Bitcoin Paranoia. Blockchain Baloney.

May 2, 2016 9:31 AM ET 30 comments
by: Kurt Dew

Summary

- I have been focusing on how blockchain works.
- The big banks are pouring billions into blockchain.
- This article focuses on the winners and losers.
- The consumer will win. The banks must cut costs very, very aggressively.

"Bad dreamer, what's your name?

Looks like we're ridin' on the same train.

Looks as though there'll be more pain.

There's gonna be a Showdown.”

- Electric Light Orchestra

This article addresses misperceptions growing around the newly celebrated fad in financial circles, blockchain. Bitcoin/blockchain is a technology with the potential to revolutionize transactions and perhaps even accounting. I will begin by putting front and center before you the most important thing to remember in understanding Bitcoin/blockchain.

There is only one blockchain, and Bitcoin is used in every single transaction on the only blockchain.

When you read almost any other discussion of Bitcoin or blockchain written for laymen, you will think that Bitcoin and blockchain are separable. They are not.
To explain: Blockchain and Bitcoin are components of a single transaction technology. Investopedia provides a surprisingly accurate definition of the pair:

"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." (Author's note: Even here there is spin. The misleading first word, "A" should be "The." Reading the definition carefully makes that clear, since only one blockchain-like thing uses Bitcoin.)

This article disputes much of what you have read or will read about blockchain. Disputing is needed. The big players, for example, have a hidden agenda that taints what their apologists say about the Bitcoin/blockchain technology, unintentionally in some cases, I believe.

The smaller advocates of Bitcoin/blockchain have other hidden agendas that color their writing too. One agenda is to distance oneself from Bitcoin's undeserved bad reputation. Another is to minimize reader awareness of the difficulties associated with getting Bitcoin/blockchain off the ground. This article will address these agendas, hoping to help to provide a sort of Rosetta Stone intended to partially clear the Bitcoin/blockchain fog.

**The technology of Bitcoin/blockchain has other implementations, most of them doomed to failure.** It is possible to use the methods of the Bitcoin/blockchain technology to imitate its properties in part. Since Bitcoin/blockchain is open source, there is no issue of patent infringement. But that is most likely because Bitcoin/blockchain has nothing to fear from competitors.

These imitative implementations are what all the reports of blockchain that omit mention of Bitcoin are talking about. If these other applications of the technology were called MacBlockchains or iBlockchains or eBlockchains, I would have no problem with them. But no. To remedy this oversight, I am going to pick a generic name for them, O'Blockchains, which I will use when I describe the genre going forward. (Irish ancestry, obviously.)

O'Blockchains, like the original, are all single, continuously updated public or private ledgers, with regularly added spreadsheets, called blocks, verified by multiple independent electronic auditors, called miners, who, as a group, approve each new block by consensus. Verification adds a block to the O'Blockchain, a single chain of blocks. Only one, Bitcoin/blockchain, uses Bitcoin.

In every public version of the O'Blockchain, the miners are compensated for their verification efforts by receipt of a cryptocurrency, like Bitcoin. Thankfully, these alternate cryptocurrencies have been separately named. No. 2 to Bitcoin in terms of use is called Ethereum. Ethereum claims to be "smarter" than Bitcoin. This is, if accurate, a logical and laudable improvement, and strengthens the parallel I have drawn elsewhere between Bitcoin/blockchain and IEX, the putative securities exchange that also threatens some of the bigs, and also threatens to make financial transactions more profitable for the rest of us. IEX is also introducing smart transactions.

**Why Does Bitcoin have a bad rap?** There are three reasons Bitcoin has a bad rap.

1. Bitcoin/blockchain is mysterious. It doesn't help that the bible of Bitcoin, (which like everything else about bitcoin is easily accessible on the internet - just google "bitcoin pdf") was written by a gentleman, Satoshi Nakamoto, who is apparently fictitious. The miners who verify blocks on the blockchain are also no one you've ever heard of, and apparently happily relatively unknown. And they are mostly located in Iceland - somewhere you've never been - because it has the globe's cheapest and most abundant energy.

