An expert discusses the state of cryptocurrencies

February 7 2024, by Thomas Gull

Credit: Unsplash/CC0 Public Domain

Cryptocurrencies like Bitcoin were created to circumvent the monopoly on money held by nation states and central banks. The digital currencies were to function more democratically and be widely disseminated. But

the opposite has happened, blockchain researcher Claudio Tessone notes.

The history of Bitcoin, the first successful cryptocurrency, begins with a white paper-cum-manifesto: in October 2008, a certain Satoshi Nakamoto published a 9-page academic paper titled Bitcoin: A Peer-to-Peer Electronic Cash System, in which he explains how a new, electronic currency that enables direct payments between users without involving banks as relay stations could work.

"Satoshi wanted to end governments' and banks' monopoly on currencies and monetary transactions," Claudio Tessone explains, adding, "Instead of them being centrally organized and controlled, Satoshi's idea was to create and oversee currencies and their value 'democratically.' This was an anarcho-capitalist concept: the market should regulate itself without state intervention."

Tessone is a professor of blockchain and distributed ledger technologies at UZH. He researches the economic incentives for cryptocurrencies and the blockchain technology that makes them possible.

Fostering trust

Satoshi Nakamoto, whose true identity is unknown, put his money where his mouth is and rolled out the Bitcoin software as an open-source code in 2009. He "mined" the first 50 bitcoins and set the rules on how to mine others. Mining is the process through which new bitcoins get minted and brought into circulation.

Nakamoto also defined what it takes to mine bitcoins: proof of work. In the realm of cryptocurrencies, "proof of work" means that participants, called miners, must prove that they have completed the computational work required to verify and validate a block of digital data records, a

multiple of which make up a blockchain, and to add it to the existing blockchain as the next block. This work is essential to the blockchain because the blockchain consists of a ledger of all verified transactions.

The gapless documentation of those transactions is designed to foster the necessary trust in Bitcoin and to supplant the faith that market participants typically place in institutions like central banks. Nakamoto phrased it this way: "What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party."

In the beginning, bitcoins were practically worthless. Software developer Laszlo Hanyecz went down in history as the person who conducted the first-ever commercial transaction using a cryptocurrency: he paid 10,000 bitcoins in exchange for two pizzas.

That would have equated to a sum of more than 600 million US dollars at the peak of Bitcoin's all-time price high. Rumor has it that Hanyecz doesn't regret his decision. His pizza purchase, in his view, was a crucial step toward establishing cryptocurrencies as a medium of exchange.

Few market participants left

In January 2013, the value of one bitcoin surpassed the USD 1,000 mark for the first time. A couple of booms and crashes later, one bitcoin today costs more than 30,000 Swiss francs.

"My wife sometimes criticized me for not having bought any cryptocurrencies even though I've been studying and researching them for more than a decade now," Claudio Tessone says. The crypto researcher attributes his personal reluctance toward cryptocurrencies to his aversion to risk. Moreover, and importantly, through his research,

Tessone is also familiar with the problems facing cryptocurrencies today.

Most cryptocurrencies have evolved quite differently than their founders intended, particularly with regard to the concept of decentralizing power and spreading it among as many participants as possible by involving many different actors in the minting of crypto coins. "What we're seeing today is exactly the opposite," Tessone explains. "Today, there are only a few giant market participants left that are capable of mining new coins," he says.

Incumbents benefit more

Why is that? Given the growth of cryptosystems today, it takes an enormous amount of computing power and, thus, an awful lot of computer hardware and energy to verify and validate data chains. That's expensive and thus requires a lot of capital. A lone market participant with their computer, therefore, no longer has any chance of doing this work and earning the right to new coins.

This is why some blockchains require "proof of stake" instead of "proof of work." Proof of stake requires less computational power but favors incumbent market participants with greater stake weight. The proof-of-work and proof-of-stake mechanisms both lead to a concentration of power in cryptocurrencies and blockchains.

That actually ought to undermine trust because trust is based on collective control by stakeholders who have a mutual interest in everything operating fairly. "If there are only a handful of them left, why should anyone trust them?," Tessone asks. "Especially if they're anonymous," he adds. Concentration of power is dangerous, the blockchain researcher says, because it's an invitation to malfeasance. "That's why laws are needed to regulate cryptocurrencies."

How could it have gotten to this point? Tessone blames it on misplaced incentives. Since it was transparent from the start how to mine new coins, participants worked out how to exploit the system by, for example, acquiring massive computing power to produce proof of work.

"Today in the crypto world, we are observing the same phenomena that prevail in the real economy: for whosoever hath, to him shall be given, or in other words, the rich get richer," Tessone says. Moreover, cryptocurrencies usually are not used as a means of payment. Most coins are hoarded as speculative assets.

Something more useful

According to Tessone, the evolution of Bitcoin and other cryptocurrencies is an example of "what can go wrong despite the best intentions." That certainly goes for Bitcoin, whose founder wanted everyone with a computer to be able to participate in it. Satoshi Nakamoto's own thoughts about this are unknown. He issued his last public message in December 2010 on the Bitcointalk online forum and then disappeared without a trace in April 2011.

Do cryptocurrencies have a future? In his analytical research, Tessone has observed that some cryptocurrencies are trying to configure their respective systems in a way that doesn't as richly reward concentration down to just a small number of participants. It remains to be seen whether that is enough to rectify the systems' current design flaws.

Tessone sees the real value of cryptocurrencies lying more in the innovations they have spawned. "Those innovations could be applied to the broader economy to do something more useful," the crypto researcher sums up.

Fraud in the digital economy

Blockchain technology creates complete transparency in the trading of digital assets such as non-fungible tokens (NFTs) or coins. When a unique digital asset of that kind is sold, the transaction is recorded in a blockchain. Despite that, digital trading opens up a wide range of possibilities for fraud.

Claudio Tessone examines fraudulent practices such as wash trading and rug pulling. In wash trading, traders engage in bogus transactions by repeatedly buying and selling the same asset to each other at a progressively higher price, creating the illusion of demand for the asset. This can dupe outside investors into acquiring the asset for an overblown price.

Tessone's research has shown that wash trading is a widespread practice. "This is startling," the blockchain researcher says, "because most perpetrators don't even cover their tracks." This means that looking at the blockchain would show potential buyers that the price was manipulated.

Another form of fraud is rug pulling. In this type of scam, investors are promised high returns if they invest in a crypto project. When enough money has been gathered, the project developers then abscond with all of the liquid funds, pulling the rug out from under the feet of the other investors and leaving them holding worthless shares (tokens) in the project.

Tessone finds it incomprehensible that many buyers and investors don't do closer due diligence when they purchase digital securities. "They often are naïve and don't understand that the transparency of the blockchain would enable them to see that they are getting conned."

Tessone is thus advocating for rules for the digital economy analogous to those governing the bricks-and-mortar economy. Switzerland already has such laws in place. "We need them worldwide," Tessone says. At the same time, though, all of the laws on the books are useless if investors don't prudently scrutinize who they are entrusting their money to.

Provided by University of Zurich