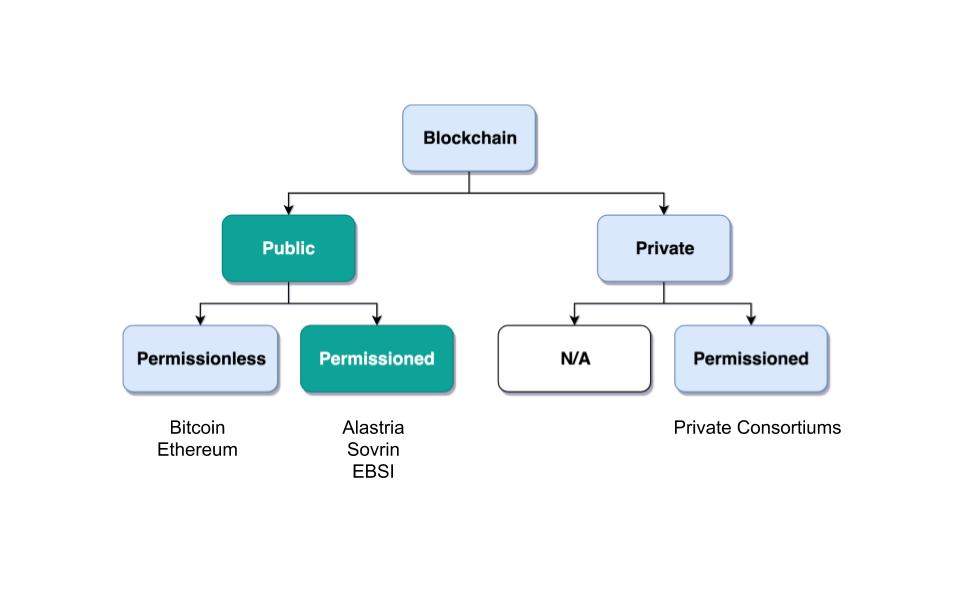
Public-Permissioned Blockchain Networks

Jesus Ruiz [hesus.ruiz@gmail.com](mailto:hesus.ruiz@gmail.com)

14-08-2019

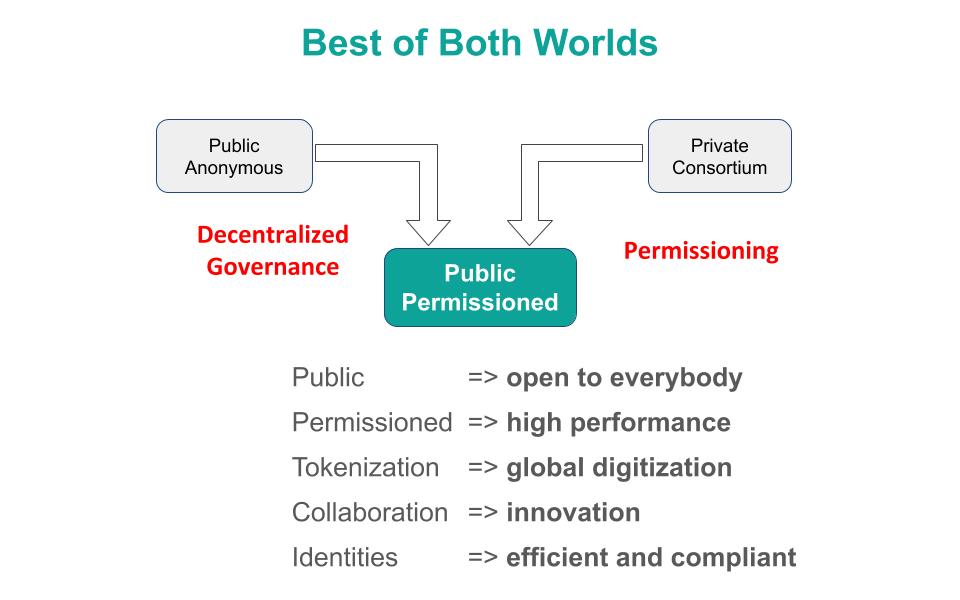
(Version: 0.2, Version Date: 14-08-2019)

Until now the words **Public** and **Permissioned** have been used as opposites, where **Permissioned** is seen as synonymous with **Private**. However, as the following sections describe, a new kind of blockchain network is emerging, being pioneered by [Alastria](https://alastria.io/). Such a network brings a lot of value to the digitization of the productive economy of a country, complementing (but not replacing) the other types of networks, namely Public-Permissionless (like Bitcoin or Ethereum) and Private-Permissioned (aka Private Consortiums).



