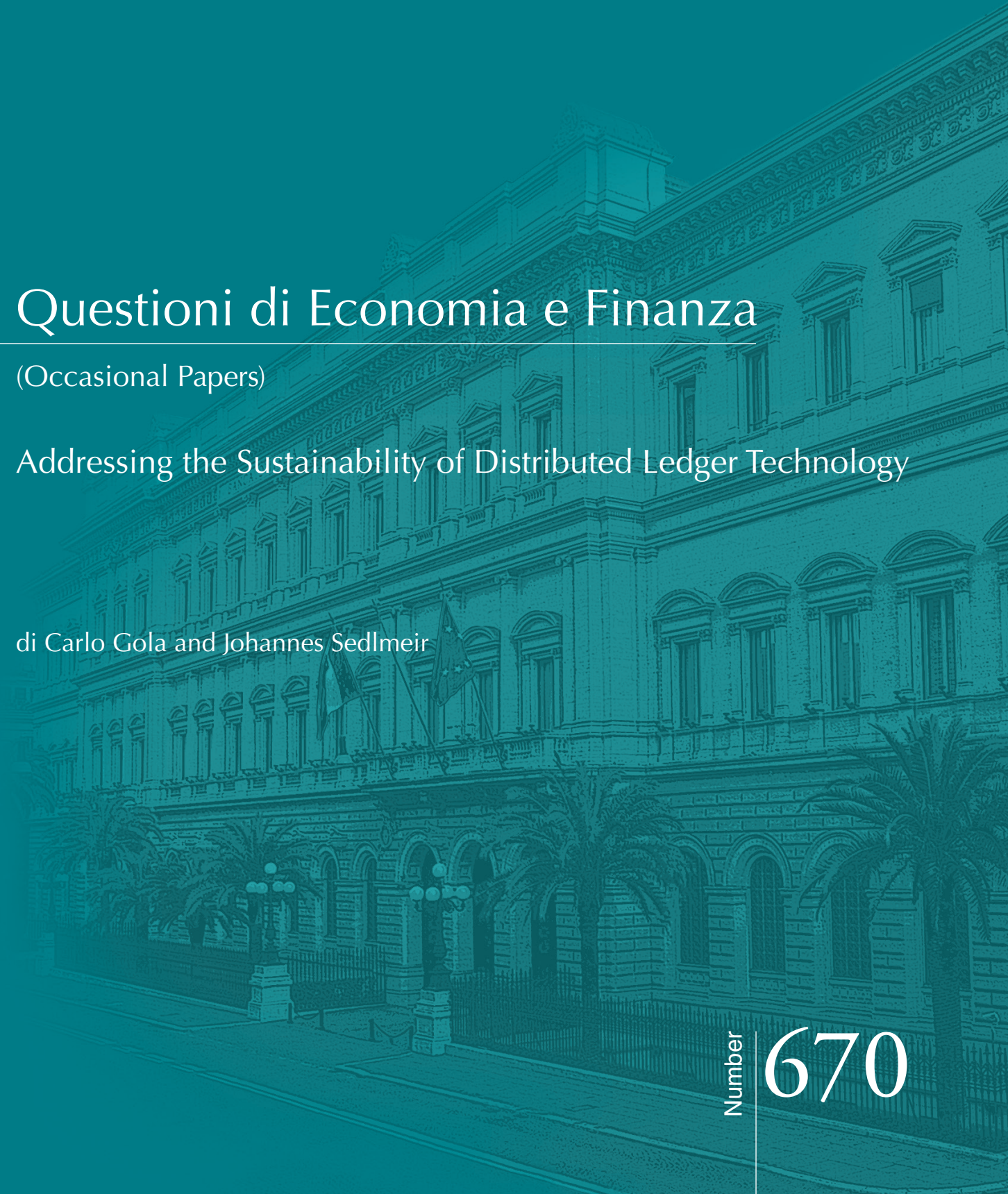
BANCA D'ITALIA
EUROSISTEMA

Questioni di Economia e Finanza

(Occasional Papers)

Addressing the Sustainability of Distributed Ledger Technology

di Carlo Gola and Johannes Sedlmeir



February 2022

Number 670

BANCA D'ITALIA
EUROSISTEMA

Questioni di Economia e Finanza

(Occasional Papers)

Addressing the Sustainability of Distributed Ledger Technology

di Carlo Gola and Johannes Sedlmeir

Number 670 – February 2022

The series Occasional Papers *presents studies and documents on issues pertaining to the institutional tasks of the Bank of Italy and the Eurosystem. The* Occasional Papers *appear alongside the* Working Papers *series which are specifically aimed at providing original contributions to economic research.*

The Occasional Papers *include studies conducted within the Bank of Italy, sometimes in cooperation with the Eurosystem or other institutions. The views expressed in the studies are those of the authors and do not involve the responsibility of the institutions to which they belong.*

The series is available online at www.bancaditalia.it .

ISSN 1972-6627 (print)
ISSN 1972-6643 (online)

Printed by the Printing and Publishing Division of the Bank of Italy

ADDRESSING THE SUSTAINABILITY OF DISTRIBUTED LEDGER TECHNOLOGY

by Carlo Gola[*] and Johannes Sedlmeir[**]

Abstract

The work proposes policies to improve the environmental sustainability of distributed ledger technology (DLT). While the proof-of-work (PoW) consensus protocol requires large amounts of electricity, several DLT protocols consume much less, while still being sufficiently reliable and decentralized. To move from a PoW protocol to a greener system, such as proof-of-stake (PoS) or proof-of-authority (PoA), the consensus of the majority of miners (measured by their computing power) is required during the transition period to preserve the security requirements. Given that miners have an incentive to maintain the status quo, this paper illustrates various policies designed to bring about the transition. We aim to show that the current policy approach adopted by banking and financial regulators, based on the principle of technological neutrality, may need a reappraisal in order to consider the 'sustainability' criterion. Policymakers should not stifle financial innovation; nevertheless they should intervene if technology is a source of negative externalities.

JEL Classification: G18, Q56, O3, O16, K2, H23, L63.
Keywords: blockchain, carbon tax, DLT, energy consumption, financial market infrastructures, green consensus protocols, prudential requirements, sustainability, environmental transaction tax.
DOI: 10.32057/0.QEF.2022.0670

Contents

[*] Bank of Italy, Regulations and Macroprudential Analysis Directorate.
[**] FIM Research Center, University of Bayreuth, Germany.

1. Introduction[1]

Technological innovation is transforming the supply of goods and services. The diffusion of decentralized cryptographic protocols favors the proliferation of digital tokens, automation (*smart contracts*), and authenticity (*cryptographic notarization*), with a plurality of functions. In the banking and financial markets, distributed ledger technology (DLT) presents new opportunities and risks while transforming the economic landscape in several sectors, including the payment, clearing, and settlement systems. The rapid and increasing adoption of crypto-assets for transferring and storing value poses legal and financial stability challenges to regulators. Still, the advancement of the digital transformation through DLT also provides many new opportunities, offering more innovative, inclusive, and transparent financial solutions and promising to reduce information asymmetries and to increase market efficiency.

DLT has, however, been subject to criticism regarding its energy consumption. Sustainability and the transition to a safe, climate-neutral, resource-efficient economy are at the center of a large and growing number of international initiatives, in line with the Paris Agreement adopted under the United Nations Framework Convention on Climate Change (the 'Paris Agreement').[2] In the banking and financial sector, several international bodies, including the Financial Stability Board (FSB),[3] the Basel Committee on Banking Supervision (BCBS)[4], the Committee on Payments and Market Infrastructures (CPMI), the International Organization of Securities Commissions (IOSCO),[5] and the recently established Network of Central Banks and Supervisors for Greening the Financial System (NGFS),[6] have conducted work or issued guidelines to promote the financing of environmentally sound and sustainable projects, while ensuring adequate safeguards for financial stability. Europe is adopting a comprehensive strategy for the financial sector to support a sustainable economy with the EU Action Plan on Sustainable Finance.[7] Under the Digital Finance Strategy,[8] the EU intends to foster innovation, reduce the fragmentation of financial markets, support the digital transformation, and mitigate IT risks. In this context, three initiatives have been launched, relating, respectively, to the Markets in Crypto-Assets Regulation (MiCAR), the Digital Operational Resilience Act (DORA), and the proposal for a Regulation on a pilot regime for market infrastructures based on DLT (*DLT pilot regime*).[9]

---

[1] We are grateful to Michele Ciampi (University of Edinburgh, UK) for his useful suggestions on how to upgrade blockchains, and to Christian Stoll (MIT Center for Energy and Environmental Policy Research) for allowing us to use some of the data presented here. We are also grateful to Gabriele Marcelli, Fabrizio Borselli, Roberta Fiori, and Concetta Galasso for their useful comments and suggestions, and to Prof. Ivan Visconti for the clarification of some important aspects. Special thanks go to Paolo Angelini for his encouragement to explore the topic of this paper. Before proceeding, a caveat is needed: given the complexity and the heterogeneous literature on the topic, errors and inaccuracies may occur. No endorsement is made of any single business model or initiative. The opinions expressed and conclusions drawn are those of the authors alone and do not necessarily reflect the views of their institutions.

[2] See: https://unfccc.int/process-and-meetings/the-paris-agreement/the-paris-agreement.

[3] See: https://www.fsb.org/work-of-the-fsb/financial-innovation-and-structural-change/crypto-assets-and-global-stablecoins/.

[4] The BCBS is the standard-setter for the prudential regulation of banks and provides a forum for regular cooperation on banking supervisory matters. Its 45 members comprise central banks and bank supervisors from 28 jurisdictions.

[5] See CPMI-IOSCO (2021), https://www.bis.org/cpmi/publ/d198.htm.

[6] Created in 2017, the NGFS is a network of 95 central banks and financial supervisors that aims to accelerate the scaling up of green finance and to develop recommendations for the role of central banks in climate change.

[7] See: European Commission (2018): https://ec.europa.eu/info/publications/sustainable-finance-renewed-strategy_en.

[8] See: https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en

[9] See the Proposals for Regulations of the European Parliament and of the Council on: Markets in Crypto-assets, and amending Directive (EU) 2019/1937 (COM/2020/593 final); digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 (COM/2020/595 final); and a pilot regime for market infrastructures based on distributed ledger technology (COM/2020/594 final).

Among the guiding principles of a prospective regulation on crypto-assets and decentralized finance ('DeFi'), the *technology-neutrality* principle is often mentioned.[10] However, as DLT is introducing a new paradigm, where economic and technological aspects are deeply intertwined, one should simultaneously consider all related aspects. In our opinion, a reappraisal of this principle is therefore necessary. This paper aims to analyze the sustainability of DLT systems (or blockchains)[11] and the ongoing technical developments.[12] We organize the paper as follows: after a brief description of the technical characteristics of DLT consensus protocols: voting-based consensus, proof-of-work (PoW), and proof-of-stake (PoS) (Section 2), we describe the explanatory variables to determine the environmental impact (Section 3). We then provide some data on the energy consumption of proof-of-work-based DLT (Section 4) and give an overview of potential strategies to promote a transition towards sustainable DLT (Section 5). Section 6 concludes.

