

# Governance in decentralized networks

Risto Karjalainen\*  
May 21, 2020

**Abstract.** Effective, legitimate and transparent governance is paramount for the long-term viability of decentralized networks. If the aim is to design such a governance model, it is useful to be aware of the history of decision making paradigms and the relevant previous research. Towards such ends, this paper is a survey of different governance models, the thinking behind such models, and new tools and structures which are made possible by decentralized blockchain technology. Governance mechanisms in the wider civil society are reviewed, including structures and processes in private and non-profit governance, open-source development, and self-managed organisations. The alternative ways to aggregate preferences, resolve conflicts, and manage resources in the decentralized space are explored, including the possibility of encoding governance rules as automatically executed computer programs where humans or other entities interact via a protocol.

**Keywords:** Blockchain technology, decentralization, decentralized autonomous organizations, distributed ledger technology, governance, peer-to-peer networks, smart contracts.

## 1. Introduction

This paper is a survey of governance models in decentralized networks, and specifically in networks which make use of blockchain technology.

There are good reasons why governance in decentralized networks is a topic of considerable interest at present. Some of these reasons are ideological. We live in an era where detailed information about private individuals is being collected and traded, in many cases without the knowledge or consent of the individuals involved. Decentralized technology is seen as a tool which can help protect people against invasions of privacy.

Decentralization can also be viewed as a reaction against the overreach by state and industry. Blockchain technology can be viewed as a means to take back control, and as a contribution to greater fairness and democracy. The interest in governance, then, rises from the desire to make sure that decentralized networks are in fact governed by the community.

For developers of decentralized networks, the lack of clearly defined decision processes will cause practical challenges. Protocol updates and technical improvements can be unnecessarily delayed if there is no well-functioning governance model in place. Disagreement among stakeholders may ultimately necessitate a protocol fork and a community split.

Some stakeholders have a financial interest. There are many early adopters with skin in the game as owners of digital tokens. For token owners, issues such as blockchain security and *bona fide* usage of project funds are of legitimate concern. The value of many a network is not in the code, but rather in the community and the ecosystem. Good governance is like a glue which binds the community into a cohesive whole and thus makes the tokens valuable.

But what do we actually mean by governance? By one definition (Bell, 2002), it is the use of institutions, structures of authority and collaboration to allocate resources and coordinate the effort and activity in society or in the economy. We look at governance as applied to the design and maintenance of network protocols. For the purposes of this paper, a consensus mechanism inherent in blockchain transactions is not governance<sup>1</sup>. And whilst community involvement in the form of ideas, comments, bug reports and contributed code can be highly valuable, it only counts as governance if there are mechanisms in place for the community to exercise genuine power. In the terminology of de Philippi and McMullen (2018), we focus on governance *of* the infrastructure, and purposely ignore governance *by* the infrastructure. We will also stay away from the question of whether decentralized governance could be used to augment or replace traditional political institutions (Atzori, 2017).

---

<sup>1</sup> However, the question of how a consensus mechanism is agreed upon is a perfectly valid issue for governance.

\*Comments and suggestions for the first version (March 5, 2020) by Franklin Allen, Matthew Fontana, John Hargrave, Petri Honkanen, Matt Innes, Ilkka Lähteenmäki, Shiv Malik, Michael Malka, Nikke Nylund, Henri Pihkala and Jarmo Suoranta are gratefully acknowledged. All remaining errors and omissions are my responsibility.

As decentralization is one of the key issues here, it will be useful to clarify what it means. In a decentralized system<sup>2</sup>, lower-level components (acting on local information) interact to achieve global goals. If the system exhibits complex system-wide behaviour, that behaviour emerges in a self-organised way without global control. There is no central authority.

Market economy (in its pure form) is an example of a decentralized system. There is no controlling authority to impose production quotas, manage the supply chain, schedule deliveries and so on. Many real-life biological systems<sup>3</sup> are decentralized and self-organising, and they can be made of large numbers of autonomous members working for the common good without a ruler or bureaucracy.

It may also be instructive to consider the opposite. In a centralized<sup>4</sup> system, there is a single entity which controls — either directly or indirectly — all lower-level components in order to achieve global goals. Access to information is controlled by one authority, and information typically passes via a single hub. Any complex behaviour exhibited by the system results from central control, direction and supervision.

A case can be made that centralized governance originates in our evolutionary history. *Dominance hierarchies* are commonly observed in many social species of mammals, fish, birds, and even insects. If group members compete for scarce resources or for a chance to mate, fighting for dominance at each encounter is wasteful. Everyone in the group may be better off if a relative ranking is maintained, and such a ranking controls the priority of foraging or access to reproduction opportunities. The resulting pecking order (as it was originally called in domesticated hens) is often hereditary.

Primatology research (see e.g. de Waal, 1982) has uncovered complicated and largely hierarchical social structures among our close relatives, including baboons, chimpanzees and gorillas. We should be careful, though, to naively apply research findings outside their original context. For instance, the concept of the alpha male (in human society) has been largely debunked (Singal, 2016). In many hunter-gatherer societies, there is evidence that points on egalitarian rather than hierarchical structures (Boehm, 1993). And even chimpanzees are capable of cooperation (Suchak et al., 2016).

The fact still remains that many ancient (and even not so ancient) societies were centralized and hierarchical. It may be the case that tribal chieftains were stronger, more brutal, or more cunning than their fellow human beings, and fought their way successfully to the top. And perhaps most people were (and still are) happy for someone else to take charge and make decisions, as long as those decisions serve the other members of the group sufficiently well.

Many human societies and institutions are centrally controlled. Centralization of authority can be traced back to the ancient times, where the Akkadian Empire in Persia, Babylonia, and the Qin dynasty of Imperial China stand out as prominent examples. The common theme in these (and other more or less contemporaneous) systems was highly concentrated political power, with the government administered by a hierarchy of trusted officials in service of the emperor or the king. If we fast forward to modern times, the now defunct Soviet Union is an ultimately unsuccessful instance of a centrally controlled political and economic structure.

Decentralized networks are a subset of decentralized systems. They are composed of interconnected computational nodes which share resources or communicate with one another in order to accomplish a shared goal. There is no central authority to control or coordinate the nodes or the network state.

Nodes in a decentralized network typically have the same relative status (this is the reason why they are often called peer-to-peer or P2P networks). The aggregate behaviour emerges from the interaction of nodes, each of which follows

---

<sup>2</sup> A *decentralized* system is different from a *distributed* system. Processing or storage may be distributed while control is still centralized and based on global information. A system can, of course, be both distributed and decentralized.

<sup>3</sup> With regret, we'll exclude biological decentralized systems from further consideration. Living systems such as ant colonies or the human immune system exhibit fascinating and complex emergent behaviour. Such systems are not digital networks, however, and the concept of governance — as understood by us humans — does not really apply.

<sup>4</sup> The word itself (*centralize*) came to use in Napoleonic France after the Revolution in the late 18th century. The antonym (*decentralize*) first appeared in the 1830's in German language.

well-defined rules or processes (which can, but need not, be identical). There is no single point of failure, and the network will typically function even if a significant portion of the nodes are off-line or non-operational.

The early Internet was effectively a decentralized network. The vision of Tim Berners-Lee for the World Wide Web, i.e. a web consisting of interlinked content, reflects the same spirit. After the early days, decentralized networks started to appear on top of the Internet. One of the first was Napster, a file-sharing service launched in 1999. Other applications followed, including BitTorrent (a protocol for distributing files over the Internet), Tor (a network for anonymous communication), as well as several P2P protocols for audio and video streaming. There are also mesh networks (where nodes connect with each other directly, dynamically, and often wirelessly), and the commercial market is growing along the development of IoT and AI applications.

To recap, decentralized networks are systems which share a number of common characteristics:

1. The system is composed of several nodes, each one of which is capable of computation and follows specific rules or processes.
2. Nodes constitute a network. Each node is connected to one or more nodes that it directly interacts or communicates with, and to other nodes indirectly. Not all nodes need to be connected or functional for the network to continue to operate; there is no single point of failure.
3. The network has a purpose or a use. It may work towards a goal (or a set of goals), or it can be employed for some productive and useful aim.
4. The network does not exist in isolation. It may exchange information or energy with an external environment or with other systems. There are boundary conditions (physical, legal, or other kinds) that constrain what the network is capable of or is allowed to do.

There are many kinds of decentralized networks, but the whole field is still too broad for our purposes. Our focus is on networks which utilise blockchain technology in their operations. Examples include Bitcoin, Ethereum, Ox, Filecoin, HyperLedger, Swarm, Polkadot, just to mention a few. Many — but not all — such networks use cryptocurrencies or digital tokens.

A blockchain is a distributed digital ledger, a growing list of records (blocks) where each block is linked (chained) to the previous one. The link is a hash of the contents of the previous block. The ledger shows the ownership of assets in its domain and the transactions<sup>5</sup> where the ownership is transferred to a new owner. The ownership is proven because the ledger is public and there is a consensus about all transactions.

The ledger is maintained by a large number of computing nodes in a peer-to-peer network. There is no central authority. The history of the ledger is immutable because the consensus requires proof, and the proof cannot be forged by any practical means. There are public blockchains (such as Bitcoin and Ethereum) as well as private and permissioned blockchains.

Different blockchains use different consensus algorithms, including proof-of-work (solving a difficult but meaningless cryptographic problem), proof-of-stake, and many others. Maintaining the integrity of a blockchain requires either a significant amount of effort or sizable collateral. In return, the nodes which validate and write new blocks are rewarded by receiving a certain amount of digital assets (tokens) in the currency of the ledger's domain.

There is a limited but increasing amount of research on blockchain governance. Wright and de Filippi (2018) review blockchain technology and explore the idea that organisations and transactions can be regulated by autonomous code. Sinclair et al. (2016) make the point that blockchains, by virtue of the consensus algorithm replacing the need for trust, can be viewed as a new and efficient governance mechanism for companies and markets. Yermack (2017)

<sup>5</sup> More complicated transactions are possible. In particular, a transaction may constitute an automatic execution of a computer program known as a *smart contract*. No human intervention is required to run such a program.

analyses the potential impact of blockchain technology (such as new methods of tracking asset ownership and voting) on corporate governance. Beck et al. (2018) look at the governance of decentralized systems from an IT viewpoint. Finck (2018) explores blockchain governance from the perspective of European Union law. Carter (2017) looks at the governance of many different crypto projects and raises a number of issues which should concern the investors in this space. Honkanen et al. (2019) have undertaken a survey of a range of whitepapers from the governance perspective.

This paper is structured as follows. Section 2 reviews the history of governance models in a non-blockchain context. Section 3 moves on to decentralized networks and addresses issues such as the governance structure, the degree of decentralization, on-chain vs. off-chain governance, and various voting and coordination mechanisms. Section 4 concludes.

## 2. What is governance?

Governance<sup>6</sup> is needed in and between nation states<sup>7</sup>, in regions within a nation, cities, corporations, non-profit organisations, societies of like-minded people, tribes, gangs, families, and teams at work or pleasure. As there are no well-established and universally approved practises for the governance of decentralized systems and blockchain protocols, let us first have a look at the society at large in the past and in the present.

Civil society is a relatively recent state of affairs. The *state of nature* is usually taken as a reference to time before organised communities. This is a topic once much debated by philosophers such as Thomas Hobbes, John Locke, Jean-Jacques Rousseau, David Hume and many others. There is no agreement of what the state of nature entailed, whether life really was<sup>8</sup> "solitary, poore, nasty, brutish, and short", or whether human beings — as naturally social animals — would have long remained in a savage condition.

Tribalism was common in the premodern world. Territories and resources were claimed by regional groups which traded and fought with each other without interference by central authority. Cooperation was essential for people within a tribal society in order to avoid friction, resolve conflicts, and manage resources.

Cooperation was relatively easy to maintain in small groups where mostly everybody knew each other. There may also be cognitive limits to the coherent group size, i.e. the number of people likely to stay together and maintain stable social relationships (Dunbar, 1992). When groups get bigger and face-to-face interactions grow less frequent, maintenance of cooperation becomes more difficult. It also becomes harder to monitor other people's contributions and to prevent free-riding and other kinds of opportunistic behaviour (Olson, 1965).

Even the most primitive societies hold religious beliefs, and organised religion provides the bridge to the next stage in the development of civil society. Religion supports collective action via reward or punishment (in the hereafter) which reinforce gains from cooperation in the present. It is a source of social cohesion, and a stepping stone on the journey towards the state and the political order (Fukuyama, 2011). Political institutions tend to develop by the time a society reaches 5,000 to 10,000 members. Maintaining a society of that magnitude or bigger does not seem to be possible without organised governance (Lutz, 2006, pp. 30-31).

Without going over the process of state building in any detail, suffice it to note that a long series of practical experiments in governance has been effectively carried out over thousands of years. We would be fools to ignore the lessons in that history. These are some of the governance models which have been tried:

- **Monarchy** is a form of governance where absolute power is held by a single hereditary ruler, often called a king or an emperor. Whilst most monarchies of today are symbolic, there are still some half a dozen absolute monarchies left. These are mostly found in the Arab countries, although there is one in Africa (Kingdom of Eswatini, i.e. the Swaziland).

---

<sup>6</sup> The Greek philosopher Plato was one of the first to consider different models of governance, and came up with the word for it. The Greek verb *kubernao* originally means to steer. See Plato (360 BC): "The Republic", chapter 6. The word appeared in French in the 13<sup>th</sup> century and in English in the 14<sup>th</sup> century.

<sup>7</sup> In earlier times, governance was mainly understood as referring to the rule of nations. The term has attracted broader usage since the 1990s. For a historical perspective, see *Étymologie du terme "gouvernance"*, a document prepared by the European Commission (retrieved on Sep 12, 2019 from [http://ec.europa.eu/governance/docs/doc5\\_fr.pdf](http://ec.europa.eu/governance/docs/doc5_fr.pdf)).

<sup>8</sup> Hobbes (1651): The First Part, Chapter 13, p. 62.

