The Lean Governance Thesis

Jack Laing

With thanks for the comments of Michael O'Rourke, Dermot O'Riordan, Nelson Ryan, Stéphane Gosselin, Adam Liposky, Lawrence Lundy-Bryan, Philippe Honigman, Louis Giraux, Felix Machart, Xule Lin, and John Light.

This document is written as a companion to the Pocket Network Constitution for informational purposes only, to help stakeholders more clearly understand their social contract with Pocket Network, and therefore does not carry the same binding interpretation as the Constitution. For this reason, this document is not subject to the Constitution's amendment restrictions and, where the contents of this document are inaccurate or perceived to imply different meanings than the Constitution, the Constitution should be taken as the source of truth.

This document assumes prior understanding of Pocket Network, for such details please refer to the Whitepaper and the Economics Paper. For Definitions, refer to the Constitution.

TL;DR

- The purpose of governance is systemic evolution, but governance limits its own evolution through path-dependent lock-in.
- Successful future-proof governance requires a balance between flexibility (optionality of future system designs) and legitimacy (conformity of new system designs to the underlying rulesets of previous system designs), which can be achieved using modularity.
- The Lean Trias Politica is a modular governance design that establishes a foundation of minimum viable legitimacy and maximizes the freedom of the Legislature to evolve as it learns.
- Pocket Network establishes throughput legitimacy through on-chain validation of decision-making inputs (Governance Stakes), cross/off-chain conservation of throughputs (Aragon/Cayman courts), and enforcement of decision outputs (parameterized Governance Transactions, controlled by the Pocket Network Foundation then Aragon Agent).
- Compliance is achieved using the Foundation as a legal wrapper, which limits external liability, and the Constitution as an internal arbitration agreement, which limits internal liability.
- Autonomy can be achieved by progressively automating the bridges between governance modules.

Modular Governance is Future-Proof Governance

Not all contracts can be smart, because the humans who write them are dumb. Human coordination institutions - firms, governments, and now blockchains - inherently contain contracts which are implicit (unspoken agreements) and incomplete (agreements with unforeseen outcomes) (Prysm Economics, 2018), because it is impossible for humans to predict and account for every contingency. The existence of such contracts means institutions will always need to adapt, contracts will always need to be rewritten. Governance defines the procedures by which this evolution takes place.

During these procedures, disputes are inevitable. Institutions without legitimate evolutionary processes, designed to resolve disputes and amend systems within an accepted (legitimate) ruleset, are likely to face mass exit of their members. This is complicated further by the fact that blockchains' implicit contracts are in flux as decentralization is bootstrapped, are often at odds with idealist decentralization philosophy, and exist in a constant state of tension and mutual evolution with their explicit contracts (Allen & Berg, 2020). These institutional dynamics are exemplified by The DAO hack (an unforeseen outcome) which highlighted an ideological conflict about immutability (misaligned implicit agreements) that lead to the Ethereum hard fork.

These dynamics are the reason that many view governance as the key competitive dimension on which blockchains will succeed. Good governance will enable blockchains to survive changing environments (Ehrsam, 2017), to obtain any feature they want (Placeholder, 2018), to attract the ex-users of their less representative competitors (Alston, 2019), and ultimately secure their network efforts (Duncan, 2017) with inimitable advantages (Arluck, 2018). Stakeholder representation is the new customer satisfaction.

> "The governance system that yields the most utility for the largest number of users with the least overhead will ultimately manage the largest communities with the most valuable data."
> (Union Square Ventures, 2007)

Where things get complicated is in using the governance system to amend itself, i.e. meta-governance. Governance is path-dependent (Arluck, 2018). The governance system you design today will be in charge of changing its own rules tomorrow, which means governance has a tendency to ossify. This is especially the case because the participants of your system will owe a debt to, derive positive externalities from, and have their perception shaped by the institutional framework you designed (North, 1991). Design the rules poorly, with hidden

biases, and it will be almost impossible to unwrite those biases. If inflexible institutions are more likely to break in the face of incomplete contracts, then such lock-in is something we should aim to limit as much as possible.