Blockchain taxonomy

A Public-Permissioned blockchain network tries to combine the permissioning feature from private consortiums with a decentralized governance model in order to obtain the best characteristics of both worlds, which is required for the implementation of many important use cases that can not fit any of the currently existing networks.



Best of both worlds

The **permissioning** property from Consortiums brings the following benefits:

* **technical** (eg. performance, scalability),
* **compliance** (eg. easier to comply with GDPR or AML regulation),
* **operational** (easier to manage and implement crisis management),
* **economical** (the infrastructure does not need for its operation an embedded cryptocurrency subject to speculation).

On the other hand, the word **public** has in this context a different meaning than the one used normally when talking about blockchain networks. A Public-Permissioned network is public in much the same way as most essential public services like *public health*, *public education* or *public roads*. If we use the analogy of those public services, we can see that:

* those public services are **permissioned**, in the sense that citizens have to identify themselves in order to access the services.
* there are **no artificial barriers** in order to access those services, but there are rules that have to be complied with. Those rules have to be transparent, fair and reasonable. This is most clear with the driver’s license, which everybody must have in order to be able to drive a car in the public roads.
* **privacy and anonymous access** are not the same, and in most cases we require both permissioning and high levels of privacy, as can be seen with the public health services.
* in some cases, the public good requires a **trade-off between privacy and permissioning**, as is the case with the license plates that cars have to exhibit ostensibly in order to be able to use the public roads.

There are public goods that do not require permissioning in order to use them, but when those goods are scarce and subject to depletion if abused, then permissioning is required in order to ensure inclusion, fair access and usage, and sustainability of the resource.

It can be argued that requiring the network to be permissioned reduces **decentralization** and increases the level of trust required by participants in the network. Indeed, in theory Public-Permissionless networks are more decentralized than Public-Permissioned ones, but in practice Public-Permissionless networks are more centralized than what they are normally assumed to be.

In addition, the scenario of anonymous transactions among anonymous actors does not reflect exactly what happens in most transactions in a modern economy, especially if the transactions involve a business and/or a physical item. For example, when a consumer buys a washing machine with the installation service included, or when a company imports components manufactured by another company in another country.

As we will see later, we think that a reasonable degree of decentralization can be achieved in Public-Permissioned networks, making them a powerful instrument for the digitization of the productive economy of a country, because the permissioning and privacy characteristics of those networks are compatible with the equivalent required properties of the economic transactions that are being implemented.

# The Governance Model

If a blockchain network is permissioned, in order to merit the name of Public-Permissioned a special Governance Model is required to ensure inclusion, fair access and sustainable usage of the network, and to avoid its control by a single entity or a cartel of entities. More concretely, this blockchain network could be considered as a new type of infrastructure implementing the following principles [[Navarro2018]](#Navarro2018):

1. **Non-discriminatory and open access:** Access is non-discriminatory, even if it is not free because pricing is determined using transparent mechanisms, typically cost-oriented. Access is open because everybody has the right to join and use the infrastructure according to the access rules.
2. **Open participation:** Everybody has the right to join the community to participate in the construction, operation, provision and governance of the infrastructure. The network should be inclusive, open to participation of any entity independent of size or sector of activity.