- **Oligarchy** denotes a society where a small group of individuals holds the power. There are different kinds of oligarchies, including aristocracy (rule by the nobility) and plutocracy (rule by the wealthy). The common denominator is authoritarian rule and the absence of democratic rights by the majority of citizens.
  - **Plutocracy** is a form of oligarchy where power is held by people of significant wealth or income. This used to be a fairly common model. Examples include the Roman Empire (where wealth was required for entry into census ranks), the Republic of Venice, and the pre-revolutionary Kingdom of France. The system survives in the City of London where the number of votes held by a business depends on the number of its employees.
  - **Timocracy** is a system where only the property owners may take part in governance. Athens in the 6th century BC was a timocracy, and so was the United Kingdom prior to 1918 (i.e. as long as the eligibility to vote depended on the ownership of a house or land).
  - **Theocracy** is characterized by a religious ideology. The laws may derive directly from religious scriptures, and the clergy typically occupies the highest offices. Iran is an example of a theocracy, and so is the Holy See (the Vatican City).
  - **Technocracy** is a governance model (and a form of meritocracy) where the decision makers are those with the most expertise in the relevant field of science or technology. No purely technocratic nations exist, but in China and Singapore the leadership often holds scientific or engineering credentials. In the corporate and the academic world, this model is much more common.
- **Feudalism** is more akin to a historical social structure than a model of governance. In a feudal society, you belonged to either peasantry, clergy, or nobility, and social mobility was largely absent. As a peasant, you provided labour and military service to a local lord in exchange for protection and the right to cultivate the land and keep some of the proceeds. Feudalism in Europe ended in the 18<sup>th</sup> century when it was superseded by monarchy and later by democracy.
- **Dictatorship** is a nation where the ruler (who can also be the head of the nation's military forces) holds absolute power. A dictatorship is an autocracy where law and order are favoured over civil liberties and political freedoms. Dissent is rarely tolerated, and there are few genuinely democratic processes.
- **Totalitarianism** is a form of governance where the ruling party holds all power in both the public and the private life of its citizens. There is often a single authority figure in charge. Widespread surveillance, tightly controlled media and propaganda are used to keep the citizens on a tight leash. North Korea is a prominent example.
- **Colonialism** is a form of governance where a nation extends its rule over other territories. The territory's resources are exploited for the good of the colonial masters. The indigenous population has few rights, and the ruling nation typically imposes its own culture and bureaucracy. Starting in the 15<sup>th</sup> century, the European monarchies established colonies in the New World, Africa, India, and the Far East. Few colonies exist at present.
- **Communism** represents the idea of common and public ownership of the economy and the means of production. In the thinking of Karl Marx and Friedrich Engels, there are no class divisions. A communist society often comes into being through a revolution. Once in place, political opposition or dissent is discouraged, sometimes violently so. There were probably no purely communist societies at any point in history, and even those supposedly in transition from socialism (such as the Soviet Union) collapsed by the end of the 20<sup>th</sup> century.
- **Corporatism** is a system where the society is organised into professional bodies or corporations which rule over people and their activities. The underlying ideas can be traced back to ancient Greece and Rome, even if the ideology was not fully formulated until the 18<sup>th</sup> century. In modern times, corporatism has been associated with fascism in Italy, industrial and financial conglomerates (*chaebols* in South Korea, *zaibatsu* in Japan) in Asia, and professional guilds and trade unions in many European nations, including Germany and Switzerland.

- **Democracy** is a form of governance where people select their leadership<sup>9</sup>. An assembly of representatives (the legislature) is chosen periodically in elections where all eligible citizens have a vote. The legislature is a forum for deliberation, and it has the authority to put in place laws which guide and regulate society. Functioning democracies are characterised by discourse, debate, and compromise in the quest of broad public interest. Democracy was born in the city state of Athens under Cleisthenes and Pericles some 25 centuries ago (see e.g. Scott and Makres, 2019).
- **Federalism** combines central and regional governments into a single entity. Regions (e.g. cantons, states, or provinces) are self-governing but have permanently delegated some powers to the central (i.e. federal) authority. The two distinct levels of government tend to be democratic and have a more or less equal status. At present, federal states include The United States, Canada, Mexico, Brazil, Argentina, India, Russia, Germany, Switzerland, and Australia. The European Union can be thought of as a federal union of nation states.
- **Anarchy** refers to the absence of a central authority or any other form of government. In anarchy, there are no public services, no enforced laws or regulations, and no meaningful diplomatic relations with the outside world. Anarchy (and arguably a return to the state of nature) typically emerges in times of conflict. Examples include some of the English Civil Wars, the French Revolution, the Russian Civil War, and most recently Somalia during the civil strife. There are still small anarchist communities in various parts of the world.

There are well-established governance models in modern corporations and non-profit organisations.

- A **limited company** is a structure which saves on the transaction costs of coordinating economic activity (Coase, 1937) and to limit the conflict between holders of productive assets (Williamson, 2002). Firms are regulated by company law in their country of domicile. The governance model is broadly similar in most free economies. Company shareholders elect a board of directors in annual (or additional, i.e. extraordinary) meetings. The board, in turn, supervises the executive management.

In practise, the management makes most of the everyday decisions and sets the strategy with a great degree of freedom. By law, though, there are some decisions (such as issuing additional share capital) which can only be made with shareholders' approval. A company charter, organisational regulations, or a shareholder agreement may place additional constraints on the exercise of power.

There are yet other kinds of economic entities such as cooperatives and partnerships. The specifics of their governance varies by country.

- A **non-profit organisation** does not have shareholders, but it may have an assembly and voting members. It will usually have a board. The organisation (and its board) is accountable to its founders, donors, members (if any), volunteers, and at least morally to the community.

There are many kinds of non-profit organisations. There are charities, non-profits, not-for-profits, associations, and foundations. A foundation can be either public or private, and operating or non-operating. The particulars of governance depend on the legal form of the organisation, its jurisdiction, and its charter or other founding document.

Common models of foundation governance include a one-tier and a two-tier model. In the former, the board includes both inside and outside directors, and the board supervises the staff. In the latter, the board consists of outside directors only. The board supervises the executive director, who in turn supervises the staff. Founders or members typically elect the board.

There has been a fair amount of experimentation in the private sector on new organisational structures. For instance, the practise of self-management has gained popularity in the past few decades (Bernstein et al. 2016). Self-managed teams organise their own work without the need for middle management or direct supervision.

---

<sup>9</sup> There are two different forms of democracies on a national level. In a presidential system, there is an elected head of the executive (the president). In a parliamentary system, the head of government is elected by the legislature. There are also hybrid forms, and democracies where a president has a largely ceremonial role.

- *Holacracy* is an example of a flat, self-managed structure (Robertson, 2007). The teams (sometimes called 'circles', 'pods', or 'cabals') consist of roles, and individuals are assigned to roles (and often to more than one team at a time) based on their capabilities. The teams govern themselves, i.e. their members decide how to go about their work. The purpose, accountability, decision making powers, and the rules for creating, changing, or removing teams are documented, and the documented structure is transparent within the organisation. Leadership is vested in roles, not individuals.
- *Sociocracy* (Romme, 1995) is based on consent within each team (consensus is not required, and voting is not used). Debate and discussion are encouraged before decisions are taken. The aim is to give people autonomy and have them decide as much as possible for themselves, but with structure in place for collaboration. In sociocracy, a clear distinction is made between governance (setting objectives and allocating resources) and operations (day to day activities within the constraints defined by governance). An organisation is seen as a collection of domains, each with a governing body in place. The governing body can be a single person (e.g. a team leader) or a group of people.

Self-managed organisational structures incorporate ideas from agile development and lean project management, methodologies which are popular in the technology sector. Free open source software (FOSS) development has been a source of inspiration for self-organising governance models<sup>10</sup>, and most blockchains rely on open-source software. The lack of control by any one party supports decentralization, and it is useful to have plenty of eyes on software when bugs can result in significant monetary loss.

Eric Raymond (1999) describes two different open-source software development models. In the "Cathedral" style, the code is developed by the core group of software developers, and external contributions are discouraged. GNU Emacs follows this style. In the "Bazaar" style, the code is made available for public testing and scrutiny even between releases, and external contributions are frequent, welcome and even essential. Linux (created by Linus Torvalds) is a prototypical example.

The open-source contribution model does not necessarily have any connection to open-source governance. In practise, governance style<sup>11</sup> ranges from centralized models (benevolent dictatorships such as Linux) to decentralized meritocracies (e.g. Apache OODT).

Many open-source projects start as cathedral-style benevolent dictatorships and move towards increasingly open bazaar-style contribution style with more formal and meritocratic governance as they mature<sup>12</sup>. Regardless of the governance model, one common trait is the existence of open forums and wikis where issues and initiatives are actively debated before decisions are made.

In economics, a common-pool resource (CPR) is a finite resource which is effectively open for all to exploit. Examples of natural commons include forests, pastures, fishing grounds, and the atmosphere. When consumers act in their own interest, the resource can easily become depleted or destroyed through overuse, pollution or congestion; this is the tragedy of commons (Hardin, 1968). However, Ostrom (1990) has shown that such resources can be sustainably managed by local communities as long as they are not solely motivated by self-interest. What is needed for effective governance of the commons is a shared protocol which provides the framework for communication, coordination and conflict resolution.

The analysis of natural commons can be extended to the management of information commons. In commons-based peer production (CBPP), people work cooperatively and in a self-organised fashion on a public and digital resource (Benkler, 2006). Examples of CBPP include FOSS projects such as Firefox and Linux, although there are many well-known initiatives where software is not the main focus (e.g. OpenStreetMap and Wikipedia).

<sup>10</sup> For a discussion of the tensions which may arise, see Fitzgerald and Ågerfalk (2005).

<sup>11</sup> For a similar categorisation by different labels, see de Laat (2007).

<sup>12</sup> For a discussion of governance in open-source development, see Demil and Lecocq (2006) and Gardler and Hanganu (2010).

Different forms of governance can and do coexist within one system. Many models are hybrids, being neither centralized nor decentralized. A system may have several hubs, components may have varying degrees of autonomy, and a mostly decentralized system may rely on some central information or retain a degree of global control. Information often flows horizontally, there are shortcuts, teams come together for a while and then disperse, and there may be distinct centers of power or transient coalitions. Even the boundaries of an organisation may be fuzzy if work is outsourced to external parties.

To recap, there is a wide range of variety in governance models on the national or regional level, in business, non-profit and the open-source sector. The differences between the models relate to the governance structure, the degree of decentralization, governance rules, processes, institutions, and the methods of coordination and the aggregation of preferences.

### Governance structure

One might be inclined to think that governance will work itself out, and in any case a little bit of anarchy may not be that bad. But a certain amount of structure is essential for good governance. There's a well-known essay on the failings of the women's liberation movement by Jo Freeman (1972) entitled "The Tyranny of Structurelessness". She makes the point<sup>13</sup> that the lack of structure only serves to give birth to an inner circle who will start inventing informal rules of the game. There is a basic information asymmetry, and the members of the inner circle may not have an incentive to share all they know. The governing elite may start off well-intentioned, but there is a great temptation for abuse of power. The outcome can be deeply unrepresentative of the larger movement at best and utterly self-serving at worst.

A governance structure may not always function as intended. Robert Michels (1911) introduced "The iron law of oligarchy", a theory which postulates that any hierarchical organisation — no matter how democratic its origins might be — runs a risk of turning into an oligarchy<sup>14</sup>. There are, alas, too many historical instances of powers percolating to a small group of privileged individuals.

One important question on governance structure is whether it is centralized, decentralized, or something in-between. Decentralized structures bring in the potential for greater diversity with different viewpoints covered by local units or individuals. Governance can become more efficient if such entities are allowed to respond to problems or contingencies in a timely manner and based on local information. Decentralized governance can also be perceived as having a higher degree of legitimacy if power is exercised by actors known to the community.

Decentralization may proceed along several different axes.

- **Political decentralization** is the transfer of power and resources from the central government to a lower level<sup>15</sup>. In nation states, devolution may involve the creation of new subnational or regional jurisdictions, putting in place local elections, and enabling local officials to take decisions without prior approval from above. In most cases, *ex post* monitoring is expected to remain.
- **Fiscal decentralization** is required if political devolution is to have substance. Local decision making bodies need sufficient financial resources to carry out their functions effectively. Possible sources of recurrent revenue include taxing powers, user charges, or the transfer of revenue from the central authority.
- **Economic decentralization** translates to the delegation of public functions through deregulation and privatisation of public utilities. Corporations, cooperatives, volunteer groups, and other non-governmental organisations may be allowed to carry out and charge for services which were previously handled or monopolised by the government.

Whilst there's good arguments for decentralized governance, it is not always the answer (Prud'homme, 1995). Decentralization may lead to the loss of economies of scale, slow decision making, the inability to coordinate the overall system, and the loss of control over scarce resources.

---

<sup>13</sup> The essay was originally given as a conference speech by Jo Freeman in 1970.

<sup>14</sup> See also the discussion on pages 52-55 in Slattery (1991).

<sup>15</sup> On the question of how to decentralise political power, the principle of *subsidiarity* is often used: The least centralized authority (or the lowest level in a hierarchy) which is capable of handling an issue effectively should do so.



## The separation of powers

One lesson in the history of governance is that uncontested power often leads to bad things. As a private scholar and an English aristocrat John Dahlberg-Acton<sup>16</sup> said:

"Power tends to corrupt, and absolute power corrupts absolutely. Great men are almost always bad men..."

The separation of powers can be an efficient defense against misbehaviour. The formalisation of this concept is usually credited to Baron de La Brède et de Montesquieu. Drawing on the precedents of the Roman Republic and the British constitutional system, Montesquieu (1751) stressed the importance of seeking a balance of power between different branches of government. In *trias politica*, the branches of government correspond to the legislature, the executive, and the judiciary<sup>17</sup>. The intent is to prevent situations where any single seat of power can exercise unchecked authority and thereby, over time, establish tyranny.

The separation of powers can be seen as a mechanism which is conducive to long-term stability of the society. It can also result in greater efficiency: As any one branch is not exercising the core functions of another, there is no need for repeated negotiation and compromise. In effect, Montesquieu was an early proponent of decentralized governance.

## Governing bodies

The governance structure often encompasses specific bodies and institutions. Having different governing bodies serves the separation of powers, but there are other functions they serve. For instance, a governing body may be to provide a forum for preparing decisions so that initiatives can be raised, background information collected and shared, and alternatives put forth, analysed, and debated.

The implementation of higher-level decisions is typically handled by a separate executive. There can also be a judiciary branch whose responsibility is to ensure that officials and the people follow the law. Additional bodies (such as the police force) may have an enforcement role. And virtually any larger organisation or society of today includes a bureaucracy, a non-elected body which handles the administration of the agreed policies.

Weber (1921) saw bureaucracy as the most efficient way of organising human activity in government and business. In his view, an ideal bureaucracy is characterized by hierarchical organization, a well-defined chain of command, clear scope, division of labor, and continuous operation. In his view, powers of the bureaucracy should be restricted and governed by laws and regulations. A well-functioning bureaucracy is administered by trained professionals whose entry to office depends on fulfilling transparent qualifications, and whose career path is guided by merit.

Many other kinds of governing bodies are possible. In a modern corporation, shareholders delegate the supervisory and strategic powers to the board of directors. The board, in turn, delegates the daily decision making powers to the management. A non-profit organisation or foundation typically has a board of directors and the executive (i.e. the day-to-day management) as well. There may also be an advisory council, different standing or ad-hoc committees, a secretariat, arbitration bodies, etc.

In general, governing bodies or office holders can be thought of as agents who act on behalf of principals (see e.g. Stiglitz, 1987), with the principals being the people, the community, the shareholders or some other stakeholders. The principals delegate some or all of their decision making powers to an agent or a group of agents.

## The rule of law

A governance structure loses much of its meaning if people don't know what that structure is. The structure and the rules of governance typically spell out who can make different kinds of decisions, and define the institutions or bodies which are used to debate, deliberate, agree on, implement, and enforce decisions.