> "A constitution that faces more barriers to adjustment is less likely to be adaptable to changing circumstances in society, and hence, is more likely to provoke the need for wholesale constitutional overhaul."
> (Alston, 2019)

If that's not reason enough, we should also acknowledge how early we are in the dominant design process for Decentralized Autonomous Organizations (DAOs). We don't know what the future may hold for the Cambrian explosion of organizational technologies emerging today, or which industry standards will dominate, so it would be foolish to commit. Second-movers are more likely to survive dominant design processes in new industries (Markides and Geroski 2004), because they avoid the opportunity costs associated with committing to a path-dependent series of innovation choices. The Ford Model-T was not the first vision of the automobile. Furthermore, it would be arrogant to assume we've already designed the best model of governance (Ehrsam, 2017). The more modular a design, the more evolutionary paths (real options) will remain open, the more innovations will be pursued, the more economic value will be realized (Clark & Baldwin, 2002).

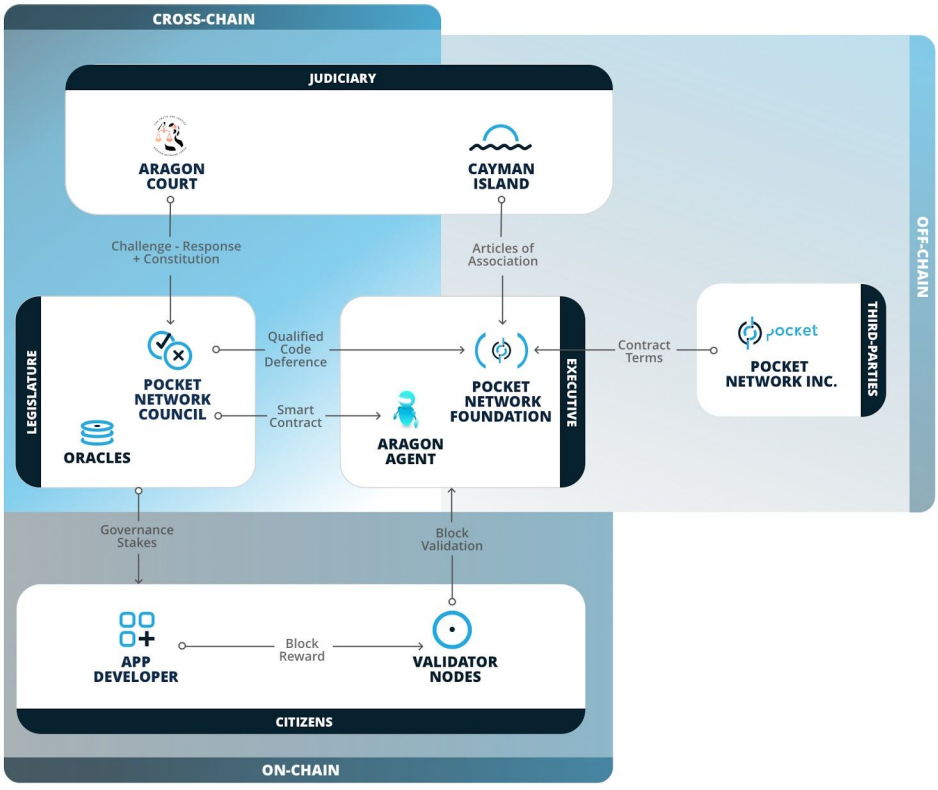
So far, blockchain governance has been optimized along the axis of "ease of change" (Sigil Fund, 2019); govern on-chain (easier to change) to maximize speed, govern off-chain (harder to change) to maximize defensibility. However, if the purpose of governance is evolution, governance is path-dependent, and options are valuable, it is most important to optimize for adaptability of the governance system itself. This can be broken down into two key characteristics: flexibility, the opportunity set of future system designs, and legitimacy, the acceptance of the authority of new system designs, where the authority of a new system is more likely to be accepted if it conforms to an underlying set of previously accepted rules and these rules include the authority to make the proposed changes. This evolutionary tension between stability and change is central to the design of institutions (North, 1991).

