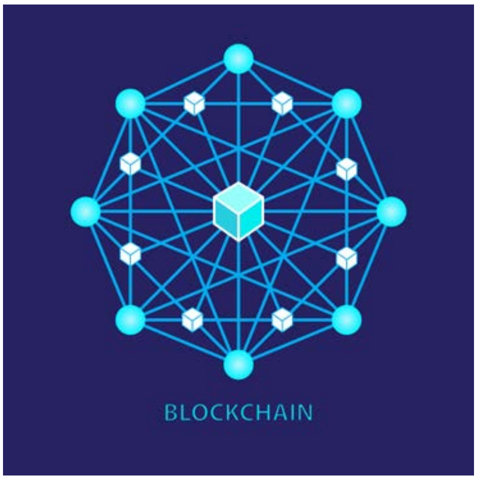
What if blockchain were to be truly decentralised?

Technological systems, once introduced in a particular socio-economic context, often evolve in unforeseen ways and may fall prey to unexpected power relations. Blockchain, as a technology that relies on decentralisation to enable storing and securing data-based transactions without central administration, is currently facing significant centralisation pressures that may undermine the purpose of operating a decentralised blockchain network. But what if blockchain fulfilled its promise to be truly decentralised?



© Beautyimage / Shutterstock.com.

Decentralisation, namely the notion that not one single entity has control over all the process, is often viewed as blockchain's key innovation, and even its *raison d'être*. The fully decentralised, self-sufficient and self-contained character of blockchain, in which there is no central body or trusted third party to authorise transactions, has made this technology extremely popular worldwide, as it enables millions of previously excluded people to participate in the next wave of economic change. Blockchain could support new forms of fully decentralised infrastructure, for applications as varied as finance, cloud databases and the management of common assets and resources.

Because blockchain has no central authority, it relies on miners to maintain these decentralised services/databases collectively. Anyone can be a miner, respectively storing the blockchain and determining the transaction records. The value of decentralised control is that it removes intermediaries, increases transaction transparency, reshapes value chains, democratises data, improves trust and reduces the risk of cyber-attacks.

Centralisation tendencies

While decentralisation cannot be absolute, given that blockchain itself is a software developed in a centralised way as a public key infrastructure, there are strong indications that blockchain, despite its open source nature, has evolved into a highly centralised structure that can undermine the wider blockchain ecosystem. Oen of the best known blockhains is that of the currency, bitcoin. Now, it is largely in the hands of major holders, known as 'whales', who have the power to manipulate the bitcoin network. First of all, the process of verifying transactions and securing a blockchain ledger against attack, called mining, has become a capital-intensive industry which requires a large amount of capital to purchase the most advanced hardware and fast processing power. The control of manufacturing of mining equipment, and of a large proportion of the network's hashing power – i.e. the amount of computing power the bitcoin network consumes in order to be continuously operational and generate new cryptocurrencies – by huge mining farms with strong mining resources, especially in China, has resulted in the top four bitcoin-mining operations holding more than 53 % of the system's average mining capacity. In the case of Ethereum, 61 % of the system's average weekly capacity is in the hands of only three miners.

It should however be noted that, as bitcoin miners depend entirely on the value of bitcoin for their revenues, dominating mining may have a negative effect on the price and integrity of bitcoin. BitInfoCharts found that only 1 000 of the 11 million bitcoin holders in the world control 35.4 % of all bitcoins in circulation. One of the main factors that reinforce centralisation tendencies is also the lack of 'scalability', meaning that blockchains are currently unable to deal with large numbers of users and, as the block size increases over time, only a few institutions will have the means to maintain blockchains. Moreover, while

Author: Mihalis Kritikos, Scientific Foresight Unit (STOA)

anyone is entitled to submit changes to the software (such as bug fixes, or incremental improvements), only a small number of individuals (the core developers) have the power to decide which changes will be incorporated into the main branch of the software.

Although originally designed as disintermediation tools, blockchain ecosystems are currently characterised by a number of third parties and profitable businesses offering intermediation services, with resilient asymmetries of information and power between developers and users. As a result of these centralisation tendencies, system vulnerabilities are emerging, and centralised failures may occur in the form of the threat of a '51% attack'. The emergence of a dominant player is a point of failure of the whole system: eliminating that player destroys the system. Given that whoever controls mining also controls the protocol, this decides which transactions are to be deemed valid, increasing the risk of abuse of a dominant position. Additionally, if the majority of the hashing power decides for or against a change, it is nearly impossible for other users of the network to oppose this decision. All these factors call into question the egalitarian potential of current distributed networks, their accessibility and their libertarian nature.

What do the centralisation trends of blockchain mean for European policy-making?

To prevent the above-mentioned centralisation tendencies in blockchain innovation, co-evolutionary design and democratised knowledge of the technical considerations behind protocol upgrades are needed. Some newer blockchain projects are planning to hardcode their decision-making processes into the software, in the form of smart contracts, a method known as 'on-chain governance', e.g. Tezos, Polkadot and Steemit.

Furthermore, authentication protocols should be designed in a way that minimises the risk of centralisation, through the introduction of the proof of stake mechanism. This is an innovative consensus algorithm that provides for mining opportunities in proportion to the amount of tokens held by a user on the network and facilitates voting for the approval of new blocks on the basis of the coins a user holds, rather than in accordance with their computing power. Pursuing innovative scaling solutions that provide alternative ways for businesses to offer lower fees and an efficient platform for users may also strengthen the decentralised nature and censorship resistance of blockchain. The introduction of open-sourcing patents such as the Blockchain Defensive Patent Licence (BDPL) is expected to encourage mining entities to grant their respective mining patents under a mutually defensive patent licence. Such a system will prevent any single mining consortium from obtaining the ability to launch majority (or near-majority) attacks, given that there is currently fierce competition amongst miners to obtain 'killer' patents that would essentially allow them to perform blockchain-related mining faster and in a more efficient manner, and address the relevant vulnerabilities.

Beyond these technical developments, the EU has adopted a series of institutional initiatives aimed at strengthening the decentralised character of this disruptive technology. The recent launch of the EU Blockchain Observatory and Forum in February 2018 has enriched the discussion on the opportunities and challenges of the decentralised character of the blockchain ecosystem. Recently, 24 European countries signed a declaration on the establishment of a European Blockchain Partnership, with a view to developing a blockchain infrastructure that can enhance value-based, trusted, user-centric digital services across borders within the digital single market. The partnership will be a vehicle for cooperation amongst Member States to exchange experience and expertise in the technical and regulatory fields, and prepare for the launch of EU-wide blockchain applications across the digital single market for the benefit of the public and private sectors. The European Parliament's Industry Committee recently agreed a motion for a resolution on 'Distributed ledger technologies and blockchains: building trust with disintermediation'. The resolution, due to be voted by the full Parliament in October, emphasises the need to safeguard trustworthy blockchain decentralisation, and calls upon the European Commission to explore the possibility of creating an EU-wide, highly scalable and interoperable network that makes use of the technology possible for European citizens. The main challenge associated with all these EU-level initiatives is to create a framework of legal and institutional certainty that would facilitate the development of scalable, efficient and high-impact decentralised solutions to social innovation challenges arising from blockchain applications.

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament. Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.

STOA@ep.europa.eu (contact) http://www.europarl.europa.eu/stoa http://www.europarl.europa.eu/thinktank (internet) http://epthinktank.eu (blog)