Defining Decentralisation in Permissionless Blockchain Systems

Riaan Bezuidenhout
Assistant Researcher, Department of Computer Science and Informatics, University of the Free State, Bloemfontein, South Africa
https://orcid.org/0000-0002-5412-7512

Wynand Nel
Lecturer, Department of Computer Science and Informatics, University of the Free State, Bloemfontein, South Africa
https://orcid.org/0000-0001-5579-6411

Jacques M. Maritz
Lecturer, Department of Engineering Sciences, University of the Free State, Bloemfontein, South Africa
https://orcid.org/0000-0003-1556-8523

Abstract

The term *decentralised* as a description of the architecture, operation, and governance of permissionless blockchain systems has become ubiquitous. However, in these contexts, the term *decentralised* has no clear definition. Blockchain ecosystems are complex, and thus it is essential to address confusion among stakeholders about their nature and promote understanding of the intentions and consequences of their implementation. This article offers a theoretical definition of the term *decentralised* in the context of permissionless blockchain systems. It is proposed that five inextricable and interconnected aspects are required, at a minimum, to warrant a claim that a permissionless blockchain system is decentralised. These aspects are disintermediation, a peer-to-peer network, a distributed blockchain data structure, algorithmic trust, and open-source principles. The relationship between the five aspects is discussed, and it is argued that decentralisation is not binary but exists on a spectrum. Any variation in one or more aspects may impact the system's decentralised nature as a whole. The researchers identify areas where further investigation in this field is required and propose instances where the knowledge garnered may be used.

Keywords

blockchain, permissionless, decentralised, disintermediation, distributed ledger, algorithmic trust, open source, peer-to-peer network

DOI: https://doi.org/10.23962/ajic.i29.14247

Recommended citation

Bezuidenhout, R., Nel, W., & Maritz, J.M. (2022). Defining decentralisation in permissionless blockchain systems. *The African Journal of Information and Communication (AJIC), 29*, 1-24. https://doi.org/10.23962/ajic.i29.14247

1. Introduction

When the term *decentralised* is used to refer to a permissionless blockchain system, the term tends to lack precision with respect to its meaning and the aspects of the system it is being used to refer to (Walch, 2019, p. 40). Many terms are used to describe technologies built on so-called *decentralised* blockchains. The terms decentralised consensus systems, decentralised applications, decentralised digital currencies, cryptocurrencies, altcoins, meta coins, smart contracts, distributed applications, distributed autonomous organisations, and distributed autonomous companies are routinely used throughout the literature (Glaser & Bezzenberger, 2015). Some authors simply refer to blockchain or blockchain technology (Holotescu, 2018). It may be that within the computer science community, the term *decentralised* blockchain is generally understood. However, one would be hard-pressed to find a clear theoretical definition for it. The vagueness represents a potential problem for any stakeholder needing to engage with the technology on some level.

This study provides a proposed clear theoretical definition of the term *decentralised* in the context of a permissionless blockchain system. In establishing and setting out the definition, this study seeks to make an important contribution to stakeholders engaging with blockchain by inserting critical, theoretically founded analysis into the subject's discourse.

What is a theoretical definition, and why is it important?

The conclusion Walch (2019) draws is that in law, the term *decentralised* already represents a legal standard that has implications for regulators and business, and its current lack of proper definition may result in misleading conclusions being drawn from it. This is exacerbated by the fact that regulators and managers have to deal with many different types of business models that are being established using blockchain systems (Stabile et al., 2020). Whether the underlying blockchain system is centralised or decentralised is fundamental to the type of business model and, therefore, its regulatory environment.

Notwithstanding its vagueness, the term *decentralised* found its way into regulators' language from early on, as this description by the US Department of the Treasury Financial Crimes Enforcement Network (FinCEN) shows:

> c. De-Centralized Virtual Currencies
> A final type of convertible virtual currency activity involves a de-centralized convertible virtual currency (1) that has no central repository and no single administrator, and (2) that persons may obtain by their own computing or manufacturing effort. (FinCEN, 2013, p. 5)

And the practice is still ongoing, as is evident in this more recent US government statement:

> The vast majority of cryptocurrencies are decentralized, as they lack a central administrator to issue currency and maintain payment ledgers—in other words, there is no central bank. (US Department of Justice, 2020, p. 3)

In the first example above, the term *decentralised* is contained in the definition of the system (decentralised virtual currency), while the second example explains what a decentralised cryptocurrency lacks, not what it contains. A theoretical definition must go beyond a superficial description. In addition to specifying what is required in a decentralised blockchain system, this study also answers the *how*, *when* and *why* questions that apply to theories in general (Bacharach, 1989). Specifically, in the context of permissionless blockchain systems, this study answers the following questions:

- What are the aspects (constituent stakeholders and components) of decentralisation in a decentralised blockchain system?
- How do these aspects combine and interact to achieve decentralisation?
- When (and to what end) do the stakeholders and components need to arrange themselves in a manner that delivers decentralisation?
- Why is each aspect necessary? In other words, why can decentralisations not exist without the presence of each aspect?

It is important to note that the end-product is not merely a list of constituent elements and their individual roles, but is more importantly also an explanation of the interactions and causal relationships between these phenomena.

Structure of the article

This article starts with a description of blockchain systems, their components, and their purpose, before defining what a permissionless blockchain system is and the environment in which it operates. The terminology and environment make up the boundary assumptions within which the theoretical definition of *decentralised* will be positioned. Specifically, the definition of *decentralised* is bounded by the key constraint of a *permissionless* blockchain system, as *permissioned* blockchain systems are specifically *not decentralised* (Vukolic, 2017). In the results, we propose a proper, theoretically founded, technical definition of the term *decentralised* in the context of permissionless blockchain systems. The article concludes with a discussion of the results and concluding remarks.

2. Background

In the literature, some authors refer to blockchain as a data structure, an ordered list of blocks, where each block contains a list of transactions, and where blocks are cryptographically linked to provide a tamper-proof historical transaction record (Nofer et al., 2017; Xu et al., 2017). The idea of a blockchain as a distributed ledger of transactions (therefore a data structure) is echoed by multiple researchers (Mulár, 2018; Rizun et al., 2015; Zheng et al., 2017). Other authors describe a blockchain as a combination of technologies such as distributed ledgers, cryptography, and consensus mechanisms that allow untrusted parties to agree on the state of transaction data that is decentralised – therefore, *a system* (Glaser & Bezzenberger, 2015; Saad et al., 2019; Tasca & Tessone, 2019).

