Blockchain: Everyone Talks The Talk, Who Will Walk The Walk?

Mar. 29, 2016 7:47 AM ET6 comments
by: Kurt Dew

Summary

- What is blockchain?

- Blockchain is a giant changing spreadsheet which will revolutionize finance.

- This article begins to explain blockchain, and its enormous investment implications.

- There will apparently be competition among national governments for blockchain domination.

For the loser now
will be later to win.

For the times they are a-changin'.

- Bob Dylan

Where will "blockchain" realize its full potential first? In Boulder Colorado, as an alternative to banking among marijuana dealers - who are presently barred from the federal banking system? Or in New York City, where the big banks seek to tame it? Or in Israel or Japan, where these surprisingly entrepreneurial governments have blessed it? I wonder. But you, the reader, should be thinking about blockchain.

Financial markets will be unrecognizable when blockchain is fully exploited. Potentially blockchain will put an end to exchanges and their clearing houses. Blockchain will make foreign currency trades easier, cheaper, and nearly instantaneous, without the cooperation of a bank; a development that is already taking place.

I have not yet begun to sort out the corporate winners and losers, but many are in this banks and fintech firms are in this game, clutching their playing cards tightly to their chests.

In this article I begin to explain blockchain and discuss its implications for investors. Let me begin with a teaser. It is my firm conviction that whether you know it or not, within five years, and possibly as soon as one year from now, you will use blockchain on a routine basis every day.

My plan for this article is that you, the reader, will be among the few who are actually aware they are using blockchain. But everyone will realize that something just made financial transactions infinitely cheaper and easier.

That teaser was really necessary, though, because understanding blockchain is a process that can only be begun with one article - and understanding blockchain is an annoying process that I have not completed. Furthermore, I have gone far enough to decide I never intend to fully understand blockchain. There are tech people for that.

What is blockchain? According to Investopedia:
A blockchain is a public ledger of all Bitcoin transactions that have ever been executed. It is constantly growing as 'completed' blocks are added to it with a new set of recordings. The blocks are added to the blockchain in a linear, chronological order. Each node (computer connected to the Bitcoin network using a client that performs the task of validating and relaying transactions) gets a copy of the blockchain, which gets downloaded automatically upon joining the Bitcoin network. The blockchain has complete information about the addresses and their balances right from the genesis block to the most recently completed block.

See what I mean? Not that clear, is it? So let me suggest first, how I think of it. Then, why I care. Then what's in the way.

How I think of it. Most readers have doubtless heard of Bitcoin. This is, in the popular mind, an internet form of money that facilitates illegal transactions and competes with gold and flat currencies. A preferred means of payment for money launderers everywhere. And popular with the counterculture.

Its value as a facilitator of illegal transactions is unquestionably an aspect of Bitcoin; and by association, blockchain. But for a moment let us set this nastiness aside and consider what the blockchain technology is, and how it is connected to Bitcoin. Because blockchain is actually likely to reduce financial criminality.

This is how I think about blockchain: Blockchain is simply a gargantuan spreadsheet. And if you noticed, the Investopedia definition gives you an idea of just how gargantuan it is now, but more to the point - how infinitely more gargantuan it could become. The real question is, if a substantial portion of the world's population began to use blockchain to pay for everything from toothpaste to $50 million loans, are there enough giga-tera-bytes of computer power on Earth to contain it?

You are probably thinking "A spreadsheet that would keep track of all the world's transactions in a day would have to be enormous." But if that's what you're thinking, you are considering only the smallest fraction of what blockchain does.

First of all, every blockchain contains the full record of all transactions from the very creation of the first blockchain. So, for example, if you buy a used car with blockchain, blockchain knows every previous owner of the car including the manufacturer, the days it changed hands, and the prices. And the same may be said of every used car bought using blockchain. Since every user has access to every transaction on blockchain - let me repeat that: every user has access to every transaction in blockchain - entrepreneurs could collect the dates of services and repairs to your used car and sell that information on every used car as well. That would certainly have an arresting effect on the used car business (pun intended). And that is some big spreadsheet.