In systems, this tension is navigated using modularity. In manufacturing systems, modularity helps to optimize flexibility (e.g. mass customization) without sacrificing efficiency (conformity to production standards) (Ernst & Kamrad, 1997). In software systems, modularity helps to expand the variety of applications without sacrificing interoperability (conformity to communication standards) (Baldwin & Woodard, 2008). In governance systems, we're looking to maximize flexibility (optionality of the future system design) without sacrificing legitimacy (conformity of the new system design to the underlying ruleset of the previous system design). So how can we apply modularity to governance?

The Lean Trias Politica

Fortunately for us, a classical bastion of decentralized political systems, the trias politica, is already modular. This system achieves legitimacy by separating the powers of the state into three independent branches (Executive, Legislature, Judiciary) who hold each other accountable; three modules who perform independent functions but are held together by a common system of checks and balances. As long as these checks and balances are upheld, democratic nations have the power to write new laws (change) without undermining the rights of their citizens. Thus, the trias politica is a more appropriate starting point for blockchain governance than models of traditional corporate governance or full on-chain governance (Lundy-Bryan, 2019).

But we're not a nation state. Our success is not derived from the control of borders and the resources held within them; as an open-source protocol, our citizens will have a much easier time leaving our borders, as a startup, our resources are transient and conditional on rapid growth. This necessitates a leaner approach to the trias politica.



Flexibility

The purpose of the Lean Trias Politica is to establish a robust foundation of minimum viable legitimacy, in order to minimize constraints on the Legislature and thereby maximize its flexibility to evolve. The Legislature defines how stakeholder interests are represented; freeing the Legislature to evolve maximizes the DAO's ability to refine how effectively it represents interests, and therefore maximize the overall system's input legitimacy (more on this later).

Cross-Chain Legislature

The more you hard-code governance on-chain, the more powerful path-dependence becomes, the more you increase the probability that the system will face incomplete contracts it is too inflexible to handle. While all formal governance has a tendency to ossify, this is especially so with on-chain governance because the options for future amendments are constrained by the technical limits of the blockchain. On the other hand, off-chain governance allows more freedom to experiment with less risk of ossification, but risks being undermined by de facto power structures if not carefully structured (Freeman, 1972). Cross-chain governance offers the best of both worlds.

Pocket Network minimizes governance on-chain, limiting functionality to on-chain validation of voting rights (Governance Stakes) and on-chain enforcement of decisions (parameterized Governance Transactions). Everything else takes place off-chain, i.e. external to Pocket Core. By leveraging external chains for the (cross-chain) legislative function, we ensure that all decision-making is trust-minimized, censorship-resistant, and ultimately robust against de facto power.

As a result:

- Governance is not constrained by the technical limits (parameters and computational capabilities) of Pocket Core, which are optimized to process blockchain relays,
- Governance can be upgraded independently of network upgrades, by amending the off-chain ruleset (the Constitution) rather than the on-chain ruleset (Pocket Core's consensus rules).

Legally-Linked Executive

Many crypto projects have committed to abolishing their foundations, but this ignores the risk of incomplete contracts (Lundy-Bryan, 2019). Whereas the manager's role in a firm is to coordinate implicit and incomplete contracts, DAOs have no managers in principle, no-one with a duty to coordinate contracts for the good of the organization, which normally creates a difficult governance problem (Allen & Berg, 2020). This is where the Pocket Network Foundation comes in, an ownerless executive function with minimal legislative authority except in the face of incomplete contracts.

Through Qualified Code Deference (Shapiro, 2018), the directors of the Foundation are compelled to execute all of the Council's decisions, unless doing so would verifiably violate their duty to steward Pocket Network. Further, the Council has the power to hire and fire directors, ensuring that this accountability relationship is enforced.

On the legal side, Foundation supervisors ensure that directors fulfil their obligations, and have the power to sue directors on behalf of the Foundation (and by extension the DAO). The first supervisor will be Pocket Network Inc (PNI), due to our familiarity with the technology and governance processes, but neutral third-parties can be hired in the future.

In the event that incomplete contracts strike, and we haven't designed the legislative processes flexibly enough to handle some unforeseen outcomes, the Foundation is an accountable baseline that we can fall back to.