To avoid ambiguity, in this study, the term *blockchain* explicitly means a distributed ledger that conforms to a cryptographically linked data structure that serves as a transaction record and makes up one component of a blockchain system. The data structure characteristics are specifically designed to enable parties to agree on the transaction record without having to trust one another. Furthermore, this study defines a *blockchain system* as a combination of stakeholders and technologies that produce, consume, or interact with required services, or are enabled by the use of a blockchain data structure. While permissionless blockchain systems may differ in their intended application and architecture, they all share essential objectives (Bezuidenhout et al., 2020).

Purpose of a blockchain system

A blockchain's purpose is to record transactions (which may include smart contract programs) that are immutable and cannot be repudiated, and that are secure, transparent and accessible (Tasca & Tessone, 2019; Xu et al., 2017). These terms (related to the nature of the blockchain data structure) are defined in the following way:

- *Immutable* refers to the principle that a recorded transaction cannot be altered or, more accurately, can eventually not be altered (Tasca & Tessone, 2019).
- *Non-repudiation* means that since a transaction cannot be altered, it can also not be undone or "taken back" (Xu et al., 2017). Immutability and non-repudiation are achieved by embedding cryptographic hash pointers into the blockchain to construct a tamper-proof log of transactions (Narayanan et al., 2016).
- *Security* in permissionless blockchain systems pivots on a trifecta of techniques that protect the ownership of data, the integrity of the blockchain, and the system's redundancy as a whole. First, data ownership security is established through public-key cryptography by allowing only the rightful owner of a private key to transact with their own data on the blockchain (Tschorsch & Scheuermann, 2016). Second, the blockchain itself consists of a sequential

series of blocks, each linked by a cryptographic hash pointer to the previous block to produce a tamper-evident log of transactions. This ensures the integrity of the blockchain (Narayanan et al., 2016). Third, a centralised system controlled by a single authority carries the risk of single-point failure (Atzori, 2017). By doing away with a centralised or root authority and by distributing copies of the blockchain across many peers on a peer-to-peer network, a permissionless blockchain uses redundancy to mitigate this type of risk.

- *Transparency* refers to the fact that all the blockchain transactions are open and, therefore, auditable by all the system's participants. In the case of permissionless blockchain systems, this means anyone with an internet connection (Tasca & Tessone, 2019).
- *Accessibility* is narrowly coupled with the idea of transparency, meaning all participants in a permissionless blockchain system have equal rights to transact on and manipulate the blockchain (Xu et al., 2017). For clarification, note that there is a juxtaposition between *accessibility* and *security* here. Accessibility implies the ability to inspect the blockchain, including all the transactions on it. This may include inspecting the data (for auditability purposes) of other participants. Accessibility also means that there is no restriction on participants to transact on the system, but transactions by participants are limited to their own data. Accessibility does not extend to the point where data ownership security is compromised.

In a permissionless blockchain system (see section 2), the definition of *decentralised* becomes critical. This is because it must remain true to its purpose while being decentralised and must therefore operate in the absence of a central trusted authority.

Permissionless blockchain systems and their environment

This study focuses on *permissionless*, i.e., public, blockchain systems. As a starting point, the emphasis is placed on the distinction between distributed and decentralised system architectures as described by Troncoso et al. (2017, p. 208). Note that these definitions are aimed at information systems in general and not blockchain systems specifically:

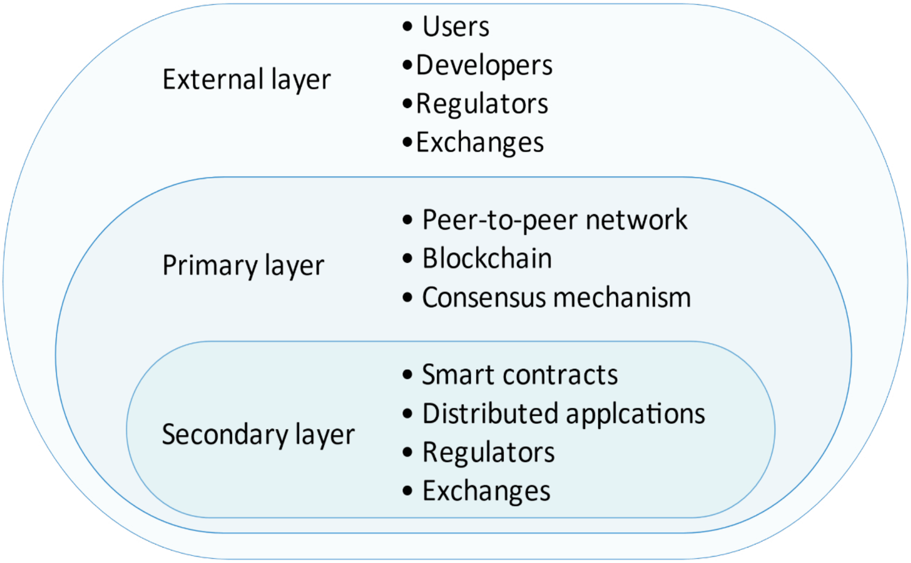
> Distributed system: A system with multiple components that have their behaviour co-ordinated via message passing. These components are usually spatially separated and communicate using a network, and may be managed by a single root of trust or authority. (Danezis & Halpin, 2017, p. 208)
>
> Decentralized system: A distributed system in which multiple authorities control different components, and no single authority is fully trusted by all others. (Danezis & Halpin, 2017, p. 208)

These two definitions show clearly that while all decentralised systems are distributed, not all distributed systems are decentralised. *Permissionless* blockchain systems do not restrict participation. Anyone can join or leave the system at will. They function on a peer-to-peer basis, without a central authority and require a decentralised consensus mechanism for participants to reach an agreement on a single correct state of the blockchain (Glaser & Bezzenberger, 2015; Tasca & Tessone, 2019; Zheng et al., 2017). These are the only type of blockchain systems where the definition of decentralised may be applicable because permissionless blockchain systems are distributed systems where different components are controlled by multiple authorities. In contrast, *permissioned* (private) blockchain systems are systems where only certain entities are allowed access to the blockchain. Although they are also distributed systems, access is controlled by a central authority, and these types of blockchain systems are not decentralised (Deshpande et al, 2017). The definition of decentralised has no meaning in the context of *permissioned* blockchain systems.

Layers in a blockchain system

Three layers of entities or components in permissionless blockchain systems make up the blockchain environment. These are the external layer, the primary layer, and the secondary layer, as depicted in Figure 1.

