Funding the Future

Article URL

Published: January 12, 2026, 5:00 pm

The problem with Bitcoin is not who supposedly created it, or did not. That's just mumbo-jumbo of no consequence. The following note was written in March following a discussion at City University and not developed further at that time, so I share it here now because I do believe that there are very real problems with Bitcoin and the supposed blockchain. But, I stress, I am open to persuasion as a person should be.

The problem that I see with Bitcoin can all be explained using double entry book keeping, plus a little bit of explanation of the supposed technology as I understand it.

The first thing to say is that there is no such thing as a Bitcoin. A Bitcoin is represented by an entry in a computer ledger kept on a peer-to-peer network, the multiple versions of which that should all reconcile comprising what is called the 'blockchain'. There is nothing intrinsically smart about this that I can see: all the peer-to-peer system supposedly does is eliminate the need for a central bank for Bitcoin.

The Bitcoins in use are all created out of thin air, as is any other currency in the modern economy. I am well aware that there is a supposed 'mining' process to create new Bitcoins and that every ten minutes or so someone who wins the 'race' to solve the utterly useless task of unravelling the next iteration of the Bitcoin algorithm has the right to put into use the coins required to clear the uncleared transactions since the last race was won. But, when they do so all they actually win is the right to put an entry into the blockchain ledger, which is the debit entry representing the new coins.

This is where the problems really begin. As far as I can see - and I may be wrong - so I accept I am open to correction here - the balancing credit is not recorded in that blockchain. In other words, the blockchain is not a ledger in the accounting sense that we have known it since Luca Pacioli invented double in 15th century Italy. It appears to be single entry record keeping. This gives rise to two issues. I will deal with both in turn as both are substantial before then considering some of the economics of this. As an aside though let me make clear that the issue of single entry I refer to is not the same as the supposed triple entry issue some talk about with Bitcoin. This is a supposed advantage of entries being duplicated in multiple versions of the ledger that it is

claimed means that fraud is hard. I am suggesting something entirely different, which is that entries may be entirely absent.

The first reason for saying so arises from the question as to what happens to that credit on the creation of this money? Credits can be three things. They are liabilities, or income, or equity reserves. That's it in double entry. In many ways it is not a very sophisticated language. To put it another way, does this mining represent someone's income? Or is it, as it would be in a bank when money is created, properly reflected as a liability (even notes and coins represent liabilities of the Bank of England, which is why notes say they represent a promise to make payment), or is this a credit to the capital of Bitcoin, albeit that no one seems to know who might own that capital?

My very strong suspicion, based on the Bitcoin narrative, is that this credit is effectively taken as income. This must mean it is credited to the account of the Bitcoin miner who then via the entry in their books treats it as income against which they offset the supposed costs of the mining process (the reality of which is, for all I know, just another Bitcoin rumour) to then take the resulting net sum after expenses for their gain. In other words, if the credit is technically a liability in the blockchain when the initial double entry for coin creation takes place then it is one that is then, apparently, settled almost immediately in the Bitcoin narrative by way of payment to the account of the miner as recompense for the costs they incur in Bitcoin creation. But we cannot be sure of that. So much for the transparency of the blockchain.

However, if I am right (and the so-called mining narrative seems to require that I am) then the blockchain has no capital left in it because the only sum available to make settlement to the Bitcoin miner will be the coins they have created. Except that, according to the blockchain, those coins are now still in the system. That can only be explained by the blockchain being a single entry system where the consequence of the capital in the system having apparently already been extracted to pay the Bitcoin miner is ignored. That is concern number one, and logic seems to suggest it must be right. After all, if there was capital in the system continual mining of new Bitcoins to clear transactions would, surely, not be needed? It is because there is no liability that can be cleared through the payment system (as happens in conventional banking, where cash can be and is cancelled on loan repayment, which is a possibility that does not appear to exist in Bitcoin) that requires the continual creation of new debits because there are no credits in the system.

This then presents the second conundrum. This is that the payment system in the blockchain is, if I am right, a continual system of reallocating the debits. Now I accept that it can be argued that this is a debit and credit process, and of course in a sense it is, but subject to the massive overall condition that all the sums must be part of a continually accumulating overall sum of Bitcoins in existence, or the miners would generate no continuing value. This is not then a system of true debits and credits in because net credits are not apparently allowed. This means that the blockchain is not remotely close to a proper banking system where the process of creating simultaneous

debits and credits that remain on the balance sheet until loan repayment, giving rise to account offsetting and so cancellation, is the fundamental process that singularly identifies the existence of a credit creating bank.

At this juncture then a note of economic concern has to be raised. A blockchain where the extraction of value (the credit transactions) is not identified but where it is said that the supply of debits is finite (as the Bitcoin algorithm must imply) has at least three important economic characteristics that pose difficulties. One is that it attempts to mirror the operations of the gold standard, which proved to be little short of an economic disaster during its period of use in the twentieth century. Secondly, because of its opacity, the system is at best inherently risky. And third, it would appear that the arrangement could, because of its opacity, be exploited. I am not saying it is: I am saying that based on my initial review I have that concern. I stress however, someone may allay my fears and so I may be wrong. But, based on what I have seen that possibility exists.

So let me summarise my concerns.

First, the blockchain, about which so much is said when Bitcoin is discussed, does not appear to be a credible accounting system. It seems to be single entry at best and such systems were rightly abandoned many centuries ago because they did not allow proper risk appraisal.

Second, the apparently missing credits within the blockchain might represent an absence of capital and so an inherently unstable system.

Third, that the system requires continual data mining suggests that all transactions are reallocations of existing and new currency and are not matched by the settlement of liabilities as would be expected in what we understand to be a banking system.

The consequence is that Bitcoin appears to be a claim on nothing at all. All banks are a confidence trick but most are at least based on the idea that a deposit may be capable of settlement out of capital, loan repayments or government guarantee (in the last resort). In the case of Bitcoin none of those credits provide such comfort - it is just the hope that there will be new debits (mined Bitcoins) that provides this comfort. And when the system is supposedly finite that seems like a perilous act of faith.

Comment would be welcome. It would be good to be wrong on this one, and you never know, I may be. But please, address the concerns. I do not need rhetoric, abuse or assertion. Just tell me what the debits and credits are and reconcile them with Bitcoin mining, the blockchain and the continual needs for new coins.