The Decentralized Future

by Roberto Capodieci - Oct 2021

In this post I will talk about decentralization and blockchain. Let me start with something we all can relate to...

We all have been through the ICO craze. We all have heard these startup pitches going like: "*We're a customer centric organization and we deliver the value of IOT, cloud, big data, machine learning, and artificial intelligence by using design thinking to drive digital transformation for the blockchain connected enterprise.*"

Then you wonder what they do, and at the end is another token: "We have launched this new token called DecibelCoin. How does it work? You just yell in your microphone to get money… It's a… *ready for the pun?* It is a <u>sound</u> investment." Ok, let me make an NFT of that joke and sell it on "OpenSea".

Let's take a look at how we got here, so that we can better understand where we are headed to. We are living in what is called the Information Age (also known as the Computer Age, or Digital Age). Humans have been through the Stone Age, the Bronze Age… Yes, I'm starting from the beginning… and it is in the Iron Age where technology started being developed. I am not saying cave men were building microchips, but an ongoing evolution of some rudimental technology led to what a couple of thousands years later became the industrial revolution.

The industrial revolution is divided into subsets (for the developers, we are talking about arrays of arrays): there is the First Industrial Revolution, based on steam power used to mechanize production, the Second Industrial Revolution, based on electric power to achieve mass production, the Third Industrial Revolution, based on electronics used to have smart production.

And now, we are in what some call "the Fourth Industrial Revolution", but I prefer calling it "the Information Age", that is based on data, information, used as service and product. The Information Age is also divided in subsets (again, for the developers, we are talking about arrays of arrays of arrays): we had the initial phase where analog content started being stored and shared in digital format, a second phase where this digital content could be sent and enjoyed over networks and eventually in the internet, a third phase where services are sold and provided by individuals and companies through the internet, and the fourth phase, which has just begun, where those products and services are offered by the community to the community: the decentralization phase.

Now to the point.

Soon, protocols for decentralized systems will start replacing those of centralized web services that currently dominate the Internet. When rather than connecting to the API of some central provider our apps will interact directly with a Peer to Peer network, we will be a step into a decentralized Internet. When, rather than connecting to an ISP that is effectively a man in the middle between our computer and the rest of the internet, we will connect to a random hot spot of a global mesh network, then even the Internet, as infrastructure, will be decentralized.

There are several tools to decentralise, and blockchain is one of the prominent technologies currently used. We all know that Bitcoin, while it has the merit to have brought to us the concept of blockchain, is just one of many decentralized services that can be run on a peer to Peer network. The adoption of

blockchain is moving beyond cryptocurrency use cases. This is happening because blockchain protocols are open and anyone can implement on top of them, clone them, modify them, and, most importantly, make them better. Please note that we are talking about bottom layer blockchain platforms, not applications developed on top of them. Here is a quote from Fred Ehrsam:

> *Blockchains are digital organisms. As organisms evolve through changes in their DNA, blockchain protocols evolve through changes in their code. And like biological organisms, the most adaptive blockchains will be the ones that survive and thrive.*

The need to evolve is big.

Most blockchain technologies, consensus systems, transaction types, are thought of with a cryptocurrency in mind. This goes down to the core of how a blockchain is secured, making those platforms weak and prone to attacks if adopted on non cryptocurrency related use cases, or when managing titles of a value higher of the blockchain internal economy. In simple terms, those blockchain are secure until the ROI of the cost of an attack makes the attack viable.

For example, using current consensus systems, blockchains that are susceptible to attacks are those that manage titles worth much more than the blockchain own market cap (for example ownership titles like warehouse receipts) and those used to decentralize the management of data with no real need for a cryptocurrency (for example documents flows such as medical records).

To decentralize and be really decentralized, a blockchain should have no administrator, no central controller or authority, or even no influential charismatic leadership. In a blockchain, each user owns and controls their data. The blockchain replaces the need to trust a third-party, with the cryptographical proof of what happened, when it did happen, and the guarantee that it did happen following the protocol rules hardcoded in the blockchain core software. A transaction that does not respect the rules is not processed. I cannot send 10 bitcoins if I don't have them.

Blockchain must be seen as a decentralized system with tools to cryptographically secure data transformation. Blockchain provides the possibility of having scarcity and thus even the singularity of digital assets, something that, in the digital world, was impossible just a decade ago. Blockchain makes it possible to reach a consensus about the current state of a piece of data without having to trust any third party to tell us what the current state of that piece of data is.

Blockchain has the potential, in the near future, to fundamentally change how we share information, buy and sell things, and interact with each other and with the institutions. We will use blockchain to prove our identity, and even verify the authenticity of everything from the food we eat to the medicine we take, and, most importantly, people will own and control the data that belongs to them.

We all know that hidden layer technologies (think: databases) are often the hardest for users to relate with, as they are invisible to them! This is a problem for blockchain as well, and its adoption has been made worse due to the often negative association with illicit activities allegedly done with cryptocurrencies. A good narrative is necessary to accelerate blockchain adoption and gain the needed trust for the technology to be accepted in multiple industries.