Figure 1: Layers in a blockchain system


External layer

- Users
- Developers
- Regulators
- Exchanges

Primary layer

- Peer-to-peer network
- Blockchain
- Consensus mechanism

Secondary layer

- Smart contracts
- Distributed applcations
- Regulators
- Exchanges

First is the layer that constitutes its mechanical operation. It consists of the blockchain, peer-to-peer network, and the consensus mechanism (Narayanan et al., 2016; Zheng et al., 2017). This will be referred to as the *primary layer.*

A second layer of more sophisticated applications can be built on top of the basic blockchain implementation through smart contracts. The meaning of the term *smart contract* is extremely broad. However, it allows for a range of automated, dynamic applications to operate independently, using the primary layer's services (Glaser & Bezzenberger, 2015). These applications will be referred to as the *secondary layer*. It is important to note that the interaction with the secondary layer applications occurs by initiating a transaction (containing the smart contract code to be executed) on the primary layer. For example, Ethereum (Buterin, 2013) allows users to pre-program transactions by submitting software code inside a transaction that executes automatically under certain conditions. These transactions do not require any additional action by the users who created them.

Blockchain systems do not suddenly spring into being and then exist in isolation; they are embedded within society at large. They are created and maintained by some entity or entities to fulfil a useful function to a community of consumers or users. These entities include:

- Developers that develop and maintain software related to both the primary and secondary layers of many blockchain systems (Bitcoin.org, n.d.; Cardanofoundation.org, 2020; Ethereum.org, n.d.). These may be not-for-profit communities or business entities that operate for profit (Glaser & Bezzenberger, 2015).
- Users who transact with the blockchain system, either directly with the primary layer or indirectly with the secondary layer. These may be individuals, organisations, or systems (including IoT devices). Users may also transact through intermediaries such as brokers or exchanges, which, in turn, can be viewed as users, organisations, or systems.
- Regulatory authorities that may scrutinise blockchain systems from time to time (Tasca & Tessone, 2019).

The entities above are examples of external stakeholders that make up an *external layer*, comprising all the parties that interact with or provide support to the blockchain system's primary or secondary layers.

The secondary layer is embedded in the primary layer and cannot exist without it. Furthermore, the external layer does not interact directly with the secondary layer but does so through the primary layer. Similarly, the primary layer does not exist without the requirement for, consumption of, and development by the external layer. Within the context provided in the preceding discussions—focusing on the distinction between the terms *blockchain* and *blockchain system*, the *purpose* of a blockchain system, and the definition of a *permissionless blockchain system* and its constituent *layers* (environment)—it is possible to define the term *decentralised*.

3. Methodology

This study investigated literature in the blockchain domain to classify the aspects that authors associated with the decentralised nature of blockchain systems. The purpose was neither to be exhaustive nor comparative, and to extract the meaning of the term *decentralised* as used by authors in information science in the context of the permissionless blockchain environment. Works that dealt with the theory of blockchain systems in general in the preceding five years (since 2016) were selected. Only peer-reviewed material was included, specifically journal articles and conference papers. The primary search was conducted through the internet search services of Academia, ResearchGate, Semantic Scholar, and SSRN. A secondary search was done by looking for appropriate material referenced in articles and papers that passed this selection process.

Each item identified in the literature was studied to determine which aspects the author(s) ascribed to the term *decentralised* in the context of a permissionless blockchain system. In some of the material set aside for further analysis, the authors' treatment of the term *decentralised* was too vague to warrant including it in the study. Eventually, of the 89 articles and papers identified for detailed scrutiny, 46 (see Appendix) were included in the results. At this point, we concluded that it was unlikely that additional interpretations of the term *decentralised* were forthcoming by including more material, and that the disqualified material up to that point did not include any information that was not present in the final 46 articles and papers.

4. Analysis from the review of existing literature

Throughout the 46 items investigated, it was found that the term *decentralised* could be associated with five aspects that apply to permissionless blockchain systems. These aspects, identified from the literature, were disintermediation, a distributed blockchain, peer-to-peer network, algorithmic trust, and open-source principles. They represent philosophical ideas (disintermediation and open-source principles), physical components (peer-to-peer network), and software implementations (distributed blockchain and algorithmic trust) which form the basis of the theoretical definition of *decentralised* in a permissionless blockchain system. Table 1 lists the five aspects of decentralisation against the author numbers in the Appendix.

Table 1: Aspects of decentralisation identified from the literature

Aspect of decentralisation	Author number in Appendix	Count
Disintermediation	1, 2, 3, 4, 14, 15, 16, 18, 19, 20, 21, 22, 23, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 38, 39, 40, 41, 42, 43, 44, 45, 46	32
Distributed blockchain	1, 3, 4, 5, 6, 9, 10, 11, 13, 14, 16, 17, 18, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 33, 36, 37, 39, 40, 41, 42, 43, 44, 45	35
Peer-to-peer network	4, 5, 9, 16, 17, 18, 24, 25, 27, 29, 30, 33, 36, 39, 41, 43, 44	17
Algorithmic trust	1, 3, 4, 5, 6, 7, 8, 11, 13, 14, 16, 17, 18, 19, 20, 24, 25, 26, 27, 28, 30, 31, 33, 34, 36, 38, 39, 40, 41, 42, 44, 45, 46	33
Open-source principles	5, 12, 20, 28, 41	5

The study did not assign any weight to the number of times an aspect presented in the literature ("Count" column in Table 1). This was done for two reasons. First, the literature reviewed did not aim to define the term *decentralisation* but assumed that decentralisation was a valid descriptor of a blockchain system because one or more of the specific aspects were present. Second, as will be shown in the results (section 5), no aspect is more important than the other; all are required in a decentralised blockchain system. Each of these aspects is now discussed in detail to provide the context of how they were represented in the reviewed literature.

Disintermediation

Disintermediation is a philosophical idea that was central to Nakamoto's introduction of Bitcoin. He posited a system of electronic payments where individuals could transact without the mediation of a central institution (Nakamoto, 2008). The idea of disintermediation, which refers to the absence of a central authority in a blockchain system, whether the transactions are meant to be of a monetary nature or not, is an assertion that comes across often in the literature. Some authors refer to a blockchain system being decentralised because of the lack of central authority within the peer-to-peer network directly, while others refer more indirectly to the absence of a central point of trust or authority. Hackius and Petersen (2017, p. 5) called it "without relying on a central authority or centralised infrastructure establishing trust", while Lin and Liao (2017, p. 653) state that "blockchain doesn't have to rely on a centralized node". This philosophical flavour can border on political ideology, as noted by Atzori (2017, p. 46): "the advocates of decentralization tend to have in common the same dissociative attitude towards centralized institutions and the State in particular". In this study, the researchers opted for the term "disintermediation" used by Holotescu (2018, p. 276) to describe the spectrum of phrases ranging from "not having to rely on a central node" to "dissociative attitude towards centralized institutions" as the term summarises all of the above ideas into a single word.

