



The Bitcoin Hype Has Been Spent, So What's Next?

It may be the case that the cryptocurrency is most valuable as a development platform for other products – products that could ultimately revolutionize the ways we think about and handle data.

By **Frederick Reese**

@FrederickReese | November 24, 2014



(Antana / Flickr)

The U.S. Marshals Service announced last Monday that it will be auctioning off 50,000 of the bitcoins it seized from the accounts of Ross William Ulbricht. Ulbricht, who operated under the pseudonym the Dread Pirate Roberts, allegedly operated the first iteration of Silk Road, the online marketplace accessible only through Tor that sold drugs, weapons and other illicit paraphernalia.

The 50,000 bitcoins are part of the total 114,000 bitcoins the Marshals seized from Ulbricht's computers. The first auction of 30,000 bitcoins was held in June.

This announcement marked the end of a tumultuous year for the bitcoin, which saw its value fall by more than two-thirds of its December 2013 high and the arrest of the alleged head of Silk Road 2.0 by federal authorities.

This year also saw the cryptocurrency's largest exchange close, with nearly half a billion dollars worth of bitcoins vanishing; the bitcoin's underlying technology – the blockchain – attacked with a foreseeable exploit; several world governments decertifying or even banning the use of cryptocurrencies; and the U.S government ruling cryptocurrencies as commodities, subject to capital gains taxes.

As the hype and craze over the new value model starts to wear off, the future of the bitcoin is murky. With some noted economists suggesting that the bitcoin's stable value may be in the double or single digits, and with the programmed difficulty for mining bitcoins continuing to rise, there is a sense that the market may grow exhausted of the bitcoin.

Sign up for our Daily Newsletter

SUBSCRIBE

MyMPN



How I Was Censored By The Guardian For Writing About Israel's War For Gaza's Gas

About the



Frederick Reese

Frederick Reese is lead staff writer for Mint Press specializing in race, poverty, congressional oversight and technology. An award winning data journalist and creative writer for over 15 years, Frederick has written about and worked for social advocacy projects and personal awareness efforts. Frederick is a jack-of-all-trades, with work experience as a teacher, a pastry chef and a story writer. Frederick has publication credits with Yahoo!, B. Couleur, and more. A native New Yorker, Frederick graduated from Colgate University in 1999 and Johnson & Wales University in 2003. Frederick started his journalistic career writing for his university's newspaper, "The Colgate Maroon-News," before starting and heading his own magazine, "The Idealist." Most recently, Frederick received a data journalism award from the International Center for Journalists for his minimum wage coverage for MintPress. Follow Frederick on Twitter: @frederickreese

"I don't believe that the bitcoin has a chance to be a viable currency," said Josh Garza, chief executive of GAW Miners, a cryptocurrency mining equipment retailer and consultancy. "One of the big confusions behind the bitcoin is that the great thing about the bitcoin is not the brand or the coin itself, but the technology behind it. It's the blockchain that makes bitcoins great.

"There will never be a time that a normal consumer will be okay logging into their bank account and seeing a different amount in their account than the day before without spending any money. The viability of the bitcoin will never make the virtual currency palatable to the average American, when other platforms, such as PayPal, offers what bitcoins offer without the value fluctuations. Once the hype dissipates, the impracticality of the bitcoin will doom the cryptocurrency. But the blockchain will remain; it's the future of how value will be recorded and shared."