2. DLT and consensus mechanisms

The term DLT describes a particular kind of distributed systems whose state is represented by a shared ledger. Information in the ledger can be read and modified by nodes (users, entities) participating in the system in a synchronized and secure way without needing a centralized, trusted third party. DLT has applications in finance and payment systems, industry, and the public sector.[13] Managing a traditional archive or ledger (be it a notary system, a real estate registry, or a payment system) typically requires a third party to which this function has been assigned. Therefore, individual economic agents must trust an institution or central counterparty. In a payment system, this trusted third party tracks the ownership relationships for assets and, thus, solves the double-spending problem.[14] By contrast, in a decentralized system – i.e., a system composed of parties who do not necessarily trust or do not even know each other – there is no distinguished trusted entity to coordinate all state updates and, thus, maintain an authoritative version of the ledger. Consequently, achieving the level of synchronization and security necessary to set up a reliable infrastructure for transferring digital assets is more challenging and requires a different approach. To find a robust agreement among all participants to the system upon the valid state of the ledger, a so-called *consensus mechanism*[15] is used, which resorts to principles of game theory and/or cryptography to guarantee the incentive structures and the functioning of the system even under the potential presence of failures or malicious

[10] Under a *technology-neutrality* principle, the regulatory perimeter and the subsequent treatment of financial products/services and activities are not influenced by the technical medium through which the product/service or activity is provided, see: OECD (2021a), p. 12.

[11] In this paper we use DLT and blockchain technology synonymously, even though the latter is, strictly speaking, a subset of the former.

[12] This paper does not cover an analysis of risks and policy implications associated with crypto-assets such as Bitcoin, but only the environmental impact of the underlying DLT. For an overview of policy issues of crypto-assets, see: Gola, C., and Caponera, A. (2019); on recent market developments, see IMF – GFSR (2021). In addition to sustainability, other overarching principles for a sound DLT protocol are a good technical base (efficiency, scalability, interoperability, operational integrity) and good decentralized governance (accountability, enforceability of AML/CFT as well as respect of privacy safeguards).

[13] See: van der Waal et al. (2020).

[14] The *double-spending problem* is specifically challenging in the digital world, where the transfer of value is translated to the transfer of digital objects – which can easily be copied if no agreed-on registry that documents the ownership relationships is used.

[15] *Consensus* is a fundamental problem in *fault-tolerant* distributed systems (DLT is a subset of distributed systems) (see Annex). Consensus involves multiple servers 'agreeing' on values. Once they reach a decision on a value, that decision should be practically final. Typical consensus algorithms make progress when a specific share (for instance, 51%) of their servers is available and follows the protocol. The threshold (or share) generally depends on security requirements (resistance only against crashes or also against malicious servers) and network assumptions (how badly can messages be delayed).

economic agents. There are three main categories of consensus mechanisms for DLT systems: proof-of-work (PoW), proof-of-stake (PoS), and proof-of-authority (PoA).[16]

- In PoW, also known as "Nakamoto consensus" as the pseudonymous creator of Bitcoin invented it, DLT participants willing to update the shared ledger need to prove that they performed a certain amount of computational work; they do so by submitting solutions of computationally intensive cryptographic problems and, thus, proving the spending of substantial energy resources;
- In PoS, DLT participants willing to update the shared ledger need to prove having a 'stake' in the system, meaning to possess a certain quantity of the specific cryptocurrency native to the DLT system itself;
- In PoA, a subset of participants with a special role in the system act as 'notaries'; they are the only participants authorized to perform ledger updates employing cryptographic signatures. With PoA, individuals earn the right to become validators, so there is an incentive to retain the position that they have gained. In practice, there are also hybrid models that are partially decentralized.

Table 1 - Types of crypto-assets

Name	PoW protocol	Type	DLT	Market capitalization *(mil. euro; Dec. 2021)*	Market share *(%)*
Bitcoin	Yes	variable	permissionless	845,075	41.19
Ethereum	Yes	variable	permissionless	434,35	21.17
Binance Coin	No	stablecoin	permissioned	84,431	4.12
Tether	Yes (§)	stablecoin	permissioned (*)	67,302	3.28
Solana	No	variable	permissionless (**)	47,807	2.33
Cardano	No	variable	permissionless	40,525	1.98
USD Coin	Yes (§)	stablecoin	permissioned (*)	36,741	1.79
XRP (Ripple)	No	variable	permissioned	35,545	1.73
Polkadot	No	variable	permissionless	25,819	1.26
Terra (Luna)	No	stablecoin	permissionless	20,710	1.01
First 10 crypto-assets				**1.638,305**	**79.85**
Total market capitalization				**2.051,688**	**100**

Source: Coinmarketcap data and market information
(§) As Ethereum-based tokens, there is no separated ledger for them, but the underlying DLT is PoW-based. Hence, transactions with these tokens are associated with mining activity, so we consider them PoW-based, too.
(*) As Ethereum-based tokens, there is no separated ledger for them, but the tokens' governance is highly centralized[17], so we consider them permissioned, although the underlying DLT is permissionless.
(**) Because of the high requirements in terms of hardware and the corresponding low number of nodes, Solana could also be considered a permissioned DLT, although formally, participation is not heavily restricted.

Both research and experience demonstrate that PoW is robust and scales to many nodes (for example, currently around 13,000[18] in the case of the Bitcoin blockchain). However, this robustness comes at the cost of high electricity consumption. Although the estimates are complex and sometimes

[16] For a basic description of proof-of-work, poof-of-stake, and related aspects (such as the role of nodes, hash functions, the 'cryptographic puzzle', etc.), see the Annex.
[17] See, for instance, Barbereau et al. (2022).
[18] This number refers to full nodes (i.e., the ones that store the entire blockchain and from which others can bootstrap), but they do not necessarily correspond to miners involved in PoW, which could be much higher.

controversial, there is consensus in the literature that PoW-based blockchains have a strong negative environmental impact. For example, Bitcoin's electricity consumption is now larger than that of industrialized countries such as Austria or Sweden.[19] On the other hand, alternative consensus mechanisms are very different and, in particular, do not have comparable energy consumption characteristics. For example, non-PoW protocols are becoming increasingly popular for newer cryptocurrencies, albeit with a lower market capitalization (see Table 1). A popular PoW-based blockchain, Ethereum, is in the process of moving to PoS (but to date, the transition has not been completed and has been delayed several times),[20] with one of the key reasons being sustainability.[21] Moreover, the consensus mechanisms for private permissioned blockchains frequently used in industry consortia or the public sector, such as Hyperledger Fabric or Quorum, are fundamentally different and not energy-intensive.

To understand the reasons for the diverging environmental footprint characteristics, it is necessary to have some fundamental understanding of the role and functioning of consensus mechanisms both in a *permissionless* (open participation) and *permissioned* (restricted participation) setting, which equally affects holders for variable and stablecoins.[22] In a permissionless blockchain, anyone can participate, and participants are pseudonymous[23] (sometimes even anonymous). Permissioned blockchains, on the other hand, operate under a governance model that facilitates a certain degree of trust. In particular, a permissioned blockchain provides a way to secure the interactions among a group of economic agents with a common goal that know each other but that may not fully trust each other. By relying on the participants' identities, a permissioned blockchain can use more traditional *crash fault-tolerant* (CFT) or *byzantine fault-tolerant* (BFT) consensus protocols that do not require energy-intensive mining activity. In the following, we start describing the "private" configuration, which is historically the first kind of DLT, conceptualized in the 1980s, and arguably simpler to understand from a technical perspective[24], and closer to the governance systems of a centralized register. Afterward, we will consider fully decentralized blockchains and illustrate the problems that some of them pose from the environmental impact point of view.

[19] DLT protocols could be helpful for improving the use of energy in peer-to-peer energy trading to Internet of Things (IoT) applications, see Andoni et al. (2019); this, nonetheless, does not necessarily justify the PoW blockchains given the considerable negative environmental effects they can have.

[20] On the Ethereum transition toward PoS, see: https://ethereum.org/en/eth2/beacon-chain/.

[21] Another key reason is scalability/performance; however, this should not be attributed to the high computational effort of mining in PoW, which is a completely separate aspect. There are several reasons why scaling PoS blockchains may be easier than PoW blockchains; one of them is the fact that *sharding* – a scaling technique that bases on splitting the blockchain into several sub-blockchains – is challenging to implement in PoW because it is difficult to foresee an account's mining power and, thus, hard to prevent significantly centralized sub-blockchains. By contrast, voting power in PoS can be observed directly through looking at the amount of cryptocurrency that an account holds and, thus, be balanced among shards accordingly.

[22] Stablecoins are designed to maintain a 'stable' value relative to reference assets (currencies, commodities, other crypto assets). For a list of stablecoins, see: https://coinmarketcap.com/it/view/stablecoin/.

[23] A 'miner' is pseudonymous if only its IP address is public. As far as crypto asset users are concerned, pseudonymity refers to the fact that the wallet is not directly tied to their name, but rather to one or more specific cryptographic keys (or "addresses"). Thereby, bitcoin owners are not identifiable *per se*, but all their transactions are publicly available in the blockchain. Crypto-assets exchanges, wallet providers, and custodians are often required by law to collect their users' personal information. Moreover, through sophisticated analysis of addresses and their transactions, substantial information can be gathered to associate IP addresses with bitcoin addresses (Biryukov et al., 2014).

[24] From a technical perspective, there are several intricate details that need to be considered to make the protocol secure in a potentially asynchronous (i.e. based on independent, parallel, events) environment like the Internet, where messages can be delayed and where components can crash or be compromised. We will not discuss these aspects in detail here.

2.1 Permissioned blockchains

In a permissioned DLT system, where only authorized nodes whose identity is known can participate, relatively simple and efficient voting-based consensus mechanisms are possible.[25] This can either mean *uniform voting weight* (one vote per party or node) or *reputation-based voting weight*. In some sense, the former corresponds to egalitarian decision-making, the latter to a representative democratic system. In both cases, the consensus mechanism creates an incentive structure that results in some kind of dynamically stable equilibrium (similar to what is obtained by Nakamoto consensus through PoW).[26]

Permissioned blockchains are often used in industry consortia or federated systems in the public sector, as there is a pre-defined set of entities that need to be involved. Permissioned blockchains can also offer a high base throughput because stakeholders can define hardware and bandwidth requirements in the consortium; the partners can typically afford a high-quality server with a good internet connection. Moreover, they allow for low latency with instant finality because it is clear who can vote, so typically there are no long waiting times to account for network latencies or failures. Thus, blocks are confirmed through being signed by a specific majority or through a leader who was determined through a majority decision. Another advantage of permissioned blockchains is that they generally have fewer (but still have) issues with excessive data visibility creating privacy problems. Moreover, the entities involved in it are known and can be held accountable for their actions, and there usually are no issues with potentially high transaction fees, while fees in the existing cryptocurrencies are sometimes difficult to control.

