The blockchain pipe dream

Nouriel Roubini & Preston Byrne | 06 March 2018

Predictions that Bitcoin and other cryptocurrencies will fail typically elicit a broader defense of the underlying blockchain technology. Yes, the argument goes, over half of all "initial coin offerings" to date have already failed, and most of the 1,500-plus cryptocurrencies also will fail. But "blockchain" will nonetheless revolutionise finance and human interactions generally.

In reality, blockchain is one of the most overhyped technologies ever. For starters, blockchains are less efficient than existing databases. When someone says they are running something "on a blockchain" what they usually mean is that they are running one instance of a software application that is replicated across many other devices.

The required storage space and computational power is substantially greater, and the latency higher, than in the case of a centralised application. Blockchains that incorporate "proof-of-stake" or "zero-knowledge" technologies require that all transactions be verified cryptographically, which slows them down. Blockchains that use "proof-of-work" - as many popular cryptocurrencies do - raise yet another problem: they require a huge amount of raw energy to secure them. This explains why Bitcoin "mining" operations in Iceland are on track to consume more energy this year than all Icelandic households combined.

Blockchains can make sense in cases where the speed/verifiability tradeoff is actually worth it, but this is rarely how the technology is marketed. Blockchain investment propositions routinely make wild promises to overthrow entire industries, such as cloud computing, without acknowledging the technology's obvious limitations.

Consider the many schemes that rest on the claim that blockchains are a distributed, universal "world computer". That claim assumes that banks, which already use efficient systems to process millions of transactions per day, have reason to migrate to a markedly slower and less efficient single cryptocurrency. This contradicts everything we know about the financial industry's use of software. Financial institutions, particularly those engaged in algorithmic trading, need fast and efficient transaction processing. For their purposes, a single globally distributed blockchain such as Ethereum would never be useful.

Another false assumption is that blockchain represents something akin to a new universal protocol, like TCP-IP or HTML were for the Internet. Such claims imply that this or that blockchain will serve as the basis for most of the world's transactions and communications in the future. Again, this makes little sense when one considers how blockchains actually work. For one thing, blockchains themselves rely on protocols like TCP-IP, so it isn't clear how they would ever serve as a replacement.

Furthermore, unlike base-level protocols, blockchains are "stateful" meaning they store every valid communication that has ever been sent to them. As a result, well-designed blockchains need to consider the limitations of their users' hardware and guard against spamming. This explains why Bitcoin Core, the Bitcoin software client, processes only five to seven transactions per second, compared to Visa, which reliably processes 25,000 transactions per second.

Just as we cannot record all of the world's transactions in a single centralised database, nor shall we do so in a single distributed database. Indeed, the problem of "blockchain scaling" is still more or less unsolved, and is likely to remain so for a long time.

Although we can be fairly sure that blockchain will not unseat TCP-IP, a particular blockchain component – such as Tezos or Ethereum's smart-contract languages – could eventually set a

standard for specific applications, just as Enterprise Linux and Windows did for PC operating systems. But betting on a particular "coin" as many investors currently are is not the same thing as betting on adoption of a larger protocol. Given what we know about how open-source software is used, there is little reason to think that the value to enterprises of specific blockchain applications will capitalise directly into only one or a few coins.

A third false claim concerns the "trustless" utopia that blockchain will supposedly create by eliminating the need for financial or other reliable intermediaries. This is absurd for a simple reason: every financial contract in existence today can either be modified or deliberately breached by the participating parties. Automating away these possibilities with rigid "trustless" terms is commercially non-viable, not least because it would require all financial agreements to be cash collateralised at 100%, which is insane from a cost-of-capital perspective.

Moreover, it turns out that many likely appropriate applications of blockchain in finance – such as in securitisation or supply-chain monitoring – will require intermediaries after all, because there will inevitably be circumstances where unforeseen contingencies arise, demanding the exercise of discretion. The most important thing blockchain will do in such a situation is ensure that all parties to a transaction are in agreement with one another about its status and their obligations.

It is high time to end the hype. Bitcoin is a slow, energy-inefficient dinosaur that will never be able to process transactions as quickly or inexpensively as an Excel spreadsheet. Ethereum's plans for an insecure proof-of-stake authentication system will render it vulnerable to manipulation by influential insiders. And Ripple's technology for cross-border interbank financial transfers will soon be left in the dust by SWIFT, a non-blockchain consortium that all of the world's major financial institutions already use. Similarly, centralized e-payment systems with almost no transaction costs – Faster Payments, AliPay, WeChat Pay, Venmo, Paypal, Square – are already being used by billions of people around the world.

Today's "coin mania" is not unlike the railway mania at the dawn of the industrial revolution in the mid-nineteenth century. On its own, blockchain is hardly revolutionary. In conjunction with the secure, remote automation of financial and machine processes, however, it can have potentially far-reaching implications.

Ultimately, blockchain's uses will be limited to specific, well-defined, and complex applications that require transparency and tamper-resistance more than they require speed – for example, communication with self-driving cars or drones. As for most of the coins, they are little different from railway stocks in the 1840s, which went bust when that bubble – like most bubbles – burst.

Nouriel Roubini is Chairman of Roubini Global Economics and Professor of Economics at New York University's Stern School of Business.

Preston Byrne is a Fellow of the Adam Smith Institute and Sole Member at Tomram Consulting.