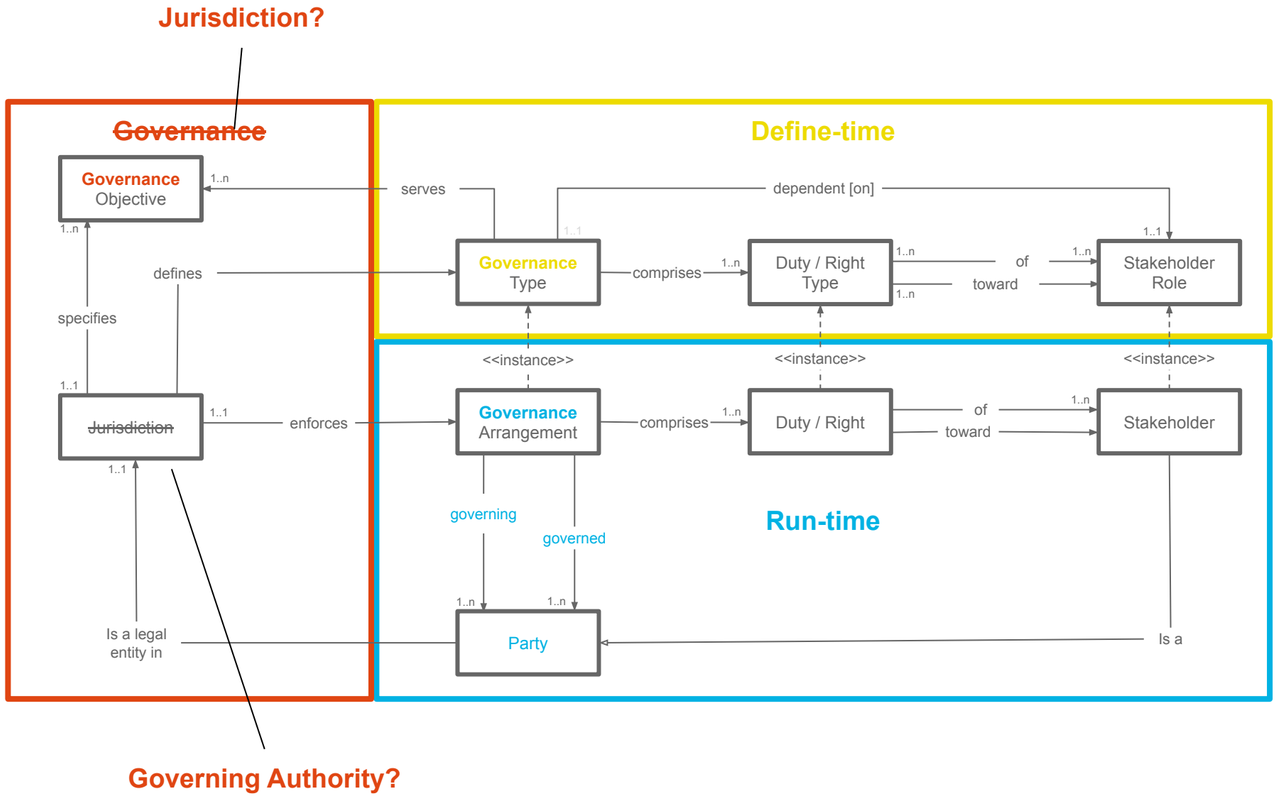
Further changes?

What if we change “Jurisdiction” to “Governing Authority” and “Governance” to Jurisdiction?

This has some attractive qualities: we seem to have a better mapping to the concept that only “actors” can do something, it wasn’t clear how a jurisdiction could specify objectives, but it seems clearer how a governing authority might.

However, we lose some of the elegance of the *Party* being either one of two types (governed or governing), and we’d need to reinstate or make clear the role of *Jurisdiction* somehow (it can’t just be the outside box). Perhaps “Jurisdiction” should be “Jurisdiction Authority”?