2. One result of the Bitcoin/blockchain innovation is that Bitcoin, like any other means of payment, is also a store of value. Any role for the Bitcoin/blockchain technology as a transaction and record-keeping method is going to be hindered badly by the popularity of this alternative use. Bitcoin speculation that the world will tire of fiat money and rush to the Bitcoin alternative is hopelessly naïve. The governments that issue fiat currencies will not be amused by the presence of a currency alternative that has a supply in an amount that is not directly determined by government policy-makers. The way forward with government is cooperation.

3. Governments are also concerned by the ability to make payments on Bitcoin/blockchain in violation of federal money-laundering law. I await the government initiative to identify a method by which this could be avoided within the Bitcoin/blockchain system. I'm sure it will be forthcoming soon. That way we will know US
government regulators have an open mind about Bitcoin/blockchain, as the UK regulators, who seem blissfully unconcerned, do.

Will the O’Blockchains amount to anything? Probably not. The essential feature of Bitcoin/blockchain which makes it likely to be the one and only successful implementation of the technology is its near-biological tendency to propagate itself.

Its self-propagating feature is this: The system works by compensating a user of massive computer power to "prove" each new block added to the blockchain. This compensation, importantly, outstrips the value of a hacker attack of Bitcoin/blockchain by the same computer. The blockchain grows this way and new blocks get bigger as demand for Bitcoin/blockchain grows. Both forms of growth increase the demand for the independent miner's computer power.

Like any system, the potential likely exists to attack Bitcoin/blockchain and hack it. However, the fundamental resource applied by hackers, computer power, would have to be present, the experts report, with force greater than 300,000+ copies of the largest supercomputer in existence operating simultaneously. There are not close to 300,000 of these supercomputers now. But if they existed, these computers would successfully function if they had the uninterrupted full power of the sun's energy for 10 minutes. I think I'll worry about global warming or something instead.

Any smaller O'Blockchain must build from zero transactions. It therefore starts small and vulnerable to attack. But don't rule out alternatives such as Ethereum that actually improve on the underlying technology, if the competing system accepts the fundamental significance of open source to Bitcoin/blockchain’s success so it can grow like Topsy. Like the internet, there will be proprietary closed blockchain systems analogous to intranets. They will be small change, technologically. But there will be only one global game-changer. And that will most likely be Bitcoin/blockchain.

Everything that either explicitly denies or opposes Bitcoin's utility without proposing an alternative is a non-starter. And that includes almost everything I have seen proposed by major corporations so far. I discuss the single exception to date here.

Why the Rap Against Bitcoin for Facilitating Illegal Transactions is Rank Hypocrisy. Yes, illegal transfers are done using Bitcoin. But criminals have an overwhelming favorite when they smuggle, trade and evade taxes. Good old paper US dollars.
The $200 Million Haul from one of "El Chapo" Guzman's Arrests.

I first learned the most important use of US paper dollars listening to economist Milton Friedman tick off the relevant statistics at a lunch hosted by the San Francisco Fed. The theme of the Friedman discussion was that the primary use of all paper currencies is payment for illegal activities. But the star is US paper. One interesting evidence of this is that the largest denomination by bills in circulation for most currencies is what Friedman called "a day's wages," in the case of the US dollar, the $100 bill. Try paying for something at a retail store with a $100 bill. They won't accept them.

The following statistics are borrowed from a paper written by Campbell Harvey, "Bitcoin Myths and Facts." You can find it here. The $100 bill constitutes 73% of the outstanding value of US paper currency. Ever received one of those from an ATM? The average Bitcoin wallet contains $4000. My wallet has never contained that much.

If our government were really concerned about media of exchange used for illegal payments, they would be looking for a trustworthy digital version of cash. The possibility has been explored by the private sector without success.
The way forward in Bitcoin/blockchain for investors: The most important key to understanding future commercial success is clear. Bitcoin is open source. It depends in no way on trust, which is to say the fundamental service a bank has provided historically - a third party that provides trust - will be getting in the way. Bitcoin/blockchain will be commercially disastrous for commercial banks.

