4.2.2 Access Control

Return to Functional Requirements

A major functional requirement is to provide a classifications of allowable nodes within the DIDO network. A detailed explanation of DIDO networks is provided by in Network Access Control.

Within each of these two classifications it is possible to have public and private access. Public and private access define who is able to write data onto a network or ledger. In contrast, open (i.e., permissionless) and closed (i.e., permissioned) determine who is able to read the data. Networks are classified as[1]:

- Permissionless Networks and Public Network - public and open
- Permissionless Networks and Private Network - public and closed
- Permissioned Networks and Public Network - private and open
- Permissioned Networks and Private Network - private and closed

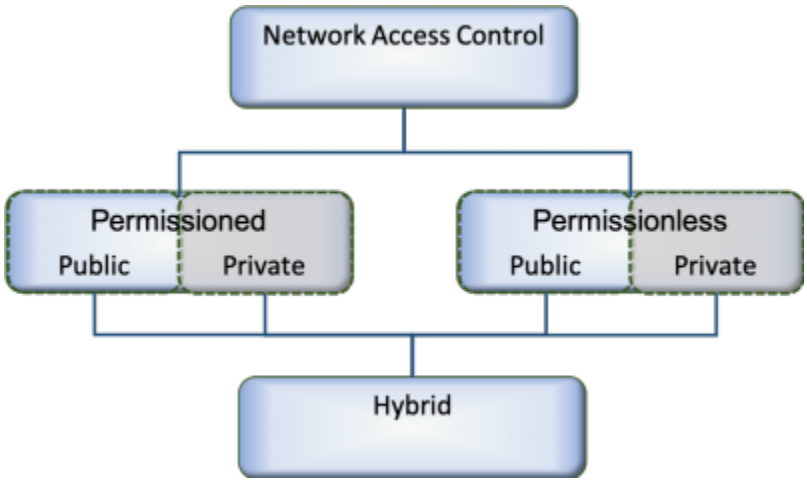


Figure 1: The Node Network Access Taxonomy

Determine the Access Control required for this DIDO by completing the worksheet presented in Table 1. Determine the characteristic required for the particular project of intrest. For example, for the Decentralization the answer should be either Permissioned or Permisionless. When the worksheet is done, use the answers to make the appropriate requirement of Permissionless versus Permissioned, public versus private, or if the requirements are a hybrid. Defining these requirements early can help avoid costly and time consuming changes later.

Table 1: Network Access Worksheet

Characteristic	Characteristic	Description
Decentralization		• **Permissionless** - Permissionless networks are decentralized and distributed. In other words, no one entity can close or terminate the network, modify the content, or censor parts of it. The larger the distributed and decentralized networks and or history are, the harder it is to tamper with.[2)] • **Permissioned** - The degree of decentralization for permissioned networks is a business decision. The extent and quality of decentralization depends upon the number of peers (i.e., nodes), the expected number of bad nodes in the network, and the type of consensus mechanism determined by the stakeholder. Permissioned blockchains usually employ an algorithm such as Byzantine Fault Tolerance (BFT), which differs from the proof of work (PoW) algorithm[3)].
Transparency		• **Permisionless** - Users or nodes have complete access to the ledger, transactions, and blocks in the blockchains, which allows for complete auditing of permissionless networks[4)]. • **Permissioned** - Transparency is not a driving force in permissioned networks and is often a major factor in the business decision to choose permissioned over permissionless networks. Most permissioned blockchains do not use cryptoeconomic coins incentive or tokens. The primary incentive of permissioned blockchain participants is to minimize the transparency, cost, time, and ease of sharing information3).
Privacy/Anonymity		• **Permisionless** - Privacy - In permissionless networks, users or nodes of the network are anonymized. Technically, permissionless networks like Bitcoin are pseudonymous, and not truly anonymous.[5)] • **Permissioned** - Anonymity - Permissioned blockchains offer fine-grained visibility into transaction details, as well as, metadata about those transactions which, in many ways, compromises the privacy of the Network participants[6)].

Characteristic	Characteristic	Description
Governance		• **Permisionless** - As a general rule, permissionless networks rely on open source software, which is ruled by open source communities (see todo). The governance of the network is by consensus. Consensus is different for many of the permissionless networksm(i.e., Proof of Work (PoW), Proof of Stake (PoS), Proof of Authority (PoA), etc). [7] • **Permissioned** - There are fundamental differences between permissionless and permissioned network governance. Permissioned governance is decided and agreed upon by members of the business network. Economic incentives, code quality, code changes, and power allocation among peers are based on the business dynamics and the common purpose and goals of the permissioned members. This allows for agile and responsive networks desired by businesses[8].
Tokens		• **Permisionless** - Permissionless blockchains employ fat protocols that compensate network contributors with Tokens. As the value and utility of the network increases, the value of the underlying tokens increases as well. This is the premise of cryptoeconomics and Initial Coin Offering (ICO) based fundraising. There are two predominant types of tokens today: monetary value tokens and utility tokens. Monetary value tokens are used in myriad ways as instruments for exchanging value. Utility tokens are akin to loyalty points: they have intrinsic value but no monetary value outside of that ecosystem.[9] • **Permissioned** - Permissioned blockchains generally do not employ a cryptoeconomic coins incentive or tokens[10].
Scalability & Performance		• **Permisionless** - For all the value blockchains bring to modern business processes, their Achilles heel often involves scalability and performance. Both Bitcoin and Ethereum blockchains suffer from poor scores in this area. For example, a recent blockchain game called Crypto kittles clogged the Ethereum network. Having said that, these are just early teething troubles, and startups are experimenting with various strategies to address this issue. Hopefully it is only a matter of time before this issue becomes a non-entity.[11] • **Permissioned** - Permissioned blockchains use consensus mechanisms, which are computationally inexpensive (when compared to proof of work (PoW)). Therefore, they enjoy substantially better scalability and performance than their permissionless network cousins[12].