An explicit goal (or possibly several goals) is often part of the rules. In a nation state, the goal may be the public good, encompassing things such as the eradication of poverty, providing an education for all, and ensuring the prosperity and safety of citizens. In a private corporation, the primary goal is the maximisation of shareholder profits. In a

<sup>16</sup> Letter to Bishop Mandell Creighton (April 5, 1887). Published in Figgis and Laurence (1907, eds.).

<sup>17</sup> There are also bipartite models, including semi-presidential systems where the executive and the legislative branch overlap.

non-profit organisation, the goal may be, for instance, the preservation of nature or improving the health or living conditions of people.

In a nation state, the structure and processes are encoded in laws and regulations. In organisations, other kinds of rules or byelaws will be in place. The *rule of law* is a distinct component of political order which limits the state power. It can be said to properly exist only where the pre-existing body of law is sovereign, i.e. those in power feel bound by the law (Fukuyama, 2011, p. 393). A basic premise is that laws are rules which — whilst binding — are in line with a broad consensus over basic human values.

There are often specialized rules in place to spell out how new rules come into being, and how existing ones can be amended or dropped. In a democracy, such rules may specify that the sovereign decision makers (the eligible adults in society) elect (vote for) a smaller number of representatives (a parliament), who then debate and decide on the rules (laws and regulations).

The rules can also manifest themselves as shared social norms (Hume, 1739; Elster, 1989) which tell participants what kind of behaviour is acceptable or desirable in different situations. Social norms emerge naturally as a result of repeated interaction over time between human beings who live, work or play together. Informal rules and traditions exist at various levels of civil society, but they may guide the interaction between nation states equally well.

### The constitution

An organisation or a country will often have a fundamental set of laws called a *constitution*, i.e. a legal foundation for an entity and its governance. As such, it may set forth the underlying goals and principles and impose limits on the powers of the elected leaders and the governing bodies. The constitution lays out basic guidelines that all other laws and regulations must be consistent with. Changing the constitution is almost always significantly more difficult than making or amending an ordinary law.

A constitution can apply to nation states, international organisations, companies, and societies and associations of various kinds. A codified constitution is contained in a single document; an uncoded constitution consists of several different (written or unwritten) sources. In a corporation or organisation, the equivalent is sometimes called a *charter*.

A constitution can define the rights and obligations of the people in different situations. It will thereby establish boundaries which cannot be legally crossed. Actions by officials or governing bodies which are not in line with the constitution are considered null and void, i.e. they have no legal meaning. In many countries, there is a constitutional court which can decide if a law is constitutional or not.

As a good thing for those contemplating drafting a constitution, the design does not need to start from a blank slate. Various constitutional principles have been tried over time. Since Aristotle differentiated between ordinary law and constitution (*politeia*), a lot of thinking and analysis has been devoted to the principles of constitutional design (Gordon, 1999).

Even though the concept of *natural law* is perhaps somewhat outdated by now, it serves to illustrate the development of constitutional thought. In the middle ages, the common understanding was that there is a body of invariant set of moral principles which should be a basis for all human conduct. St. Thomas Aquinas (a Dominican friar and philosopher in the 13th century) developed earlier ideas<sup>18</sup> to conclude that a law which deviates from the natural law is nothing but a perversion. He came up with the phrase “*Lex iniusta non est lex*”, i.e. an unjust law is not a law. The implication is that unjust laws need not be followed.

In the Age of Enlightenment in the 18th century, the work of philosophers Thomas Hobbes, John Locke, Jean Jacques Rousseau and others gave rise to the theory of the *social contract*. The idea is that people may be willing to surrender some of their freedoms to a ruler in exchange for protection of their property, well-being, and the social order. In other words, a social contract is an unspoken agreement between the people and their government. The people agree to follow certain rules imposed from above because they trust that the government will carry out its functions effectively, fairly, and without placing undue burden on the people.

---

<sup>18</sup> This concept (as so many others) can be traced back to ancient Greeks. Thomas Aquinas combined Aristotle’s views on goodness and happiness with Catholic theology in his *Summa Theologica*, a hugely influential philosophical work. In his writings in the 17<sup>th</sup> century, Hugo Grotius made the point that natural law can be secular, i.e. it need not be tied into a religious set of beliefs.

Most people for most of the time follow the social contract, but not because of any blind obedience. There are incentives: People understand that the constitution and the government provide for their safety and prosperity, social stability, the lack of violence, fairness of the society, and so forth. At times of war and upheaval, the social contract can get easily broken. More pressing motivations — such as the need for the immediate survival of oneself or one's family — can take precedence.

Drawing on ideas such as the above, Lutz (2006) suggests that there are three essential building blocks in a good constitution: A cultural element, a power element, and a justice element.

- The **cultural element** reflects the fact that humans, as a species, have spent more time accumulating culture than evolving biologically. Since Aristotle, constitutions have defined a way of life by using values and justice as the organising principles. A constitution, therefore, should recognize the cultural element that the community aspires to. This is often expressed as a preamble or a declaration of ideals.
- The **power element** defines the decision making institutions, and identifies the supreme power with the final say. In a nation state, this element also provides the framework for political struggle and for the distribution of power. Conflict between different stakeholders is unavoidable, and the constitution should create a framework that structures the conflict so that it can be managed politically, and does not need to be resolved through violence in the streets. For instance, a network constitution might allow the community to disband the network executive and trigger a re-election, similar to a vote of no-confidence in political systems.
- The **justice element** makes a governance model predictable. Since the constitution is known and public, there is a common understanding in the community of what is the proper process of decision making. The justice element can incorporate the concept of the separation of powers to prevent any single party — such as the founding team or a wealthy token holder — from violating the shared sense of justice. There may also be explicit limits on the decision making powers by those in the core team, as well as a bill of rights which protects community members.

There is no optimal constitution. Countries and societies are all different, and even where a successful solution to governance has been found, it will not last. Change is inevitable, and political institutions invariably lag behind the social and economic drift in society.

Constitutional government is not a natural form of political organisation. It is simply a tool which can help us achieve elementary human objectives: Self-preservation, liberty, predictability, fairness, coordination, cooperation, sustainable innovation, and the pursuit of happiness. Human nature is fallible but capable of greatness. A constitution, at its best, can channel it in a positive direction.

### Voting systems

Voting is a widely used method for aggregating preferences and arriving at collective decisions in politics, in the corporate sector, and in non-governmental organisations. Voting is something we will come back to, but let us take a moment here to introduce some of the relevant issues.

Voting can be used for the selection of individuals for an assembly, to approve or reject a proposal, or to decide between different initiatives such as protocol improvement proposals. In a democracy (e.g. a nation, a local region or a city), the *electorate* consists of typically all citizens who are legal residents of the jurisdiction and old enough to vote. In a limited company, any shareholder can typically vote, but the voting rights may be constrained by a corporate charter or a shareholder agreement.

A voting system can take many forms. In *plurality voting*, the alternative or the candidate with the highest number of votes wins. In *majority voting*, a candidate needs more than one half of the votes to win. The *basis* is the numerical threshold for what constitutes a majority. For some types of decisions, a supermajority — such as two thirds or 75% of votes — may be required. A *quorum* (a minimum number of members present) may be required before a decision making body can conduct its business and take a binding vote.

If there are more than two candidates, more than one round of voting may be needed. In *approval voting*, a voter may approve any number of candidates (the most-approved wins). *Ranked voting* is an ordinal system where each voter ranks the candidates in line with his or her preferences.

There are also cardinal systems where a voter attaches numerical scores to candidates, and the scores are tallied to determine the winner. The Janeček method allows both positive and negative votes. Some electoral systems use weighted voting. In shareholder meetings, the number of votes you have corresponds to the number of shares you own. In delegative democracy<sup>19</sup>, constituents can either vote themselves or allow other people to vote on their behalf.

There is no voting system which obeys all of some seemingly desirable criteria of fairness. Any reasonable voting mechanism is either dictatorial or subject to tactical voting (i.e. if you know how other people have voted, you have an incentive to game the system and not vote in line with your true preferences). In other words, rationality can be lost when individual preferences are aggregated into collective choice.

Arrow's impossibility theorem (Arrow, 1950) shows that there is no ordinal (ranked) voting mechanism which satisfies the conditions of unrestricted domain, non-dictatorship, weak Pareto efficiency, and independence of irrelevant alternatives.

It's tricky to concisely spell out what these conditions mean, but they roughly translate to the following: Voters' preferences yield a unique and complete aggregate ranking. There is no single voter whose preferences override all others. If each voter strictly prefers one alternative to another, the collective ordering agrees. And if a new alternative is introduced, voters will not want to change their preferences over the existing ones.

There is a related result known as Gibbard-Satterthwaite theorem (Gibbard, 1973; Satterthwaite, 1975). With at least three alternatives, there is no social choice mechanism which satisfies the axioms of unrestricted domain, non-dictatorship, no chance of ties (so that the collective choice always produces one winning alternative), and the impossibility of manipulating the collective choice (by someone misrepresenting their true preferences).

If there are only two alternatives, majority voting satisfies the remaining conditions in Arrow's impossibility theorem as well as Gibbard-Satterthwaite theorem<sup>20</sup>. More generally, for each voting mechanism there is a Nakamura (1979) number. If the number of alternatives is greater or equal to the Nakamura number (which is always an integer), there are circumstances where rational choice is impossible.

Fair elections are a cornerstone of many governance models. Voters' identity is therefore checked in person at polling stations, privacy in the voting booth is guaranteed, and elections are monitored by neutral observers. In practise, though, it is not always the case that elections are carried out objectively and without interference.

Voter manipulation is not a new thing, and it is not difficult to find instances of vote buying<sup>21</sup> and other abnormalities in history. You might think that vote buying is a thing of the past. Doing so is a crime, after all, and compliance is hard to enforce (I can drink the beer you bought, vote whichever way I like, and you'll be none the wiser). Alas, that is not quite the case. There are still countries where politicians hand out jobs and plain cash in order to win elections (Kitschelt and Wilkinson, 2007). According to surveys, about 17% of voters in Africa and 25% in Latin America have been offered material benefits in exchange for their votes (Stokes et al., 2014). An analysis of monetary aggregates (after all, a good amount of cash would be needed in the days leading to the poll) suggests that the going market price ranges between \$10 and \$50 per vote, depending on the election and the country (Aidt et al., 2015).

---

<sup>19</sup> Proxy voting is common in non-profit organisations and corporate shareholder meetings. Delegative democracy is effectively a form of proxy voting where the proxy is in force until cancelled, and with transparency enforced on delegated votes. The proxy can be transitive, i.e. the voting power may be further delegated.

<sup>20</sup> Rearranging the election as a sequence of pairwise choices does not disprove either theorem but can radically affect the outcome with *a priori* less popular becoming much more likely to be eventually approved (think of how a tennis tournament works).

<sup>21</sup> There was a time when inducements were commonly of the bibulous kind; see e.g. Sismondo (2011), pp. 45-46.

### 3. Governance models in decentralized networks

This is a comment by Nick Szabo, a libertarian and the inventor of the smart contract (Paumgarten, 2018):

“Blockchain governance generally comes in only three varieties: (1) Lord of the Flies, (2) lawyers, or (3) ruthlessly minimized.”

As a response to a question, “Why ruthless?”, Szabo replied, “Otherwise the children or the lawyers will win.”

We don’t think the governance landscape is quite that desolate. But it is a fair question if governance in decentralized networks can be similar to what we find in other parts of society. Will any of the existing models still work? Can we at least borrow some of their features? Is something completely new desired or even required for technological reasons?

To briefly review how blockchain technology came about, Haber and Stornetta (1991) proposed saving hash values of digital documents (along with a timestamp) in a data structure which contains hashes of the previous records — in other words, a blockchain.

A few years later in 1994, Nick Szabo came up with another innovation in the form of smart contracts (Szabo, 1996). These are computational structures which are automatically and irreversibly executed in a blockchain, thereby implementing a well-defined process or a program in computer code.

A blockchain only works if there is a global consensus about its contents. The foundation for the consensus mechanism is the proof of work (PoW) concept, an idea introduced by Dwork and Naor (1993). Some years later, Hal Finney (2004) suggested a system where double spending of tokens was impossible (Jakobsson and Juels, 1999) and reusable proof of work was rewarded by digital Hashcash tokens.

These early efforts still involved a centralized and trusted server. All changed when Satoshi Nakamoto (2008) published his breakthrough Bitcoin paper<sup>22</sup>. Building on the previous work, he added an incentive layer and a consensus mechanism. Bitcoin miners are rewarded by a proof-of-work mechanism, with miners’ work verified (and consensus reached) by the majority of nodes in a decentralized network.

In our view, the ethos of decentralization brings a number of new issues to the table. The emergence of decentralized systems and rising concerns about the overreach by the state and data-driven enterprises has elevated governance to the forefront of the techno-political debate. And governance processes were necessarily off-chain in the past. The concept of on-chain simply did not exist; blockchain technology was only invented in the 1990’s and in the 2000’s.

Unpermissioned blockchains implement a resource in the form of a public ledger with immutable and transparent transactions. That resource is finite as greater use imposes a burden to network nodes in terms of storage, computation, and transmission bandwidth. Blockchains can therefore be viewed as a form of commons-based peer production or CBPP (Arvidsson et al., 2017; Red, 2019; Rozas et al., 2018), and they provide new ways of overcoming some of the limitations in open-source development. In particular, incentive mechanisms based on cryptocurrency can help solve the lack of funding which is often a constraint on volunteer-based projects. These mechanisms are a game-changer, in a sense, as they open the door for vendor-neutral and scalable public infrastructure such as worldwide money or computing networks.

Given that a smart contract can execute almost any kind of computation, it can obviously crunch through contractual clauses such as could be found in a legal contract. Technically, then, smart contracts could be used to implement at least a part of various governance processes. And there is another potentially useful blockchain feature: Off-chain contracts can be tokenized and thus immutably recorded by saving a hash code in a blockchain. What this means is

<sup>22</sup> Satoshi Nakamoto is a pseudonym. Despite much speculation, there is still no certainty about the identity of the Bitcoin inventor.

that a reference to a document — such as a user agreement or even a constitution — can be provably included in transactions between users of a decentralized network.

As mentioned in the introduction, the lack of an effective and well-defined governance model can lead to problems. Unclear governance can stop a decentralized project in its tracks, not to speak of the time, the effort and the expense wasted on resolving the legal ramifications which may follow. Situations may arise where timely decision making and software fixes may be required to avoid financial loss.

