KNOWLEDGE@WHARTON

INNOVATION

Why Blockchain Isn't a Revolution

Jun 20, 2018 North America Opinion

The terms Bitcoin and blockchain are sometimes used interchangeably, but there's actually some misunderstanding about the innovation. In this opinion piece, Kevin Werbach, Wharton professor of legal studies and business ethics, explains the differences among the three groups that comprise this technology: cryptocurrency, blockchain and cryptoassets.

These days it's hard to avoid pronouncements about how cryptocurrencies and blockchain technology could change everything (or at least, create massive wealth). Yet there's an equally loud chorus labeling them a massive scam, useless, and dangerous. And a surprisingly large audience still doesn't understand what's going on. One big reason for the confusion is that we're not all talking about the same things.

The three communities share a basic set of design principles and technological foundations, but the people, goals, and prospects are almost completely distinct. Those involved don't help much by sniping constantly about which is the "real" movement. So, let me try to clarify things.

There is **cryptocurrency:** the idea that networks can securely transfer value without central points of control. There is **blockchain**: the idea that networks can collectively reach consensus about information across trust boundaries. And there are **cryptoassets**: the idea that virtual currencies can be "financialized" into tradable assets. The first truly is a revolutionary concept, but the jury is still out on whether the revolution will succeed. The second and third are game-changing innovations on the path to significant adoption, which are nonetheless essentially evolutionary.

Cryptocurrency ('Trust-Minimizing')

Cryptocurrency is what you've probably heard the most about, starting with Bitcoin. The easiest way to understand it is not to puzzle over the details of mining or digital cash. Instead, focus on the decentralization of trust, as I do in my forthcoming book.

Many activities require trust. Without trust, a $20 bill is just a green piece of paper, a vote in an election is a pointless ritual, and someone offering me a ride in their car is a potentially dangerous stranger. Traditionally, trust meant depending on partners, institutions, or intermediaries. Those centralized trust architectures are powerful; among other things, they brought us modern industrial civilization. But there's a downside to trust. Trust implies vulnerability. The people, governments, and companies we trust may turn out to be untrustworthy, for any number of reasons. Bitcoin showed that something valuable — money — could be trusted without trusting anyone in particular to verify transactions.

The idea, if brought to full fruition (and that's a huge "if"), could transform society. We could have transparent companies that truly reflect the will of their stakeholders, governments that truly reflect the will of their citizens, an internet freed from the corrupting value-extraction of powerful gatekeepers, the end of fake news, and massive automation of daily life for the betterment of humanity. Or at least, we could have solutions that markedly improve on the status quo. Decentralization is valuable in all sorts of ways.

> **"Bitcoin showed that something valuable — money — could be trusted without trusting anyone in particular to verify transactions."**

There's a cost. (There's always a cost.) For Bitcoin, the costs involve a very slow network with limited functionality that wastes massive amounts of electricity and enriches a side community of miners. Maybe those are worth it. Maybe technological advances, through the parade of new blockchains and blockchain enhancements, will drive down the costs. We don't know yet. Yes, the bitcoin in circulation is notionally worth north of $100 billion, but that's cryptoasset thinking. Is anyone using bitcoin yet to *do* something, other than to get rich, to make a point, or to avoid law enforcement? And it gets steadily worse as one progresses down the list of nearly 2,000 (or perhaps many more) extant cryptocurrencies.

There's also a catch. (There's always a catch.) What works for small groups, bounded applications, and idiosyncratic users doesn't necessarily survive the climb to the mainstream. If it does, it often becomes something completely different. Until Facebook came along, it wasn't clear anyone could make real money on social networking, which was just a frivolous exercise for kids anyway. The fact Facebook did come along doesn't prove it was inevitable.

Some of those betting on the cryptocurrency revolution may be proven right. It's an exciting bet, with all kinds of potential upside, but still a gamble. There's a reason true revolutions don't happen often. And when they do, there tends to be heavy collateral damage.

Blockchain ('Tracking')

The blockchain* phenomenon grows from the same root as cryptocurrencies — the Bitcoin white paper of 2008 and its antecedents — but seeks something very different. Rather than trying to do without trust, blockchain starts from the premise that our trust is too limited. We only *really* trust ourselves, or our own organization. Yet no person, or company, is an island. Even the government of an island isn't an island, for that matter, when it has to trade and interact across the water.

The world is filled with processes, especially among larger companies and governments, where things must be tracked from one trusted zone to another. Firms spend $10 trillion per year globally on "logistics," which is short for putting stuff on transportation systems controlled by someone else. Manufacturers, distributors, and retailers keep their own trusted (yet independent) records of the same items as they flow through supply chains. When you walk into a new hospital or doctor's office, your medical records don't necessarily walk in with you. They are even less likely to walk out together with the new ones you generate. All of these breakdowns in information flow feed the fearsome dragon known as transaction costs. According to the dominant school of economics today, the effort to slay that dragon is the essential driving force in the economy.

A significant chunk of the transaction costs between firms (and sometimes within them) flow from the limited elasticity of trust. If every party to a transaction trusted the information involved, even though they didn't trust one another, costs could fall and performance could improve drastically. That is the essence of the blockchain vision.

