



Become a Client (<http://info.constellationr.com/become-a-client>)

(L)

# Bearish on the Blockchain: Six Counterpoints and Cautions from Constellation VP and Principal Analyst Steve Wilson

Analyst: [Chris Kanaracus \(/users/chris-kanaracus\)](/users/chris-kanaracus) on November 17, 2015

[Twitter](http://twitter.com/share?text=Bearish+on+the+Blockchain%3A+Six+Counterpoints+and+Cautions+from+Constellation+VP+and+Principal+Analyst+Steve+Wilson+via+%40ConstellationRG+&url=https://www.constellationr.com/content/bearish-blockchain-six-counterpoints-and-cautions-constellation-vp-and-principal-analyst) ([http://twitter.com/share?text=Bearish on the Blockchain: Six Counterpoints and Cautions from Constellation VP and Principal Analyst Steve Wilson via @ConstellationRG &url=https://www.constellationr.com/content/bearish-blockchain-six-counterpoints-and-cautions-constellation-vp-and-principal-analyst](http://twitter.com/share?text=Bearish+on+the+Blockchain%3A+Six+Counterpoints+and+Cautions+from+Constellation+VP+and+Principal+Analyst+Steve+Wilson+via+%40ConstellationRG+&url=https://www.constellationr.com/content/bearish-blockchain-six-counterpoints-and-cautions-constellation-vp-and-principal-analyst)) [Facebook](http://www.facebook.com/sharer.php?u=https://www.constellationr.com/content/bearish-blockchain-six-counterpoints-and-cautions-constellation-vp-and-principal-analyst) (<http://www.facebook.com/sharer.php?u=https://www.constellationr.com/content/bearish-blockchain-six-counterpoints-and-cautions-constellation-vp-and-principal-analyst>)



Public access to this Insight will expire in 11 days. [For complete access to Insights, become a member today.](http://info.constellationr.com/insights-waitlist) (<http://info.constellationr.com/insights-waitlist>)



The news cycle **has become saturated** ([https://www.google.com/search?q=blockchain&oq=block&aqs=chrome.0.69i59j69i57j0j69i60j0l2.1311j0j7&sourceid=chrome&es\\_sm=91&ie=UTF-8#q=blockchain&tbm=nws](https://www.google.com/search?q=blockchain&oq=block&aqs=chrome.0.69i59j69i57j0j69i60j0l2.1311j0j7&sourceid=chrome&es_sm=91&ie=UTF-8#q=blockchain&tbm=nws)) with stories on “the blockchain,” a new distributed database or ledger technology, invented to underpin the Bitcoin digital currency. Governments, Wall Street and dozens if not hundreds of startups view the blockchain as having potential to transform the financial services industry, and way beyond.

Constellation Research VP and Principal Analyst [Steve Wilson \(https://www.constellationr.com/users/steve-wilson\)](https://www.constellationr.com/users/steve-wilson) isn’t so sure. “Like a lot of these things, it’s the first example of something that solves an impossible problem,” he says. “Blockchain is not even good for what it’s designed to do. It’s not even the model T Ford of electronic cash.”

But where Wilson starts to get really concerned is when the blockchain is held up as a cure for other vexing problems, namely identity.

“The blockchain and Bitcoin has inspired people to think about trusted identity,” Wilson says. “But there are very few identity experts buying into this. People should know better than to talk up cryptographic technology as some magic recipe for trust.”

“On the positive side, there’s a great deal of innovation happening [with blockchain], whether behind closed doors or in these research consortia,” Wilson said. “But you’re just not going to produce global trust with it, like the [front page of the Economist \(http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine\)](http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine) says.”

It’s time for the industry to temper its exuberance for the blockchain as a panacea for trusted identity, says Wilson, who offers six arguments for such caution.

## History: It Tends to Repeat Itself

“Throughout the 1990s and early 2000s, a string of hopeful businesses were started up around the promise of ‘trust’ being created by a special technology called Public Key Infrastructure,” Wilson says. “Many companies even had the hubris to put ‘trust’ in their name. We learned then that technology in and of itself does not beget trust. The enthusiasm for blockchain for trust is ignoring history.”