Disintermediation means that any party that aims to participate in the blockchain system's primary layer (for instance, join the peer-to-peer network, submit a transaction, or attempt to extend the blockchain) can do so without the permission of any other party. Furthermore, any party that participates in the primary layer of the blockchain system may send data to, or receive data from, any other party. This can be done by contacting that party directly or through an intermediary, and if it does so through an intermediary (another node or series of nodes on the network), the party can expect that the data will be transmitted without any interference or changes whatsoever. This includes any undue delay in transmission. We argue that, as part of a theoretical definition, disintermediation can be interpreted as a software policy, loose standing from the motivations, political or otherwise, of any party that engages with the blockchain system.

Distributed blockchain

The most common reference regarding the nature of the blockchain data structure among authors reviewed includes the notion of a *ledger*, *transaction ledger*, or *transaction record*, distributed or shared among the nodes of the peer-to-peer network. For example: "At the heart of these systems is a shared ledger that reliably records a sequence of transactions" (Chen & Micali, 2017, p. 1); "Every different user constitutes a network node and maintains a copy of the ledger" (Konstantinidis et al., 2018, p. 384); and "The information about every transaction ever completed in Blockchain is shared and available to all nodes" (Limata, 2019, p. 5). Other authors used the term *distributed database*, for instance: "A blockchain is a distributed ledger database" (Manski, 2017, p. 512), and "a distributed database of records" (Perwej et al., 2019, p. 82).

All these terms refer to the cryptographically linked, tamper-proof blockchain data structure identified in section 2. In the context of decentralisation in permissionless blockchain systems, the blockchain has no central custodian and is duplicated on many peers (but it need not be duplicated on all) on the peer-to-peer network.

Peer-to-peer network

A peer-to-peer network refers to the well-known network topology where no central node controls access to or data flow within a network (Schoder et al., 2005; Schollmeier, 2001). Logically it makes sense to argue that a peer-to-peer network is the only network topology that enables disintermediation because, if the network is hierarchical, the ability for stakeholders to interact with the network or transmit or receive data on the network will not meet the standard set for disintermediation (see above).

In the literature reviewed, the purpose of the peer-to-peer network was named in relation to the storage of copies of the blockchain (Boudguiga et al., 2017; Labazova, 2019), the verification of transactions, the recording of transactions, and the verification of the validity of the blockchain (Atzori, 2017; Nawari & Ravindran, 2019). We add to these functions the provision of disintermediated communication (data exchange) between stakeholders and components.

Algorithmic trust

Disintermediation requires a transparent method whereby parties can agree that additions to the blockchain are valid. This mechanism is called a consensus algorithm (Tschorsch & Scheuermann, 2016; Zheng et al., 2017) and constitutes a distributed protocol (Blocki & Zhou, 2016; Cachin & Vukolic, 2017) to deliver community trust (Aste et al., 2017). Many terms exist to summarise how participants in a permissionless blockchain system eventually agree on a single correct blockchain (transaction history) and verify that the blockchain has not been tampered with. In the reviewed literature, these descriptions included mostly references to cryptography, proof-based consensus, and trust by computation. The consensus process in a permissionless blockchain system aims to select the node that is allowed to add a block of transactions to the blockchain at random (Glaser, 2017). Essentially, the community of participants in a blockchain system accept a set of digital governance rules or "cryptolaw" (Rueda et al., 2020, p. 182), which will govern the system.

For this study and in the context of permissionless blockchain systems, we define algorithmic trust as a set of rules that disintermediated stakeholders share to manage the blockchain's extension and security. Logically these rules must be consistent (the same for all stakeholders), transparent (the details of how they work must be known to all stakeholders), and rigid (not changeable at the whim of any minority). However, algorithmic trust extends beyond the computational processes verifying and adding transactions or transaction blocks to the blockchain; the consistency, transparency, and rigidity requirements also apply to the communication protocols of the peer-to-peer network because these play a critical role in the disintermediation process.

Open-source principles

The meaning of open-source development (Glaser & Bezzenberger, 2015), open-source system (Lin & Liao, 2017), and developers operating on open-source principles (Tasca & Tessone, 2019) is more difficult to pin down into a single definition. Arguments will be presented in the discussion that the source code of the system must be open-source. This includes all modules that control communication, security, verification, and consensus. However, it goes beyond software. The entire decision-making structure of the developer community must be transparent. On the other hand, to demand that the decision-making structure must be open for participation by every stakeholder that wishes to do so seems more idealistic than practical.

5. Results

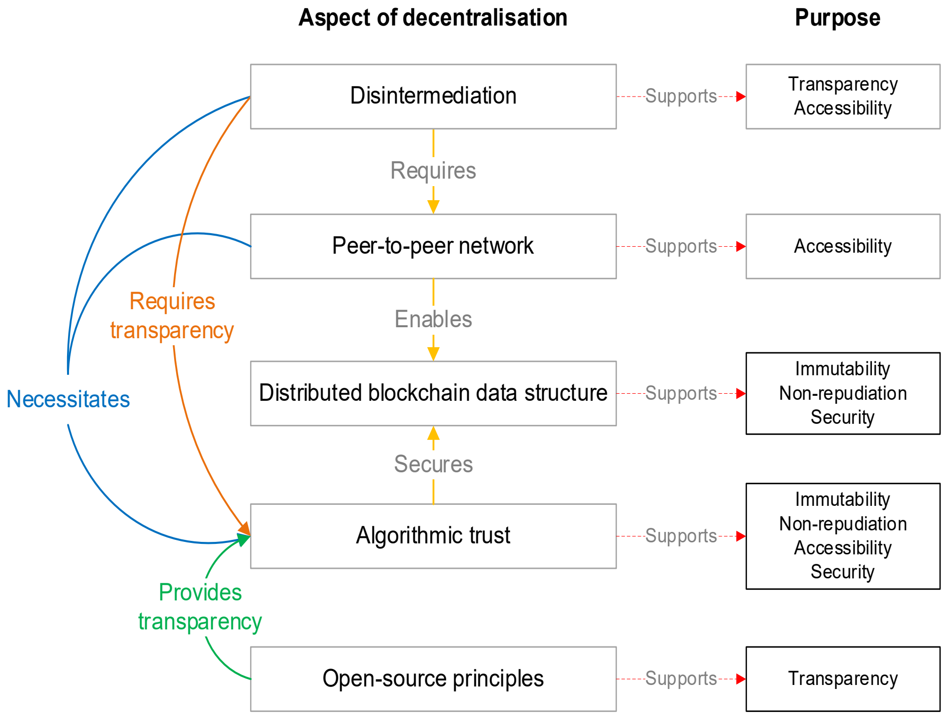
Armed with the five aspects of *decentralisation*, namely disintermediation, a distributed blockchain, a peer-to-peer network, algorithmic trust, and open-source principles identified from the literature (see section 4), it is now possible to construct a theoretical definition of the term *decentralised* or *decentralisation*, in the context of permissionless blockchain systems.