Here are the "tells" to identify baloney when assessing the value of any of the thousands of commercial projects announced by the banks like JPMorgan Chase (NYSE:JPM) and Goldman Sachs (NYSE:GS); the startups that the bigs have invested billions supporting; the non-bank investor-funded startups; the projects announced by the big IT firms such as IBM (NYSE:IBM), Microsoft (NASDAQ:MSFT) and Google (NASDAQ:GOOGL) (NASDAQ:GOOG); and the internal projects announced by exchanges such as NASDAQ (NASDAQ:NDAQ) and the Australian Stock Exchange.

If they avoid the use of the name Bitcoin (or worse, dump on it), the project is a no-go. If the use of blockchain is internal, never reaching an open source transaction engine, forget it.

The winners will be gateways - Apps to get to the open source host, or perform functions the open source technology enables. And like their cousins on the internet, they will mostly be free.

So while investors, in particular, and ordinary users of financial services, in general, are going to benefit enormously from Bitcoin/blockchain, relying on a supportive UK regulatory establishment, for retail investors it's a different story. The retail investor profit opportunities from this technology will very likely follow the path of the internet users, like Amazon (NASDAQ:AMZN) and Facebook (NASDAQ:FB). In other words, the creators get rich before the rest of us get in.

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 (30)

wamban
This article misses a very important point: the blockchain is entirely separable from Bitcoin. See this article here (http://bit.ly/1Ob6Jhk), where permissioned ledgers are discussed. Any cryptographically secure system employing one-way hashing and other characteristics of the Bitcoin framework can be considered a blockchain. Think of use cases among a consortium of big players - ranging from medicine to banking to real estate, and so on. Many blockchain systems existing independently of each other.

02 May 2016, 11:51 AM

Kurt Dew, Contributor
Author’s reply » I enjoyed reading the link. It did exactly what I wish other sources would do. It did not use the word blockchain to describe the generic product. It characterized the various alternatives using generic descriptions. Each O'blockchain has its own O'crypto-currency. Bitcoin's version of blockchain has a major head start.

I have made a business judgement in the article. One or at most two, O'blockchains will survive the effects of user selection. I like Bitcoin's chances but I have not ruled out Ethereum. I am aware of the facts you describe.

02 May 2016, 12:03 PM

Kurt Dew, Contributor
Author’s reply » There is a error in this piece I would like to correct. The sentence that describes how much cash is held by individuals states: "The average bitcoin wallet contains $4000." Not sure how "bitcoin" sneaked into that sentence. The actual statistic behind the remark is that there are cash dollars outstanding of about $4000 for every man, woman, and child in the US. I believe this does no damage to the point: Most US $ are held for illegal purposes.

02 May 2016, 12:11 PM

Momintn
Blockchain does not depend on the use of bitcoin. Ledgers can be maintained in any currency. It's simply a matter of who owns what and everyone having the same ledger that is secure and accurate.
IBM insists that its cloud is the best place to do this. Here are some links.
http://ibm.co/1rr39eq play video at bottom
http://ibm.co/1ObgbRR

02 May 2016, 12:21 PM

Kurt Dew, Contributor
Author’s reply » I anticipated this semantic issue.

Yes, other ledgers can be maintained in other crypto-currencies.

Also in the Bitcoin/blockchain implementation, the transactions of interest can be in any currency. The one I discuss elsewhere is
Circle/Barclay's Bitcoin/blockchain implementation of a system of transfer of UK sterling for Euros. But a tiny fraction of Bitcoin is part of those trades.

I am partially aware of what IBM is doing and in touch with IBM representatives. They have indicated that they have a cloud but have not yet tried to persuade me that it is the best place to do transactions. That persuasion will be challenging.

02 May 2016, 12:45 PM

Momintn
IBM said two of its customers, London Stock Exchange Group PLC and Japan Exchange Group Inc. are now exploring ways of using the blockchain code in their businesses.
Good article here: http://on.wsj.com/1OboWeW
Can also run on the IBM mainframe.

02 May 2016, 12:58 PM

Kurt Dew, Contributor
Author’s reply » Thanks, Momintn. I look forward to hearing the full story from them.