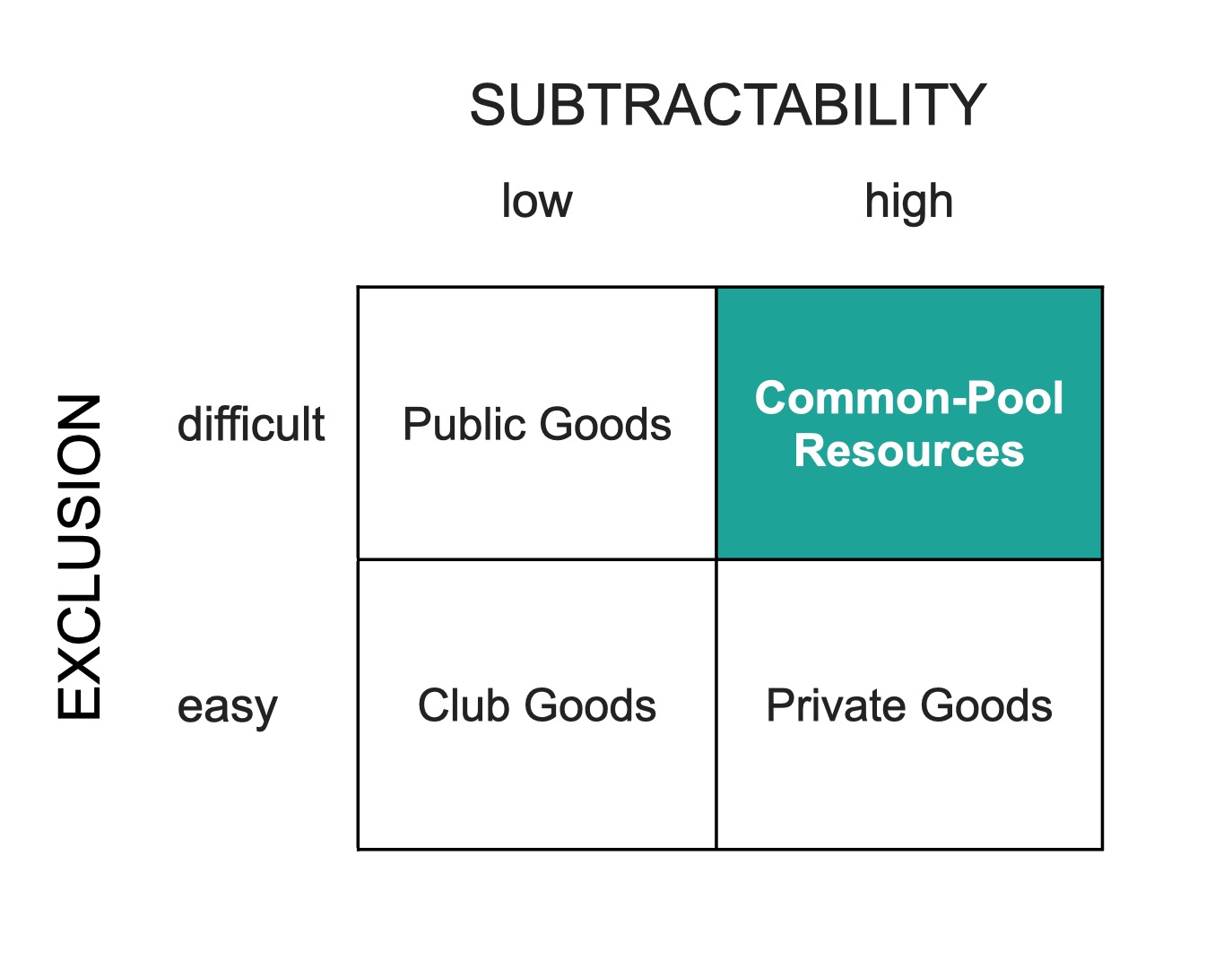
Such a governance model is critical in providing the required level of trust, or confidence, in the network from all participants. Running a network that is at the same time permissioned, public (in the sense of inclusive) and sustainable, presents many challenges that have to be addressed explicitly and are specific to this type of network and that do not appear in either Public-Permissionless or Consortium networks.

## The blockchain as a Common-Pool Resource (CPR)

As exemplified in the *Blockchain trilemma* [[Buterin2014]](#Buterin2014), blockchain networks can be considered as a technical resource that can not be scaled easily. If we consider for example the throughput (number of transactions per unit of time that the network can process globally for all users), we can see that with a given blockchain technology this resource does not scale easily. This is in contrast with other infrastructures like the Internet connectivity, where the bandwidth can be scaled by adding communication lines in parallel. Or in traditional applications, adding more machines or bigger ones can scale the number of transactions per second.

In this sense, a Public-Permissioned blockchain network can be considered as a communal resource similar to the ones described by Elinor Ostrom, Nobel Prize in Economics 2009 [[Ostrom1990]](#Ostrom1990). Ostrom’s studies focussed on how communities can manage to successfully govern communal resources, contrary to what is described in Hardin’s influential article on *The tragedy of the commons* [[Hardin1968]](#Hardin1968).

This governance model is different from the two standard ways of managing private goods or public goods, and is the most efficient for goods that have the property of subtractability, like private goods, but they share the difficulty of exclusion with public goods. This concept is represented in the next figure.



Common-Pool Resources

## On-chain Governance complementing Off-chain Governance

A unique property of a blockchain network with respect to all other Common-Pool Resources (natural resources or classical technical infrastructures) is the ability to encode some governance rules using the programmable nature of the blockchain, making the enforcement of the rules not only transparent but also automatic and immutable. This is what we call ``**on-chain governance**''. The literature has a small number of documents describing governance models and their automated implementation based on the blockchain (eg. [[DavidsonEtAl2016a]](#DavidsonEtAl2016a)), but in general they are at the application (dApp) level, and they assume the existence of a blockchain network with the appropriate characteristics [[RozasEtAl2018]](#RozasEtAl2018). We are instead interested on the governance model required for the management and operation of a blockchain network infrastructure which is Public-Permissioned as described above. That is, on *governance* ***of*** *the blockchain* instead of *governance* ***by*** *the blockchain*. And specifically on the on-chain governance of the blockchain network infrastructure, in contrast to the off-chain governance processes.

