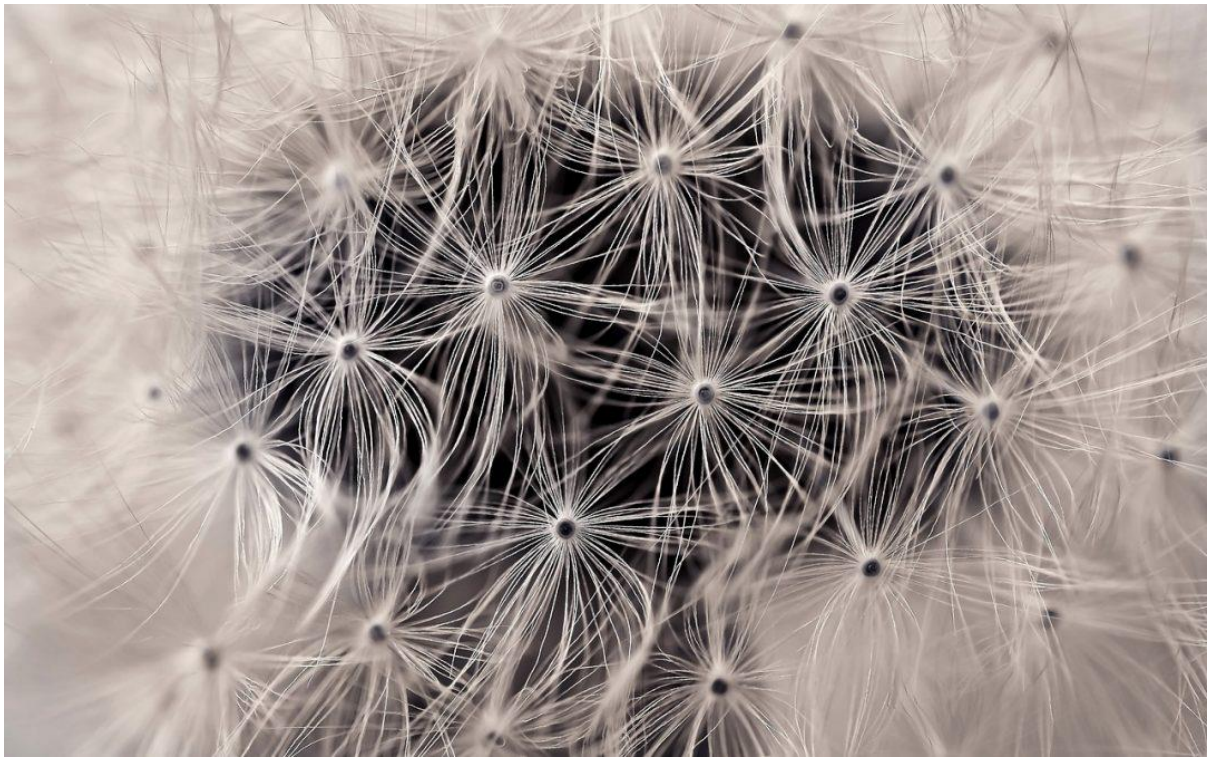
DECENTRALIZED DIGITAL NETWORKS
A POTENTIAL FOR A NEW WAY OF HUMAN COOPERATION?

REGINA SIBYLLE SURBER[1]
9 AUGUST 2021



Global society is currently witnessing the development of '*decentralized digital networks*' and applications that run on them. The text briefly describes the main underlying idea of this pragmatic and revolutionary new technology as well as some of its societal potentials.

[1] Regina Surber is a PhD candidate at the Department of Philosophy of the University of Zurich and works as a scientific advisor for both ICT4Peace and the ZHET with the current focus on the dual-use and human rights of AI-enabled technology.

DECENTRALIZED DIGITAL NETWORKS
A POTENTIAL FOR A NEW WAY OF HUMAN COOPERATION?

Key points:

- A decentralized digital network distributes information-processing workloads across multiple devices instead of relying on a single central server (centralized digital network).

- In contrast to centralized digital networks, decentralized digital networks enable a great degree of user privacy, are safer against cyberattacks, and data is ideally owned by the network user.

- In a centralized digital network, network users need to trust the central server 'agency.' In a decentralized digital network, the users need to trust the autonomous algorithm that enables user coordination within it.

- Applying decentralized technological processes can reduce or even eliminate the role of intermediaries across industries.

- Any digital application can be built on a decentralized digital network. Cryptocurrencies and the Web 3.0. are such applications. They have the potential to disrupt the current global financial system as well as the way humans exchange values on the web.

- Every aspect of human coexistence requires coordination of human activities. Until now, this coordination – especially economics and nation-states – has happened in a centralized manner. Decentralized digital networks offer a potential for creating a hierarchy-free digital world of secure human exchange of information, money, values, goods, etc.

I. CENTRALIZED DIGITAL NETWORKS

In order to understand the innovative potential of decentralized digital networks, it helps to first contrast them to centralized digital networks that currently undergird most of global society's interaction online.