> **"Trusting your own records on a blockchain is tantamount to trusting everyone else's records, because those records are one and the same."**

Trusting your own records on a blockchain is tantamount to trusting everyone else's records, because those records are one and the same. The duplication of settlement, the further duplication of reconciliation, the further duplication of auditing, and perhaps the further duplication of regulatory reporting, can all fold into the original transaction. The most prominent companies in the world are participating in all manner of blockchain trials and consortia because they see the huge potential. Decentralization here is one design goal among several, not a foundational requirement as with cryptocurrencies. So these systems typically are "permissioned," with essential functions limited to identified participants.

As with cryptocurrencies, there are aspects of this story that are still speculative. Because the blockchain thesis doesn't assume any radical changes in markets or business models, though, it's a question of degree only. Cryptocurrency advocates carp that you don't *need* a blockchain for any of these arrangements. Well, you don't need a blockchain to create digital money either. It's only

when you want to add the condition that banks can't intermediate, governments can't block transactions, and no one can influence the money supply that Bitcoin has a purpose. The blockchain thesis similarly targets a particular class of scenarios. Traditional database solutions don't solve these problems because the people and companies involved don't agree in practice, not because of some failing in theory.

Cryptoassets ('Trading')

Cryptoassets take cryptocurrency tokens, turn them into instruments of trading, and spin ever more complex financial instruments out of the threads they produce. The potential scale is immense, with trillion-dollar markets not that unusual in modern finance. Where this effort diverges from the first is that it views cryptocurrencies not as a way to facilitate activities without centralized trust, but as a new investment asset class. Because they are natively digital, cryptoassets can in theory be traded more efficiently than existing instruments. They are inherently flexible and global. Virtually all of the major Wall Street players are eager to get in on the action, as are the institutional investors that supply them with capital. Regulatory concerns that kept them out are gradually being addressed.

Once the fundamental value of a digital token on a decentralized network is established, why not just use it to make money? (Sorry, to "engage in socially optimal capital formation.") Cryptoassets depend on the *fact* of cryptocurrencies, because there needs to be something valuable to trade. Securities must be secure. But cryptoassets ignore or reject the *idea* of cryptocurrencies, that trust is "almost an obscenity" (to quote the man who did the original security audit on Bitcoin). To the cryptoasset trader, both trust and the absence of trust are nothing but means to an end, known as liquidity.

Permissioned blockchains will also support tokenized assets, by the way, including eventually sovereign currencies. The difference is that the goal will be effective tracking more than profitable trading.

Another way to think of this is that cryptoassets divorce the exchange function of cryptocurrency tokens from their utility functions. If you want to use bitcoin to pay merchants, Ethereum's ether to purchase computing cycles for distributed applications, Filecoin to purchase cloud file storage, or Augur Rep to verify the results of prediction markets, you put a value on those tokens based on what you get out of the application. In theory, more demand for use in the application means less available supply, which pushes up the price. In practice, none of the applications are significant

yet, so the value of the tokens is highly speculative. Speculation isn't necessarily a bad thing; it's the appetite for risk that drives financial markets. Sometimes, though, that speculation drives markets over a cliff. The key question for cryptoassets is whether and how speculative instincts will be modulated.

> **"Cryptoassets divorce the exchange function of cryptocurrency tokens from their utility functions."**

If cryptoasset markets develop, there are all sorts of interesting possibilities for "tokenizing" physical things like commodities and real estate, digital things like intellectual property, and other kinds of rights, using the financial engineering and analytics tools Wall Street has developed over the years. The necessary foundations are already being built.

Don't Cross the Streams

The stories aren't mutually exclusive, per se. The success or failure of any one vision doesn't necessarily imply much about the others. Cryptocurrencies have the most disruptive potential, because they promise to decentralize power. That also creates the biggest barriers to success. Both blockchain systems and cryptoassets scale back that decentralization for other benefits. They differ in the uses they target, so it's not a competition to determine the right answer. Crossovers can generate significant opportunities, but they need to be evaluated in their own lane. Initial coin offerings (ICOs), for example, fuse cryptocurrencies and cryptoassets. Should they be assessed as a new form of crowdfunding or a way to kickstart decentralized economies? What counts as success or failure looks different depending on the answer.

Deciding which is the "real" phenomenon can be an entertaining parlor game, but it's ultimately not enlightening. Any judgments about success or failure of blockchain-related technologies need to be couched in terms of the relevant sub-category. When observers point to enterprise adoption and high prices on cryptoasset exchanges as evidence for the viability of cryptocurrencies, they're crossing the streams. The fact that there's massive fraud and theft in the ICO world doesn't tell

you much about government initiatives around distributed ledgers. Whether or not there's a good business putting banks on blockchains(or something blockchain-like) says little about the prospects for decentralized automated organizations.

The sooner we stop treating this as a unitary phenomenon, the more we'll be able to assess developments accurately.

**I use the term 'blockchain' for this category, because it emphasizes the value of the ledger over the currency or decentralization. Speaking precisely, though, most cryptocurrencies and cryptoassets use blockchains as well. And not every 'blockchain' system employs the data structure of a hash-linked chain of blocks.*

This article first appeared in Medium.