Consequences of either software vulnerability or weak governance can be non-trivial. Several notable examples have been reported in public over the past few years, including the following well-known cases:

- The DAO was launched in April 2016 with the aim of funding development proposals as voted by the DAO members. Crowdfunding for the project was popular with over \$150M raised. However, there were vulnerabilities in the code, and unknown user(s) managed to transfer roughly 3.6 million ETH (equivalent to about \$50M at the time) to a subsidiary account. After a lively discussion, the Ethereum community decided to create a hard fork which restored almost all of the diverted funds back to the original contract<sup>23</sup>.
- In 2017, the Tezos project carried out an ICO and raised the equivalent of \$232 million. A battle for control soon ensued between Arthur and Kathleen Breitman (the two founders whose Delaware-based company owns the Tezos code) and Johann Gevers, the president of a Swiss Tezos foundation (which holds the funds collected in the ICO); see Lewis-Kraus (2018).
- In the EOS project, there were bugs in the code to the extent that ill-intentioned parties could create new tokens, steal existing ones, or potentially even take over the entire network (Borak, 2018). Sure enough, some \$240,000 worth of EOS tokens were stolen (Canellis, 2018) from a hacked decentralized app (dApp).

Even if a decentralized network were well-designed, managed to avoid technical glitches and steer clear of hacking attempts, technological or commercial landscape may change so that change is essential. If the governance model leads to a stalemate or to slow decision making, a protocol may find itself obsolete and out of use.

### Governance models in use

What kind of governance models are actually being used in decentralized systems? On the whole, it is safe to say that governance is very much work in progress, if not in many cases ignored altogether. If we look at what's there today, the following broad categories emerge:

- **Benevolent dictatorship.** This is an autocratic model where one person holds the ultimate power, and makes the final decisions if the community or the wider team is in disagreement. The case was different a few years ago, but at present we are not aware of any popular network where a single decision maker rules supreme.
- **Technocracy.** In many well-known blockchains, the core developers are the final arbiters of the technical feasibility of protocol changes and have the ability to make changes to the codebase. In practise, the core team is often forced to consider the public support of the community and the views of major stakeholders such as miners and crypto wallet providers.

Monero is an example of a network where the governance is in the hands of the core developers. There is a donation-based crowdfunding system in place. There is also an active open source community which makes genuine contributions to the codebase in Github. Ultimately, though, a seven-person core team is in charge.

Bitcoin started out as a reasonably pure instance of governance by core developers, with the process based on Bitcoin Improvement Proposals (BIPs). The consensus within a small group of developers is still the goal, even if the present reality is somewhat nuanced. As discussed by de Philippi and Loveluck (2016), governance ultimately depends on wider support. If there is more than one possible implementation of the protocol, the miners will decide which code to run, and wallet providers will decide which implementation to support. If token users and app developers refuse to support the new version, the miners and wallet providers will have

---

<sup>23</sup> The resolution caused the blockchain to split into two, each with its own active cryptocurrency. Ethereum reversed the results of the DAO hack, and Ethereum Classic remains the original (unforked) chain. See e.g. DuPont (2018).

little choice but to agree. The core developers need to take all these views into account when they work towards a consensus.

Although many details are different, the process<sup>24</sup> is broadly similar in other protocols such as Aragon or Ethereum. In the latter, contributors can create Ethereum Improvement Proposals (EIPs). After a technical feasibility analysis, the core developers will aim to reach a consensus on the proposal. They will also try to ensure that miners and nodes are on board with the suggested change.

It is not difficult to appreciate how and why a technocratic model of governance can emerge. Decentralized networks are based on technology which is on the cutting edge and sometimes experimental, and unforeseen problems will emerge. The solutions are often developed in open source projects. Deep technical knowledge is needed, and that is what the core teams have.

- **Democracy.** There are protocols where token holders make at least some of the decisions, either directly or indirectly via delegates.
  - **Direct democracy.** As a political system<sup>25</sup>, this is one where the citizens make decisions personally. In the decentralized space, the counterpart is a model where any token holder can vote. In MakerDAO, for instance, token owners vote directly on changes and risk parameters in the credit system which underlies the stablecoin mechanism. Voting is also possible on a part of the operational spending, and there is advisory voting (so-called soft consensus) on other issues.
  - **Representative democracy.** This is a model where people elect<sup>26</sup> a subset of the public as the decision making body. As far as we know, representative democracy has not been tried as a stand-alone governance model of decentralized networks. However, a number of networks do have steering committees in place. Such committees are often elected by the entire community, or sometimes by only the active members of the community. Examples include BitShares, Corda, Hyperledger and VeChain. As a rule, the decision making powers of such committees are limited and often apply to technical issues only.
  - **Delegative democracy.** This is a governance model where each participant can either vote directly or yield their voting power to somebody else (Ford, 2002). In the interest of accountability, delegates' decisions are usually made public. This is a fairly common model in decentralized protocols. Typically any community member can raise initiatives for the ballot. Token holders can either vote directly or delegate their voting power to a proxy securely (i.e. without revealing their private keys), and can revoke the delegation at any time. Most delegative democracies (in the present context) are effectively plutocracies.

Liquid democracy is a subset of delegative democracy<sup>27</sup>, the main difference being the voter's ability to approve or ignore the vote cast by the delegate (Schiener, 2015). In other words, I can delegate my vote to you, but I will see your choice before votes are counted. If I'm happy with your decision, I will do nothing and the vote stands. If I don't like your choice, I still have time to override you and vote directly.

- **Plutocracy.** There are a number of protocols where the decision making power depends on wealth. If a tokenised voting system in a nominally direct democracy assigns one vote to one token, then that system is effectively a plutocracy. This model often arises in networks where the consensus mechanism requires a stake, i.e. a token deposit placed in what is effectively an escrow account.

There are different consensus mechanisms which use staking, including proof-of-stake (PoS) and delegated proof-of-stake (DPoS). There are also ledgers where so-called masternodes handle some of the network

<sup>24</sup> This process is largely in line with how the Python programming language is maintained with Python Enhancement Proposals (PEPs). There are also similarities with the development of Internet protocols, where a Request for Comment (RFC) is the historical counterpart of PEP.

<sup>25</sup> This is a rare system these days. *Landsgemeinde* is one of the oldest forms of direct democracy, and still in use in two cantons in Switzerland. Eligible citizens meet in the open air on certain days and vote by raising hands.

<sup>26</sup> Sortition (also known as *demarchy*) is a variation where representatives are chosen at random from a larger pool of candidates. It can be used, for instance, to select legal juries and advisory citizens' assemblies.

<sup>27</sup> The usage is fluid, and sometimes delegative and liquid democracy are used interchangeably.

functionality. There are variations; for instance, it may be possible both to stake tokens for the right to take part in PoS consensus and stake tokens for the right to operate a masternode in one network.

- In **proof-of-stake**, a node operator locks away a stake for the right to participate in block creation. One of the nodes with stake is selected at random to verify transactions and to produce a new block, with the odds tilted in favour of bigger stakes (other factors such as the time of staking and the time of the most recent selection may be relevant). A transaction fee is paid as a reward to the node which was selected to write the new block. If the node validates a fraudulent transaction or misbehaves in some other way (e.g. by trying to double-spend tokens), the stake is forfeited, and the node may lose the right to participate in staking. BlackCoin, Lisk, NXT and Peercoin are examples of networks with a PoS consensus algorithm.
- In **delegated proof-of-stake**, the token holders choose a small number of nodes as delegates by staking tokens with different candidates (depending on the system, a user may also be able to delegate their voting power to another user). Every time a new block is due, one of the delegates is chosen at random to verify transactions and to create the block. The selected node receives a transaction fee as a reward, and a part of that reward is shared, in proportion, with those who voted for the delegate. DPoS examples include Æternity, Ark, Bitshares, Cardano, Cosmos, Decred, EOS, Lisk, Nano, NEO, Steem and Tezos.
- **Masternodes** exist in different kinds of networks regardless of the consensus mechanism (proof-of-work, proof-of-stake, or some other). Masternodes are synchronised and fully connected nodes<sup>28</sup> which provide additional services to the network. They won't create new blocks, but (depending on the network) they can validate new blocks, carry out instant or private transactions, or provide some other functionality (e.g. storage or some other useful activity). A significant stake (as well as a certain amount of technical knowledge) is required<sup>29</sup> for the right to run a masternode, and the operators are compensated for their services. Examples of blockchains with masternodes include Dash, Energi, Phore, PIVX, Syscoin and Zcoin.

There are many different staking mechanisms, the number of possible block producers varies, and the usage of terms is not consistent. Block producers can be called 'witnesses', 'delegates', 'notaries', or 'forgers', and yet other conventions exist. In some networks, the role of block producers is explicitly separated from delegates with a decision making role. In the latter case, delegates typically have the capability to monitor and amend network parameters such as fees, block size, block rewards, and the length of transaction cycle.

Nodes or masternode operators are often eligible to vote (or have a veto) on protocol changes and network updates. They may also have a say on the use of the development budget. The idea is that the network retains a part of the block rewards, and the infrastructure operators decide on how to spend that part in the maintenance and further development.

In the case of DPoS governance, there is a symbiotic financial relationship between token owners and delegates. If you think of an analogue in politics, it is as if members of parliament were given individual taxing powers proportional to the number of votes they've attracted. The representatives of the voting public would then hand back to constituents some of the taxes they collect and keep the rest.

In networks where delegation is used, a token holder can usually only vote for a block producer. This is different from an idealised liquid democracy, where anyone with basic qualifications is free to nominate themselves as a candidate. In liquid democracy, voters would be expected to vote for candidates who are knowledgeable, perhaps known in person, and whom they trust to look after their interests — including interests beyond a payback.

Delegated blockchain governance is effectively a mutually beneficial arrangement between a number of powerful block producers and a larger number of token holders. As such, it can be viewed as *patronage*. One saving grace is that participation is open to all and follows well-defined rules which are coded in the blockchain. DPoS is a form of *programmatically distributed* which has been deemed legal in the US by the

<sup>28</sup> A fully connected node ("full node") maintains a complete copy of the blockchain's transaction history. It receives, stores and broadcasts all transactions but does not create new blocks. A miner is always a full node, but a full node is not necessarily a miner.

<sup>29</sup> The stake required to run a masternode is locked down as a guarantee that the operator fulfills its obligations. In a typical setup, a masternode loses its status if it goes offline for a non-trivial length of time or if the collateral falls below a threshold.



Supreme Court (see Stokes et al., 2014, pp. 8-9). Patronage without public rules would constitute *clientelism*, a system which is illegal and prone to various kinds of biases and abuse.

- **Private governance.** There are many public networks created by a private entity. There are also permissioned and consortium networks which serve the objectives of a commercial enterprise or a group of organisations.
  - **Corporate governance.** There are decentralized projects which are being developed by a limited company. If no other governance model has been defined and implemented, the network is effectively governed by that company. Corporate governance applies with shareholders having the ultimate power, and with board of directors monitoring the executive management of the company<sup>30</sup>. Examples include EOS and Ripple.
  - **Non-profit governance.** There are networks and blockchains which are governed by a foundation or other kind of non-profit organisation<sup>31</sup>. Decisions are typically made in either one-tier or two-tier model. There is a board of directors and possibly executive management answerable to the board. Examples include IOTA, NEM, Augur, and Lisk.
  - **Consortium governance.** If the network is developed or run by a commercial consortium, the concept of decentralization may not be of primary interest. The nodes are run by known and trusted parties consisting of limited companies or other organisations. Having a shared and single source of truth via a blockchain may be the key motivation for setting up the consortium.

In any consortium, there is a written agreement which covers issues such as the term, the rights and responsibilities of consortium members, how to add new members, how to withdraw, a definition of the governance bodies, a description of the decision making process, and a mechanism for dispute resolution. A consortium may be open to all who wish to join, or it may be a private one. In the latter case, the entry to the consortium will be subject to agreement by the other members. Examples of consortium blockchains include Corda, Hyperledger, and Quorum.

- **Futarchy** was originally proposed in 2000 by Robin Hanson (2007, 2013). It is a governance model where the community first defines its values in terms of concrete metrics, and a prediction market is then used to decide which policy is likely to best achieve the desired outcome.

As an example, the metric might be something like “The market share of newly registered passenger electric vehicles in 2023 is 15%”, or perhaps “The coin price, as reported by CoinMarketCap on 31 December 2020 at 12 noon UTC, is \$0.25 per coin”. Once the metric is agreed, a prediction market for policy alternatives is set up. The alternatives could include proposals such as “Build a comprehensive national charging infrastructure by the end of 2022”, or “Let the private sector to sort out the charging infrastructure”. Or there might be policies such as “Implement the improvement proposal no. 12A” and “Implement the improvement proposal no. 12B”.

The metrics and policy proposals are published, the prediction market is opened and allowed to run for a predetermined length of time. In the prediction market, there is a token for each policy, and the token price is linked to the metric (e.g. €0.1 per 1% of electric vehicle market share or \$1 per coin). Once the market closes, all trades in the losing token are cancelled. Anyone holding the winning token is paid an amount determined later by the metric. For instance, if you hold 100 winning tokens in the electric vehicle (EV) case and the EV market share in 2023 turns out to be 12%, you will be paid €120. If you hold 1000 winning tokens in the crypto case and the market price ends up at \$0.30 per coin, you will be paid \$300.

There are a number of potential weaknesses in futarchy, including the chance of market manipulation, excessive price volatility, low participation, the subjectivity of values, and the difficulty of measuring the impact of different policies<sup>32</sup>. And financial markets, in general, are not known for universally accurate price discovery. There are potential advantages, too, including tangible incentives for the electorate, channeling

<sup>30</sup> Hedera Hashgraph represents a variation where a governing council determines the direction of the software development and the platform strategy. The council is composed of term-limited global enterprises across multiple industries. As such, the governance is certainly decentralized, albeit within a limited group of large corporations.

<sup>31</sup> There are also duopolies where governance is effectively shared by two organisations. Zcash Foundation and Electric Coin Company are two examples.

<sup>32</sup> See the “Argument Against” in Buterin (2014).

wealth and influence for those with better information and analytical acumen, and a focus on policies as opposed to personalities.

Futarchy is a largely untried mechanism in either political governance or in blockchains, but it might technically fit in nicely with on-chain governance and DAOs. As far as we know, Amoveo is the only decentralized network which uses futarchy, although Tezos and Gnosis are experimenting with the concept.

In practise, neat distinctions between different models are often hard to make. Network governance may share features of democracy, plutocracy, or meritocracy, and there may also be a corporate entity or a foundation which retains a significant decision making role.

A wide range of variety in governance models have been tried on the national or regional level, in business, non-profit and the open-source sector. There are obvious counterparts to many of these in the decentralized space. In order to identify the relevant issues, let's have a look at where these models differ from one another. As we see it, the main differences relate to the question of who makes the decisions, what are the rules and processes, and what are the governing bodies and institutions.