Self-enforcing agreement – Popular examples for voting-based consensus mechanisms are *crash-fault-tolerant* (CFT) consensus mechanisms like an algorithm known as Redundant and Fault-Tolerance (RAFT) (used, for instance, in Hyperledger Fabric and Quorum),[27] and *Byzantine Fault Tolerance* (BFT) (see Annex). These types of protocols often make some use of a reputation system, which is why the name "proof-of-authority" is sometimes used. *Fault tolerance* is a feature of the DLT to reach consensus (agreement on the same value or set of information) even when some of the nodes in the network fail to respond or respond with incorrect information. This typically requires some interactions among members. The critical value is the maximum number of crashes (or failures, including malicious attacks) that the network can withstand at any time for a given total number (N) of active nodes. Both CFT and BFT consensus mechanisms are not a new development in computer science; CFT systems have been conceptualized already in the 1980s (e.g., Paxos),[28] [29] and a form of BFT consensus (PBFT) was already implemented in 1999.[30] CFT systems are present in many distributed, high-performance cloud systems that require high availability guarantees, today, for example, in AWS' Dynamo DB.[31] Through the attention for blockchains and decentralization after the invention of Bitcoin, however, many new systems with higher fault tolerance for cross-organizational applications of blockchains have been developed. The key difference is in the assumptions and capacity to withstand threats or failures: CFT can support less than N/2 system

[25] It is important to recognize that the distinction between 'permissioned' and 'permissionless' concerns the governance, i.e., organizational features of the DLT; from a pure technical perspective the main difference is between a fully centralized infrastructure (as traditional payment systems) and a decentralized one (DLTs having two or more nodes). A decentralized system is a collection of autonomous computing elements that appear to its users as a single coherent system to achieve a unified goal. For more details on this point, see: Urbinati (2021), pp. 61-62.
[26] See: Badertscher et al. (2018).
[27] For a nice visualization of the consensus mechanism produced by the RAFT algorithm, see: https://raft.github.io/.
[28] See: https://en.wikipedia.org/wiki/Paxos_(computer_science).
[29] See: Lamport (2001).
[30] See: Castro and Liskov (1999).
[31] See: Sedlmeir et al. (2022).

failures, while there are no guarantees on adversary nodes. BFT provides correctness guarantees in the presence of less than N/3 failures[32] of any kind, including byzantine.

Most voting-based permissioned consensus mechanisms have a notion of an *elected leader* that proposes blocks that the remaining *follower nodes* then confirm. The server 'elected' as leader is chosen before each validation, but it can also last for more than one validated block. The leader is the sole node responsible for ordering and committing new transactions to the DLT. If the leader crashes or does not behave according to the rules, it is replaced in a new election before validating the new block of transactions. These decentralized self-organized consensus mechanisms involve two or three steps (depending on the protocol):[33]

- **Pre-prepare**: the *leader* declares the intention of committing to a new block
- **Prepare**: *followers* confirm the intention of committing to a new block proposed by the leader (this step is needed only under the BFT protocol)
- **Commit**: the *leader* commits or aborts the transaction, broadcasting the action to the *followers*. If the leader crashes, a new leader is elected, and the transition returns to phase one ("pre-prepare").[34]

The repeated communication is for mutual reassurance between the nodes. Hence, even if the current leader crashes or misbehaves after having sent notifications of a decision ('new block') only to a subset of following nodes, they can still find agreement in the next step. While nodes blindly follow the leader in CFT and are hence vulnerable to a malicious leader, in BFT, the second round of messages allows nodes to learn about the decisions of the other nodes. This cross-checking enables detecting and replacing a malicious leader.

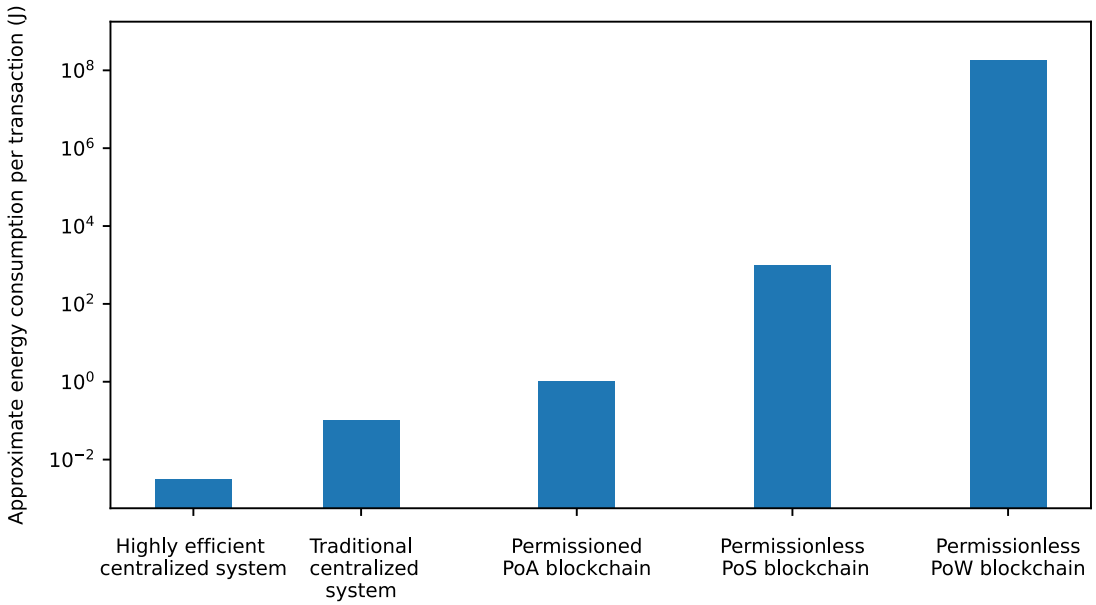
Efficiency and environmental footprint - The computational complexity of voting-based consensus mechanisms grows with the number N of nodes in the network. As a rule of thumb, the leader – who does the most work and becomes the bottleneck – needs to send and receive N messages per block under CFT and 2N messages under BFT. In the case of BFT, each of these messages contains up to N digital signatures that can, however, be aggregated. Consequently, these consensus mechanisms are only suitable for distributed ledgers with a moderate number of nodes; performance degradation often becomes significant with more than 50 nodes already.[35] Therefore, as long as performance degradation is moderate, this also means that no considerable compute power is necessary for consensus. By experience, checking individual transactions' signatures and updating the database state consumes more resources than consensus when blocks are not too small.

In terms of energy consumption, this implies that a permissioned blockchain with N nodes consumes around N times the energy of a centralized system, but still much less than a fully decentralized system (see Figure 2). The figure illustrates that a permissionless PoW-based DLT consumes around a thousand times more energy than a permissionless PoS-based DLT, around a million times more than a permissioned PoA-based DLT or a traditional centralized system, and up to a billion times more energy than a highly efficient centralized system. This result is clearly an approximation, since a centralized system would not do as many cryptographic operations like signature checks and

[32] This, however, is true only if there is no upper bound on the delay of messages – with strong synchronicity assumptions, less than N/2 is possible.
[33] See: EU Blockchain Observatory and Forum (2021).
[34] CFT consensus mechanisms can operate while most nodes have not crashed but cannot cope with malicious nodes, as the followers blindly "follow" the leader as long as it is running. As a result, CFT consensus mechanisms should be used only in blockchains with a high level of pre-existing trust or at least accountability between nodes, or if some degree of fault-tolerance against malicious behavior is achieved on another level (e.g., in Hyperledger Fabric) (see EU Blockchain Observatory and Forum (2021), p. 11.
[35] See: Sedlmeir, Ross, et al. (2021).

hashing; on the other hand, one needs to keep in mind that centralized systems rarely run without any redundancy to be prepared for a power outage or a crash, but in different applications, different degrees of redundancy are required. Specifically, some redundancy across organizational boundaries is often intentional in blockchain applications. Consequently, while the replicated operation of transactions in a typical permissioned blockchain may make it one or two orders of magnitude more energy-intensive than a highly efficient, idealized centralized system, energy consumption is still not far from that of a standard enterprise application. Moreover, suppose one can only save small amounts of paper or travel through digitizing additional workflows for which so far, no centralized system could provide a digital solution (e.g., for organizational reasons). In that case, there will likely be net energy savings.

Figure 2 – Approximate energy consumption per transaction



Source: Adapted from Sedlmeir et al. (2020). On the y-axis, (J) is the physical unit "Joules" for energy consumption; one Joule corresponds to maintaining a power of 1 Watt for 1 second, i.e., 1 J = 1 Ws.

To put this in a concrete context of the banking sector, let's take the case of a Central Bank Digital Currency (CBDC). As is well known, central banks are discussing how a DLT-based digital currency could support a central bank in performing its functions and analyzing potential design options.[36] Let's imagine a wholesale CBDC in which 30 organizations run high-performance servers as DLT nodes that consume up to 500 W each. In a cloud-based instance, this could correspond to a server with 28 cores and 196 GB of RAM that runs consistently on high CPU and memory utilization.[37] Detailed measurements with Hyperledger Fabric and Quorum suggest that common permissioned blockchains struggle to parallelize well enough to make use of such high-performance hardware configurations and seem to reach a level of saturation with 8 cores and 32 GB of RAM already, achieving a few thousand simple transactions per second[38,39]. Blockchains like Solana have conducted further optimizations that allow for better parallelization and, thus, hardware resource utilization but

[36] For a comprehensive overview, see: Urbinati et al. (2021).
[37] See, for example, https://medium.com/teads-engineering/estimating-aws-ec2-instances-power-consumption-c9745e347959.
[38] See: Guggenberger et al. (2021).
[39] See: Androulaki et al. (2018).

still only require 12 cores and 128 GB of RAM per node.[40] Assuming such ongoing improvements in parallelization, it seems realistic that a permissioned blockchain as the backend of a European CBDC run by 30 nodes in a voting-based blockchain would consume approximately 15,000 W, provided that the infrastructure for networking is already in place. The reader may want to compare this to 10 hairdryers, a fraction of an electric vehicle's peak fast-charging power or 1 % of the peak power of a small wind turbine. Client applications would need to be added, but there are no considerable differences compared to a centralized backend in this regard.