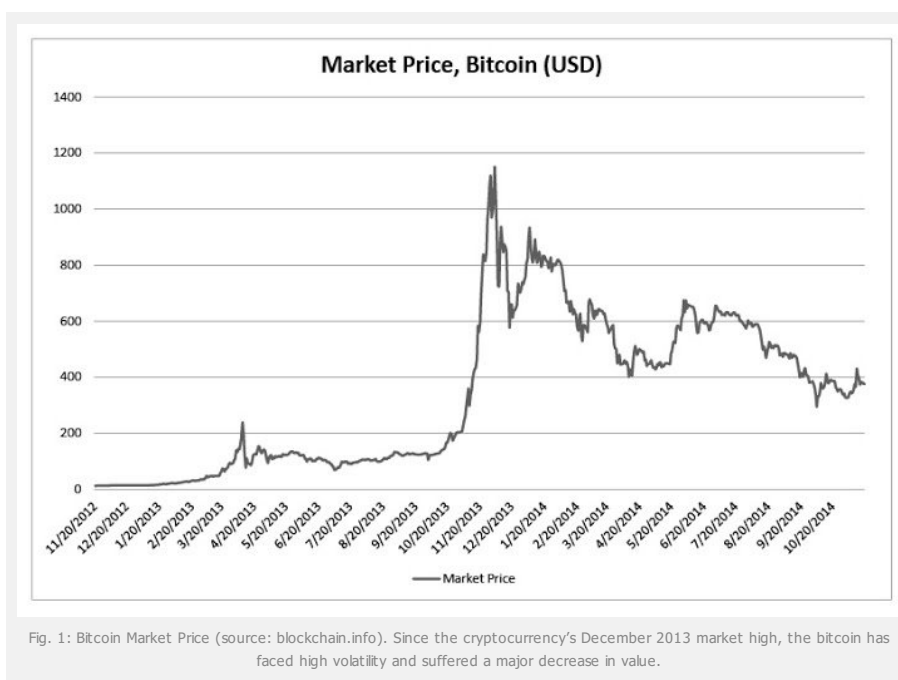
Understanding the blockchain

A blockchain is the sequential database that records transactions for a cryptocurrency. As it is distributed openly through a peer-to-peer network, with no single entity controlling or owning it, it is a truly public record of assets and debts. All mined cryptocurrencies are recorded to their respective blockchains, as are all transfers and sales. Fraud, in theory, can be easily rooted out by comparing one version of the blockchain to others.

This type of system makes it considerably easier to create a trackable, easily-accountable virtual currency system. With bank-based systems, such as PayPal, transaction logs are not publicly-accessible, forcing the consumer to rely on the bank's word to ensure that his or her funds are safe and transactions will be honored. In a blockchain system, however, a chain of cryptographic proofs ensures the integrity of the blockchain's data, which can be reviewed publicly. The proof chain reflects the amount of computational work needed to construct it; all the cryptocurrency's network has to do to verify a blockchain is to find the blockchain with the longest proof chain. This would be the chain that was worked on the most and is therefore the most accurate.

The blockchain technology potentially offers a new way to authenticate not only financial transactions, but all types of data- and record-keeping. Last Monday, Fathom, a cryptocurrency manufacturer, [released a whitepaper](#) suggesting a methodology for creating a new architecture that would both secure and make trackable large record databases without the drain on processing power that occurs from processing an overaccumulation of data.

The proposed system would assign a Merkle root — a unique hashcode which represents the processing needed to verify the record — that would then be added to a blockchain. According to the authors of the whitepaper, this approach limits the searchable item in a major database to a single token, making it easier and less resource-intensive than a typical database search. Additionally, the blockchain's peer-to-peer cumulative processing power simplifies the archival processes needed to manage large accumulations of data.



1 writer: @frederickreese

Recent Articles by Frederick Reese

- [GOP Needs To Clear Net Neutrality, Immigration Reform Hurdles On The Way To 2016](#)
- [2014 Elections Paint Gruesome Future For Republican Party](#)
- [The Fate Of Net Neutrality: A Complicated Dance Between Corporate Interests And Consumer Demand](#)
- [Racism And Unchecked Police Violence: An American Epidemic](#)
- [Race And Racism Define Southern Politics, But Maybe Not For Long](#)

Related Stories on Mint Press



Phoenix Police Ignite Outcry After Shooting Unarmed Black Man

Systemic Injustice Condemned As Ferguson Galvanizes National Outrage

How To Deal With Friends' Racist Reactions To Ferguson

Racial Gap In U.S. Arrest Rates Show 'Staggering Disparity'

Harvard University And UNC Chapel Hill Being Sued Over Affirmative Action Policies

UC Berkeley Students Petition To Get Bill Maher Speech Canceled Because He's A "Blatant Bigot"

Racism And Unchecked Police Violence: An American Epidemic

VIDEO: LAPD Detain Black Actress For Kissing White Boyfriend In Public, Suspecting Her Of Prostitution

Daily Digest

Egypt Security Forces Disperse Anti-Mubarak Rallies After Closing Tahrir Square



Rethinking how data is handled

An example cited by the whitepaper is the mortgage claim crisis of 2008. In the aftermath of the banking collapse of 2007, paper-based titles were mishandled or lost, causing a number of incorrect foreclosures. Additionally, because the mishandling of the paperwork effectively broke the chain of title, many homeowners are still coping with legal ambiguity.

