Five Reasons Why Cryptocurrencies Matter

Atis E

Follow

--

1

Listen

Share

Right now, the cryptocurrency market is down from its all-time high, and some of its newly attracted investors and enthusiasts risk losing their interest in the technology. It's a good time to take a step back and reexamine the fundamentals. While it's not possible to say which way the market is going to go from here, one thing is for sure — cryptocurrencies are here to stay. Here's why.

1. Global scale cooperation without trust

What makes humans so powerful? It's not our intelligence. Humans in the Stone Age had the same brain capacity as the modern humans. However, as a population Stone Age humans were weak, vulnerable, and exposed to a number of dangers. The power of the modern humans comes from their ability to cooperate in large groups.

The Internet is so important because it enables world-scale cooperation. Some of the great achievements of such cooperations are Wikipedia and large open source software projects, such as the Linux operating system.

However, trust has always been a prerequisite for cooperation between distinct parties. Whenever the levels of trust between the parties were not sufficient, the solution was to have more centralization. For example, even though I do not personally know and trust all of my next-door neighbors, it does not preclude us from peaceful cohabitation. To make this situation possible, all of us needed to place a sufficient trust on the government and other centralized institutions such as the banks and police. This may sound fine, but clearly, this idea doesn't scale that well even to a national level, not to mention regional and global levels. Now that we're faced with some truly global-scale problems, we also need global-scale solutions. Unfortunately, the levels of trust between world's nations and regions are as low as ever, hence it's difficult to make a real progress on coordinated solutions for global problems such as the global warming and the world-changing impact of AI.

Blockchain — the technology behind most cryptocurrencies — is so revolutionary because it allows to exchange value directly between parties. It doesn't require that these parties trust each another, or that they trust an intermediary. It replaces trust in central organizations with trust in source code. How do we know that this idea works? One evidence for this is the market capitalization of Bitcoin. It's based on a global, trustless network, and it's worth 500 billion dollars. Despite this lucrative sum of money, Bitcoin itself has never been hacked.

Cryptocurrency is just the first application of the blockchain technology; the proof-of-concept. However, the upcoming future applications of blockchain will not be isolated from cryptocurrencies; they will use cryptocurrencies as their base layers. For an example, consider a smart contract that defines an escrow mechanism. It's only reasonable to place as much trust on this contract as the total value of its underlying blockchain. If this smart contract is running on a currency with total valuation of less than one million, and it requires that party A pays one million USD to party B, then for party A it would be more profitable to gain control over the currency (through obtaining majority of mining power or otherwise), rather than to pay up the whole sum. Therefore only large, open blockchains backed by valuable platforms provide sufficient amount of trust for large-scale projects.

What are some examples of such projects? The blockchain technology allows to scale governance to a large number of people. Therefore the answer is "almost anything that governments and corporations currently do, and more." Through smart contracts, people will be able to participate in decision making directly, by voting with their tokens. At the moment, we continuously hear concerns from the many who are feeling left out of the "control loop" over their countries, lives, and the future in general. For good or for bad, blockchain-based technologies provide an option for the average citizen to become more directly involved in decision making. It's up to us to make the political decision whether to use this option. In any case, those with more money and influence will be able to capitalize on their powers through obtaining larger stakes in the upcoming decentralized autonomous organizations of the future.

A regular contract requires that all the parties are legal subjects under a shared legal system, which, for example, makes intellectual property rights so difficult to enforce on a global scale. Smart contracts enable peer-to-peer deals between parties who do not know each another, may not speak the same language, and may not even be traditional legal entities. For instance, IoT devices with associated wallets are valid parties in a smart contract. Imagine a smart car that communicates with other cars to autonomously negotiate priority rights-of-way! Machine-to-machine transactions may be one of the killer apps for smart contracts.

2. A resilient technology

Brick & Mortar institutions may appear to be stable than they actually are, because we're used to associate stability with an imposing physical presence. Cryptocurrencies, on the other hand, appear to be the opposite of "stable": they are volatile and clearly under the control of a myriad of external factors. Yet there are reasons to think that the ideas and technologies behind cryptocurrencies will fare much better in the long term than any present-day institutions.

I was born in the USSR, a country that used to command great power and resources. The USSR dissolved in 1991, even though the majority of its citizens still supported it, and some of them continued to passionately believe in it. Before the USSR, there was the Russian Empire — a country that also used to command great power and resources. This empire collapsed in 1917, even though many people in 1917 still supported and passionately believed in monarchy. This belief did not save the Empire. Today we have the European Union. The European Union is not like the USSR or colonial empires of the past; it aims to be a decentralized and democratic organization. But much as I like the EU, I'm open to the possibility that one day I could wake up and find that the EU doesn't exist anymore.

Some ideas are brittle, like those of empires and world powers. Others are resilient. Cryptocurrencies are based on the blockchain, which is a resilient idea. Why is that?

First of all, blockchain is a distributed

technology. In a central system, a single attack on the central node may be fatal. In contrast, a blockchain survives as long as at least some participants continue to believe in it — and they will, because blockchains also happen to be censorship resistant. As evidence for the resilience of cryptocurrencies, consider that so far they always have been able to bounce back after market crashes, hacks, and various other kinds of attacks. On the average, Bitcoin suffers several large price corrections per year. It regularly loses confidence of the markets, the mass media, and the general public; and still it survives! The temporary crises do not matter. As long as there are people who passionately believe in Bitcoin, it's going to have real value.

Second, blockchain is a technology.