Constitution & Court

Whereas Pocket Core's consensus rules define the explicit contracts of using Pocket Network, the Constitution is an off-chain "protocol" that defines the "social contract" (Berg & Berg, 2018), aiming to demystify implicit contracts and coordinate responses to incomplete contracts. Meaningful norms are hard to express in their entirety, let alone on-chain, so defining the spirit of these norms and enforcing them off-chain is the most viable approach (Buterin, 2017). Because the legislative scope of a human-readable constitution is much larger than that of a blockchain, which affords its flexibility, this should also be paired with a robust judicial function (Alston, 2019). Due to the recursivity of constitutional amendments, constitutions often have provisions which enable defense against amendments that violate the spirit of the law (Alston, 2019), however this can cause confusion for judicial interpretation and leave room for political opportunism (Berg & Berg, 2018).

In accordance with the above considerations, we have defined a constitution that differentiates Statutes (the letter of the Constitution) from Principles (the spirit of the Constitution), which can be enforced off-chain (i.e. external to Pocket Core) using Aragon Court. The former will be used to enforce operational rules, e.g. flagging incorrectly formatted proposals, while the latter can be used to enforce norms in the face of existential governance crises, e.g. rejecting governance upgrades that undermine our values.

By defining a comprehensive constitutional ruleset, which founding stakeholders will consent to at the onset and new stakeholders will then be required to sign when joining, we also make Pocket Network's decision-making more efficient, because stakeholders will be forced to argue on the merits of their perspective rather than arguing to change the process itself in their favor (Alston, 2019).

Legitimacy

Pocket Network's legitimacy is established using two distinct but loosely integrated rulesets: an off-chain ruleset (the Pocket Network Constitution) and an on-chain ruleset (the Pocket Core consensus rules).

These rulesets are legitimate according to several key academic perspectives:

- **Political legitimacy (Locke, 1689):** political legitimacy, derived from popular consent, is established when Users consent to the Pocket Network Constitution, through their Use of Pocket Network's services (see 'Informed Consent' in the Constitution), and Validator Nodes consent to the Pocket Core consensus rules, through their decision to use those consensus rules when validating transactions and/or to validate the transactions that upgrade those consensus rules,
- **Rational-legal legitimacy (Weber, 1922):** rational-legal authority is enforced by the Judiciary, both cross-chain (Aragon Court) and off-chain (Cayman Island courts), which both have the power to ensure that the laws of the Constitution are obeyed,
- **Substantive legitimacy (Weigand, 2015):** the Constitution's Principles establish a set of shared values that authorize the sacrifice of individual advantages in pursuit of a greater good, which individuals subscribe to when they consent to the Constitution,
- **Input and output legitimacy (Scharpf, 1997):** input legitimacy (representativeness) is established through permissive access, giving everyone the right to a vote if they validate their stakeholder status, and output legitimacy (effectiveness) is established in the long-term by empowering the legislative branch to refine the system to optimize for the effectiveness of decisions
- **Throughput legitimacy (Schmidt & Wood, 2019):** the integrity of governance inputs and outputs are enforced through the trias politica, which ensures that no party has the power to corrupt the throughput of policies.

On-chain governance is popular because it achieves throughput legitimacy with minimal coordination effort, through automatic validation and enforcement of token votes. If we view governance as a decision function (Buterin, 2017), validation and enforcement of votes achieves throughput legitimacy because it helps token holders to trust the integrity of the decision outcomes, even if they had a different preference (Sigil Fund, 2019).