In conclusion, we can state that if the DLT is designed in a permissioned setting, under fairly general conditions, the energy consumption is not at all an issue, even if compared with a fully centralized system. Moreover, they offer solid performance, and from a theoretical standpoint (as well as from the anecdotal evidence available so far), voting-based consensus mechanisms seem to be resistant to external adverse events. The only limitation is the number of nodes that this setting can support since the performance degradation typically becomes significant with more than 50 nodes. Improved consensus mechanisms like HotStuff BFT may relax these limitations to several hundreds of nodes.[41]

2.2 Permissionless blockchains

Let's now turn to permissionless DLT, for which the first consensus mechanism was introduced in the Bitcoin blockchain and adopted by hundreds of other crypto-assets that build on an open system. There is no control over the number, affiliation, and identity of entities that participate in consensus within this setting.[42] Each member of the network operating the protocol (typically open source, i.e., associated software components that are freely available through the web) can participate in consensus, validating and confirming the correctness of the transaction just connecting their computer to the internet and maintaining an own copy of the ledger. A well-known problem in this context is the 'Sybil attack' – attacks where a malicious agent tries to subvert the majority rule of the Network service by creating many pseudonymous identities and using them to gain a disproportionately large influence. Without countermeasures, this would – at modest cost – allow to take a disproportionate voting power in the system and outvote the honest majority, compromising the network's integrity and trust guarantees. Hence, permissionless distributed ledgers need to incorporate defense against Sybil attacks.

The common approach to prevent Sybil attacks is to couple participants' voting power in consensus to some scarce resource that one cannot replicate at low costs and that can be verified in the decentralized system.[43] The first mechanism to achieve this was Poof-of-Work (PoW), suggested by the pseudonymous Satoshi Nakamoto for the Bitcoin network. The scarce resource in PoW is computational work, which is associated with computing expenditures: 'mining' hardware and electricity. Computational work is proven by solving cryptographic hash puzzles, more precisely, finding pre-images under a specific cryptographic hash function (for instance, the Secure Hash Algorithm (SHA-256) in Bitcoin; see Annex) that starts with a certain number of zeros, determined by the current difficulty. As no more efficient way than brute-force (random trial and error) is known to date for finding such pre-images, an entity that presents a solution will, on average, have tried a large number of pre-images and, thus, in expectation has provably invested computational resources.

[40] See: https://docs.solana.com/running-validator/validator-reqs.
[41] See: Jalalzai et al. (2020).
[42] It is possible to use a permissionless DLT to provide *public* access to the network, while keeping a *private* and therefore limited access to the participants in the agreement procedure (consensus protocol) responsible for the maintaining the state of the system.
[43] See: Sedlmeir et al. (2020).

Solving the cryptographic puzzle makes the miner eligible to create the next block and receive corresponding rewards in the form of new crypto coins created by the protocol and the fees for the transactions included to incentivize participation. In the long run, an entity's share of hashing power in the network is the share of blocks produced by this entity. This makes 'voting power' proportional to 'computational power' and, thus (with a different proportionality factor depending on the hardware used), electricity consumption, establishing the tying between voting weight and a scarce resource as intended on average. Collective consensus on the status of the updated database is reached when the majority, in the metric of hash-rate, of nodes (called 'miners') operating in the network, agree that a given block is correct. More precisely, when 51%[44] of the computing power used globally by the miners operating on the blockchain *at that particular moment* (in fact, rather for around an hour or so) is reached.[45] Originally, it was intended that PoW is essentially a 'one-CPU-one-vote' system.[46] However, the large incentives have led to the development of specialized hardware – called application-specific integrated circuits (ASICs) many orders of magnitude more energy-efficient in computing hashes than CPUs, so mining with CPUs in common computers is no longer attractive from an economic perspective.

From the above, and in the light of what we describe in the Annex, it follows that the great computational effort is not an inefficiency of PoW, but rather a feature deliberately inserted in the protocol as a sufficient condition to increase the costs of updating the ledger and, in doing, so discouraging malicious behavior by the miners. It is not about the inefficiency of existing hardware: In the long run, PoW's energy consumption does not decrease when more energy-efficient mining hardware becomes available because the complexity of the computational puzzles will increase automatically. Instead, a balance of rewards (for new blocks created) and costs (capital expenditures and operating expenses) determines the energy consumption. To contribute to the validation of the transactions requested by the end-users, miners are rewarded for contributing a new block with a certain number of native tokens plus a *variable fee* paid by the end-users for their transactions. The higher the price of the digital token (quoted and exchanged against money or other digital tokens), the greater the incentive to incur the computational costs (the *break-even point* is lower). In the case of Bitcoin, the algorithm is designed to generate a pre-defined number of tokens – 21 million. Once this number is reached, the process should continue with only the contribution of the fees.[47] While this may mitigate the energy consumption problem because the economic value of energy spent will not exceed the total transaction fees at this point, we believe that the cumulative negative environmental effect remains problematic. Only a coalition equal to 51% of the 'miners' (again weighted by hash rate) could change the algorithm (see Section 5). This is a double-edged sword: on the one hand, this could prove useful to address a problem for which a change in the protocol is required to solve it; on the other hand, it can be less secure against future *51% attacks* with malicious purposes.[48]

[44] In fact, there are strategies for an adversary that – depending on the nodes' behavior – could reduce the required minimum threshold of an adversary's computing power to 25% or 33%. However, for simplicity, we will refer to 51%. For more details, see: Eyal and Sirer (2014).

[45] It is important to underline the specification 'at a given moment': in principle, in market situations where few miners are active on the blockchain, a few mining groups could coordinate themselves and reach 51% of the computing power.

[46] See: Nakamoto (2008), p. 3.

[47] The phasing-out is set by the Bitcoin core software through a mechanism that periodically halves the number of new tokens created per block approximately every four years.

[48] For example, in March 2013, a software review caused a hard fork in the Bitcoin network, which could have created a generalized double-spending problem. Only the timely intervention of two mining pools allowed the system to resume its proper functioning, see: Musiani *et al.* (2018). This event shows that if a sufficiently big mining pool can coordinate a strategy, it could in principle promote a transition toward a cleaner technology (see Section 5).

As already mentioned, another popular consensus mechanism for permissionless blockchains is proof-of-stake (PoS), in which the scarce resource is each user's share of the blockchain's native token (see Annex). While this mechanism is not energy-demanding by design and seems to provide comparable security guarantees, the initial coin allocation is critical since poor initial distribution can result in the permanent concentration of power. The probability of creating the next block is proportional to the number of coins held (or received by delegation). Consequently, remuneration corresponds to interest at a rate that is – on average – the same for every participant. While rich users get more rewards in absolute figures, their relative stake and, thus, their voting weight does not change over time.[49] PoS systems are orders of magnitude less energy-intensive than PoW systems. The remaining inefficiency comes from replication, as all nodes perform the same validation and database operations. Since permissionless blockchains can have many nodes, the energy consumption of a PoS blockchain can hence be thousands of times higher than that of an idealized centralized system. However, suppose nodes use appropriate hardware like a Raspberry Pi or servers that are running anyway. In that case, the total power consumption per transaction can still be lower than that of centralized systems with less targeted redundancy and operational inefficiencies, like VISA or PayPal.[50]

3. The explanatory variables for the environmental impact assessment of PoW blockchains

A growing body of literature tries to estimate the environmental impact of blockchains.[51] The most common estimation model is of the 'bottom-up' type. It considers the individual polluting factors mainly based on technical criteria. Let's see the main aspects.[52]

- **Computational devices (hardware)** – The first aspect to consider is miners' type of electronic device. More powerful hardware allows the 'cryptographic puzzle' (see Annex) to be solved faster. It, therefore, increases the probability of outpacing the competitors in the race to win the digital token. The metric is given by the number of attempts (*hashes*) to find solutions per second (often measured in trillions of hashes (Terahashes) per second).[53] Over the years, the industry has produced increasingly powerful and efficient dedicated processors. Currently, ASICs are capable of processing tens or hundreds of Terahashes per second. Some cryptocurrencies, however, use hashing algorithms in which ASICs do not have a meaningful advantage over traditional graphics cards (GPUs). Miners enter the market and activate or deactivate their computers according to the expected profit (for given operating costs). Since it is hardly possible to know exactly the type of devices used by miners globally, scholars have proposed various expedients, such as estimates on the devices available on the market, the most efficient ones for certain blockchains, or a basket of those considered most used. The estimates tend to provide a range between a minimum and maximum value that is often quite large.[54]

- **The difficulty of the cryptographic puzzle** – The next step concerns the complexity of the cryptographic puzzle. The difficulty is typically time-dependent to keep the block production rate constant. Specifically, suppose hardware becomes more energy efficient over time. In that case, mining is more attractive for miners with the newest hardware, so the hash rate increases, and so

[49] See: EU Blockchain Observatory and Forum, (2021), p. 12; Roşu & Saleh (2020).
[50] See: Platt et al. (2021).
[51] See the list of papers in References, in particular, EU Blockchain Observatory and Forum (2021).
[52] See: Cambridge Bitcoin Electricity Consumption Index (CBECI).
[53] See Gallersdörfer et al. (2020).
[54] See: CBECI (2021).

does the difficulty to keep the rate of solved puzzles and, thus, new blocks stable. Hence, improved hardware does not decrease energy consumption in the long run. Different platforms provide time series relating to the past trend of the average timing to solve the puzzle. Therefore, considering the use of the main algorithms[55], it is possible to calculate the electricity consumption of the previously estimated compatible electronic devices. The greater the complexity of the cryptographic puzzle, the greater the electricity consumption required to solve it, all other parameters being equal. In the Bitcoin blockchain, the difficulty is adapted approximately every two weeks, determined by the moving average calculated on the frequency of blocks validated.[56]

- **Location of the miners** – To estimate the environmental impact, a next step must be taken. In particular, it is necessary to know where the miners' hardware is located. Locating miners can be very difficult.[57] Indeed, it should be kept in mind that they will often operate in groups ('mining pools'), aggregating the computing power of hundreds of ASICs located in various parts of the globe, often concentrated where the cost of energy is low and/or the climate is cold. Some authors estimate that, until recently, around 70 % of mining pools operated in China in 2019.[58] Once the miners' locations have been identified, it is possible to calculate their environmental impact based on the energy sources used to generate electricity in the countries considered (coal, nuclear, hydro, wind, etc.). The degree of associated CO_2 emissions ('carbon intensity') is measured in grams of CO_2 per kilowatt-hour of electricity (gCO2eq / kWh). In China, this value is on average 711, against 489 in the United States, 158 in Canada, and 13 in Sweden. Yet, it should be noted that mining often happens where electricity is particularly cheap, for example, close to hydropower during the rainy season, and hence can have a share of green electricity that is larger than the average mix in the power grid.