Now wrap your mind around the fact that the blockchain is updated every ten minutes, not once a day. If this sounds like so many computations that a single computer - even a very, very, big computer - might choke on the job, you're getting the idea.

But that's not the end of it. Many computers must agree on the entire update for it to become a new blockchain. So no single computer can create the blockchain that the world uses for the next ten minutes, which is part of the elegance of the invention. If no computer can update blockchain on its own, is blockchain unhackable?

Perhaps one computer operator or operators, using multiple computers, could update blockchain on her own. Perhaps. She would need to match the computing power of the "miners" computers. (Miners are the collection of computer operators who collectively manage blockchain.) Miners have a large amount of computing power, currently about 9,800,000 petaFLOPs - that's 9.9 sextillion (9.8 followed by 21 zeroes) operations per second. Learn more here. "Currently, the world's fastest supercomputer is China's UDT Tianhe-2 which runs at 'only' 33.9 petaFLOPS. Hence, to match the distributed power [of blockchain], you would need nearly 300,000 of the world's fastest supercomputers," explains Campbell Harvey of Duke University, here. (my insertion) So it could be done.
I have no current plans to try. On the other hand, while blockchain itself has not been hacked, several applications based on blockchain, such as blockchain storage facilities, have. And as with any system that is purportedly secure, the attempts at hacking are constant and determined.

Blockchain. Simple, really.

OK. Enough painful blockchain explanation. No, I haven't explained it, but that's all I've got for now. But you can see it's not a bunch of drug dealers. It's a bunch of operators of really big computers, spending their days updating monster spreadsheets. If you think that sounds unromantic, consider that they are mostly located in Iceland where the energy costs needed to run these monster computers flat out, 24 hours a day, is the cheapest in the world.

I will further explain how blockchain works in later articles, including the critical issues of hackability and government regulation.

Why I care. Think about any of the world's transactions clearing mechanisms. The Fed clears the world's Treasury bills. The banks clear the payments in your city, the world's checks and credit card payments, foreign exchange trades, and some OTC swaps. The DTCC clears the US securities markets. There are several futures clearing houses. There are many other exchanges, for everything from seafood to jobs, all over the world.

Any mark-to-market clearer - including the most efficient, futures exchanges - clears and updates portfolio values at best twice daily. But in theory, with blockchain, all these exchanges can discard all their electronic systems, move their operations to blockchain, and increase the frequency with which positions are margined to every ten minutes!

Poof!! Several billion dollars saved! Daylight and T+3 risk? Vanished! No more three days to clear a trade. In fact, the exchanges might as well be disbanded.
The only exchanges left would be the OTC swaps clearing houses. They would still be necessary because clearing OTC swaps requires human opinion, not market transactions. In other words, because nobody is sure what an OTC swap is worth, a spreadsheet can't be used to value them. This fact is a little awkward. That the OTC clearing houses guess at the value of their $300 trillion + in swaps was not so public before blockchain. But perhaps once the globe confronts this stupidity, the result would be a sane way of clearing OTC swaps.

**What's in the way?** But could this all blockchain magic work? There is no government regulation! Well, obviously not the way blockchain works today. If nothing else, governments would have to provide insurance that the whole thing doesn't crash one fine day.

And until recently, I thought that problem, and of course the dealer bank and exchange oligopolies, would be enough resistance to slow the introduction of blockchain to a snail's pace.

But I may have been wrong. Enter the Japanese and Israelis - governments that are becoming enthusiastic about the future of blockchain. I'm not sure why the Israelis are so supportive of blockchain. Perhaps it's their citizen's outsize number of retail foreign currency transactions.