02 May 2016, 01:05 PM

The cave
Lots of misunderstandings in this article. The use of 'consensus' as an 'acceptance' mechanism in exchange of some 'value', is the method the bit coin uses. Once can implement any other method. E.g. having a supervision entity that checks all the transactions. This is what we have now in the financial system (central banks, etc.) and it takes like three days to do an international transfers and double check that everybody is on the same page. What if the transactions (the ledger) are automatically shared among all the participants? This technology will be disruptive, like micro trading... it tooks some time to do stock transactions and now we can do thousands of them in few milliseconds. ...

02 May 2016, 12:37 PM

Kurt Dew, Contributor
Author's reply » Cave,
Thanks for your remarks.

02 May 2016, 12:47 PM

User354
Any opinion on stock symbol: BTCS

02 May 2016, 08:13 PM

Kurt Dew, Contributor
Author’s reply » No. I am not a fan of Bitcoin as an investment.

02 May 2016, 08:33 PM

hawkeyec
You have no choice. Any transaction medium is, by definition, also an investment. If Bitcoin is really a store of value, albeit an unstable one, it is also an investment. If you have it in your wallet, you are an investor. As the value on a unit of Bitcoin IS unstable it will not be a very popular one to hold. There are not many "laws" in economics that seem to be true over time. One of them that does is Gresham’s Law which states: "Bad money drives out good." When someone gets a Canadian quarter in their change, what's the first coin they will spend? People won't keep or store value in money which is somehow flawed. That big block of c-notes is a popular mechanism because regardless of your politics or other factors, I can give one of those notes to anyone, anywhere and it will probably be accepted. It can be parked in a box in my garage and it will still be good ten years from now. 100 will still be 100. What will a Bitcoin be in ten years?

03 May 2016, 11:12 AM

Kurt Dew, Contributor
Author’s reply » Graham's law will apply to me. I will hold the minimum amount necessary to facilitate transactions. It cannot be zero, as you suggest, or the miners don't get compensated for their "proof of work." Luckily for the rest of us, there seems to be a substantial interest in buying and holding bitcoin. Not for me.

03 May 2016, 11:21 AM
User354
More than bitcoin. Check out their web site. BTCS Inc. ("BTCS") is an early mover in the blockchain and digital currency ecosystems and the first "Pure Play" U.S. public company focused on blockchain technologies. They've launched an ethereum platform and acquired Spondoolies.

04 May 2016, 10:43 AM

Kurt Dew, Contributor
Author's reply » Thanks! I'll check it out.

04 May 2016, 11:09 AM

Kurt Dew, Contributor
Author's reply » Read through p 12 so far. I really appreciated the balanced, brief, explanation of the relationship between BitBlock and other means of payment. The history might be expanded to include hawala. This is a transactions technology older than banking -- yet open source, distributed, and trust is created not by customers but by relationships among hawaladirs (bank-like-entities). Motionless. Your money never moves. Speed is as fast a an email. Very low commissions. Also has a bad rap. Mostly used in the Near East, India, and United States.

05 May 2016, 11:37 AM

User354
Thanks Kurt

05 May 2016, 12:15 PM

ghiblinewt
"It doesn't help that the bible of Bitcoin, (which like everything else about bitcoin is easily accessible on the internet - just google " bitcoin pdf".) was written by a gentleman, Satoshi Nakamoto, who is apparently fictitious."
Looks like the real "Mr Nakamoto" has outed himself.
"Craig Steven Wright, an Australian entrepreneur, identified himself as the creator of bitcoin almost five months after he was outed in media
reports as the man behind the virtual currency. Wright said in a blog post and interviews with three media organizations that he developed the original bitcoin software under the pseudonym Satoshi Nakamoto, a claim that's been disputed by others. Wright provided technical evidence, including the original encryption keys, that have been confirmed by prominent members of the bitcoin community, the BBC reported.

http://bloom.bg/1NiQ6Wg

03 May 2016, 02:39 AM

Kurt Dew, Contributor
Author's reply » I saw that report the morning that I posted this. The world of BitBlock does not seek notoriety, does it?