### Who decides?

Decentralized networks often start out as technology projects where the founding team or the core developers make the decisions. At the early stage, governance typically takes the form of a beneficial dictatorship or a technocracy. Once the project matures, the founding team or the project owners may decide to step away and put in place a different governance model. This is the point where the question arises as to who should take part of governance. These are some of the potential decision makers:

- **Token holders.** There may be a token associated with the network. If so, token<sup>33</sup> holders will certainly be interested in governance, all the more so if they participated in crowdfunding the project or have purchased a significant number of tokens in a secondary market. If nothing else, token holders will want to see that project funds are being used appropriately and in their best interests.
- **Financiers.** There are different ways to finance decentralized projects. Some will be crowdfunded, whilst others may attract financing from friends and family, business angels, venture capital funds, high net-worth individuals, etc. In return for funding, backers may well ask for a stake or for a decision making role.
- **Node operators.** In any protocol with an associated blockchain, computing nodes are needed to ensure that consensus is being reached and to actually create new blocks. In PoW blockchains, this functionality is provided by miners. In PoS blockchains, there are delegates. Regardless of the consensus mechanism, block producers will receive rewards for creating valid new blocks. Owners and operators have an interest in smooth running of the network, in financial rewards, and in governance.
- **Service providers.** There may be nodes which provide various kinds of services: Validating new blocks, facilitating instant value transfer, providing bandwidth or storage, carrying out arbitration, maintaining reputation metrics, etc. Depending on the network, the service providers may be called masternodes, or they may go by some other name. Service providers typically receive compensation for their efforts.
- **Core developers.** The project team and the core developers of the network have the expertise and the interest in maintaining and developing the technology. If there is a previously agreed technical roadmap, software development is often carried out as a routine matter without wider consultation. The core team would still be expected to flag any higher-level issues so that they can be resolved by the governance model.
- **Network users.** Decentralized networks cater to many different types of users, including consumers, various types of businesses, and decentralized applications (dApps).
- **Content producers.** A network may be used to share or distribute digital content such as sensory data, music, videos, images, etc. The content producers have an interest in continued functioning of the network and in

---

<sup>33</sup> Coin is an alternative term for a token. Whilst there is no unilaterally accepted definition of either, one key difference relates to their use. Cryptocurrency coins (e.g., Bitcoin, Ether) can be used independently of a native platform. Tokens (e.g., Golem, BAT) exist on a particular platform such as Ethereum or EOS.

the rules which guide content sharing, royalty terms, copyright issues etc. They may also care about the technology as far as it affects the security, throughput and capacity.

- **Application developers.** Many networks constitute platforms for the execution of various kinds of decentralized applications or microservices. The developers of such apps have a natural interest in the welfare and success of the network and its ecosystem.

There are often external stakeholders who try to influence the process. While they may not have explicit powers, they can have an impact by persuasion of individuals in the governing bodies or by influencing the public opinion. In politics, there are lobbyists, think tanks, non-governmental and religious organisations, the media, and so on. In the decentralized space, potential stakeholders include traders who buy and sell tokens in the pursuit of profits or diversification. Given the multitude of potential stakeholders, some filtering will be needed. You cannot expect to have influence without a significant stake or a legitimate interest. Since many issues will be technical and non-trivial, you also need to be motivated and informed before you can usefully take part.

There is a transaction cost to governance in terms of time and attention. Transaction cost economics have been applied to corporate governance, and the same framework can be useful in the analysis of different governance structures in blockchain-based systems (Pietrewicz, 2018). The import of transaction costs is affected by the frequency of interaction, the technology in use, uncertainty about the consequences of decisions, asset specificity, and the motivation, preferences and expertise of individual actors. For instance, the appropriate governance model in decisions with far-reaching or irreversible consequences may be very different from the process best employed in everyday decisions of little consequence.

### What is governed?

What are the things that can or should be governed in decentralized networks and blockchain protocols? As we see it, technical, moral and ethical questions can be objects of governance.

- **Technical issues.** What is the technical direction of the codebase that implements a decentralized protocol? For instance, there might be important design choices such as the consensus mechanism (say, proof of work vs. proof of stake). Another obvious governance question is how new R&D initiatives or development projects are to be chosen.
- **Protocol changes.** Technical or ethical considerations or a fundamental disagreement among stakeholders may necessitate a protocol split<sup>34</sup>. A permanent *hard fork*<sup>35</sup> may introduce fundamentally new features, to repair serious bugs in the codebase, or to reverse malicious transactions. If not all nodes agree to follow the new rules, a split of the blockchain in two will occur. An agreed protocol change can also be implemented as a *soft fork*. A soft fork is backward-compatible, and older versions of the codebase continue to function even if some (but not all) nodes have moved to a new version of the software.
- **Network access.** Is the network public (permissionless) or permissioned (closed)? Is the protocol accessible to anyone willing to join? Are there prerequisites — technical or other kinds — which have to be satisfied before access is granted? These are the kind of issues that will arise:
  - What are the qualifications for network access?
  - Who grants access and manages user accounts?
  - What is the process for signing up or withdrawing?
  - Can access be terminated by the network or by the community?
  - What are the privacy terms and the terms of use for data sharing?
  - Does personal identity need to be disclosed? If so, how is it authenticated?
  - What is the process for raising and handling disputes?
  - Is there a reputation system which rates the users?
  - What are the users' rights and responsibilities?
  - What are the users' decision making or voting powers?

<sup>34</sup> The two well-known examples include the forks which led to Bitcoin Cash (BCH) and Ethereum Classic (ETC).

<sup>35</sup> Accidental and transient forks may occur in cases where two miners find a block at about the same time. Such forks are resolved when miners abandon (and orphan) the blocks which are not part of the longest chain.

- **Rights and responsibilities.** What are the rights and responsibilities of network participants and users? Are there different roles for different parties? Is there some mechanism (e.g. a reputation system) which modulates the influence of the participants? What is the software license for the codebase?
- **Privacy.** Are protocol stakeholders identified or can they remain anonymous? Will a user or a participant need to reveal their identity in order to participate in governance? Are there privacy practises or laws which are imposed by a nation state?
- **Content moderation.** There are P2P networks which allow users to record (with a hash) some digital content in a blockchain or distribute it to others. Given that such content (data, documents, pictures, videos, music, etc.) may contain illegal, pirated or offensive material, should it be moderated? If so, exactly how? Is there a ranking system maintained by network users? Or should the content be left well alone?
- **Use of revenue.** If the use of protocol in a decentralized network results in accrued funds (e.g. tokens collected via a transaction tax), how is that revenue spent? Is it distributed to network participants? Or is it used to fund further technical development? What are the precise rules which govern the use of revenue?
- **Governance model.** Ultimately, adopting a governance model or changing the model are valid targets of governance.

### The degree of decentralization

It can be non-trivial to assess the actual degree of (de)centralization. Sometimes the call is easy: If the power is in the hands of a foundation or a corporation, the governance is centralized. But what about a technocracy where the core team holds the power? Is it centralized because there's one team whose membership rarely changes? Or is it decentralized because there's, say, a dozen decision makers? Or consider a ledger with a delegated proof-of-stake mechanism: It can appear to be a decentralized solution, but in practise decisions may be driven by a small number of wealthy token holders.

If we take this line of thought still further, who is to say that an oligarchy or plutocracy is centralized? If we had to think of a technical definition, the obvious one would equate decentralization with the absence of any one actor who can dictate decisions. So is a system with two or three or more decision makers with genuine power decentralized? Or is it perhaps a wider community involvement that we really have in mind when we speak about decentralization?

The reality is that there are many dimensions of decentralization, such as the distribution of mining activity, the contributions to the codebase, trading activity in crypto exchanges, the ownership and geographic distribution of network nodes, and the concentration of token ownership. One possible method of measurement involves the calculation of a Gini coefficient in any of these dimensions. Srinivasan and Lee (2017) have suggested a *Nakamoto index*, calculated as the minimum number of entities which is required to achieve more than 50% of the total of the quantity of interest (*Satoshi index* is the normalised version expressed as a percentage).

Many other indicators are possible, and the proper measurement of decentralization is really a topic for a separate paper. There is a large body of existing research in graph theory which should prove helpful. There are indices such as degree, closeness, betweenness, eigenvector centrality etc. Such analytics were first developed for social networks, but similar methods have been successfully applied to the analysis of computer or transportation networks and the spread of diseases. Centrality indices can identify the most important vertices in a graph, but their accuracy can be highly dependent on network topology. There is an interesting dual approach which seeks to quantify the role of individual nodes with various kinds of influence metrics.

Kwon et al. (2019) show that full decentralization is theoretically impossible without a trusted third party and reliable identity management, unless the protocol can impose a *Sybil cost* (i.e. the condition where the cost for one participant running multiple nodes is greater than the total cost for multiple participants each running one node). Their analysis involves consensus mechanisms, but the results may apply to governance models as well.

As mentioned, blockchains can be viewed as a form of a digital commons heavily based on open-source code. Schweik and English (2013) carried out a five-year empirical study and found that as FOSS projects grow, they tend to move away from unstructured collaboration and towards formalized systems of governance. Based on network analysis of online music production communities, the analysis by Wang and Cheliotis (2016) indicates that the introduction of formal structure can lead to more decentralized engagement. Conversely, the lack of structure can result in a higher

degree of centralization as a small number of participants emerge as community leaders. To the extent that such results carry over to the blockchain context, a formal decision making structure may be a necessary (while not sufficient) precondition for decentralized governance.

There are very few studies about the actual degree of decentralization in the governance of blockchain systems to date, probably because good data is hard to find. In the case of Bitcoin and Ethereum, Azouvi et al. (2019) looked at the number of developers contributing to the codebase in Github and the number of people involved in discussions. Centrality metrics suggest that both Bitcoin and Ethereum are fairly concentrated as far contributions to the code repositories are concerned, and generally only a handful of people are in the habit of participating in online discussions.

Tools such as Alethio and Etherscan<sup>36</sup> can be useful in quantifying and visualising the concentration in decentralized networks. On Ethereum, there is exploratory research by ConsenSys on issues such as the dispersion of token ownership, the concentration of wealth, and the influence of mining pools. What Muzzy and Anderson (2019) found, for instance, is that in 2019 four main pools accounted for over 72% of quarterly block production, and there were only two pools which together paid out to nearly 70% of the miners. Ethereum nodes appear to be geographically well diversified, though.

### Off-chain vs. on-chain governance

Blockchain technology — such as smart contracts and token curated registries — opens up novel possibilities in governance. In principle, you can now implement various decision processes in computer code, on-chain, if you will.

Tezos is an example of a blockchain with on-chain governance (Arluck, 2019). In Tezos, anyone can propose a change in network parameters in the form of a code update. If the proposal is accepted in on-chain voting by miners (called ‘bakers’ in Tezos), the code becomes active in a test network. The new code is run for a period of time. If no problems arise and the proposal is confirmed in a second vote, the code is automatically implemented in the main network.

With on-chain governance, structures such as Decentralized Autonomous Organisations (DAOs) are now possible. DAO is an entity where the rules of governance are hard-coded as a collection of smart contracts, and executed when required<sup>37</sup>. In other words, a DAO is an organisation where humans or other entities interact via a protocol encoded as a computer program. Blockchains which are mentioned as being DAOs<sup>38</sup> include Dash, Decred, and MakerDAO.

As an example of what on-chain can accomplish, let’s recall that many decentralized systems which can be viewed as digital commons. As discussed by Red (2019), blockchains have one advantage compared to other common pool resources: They allow for the enforcement of network rules at a minimal expense. Cryptography is key to this capacity, because it makes it much easier for defenders to verify the authenticity of information than it is for attackers to introduce corrupt information. For instance, there might be an agreed rule to limit the bandwidth consumed by any network participant. Bandwidth usage could be measured and overuse automatically penalised by a smart contract.

The implementation of decisions by a DAO often requires some off-chain action. For instance, an agreed resolution may necessitate a software upgrade by each node in a network, and those nodes are operated by people. A DAO may need other services. Whilst some services can be handled by decentralized apps, work can be also carried out by community members, other professionals, or third-party companies. Digital payments for the services are released by the smart contracts when the conditions for doing so are satisfied.

As one of the strengths of blockchain technology is the ability to prove the ownership of assets and enable secure digital transfers, a decentralized ledger is a natural habitat for a DAO. However, the fact that funds are controlled by code makes a DAO vulnerable. If code changes take effect automatically after on-line voting, a coalition of whales<sup>39</sup> with nefarious motives could, in principle, approve a take-over of funds in a DAO (Zoltu, 2019).

There are platforms (Kronovet, 2019) which facilitate the creation of a DAO, including Aragon, DAOstack, Colony, and MetaCartel. Each of these platforms comes with different features and a somewhat distinct philosophy. Aragon, for instance, is agnostic about the decision making model, and offers a permissioning system and a scripting language which can be used to build a new organisation by connecting different modules together. In Colony, a proposal gets

<sup>36</sup> See <https://public.tableau.com/profile/alethio#!/> and <https://etherscan.io/>, respectively.

<sup>37</sup> Daniel Larimer (2013) first proposed the concept, and Ethereum made the idea feasible a bit later.

<sup>38</sup> Pure DAOs are hard to find. There often seems to be some third party or entity which holds the ultimate power or the veto.

<sup>39</sup> In the crypto space, a “whale” is an individual or entity who owns a significant amount of tokens.

funded faster if it is backed by better reputation (Mannan, 2018). DAOstack incorporates a prediction market where bets can be placed on a proposal being accepted or not (this forces the participants to focus their attention). In Moloch (an Ethereum community funding initiative), proposals are considered in sequence with a single proposal in scope at any one time. Any prospective member must offer a sacrifice to Moloch in the form of either some useful work or additional funds, and the existing members vote, on-chain, on his or her fate (the fate as to admission, that is).

Taking governance on-chain or setting up a DAO does not necessarily make governance easier. As a brief summary, these are some of the issues which will arise.

- Who can participate in decision making and raise initiatives?
- What is the process of raising new initiatives?
- How are preferences aggregated and different viewpoints reconciled?
- If voting is used, what is the process, the quorum, and the acceptance threshold?
- What are the governing bodies?
- Is there some sort of separation of powers?
- What is the dispute resolution mechanism?
- Does the DAO implement a legally binding contract?
- What are the incentives for participation in governance?
- What is the process for amending the code if the DAO needs to adapt?

On-chain governance does not imply decentralization. A DAO can implement pretty much any governance model, including autocracy, oligarchy, meritocracy, or some community-oriented system. In other words, the degree of decentralization and the degree of human involvement (i.e. on-chain vs. off-chain) are two distinct dimensions. Any governance model can be characterised by where it fits in the space which those dimensions span. The point is well made in a blog post by Smits (2018):

“There are two sets of models: centralized vs. decentralized and on-chain vs. off-chain. The first duel is the classic blockchain paradox which calls into question contemporary authority structures. The second refers to human involvement and the extent to which decision making processes are automated.”

In any case, the true decision makers are necessarily off-chain entities. We are not aware of any sentient being which lives in a purely digital realm.

### Legal issues

Decentralized networks do not exist in isolation. Regardless of the governance model, they are likely to fall under the jurisdiction of one or more nation states, and legislators, regulators and tax authorities will take an interest. Even if you were in full agreement with the laws of one domicile, there are other nations where the laws will be different. It's in practise impossible to be in line with up to 200 or more different sets of often contradictory laws.

There is a degree of arbitrariness about the relevant jurisdiction. A controlling entity may be based in one country, but network nodes and users may be found in many different countries. If needed, therefore, courts or arbitrators will simply decide which governing law applies. On the other hand, if users and transacting parties make an explicit choice of the governing law, most courts would respect that choice, assuming it is properly formulated and recorded. The stakeholders would, presumably, choose a jurisdiction and legal system which minimally interferes with the operations of decentralized networks.