It's not possible to "undiscover" technologies; once out in the open, they usually remain to be known as long as they remain useful. Many people associate Bitcoin with specific politics. But one doesn't have to be a libertarian, or believe in any politics whatsoever, in order to use blockchains! As an evidence for this, governments and banks are planning to issue their own, centralized blockchains and cryptocurrencies in the near future. But so can anyone else — and if they decide to make their cryptocurrency distributed, open and public, it has a better chance to survive in the long term, as then it will lack a single point of failure.

3. An alternative to governments and central banks

Fiat currencies have no intrinsic value. They are supported by trust in governments and central banks. Cryptocurrencies, on the other hand, are supported by distrust in governments. One can used to hedge the other.

You do not need to believe that governments are "evil" in order to admit that they occasionally screw up. Everyone makes mistakes; when entities with great powers make mistakes, their mistakes sometimes have great consequences. From a practical perspective, putting some funds in cryptocurrencies allows us to hedge against such mistakes. I would personally prefer that the governments did not screw up — even if that meant cryptocurrencies end up losing some of their value. But it cannot hurt to be prepared for the eventuality that fiat currencies might lose large parts of theirs. A new economical crisis, a new war or an environmental catastrophe with global impact are all realistic risks we need to consider. Using gold or other commodities is one way how to insure yourself against them. Using Bitcoin and other cryptocurrencies is another, a more convenient and newer way. Historically, Bitcoin has been uncorrelated with other asset classes, and should have extra demand in case of crisis.

On a different-but-related note, some governments and central banks around the world clearly don't have the best interest of their citizens in mind. Through the history, this has always been the case for some countries. Now, for the first time in history, citizens of these countries have the choice to opt out of their systems — for example, by storing their savings in cryptocurrencies instead of a hyper-inflationary fiat currency. Suddenly, the oppressive, corrupt or incompetent governments don't have as much power as they had before. Suddenly, these governments have a competition, in the form of alternative providers of financial and other services — services on which the governments so far has had exclusive monopolies. Suddenly, these governments cannot easily censor or shutdown their private competition anymore, as it's based on a resilient and distributed technology: there is no single central point to censor or shutdown.

Again, you don't necessarily need to be anti-governments in order to support this mechanism, which is just a new incentive for the good governments to do a better job in serving their citizens.

4. An alternative to corporations

For a while, it seemed that not only globalization is inevitable, but that centralization is inevitable as well. It seemed that we had just two options —either to give more control to governments, or to give more control to large corporations. From these two options, the Western world has preferred the second one. As a result, we have ended up in a situation where companies like Facebook, Twitter, Google, Amazon and Microsoft have uncomfortably large amounts of knowledge about our lives and power from that.

Now, an opening for a third option suddenly is here. Decentralized, blockchain-based social networks already exist. We have Steemit in addition to other blogging platforms. We haveDtube in addition to YouTube. In addition to Twitter, we have… a number decentralized of Twitter clones?

I don't want to create the impression that decentralized social media is going to replace Facebook soon. The technology is simply nowhere there yet; in particular customizing the access levels of content could be challenging to implement, as everything in a blockchain is public by default.

However, once implemented, decentralized blockchain-based social networks and other online services would let us to own and monetize our online presence. The digital trace that we constantly leave behind would belong to us first, not to corporations, as it's now.

5. Wealth creation and exposure to saving & investing

Cryptocurrencies have value beyond speculative investments, as already discussed; but there is no reason to completely dismiss this aspect either.

The total capitalization of the cryptocurrency market isaround 600 billion dollars. The amount of money put into the market so far is much lower than that, as most investments in this market were made when the valuations of cryptocurrencies were much lower than they are now. Even though the 600 billion never could be extracted from the market in the short term (because a large-scale sell-off would cause the prices to drop), added value eventually could be extracted in the long term. Clearly, a significant creation of wealth has taken place.

Crypto-enthusiastic millennials and the people from developing countries have many reasons to be dissatisfied with the state of global economy today. If this new asset class of cryptocurrencies wasn't here, a lot of them would not save or invest their money at all; the people in these groups are seldom attracted by the relatively small gains promised by traditional investments. Arguably, even if the cryptocurrency market drops and most participants end up losing value compared to their initial investment, these first-time investors will still get some long-term benefits from their exposure to cryptocurrencies — not the least through increased experience and knowledge about saving and investing.

Conclusion

When looking back at the most significant recent innovations from computer science, two technologies stand out in particular — cryptocurrencies and deep learning. However, while the victory march of deep learning makes me anxious and concerned about the future, the arrival of distributed ledger technologies has the opposite effect.

With deep learning, we're giving away understanding and expecting increased power

in return. This a dangerous trade-off. Deep learning algorithms automate tasks that previously required humans, and in this way give more power to those who own and control the algorithms. However, solving some real-world problems by using deep learning does not directly translate into more knowledge or insight. In the long run, we risk to become surrounded by larger and larger piles of data processed by more and more impenetrable algorithms — algorithms that we cannot comprehend, but that nevertheless make decisions relevant to our lives.

The blockchain technology promises the opposite: to empower individuals through efficient cooperation without mutual trust, and at the expense of governments, corporations and other centralized organizations. The trust can be built up through the cooperation, but isn't a necessary prerequisite for it anymore. If implemented correctly, distributed ledger technologies will allow us to scale up direct, democratic governance to global levels — something we sorely need due to the pressing global problems.

The author,

[Dr Atis Elsts

](http://www.bristol.ac.uk/engineering/departments/eeng/people/atis-elsts/overview.html), is a Research Associate in Internet of Things in the University of Bristol, UK. All opinions are his own.