During a Reddit Ask Me Anything session last week, [Factom President Peter Kirby explained](#):

Making exchanges honest is one of the first projects that's being done on Factom. You can run a proof-of-audit on steroids – letting you produce a true audit trail of every transaction at every moment. That'll really get businesses to sit up and notice.

The other application that will pop up right away is title records – because they secure such a large portion of a country's wealth. ...

Big companies like Bank of America and BP have been fined \$10's of billions for losing track of their systems of record. So you'll see a lot of fast movement in the opportunity to move mortgage and energy systems onto Factom.

Lots of interesting things being built on Factom – my guess is the first ones will be the simple options that solve a lot of pain.

The Factom model would create “sidechains” or “entry chains” that would anchor themselves into the bitcoin blockchain. Each of these “entry chains” would be composed of “entry blocks” — directories linked to the metadata for the records or data they are meant to archive. As these “entry blocks” and “entry chains” would be cryptographically signed, they would inherit the security of the bitcoin blockchain itself.

Such a system would be immediately auditable and traceable, which would, theoretically, create a fully transparent data structure. Such a system could create, for example, a voting system in which every vote can be accounted for, a government accountability system that can track all monies spent, or a unified accounting system that can allow for departments and independent systems to join or leave with ease.

“The dream of many is to extend the honesty inherent to an immutable ledger validated by math to chaotic, real-world interactions,” the whitepaper reads. “By allowing the construction of unbounded ledgers backed by the blockchain, Factom extends the benefits of the blockchain to the real world.”

The viability of the bitcoin

Many developers and technologists believe that the future of the bitcoin lies in serving as a development platform for other products, not necessarily as a viable commodity on its own. A large part of this speculation is bolstered by recent news regarding major bitcoin seizures.

Marcus Asner is a partner with the law firm Arnold & Porter LLP. He is also the former chief of the Major Crimes Unit (now known as the Complex Fraud Unit) for the U.S. Attorney's Office for the Southern District of New York. Speaking with MintPress, Asner pointed out that one of the bitcoin's major selling points — its anonymity in use, which made it attractive to libertarian- and anti-government intervention-minded individuals — has been proven to be a fallacy.

“My take on the situation is that law enforcement is getting better and better at tracking bitcoin use,” Asner said. “It's to the point that, if I was a criminal, I would seriously reconsider using bitcoins for my crimes. The bitcoin has become so traceable; the one thing that was particularly compelling about the recent arrests that they were able to figure out who the criminals were, even though they used Tumblr.”

Asner pointed out that, similar to emails — which, at one time, were also thought to be anonymous — the myth of anonymity for the bitcoin was broken by a need to investigate and prosecute computer crimes. While this newly-discovered transparency is applauded by the mainstream bitcoin community as a needed assurance of the cryptocurrency's legitimacy, it is also an engine for the deflation of the bitcoin's hype.

With the volatility of the bitcoin market, the capital gains tax imposed on the shift in values, the cumbersome recording requirements imposed by the Internal Revenue Service, the lack of full international support of the virtual currency, and the fact that there are nearly 550 other cryptocurrencies competing with the bitcoin, it's difficult to say whether the bitcoin can survive or even forecast what form it may take in the future.

California Drought Worst in 1,200 Years: Study



Rolling Stone, Journalistic Integrity, And The Fight Against Campus Rape



Inside, And Kicked Out Of, ALEC's Secretive Policy Summit



VIDEO: Low-Wage Workers Retake National Stage in 'Fight for 15'



Obama Ready To Defy Base In Order To Advance Trans-Pacific Partnership



Israeli Forces Shoot Palestinian Cameraman In West Bank As Settler Violence Continues