Decentralisation defined

The aspects of decentralisation are inextricable, and decentralisation cannot exist if any one aspect is lacking. However, a theoretical definition must explain not only which aspects are required, but also when and why each aspect is required and how it contributes to decentralisation. Figure 2 shows the interrelationships between the aspects of decentralisation and how these aspects support the purpose of a decentralised blockchain system.

The primary driver of the decentralisation process is the aspect of disintermediation at the top centre of Figure 2. The requirement that the blockchain system must be permissionless (by definition) is the reason why disintermediation is needed. Any party must be allowed to participate in the blockchain system *without the permission* of any other party. In practice, it means that the blockchain must, in the first instance, be available to anyone or any system that may want to use it for any purpose it may see fit – because no permission is needed. Secondly, disintermediation also means that any party can send valid data to any number of the nodes on the peer-to-peer network with the expectation that it will be propagated across the whole network and be accepted as part of the blockchain. Valid data refers to a transaction, a new addition to the blockchain, or any other data that may form part of the system's operation. The processing of any valid data by any source must be indistinguishable from any other valid data from any other source. In other words, disintermediation gives rise to a software policy of data and source equivalence. Disintermediation supports the permissionless blockchain system's purpose of transparency and access.

Figure 2: Interrelationships between the aspects of decentralisation and how they support the purpose of a decentralised blockchain system



Disintermediation creates the requirement for a peer-to-peer network—the second aspect of decentralisation in Figure 2. A peer-to-peer network requires no central authority to grant or deny access to any would-be participant. Peers on the network do not screen data in any way except for checking its validity according to the consensus rules of the system. It allows for the unencumbered flow of data between all the stakeholders in the system. The peer-to-peer network supports the permissionless blockchain system's purpose of accessibility.

A peer-to-peer network enables a distributed blockchain environment—the third aspect of decentralisation in Figure 2. The distributed blockchain ensures that the transaction data has no single custodian. A distributed blockchain contributes towards the blockchain system's purpose of security by providing redundancy of the blockchain and operational nodes. Since the blockchain is also a tamper-proof log of transactions, it also supports the purposes of immutability and non-repudiation.

The requirement for algorithmic trust is a consequence of disintermediation (the fourth aspect of decentralisation in Figure 2) and the peer-to-peer network. Since no central authority exists in a permissionless blockchain system to serve as an authoritative source of truth concerning which information is to be trusted or not, it requires a mechanism for algorithmic trust. Algorithmic trust is the implementation of the software policy of data and source equivalence, the security protocols, and the communication protocols of the system (section 4). It provides both the mechanism for constructing valid data to be transmitted on the peer-to-peer network and the mechanism whereby all participants can verify the validity of data received. Algorithmic trust ensures accessibility through data and source equivalence, immutability through accessibility, and non-repudiation and security through data validation of transactions, new transaction blocks, and the blockchain.

In practice, algorithmic trust is the result of software programs that are executed by participants in the blockchain system. The programs may construct and broadcast new transactions to the peer-to-peer network, they may verify transactions and attempt to construct new blocks of transactions to add to the blockchain, they may broadcast new transaction blocks or new versions of the blockchain to the peer-to-peer network, or they may validate newly received transaction blocks or blockchain versions. In section 4, we argued that three requirements must apply to the rules that these software programs follow. The rules must be consistent (the same for all stakeholders), transparent (the details of how they work must be known to all stakeholders), and rigid (not changeable at the whim of any minority). These requirements necessitate that all stakeholders have access to the details of how algorithms are implemented in the code, and the permissionless blockchain system must therefore operate on open-source principles – the fifth aspect of decentralisation in Figure 2. Open-source principles ensure the transparency that is required by disintermediated parties to function in an environment of algorithmic trust. It is the pivotal aspect that allows permissionless blockchain systems to fulfil their purpose of transparency. Section 6 will explain, however, that this is the most precarious aspect of the decentralisation of a permissionless blockchain system.

Our definition of *decentralisation* in a permissionless blockchain system can be summarised as follows:

> *When a **distributed blockchain** data structure is implemented between **disintermediated** parties, it provides the basis for a decentralised blockchain system. This creates the logical requirement for a **peer-to-peer network** topology that serves to transmit data between parties and store the blockchain in a distributed manner. Since no central authority exists in this system to serve as an authoritative source of truth concerning which information is to be trusted or not, it requires a mechanism for **algorithmic trust**. This algorithmic trust mechanism must be auditable by any stakeholder in the system and must, therefore, operate on **open-source principles**. These five aspects are a minimum requirement to define a decentralised, permissionless blockchain system.*

5. Discussion

As the results have shown, the aspects of decentralisation are inextricable and thus cannot be viewed in isolation. If all five aspects of decentralisation are present, one may ask if it is enough to define the blockchain system as decentralised. The answer is no. One must consider the presence of the five aspects and their individual nature, which may be much more nuanced. For example, many consensus algorithms have been proposed for blockchain systems that operate between disintermediated parties. Two of the most prevalent are proof-of-work and proof-of-stake, which are both probabilistic. They aim to give all participants a random chance of adding a new block of transactions to the blockchain. However, this random chance does not mean equally probable for all participants; in fact, there may be significant discrepancies that give some parties a larger chance of proposing a block than others (Nguyen & Kim, 2018).

In the case of Bitcoin (using proof-of-work), it is generally accepted that when 51% of the computing power in the network is centralised, then the consensus mechanism loses its decentralised nature (Eyal & Sirer, 2014). Eyal and Sirer (2014) have, however, shown that even at concentrations as low as 25%, consensus can be manipulated to some extent in favour of some stakeholders. It shows that decentralisation is not a binary aspect (it exists on a spectrum (Walch, 2019)), and for any stakeholder to evaluate the decentralisation of algorithmic trust, the software needs to be open-source (so that its exact mechanics can be interrogated, as Eyal and Sirer (2014) have done).

Similarly, Di Bella et al. (2013, p. 21) have shown that evidence exists to indicate that a small core (concentrated group) of developers take the most important decisions about the *"architecture and evolution"* of open-source software projects. This type of centralised behaviour has many examples within the developer communities of Bitcoin and other blockchain systems. Gervais et al. (2014) and Walch (2019) warn that, despite the presence of open-source principles, the algorithmic trust mechanisms of both Bitcoin and Ethereum have been altered through the decisions taken by a small group of developers and miners. On the other hand, practical considerations regarding the maintenance of complex software systems preclude consultation with every stakeholder.