## The eight principles for managing a Commons

Ostrom [[Ostrom1990]](#Ostrom1990) defines eight principles for efficiently managing Common-Pool Resources:

|  |  |  |
| --- | --- | --- |
|  | Principle | Description |
| **1.a** | **User boundaries** | Clear boundaries between legitimate users and nonusers must be clearly defined. |
| **1.b** | **Resource boundaries** | Clear boundaries are present that define a resource system and separate it from the larger biophysical environment. |
| **2.a** | **Congruence with local conditions** | Appropriation and provision rules are congruent with local social and environmental conditions. |
| **2.b** | **Appropriation and provision** | The benefits obtained by users from a common-pool resource (CPR), as determined by appropriation rules, are proportional to the amount of inputs required in the form of labor, material, or money, as determined by provision rules. |
| **3** | **Collective-choice arrangements** | Most individuals affected by the operational rules can participate in modifying the operational rules. |
| **4.a** | **Monitoring users** | Monitors who are accountable to the users monitor the appropriation and provision levels of the users. |
| **4.b** | **Monitoring the resource** | Monitors who are accountable to the users monitor the condition of the resource. |
| **5** | **Graduated sanctions** | Appropriators who violate operational rules are likely to be assessed graduated sanctions (depending on the seriousness and the context of the offense) by other appropriators, by officials accountable to the appropriators, or by both. |
| **6** | **Conflict-resolution mechanisms** | Appropriators and their officials have rapid access to low-cost local arenas to resolve conflicts among appropriators or between appropriators and officials. |
| **7** | **Minimal recognition of rights to organize** | The rights of appropriators to devise their own institutions are not challenged by external governmental authorities. |
| **8** | **Nested enterprises** | Appropriation, provision, monitoring, enforcement, conflict resolution, and governance activities are organized in multiple layers of nested enterprises. |

## On-chain governance and the CPR principles

When we see the applicability of Ostrom’s CPR managing principles to a Public-Permissioned blockchain network, we see that there is a potential to automate the execution and enforcement of some of the principles in a way that would be impossible for any other type of CPR. A summary can be found in the following table.

|  |  |  |
| --- | --- | --- |
|  | Principle | Description |
| **1.a** | **User boundaries** | Self-Sovereign Identities (associated to legal identities) both for natural and juridical persons. |
| **1.b** | **Resource boundaries** | Decentralized permissioning of nodes via Smart Contracts connected to Trusted Third Parties (TTPs) and other official Registries and Regulatory bodies in the country (eg. the Spanish Business Registry for normal businesses, or the Ministry of Education for Universities). |
| **4.a** | **Monitoring users** | Using Gas to control resource usage by accounts (self-monitoring).Need transaction origin traceability (enode that injected tx) |
| **4.b** | **Monitoring the resource** | Monitor the Consensus execution (eg. report detectable Crash and Byzantine behavior) in a transparent way |
| **5** | **Graduated sanctions** | Automated proactive and reactive management of the Consensus set via Smart Contracts complemented with off-chain sanctioning. |
| **6** | **Conflict-resolution mechanisms** | At the lowest level of the operation of the network, the same mechanisms used for monitoring and graduated sanctions are used for automated arbitration of conflicts arising among members (eg. non-compliance to the Service Level Objectives defined in the operational policies of the network). |

# The Consensus algorithm and On-chain Governance

The consensus algorithm is one of the most important components of a blockchain network, affecting many aspects of the system like scalability, sustainability and even to the governance of the technical platform. In addition, governance of the consensus set is critical to the level of trust that this network has for the rest of the participants (the so-called *regular nodes*).

The current Alastria network, *Red T*, uses *Istanbul Byzantine Fault Tolerance* (IBFT) as consensus algorithm, which belongs to a family of PBFT consensus algorithms sharing many of the properties heavily discussed and formally proven during the last decades, and its properties are very well known ([[CastroLiskov1999]](#CastroLiskov1999), [[CastroLiskov2002]](#CastroLiskov2002)).