Currently, most digital networks are *centralized*.[2] Centralized networks are arranged around one central server. In simple words, the central server 'verifies' all the data processing happening amongst the users in the network. The central server thereby aims to solve an

[2] The majority of today's web services – incl. YouTube or our online banking accounts – are based on centralized networks.

important problem that arises in all networks composed of a great number of users: in a network of many users that do *not* know each other's identity – and in the digital space (but not only) knowing users' identity is per se difficult – the individual users *cannot trust* that the information they receive from each other is not deceptive, nor can they trust that the information they themselves send out is not intercepted before it reaches the intended recipient. Without mutual trust they cannot reach a consensus about a certain issue. E.g., how can I know the email *really* came from you? Or, as digital objects are easy to duplicate, how can I be sure that the money I was sent was not simultaneously sent to someone else? One solution is the establishment of a central agency, the central 'server'. It figures as a monitoring device for the information flow and as an authority for publishing correct information in the network. In the email example this is the email-provider. In the money transaction example, this is a payment processor, an automated clearing house, or a bank (ultimately central banks). As the previously un-centralized networks face a trust problem when wishing to reach a consensus, they became centralized, and thereby hierarchical.

I.I. The trust problem of centralized digital networks

In order for a centralized network to function, the members must *trust* that the central authority, with its capacity to monitor the information flow in the network and its power to decide which pieces of information are true and which are not, does not *itself* deceive the members of the network. To give an example: in the traditional financial system, banks are *trusted* to show clients their balances and transaction histories in an honest manner. If a bank did attempt to lie, or defraud, its customers, a central authority higher up in hierarchy – the central bank or government – is then again trusted to rectify the bank's breach of trust. It follows that, whereas the consensus problem of decentralized networks is solved by establishing a central authority, the *source* of the problem – the problem of *trust* – is *not* solved, but merely relocated: given that centralized systems also require trust in a central authority, they are again vulnerable to corruption – not by its individual members, but by the central authority those members had established.

I.II. Disadvantages of centralized digital networks

Centralized digital networks face a number of drawbacks: First (1), the central server constitutes the network's single point of failure; if it crashes, the entire network is likely to shut down. Second (2), as there is only a single point of failure, cyber attackers must only compromise one target in order to disrupt the network. Third (3), given its centralization, data ownership and computational resources are not distributed evenly among the network. Hence, data, knowledge, and, thus, power, is located at the central server agency which needs to be trusted not to abuse it. Fourth (4), as there exists only one central depository of user data, centralized networks always involve an inherent privacy risk. If the main server is attacked, taken offline, or itself corrupted, user data may be lost.

II. Decentralized digital networks

Decentralized digital networks are a conglomerate of connected, but separated digital entities or users that communicate with each other *without* a central server. A great example of decentralized digital systems is a 'blockchain'.

In a blockchain, *every* network user must 'approve' of anything that happens in the network. Whenever information is exchanged between two or more users in the network, this is recorded and stored on *each individual* computer device – i.e. with every user – in the network. The data record of all transaction information gathered during a certain time period is called a 'block.' With transactions unfolding over time, those 'blocks' are added to the 'chain of data' in the network – hence the name 'blockchain.' It follows that the 'truth' that all network users must agree upon *is* the blockchain – that is, the decentralized network itself.

It is not so that users manually approve a transaction on a blockchain. This is handled by an autonomous algorithm that runs the decentralized digital network. The upshot is that the protection against information manipulation and misuse is *enshrined in* the technical structure of the decentralized network itself. There is no central server needed anymore. The blockchain is a decentralized database the technology of which ensures that the above-explained trust problem between network users does not arise. This is why some argue that blockchain is the first ever digital *solution* to the trust problem. However, also with decentralized digital networks, trust is still needed – not in other network users, nor in a central agency – but *in the system itself*.

II.I. Advantages of decentralized networks

It helps to visualize the blockchain network as a 'book' that stores every information exchange that has *ever* taken place on the network, and blocks as 'pages' that continuously update the state of exchanges in the network. As *each* computer device in the network maintains a copy of each 'page', this makes it almost impossible for a single computer (user) to change a page in retrospect. Hence, decentralized digital networks have the advantage (1) that whatever is agreed upon within them is almost impossible to manipulate. In addition (2), decentralized networks enable a greater degree of user privacy, since information saved on the network is disseminated across multiple points instead of passing through a single point. (3) This also makes data flows more difficult to track across a network, and eliminates the risks of having a single target that malicious actors can go after. In decentralized networks, data ownership and computational resources are ideally shared equally across the network. In addition (4), network users must not trust in a single central agency to both publish data correctly and not misuse it. Furthermore (5), centralized networks require a trusted third party, a central authority, or a 'middleman', to secure information exchange and transactions. With the possibility of decentralized systems, those previously necessary intermediaries are no longer needed. This saves time and money, and has the potential to 'give back power' to the network users:

II.I.II. Societal and economic potentials of decentralized digital networks

Decentralized networks can undergird many, if not *any*, digital application. Today, there already exist, e.g., blockchain-based contracts, software ensuring the secure sharing of medical data, cross-border payment software, personal identity security software, anti-money laundering tracking systems, voting mechanisms, or supply chain and logistics monitoring. Currently, though, the two most groundbreaking potentials are cryptocurrencies and the Web 3.0:

II.I.II.I. Cryptocurrencies

Today, decentralized networks' potential is arguably being demonstrated strongest in the financial sector. The reason is that money is a prime example of the above-described trust problem. The root problem with all conventional currency is the trust that is required to make it work: governments and central banks must be trusted not to debase currencies. However, over the course of history, this trust has been breached many times.

Bitcoin was the very first currency that runs on a blockchain and that, hence, does *not* require trust in central monetary agencies. It is a *crypto*currency because it is secured by advanced cryptography. In very simple words, the algorithmic mechanism is the following: all members of the blockchain agree on every financial transaction occurring amongst them. Thereby, they verify who owns how many bitcoins at what time and establish a functioning money without a centralized authority.[3]

Cryptocurrencies are traded directly between two or more participants of a decentralized network. This is called 'peer-to-peer trading'. Peer-to-peer trading removes the centralized middleman, allowing the users of the platform to pay minimal or zero fees to use the service.

In contrast, most traditional financial institutions charge fees and impose limits on the size, type, and number of transactions a client can execute. Additionally, some transactions in the classical centralized financial systems can take anywhere from 30-90 days to settle depending on the transaction type. Bitcoin transactions, in turn, can achieve final settlement in as little as one hour.

Central banks figure as gatekeepers of the current centralized money transaction process. They make money through interests and through the management of money and transactions. Hence, widely used cryptocurrencies and peer-2peer trading systems would make central banks, and banks in general, potentially obsolete. With decentralized financial systems, no bank nor corporation would make money out of human financial exchange – only humans themselves would profit.

This may be the reason why almost every central bank worldwide is currently trying to develop its own digital version of its fiat currency.[4] Those currencies are called *central bank digital currencies (CBDCs).* Regulated by a country's monetary authority, CBDCs are designed to replace traditional fiat and increase ease of use for those that deploy them. However, unlike blockchains, CBDCs are not decentralized. Hence, central banks must be trusted not to compromise money holders' privacy. Critics regard repercussions concerning financial privacy as well as censorship as a great risk inherent to CBDCs.

In short: the governmental resources invested in the development of CBDCs can be understood to reflect the disruptive power of applications running on decentralized systems.

II.I.II.II. Web 3.0

The term Web 3.0 refers to a vision of the 'third generation' of computing. It anticipates that technologies like blockchain will decentralize the internet, thereby disintermediating

[3] Some large companies, e.g. Microsoft and AT&T, accept Bitcoin as a legitimate source of funds. Most countries have not clearly determined the legality of bitcoin, preferring instead to take a wait-and-see approach. Some countries have indirectly assented to the legal use of bitcoin by enacting some regulatory oversight. However, as of June 2021, El Salvador is the only country that recognizes bitcoin as legal tender.

[4] As of August 2021, app. 83 countries are researching and developing CBDCs.

companies like Facebook, Amazon, Google, LinkedIn, and Apple to enable the online exchange of value, and allow users to own their data. Web 3.0 is designed to benefit all participants using a peer-to-peer model for websites, applications, and the internet as a whole. It aims to be an open, public, censorship-resistant, borderless, free internet. Analogous to a decentralized financial system: no corporation would make money out of human information exchange on the web – only the humans themselves would profit.
Every aspect of human coexistence requires coordination of human activities. Up to now, those activities – most notably economics and nation-states – have been coordinated in a centralized manner. The more global digitalization proceeds, more ways of human interaction go digital. Decentralized digital networks offer the potential for creating a hierarchy-free digital world of secure human exchange of information, money, values, goods, etc.

--

III. Key Questions

- Decentralized digital networks require trust in the algorithms that run the network. This raises a series of new questions, most importantly: can a technological artifact be a trustee? If so, what technological conditions must be in place?

- The existing global centralized human coordination mechanisms are challenged by a promising new technology favoring decentralization, and a peer-to-peer, safe and open digital exchange of values. Will those two mechanisms of human cooperation continue to coexist? Will there be a transition from centralized to decentralized human digital interaction? How would such a transition look like? Would it be socially disruptive, or could one pave the way for a smooth passage? How?

- Given the potentially tremendous influence of decentralized digital networks on every aspect of future human (co-) existence and cooperation, democratic legitimization of the algorithms that run those networks seems key. However, as those algorithms are very complex, their development and design could hardly be agreed to democratically. Hence, their application requires trust in the technologically knowledgeable. How to ensure that it is not abused?

Geneva and Zurich, 10 June 2021