6. Conclusion

The introduction to this article identified the confusing nature of the term *decentralised* in blockchain literature and made the case for a proper definition of the term. A review of a large body of recent blockchain literature has identified five aspects (disintermediation, distributed blockchain, peer-to-peer network, algorithmic trust, and open-source principles) that are required for a permissionless blockchain system to be defined as decentralised. Table 1 shows that while many authors have some of these aspects in mind, very few refer to all of them in unison when claiming decentralisation. The confusion seems to arise from this incomplete description that is often used by authors. Perhaps the term is so ubiquitous that not much thought is given as to the details of its meaning. This study addresses the shortcoming by providing authors with a set of five aspects to consider when they refer to a permissionless blockchain system as decentralised, and therefore it contributes to the understanding of blockchain technology. The study goes further by describing the interrelationships between these aspects, acknowledging that the aspects are not of an entirely fixed nature and must be evaluated against the real-world practicalities that are faced by all complex systems.

This article represents an opening statement, a foundation on which arguments that seek to answer many unanswered questions about the implications of decentralisation and its building blocks may be built. Especially in the fields of blockchain governance and regulation, there remains much work to be done in the interpretation of these aspects and how they affect the legal standing of permissionless blockchain systems. It is also important to the ongoing search for better blockchain technology, such as data structures, cross-chain functionality, and consensus algorithms. Consideration should be given to the implications of these technological advances for the decentralised nature of the blockchain system.

We stopped short of investigating or making claims about the nature of decentralisation in the secondary layer of blockchain systems. This is an important shortcoming that must be addressed in future research efforts. Finally, while it was not the purpose of this article, the definition may also serve as a basis for refuting false claims about decentralisation in a blockchain system that is in fact not decentralised.

References

Adhami, S., Giudici, G., & Martinazzi, S. (2018). Why do businesses go crypto? An empirical analysis of initial coin offerings. *Journal of Economics and Business, 100,* 1-37. https://doi.org/10.1016/j.jeconbus.2018.04.001

Alharby, M., & Van Moorsel, A. (2017). A systematic mapping study on current research topics in smart contracts. *International Journal of Computer Science and Information Technology*, *9*, 151–164. https://doi.org/10.5121/ijcsit.2017.9511

Ali Syed, T., Alzahrani, A., Jan, S., Siddiqui, M., Nadeem, S., & Alghamdi, T. (2019). A comparative analysis of blockchain architecture and its applications: Problems and recommendations. *IEEE Access*, *7*, 176838–176869. https://doi.org/10.1109/ACCESS.2019.2957660

Aste, T., Tasca, P., & Di Matteo, T. (2017). Blockchain technologies: The foreseeable impact on society and industry. *IEEE Computer*, *50*(9), 18–28. https://doi.org/10.1109/MC.2017.3571064

Atzori, M. (2017). Blockchain technology and decentralized governance: Is the state still necessary? *Journal of Governance and Regulation*, *6*(1), 45-62. https://doi.org/10.22495/jgr_v6_i1_p5

Bacharach, S. B. (1989). Organisational theories: Some criteria for evaluation. *Academy of Management Review*, *14*(4), 496–515. https://doi.org/10.5465/amr.1989.4308374

Beck, R., & Müller-Bloch, C. (2017). Blockchain as radical innovation: A framework for engaging with distributed ledgers. In *Proceedings of the 50th Hawaii International Conference on System Sciences,* 4-7 January, Waikoloa Village.

Beck, R., Stenum Czepluch, J., Lollike, N., & Malone, S. (2016). Blockchain – The gateway to trust-free cryptographic transaction. In *European Conference on Information Systems,* 12-15 June, Istanbul. https://doi.org/10.24251/HICSS.2017.653

Bentov, I., Gabizon, A., & Mizrahi, A. (2016). Cryptocurrencies without proof of work. In *2016 Financial Cryptography and Data Security Conference,* 22-26 February, Barbados. https://doi.org/10.1007/978-3-662-53357-4_10

Bezuidenhout, R., Nel, W., & Burger, A. (2020). Nonlinear proof-of-work: Improving the energy efficiency of Bitcoin mining. *Journal of Construction Project Management and Innovation*, *10*(1), 20–32. https://doi.org/10.36615/jcpmi.v10i1.351

Bitcoin.org. (n.d.). Bitcoin communities. https://bitcoin.org/en/community

Blocki, J., & Zhou, H.-S. (2016). Designing proof of human-work puzzles for cryptocurrency and beyond. In Hirt, M., Smith, A. (eds), *Theory of cryptography* (pp. 517–546). Springer. https://doi.org/10.1007/978-3-662-53644-5_20

Boudguiga, A., Bouzerna, N., Granboulan, L., Olivereau, A., Quesnel, F., Roger, A., & Sirdey, R. (2017). Towards better availability and accountability for IoT updates by means of a blockchain. In *2017 IEEE European Symposium on Security and Privacy Workshops* (pp. 50–58), 26-28 April, Paris. https://doi.org/10.1109/EuroSPW.2017.50

Burilov, V. (2019). Regulation of crypto tokens and initial coin offerings in the EU. *European Journal of Comparative Law and Governance*, *6 (2019)*, 146–186. https://doi.org/10.1163/22134514-00602003

Buterin, V. (2013). *A next generation smart contract & decentralized application platform*. https://ethereum.org/en/whitepaper

Cachin, C., & Vukolic, M. (2017). Blockchains consensus protocols in the wild. In *Proceedings of the 31st International Symposium on Distributed Computing*, 16-20 October, Vienna. https://doi.org/10.1109/EDCC.2017.36

Calvão, F. (2019). Crypto miners: Digital labor and the power of blockchain technology. *Economic Anthropology*, *6 (1)*, 123–134. https://doi.org/https://doi.org/10.1002/sea2.12136

Cardanofoundation.org. (2020). Foundation team. https://cardanofoundation.org/en/team

Chen, J., & Micali, S. (2017). *Algorand.* https://www.algorand.com

Chen, L., Xu, L., Shah, N., Gao, Z., Lu, Y., & Shi, W. (2017). On security analysis of proof-of-elapsed-time (PoET). In *Stabilization, Safety, and Security of Distributed Systems: 19th International Symposium*, 5-8 November, Boston. https://doi.org/10.1007/978-3-319-69084-1_19

Dai, H.-N., Zheng, Z., & Zhang, Y. (2019). Blockchain for internet of things: A survey. *IEEE Internet of Things Journal*, *6*(5), 8076–8094. https://doi.org/10.1109/jiot.2019.2920987

Deshpande, A., Stewart, K., Lepetit, L., & Gunashekar, S. (2017). *Distributed ledger technologies/blockchain – Challenges, opportunities and the prospects*. https://doi.org/10.7249/RR2223

Di Bella, E., Sillitti, A., & Succi, G. (2013). A multivariate classification of open source developers. *Information Sciences*, *221*, 72–83. https://doi.org/10.1016/j.ins.2012.09.031

Dierksmeier, C., & Seele, P. (2020). Blockchain and business ethics. *Business Ethics: A European Review*, *29*(2), 348–359. https://doi.org/10.1111/beer.12259

Ethereum.org. (n.d.). Community. https://ethereum.org/community

Eyal, I., & Sirer, E. G. (2014). Majority is not enough: Bitcoin mining is vulnerable. In *18th International Conference on Financial Cryptography and Data Security*, 3-7 March, Barbados. https://doi.org/10.1007/978-3-662-45472-5_28

Financial Crimes Enforcement Network (FinCEN). (2013). *Guidance note FIN-2013-G001*. US Department of the Treasury.