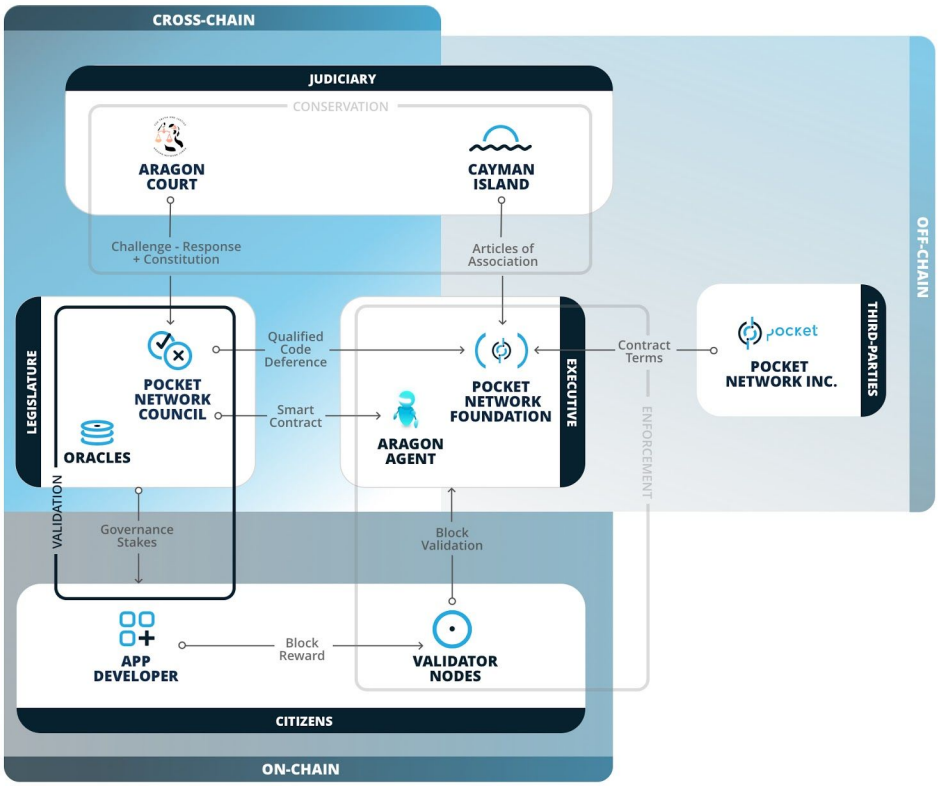
However, on-chain governance does this in sacrifice of input legitimacy (token holders are unlikely to be representative of all stakeholders) and output legitimacy (on-chain governance has a narrower set of amendment options and thus a narrower set of evolutionary paths).

Whereas Pocket Network's hybrid governance system can evolve dynamically by amending the off-chain ruleset (Constitution), which is constrained only by the limits of the human language and the infinitely compounding set of tools available to us, fully on-chain governance systems

can only evolve by amending their on-chain rulesets, which are constrained by the limits of their parameters and computational capabilities.

Automation is not the only way to achieve throughput legitimacy, which means these are unnecessary sacrifices to make. I will now outline in-depth how Pocket Network achieves throughput legitimacy using the Lean Trias Politica.

Validation of Inputs



Input legitimacy is achieved when policies are representative of all stakeholders.

We validate the identity of stakeholders through a Governance Stake, wherein stakeholders signal their desire to participate in the Council by depositing POKT to the DAO's on-chain treasury. These stakes encompass the entirety of the on-chain legislative function; they perform the minimal function required (signaling on-chain stakeholder status) while outsourcing validation, throughput, and enforcement of stakeholder decisions off-chain.

Using this Governance Stake, we chart two routes to Sybil resistance, designed to be accessible to genuine stakeholders but such that the opportunity cost is too high to maintain multiple voting identities:

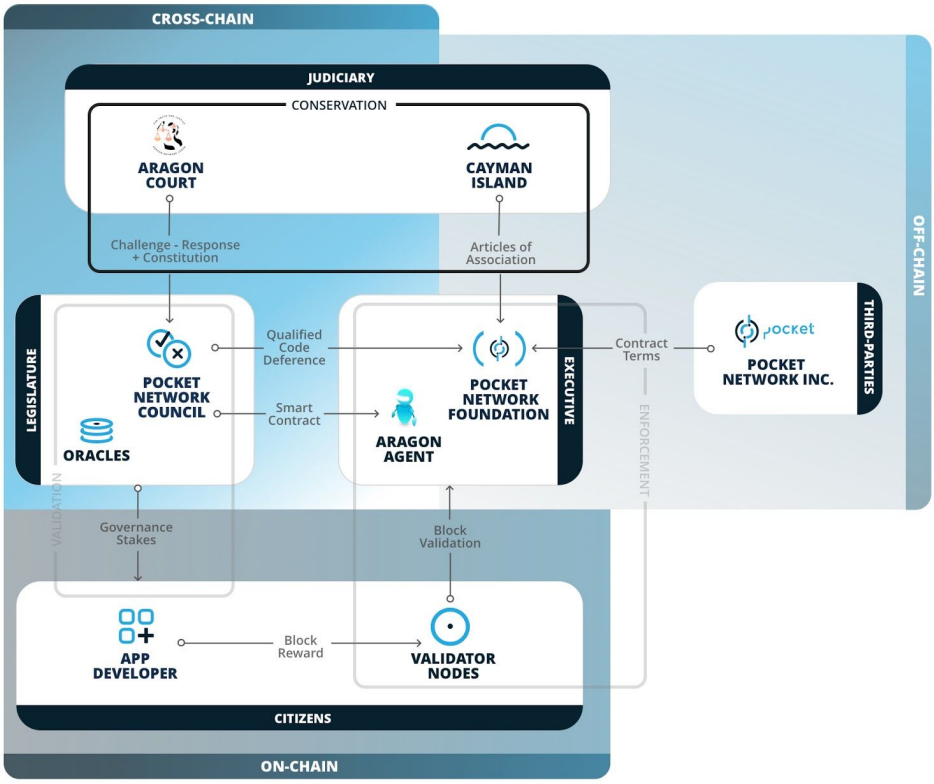
- A **Trust-minimized Stake** increases liquidity costs so that they are equivalent to the value of the treasury; a trust-minimized staker must stake an amount equal to the value of the treasury divided by the number of current voters. This will be very expensive at launch, reflecting the small scale and resultant vulnerability of the Legislature, and the cost will gradually decrease as the Legislature scales until it reaches the willingness-to-pay of trust-minimized stakers, akin to a Dutch auction for trust-minimized votes.
- A **Trusted Stake** increases social costs through a series of gamified quests that stakeholders must complete, or through the requirement of being trusted and vouched for by a Champion, which in turn enables us to allow a monetarily cheaper stake.

To maximize representation, there should be no constraints or biases that make it easier for any one stakeholder category to be heard by the system (e.g. to vote). In pursuit of this, we make access to voting rights permissive. Obtaining a vote does not require majority approval from existing voters; if you abide by the stakeholder validation criteria, Aragon Court will ultimately enforce your right to vote. This means we know that anyone not participating in the Legislature can be viewed as an abstention (indifferent), meaning that ultimately decisions will reflect an unbiased aggregation of stakeholder preferences.

Finally, the amendability of the Constitution provides another route to "dynamic legitimization" of inputs, reinforcing political legitimacy by giving those who do not wholly consent to the Constitution the power to amend it.

> "If those currently governed by a given constitution can change it, provided the need to do so is sufficiently agreed upon, then they are more likely to view the constitution as reflecting their needs and goals surrounding governance."
> (Alston, 2019)

Conservation of Throughputs



Throughputs are conserved by the Judiciary, who serves as a neutral third-party that upholds the laws of the Constitution, thereby ensuring rational-legal legitimacy.

If rules (such as those in a constitution) are not adhered to, de facto authority will be claimed by the entities who have the bargaining power as determined by endogenous governance (consensus mechanisms in blockchains). We see this with the EOS constitutions, of which there are multiple unenforced versions and de facto authority has emerged according to the Delegated Proof of Stake (DPoS) consensus mechanism (Berg & Berg, 2018). Using Aragon Court, we ensure that all actions within the Council are subject to peer-to-peer enforcement and will ultimately be held accountable against the Constitution.

To ensure that the Constitution itself is not compromised, we allow de facto interpretations of the Constitution's values (Principles) to overturn amendments that technically follow the rules (Statutes), as well as defining immutable or quasi-immutable clauses that are impossible or harder to change. This in turn upholds substantive legitimacy by empowering the Judiciary to enforce the DAO's shared values.