Perhaps we should include the concepts of “Governing Authority” and “Governing Body” as explained in the ToIP Governance Meta Framework?

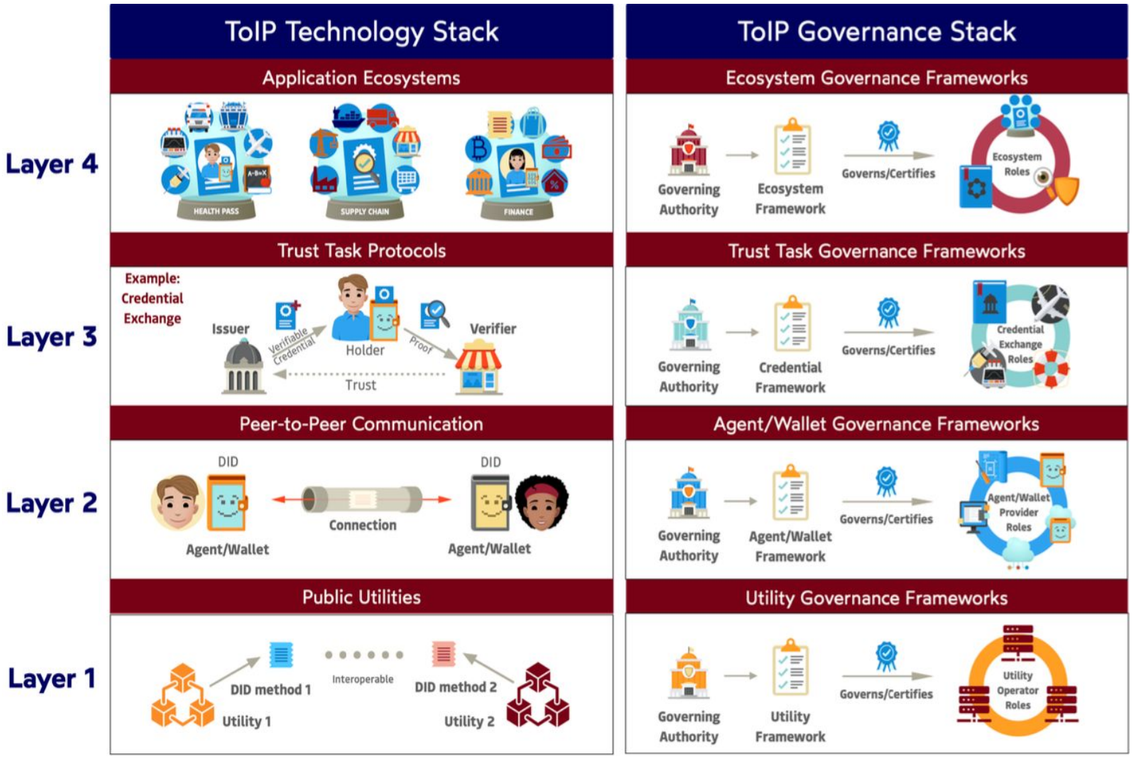


sezoo

…in the context of ToIP

sezoo

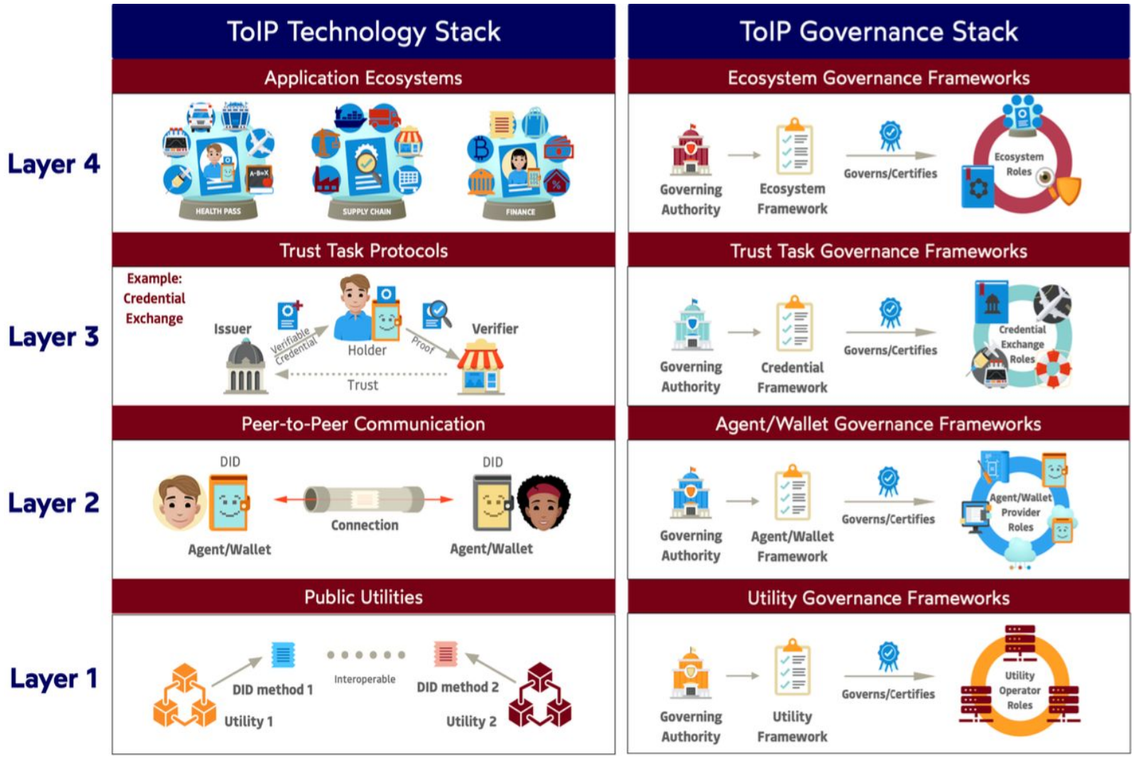
How would this mental model affect how we might interpret governance in the ToIP framework?



This is the ToIP “Stack” diagram as of September 2023 (there are updates being considered)

sezoo

We can see that there are defined elements and protocols in each layer of the technology stack, and we can see that in this representation of the framework, each layer has governance through a “Governing Authority”