03 May 2016, 06:31 AM

petguy55
Wonder if bitcoin can back it's "currency" with gold or silver....why not? Other startups have done this to protect the baseline. Validates the systems and protect further from paper currency

03 May 2016, 10:20 AM

Kurt Dew, Contributor
Author's reply » There seems to be no interest among the miners in this possibility. Maybe they don't want to hold gold as a reward for their efforts.

03 May 2016, 11:24 AM

tucsonjji must be naive... what the heck is the value of bitcoin? What is it based on? Always sounded like a tulip bulb scam or a ponzi deal to me...

03 May 2016, 10:45 AM

Kurt Dew, Contributor
Author's reply » As a store of value, it is a disaster. Its price is very volatile. It has a positive value because it represents the work effort
of the miners who validate BitBlock transactions.

All crypto-currencies are, like fiat money, ultimately backed by the willingness of individuals to hold them. The same is true of anything of value.

The practical use of bitcoin is that a very small amount of it (the default amount is 0.0005 bitcoins but amounts vary) is necessary to compensate the miners for confirming a transaction. So you could send Euros to France for US $ (in theory) in about 10 minutes with a 0.00005 Bitcoin transaction fee. Barclays intends to make sterling for $ transactions to New York State practical in the near future.

03 May 2016, 11:17 AM

millionairemile
Hi Kurt,

I love your read-through: " As a store of value, it is a disaster. Its price is very volatile."

As investors, major volatility is seldom embraced. I'll have my fiat currency in good old US dollars, thanks.

Thanks for the article. Hope things are going well.

04 May 2016, 10:40 AM

Kurt Dew, Contributor
Author's reply » Thanks millionairemile. These pesos are killing me! I really need Bitcoin to double the trouble.

04 May 2016, 11:12 AM

minorman
Dear Kort Dew,

Many thanks for providing one of the precious few essentially accurate articles on Bitcoin on SeekingAlpha. One minor correction - the minors are NOT mostly based in Iceland. They are, in fact, mostly based in China, which, incidentally, is one of Bitcoin's biggest current problems and arguably holding Bitcoin back. (Blocksize/scaling controversy)

Around new-year, I wrote about this in my recurring annual status of Bitcoin (best currency in 2015):

http://bit.ly/1rtijQg
Kurt Dew, Contributor
Author's reply » First, thanks. I am learning a great deal from the comments to this article.

I write mostly on my gut, but I do my reading. I do try to show the reader what is gut and what I read.

The Iceland remark was tongue in cheek. I think, however, most of the computers are located there because of the cheap thermal power.

Bitcoin is an enormous topic, and I have merely scratched the surface. You bring up China and the bitcoin folk there. China has been supportive of bitcoin which I find counter-intuitive in an authoritarian regime. Putin apparently thinks Bitcoin is the scourge of God.

My purpose in this article is to nudge what I find to be a little fear of the bitcoin boogyman, on one hand. And second to suggest that the powers that be may be spending billions pointlessly. But being a power that IS means not having to say you're sorry when you waste billions.

There is a fundamental issue that bitcoin raises. In the age of hacking, are trust-based systems even economically viable? I don't think so. So I think something like BitBlock is inevitable.

My guess is, the smart systems like Ethereum will function as a Bitcoin sideline, because greater simplicity is better in enormous things, but the reality is above my IT IQ.

03 May 2016, 11:47 AM

Steven Quint, Contributor
Bitcoin will fail because the currency is deflationary. People are hoarding it rather than spending. No government in the world can allow a deflationary currency to exist en masse and compete with their fiat. It is too threatening.

I know people think about the evils of governments and inflation. The truth is that we'd all be slaves to our forebears' mistakes if it were not for currency debasement. Inflation is the way we disrupt the old regimes.

If a deflationary currency ever came about (again), people would attempt to make money by simply hoarding money. It causes it's own crash.
minorman
Ah - the old "deflation is bad" argument...
Well at least, you agree with Krugman
http://seekingalpha.co...
- even though the argument put forward is wrong in my opinion.

04 May 2016, 08:26 AM

Kurt Dew, Contributor
Author’s reply » I think the real issue with Bitcoin is the danger that the miners lose incentive to continue their function.

04 May 2016, 08:41 AM