- **Value of the digital token and other economic aspects** – The last and fundamental step to estimate the environmental impact of PoW blockchains concerns economic variables. They are: fixed costs (amortization of the cost of electronic devices; both hardware and software) and variable costs (electricity – the price of which varies a lot over time and geography, device cooling costs, labor costs, etc.). On the revenue side, the number of digital tokens created per time (depending on block time and the number of new tokens per block), the token's market value, the fees offered by end-users according to the mechanism described above. Based on these values, the break-even point determines miners' entry or exit and their degree of activity, depending on the expected net revenues. Summarizing, the price of tokens, the number of coins created per block, the average transaction fees and number of transactions per block, and the average block time impact the revenues from creating blocks in a time interval and, thus, the amount of electricity spent in economic equilibrium. Often a lower bound on electricity costs – a parameter that is challenging to determine because of its temporal and geographical sensitivity – is used to determine an upper bound on total electricity consumption.

[55] See: Gallersdörfer et al., op. cit., p. 1845.
[56] See: Nakamoto, op cit., p. 3.
[57] Some authors have tried to identify miners' location through their IP addresses (see: Stoll et al. (2019), pp. 7-8).
[58] See: Stoll et al. (2019). In June 2021, China's authorities started enforcing a complete ban of all Bitcoin mining active in the country. According to Financial Times research, Bitcoin miners shipped roughly 2 million mining machines out of China following the ban, with the largest share (of 14 major companies that could be tracked) shifting towards Russia, followed by Kazakhstan and the US.

4. Some data on the energy consumption of PoW-based DLT

For the problems briefly described above, estimates on the energy consumption of blockchains are sensitive to the assumptions adopted by the model. Almost all contributions on the subject use average (or median) values and a range of minimum and maximum values that respectively represent the most and least favorable situation in terms of environmental impact. However, there is a broad agreement that blockchains based on PoW have a very significant[59] and by far a greater environmental impact than other protocols. We report below the data of two sites that estimate real-time electricity consumption of Bitcoin's blockchain.

At the time of writing (January 2022), the CBECI index[60] estimates for Bitcoin a global average power consumption of 13,9 Gigawatts (GW). The minimum value is 5.2 GW, and the maximum value is 34.9 GW. The minimum value reflects a conservative estimate (for example, assuming that most miners use highly efficient ASICs). The best guess of annualized consumption is equal to 121.9 TWh. The index for Bitcoin calculated by Digiconomist[61], based on a different analysis on average power consumption, estimates an annualized use of 204.5 TWh. To give a comparison, Italy has an installed capacity of 116.4 GW and an average annual electricity consumption of 302.7 TWh.[62] Some authors[63] have estimated that the carbon intensity of Bitcoin mining is around 480-500 gCO2eq / kWh on average. Hence, in 2019 an advanced ('instant') payment system such as that adopted by the ECB for the euro (called TIPS) had a CO_2 emission impact 40 thousand times lower than that of Bitcoin.[64]

Furthermore, according to a recent study, [65] at peak Bitcoin price levels seen early in 2021, the annual amount of e-waste for which Bitcoin mining is responsible[66] may grow beyond 64.4 metric kilotons in the midterm, which highlights the dynamic trend if the Bitcoin price rises further. Consequently, one Bitcoin transaction not only consumes around 1,000 kWh of electricity but also causes about 272g of e-waste. However, the "per transaction" metric should be taken with caution. If Bitcoin chooses to operate more transactions by increasing block size (or considering off-chain transactions like in the Lightning Network), this would not increase the total energy consumption and e-waste production but improve the per-transaction metric.

We note that there are also significant differences between cryptocurrencies that use other consensus mechanisms based on their technical and economic parameters (token's market value, number of new tokens rewarded for a block, block time, transaction fees). As can be seen from Table 2, Bitcoin is by far the one that, cumulatively, consumes the largest amount of electricity. In particular, the last column of the Table 2 provides the total power consumption of various blockchains. The power consumption needed to validate one block is obtained multiplying the electricity needed by the average validation time (e.g., 10 minutes for Bitcoin and 13 seconds for Ethereum). Since Bitcoin has a very high validation time, it has by far the highest power consumption.

---

[59] A well-known publication that appeared in Nature Climate Change went so far as to state that the Bitcoin blockchain, if it were to follow the historical pattern observed in other technologies, could by itself lead to a rise in global warming by two degrees in the next decades (see: Mora *et al.* (2018). Although the debate sparked by this article has highlighted an overestimation of the phenomenon having disregarded various aspects impacting Bitcoin's energy consumption, specifically that there is no linear dependence on the number of transactions processed, it sheds light on the relevance of the problem. On this debate see: O'Dwyer & Malone (2014); Vranken (2017); Li (2017); Krause & Tolaymat (2018); de Vries (2018); Zade et al (2019); Li et al. (2020); Sedlmeir et al., (2020); Lei (2021); Sedlmeir, Buhl et al. (2021).

[60] See: https://cbeci.org/.

[61] See: https://digiconomist.net/bitcoin-energy-consumption.

[62] See: https://en.wikipedia.org/wiki/Electricity_sector_in_Italy.

[63] See: Stoll et al. ivi.

[64] See: Tiberi (2021).

[65] See: de Vries & Stoll (2021).

[66] E-waste are electronic products that are unwanted, not working, and at the end of their useful life.

Table 2 - Crypto activities and energy consumption[67]

Name	Algorithm	Hardware compatible	Rated power of a single device (W)	Number of attempts per second to solve the 'proof-of-work' puzzle *(network)*	Efficiency of single devise *(number of attempts per second per W)*	Rated power (Blockchain power consumption) (kW)
Bitcoin	SHA-256	Bitmain Antminer S17 Pro 53 TH	2094	1.09e+20	2.53e+10	4,291,366
Ethereum	Ethash (*)	GPU	90230	1.64e+14	2.28e+05	719,087
Monero	RandomX (*)	GPU	80–190	1.27e+09	6.00e+00	210,277
Litecoin	Script	Innosilicon A4 + LTC Master	750	1.36e+14	8.27e+05	164,796
Bitcoin Cash	SHA-256	Bitmain Antminer S17 Pro 53 TH	2094	3.88e+18	2.53e+10	153,374
Bitcoin SV	SHA-256	Bitmain Antminer S17 Pro 53 TH	2094	3.04e+18	2.53e+10	120,077
Zcash	Equihash	Innosilicon A4 + LTC Master	1550	4.42e+09	9.00e+01	49,022
Ethereum C	Ethash (*)	GPU	90–230	9.87e+12	2.28e+05	43,278
Dash	X11	Sondoolines SPx36	4400	4.59e+15	1.23e+08	37,386

(*) ASIC-resistant algorithms
Source: Gallersdorfer et al. (2020).

5. On the transition from a non-green to a green DLT[68]

We have seen that various DLT configurations have very different environmental impacts, mainly depending on the consensus protocols adopted. Therefore, it is important to see whether there are feasible and robust technical solutions to promote a transition from non-green to green DLTs.[69] We aim to show that, in principle, this transition is possible, either through a greater environmental awareness by active nodes using PoW-based DLT or through policy interventions such as a Pigouvian tax on mining activity or a conservative prudential treatment of banks' exposure on PoW-based crypto-assets. The first approach (endogenous change of the DLT consensus by market players) can

[67] The scientific notation of Table 2 is as follows: 1.09e+20 means that 1.09 is multiplied by 10^{20} (one with twenty zeros); therefore, 1.0e+06 is a million, 1.0e+09 is a billion, and 1.0e+12 is a trillion, etc. When dividing the number of attempts per second by the efficiency of each single device (i.e., the number of hashes per second and Watt or, equivalently, per Joule), we obtain the total power consumption.
For Bitcoin, this would be 1.09e+20 / 2.53e+10 W = 0.43e+10 W ≈ 4 300 000 000 W = 4 300 000 kW. The unit of 1kW denotes energy per second; 1kW is the power at which, for example, an average hairdryer or ten 100 W light bulbs or a hundred 10 W led lamps consume when they are running; it means that per second, an energy of 1 kJ is consumed.

[68] We are grateful to Michele Ciampi for the useful suggestions provided for this section.

[69] One strategy to decarbonize blockchains would be to ensure that all blockchains are powered by 100% renewable electricity, as suggested by the EU Blockchain Observatory and Forum (2021), pp. 43-44. Considering the recent COP 26 agreements, this seems to be a long-term strategy, also taking into consideration that miners (or pools of miners) can swiftly move the location of their mining farms and/or nodes to a country with cheaper but not yet decarbonized electricity provisioning. Even more, based on a solution to the cryptographic puzzle it cannot be determined where the computational resources were spent. One should also take into account that owing to the limited supply with green energy in the foreseeable future, this would to some extent also only represent a shift from renewable energy consumption elsewhere and, thus, not be helpful for reaching overall climate-related goals.

be difficult to reach when taking the perspective of relevant stakeholders. For instance, a transition from PoW to PoS would imply that miners lose their business, and their hardware may become useless. Hence, there is a strong incentive to maintain the *status quo*, particularly if expensive ASICs processors are used that are not useful for tasks other than mining. We, therefore, propose a second approach based on the intervention of the policymaker. To our knowledge, literature on the topic is scarce, so we limit the discussion to a few considerations, first by discussing how PoW blockchains can be upgraded.

5.1 Upgrading blockchains

A way to transform energy-intensive blockchains into more ecological blockchains is to modify the consensus mechanism by updating the nodes' software. The redesign of a blockchain system generally has different aims, from changes of some parameters (e.g., the maximum block or transaction size, the number of tokens created per block, etc.) to changes of the validation rules at any level, or even changes of the consensus protocol itself (e.g., moving from PoW to PoS). In the past, the reason for such changes has often been the protection of the protocol against adversary attacks or the improvement of some aspects of the system, like transaction throughput. As underlined by Ciampi et al. (2020), a software update comprises of three important decisions: a) what update proposal should be implemented; b) an evaluation of whether the implementation is appropriate to be deployed in that specific blockchain; and c) when and how the changes should be activated.

A pre-condition for the successful transition to a new regime is that the security requirements hold during the whole transition period, i.e., both before (e.g., 51% of miners being honest) and after the update (e.g., 51% of the stake held by honest nodes). There is typically no endogenous incentive-compatible mechanism to reach this condition; instead, the strategy is an exogenous proposal (i.e., a process initiated by a coalition of miners) accepted by the majority (e.g., in terms of voting or computational power) the participants. A second pre-condition refers to the necessity to rely on the honest parties' full operational availability online and their willingness to perform all the needed changes (e.g., installing new software or hardware) during the upgrading process. Suppose the second pre-condition is not met, and some nodes are offline during the transition. In that case, these nodes might not know that an update has happened and could join a blockchain that is now compromised (since the honest nodes that were online are now working on extending the updated blockchain and have left the old blockchain). A possible way out could be to rely on a trusted third party or introduce a transitory 'dual' regime, relying on a second compatible blockchain during the updating process.[70]

Protocol changes might typically require a blockchain bifurcation (or 'fork'). A fork is a radical change of the blockchain, which renders new blocks created with the old version of the software invalid when checked with the latest software. If these changes are radical, users must update their software to the newest version, as previous variants are no longer compatible. At the end of the separation, two networks are operative if a group of nodes continues with the old one; if, on the contrary, there is a full agreement on the upgrading process, the original blockchain ceases to operate. It is important to underline that a switch from PoW to PoS makes it no longer necessary to spend significant resources on hardware and energy. Miners must then sell their hardware on the second-

[70] The properties required by the ledger protocols for allowing updatable blockchains are described by Ciampi et al. (2020).

hand market or participate in other PoW-based cryptocurrencies with the same underlying hashing algorithm and potentially lower revenues.