The Constitution in combination with Aragon Court enables us to design more permissive governance, which ultimately protects minority stakeholders and empowers them to correct corrupted throughputs (Duncan, 2018):

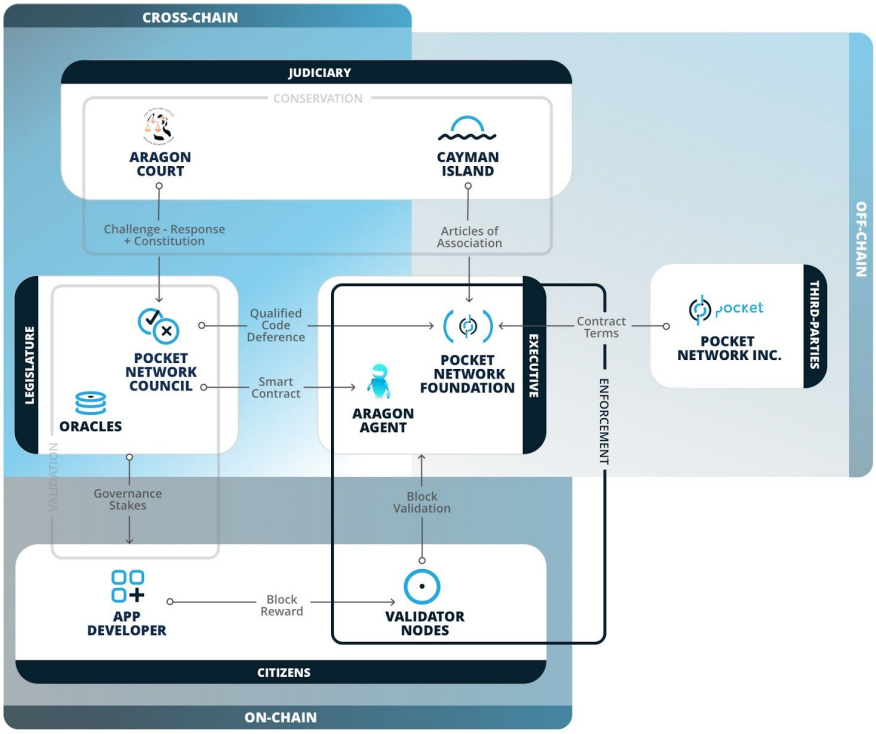
- Minority stakeholders do not require an approval vote to be accepted into the Council. They can mint themselves a voting token and any challenges on the action will be adjudicated by Aragon Court.
- Even if bad actors manage to infiltrate a majority of the Council, minority stakeholders can block all of their actions and burn their voting tokens according to the same permissive process by which voting tokens are minted, adjudicated by Aragon Court.

If you lose your voting token, you lose your Governance Stake. This means that although exit from the DAO is permissionless in normal circumstances, any of your peers can change this by burning your token before you do.

Finally, total transparency is upheld in all three modules of the Lean Trias Politica, democratizing the conservation effort:

- While off-chain, both the Legislature and Judiciary (Aragon Court) operate on external blockchains, meaning all actions will be time-stamped and verifiable,
- While not operating on a blockchain, the Foundation's articles compel directors to publicize all information concerning resignations of Directors/Supervisors and appointment/removal of Alternate Directors and/or Secretaries.

Enforcement of Outputs



The leanest way to do arbitrary on-chain execution is to parameterize as many decisions as possible, allow these parameters to be changed by submitting transactions to the blockchain, then define the permissions to control these parameters using an Access Control List (ACL). This functionality can be applied to protocol upgrades by defining a parameter to activate protocol upgrades and using full node software (Pocket Runner) that will automatically update nodes when the "activate" transaction is confirmed. The result of these measures is a tighter coupling of off-chain coordination with on-chain finalization; executing decisions becomes a simple transaction, which minimizes the coordination effort of full nodes. In other words, we transform complex coordination into a simple decision function (Buterin, 2017).