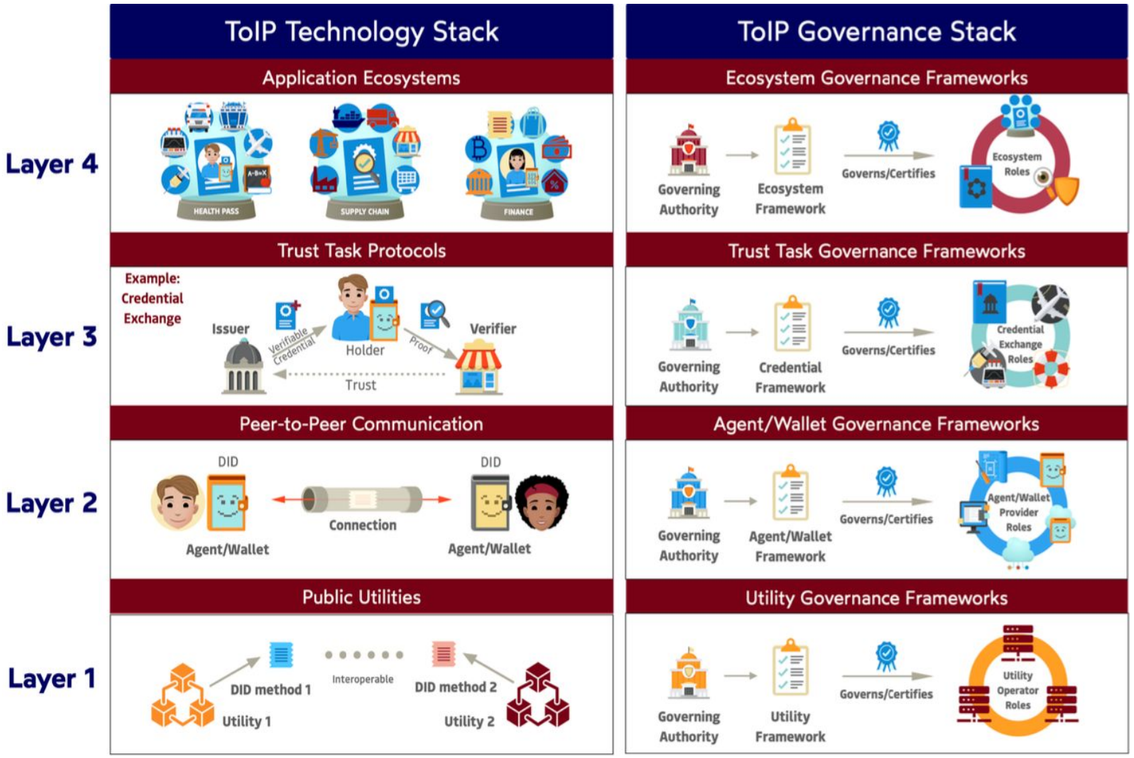


Note that the requirement to declare how something is governed is the same regardless of whether the element is an issuer, a verifier, an agent, a trust registry, a verifiable credential definition, a DID Doc, a communication protocol etc. etc.

The “how” references the governance arrangement(s) and this defines the specific governance objectives, outcomes, rights and duties relevant to the entity in its jurisdiction.

sezoo