Gaggioli, A. (2018). Blockchain technology: Living in a decentralized everything. *Cyberpsychology, Behavior, and Social Networking*, *21*(1), 65-66. https://doi.org/10.1089/cyber.2017.29097.csi

Gervais, A., Karame, G., Capkun, V., & Capkun, S. (2014). Is Bitcoin a decentralized currency? *IEEE Security & Privacy*, *12(3)*, 54–60. https://doi.org/10.1109/MSP.2014.49

Glaser, F. (2017). Pervasive decentralisation of digital infrastructures: A framework for blockchain-enabled system and use case analysis. In *Proceedings of the 50th Hawaii International Conference on System Sciences*. https://doi.org/10.24251/HICSS.2017.186

Glaser, F., & Bezzenberger, L. (2015). Beyond cryptocurrencies – A taxonomy of decentralized consensus systems. In *ECIS 2015 Completed Research Papers*, 29-26 May, Münster.

Hackius, N., & Petersen, M. (2017). Blockchain in logistics and supply chain: Trick or treat? In *Hamburg International Conference of Logistics*, 14 October, Hamburg. https://doi.org/10.15480/882.1444

Holotescu, C. (2018). International Scientific Conference on eLearning and Software for Education. In *International Scientific Conference on eLearning and Software for Education*, 19-20 April, Bucharest.

Homoliak, I., Venugopalan, S., Hum, Q., & Szalachowski, P. (2019). A security reference architecture for blockchains. In *2019 IEEE International Conference on Blockchain* (pp. 390–397), 14-17 July, Atlanta. https://doi.org/10.1109/Blockchain.2019.00060

Inghirami, I. E. (2018). Accounting information systems in the time of blockchain. In *itAIS 2018 Conference* (pp. 1–15), 12-13 October, Pavia.

Konstantinidis, I., Siaminos, G., Timplalexis, C., Zervas, P., Peristeras, V., & Decker, S. (2018). Blockchain for business applications: A systematic literature review. In *BIS, 320,* 384-399. https://doi.org/10.1007/978-3-319-93931-5_28

Kotobi, K., & Bilén, S. (2017). Blockchain-enabled spectrum access in cognitive radio networks. In *2017 Wireless Telecommunications Symposium*, 26-28 April, Chicago. https://doi.org/10.1109/WTS.2017.7943523

Kuo, T.-T., Kim, H.-E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association*, *24*(6), 1211–1220. https://doi.org/10.1093/jamia/ocx068

Labazova, O. (2019). Towards a framework for evaluation of blockchain implementations. In *International Conference on Information Systems*, 15-18 December, Munich.

Lewenberg, Y., Sompolinsky, Y., & Zohar, A. (2015). Inclusive block chain protocols. In *International Conference on Financial Cryptography and Data Security* (pp. 528–547), 30 January, San Juan. https://doi.org/10.1007/978-3-662-47854-7_33

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. *Future Generation Computer Systems*, *107*, 841–853. https://doi.org/10.1016/j.future.2017.08.020

Limata, P. (2019). Blockchains' twilight zones. A reasoned literature review for a critical primer. *EconomEtica*, *76*.

Lin, I.-C., & Liao, T.-C. (2017). A survey of blockchain security issues and challenges. *International Journal of Network Security, 19*(5), 653–659. http://dx.doi.org/10.6633/IJNS.201709.19(5).01

Maas, T. (2019). Initial coin offerings: When are tokens securities in the EU and US? *SSRN Electronic Journal*. 1-77. https://doi.org/10.2139/ssrn.3337514

Manski, S. (2017). Building the blockchain world: Technological commonwealth or just more of the same? *Strategic Change*, *26*(5), 511–522. https://doi.org/10.1002/jsc.2151

Maume, P., & Fromberger, M. (2019). Regulation of initial coin offerings: Reconciling US and EU securities laws. *Chicago Journal of International Law*, *9*(2), 547–585. https://doi.org/10.2139/ssrn.3200037

Mulár, B. O. (2018). *Blockchain technology in the enterprise environment*. Masaryk University.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://bitcoin.org/bitcoin.pdf

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies*. Princeton University Press.

Nawari, N., & Ravindran, S. (2019). Blockchain technology and BIM process: Review and potential applications. *Journal of Information Technology and Construction*, *24*, 209–238. https://www.itcon.org/2019/12

Nguyen, G.-T., & Kim, K. (2018). A survey about consensus algorithms used in blockchain. *Journal of Information Processing Systems*, *14*(1), 101-128. https://doi.org/10.3745/JIPS.01.0024

Niranjanamurthy, M., Nithya, B., & Jagannatha, S. (2018). Analysis of blockchain technology: Pros, cons and SWOT. *Cluster Computing, 22*, 14743-14757. https://doi.org/10.1007/s10586-018-2387-5

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business and Information Systems Engineering*, *3*(59), 183–187. https://doi.org/10.1007/s12599-017-0467-3

Perwej, A., Haq, K., & Perwej, Y. (2019). Blockchain and its influence on market. *International Journal of Computer Science Trends and Technology*, *7*(5), 82–91. http://dx.doi.org/10.33144/23478578/IJCST-V7I5P10

Rizun, P. R., Wilmer, C. E., Burley, R. F., & Miller, A. (2015). How to write and format an article for Ledger. *Ledger*, *1(1)*, 1-12

Rueda, R., Šaljić, E., & Tomic, D. (2020). The institutional landscape of blockchain governance: A taxonomy for incorporation at the nation state. *TEM Journal*, *9*(1), 181–187. https://doi.org/10.18421/TEM91-26

Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D., & Mohaisen, A. (2019). Exploring the attack surface of blockchain: A systematic overview. *ArXiv.Org*. https://arxiv.org/abs/1904.03487

Schoder, D., Fischbach, K., & Schmitt, C. (2005). Core concepts in peer-to-peer networking. In Subramanian, R., Goodman, B. (eds), *Peer-to-peer computing*, 1-27. https://doi.org/10.4018/978-1-59140-429-3.ch001

Schollmeier, R. (2001). A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. In *First International Conference on Peer-to-Peer Computing*, 27-29 August, Linkoping.