A well-known fork occurred in 2017[71] on the Bitcoin blockchain, which resulted in a split, creating Bitcoin Cash.[72] In November 2021, a second important upgrade resulted in a 'soft fork'[73] It is unclear to what extent a sustainability-related fundamental transition is possible in a fully decentralized setting. Still, these forks seem to suggest that this process is feasible. Yet, changing the consensus mechanism may be much more complex than updates observed so far, as the timeline of Ethereum's transition from PoW to PoS illustrates.

As stated above, it is clear that there is a strong 'path-dependency', which is all the more important the higher transaction costs and risk of creating an unintended permanent bifurcation of the blockchain are. In this regard, voluntary private-sector-led initiatives such as the Crypto Climate Accord or community-driven initiatives on DLT de-carbonizations move in the right direction. However, we believe that endogenous incentive structures may not be sufficient.

5.2 DLT environmental policies

In the following sections, we illustrate some policy tools aiming at disincentivizing the use of non-green DLT protocols. They range from a softer regulatory stance, based on disclosure and corporate social responsibility, to more disruptive measures like banning PoW. Clearly, a comprehensive, global agreement among competent authorities would be highly desirable to avoid forms of regulatory arbitrage, specifically for transnational permissionless and pseudonymous DLT networks.

As we pointed out in the previous sections, while a per-transaction metric for energy or e-waste production through PoW cryptocurrencies is a nice illustration of their sustainability issues relative to their utility as a medium of exchange, it does not reflect that the total energy and e-waste production is largely independent of the number of transactions processed; indeed, as now should be clear from the previous sections, it reflects the economic value of blocks generated by miners per time (which depends to the number of new tokens created per block, their market value, and (currently often to a lesser extent, with some exceptions like Ethereum) transaction fees). Consequently, policy measures should arguably not simply focus on reducing the number of transactions processed on PoW DLT, as this would ignore the fundamental drivers for PoW DLTs' energy consumption. We also argued why improving the energy efficiency of mining hardware does not help improve PoW's sustainability. Instead, measures against the energy consumption and e-waste production of PoW-based cryptocurrencies need to consider the economic equilibrium that determines whether stakeholders engage in mining activity: the expected rewards through creating new blocks – determined by the value of newly generated tokens (and to a smaller extent transaction fees) – need to be larger than the

[71] On August 1st, 2017, Bitcoin's miners reached an agreement to improve the throughput (ability to handle high volumes of transactions) of the Bitcoin blockchain. Some miners disagreed, which lead to a fork in the chain, creating Bitcoin Cash. See, for instance: https://en.wikipedia.org/wiki/Fork_(blockchain) and https://en.wikipedia.org/wiki/SegWit.
[72] Bitcoin Cash had its own split on Nov. 15, 2018, into Bitcoin Cash and Bitcoin SV, see: https://www.investopedia.com/news/all-about-bitcoin-cash-hard-fork/.
[73] The upgrade aimed at improving privacy and flexibility to smart contacts and related aspects (for example the establishment of decentralized autonomous organizations). See: https://www.nasdaq.com/articles/understanding-taproot-in-a-simple-way-2021-11-12.

expenditures for mining hardware and electricity. Consequently, there are three immediate main targets for policymakers to reduce the ecological impact of PoW:

(1) Increasing the costs for spending electricity and hardware. This could be achieved by a global carbon tax, for instance, on e-waste or carbon emissions caused by non-green electricity generation. However, while international countermeasures against carbon emissions and e-waste are a promising path from an economic and environmental perspective, we do not consider it further, as it is outside the specific DLT domain and probably even more difficult to achieve.

(2) Introducing financial market standards or indirectly reducing the market value of non-green tokens through disincentivizing their ownership as investment or trading.

(3) Introducing a well calibrated carbon tax on the creation of new blocks; this would incorporate in miners' private costs the social costs due to the use of non-green electricity, and/or introducing an environmental transaction tax (this would imply an indirect incentive to reduce the amount of electricity spent by miners as it decreases their net revenues and, thus, the break-even point of revenues and expenses that include electricity costs).

The sooner and more gradually these measures are taken, the less disruptive they would likely be on PoW-based crypto market. Indeed, one needs to consider that for PoW blockchains, reducing energy consumption always implies reducing the blockchain's security against 51% attacks. This may be particularly problematic when there are many unused yet still functional ASICs that attackers could own from previous mining activity or buy cheaply on the second-hand market when mining activity has been significantly reduced through regulatory measures. So far, 51% attacks have mainly been observed with PoW blockchains where another, "larger" PoW blockchain uses the same ASICs for hashing. The selection and calibration of the proposed regulatory measures should be aimed at minimizing these risks in order to contain unintended consequences.

Independent of the category that one of these measures belongs to, one could use the revenues from an associated tax for offsetting a share of the remaining environmental externalities. In the following, we will introduce some potential policy measures that address these approaches.

Financial disclosure - The softer regulatory approach is based on financial disclosure. In March 2018, the EU Commission put forward the Action Plan on Sustainable Finance. As part of action 9 of the action plan, the Commission proposed a regulation (adopted in March 2021) on the sustainability-related disclosures in the financial services sector (FSDR)[74].

Therefore, current European regulations already lay down sustainability disclosure obligations for manufacturers of financial products and financial advisers toward end-investors. It does so to integrate the consideration of sustainability risks by financial market participants (i.e., asset managers, institutional investors, insurance companies, pension funds, etc., all entities offering financial products where they manage clients' money) and financial advisers in all investment processes and for financial products that pursue the objective of sustainable investment.

In line with this approach, a recent study[75] suggests financial investors in Bitcoin to compute their carbon footprint using either a *transaction-based metric* (share of blockchain space used relative to the total blockchain growth) or an *ownership-based metric* (Bitcoins held by the investor relative to Bitcoins in circulation for a specific period). The authors of this proposal believe that this approach

[74] See: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R2088&from=EN.
[75] See: Frankfurt School Blockchain Center – intas.tech (2021).

provides an opportunity for crypto-assets managers, crypto exchanges, and custodians to take responsibility and action in line with the Environmental, Social, and Corporate Governance (ESG) requirements of the FSDR.

Financial market infrastructures – A second policy tool relies on the 'good governance' of market infrastructures based on the Principles for Financial Market Infrastructures (PFMI).[76] PFMI are international standards for payment systems, central securities depositories, securities settlement systems, central counterparties, and trade repositories. They are issued by the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO). To address the novelties introduced by DLT, the CPMI – IOSCO joint initiative has recently promoted a consultative process on 'systemically important stablecoin arrangements' (SA). The consultation does not aim to create additional standards for SAs, but rather to provide more clarity for the authorities seeking to adapt the PFMI to non-multicurrency SAs (the consultation excludes multicurrency SAs and unbacked crypto assets).

Stablecoins' usability as a means of payment relies on the core functions performed by SAs. In particular, the SA *transfer function* enables the transfer of coins between participants and a mechanism for validating transactions. The SA is considered "systemically important" by the competent authority and would be expected to observe all relevant PFMI, such as good governance, comprehensive risk management, clear and final settlement functionalities, robust and timeliness convertibility, and little or no credit or liquidity risk in both normal and stressed conditions. According to the CPMI-IOSCO, SAs may present some notable features compared with existing, traditional financial market infrastructures (FMIs). They are related to (i) the potential use of settlement assets that are neither central bank money nor commercial bank money and carry additional financial risk; (ii) the interdependencies between multiple SA functions; (iii) the degree of decentralization of operations and/or governance; and (iv) a potentially large-scale deployment of emerging technologies such as distributed ledger technology (DLT)".[77] In our opinion, the 'sustainability' of the stablecoins' consensus protocol should be included in this list. Consequently, the PFMI should create an additional standard to respect his requirement.

Prudential standards – Another potential policy approach is discouraging banks and other intermediaries from taking exposure in non-green PoW-based crypto-assets. This policy would be under the Basel Committee on Banking Supervision (BCBS) remit.[78] In June 2021, the BCBS[79] issued a Consultative Document proposing a differentiated prudential treatment for crypto-assets. The consultation paper divides crypto-assets into two broad categories:[80] Crypto-assets (Group 1a) that are tokenized versions of traditional assets[81] (equities, bonds, etc.), and (Group 1b) crypto-assets with an effective 'stabilization' mechanism (stablecoins).[82] The BCBS proposes applying capital

[76] See: https://www.bis.org/cpmi/info_pfmi.htm.
[77] See: CPMI – IOSCO (2021), p. 4
[78] The objective of the Basel capital framework is to ensure that the bank's capital resources properly reflect its capacity to absorb losses. Banks' capital resources need to be supported by a realizable value of its assets also in stressful market conditions (i.e. the asset should in principle remain 'liquid' (sellable) at all time and at a reasonable price).
[79] See: Basel Committee on Banking Supervision (2021).
[80] For a more granular taxonomy of crypto-assets and related accounting and prudential standards, see: Gola & Caponera (2019).
[81] Tokenized traditional assets must be digital representations of traditional assets using cryptography, DLT or similar technology rather than recording ownership through the account of a central securities depository (CSD) or custodian.
[82] A 'stabilization mechanism' is that the value of the token is pegged to the value of a reserve. According to the BCBS, this could be achieved by referencing other crypto-assets as underlying assets (including those that reference other crypto-assets that have traditional assets as underlying). If they are stabilized using only an algorithm (for instance through a

requirements at least equivalent to those of traditional assets (with further consideration for capital add-ons). Moreover, the BCBS proposes new guidance on applying current rules to capture the risks relating to stabilization mechanisms (with additional considerations for capital add-ons). Group 2 are all other crypto-assets (such as Bitcoin, Ether, Algorand, Ada, Nxt, etc.) and other stablecoins that fail to meet the criterion established for Group 1b. For Group 2, the BCBS is proposing a very conservative prudential treatment. In particular, to discourage banking and financial institutions from taking exposures in this class of tokens, the BCBS is considering to apply the most rigorous prudential treatment based on a 1250 % risk weight applied to the maximum of long and short positions.[83] So far, however, no decision has been made. The BCBS is also evaluating whether to increase the granularity of both macro groups and calibrate the provision following a risk-based principle. Should this approach be adopted, other things being equal, more liquid crypto-assets such as Bitcoin would have a less penalizing prudential treatment.