When applied to the blockchain, the PBFT variants comply with the **Robustness property** [[Saltini2019]](#Saltini2019) when the maximum number of Byzantine validator nodes **t** follows the well-known relationship with **n**, the total number of validator nodes:

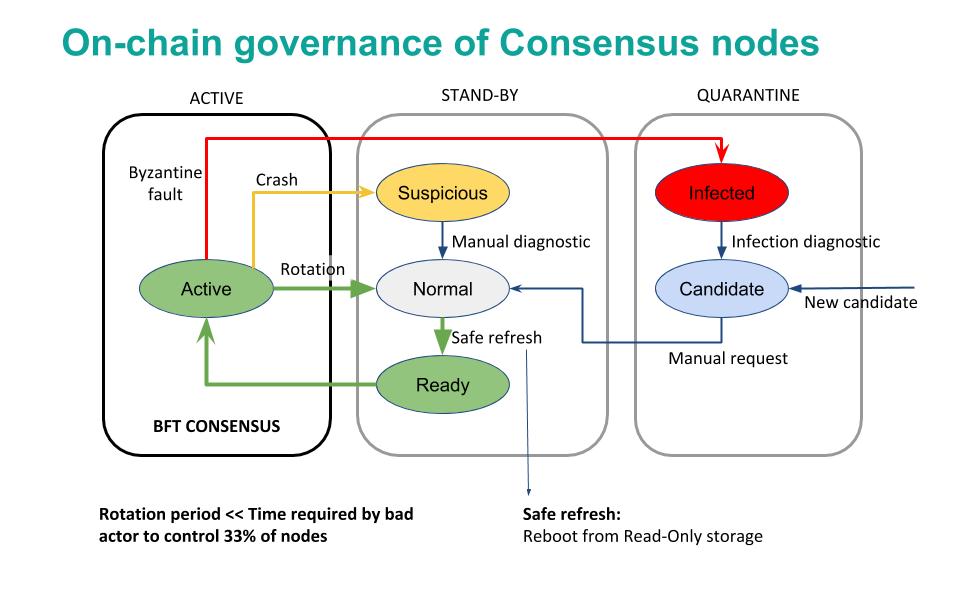
**n = 3t + 1**.

However, standard implementations of PBFT and in particular IBFT, tend to focus on masking failures. That is, they make failures transparent to the users, but they do not manage those failures in a way that proactive or reactive measures can be taken to ensure the long-term health of the network.

This is the reason why Alastria is implementing a set of tools surrounding the base IBFT consensus algorithm, which together with complementary off-chain governance processes allow the realization of the the principles of the governance of the blockchain as a Common-Pool Resource.

## An example of on-chain governance of the Consensus set

The subject is too complex to be thoroughly treated in a reduced space, but the following figure describes a summary of an example of on-chain governance of the blockchain network.



On-chain governance of consensus nodes

The following aspects can be observed:

* The consensus nodes in the Active state (that is, executing the base IBFT algorithm) are being monitored, as per principle 4.b of the CPR governance principles
* The events signaling different types of faults are used for the reactive governance of the nodes. Even though it is not shown in the figure, in addition to the automated reaction, the events are reported in a way that any participant in the blockchain network (not just the consensus nodes). This is required to implement the high levels of transparency and collaborative monitoring that are required for the effective management of CPR resources.
* Depending on the severity of the fault detected (crash or byzantine), the system reacts automatically applying a graduated set of sanctions, as per the principle 5 of CPR governance. For example, when the fault is byzantine, the consensus node affected is put in quarantine, effectively stopping the node from participating in the consensus execution. If the owner is willing to continue participating, a manual process (off-chain governance) is required, with sufficient explanation and justification to the other members in order to be accepted again.

# References

Vitalik Buterin. "On sharding blockchains" (2014). Ethereum Wiki.

Miguel Castro and Barbara Liskov. "Practical Byzantine Fault tolerance" (1999). Proceedings of the Third Symposium on Operating Systems Design and Implementation, New Orleans, USA, February 1999. DOI: 10.1.1.17.7523.

Miguel Castro and Barbara Liskov. "Practical Byzantine Fault Tolerance and Proactive Recovery" (2002).

Sinclair Davidson and Primavera De Filippi and Jason Potts. "Economics of Blockchain" (2016). Public Choice Conference. DOI: 10.2139/ssrn.2744751.

Garrett Hardin. "The Tragedy of the Commons" (1968). Science, New Series.

Leandro Navarro. "Network infrastructures: The commons model for local participation, governance and sustainability" (2018). APC Issue Paper.

Elinor Ostrom. "Governing the Commons: The Evolution of Institutions for Collective Action" (1990).

David Rozas and Antonio Tenorio-Fornés and Silvia Díaz-Molina and Samer Hassan. "When Ostrom Meets Blockchain: Exploring the Potentials of Blockchain for Commons Governance" (2018).

Roberto Saltini. "Correctness Analysis of IBFT" (2019). arXiv:1901.07160 [cs].