## Bringing a Knife to A Gunfight

“The blockchain is a special form of decentralised digital ledger, invented for a particular cryptocurrency,” Wilson says. “Specifically, the blockchain is to prevent double spend of electronic cash. Blockchain was not invented for identity or trust, and it’s not even a very good solution for digital money. It’s incredibly expensive, and slow, taking 10 minutes to finalize a transaction, and with a maximum global throughput of three or four transactions per second.”

## A Question of Scale

“It’s hard to scale the blockchain down to private or application-specific use cases,” Wilson says. “The ‘proof of work’ required to vote on the order in which things are added to the chain, and the resulting certainty in the truth of the ordering, is proportional to the size of the peer-to-peer network. People talk casually of ‘blockchain technologies’ being spun off the [Bitcoin] blockchain to cater for non-currency applications, but the economics of private proof-of-work hasn’t been worked out yet.”

“Note how the advocates first loved Bitcoin,” he adds. “And then they earnestly said, ‘actually it’s not about Bitcoin but rather it’s about the blockchain.’ And now they say kind of slyly, ‘it’s not about the the blockchain but rather it’s about blockchain technology.’ The story is evolving faster than the proven use cases. It’s just too speculative. And the further they shift the focus, the less precise they get.”

**Take Off the Rose-Colored Glasses**

“It’s utopian to think you can decentralize all aspects of ‘trust,’ Wilson says. “The drive to do so is often based on nothing more than a distaste for hierarchies. But hierarchies in business are inevitable, and good for everyone, because they provide clarity and accountability. Look at the [Honduras land title blockchain application \(http://in.reuters.com/article/2015/05/15/usa-honduras-technology-idINKBN0O01V720150515\)](http://in.reuters.com/article/2015/05/15/usa-honduras-technology-idINKBN0O01V720150515), said to eliminate corruption. How’s that? If the digital ledger containing the land titles is inviolable, so what? Nothing stops fake or ill-gotten titles being written onto the blockchain. No technology on its own is ever going to stop fraud.”

**The ‘Perfect’ Argument Doesn’t Add Up**

“People talk of ‘math-based currency’ as being perfect, but they forget the steps that go from math to real world systems,” Wilson says. "Good mathematics is necessary but not sufficient for good implementations. In reality, Bitcoin’s security rests on the assumption that no one can control the peer-to-peer network. There have been times when giant bitcoin mining conglomerates have challenged that assumption, and there may be more subtle scenarios where the competing temporary chains can be gamed to delay or corrupt the consensus process.”

**Finally—Open Source Does Not Equal Utopia**

“The blockchain code is maintained by an open source community which struggles to agree on design decisions,” Wilson says. “We have seen spectacular security failures in open source software recently, like the [Heartbleed bug \(https://www.constellationr.com/content/security-heartache\)](https://www.constellationr.com/content/security-heartache) which rendered SSL security leaky on all Apache servers. The fault was a simple buffer overrun error, which had existed in the open source code for nearly two years before it was noticed by white hats and fixed. Can anyone guarantee that the blockchain software is in better shape—now and into the future—than the Open SSL libraries?”

**Business Research Theme:**

[Tech Optimization & Innovation \(/business-theme/tech-optimization-innovation\)](/business-theme/tech-optimization-innovation), [Safety and Privacy \(/business-theme/safety-and-privacy\)](/business-theme/safety-and-privacy), [Data to Decisions \(/business-theme/data-decisions\)](/business-theme/data-decisions), [Matrix Commerce \(/business-theme/matrix-commerce\)](/business-theme/matrix-commerce)

**Research Role:**

[Chief Information Officer \(/taxonomy/term/15\)](/taxonomy/term/15), [Chief Digital Officer \(/roles/chief-digital-officer-0\)](/roles/chief-digital-officer-0), [Chief Customer Officer \(/taxonomy/term/11\)](/taxonomy/term/11)