In on-chain governance or a DAO, the decision processes and rules are written in computer code. The good thing about code is that it is unambiguous, deterministic and transparent, and there is no room for interpretation. In time, the widespread deployment of self-executed, autonomous contractual code may even lead to blockchain law, a subset of law which has been dubbed *lex cryptographia* by Wright and de Filippi (2015).

The problem is the fact that any formal rules will be incomplete. A smart contract assumes that the incentives are financial and the counterparties are rational. These assumptions may not always hold, and there will be situations which are not covered by the code. In any case, how do you settle claims in code between parties who have valid arguments based on ethics and natural justice? State power and decentralisation don't always go hand in hand when a network challenges the status quo (Malik, 2019).

These kinds of considerations lead to the question of whether an on-chain governance model should in fact aim for a legal contract (Sanitt, 2018). It is not yet clear if smart contracts, DAOs and other decentralized constructs are ready for recognition by law (Herian, 2018). A binding contract with a choice of the governing law would help to minimise conflict between a multitude of national laws, and an arbitration clause would serve to establish a dispute resolution mechanism.

At present, DAOs are not legal entities anywhere that we know of<sup>40</sup>. You can, of course, register a DAO as a corporation and thereby gain the protection offered by an established legal structure, along with all the corresponding duties and obligations. But is a DAO controlled by a limited company a true DAO any more?

There is also an interesting question of who — if anyone — owns a DAO. When a DAO is created, tokens may be issued, and those tokens may allow their holder some voting power. But unless the tokens are created in a *security token offering* (STO) or a similar framework, they do not give the token owner any legal claim of ownership. Or does a DAO own itself?

In some sense, DAOs are similar to *labor managed firms* (LMFs). In a LMF, the suppliers of labour — rather than the suppliers of capital — hold the ultimate power, including the right to hire or dismiss executives. There is a related concept of *steward-ownership* where the profits are a means to an end, and the company is controlled by the employees and the people who hold active roles in it (Makkone, 2018). This is not a fringe idea; there are giant companies like John Lewis, Zeiss and Bosch which function this way.

Arbitration, in itself, is a widely accepted and mature form of dispute resolution outside the court system, and it neatly sidesteps the incompleteness of a governance model. There are protocols which are emerging as possible forums for blockchain arbitration, including Aragon, Jur, Kleros, Mattereum, and Oath.

In order to create a contract, the document with the agreed rules can be hashed and saved in a blockchain with the hash included in any subsequent transaction. If you take this line of thought further, you can incorporate the constitution in the network terms of service. If a user cryptographically signs the terms, the contract will have a good chance of standing in a court of law.

## Coordination

A coordination mechanism is an essential part of governance. Without cooperation and coordination, it is difficult to avoid conflict, resolve disputes, allocate work, and manage resources in a community or a society.

If you have a limited number of decision makers or a relatively small core group of developers, you can simply talk to one another and try to reach a consensus. There can of course be different formal steps in that process, such as forums and mailing lists and either remote or face-to-face meetings.

There are well-known networks (including Bitcoin and Ethereum) where the coordination relies on the achievement of consensus within a group of core developers or some other inner circle. There is usually a well-defined process for dealing with improvement proposals, i.e. with suggested changes to the codebase or network parameters. This is what typically happens in such a process:

1. A contributor comes up with an idea of how to amend or upgrade the network. He or she writes a proposal and posts it to GitHub or some other agreed repository.
2. A debate takes place in developer meetings, via teleconferencing, in community channels, online forums or mailing lists.

<sup>40</sup> Whilst a DAO may not be a legal person, it may still be a taxable entity. See Shakow (2018).

3. Core developers review the proposal, provide feedback, discuss the pros and cons, consider the risks, and aim for off-chain consensus.
4. A decision is made. The proposal is likely to be approved if the proposal is technically viable, funding is available, and consensus is reached.
5. The change is implemented. In some networks, the core developers will put the upgrade in place; in others (such as Bitcoin), the upgrade needs implementation by the majority of miners.

There are other coordination mechanisms made possible by blockchain technology. A token curated registry (TCR) can be used to maintain dynamic and high-quality lists (Goldin, 2017). Anyone can propose adding an item to the list, but the proposal must be backed by a stake of tokens. The stake can be forfeited if successfully challenged (Tabarrok, 2018).

TCR incentivises the participants to pool their knowledge with an immediate payout for taking part in curation and a longer-term reward if the embedded knowledge results in token price appreciation. The effectiveness of a TCR can be analysed from a game-theoretic viewpoint<sup>41</sup>. Depending on the parameters, coordination may well happen, but truth-telling is not necessarily the dominant strategy. A curation market resembles a Keynesian beauty contest where those players win who best predict the others' choices up to the  $n$ 'th degree. The outcome may turn out to be a focal (Schelling) point, and it may or may not be the optimal choice.

Curation markets can be used to maintain simple whitelists or blacklists. AdChain, for instance, seeks to maintain a list of non-fraudulent publisher domain names and webpages. A similar mechanism could be applied to quality assessment for data content, and even to the identification and approval of new features or improvement proposals in open-source projects.

### Voting mechanisms

Voting is another widely used method of aggregating preferences. Regardless of whether voting takes place on-chain or off-chain, there are a number of options and parameters. In a decentralized network, token holders, network users or the operators of network nodes are possible members of the electorate. These are some of the possibilities for the electoral system:

- **Equally weighted voting** is used in almost all national and local political elections. In decentralized networks, this principle translates to one vote per one token holder, or one vote per an infrastructure operator, as the case may be.
- **Weighted voting** is a system where the number of votes held by any one person or entity depends on some quantifiable metric.
  - In a plutocracy, the weight is proportional to the number of tokens at stake by each voter. Any monotonic and increasing function of the stake works, too. In principle, the weighting scheme can be regressive so that voting power saturates at higher levels of wealth.
  - As an example of a regressive weighting scheme, Saga uses a balanced voting system (Man et al., 2019). The aim is to take into account the interests of those with large amounts of tokens as well as those with lesser holdings but who add value as members of a bigger community. The voting power is a weighted average of stake-based voting and equal-weighted voting, with the Gini coefficient used as the weighting factor.

For instance, if there are 1 million users (fish, if you will) with 100 tokens each and 12 whales with 100 million tokens each, a stake-based system would translate to a plutocracy with whales (as a group) holding 55% of the voting power. In equal-weighted voting, the whales would hold a miniscule amount of power. In balanced voting<sup>42</sup>, the whales (as a group) would hold 25% of the voting power. Their views would count, but they would be unable to dictate decisions.

---

<sup>41</sup> A useful first step towards a game-theoretic analysis (even if it ignores any long-term rewards from token appreciation) has been taken by Asgaonkar and Krishnamachari (2018).

<sup>42</sup> In this case, the Gini coefficient is approximately 0.545.



- The weight can be proportional to accumulated gas<sup>43</sup> spent by each voter. This kind of weighting scheme favours established, long-term users at the expense of newcomers. The longevity of a node or of the network user are possible alternative metrics. A reputation management system<sup>44</sup> can be used to update the voting power, reward users or nodes in good standing and punish misbehaviour.
- In **delegated voting** and in liquid democracy, the electorate (e.g. all token holders) chooses a much smaller number of representatives who make decisions on their behalf<sup>45</sup>. If the idea is that the delegates are those who best understand the technology, then the governance model becomes one of meritocracy or a technocracy. In many PoS and DPoS protocols, the staked nodes can vote on governance decisions.
- In **quadratic voting** (Lalley and Weyl, 2018), a voter can apply more than one vote to an alternative, but the marginal cost increases at each step (so that the second vote would require 4 credits, the third 9 credits and so on). The intuition is that the more you value something, the more you should be willing to spend on the marginal vote.

The effect of quadratic voting can be similar to balanced voting (see above for the use of the Gini coefficient to adjust voters' influence). Broadly supported initiatives are favoured, and wealthy individuals cannot easily dominate the outcome.

The idea has been extended to **quadratic funding** (Buterin et al., 2018) where the funding allocated to a public goods project is proportional to the square of the sum of the square roots of all the contributions received. Quadratic funding is used in GitCoin, a bounty platform for open source code on the Ethereum blockchain.

- **Score voting** is a mechanism where each voter attaches a numerical score to some (but not necessarily all) alternatives. There may be a budget constraint, i.e. a fixed number of credits that each voter can distribute. Eximchain is an example of a ledger which combines score voting and quadratic voting.
- **Federated voting** is an interesting voting mechanism which can also be used as a consensus algorithm. In a round of federated voting, the nodes exchange messages until each node can confirm that there is a local quorum which is happy with the same alternative. If the nodes follow the protocol over successive rounds, the quorum (assuming some technical conditions hold) keeps expanding until all nodes agree. This procedure is called Federated Byzantine Agreement (FBA), and it is a key part in the consensus protocol in Ripple, Stellar and Tixl. We see no obstacle, in principle, for wider application.

Although voting is usually associated with democracy, it can be equally well used in an oligarchy or plutocracy, or in fact in any meeting or group. Voting is simply a mechanism to elicit a decision and has no value in itself. You can have good governance without voting and bad governance with voting. There is no point in putting every decision up for a vote. As pointed out by Sheng (2018), having the community participate in largely symbolic votes on trivial topics does not equate to decentralized governance or genuine community involvement.

## Digital voting

Most elections in the physical world use paper ballots, even if the tallying is often done with computers. Since the 1960's, on-site electronic voting has been used in many countries. The next step is remote electronic voting (via the Internet), and it is being used in Estonia and in many cantons in Switzerland. A blockchain-based system has been trialled in Zug (Allen, 2018).

Remote voting brings in potential advantages in the form of lower costs, faster counting, more convenience (and hence better turnout) and ease of access by those living overseas. On the other hand, electronic voting can exacerbate the potential for election fraud. Deterrence measures that work in the physical world do not easily carry over to online voting. Weak encryption or software bugs can make the system vulnerable to manipulation remotely and on a massive scale.

<sup>43</sup> "Gas" is the transaction cost for token transfers or for the execution of smart contract code in a blockchain.

<sup>44</sup> Designing a good reputation system is a research question in its own right. Algorithms do exist; see e.g. Kamvar et al. (2003).

<sup>45</sup> In on-chain voting, tokens are locked down for the duration of the voting. As an incentive for long-term thinking, it is also possible to give a greater say to stakeholders who stake their tokens for a longer period. This is what e.g. MakerDAO does.

Voter coercion can take many forms, such as influence by third parties, vote buying, voter reprisals, etc. Two things are needed in order to digitally replicate the off-chain ideals of a fair ballot: Verifiability and confidentiality. Verifiability covers issues such as reliably checking voter eligibility, proving that votes are faithfully recorded and the results correctly added up. Confidentiality translates to ballot secrecy so that a vote cannot be associated with the voter's real-life identity, wallet address, or some other traceable identifier.

Cryptography can help achieve confidentiality in digital ballots (Chaum et al., 2010). Possible techniques include *mix networks* (a set of tabulation servers which run a mixnet over encrypted votes, resulting in random permutation of votes before counting), *homomorphic encryption* (where a server adds up all the encrypted votes and decrypts the result so that individual votes are never decrypted), and *blind signatures* (a commutative blinding operation where an authorisation server does not know what they digitally signed).

Blockchains with their immutable audit trails may seem like an obvious choice for a digital election platform<sup>46</sup>. However, blockchain technology can make life easier for those bent on ballot manipulation<sup>47</sup>. With a certain fluency in programming and cryptography, you can create an automated marketplace to buy votes, and a smart contract can verify that you got what you paid for before compensating the sellers. In contrast to the physical world, anyone involved has much less of a risk of getting caught.

In order to prevent vote buying, a digital voting system must be unable to provide proof (cryptographic or otherwise) of which way a vote was cast. If you cannot prove which box you ticked, then an attacker cannot credibly dictate your choices. In liquid democracy, though, you need that very capability: A delegate needs the ability to prove to original vote holders how they voted.

Delegated voting systems — as used in most DPoS blockchains — are vulnerable to mischief yet in other ways. For instance, a cartel of block producers can collude to blacklist accounts which threaten their profitable positions. Or a coalition of nodes may vote for another to maintain their power.

A plutocracy can bias voting results. As a real-life example, a system parameter in MakerDAO (DAI stability fee) was adjusted in October 2019 in an on-chain vote. The outcome cannot be described as a result of community consensus. A single individual (who at that time owned 7.5% of the token supply) decided the election with 94% of the vote (Onggunhao, 2019).

It is difficult to find comprehensive data on participation in on-chain ballots, but the evidence suggests that not many token holders bother to take part (Learner, 2019). There are many cases where turnout has fallen below 10%, although there have been positive outliers (e.g. Decred Politeia #Pi4 at 32%, Cosmos Proposal 1 at 38%, Tezos Athens at 50% or above, and Decred Lightning at 54%). The presence of whales can significantly skew these numbers, and the turnout can fall dramatically if measured in terms of participating wallet addresses.

There are ways to encourage community participation. For instance, a network can automatically maintain a reputation score for each user and adjust users' influence in governance in line with their score. Token holders can be incentivised to vote via staking rewards or by redistribution of tokens among those who participated. As a counter-argument, people are not paid to vote in political elections<sup>48</sup>. Those who truly care about what happens to their country or society will take part in the debate, cast a vote and participate in other ways.

In one-person-one-vote systems, the very anonymity of blockchains can be an obstacle to fair voting. In a Sybil attack,<sup>49</sup> a malicious party can gain disproportionate influence by creating a large number of fake identities or addresses which appear to be genuine. This poses a dilemma. Because you want to keep the ballot secret, you don't want to know the voters' identities. On the other hand, you also want to make sure that nobody can vote more than once.

One way to create a coercion resistant voting mechanism is to authenticate each voter but keep the authentication mechanism separate from the actual (digital) voting ticket. Once authenticated, a voter is given a unique digital token (a pair of private and public cryptographic keys) as well as a list of addresses which represent the alternatives on the

---

<sup>46</sup> There is already at least one commercial online voting system on the market, Polys by Kaspersky, see <https://polys.me/>.

<sup>47</sup> See Daian et al. (2018) for an analysis of how on-chain vote-buying could work and what can be done to prevent it.

<sup>48</sup> There are countries where you are fined (or worse) if you don't cast a vote when asked to do so. In decentralized systems, obligatory voting is not seen as good practise.

<sup>49</sup> This type of attack is named after a psychological case study of Sybil Dorsett (a pseudonym for the late Shirley Ardell Mason). She was a woman with dissociative identity disorder, manifested in her sixteen different (albeit timewise consecutive) personalities.

ballot. Tokens are generated by a trusted third party or by a secure decentralized mechanism so that they are not traceable to voter identity. In the tallying phase, tokens are validated blindly (using a mixnet, for instance) against the original voter roll. This is the essence of coercion resistant remote voting systems such as Civitas (Clarkson et al., 2008) is based on a voting scheme by Juels et al. (2005).