Our mental model for Governance has reinforced the idea that we need each “party” to declare how they are governed, the objectives and outcomes of the governance, and by who (where this may be more than one party).



sezoo

Side Note:

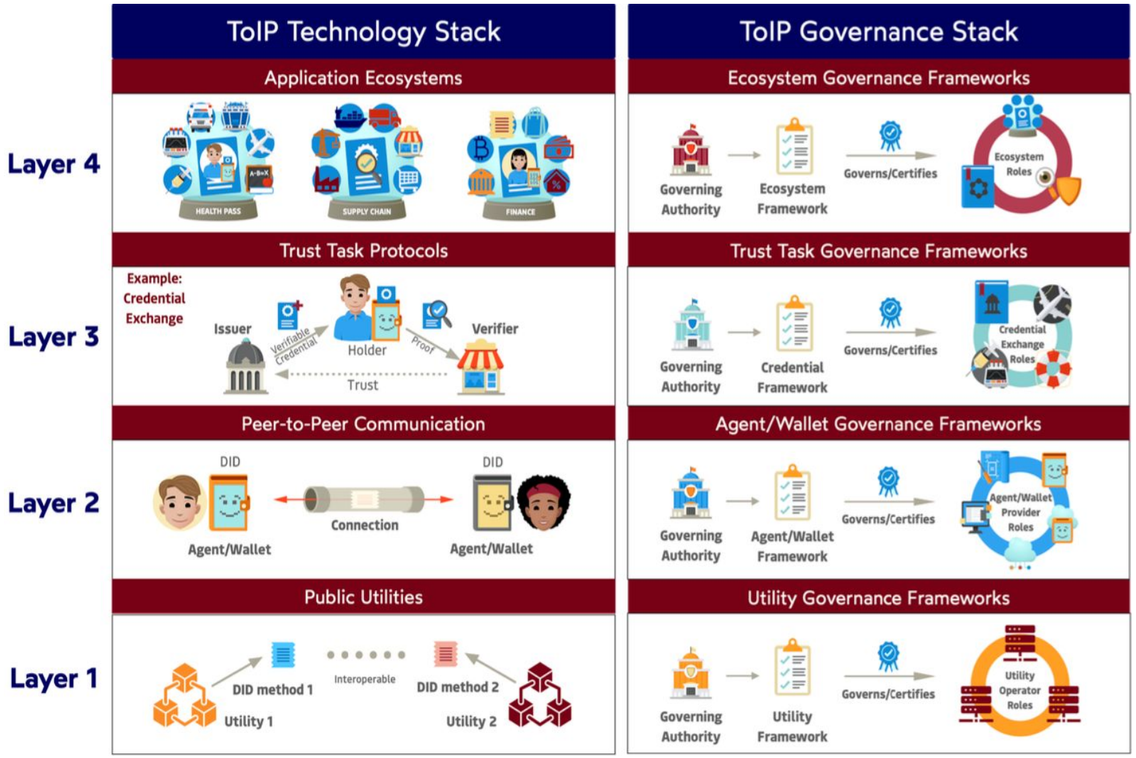
One way of thinking about the role that governance plays in enabling trust is to think of the “technology stack” as ensuring that we can deliver data that is trust **worthy,** that is it is worthy of trust in that the cryptographic proofs available ensure that we can trust who authored it and whether it has been tampered with or not.