The first permission holder in the ACL will be the Foundation. As described above, the Foundation is legally compelled to execute the Council's decisions, unless doing so would violate their duty to steward Pocket Network. This serves as a decentralized baseline for enforcement of outputs. Whereas legal entities such as Decred Holdings Group LLC (DHG) are legal custodians of treasury funds (Wharton Cryptogovernance Workshop), the Foundation's control of the treasury is deferred to the Council. They cannot make financial transfers that were not first approved by the Council (either directly or through allowances written into the Constitution) and their control of the on-chain treasury account is determined by the ACL,

which can be modified at any time by a protocol upgrade. In fact, the Foundation will have their own separate multi-sig account for their own discretionary spending and will have to submit funding proposals to the Council like any other entity.

The ACL is completely upgradeable, which means achieving automatic enforcement of outputs, à la "on-chain governance", is simply a matter of swapping the Foundation account for an automated agent (e.g. Aragon Agent). More on this in 'Autonomy' below.

The last step of execution is confirmation by validator nodes. As the actors responsible for transaction finalization, in a system where all governance outputs are represented by transactions, validator nodes possess the "right to bear arms" against the entire government apparatus. In this sense, validator nodes are the representatives of the general citizenry of Pocket Network, trusted as such due to Pocket Network's unique block reward, which directly aligns node incentives with the users (developers) on the other side of the market. This is Pocket Network's on-chain "endogenous governance", which ensures that the bargaining power is in favor of the users; contrast this with most other blockchains, where node incentives are misaligned with users (Proof of Work) or incentivize politicking (DPoS) (Berg, Berg & Novak, 2018).

Compliance

Due to its non-profit purpose, Pocket Network's DAO does not face the same legal risks that many other DAOs do. If we did not use a legal wrapper, the DAO's legal status would default to being a not-for-profit unincorporated association, which in many jurisdictions confers the same limited liability benefits that corporations do (Shapiro, 2020).

However, relying on this would limit the flexibility of the DAO to evolve its purpose, because it would limit the jurisdictions that the DAO can operate in (jurisdictions with the above interpretation) and any sign of profit would turn the DAO into a general partnership with unlimited liability for all members.

As described above, we're using Qualified Code Deference to hold the Foundation fully accountable to the Council. They must execute all of the Council's decisions except in the case of "Material Adverse Exception Events" (i.e. failures resulting from incomplete contracts). In practice, this means the Foundation has a veto on decisions that would violate their duty to steward Pocket Network and the power to coordinate on fixing/replacing modules of the government apparatus.

This also results in the Foundation serving as a legal wrapper for the DAO, shielding the DAO from external liability. The Foundation will be the DAO's representative in all relationships involving parties who have not signed the Constitution, including service agreements with

third-parties and modifications to Pocket Network that could be viewed to incur tort (e.g. protocol upgrades that cause bugs). They will continue to hold this representative role even in the final autonomous state described in 'Autonomy' below.

In the other direction, the Constitution shields the DAO from internal liability, by serving as an internal arbitration agreement that limits liability between the stakeholders who sign it. Anyone who signs the Constitution in the process of joining the Council waives their right to sue the DAO in any courts other than Aragon Court (though this does not stop them from suing the Foundation for violation of its responsibility to the DAO).

Upgradeability

The Constitution is the foundation of Pocket Network's governance. Upgrading governance, as a coordination problem, is therefore as simple as approving amendments to the Constitution. Once such an amendment has been approved, the relevant parties (Foundation, PNI) will be compelled to execute the upgrade due to the system of checks and balances we have delineated above.

Upgrading modules is as simple as voting to approve the upgrade, configuring the upgrade, then re-staking Governance Stakes (in the case of upgrading the Legislature) or modifying the ACL (in the case of upgrading the Executive).

Autonomy

Complete autonomy (i.e. automation) is not necessary for throughput legitimacy, but is still desirable for its “unstoppable” (non-coercible) character.

Due to its modularity, this governance system can eventually automate itself. Transforming its coordination problems into simple decision functions is simply a matter of automating the bridges between governance modules. For example, oracles could be used for automatic validation of inputs (e.g. by querying Pocket Network for a prospective voter's stakeholder status), bots powered by AI/NLP could be used for automatic conservation of throughputs (e.g. by automatically flagging proposals that break formatting rules), and smart contracts could be used for automatic enforcement of outputs (e.g. Aragon Agent).