There are different ways to authenticate voters. For instance, you could verify the real-life identity with facial recognition software which compares identity documents to a photograph or video of the face. However, the technology can be expensive and unreliable, and you would need to trust whomever provides the verification service. Another possibility is to use the address of a token wallet as identity. This option is not foolproof: It depends on the secure storage of a single piece of information (the private key), and there's no ballot secrecy (anyone can find out how all the others voted)<sup>50</sup>. Privacy can be elusive because the wallet address and token balance are visible in the blockchain. If the wallet can be linked with an IP address, email address, or a phone number, it can be fairly easily traced back to an individual.

A digital identity (DID) is emerging as a possible solution to privacy concerns. In Estonia, for instance, every citizen has a state-issued DID which can be used for access to government services via a digital signature. In elections, the identity is authenticated remotely using an ID card with an electronic chip. However, the security of the system has been rightly criticized (Heiberg and Willemson, 2014).

Self-sovereign identity (SSI) combines a digital identity with blockchain technology. The idea is that an individual can selectively disclose only the required attributes about their person and identity as and when needed. A trusted verifier cryptographically checks with the issuing authority (such as the government) that the disclosed information is valid and in force. This is done with a zero-knowledge proof so that the verifier never sees the original documents (e.g. an ePassport) or any unrelated information (i.e. attributes which are not relevant for the purpose at hand).

The aim of SSI is to have each individual own and control their identity. However, the technology is not quite there yet; industry standards are still evolving and integrations to the national public key infrastructure are lacking. This is an active area of experimentation, though, and potential solutions such as Blockpass, Circles, Civic, HumanityDAO, Sovrin, uPort, and others are in tight competition for market share.

We do not have evidence that Sybil attacks, vote buying, voter coercion, collusion or other kinds of shenanigans are actually taking place in on-chain elections. But underhand practises are possible, and the risk must be taken into account in the design and implementation of on-chain governance models.

### What is good governance in decentralized networks?

Given the multitude of possible models, the obvious question arises as to what constitutes good governance. The answer obviously depends on the network, its purpose, and the culture of the community. Good governance can be understood as a model (consisting of rules, processes and institutions) which fulfills the interests and satisfies the preferences of stakeholders.

As discussed, having a well-defined structure is important. If there are no institutions and no transparency about governance processes, those in the know may be tempted to use the system to their own advantage. As part of the structure, the separation of powers is a useful safeguard against misbehaviour. The concept of *trias politica* may not carry over neatly to the decentralized space, but something similar is worth considering.

Dispute resolution will be needed sooner or later; conflict between stakeholders is unavoidable. A good governance model provides a framework for resolving disputes peacefully and reduces the risk of community split. It is best to have an agreed process reconciling different viewpoints in place ahead of the time when it might be required. For

<sup>50</sup> There are election protocols such as the Open Vote Network (OVN) which can guarantee privacy (Hao et al., 2010). The computational cost is of the order  $O(n)$  where  $n$  is the number of voters. This may work for small communities, but better algorithms are needed to make such protocols practical for even a medium-size electorate.

instance, the mechanism might allow the community to disband the executive and trigger a re-election, similar to a vote of no-confidence in political systems.

Enforcement of stakeholders' compliance with the rules is needed. An unpermissioned decentralized network is a common resource, and monitoring is essential both to prevent abuse and to share rewards in an equitable fashion. Cryptography and on-chain mechanisms can be used to automate this function by e.g. penalising excess resource usage or by distributing micropayments against verified work.

Incentives are important for network operations as well as its governance. There are economic, social, moral, and psychological. Social incentives work well in smaller groups of people (such as the core developers) where members are in frequent or face-to-face contact with one another. Developers can also be motivated by social recognition for their contributions and from pure enjoyment from working on the project<sup>51</sup>. But developers will not survive on recognition alone: They also need to get paid.

Coordination is an essential part of functional governance. This includes the aggregation of different preferences and efficient allocation of resources either by a consensus-seeking process or by other means. Consensus-seeking processes may work well when the true decision making group is small. If the views of the wider community are to be aggregated and reconciled, voting is a practical alternative.

A constitution has been found to be a useful device as a transparent foundation of organisations and political entities. Having a constitution as the basis of governance is an equally good idea in the decentralized space. The community, in effect, self-selects a group of people. The cultural element of the constitution may therefore emerge naturally from the history of the project, and it may incorporate values such as privacy, freedom, self-sovereignty, transparency, and democracy. There are already networks with a constitution, charter, manifesto, or byelaws already either in place or in development. These include projects such as Aragon (2018), Civil (2018), Decred (2019), and Saga (2020). More are likely to follow.

It is a good idea to get to know the thinking in the community as to project governance. Regular interaction in online forums and offline events obviously helps, but formal surveys can be useful too. A governance survey was carried out recently in the Ethereum community (Beylin, 2019). Similar efforts in other protocols would be welcome.

In the Ethereum survey, 70% of respondents were token holders. Some 24% were developers, 15% investors, 12% researchers, and 5% miners or stakers. About 90% were aware of the vision and agreed with it. Participation was fairly active, with 71% having taken part in community polls, 57% in various discussions, and somewhat fewer in EIP submissions and core developer meetings. As a group, core developers were fairly highly trusted to do the right thing in the best interests of the project.

Some 46% favoured direct democracy and 32% representative democracy as the governance model (these numbers are, of course, in direct contradiction with how Ethereum is actually governed). Only 35% had participated in online voting, citing the lack of trust and the technical difficulty as reasons (the lack of good UX continues to be an Achilles heel in this space). Several targets for improvement were raised: Better access to information, broadening the community outside the early adopters, more competition and collaboration, and higher accountability.

While these numbers may be biased due to the sample size (282 respondents) and self-selection (those most in line with a decentralized vision are the most likely to respond), the results are still interesting.

Legitimacy is a broad and perhaps ill-defined term, but it is safe to say that the process and community participation matters. Community involvement can take different forms such as taking part in debates, contributing to the codebase, helping with testing and bug reporting, developing applications, standing up as community representatives, and voting for improvement proposals and other initiatives. If on-chain governance is the aim, it is useful to remember that not everyone will be technologically savvy enough to take part.

---

<sup>51</sup> Lakhani and Wolf (2005) surveyed 684 software developers in 287 FOSS projects. They found that intrinsic motivation, i.e. the enjoyment from working on the project, was the strongest motivator.

Ultimately, community members should genuinely believe that the model is in a sense “right”, in line with their values, and serves their interests. In the decentralized space, there’s always a potential for mutiny. If the governance model does not allow sufficient means for conflict resolution, the community can always revolt, do a hard fork and create a parallel network. The threat of forking is a powerful check for poor governance<sup>52</sup>.

Finally, we should be humble and acknowledge that what works today may not work in the future. There’s going to be technological innovations, business models will need tinkering, and experimentation will be required. Good governance allows the network to adapt when the environment changes. In the extreme, the governance model itself may need to be amended or replaced to make adaptation possible.

## 4. Conclusion

This paper is a review of governance issues in decentralized networks. Our motivation is a view that effective and legitimate governance is paramount for long-term viability of such systems. And if you are thinking ahead to the next stage of network governance, it is useful to be aware of the previous research, the successes and failures of different governance models, and the relevant tools and institutions.

In the long term, a decentralized network can only be sustained if there is an incentive compatible structure in place. One objective of governance can be a creation of a model where participants contribute to common goals even when they act in their own interests. The incentive structure is related to the monetary policy and token economics in the network, and its design is a non-trivial problem in its own right.

Decentralized technology enables the implementation of governance models in ways which were simply not feasible five or ten years ago. On-chain voting is now possible, and there are new building blocks such as token curated registries. New kinds of entities such as decentralized autonomous organisations (DAOs) are now possible, with the rules of governance coded as automatically executed computer programs. There are possible advantages to on-chain governance in the form of transparency and an audit trail.

A governance model should not be confused with its implementation. A decentralized network can have off-chain governance, and a non-blockchain-system can have on-chain governance. DAOs and their variants are simply tools, and they do not solve any of the underlying issues by themselves. On-chain governance does not remove the need for human input, informed debate and consensus-building. The ultimate decision makers are still human beings with sometimes conflicting interests.

---

<sup>52</sup> For an analysis of blockchain governance in the light of different theories of the social contract, see Reijers et al. (2016).

## References

Aidt, Toke, Zareh Asatryan, Lusine Badalyan, and Friedrich Heinemann (2015): "Vote Buying or (Political) Business (Cycles) as Usual?", ZEW - Centre for European Economic Research, Discussion Paper No. 15-017.

Allen, Matthew (2018): "Swiss blockchain voting platform begins trial". Retrieved on May 16, 2020 from [https://www.swissinfo.ch/eng/crypto-valley\\_swiss-blockchain-voting-platform-begins-trial/44215246](https://www.swissinfo.ch/eng/crypto-valley_swiss-blockchain-voting-platform-begins-trial/44215246).

Aragon (2018): "AGP-0: The Aragon Manifesto". Retrieved on May 16, 2020 from <https://github.com/aragon/AGPs/blob/master/AGPs/AGP-0.md>.

Arluck, Jacob (2019): "Jacob Arluck · Reflecting on Athens, the first self-amendment of Tezos". Retrieved on May 16, 2020 from <https://medium.com/p/4791ab3b1de1>.

Arrow, Kenneth J. (1950): "A Difficulty in the Concept of Social Welfare", Journal of Political Economy, vol. 58(4), pp. 328–346.

Arvidsson, A., Caliandro, A., Cossu, A., Deka, M., Gandini, A., Luise, V., & Anselmi, G. (2017): "Commons based peer production in the information economy". Retrieved on May 20, 2020 from [https://www.academia.edu/29210209/Commons\\_Based\\_Peer\\_Production\\_in\\_the\\_Information\\_Economy](https://www.academia.edu/29210209/Commons_Based_Peer_Production_in_the_Information_Economy).

Asgaonkar, Aditya and Bhaskar Krishnamachari (2018): "Token Curated Registries - A Game Theoretic Approach". Available at <https://arxiv.org/abs/1809.01756v1>.

Atzori, Marcella (2017): "Blockchain technology and decentralized governance: Is the state still necessary?", Journal of Governance and Regulation, vol. 6(1), pp. 45-62.

Azouvi, Sarah, Mary Maller and Sarah Meiklejohn (2019): "Egalitarian Society or Benevolent Dictatorship: The State of Cryptocurrency Governance", in: A. Zohar et al. (eds.), "Financial Cryptography and Data Security", FC 2018, Lecture Notes in Computer Science, vol 10958, pp. 127-143. Springer, Berlin, Heidelberg.

Beck, Roman, Christoph Müller-Bloch, and John Leslie King (2018): "Governance in the Blockchain Economy: A Framework and Research Agenda", Journal of the Association for Information Systems, vol 19(10), pp. 1020-1034.

Bell, Stephen (2002): "Economic Governance and Institutional Dynamics". Oxford University Press.

Benkler, Yochai (2006): "The wealth of networks". Yale University Press.

Bernstein, Ethan, John Bunch, Niko Canner and Michael Lee (2016): "Beyond the Holacracy Hype: The Overwrought Claims—and Actual Promise—of the Next Generation of Self-Managed Teams", Harvard Business Review, vol. 94, July–August, pp. 38-49.

Beylin, Eva (2019): "Ethereum Governance Survey Results". Retrieved on May 16, 2020 from <https://medium.com/p/c67c11695f2a>.

Boehm, Christopher (1993): "Egalitarian Behavior and Reverse Dominance Hierarchy", Current Anthropology, vol. 34 (3), pp. 227–254.

Borak, Masha (2018): "Qihoo 360 discovers high-risk security issues in EOS, says 80% digital wallets have problems". Retrieved on May 16, 2020 from <https://technode.com/2018/05/29/qihoo-360-security-issues-eos/>.

Buterin, Vitalik (2014): "An Introduction to Futarchy". Retrieved on May 16, 2020 from <https://blog.ethereum.org/2014/08/21/introduction-futarchy/>.

Buterin, Vitalik, Zoë Hitzig, and E. Glen Weyl (2018): "Liberal Radicalism: A Flexible Design For Philanthropic Matching Funds". Available at <https://ssrn.com/abstract=3243656>

Canellis, David (2018): "Hacker exploits EOS smart contract to steal \$200K from gambling app". Retrieved on May 16, 2020 from <https://thenextweb.com/hardfork/2018/09/14/eos-gambling-app-hacked>.

Carter, Nic (2017): "A Cross-Sectional Overview of Cryptoasset Governance and Implications for Investors", M.Sc. thesis, University of Edinburgh Business School.

Chaum, David, Markus Jakobsson, Ronald Rivest, Peter Ryan, Josh Benaloh, Miroslav Kutylowski, and Ben Adida (2010, eds.): "Towards Trustworthy Elections: New Directions in Electronic Voting". Springer.

Civil (2018): The constitution. Retrieved on May 16, 2020 from <https://learn.civil.co/constitution/>.

Clarkson, Michael, Stephen Chong, and Andrew Myers (2008): "Civitas: Toward a Secure Voting System", IEEE Symposium on Security and Privacy, pp. 354-368.

Coase, Ronald H. (1937): "The Nature of the Firm", *Economica*, vol. 4(16), pp. 386-405.

Daian, Philip, Tyler Kell, Ian Miers, and Ari Juels (2018): "On-Chain Vote Buying and the Rise of Dark DAOs", Retrieved on May 16, 2020 from <https://hackingdistributed.com/2018/07/02/on-chain-vote-buying/>.

Davidson, Sinclair, Primavera De Filippi and Jason Potts (2016): "Economics of Blockchain", Public Choice Conference, Fort Lauderdale, United States.

Decred (2019): The constitution. Retrieved on May 16, 2020 from <https://docs.decred.org/governance/decred-constitution/>.

de Filippi, Primavera and Benjamin Loveluck (2016): "The invisible politics of Bitcoin: governance crisis of a decentralized infrastructure", *Internet Policy Review*, vol. 5(3), pp. 1-28.

de Filippi, Primavera and Greg McMullen (2018): "Governance of blockchain systems: Governance of and by Distributed Infrastructure", research report, Blockchain Research Institute and COALA.

de Laat, P.B. (2007): "Governance of open source software: state of the art", *Journal of Management & Governance*, vol. 11(2), pp. 165-177.

Demil, Benoit and Xavier Lecocq (2006): "Neither Market nor Hierarchy nor Network: The Emergence of Bazaar Governance", *Organization Studies*, vol. 27(10), pp. 1447-1466.

de Waal, Frans (1982): "Chimpanzee Politics: Power and Sex Among Apes". Johns Hopkins University Press.

Dunbar, Robin I.M. (1992): "Neocortex size as a constraint on group size in primates", *Journal of Human Evolution*, vol. 22(6), pp. 469-493.

DuPoint, Quinn (2018): "Experiments in algorithmic governance: A history and ethnography of "The DAO," a failed decentralized autonomous organization", pp. 157-177 in: Malcolm Campbell-Verduyn (ed.), "Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance". Routledge.