But the Japanese are easier to figure out. The Japanese Government has created a quandary for their somewhat long-suffering citizens. The Japanese people are among the world's least willing to give up paper currency. Yet the Japanese central bank has joined the move to negative interest rates, meaning it is cheaper to bury currency in the back yard than to deposit yen in a bank - probably creating the world's largest concentration of overstuffed mattresses, and a collapse in the price of Japanese goose down. The Japanese Government is looking desperately for a reason its citizens might have for parting with currency.

Other issues are 1. Squabbling among the "miners" who run the computers that create new blockchains. 2. The question of competition for blockchain. Is there a better alternative to Bitcoin's blockchain? Should there be more than one blockchain?

Blockchain is not just a big honking spreadsheet. It has incredible potential. And, undoubtedly big possible problems. But it's certainly worth a long, close look.

**Disclosure:** I/we have no positions in any stocks mentioned, and no plans to initiate any positions within the next 72 hours.

I wrote this article myself, and it expresses my own opinions. I am not receiving compensation for it (other than from Seeking Alpha). I have no business relationship with any company whose stock is mentioned in this article.

---

**Comments (6)**

**Martin Lowy, Contributor**

Very well done, Kurt. I think I know about as much as you do about block chain--and friends ask me to explain block chain all the time--I can't! But I do get the potential.

Work with me, please. Why should there not be a "Ghost of Gold" that would be a global currency exchangeable at any time for any national or supranational currency? The amount of GoG would not be fixed, but it could grow not by techie miners finding more but by frugal nations earning the right to own more and thereby to distribute that to their frugal citizens?

The global currency would be stable, instantly exchangeable, and, by the nature of its architecture, could inhibit nations from managing their currencies or from running up debts in excess of their ability to repay.

The first issuance would be hotly contested. How much by population, how much by GDP etc? But it could
Kurt Dew, Contributor

Author’s reply »  Hi Martin,

As you’re undoubtedly aware, there are two schools of thought among the miners. The original idea was for a currency that was beyond government control. Someone intelligent, apparently we don’t know who, realized that if its value was within anybody’s control, it would be ultimately government controlled, or stopped. So Bitcoin, as it stands, is not value-controllable by anyone.

Your concept is of a collection of frugal nations. I look about me, and I don’t see any frugal nations that are capable of forming an agreement on something like the value of a currency that replaces theirs. There is, of course, the Euro, an exception that proves the rule.

My interest is in blockchain, although clearly the “miners” must have incentives to do their thing, so without some Bitcoin, or thing like Bitcoin, there is no blockchain. But I will focus on the applications that use the smallest possible amount of bitcoin, or some Bitcoin-like unit of account, for the purpose of facilitating transfers.

The transaction method seems to me possible for governments to support. I don’t think any government will support a commodity money. And I do believe without government support there is no chance of bringing this transaction method into being.

As I develop this topic, we can continue to talk.

29 Mar 2016, 05:47 PM

whidbey

This is wonderful, if too brief. Please keep writing.

29 Mar 2016, 05:42 PM

Kurt Dew, Contributor

Author’s reply »  Yep. Its going to take several articles.

29 Mar 2016, 05:57 PM

Sleepless in the Alps

Whew! You’re smart, Kurt!

We don't get it, but that’s OK. Can't see how the big banks will let anyone eat into their Forex trading, but you never know. Certainly some of the investment banks must be all up in blockchain tech as we speak (see Kurt Dew's comment section where 4 Swiss chicks describe the inner workings of Goldman...)
Anyway, enlighten us more...

Heidi and the Girls

PS: Clarissa thought "blockchain" had something to do with 50 Shades of Grey. We straightened her out.

29 Mar 2016, 06:18 PM

**Kurt Dew, Contributor**

Author's reply » Maybe you noticed. I don't get it either. But I'm trying.

The big banks are, they tell us, "spending billions" on blockchain. There is an interesting person, Blythe Masters, that once invented credit default swaps. She now is financed by the big banks to develop blockchain technology. Can you say "show pony?"

That Clarissa....

29 Mar 2016, 06:50 PM