Characteristic	Characteristic	Description
Open Read and Write		• **Public** - Anyone can participate by submitting transactions to the blockchain, such as Ethereum or Bitcoin; transactions can be viewed on the blockchain explorer.[13)]
Ledger Is Distributed		• **Public** - The database is not centralized like in a client-server approach, and all nodes in the blockchain participate in the transaction validation.[14)]
Immutable		• **Public** - When something is written to the blockchain, it can not be changed, in other words it is immutable.[15)]
Secure Due to Mining		• **Public** - For example, with Bitcoin, obtaining a majority of network power could potentially enable massive double spending, and the ability to prevent transaction confirmations, in addition to other potentially malicious acts.[16)]
Enterprise Permissioned		• **Private** - The enterprise controls the resources and access to the blockchain, hence private and/or permissioned.[17)]
Faster Transactions		• **Private** - When you distribute the nodes locally, but also have far fewer nodes that participate in the ledger, performance is faster.[18)]
Better Scalability		• **Private** - Being able to add nodes and services on demand can provide a great advantage to the enterprise.[19)]
Compliance Support		• **Private** - As an enterprise, you would likely have compliance requirements to adhere to; having control of your infrastructure enhances ability to satisfy this requirement more seamlessly.[20)]
Consensus More Efficient		• **Private** - Enterprise or private blockchains have fewer nodes and usually a different consensus algorithm, such as BFT vs PoW.[21)]
Private Transactions		• **Hybrid** - Transaction are private but verifiable using the ledger's immutable data objects (i.e., leverage its public state). In its public state, each transaction gets approved by a massive network and is essentially secure and trustworthy. Hence, there is no need for a central governing body or an exhaustive chain of intermediaries to supervise things. So, any change done to a transaction will undergo a “kindred” approval process, making it next to impossible for a single actor to meddle with the transaction or entries[22)].

Characteristic	Characteristic	Description
Equality		• **Hybrid** - Everyone in the network has equal rights to view, modify, and append their consent to a transaction. In addition, the identity of transacting parties is never disclosed to all the visible network participants. [23].
Non-Repuddiation		• **Hybrid** - Anonymity is simply not acceptable to financial institutions and regulated industries with their strict Know Your Customer (KYC) standards. [24].
Confidentiality		• **Hybrid** - Unrestricted visibility of the public state of the network exposes all the data to a colossal network breach, which is counter to data confidentiality obligations, as well as their business concerns.[25].

- **Note:** Another category of networks is a hybrid network, which makes it possible to restrict the visibility of information on the network using a combination of

public, private, permissionless and permissioned networks. Therefore, hybrid networks are appealing to regulated markets because they offer the benefits of public blockchain and private blockchain together.[26]

1) , 14) , 15) , 16) , 17) , 18) , 19) , 20) , 21)
"Public Vs Private Blockchain In A Nutshell", Demiro Massessi, 12 December 2018, https://medium.com/coinmonks/public-vs-private-blockchain-in-a-nutshell-c9fe284fa39f

2) , 3) , 4) , 5) , 6) , 7) , 8) , 9) , 10) , 11) , 12)
"Nuances Between Permissionless and Permissioned Blockchains", Anant Kadiyala, 18 February 2018, https://medium.com/@akadiyala/nuances-between-permissionless-and-permissioned-blockchains-f5b566f5d483

13)
"Public Vs Private blkchn In A Nutshell", Demiro Massessi, 12 December 2018, https://medium.com/coinmonks/public-vs-private-blockchain-in-a-nutshell-c9fe284fa39f

22)
"If you Thought Blockchain was Amazing, Wait till You Read about Hybrid Blockchain", Atul Khekade, 20 January 2018, https://www.entrepreneur.com/article/307794. This article uses the term "agnate approval" rather than "kindred approval"; however, agnate limits a kindred relationship to males only. Thus, we prefer the term "kindred" over "agnate"

23) , 24) , 25)
"If you Thought Blockchain was Amazing, Wait till You Read about Hybrid Blockchain", Atul Khekade, 20 January 2018, https://www.entrepreneur.com/article/307794

26)
"Hybrid Blockchain: Decentralized Option for Highly Regulated Markets - Few players in highly regulated markets have adopted blockchain technology. However, hybrid blockchain will change this.", Mina Down, 14 November 2018 https://blog.goodaudience.com/hybrid-blockchain-decentralize-highly-regulated-markets-900f30a37903

From:
https://www.omgwiki.org/dido/ - **DIDO Wiki**

Permanent link:
https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:1.4_req:1_func:access&rev=1627581189

Last update: **2021/07/29 13:53**