Dwork, C. and M. Naor (1993): "Pricing via Processing or Combatting Junk Mail". In: E.F. Brickell (ed.): "Advances in Cryptology — CRYPTO' 92". Lecture Notes in Computer Science, vol 740. Springer, Berlin, Heidelberg.

Elster, Jon (1989): "Social norms and economic theory", *Journal of Economic Perspectives*, vol. 3(4), pp. 99-117.

Figgis, J.N. and R.V. Laurence (1907, eds.): "Historical Essays and Studies". Macmillan, London.

Finck, Michèle (2018): "Blockchain Regulation and Governance in Europe". Cambridge University Press.

Finney, Hal (2004): "RPOW - Reusable Proofs of Work". Retrieved on May 16, 2020 from <https://nakamotoinstitute.org/rpow/>.

Fitzgerald, Brian and Pär J. Ågerfalk (2005): "The Mysteries of Open Source Software: Black and White and Red All Over?", Proceedings of the 38th Hawaii International Conference on System Sciences (HICSS-38 2005), 3-6 January.

Ford, Bryan (2002): "Delegative Democracy". Retrieved on Oct 16, 2019 from <https://bford.info/deleg/deleg.pdf>.

Freeman, Jo (1972): "The Tyranny of Structurelessness", *The Second Wave*, vol. 2(1). Retrieved on Oct 17, 2019 from <https://www.jofreeman.com/joreen/tyranny.htm>.

Fukuyama, Frances (2011): "The Origins of Political Order: From Prehuman Times to the French Revolution". Farrar, Straus and Giroux.

Gardler, Ross and Gabriel Hanganu (2010), "Governance models". Retrieved on May 15, 2020 from <http://oss-watch.ac.uk/resources/governancemodels>.

Gibbard, Allan (1973): "Manipulation of voting schemes: A general result," *Econometrica*, vol 41(4), pp. 587–601.

Goldin, Mike (2017): "Token-Curated Registries 1.0". Retrieved on May 15, 2020 from <https://medium.com/p/61a232f8dac7>.

Gordon, Scott (1999): "Controlling the State: Constitutionalism from Ancient Athens to Today", Harvard University Press.

Haber, S. and W.S. Stornetta (1991): "How to time-stamp a digital document", *Journal of Cryptology*, vol. 3, pp. 99-111.

Hanson, Robin (2007): "Shall We Vote on Values, But Bet on Beliefs?". Retrieved on May 15, 2020 from <http://mason.gmu.edu/~rhanson/futarchy.pdf>.

Hanson, Robin (2013): "Shall We Vote on Values, But Bet on Beliefs?", *Journal of Political Philosophy*, vol. 21(2), pp. 151-178.

Hao, Fen, Peter Ryan, and Piotr Zieliński (2010): "Anonymous voting by two-round public discussion", *IET Information Security*, vol. 4(2), pp. 62-67.

Hardin, Garrett (1968): "The Tragedy of the Commons", *Science*, vol. 162(3859), pp. 1243–1248.

Heiberg, Sven and Jan Willemson (2014): "Verifiable internet voting in Estonia", 6th IEEE International Conference on Electronic Voting (Lochau/Bregenz, Austria), pp. 1–8.

Herian, Robert (2018): "Legal Recognition of Blockchain Registries and Smart Contracts", draft report prepared for a workshop on "Blockchains & smart contracts legal and regulatory framework", Paris, France, 12th December. DOI 10.13140/RG.2.2.12449.86886.

Hobbes, Thomas ([1651], 2012): "The Leviathan". Oxford University Press.

Honkanen, Petri, Magnus Westerlund and Mats Nyland (2019): "Governance in Decentralized Ecosystems: A Survey of Blockchain and Distributed Ledger White Papers", *Cloud Computing 2019*, Venice, Italy.

Hume, David ([1739], 1978): "A Treatise of Human Nature", Oxford University Press.

Jakobsson, Markus and Ari Juels (1999): "Proofs of Work and Bread Pudding Protocols", *Secure Information Networks: Communications and Multimedia Security*, Kluwer Academic Publishers, pp. 258–272.

Juels, Ari, Dario Catalano and Markus Jakobsson (2005): "Coercion-Resistant Electronic Elections", *WPES'05: Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, pp. 37-63

Kamvar, Sepandar, Mario Schlosser and Hector Garcia-Molina (2003): "The EigenTrust Algorithm for Reputation Management in P2P Networks", *Proceedings of the 12th international conference on World Wide Web*, pp. 640–651.

Kitschelt, Herbert and Steven Wilkinson (2007, eds.): "Patrons, Clients and Policies. Patterns of Democratic Accountability and Political Competition". Cambridge University Press.

Kronovet, Daniel (2019): "Aragon, DAOstack, Colony, Moloch". Retrieved on May 16, 2020 from <https://kronosapiens.github.io/blog/2019/06/16/aragon-daostack-colony-moloch.html>.



- Kwon, Yujin, Liu Jian Li, Kim Minjeong, Song Dawn and Kim Yongdae (2019): "Impossibility of Full Decentralization in Permissionless Blockchains", Proceedings of the 1st ACM Conference on Advances in Financial Technologies, October 21-23 2019, Zurich, pp. 110–123. Retrieved on May 15, 2020 from <https://doi.org/10.1145/3318041.3355463>.
- Lakhani, Karim and Robert Wolf (2003): "Why Hackers Do What They Do: Understanding Motivation and Effort in Free/Open Source Software Projects", in: J. Feller, B. Fitzgerald, S. Hissam, and K. R. Lakhani (eds.): Perspectives on Free and Open Source Software. DOI: 10.2139/ssrn.443040.
- Lalley, Steven and E. Glen Weyl (2018): "Quadratic Voting: How Mechanism Design Can Radicalize Democracy", American Economic Association Papers and Proceedings, 1(1), pp. 1-5. Available at <https://ssrn.com/abstract=2003531>.
- Larimer, Daniel (2013): "Overpaying For Security". Retrieved on May 16, 2020 from <https://letstalkbitcoin.com/is-bitcoin-overpaying-for-false-security>.
- Learner, Roy (2019): "Blockchain Voter Apathy". Retrieved on May 16, 2020 from <https://medium.com/p/69a1570e2af3>.
- Lewis-Kraus, Gideon (2018): "Inside the Crypto World's Biggest Scandal", Wired, 19 June 2018.
- Lutz, Donald S. (2006): "Principles of Constitutional Design". Cambridge University Press.
- Makkonen, Juha (2018): "Steward-ownership is capitalism 2.0". Retrieved on May 16, 2020 from <https://medium.com/p/76a1c50a6d88>.
- Malik, Shiv (2019): "In Defence of Szabo's law: Round Robin by design". Retrieved on May 16, 2020 from <https://medium.com/p/f637eb2515b1>.
- Man, Ido, Ron Sabo and Ehud Segal (2019): "Resolving the Stake-Based vs. Participant-Based Voting Dilemma". Retrieved on May 16, 2020 from <https://blog.saga.org/resolving-the-stake-based-vs-participant-based-voting-dilemma-de0b50376f8f>.
- Mannan, Morshed (2018): "Fostering Worker Cooperatives with Blockchain Technology: Lessons from the Colony Project", Erasmus Law Review, vol. 11(3), pp. 190-203.
- Michels, Robert (1911 [in German]): "Political Parties: A Sociological Study of the Oligarchical Tendencies of Modern Democracy". Translated to English in 1915 by Eden and Cedar Paul for Hearst's International Library Co. Reprint in 2010.
- Montesquieu ([1751], 1949): "The Spirit of Laws". Hafner Press, New York.
- Muzzy, Everett and Mally Anderson (2019): "Measuring Blockchain Decentralization". Retrieved on May 16, 2020 from <https://consensys.net/research/measuring-blockchain-decentralization/>.
- Nakamoto, Satoshi (2008): "Bitcoin - A Peer-to-Peer Electronic Cash System". Retrieved on Sep 16, 2019 from <https://bitcoin.org/bitcoin.pdf>.
- Nakamura, Kenjiro (1979): "The vetoers in a simple game with ordinal preferences", International Journal of Game Theory, vol. 8, pp. 55–61.
- Olson, Mancur ([1965], 1971): "The Logic of Collective Action: Public Goods and the Theory of Groups". Revised ed., Harvard University Press.
- Onggunhao, Daniel (2019): "Wow. The @MakerDAO stability fee (interest rate) has dropped to 5.5%. A single whale (with 97% of voting power) made the decision. Went from 2,489 votes a few hours ago, to 44,539 votes." October 28, 2019, 3:25 PM. A tweet, retrieved May 16, 2020 from <https://twitter.com/onggunhao/status/1188824097918029825>.
- Ostrom, Elinor (1990): "Governing the Commons: The Evolution of Institutions for Collective Action". Cambridge University Press.

- Paumgarten, Nick (2018): "The Prophets of Cryptocurrency Survey the Boom and Bust". The New Yorker, October 22, 2018.
- Pietrewicz, Lesław (2018): "Token-based blockchain financing and governance: A transaction cost approach", a preprint.
- Prud'homme, Rémy (1995): "The Dangers of Decentralization", The World Bank Research Observer, vol. 10(2), pp. 201-220.
- Raymond, Eric S. (1999): "The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary". O'Reilly.
- Red, Richard (2019): "Peer Production on the Crypto Commons", version 0.8, retrieved on May 18, 2020 from <https://cryptocommons.cc/download>.
- Reijers, Wessel, Fiachra O'Brolcháin and Paul Haynes (2016): "Governance in Blockchain Technologies & Social Contract Theories", Ledger, vol. 1, pp. 134-151. DOI 10.5915/LEDGER.2016.62
- Robertson, Brian (2007): "Evolving Organization", Integral Leadership Review, vol. 7(3).
- Romme, Georges (1995): "The sociocratic model of organizing", Strategic Change, vol. 4, pp. 209-215.
- Rozas, David, Antonio Tenorio-Fornés, Silvia Díaz-Molina and Samer Hassan (2018): "When Ostrom Meets Blockchain: Exploring the Potentials of Blockchain for Commons Governance", retrieved on May 20, 2020 from <https://www.ssrn.com/abstract=3272329>.
- Saga (2020): A provisional constitution. Retrieved on May 16, 2020 from <https://www.saga.org/governance>.
- Sanderson, Stephen K. (1995): "Civilizations and World Systems: Studying World-Historical Change". Rowman & Littlefield, pp. 118–119.
- Sanitt, Adam (2018): "Legal analysis of the governed blockchain". Retrieved on Jan 7, 2020 from <https://www.nortonrosefulbright.com/en/knowledge/publications/0d56a3a5/legal-analysis-of-the-governed-blockchain>.
- Satterthwaite, M. (1975): "Strategy-proofness and Arrow's conditions: existence and correspondence theorems for voting procedures and social welfare functions", Journal of Economic Theory, vol. 10, pp. 187–217.
- Schiener, Dominik (2015): "Liquid Democracy: True Democracy for the 21st Century". Retrieved on May 16, 2020 from <https://medium.com/p/7c66f5e53b6f>.
- Schweik, Charles and Robert English (2013): "Preliminary steps toward a general theory of Internet-based collective-action in digital information commons: Findings from a study of open source software projects", International Journal of the Commons, vol. 7(2), pp. 234–254.
- Scott, Alev and Andronike Makres (2019): "Power & the People: Lessons for Today from the Birthplace of Democracy". Riverrun.
- Shakow, David J. (2018): "The Tao of The DAO: Taxing an Entity That Lives on a Blockchain", Faculty Scholarship at Penn Law.
- Sheng, Tony (2018): "Not all governance is voting". Retrieved on May 16, 2020 from <https://tonysheng.substack.com/p/voting-governance>.
- Singal, Jesse (2016): "How America Became Infatuated With a Cartoonish Idea of 'Alpha Males'", New York Magazine. May 18, 2016.
- Sismondo, Christine (2011): "America Walks Into A Bar". Oxford University Press.
- Slattery, Martin (1991): "Key Ideas in Sociology". Macmillan.

- Smits, Willem-Jan (2018): "Blockchain Governance: What Is It, What Types Are There and How Does It Work in Practice?". Retrieved on Sep 16, 2019 from <https://watsonlaw.nl/en/blockchain-governance-what-is-it-what-types-are-there-and-how-does-it-work-in-practice/>.
- Srinivasan, Balaji S. and Leland Lee (2017): "Quantifying Decentralization". Retrieved on May 15, 2020 from <https://news.earn.com/quantifying-decentralization-e39db233c28e>.
- Stiglitz, Joseph (1987): "Principal and agent", *The New Palgrave: A Dictionary of Economics*, vol. 3, pp. 966–971.
- Stokes, Susan, Thad Dunning, Marcelo Nazareno, and Valeria Brusco (2014): "Brokers, Voters, and Clientelism: The Puzzle of Distributive Politics". Cambridge University Press.
- Suchak, Maliny, Timothy Eppley, Matthew Campbell, Rebecca Feldman, Luke Quarles and Frans de Waal (2016): "How chimpanzees cooperate in a competitive world", *Proceedings of the National Academy of Sciences*, vol. 113, pp. 10215–10220.
- Szabo, Nick (1996): "Smart contracts: building blocks for digital markets". Retrieved on Sep 16, 2019 from [http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart\\_contracts\\_2.html](http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html).
- Szabo, Nick (1997): "The Idea of Smart Contracts", Retrieved on May 15, 2020 from <https://nakamotoinstitute.org/the-idea-of-smart-contracts>.
- Tabbarok, Alex (2018): "When Can Token Curated Registries Actually Work?". Retrieved on May 16, 2020 from <https://medium.com/p/2ad908653aaf>.
- Wang, Rong and Giorgos Cheliotis (2016): "Institutional and Entrepreneurial Engagement in Commons-Based Peer Production", *International Journal of Communication*, vol. 10(2016), pp. 4258–4279.
- Weber, Max (1921): "Economy and Society", Chapter 6 ("Bureaucracy"). See the English translation in Tony Waters (2015, ed.): *Weber's Rationalism and Modern Society: New Translations on Politics, Bureaucracy, and Social Stratification*, Palgrave MacMillan, pp. 73-128.
- Williamson, Oliver E. (2002): "The Theory of the Firm as Governance Structure: From Choice to Contract," *Journal of Economic Perspectives*, vol. 16(3), pp. 171-195.
- Wright, Aaron and Primavera de Filippi (2015): "Decentralized Blockchain Technology and the Rise of Lex Cryptographia", *SSRN Electronic Journal*. DOI 10.2139/ssrn.2580664.
- Wright, Aaron and Primavera de Filippi (2018): "Blockchain and the Law: The Rule of Code". Harvard University Press.
- Yermack, David (2017): "Corporate Governance and Blockchains", *Review of Finance*, vol. 21(1), pp. 7–31.
- Zoltu, Micah (2019): "How to turn \$20M into \$340M in 15 seconds". Retrieved on May 16, 2020 from <https://medium.com/p/48d161a42311>.