Our suggestion is to implement the above-mentioned prudential policy, also considering the differentiated environmental impact of various DLTs. In particular, we suggest introducing a sustainability criterion for both Group 1 and Group 2 that would discourage banks' exposure in crypto-assets based on DLTs having a sizable carbon footprints. To do so, one could introduce a penalizing factor for energy-intensive crypto-assets to all PoW-based tokens. (i.e., a prudential treatment based on a 1250 % risk weight applied to the maximum of long and short positions). Investors can easily check from the token's White Papers which type of consensus protocol is adopted. It is worth mentioning that in the long run, less energy-dependent crypto-assets could also be less volatile, as they would most likely be less affected by idiosyncratic events (such as the recent decision by Chinese authorities to ban all 'miners' operating in the country, or the high volatility of energy prices).

Pigouvian or environmental transaction tax – These policy instruments intends to discourage the use of non-green DLT crypto-assets. A traditional corrective measure is a Pigouvian tax (or *carbon tax*),[84] graduated according to the impact in terms of CO_2 emissions.[85] In particular, it would be about increasing the marginal cost per created block for each PoW-based blockchain. In principle, the tax should ensure that the marginal environmental damage[86] per validated block equals the marginal cost of CO_2 abatement. This approach has been applied with good results in several countries, albeit in different contexts.[87] If the PoW-DLT setting does not allow the direct taxation of validated blocks, a taxation on PoW-based transactions could be introduced (similar to a Tobin tax). In both cases, the

protocol that increases or decreases the supply of the crypto-asset in order to peg the reference currency; s.c. 'algorithm-based stablecoins') they are not considered to meet the 'stabilization' criterion and, therefore, are included in Group 2.

[83] An alternative to the *risk weight approach*, is the *full deduction approach*; both the approaches are currently under discussion. When there is significant uncertainty on the realizable value of an asset, the asset should be fully deducted from high quality (CET1) regulatory capital as the capital is already "spent" on an asset that cannot be readily monetized. There are pros and cons. In general, under the risk weight approach, some banks may require to hold two or three times more capital (not only CET1, though) than the actual exposure.

[84] A Pigouvian Tax is a tax imposed on any market activity that generates *negative externalities*. In the presence of negative externalities, the social cost of market activity is not covered by the private cost of the activity. The tax is intended to correct the undesirable and inefficient economic equilibrium (a market failure), and does so by being set equal to the external marginal cost of the negative externalities. In addition to taxes, there are other policy tools, such as tradable permits, market friction reductions, or government subsidies. For a discussion, see: Stavins (2003).

[85] The current EU crypto-assets tax regime is described here: https://www.osborneclarke-fintech.com/2018/12/19/taxation-of-cryptocurrencies-in-europe-an-overview/; for the US crypto-assets tax regime, see: https://www.nerdwallet.com/article/investing/bitcoin-taxes.

[86] See: Gallersdörfer et al. (2021).

[87] See: OECD (2019); OECD (2021b).

tax revenues could be used for environmental purposes. The introduction of the tax should be gradual to minimize the market impact.

In particular, when possible, the tax would be collected on behalf of the Tax authority by DLT members (for instance, Enterprise Ethereum Alliance members): the DLT members shall ask registered nodes (if identifiable) to certify the location of the servers utilized[88] and to pay a calibrated Pigouvian tax depending on the carbon intensity of the country where the server is located.[89] Therefore, as some mining facilities use green energy, a more granular tax calibration could also be adopted. Specific exemptions could be granted to DLT initiatives accepting tokens only from miners compliant with the carbon footprint requirements set by ISO 14068 or similar standards.[90] Crypto-asset users would, therefore, have an incentive to operate with such DLTs.

If the DLT is fully decentralized (as in the case of Bitcoin), an environmental transaction tax could be introduced and collected by crypto-asset *exchanges* on behalf of the Tax authority. This approach assumes that most crypto transactions are channeled through an exchange platform. We are aware that end users can transact without utilizing an *exchanger*. However, this bilateral, over-the-counter strategy generally implies higher transaction costs, particularly if the professional (not retail) node operates with many counterparties. The environmental transactions tax could be linked to the CBEC index and could be applied to all PoW-based crypto assets and be updated, for instance, every six months based on the estimated average consumption of the previous six months or another moving window average.

We have decided to propose excluding *wallet providers* from the taxation: we deem the involvement of this class of service providers problematic, since a taxation could further incentivize the use of 'unhosted wallets' (sometimes called also self-hosted or non-custodial wallets), which is a software installed on end users' computers, phones or other devices. The cryptographic keys and transactions associated with tokens in an unhosted wallet are controlled directly through individuals, without the need of an intermediary. Users of unhosted wallets can receive, send and exchange their crypto assets without revealing their identity.

Banning 'mining' activity - The most rigorous but disruptive policy against PoW is banning 'mining' activity. As already mentioned, the Chinese authorities have recently adopted and enforced this decision. In May 2021, through a joint statement, the Swedish Financial Supervisory Authority and the Swedish Environmental Protection Agency said that "the energy-intensive mining of crypto-assets should be prohibited." The authorities supported this conclusion noticing that not only "the social benefit of crypto-assets is questionable", but that they "have a significant negative impact on climate change, as mining leads to both large emissions of greenhouse gases and threatens the green transition that needs to happen urgently."[91] More recently, Erik Thedéen, vice-chair of the European Securities and Markets Authority (ESMA), told the Financial Times that cryptocurrencies are posing the Paris agreement at risk.[92]

[88] As already mentioned, the miner can use servers or mining hardware located in another country, where energy is less expensive or cooling is less energy intensive.
[89] Data are available here: http://www.globalcarbonatlas.org/en/CO2-emissions.
[90] See: https://www.iso.org/standard/71206.html.
[91] On the Swedish Authorities joint statement, see:https://www.fi.se/en/published/presentations/2021/crypto-assets-are-a-threat-to-the-climate-transition--energy-intensive-mining-should-be-banned/.
[92] See: https://www.ft.com/content/8a29b412-348d-4f73-8af4-1f38e69f28cf

6. Conclusions

Several international organizations have paid considerable attention to blockchain technology and related applications in recent years, including the creation and distribution of crypto-assets. The regulators' approach is currently mainly focused on overseeing financial and payment systems risks, consumer protection, AML/CFT, and cyber risks. This has been done following the *technological neutrality* principle, along with the 'same activities, same risks, same rules' regulatory approach. The law should not impose or favor one technology if other technologies are likely to meet the same objectives. This principle is valuable, as it is important for regulations to avoid stifling financial innovation. However, given that the energy consumption and e-waste accumulation associated with some DLT protocols can generate significant negative externalities, we believe that it is necessary to include an *environmental sustainability criterion* in ongoing regulatory initiatives. This can be done by pushing DLT users towards ecological DLTs. Alternative DLTs are already available; they consume much less energy, while still being sufficiently reliable and decentralized.

This paper gives an overview of the main related aspects, showing that permissioned DLT with a voting-based consensus or permissionless DLT with a PoS consensus provides an option to deploy sustainable DLTs. We illustrate several policy tools: the improvement of financial transparency and corporate social responsibility policies; the inclusion of the sustainability principle into the good governance of market infrastructure guidelines; a prudential standard aimed at limiting the ecological footprint produced by PoW-based blockchains; a carbon tax and/or an environmental transaction tax; and, finally, the banning of 'mining' activity.

Annex

To manage a decentralized database by uncoordinated parties, it is necessary to resort to an incentive system (e.g., a lottery or a voting system) that facilitates converging toward a shared solution. Highly popular are consensus mechanisms called proof-of-work or proof-of-stake. In the following, we limit ourselves to providing the basic components of the two protocols. The 'Byzantine fault-tolerant consensus' is also mentioned since it gives a good intuition of the problem at stake.

'Byzantine fault-tolerant consensus' (BFC) – The family of BFT consensus is based on a seminal paper published in 1982 by Lamport, Shostak, and Pease. The paper's abstract frames the problem in a very effective manner: "Reliable computer systems must handle malfunctioning components that give conflicting information to different parts of the system. This situation can be expressed abstractly in terms of a group of generals of the Byzantine army camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is finding an algorithm to ensure that the loyal generals reach an agreement. It is shown that, using only verbal messages, this problem is solvable if and only if more than two-thirds of the generals are loyal so that a single traitor can confound two loyal generals. With unforgeable written messages, the problem is solvable for any number of generals and possible traitors".[93] If the assumptions change (for instance, because messages on the internet can be delayed indefinitely, the result (i.e., the two-thirds ratio) can change as well (it could be, for instance, 51%).

Proof-of-work (PoW) – The system adopted by Nakamoto (2008) (pseudonym) uses solving 'cryptographic puzzles' to find agreement. The PoW consists of looking for a value ('nonce') which, once inserted in a block and put through an algorithm called Secure Hash Algorithm (SHA-256), generates a number (called '*hash*') with a specific property. The SHA-256 algorithm is a particular unidirectional (non-invertible) function where finding pre-images (the solution) is practically impossible analytically or strategically and requires a trial and error approach; once the solution is known, it is, however, easy to verify its correctness. The database (the blockchain) is public and updated sequentially by the owners of the computers on the network (called 'nodes') who have a synchronized copy of the database on their PC to change its status. In the case of Bitcoin, each block represents the handover of numerous transactions (for example, 2500 transactions); on average, 150-200 blocks of transactions are validated per day.

In other words, PoW involves finding a random number (nonce) so that the hash value of the nonce – together with other data – takes on a certain form. In the case of Bitcoin, this is the requirement that the integer representation of the hash value is smaller than a certain upper limit. The choice of this upper limit thus defines a measure of complexity of the 'cryptographic puzzle'. The incentive system to solve the puzzle is based on the role of miners who compete with each other to 'win' a certain number of digital tokens (for example, to date, 6.25 Bitcoins) for each created block.

The longest chain of transaction blocks is considered the valid one (technically the 'heaviest' one being the one that represents the complete history of the 'correct' (or final) transactions since the birth of that given blockchain). It is the one that is reached by the majority (51%) of the network's computing power.

Proof-of-stake (PoS) – PoS protocols are a class of Consensus (computer science) for blockchains that work by selecting validators in proportion to their quantity of holdings (commitment at stake) in the associated cryptocurrency.

[93] See: Lamport et al. (1982), p. 1.

There is a great variety of proof-of-stake (PoS) consensus mechanisms, either based on an initial commitment by the DLT's members (i.e., an initial 'capital') or an accumulation over time of a scarce resource. For instance, the probability of creating a new block is proportional to the number of coins held. The incentive for participants to behave correctly consists of locking the capital for some time period after creating a block, so that detected misbehavior could result in the loss of the 'capital' put into play ('at stake').[94] Sometimes, this is also called 'slashing'. However, there are also protocols that do not require the locking of capital but instead reward the rest of the system. There are also mixed forms where an initial validator set for some epoch is chosen randomly, weighted by stake, followed by a round of permissioned, voting-based consensus (for example, in Agorand and PoS-based Tendermint).