Furthermore "blockchain" is like the new cloud, big data, or AI: too many people are using it as a buzzword without even knowing what they are talking about. Blockchain should be used to solve real problems, but it is unfortunately often forced in projects without a real need for it, just for marketing purposes.

A real working decentralized system has no centralized ownership or point of control as it belongs to the people running its P2P network nodes. Companies that create real decentralized systems hand them over to the public, remaining with no control over it, besides, maybe, owning a big chunk of its economy. The node application code is in the hands of the open source community, and the full project is public.

Once the system is public, and its code is open source, then the project is really decentralized: the public members who support the funding of the project directly contribute to the development process done by the open source community. Those that run a node of a system's peer to peer network, are contributing to the system itself by running the network, creating collective value and strengthening the system. They should be monetizing from the users' activities.

When users pay for services consumed in the P2P network, those payments should be split among the P2P node owners. Node operators need in fact to be compensated for the processing power and costs which they have allocated to run their nodes. Current systems reward ONLY the accounts that create new blocks, while the rest of the network remains uncompensated. The way to go is the reverse: punish the accounts that do NOT do a block when they should!

Let's pay attention: I am not saying that there should be no way or opportunity for businesses to monetize on decentralized services! What I've been talking about until now is the lower layer, the blockchain platform itself, which needs to be really decentralized.

Yet, decentralized applications, built on top of an open and public blockchain, may have a central point of control, an administrative account, user levels, and specific monetization methods. There is a world of services to be implemented and that are being implemented, starting from hybrid apps (that use blockchain just for some of their processes), to DAOs (applications that are fully working on the blockchain).

Many of these decentralized systems will replace existing online services and applications, but others are new, and would never have had a chance to exist if a decentralised platform to run them didn't exist. Blockchain, and more widely decentralization, offers great opportunities, and we need to focus on and use those when deploying new projects. I will share with you the story of what I believe is one of the biggest missed opportunities, when it comes to decentralization, in recent history.

We all know what Torrent is, right? No? I am sure none of you has ever done this, but Torrent is a peer to peer protocol for a network mostly used to download pirated movies and music. Well, Torrent is decentralized in its nature, as it is a Peer to Peer network, and it is the first file sharing systems authorities have not been able to shut down. Torrent is at the basis of what a blockchain is today. A blockchain cannot be shut down (if it runs on a solid protocol).

As I am heading to the end of this post, as promised I leave you with an interesting short story. Title: "The missed opportunity of the music and movie industry"

Consumers always bought music and movies. And (the more criminals) made copies of music cassettes and VHS tapes for their families and friends. This behaviour was tolerated as the loss of quality of the audio and video in analog copies made the chain of copies of copies of copies quite short.

Flashback to the beginning of the post: as we entered the first phase of the information era and content became digital, people started making copies of CDs and DVDs. At this point there is no loss

of quality, as digital copies are as good as the original. For this reason digital copies were much less tolerated. But it gets worse.

Huge drama, screaming, people running desperately in the corridors of the music and movie industry offices, management pulling hair off their heads - I am just guessing - as soon as we entered the second phase of the information era, and digital content can now be copied over the internet. The music and movie industry lobbied the governments to shut down any website, forum, and online file storage that was used to trade pirated content. Napster has been the last to stand. The music industry's litigation worked against them and Napster was served with an injunction and shut down its server in July 2001.

Then Torrent came along: a Peer to Peer network that simply cannot be stopped. The music and movie industry, now together with the software industry, as software piracy over P2P was also rampant, lobbied the governments to arrest the final users, calling them "pirates". Under U.S. law, IP infringement may result in up to five years imprisonment and a $250,000 fine. This is per item copied. While copying 1 song or a movie counted as 1 infringement, Illegally downloading MSWindows meant an infringement for each application in it: the calculator app, the notepad app, etc.

Young kids end up with multiple life sentences just for downloading pirated software from Torrent. Did this move, made by the music, movie, and software industry, accomplish to stop piracy over P2P? No. - Did they gain the sympathy of the general public? No. They were too focused to fight the windmills (if you don't get the analogy, go read Don Quixote, a novel by Miguel de Cervantes), and they missed what I believe was a great opportunity.

The possibility to sell all their ever created content, everywhere in the planet, from big cities to the smallest villages in remote countries, through a network they didn't even have to manage or pay for. They just needed to share via Torrent DRM locked content, provide free previews and the means to pay to unlock the DRM. They had the perfect wave to surf, and they missed it.

As Bitcoin, and with it the blockchain, came along, a few years later, the disrupted industry wasn't the one of music and film, but the world financial sector. I am glad that this time the reaction had been different, and as we see there is support for innovation in the financial sector.

So, let's surf this magic wave all together, as there are tons of opportunities, and we have a lot of work to do!