We then need to decide if we “trust” the information we’ve verified enough to go ahead with a transaction.

If we haven’t previously heard of the issuing organisation, we might choose to find out how they are governed, and if we don’t recognise that body, we might go further to find out who governs them.

Thus we use the “governance stack” not only to ensure governance is performed in creating and operating an implementation, but to gather governance evidence during verification of data that helps us make a trust decision.

Governance is a separate and necessary “dimension” of our trustworthy checks.



sezoo

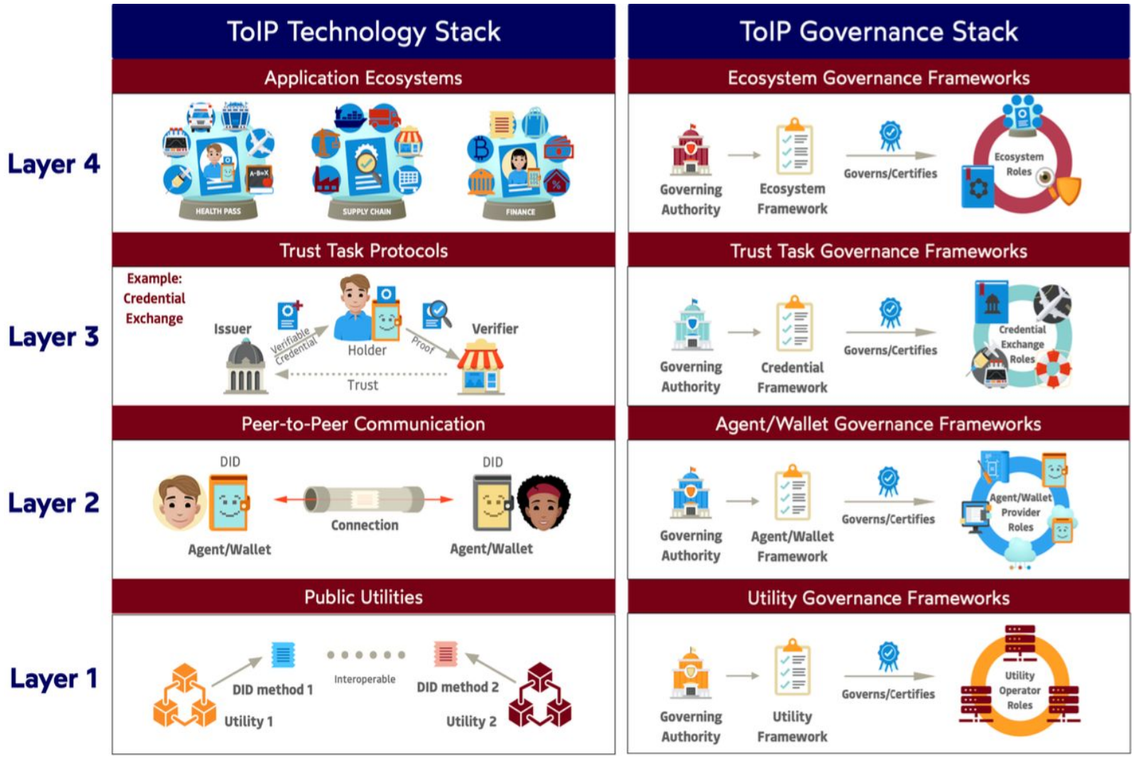
It has also highlighted that we need to “traverse” governance graphs.