PoS is therefore based on a semi-probabilistic process that randomly selects the set of validators active in the blockchain updating process for adding new blocks to the chain, weighted by their stake: the probability is higher for validators with a larger capital. As in PoW blockchains, the beneficiary will get new digital tokens and/or transaction fees as a reward. In some configurations, 'reputation' is measured by the age of the digital coins owned. This creates some kind of entry cost or barrier to entry for newcomers. As already mentioned, the main challenge of this much less energy-intensive algorithm in systems with unclear or distributed governance is the initial fair distribution of coins.[95]

Many PoS consensus protocols use different metrics and features. The main difficulty is to design a protocol resistant to 'nothing at stake attacks' and 'long range attacks': in the first type of attacks, the validator has an incentive to simultaneously add the same block on several branches (forks) of the blockchain to maximize the probability of winning the new digital token. Moreover, in the case of transactions with values higher than the invested capital, the correct incentive mechanism would cease. The second threat (also called history attacks) concerns the case in which the attacker tries to alter the blockchain while not currently having more capital at stake, but mainly old digital coins (i.e., prolonged ownership of a limited amount of coins, but sufficient to control the entire network).[96]

[94] Examples of digital tokens built on PoS blockchains are: Algorand, Cardano, EOS, Polkadot, Tezos, TRON, and in perspective Ethereum 2.0.

[95] In this paper, we do not consider other relevant aspects such as i) liveness: in the case of a reduced number of miners, PoW blockchains still grow, even though more slowly; instead PoS blockchains have higher risks of being stuck (e.g., if in Algorand there are not enough committee members to approve the next block); ii) *block producers' potential anonymity*, which can also be achieved on PoS blockchains, for example, with zero-knowledge proofs (see, for instance, https://doi.org/10.1109/SP.2019.00063), adding, however, considerable complexity.

[96] See; Li *et al*. (2020), pp. 6-7.

References

Andoni, M. Robua, V. Flynna, D., Abramb, S., D. Jenkins, McCallumd, P. Peacockd, A. (2019), 'Blockchain Technology in the Energy Sector: A Systematic Review of Challenges and Opportunities', *Renewable and Sustainable Energy Review*, 100, pp. 143-174.

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y. and Muralidharan, S. (2018), 'Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains', In *Proceedings of the 13th EuroSys Conference*.

Badertscher, C., Garay, J., Maurer, U., Tschudi, D., and Zikas, V. (2018), 'But Why does it Work? A Rational Protocol Design Treatment of Bitcoin', Proceedings of Eurocrypt.

Barbereau, T., Smethurst, R., Papageorgiou, O., Sedlmeir, J., Fridgen, G. (2022). Decentralized Finance's Unregulated Governance: Minority Rule in the Digital Wild West, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4001891

Biryukov, A., Khovratovich, D. and Pustogarov, I. (2014). Deanonymisation of Clients in Bitcoin P2P Network. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pp. 15-29.

Castro, M. and Liskov, B. (1999), 'Practical Byzantine Fault Tolerance', In *OSDI* (Vol. 99), pp. 173-186.

Ciampi, M., Karayannidis, N., Kiayias, A., and Zindros, D. (2020), 'Updatable Blockchains', 25th European Symposium on Research in Computer Security Proceedings Part II, pp. 590-609.

CPMI – IOSCO (2021), 'Application of the Principles for Financial Market Infrastructures to Stablecoin Arrangements'.

de Vries, A., 2018. 'Bitcoin's Growing Energy Problem', *Joule*, 2, pp. 801-805.

de Vries, A., Stoll, C. (2021), 'Bitcoin's Growing E-waste Problem', *Resources, Conservation and Recycling*, Elsevier, 175.

Eyal, I. and E. G., Sirer (2014), 'Majority is Not Enough: Bitcoin Mining is Vulnerable', In *International Conference on Financial Cryptography and Data Security*, pp. 436-454.

EU Blockchain Observatory and Forum (2021), *Energy Efficiency of Blockchain Technologies*.

EU Commission (2018), FinTech Action Plan: For a More Competitive and Innovative European Financial Sector, COM 109.

Frankfurt School Blockchain Center – intas.tech (2021), 'The Carbon Emissions of Bitcoin From an Investor Perspective'.

Gallersdörfer, U., Klaaßen, L. and Stoll, C. (2020), 'Energy Consumption of Cryptocurrencies Beyond Bitcoin, Joule Commentary', 4, pp. 1839-1851.

Gallersdörfer, U., Klaaßen, L. and Stoll, C. (2021), 'Accounting for Carbon Emissions Caused by Cryptocurrency and Token Systems', https://arxiv.org/abs/2111.06477.

Gola, C., and Caponera, A. (2019), 'Policy Issues on Crypto Assets', LIUC paper, 7.

Guggenberger, T., Sedlmeir, J., Fridgen, G., & Luckow, A. (2021), 'An In-Depth Investigation of Performance Characteristics of Hyperledger Fabric', https://arxiv.org/abs/2102.07731.

Hafid, A., A.S. Hafid, and Samih, M., (2020), 'Scaling Blockchain: A Comprehensive Survey', IEEE Access, 8.

IMF (2021), 'The Crypto Ecosystem and Financial Stability Risks', *Global Financial Stability Report*, Chapter 2.

Jalalzai, M.M., Niu, J., Feng, C. and Gai, F. (2020), 'Fast-Hotstuff: A Fast and Resilient Hotstuff Protocol', https://arxiv.org/abs/2010.11454.

Krause, M.J., Tolaymat, T. (2018), 'Quantification of Energy and Carbon Costs for Mining Cryptocurrencies', *Nature Sustainability*, 1, 711-718.

Lamport, L. (2001), 'Paxos Made Simple', *ACM Sigact News, 32*(4), pp. 18-25.

Lamport, L., Shostak R., and Pease, M. (1982), 'The Byzantine Generals Problem', *ACM Transactions on Programming Languages and Systems*, 4:3, pp. 382-401.

Lei, N., Masanet, E., Koomey, J., (2021), 'Best Practices for Analysing the Direct Energy Use of Blockchain Technology Systems: Review and Policy Recommendations', *Energy Policy*, 156.

Li, A., Wei, X., and He, Z. (2020), 'Robust Proof of Stake: A Consensus Protocol for Sustainable Blockchain System', *Sustainability*, 12:2824.

Li, W., Andreina, S., Bohli, J-M., and Karame, G., (2017), 'Securing Proof-of-Stake Blockchain Protocols', In *Lecture Notes in Computing Science*, NEC Laboratories Europe.

Mora, C., Rollins, R.L., Taladay, K., Kantar, M.B., Chock, M.K., Shimada, M., and Franklin, E.C, (2018), 'Bitcoin Emissions Alone Could Push Global Warming Above 2°C', *Nature Climate Change*, *Nature*, 8(11), pp. 931-933.

Musiani F., Mallard A., Méadel C. (2018), 'Governing What Wasn't Meant to be Governed. A Controversy-Based Approach to the Study of Bitcoin Governance'. In *Bitcoin and Beyond. Cryptocurrencies, Blockchain, and Global Governance*, Campbell-Verduyn M. ed., Routledge.

Nakamoto, S. (2008), 'Bitcoin: A Peer-to-Peer Electronic Cash System', White paper.

O'Dwyer, K., and Malone, D. (2014), Bitcoin Mining and its Energy Footprint. In: Proceedings of the 25th Joint IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014). IET, pp. 280-285.

OECD (2019), Taxing Energy Use, Using taxes for climat action, Paris.

OECD, (2021a), *Regulatory Approaches to the Tokenisation of Assets*, OECD Blockchain Policy Series, Paris.

OECD (2021b), *Effective Carbon Rates 2021. Pricing Carbon Emissions Through Taxes and Emissions Trading*, Paris.

Platt, M., Sedlmeir, J., Platt, D., Tasca, P., Xu, J., Vadgama, N. and Ibañez, J.I. (2021), 'Energy Footprint of Blockchain Consensus Mechanisms Beyond Proof-of-Work', https://arxiv.org/abs/2109.03667.

Roşu, I., Saleh, F. (2020), 'Evolution of Shares in a Proof-of-Stake Cryptocurrency', *Management Science*, 67:2.

Sedlmeir, J., Buhl, H.U., Fridgen, G., and Keller, R. (2020), 'The Energy Consumption of Blockchain, Technology: Beyond Myth', *Business & Information Systems Engineering*, 62(6), pp. 599-608.

Sedlmeir, J., Buhl, H.U., Fridgen, G., and Keller, R. (2021), 'Recent Development in Blockchain and their Impact on Energy Consumption', https://arxiv.org/abs/2102.07886.

Sedlmeir, J., Ross, P., Luckow, A., Lockl, J., Miehle, D., & Fridgen, G. (2021), 'The DLPS: A New Framework for Benchmarking Blockchains', In *54th Hawaii International Conference on System Sciences*, pp. 6855-6864.

Sedlmeir, J., Wagner, T., Djerekarov, E., Green, R., Klepsch, J. and Rao, S. (2022). 'A Serverless Distributed Ledger for Enterprises', In *55th Hawaii International Conference on System Sciences*.

Stavins, R.N. (2003), *Experience with Market-Based Environmental Policy Instruments*, In *Handbook of Environmental Economics*, Karl Göran Mäler & Jeffrey R. Vincent eds.

Stoll, C., Klaaßen, L., and Gallersdorfer, U., (2019), 'The Carbon Footprint of Bitcoin', MIT – CEEPR, Working paper, 18.

Tiberi, P. (2021), 'The Carbon Footprint of the Target Instant Payment Settlement (TIPS) System: A Comparative Analysis with Bitcoin and other Infrastructures', Approfondimenti. Mercati, infrastrutture, sistemi di pagamento, Banca d'Italia, 5.

Urbinati, E., Belsito, A., Cani, D., Caporrini, A., Capotosto, M., Folino, S., Galano, G., Goretti, G., Marcelli, G., Tiberi, P., Vita, A. (2021), 'A Digital Euro: A Contribution to the Discussion on Technical Design Choices', Approfondimenti. Mercati, infrastrutture, sistemi di pagamento, Banca d'Italia, 10.

van der Waal, M.B., Ribeiro, C.D.S., Ma, M., Haringhuizen, G.B., Claassen, E. and van de Burgwal, L.H., (2020), 'Blockchain-Facilitated Sharing to Advance Outbreak R&D', *Science*, 868, pp. 719-721.

Vranken, H., (2017), 'Sustainability of Bitcoin and Blockchains', *Current Opinion in Environmental Sustainability*, 28, pp. 1-9.

Zade, M., Myklebost, J., Tzscheutschler, P., and Wagner, U. (2019), 'Is Bitcoin the Only Problem? A Scenario Model for the Power Demand of Blockchains', *Frontiers in Energy Research*, 7:21, pp. 1-12.