Stabile, D. T., Prior, K. A., & Hinkes, A. M. (2020). *Digital assets and blockchain technology: US law and regulation* (1st ed.). Edward Elgar.

Tama, B. A., Kweka, B. J., Park, Y., & Rhee, K. (2017). A critical review of blockchain and its current applications. In *2017 International Conference on Electrical Engineering and Computer Science (ICECOS)* (pp. 109–113), 22-23 August, Yogyakarta. https://doi.org/10.1109/ICECOS.2017.8167115

Tasca, P., & Tessone, C. J. (2019). A taxonomy of blockchain technologies: Principles of identification and classification. *Ledger*, *4*. https://doi.org/10.5195/ledger.2019.140

Troncoso, C., Isaakidis, M., Danezis, G., & Halpin, H. (2017). Systematizing decentralization and privacy: Lessons from 15 years of research and deployments. *Proceedings on Privacy Enhancing Technologies*, *2017*(4), 307–329. https://doi.org/10.1515/popets-2017-0056

Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys & Tutorials, 18*, 2084–2123. https://doi.org/10.1109/COMST.2016.2535718

Tselenti, D. (2019). Blockchain(ed) in "computational parasitism." In *Piracy and Beyond: Exploring 'Threats' in Media and Culture* (pp. 1–13), 23-25 October, Moscow.

US Department of Justice. (2020). *Cryptocurrency enforcement framework*. Report of the Attorney General's Cyber-Digital Task Force. https://www.justice.gov/ag/page/file/1326061/download

Vukolic, M. (2017). Rethinking permissioned blockchains. In *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*, 3-7 April, Abu Dhabi. https://doi.org/10.1145/3055518.3055526

Walch, A. (2019). Deconstructing "decentralization": Exploring the core claim of crypto systems. In C. Brummer (Ed.), *Cryptoassets: Legal, regulatory, and monetary perspectives*. Oxford University Press. https://doi.org/10.1093/oso/9780190077310.003.0003

Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, B., Bass, L., Pautasso, C., Rimba, P. (2017). A taxonomy of blockchain-based systems for architecture design. In *2017 IEEE 6th International Congress on Software Architecture*, 3-7 April, Gotenburg. https://doi.org/10.1109/ICSA.2017.33

Zheng, Z., Xi, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE 6th International Congress on Big Data*, , 25-30 June, Honolulu. https://doi.org/10.1109/BigDataCongress.2017.85

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, *14(4)*, 352–375. https://doi.org/10.1504/IJWGS.2018.095647

Appendix: Listing of reviewed literature

Author(s)	Topic	Applicable layer	Type of literature[1]
1. Adhami et al. (2018)	Initial coin offerings	Primary	J
2. Alharby & Van Moorsel (2017)	Blockchain research theory	Secondary	J
3. Aste et al. (2017)	Blockchain impact on society and industry	Primary	J

Author(s)	Topic	Applicable layer	Type of literature[1]
4. Atzori (2017)	Decentralised governance	External Primary	J
5. Beck & Müller-Bloch (2017)	How society deals with blockchain	External Primary	C
6. Beck et al. (2016)	Application of blockchain	Primary	C
7. Bentov et al. (2016)	Cryptocurrencies, consensus protocols	Primary	C
8. Blocki & Zhou (2016)	Cryptocurrencies, consensus protocols	Primary	C
9. Boudguiga et al. (2017)	Application of blockchain	External Primary	C
10. Burilov (2019)	How society deals with blockchain	Secondary	J
11. Cachin & Vukolic (2017)	Consensus protocols	Primary	C
12. Calvão (2019)	Blockchain impact on society and industry	Primary	J
13. Chen et al. (2017)	Consensus protocols	Primary	C
14. Dai et al. (2019)	Application of blockchain	External Primary	J
15. Dierksmeier & Seele (2020)	Blockchain impact on society and industry	Primary	J
16. Gaggioli (2018)	Blockchain impact on society and industry	External	J
17. Glaser (2017)	Application of blockchain	Primary Secondary	C
18. Hackius & Petersen (2017)	Application of blockchain	External Primary	C
19. Holotescu (2018)	Blockchain impact on society and industry	External Primary	C

Author(s)	Topic	Applicable layer	Type of literature[1]
20. Homoliak et al. (2019)	Blockchain security	Primary	C
21. Inghirami (2018)	Blockchain impact on society and industry	Primary	C
22. Konstantinidis et al. (2018)	Application of blockchain	Primary	C
23. Kotobi & Bilén (2017)	Application of blockchain	Primary	C
24. Kuo et al. (2017)	Application of blockchain	Primary	J
25. Labazova (2019)	Blockchain research theory	External Primary	C
26. Lewenberg et al. (2015)	Blockchain data structures	Primary	C
27. Li et al. (2020)	Blockchain security	Primary	J
28. Limata (2019)	Blockchain impact on society and industry	External Primary Secondary	J
29. Lin & Liao (2017)	Blockchain security	Primary	J
30. Maas (2019)	How society deals with blockchain	Primary	J
31. Manski (2017)	Blockchain impact on society and industry	External Primary Secondary	J
32. Maume & Fromberger (2019)	How society deals with blockchain	External Primary	J
33. Nawari & Ravindran (2019)	Application of blockchain	External Primary Secondary	J
34. Nguyen & Kim (2018)	Consensus protocols	Primary	J
35. Niranjanamurthy, Nithya & Jagannatha (2018)	Blockchain research theory	Primary	J

Author(s)	Topic	Applicable layer	Type of literature[1]
36. Nofer et al. (2017)	Application of blockchain	External Primary Secondary	J
37. Perwej et al. (2019)	Blockchain impact on society and industry	External Primary	J
38. Rueda et al. (2020)	Application of blockchain	External Primary Secondary	J
39. Ali Syed et al. (2019)	Application of blockchain	External Primary Secondary	J
40. Tama et al. (2017)	Application of blockchain	External Primary	C
41. Tasca & Tessone (2019)	Blockchain taxonomy, ontology or classification	Primary Secondary	J
42. Tschorsch & Scheuermann (2016)	Blockchain taxonomy, ontology or classification	Primary	J
43. Tselenti (2019)	Blockchain impact on society and industry	External Primary	C
44. Xu et al. (2017)	Blockchain taxonomy, ontology or classification	Primary	C
45. Zheng et al. (2017)	Blockchain taxonomy, ontology or classification	Primary	C
46. Zheng et al. (2018)	Application of blockchain	Primary	J
Count (J = 26, C = 20)			

[1] J = Peer-reviewed journal article, C = Peer-reviewed conference paper