A simple example might be where someone provides a proof that they hold a University degree as part of their application for a job.

The Verifier might do the usual checks on the offered proof (who issued, to who, is it intact, has it been revoked etc.).

If they don’t “know” the University, they may want to check that the issuer **is a** University. They may want to understand who “governs” their status as a University, by what standards they are governed by etc.

So we need a governance / trust spanning protocol. Rather than develop a new one, we should see if one, or a combination of, existing protocols would work.



sezoo

Background and left over slides

sezoo

We'll need to define the meaning of a few terms that we've used in this pack

While these terms have other meanings elsewhere, we want to make sure that within this pack, the meaning we intend is clear.

We want to start with as few as possible, we'll use these concepts and how they interrelate to build the others.

sezoo

Party

An organisation or a person that is involved in a process and is able to take action, have objectives, and make decisions.

Note 1. We want to use simple words. We could for example use to the word “entity”, but this is not a word that most people use in conversation, and “party” is also used in law to describe relationships in contracts, and that can work for us here too.

Note 2. We might consider including “things” as another type of party, but unless they are capable of having objectives, taking actions, and making decisions, we won’t be able about to think about “governing” them in the same way that we can with organisations and people. We will likely need to think about how the creation, installation, setting, operation of “things” is governed rather than the “things” themselves. We might also require that “things” be built to (and be proven to meet) standards - but they are not a “party” in the sense we’re using here.

We will clearly need to take care with autonomous systems and AI…

But we’re getting a bit ahead of ourselves here… back to the simple building process…

sezoo

Jurisdiction

We might give a formal definition of a jurisdiction as the legal environment in which laws can be defined and policed.

We may need to relax this constraint, we want to consider governance by self-regulated sectors or entities, the peak bodies of sporting codes etc, so these also can be a form of “Jurisdiction”.

Jurisdiction then becomes the context in which governance is recognised.

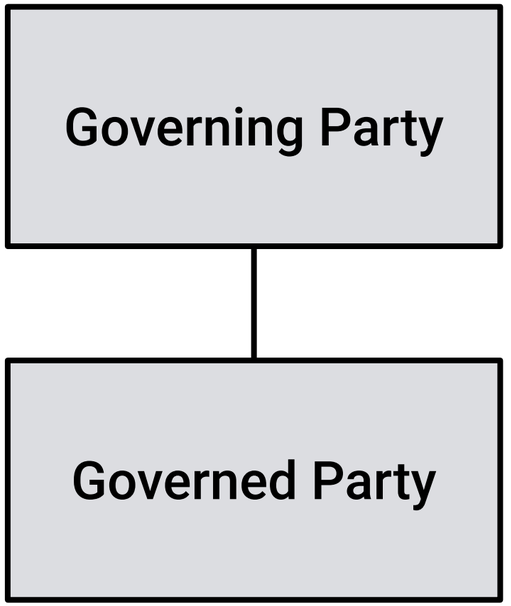
sezoo

Side Note:

In some situations, we might distinguish between “external” and “internal” governance.

External

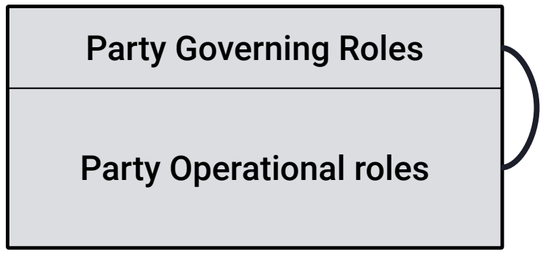
Here the governing party and the governed party are independent of each other.



Internal

Here “governance” is provided by internal roles. Audit and Risk committees, Chief Risk Officers, Probity Officers are examples of roles that are internal to an organisation (they are employees), but intended to provide independent advice to the organisation.

An organisation might also be “self-governed”, with no external governance.



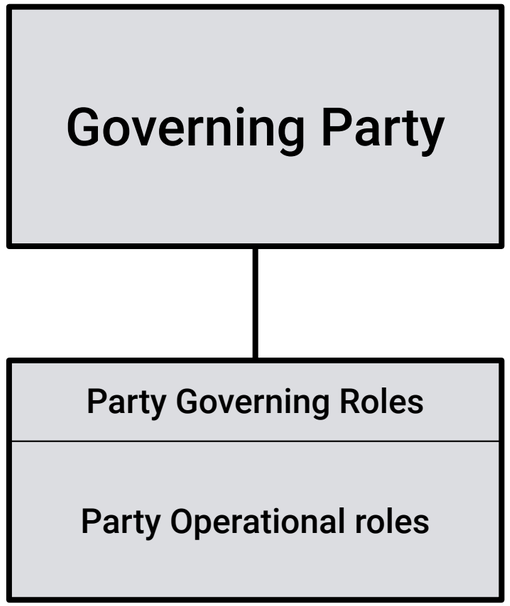
sezoo

Side Note:

And sometimes both internal and external governance is present.

We want **both** to be possible in the mental model.

Observation: we will want it to be possible for a party to declare **how** it is governed, whether that is external/internal, both, or (perhaps) neither and by who and where.

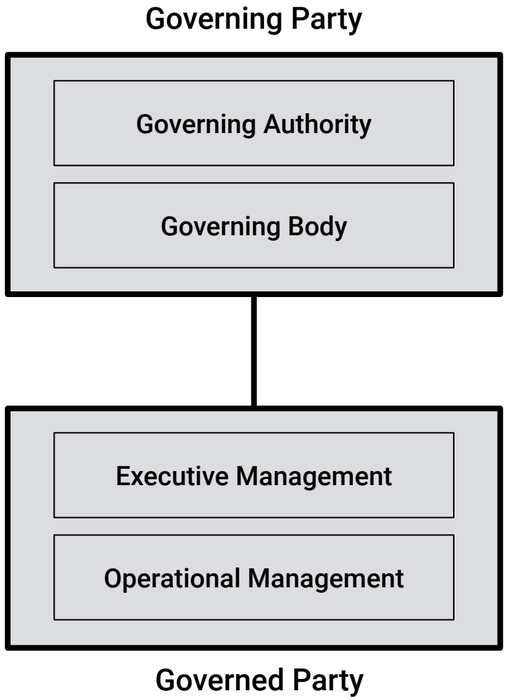


sezoo

Side Note:

We might also consider that creating rules, and auditing and enforcing rules are separate.

For now we'll keep to a simple governed and governing party.



Sets framework of rules, standards, regulations, law.

Executes framework: licences, regulates, monitors, measures, audits, rewards and punishes

Manages, operates, decides, checks and aims to comply with rules, standards, regulations, laws.

Executes the operating system

sezoo

Side Note:

We are only describing **how** something is governed, not **how well** something is governed.

While we can understand that there may be recognised “levels of governance”, and even certified “governance maturity models” etc., we don’t need to define these levels to have a working mental model.

We may however want to state **if** any particular party and arrangement meets any recognised standards of governance.

If they already exist, let’s enable their use.

sezoo