VIDEO: NYPD Police Union Blames Eric Garner For His Own Death



Follow

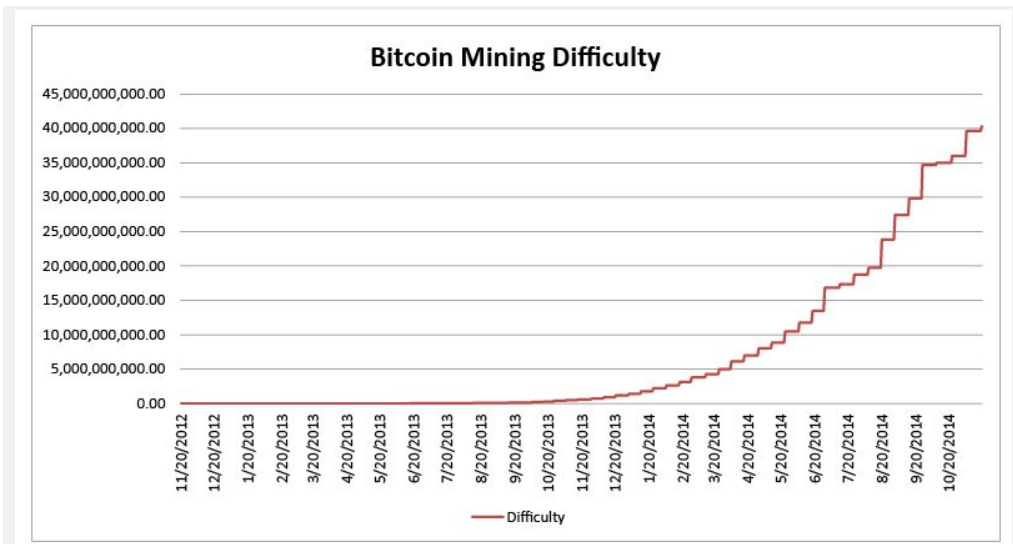


Fig. 2: Bitcoin Mining Difficulty (source: blockchain.info). As the value of the bitcoin drops, the programmed difficulty in finding new bitcoin blocks and the additional investment in processing power to overcome this increased difficulty may prove fatal toward the mining of new bitcoins and the expansion of the market cap.

“It wouldn’t be the least bit surprising to see the best bits of Bitcoin be grafted into new products and services (like facilitating international transfers),” said David Yermack, professor of finance at New York University Stern School of Business, [to CNN](#).

“A lot of the breakthrough products tend to get taken over pretty quickly by improved versions and I think that’s likely going to be the fate of Bitcoin. It’s certainly played a role in raising issues and opening possibilities that people were only dimly aware of before. But if I owned Bitcoins, I would be a seller at the current market price as I think a year from now they may be all but worthless.”

While most analysts believe that bitcoin’s risk will eventually be factored into the cryptocurrency’s selling price — which would reduce the volatility — it may be that the true worth of the bitcoin is to show the flaws in the cryptocurrency model toward the development of a more secure, more stable product. While bitcoin’s existence in the near-future is secure, as the cryptocurrency’s blockchain is the first of its class and sets the industry standard for stability, the future of cryptocurrencies and cryptographically-signed data archiving suggests that the way the world deals with and understands data is bound to change in interesting and revolutionary ways.

“With any financial system, you are going to have these hiccups and flaws, regardless of the mechanism you use to transfer money,” Asner pointed out. “But these flaws are not necessarily fatal to the blockchain, as the idea is fundamentally sound.”

Share this article!



[Print This Story](#)

This entry was posted in [Inside Stories](#), [National](#), [Top Stories](#) and tagged [Arnold & Porter LLP](#), [bitcoin](#), [commodities](#), [cryptocurrency](#), [currency](#), [David Yermack](#), [digital currency](#), [encryption](#), [Factom](#), [Marcus Asner](#), [New York](#), [Peter Kirby](#), [Silk Road](#), [tech](#), [Technology](#), [Tor](#). Bookmark the [permalink](#).

← VIDEO: Citizen Journalist Bassem Masri Tells CNN Why Free Speech Matters In Ferguson



Worldwide, Tobacco Regulators Monitoring Philip Morris Lawsuit Against Uruguay →



What's HOT on MPN

Charges Dropped For Cop Who Fatally Shot Sleeping 7-Year-Old Girl

US Police Have Killed Over 5,000 Civilians Since 9/11

The Christian Terrorist Movement No One Wants To Talk About

How I Was Censored By The Guardian For Writing About Israel's War For Gaza's Gas

EDITOR'S PICKS

- How I Was Censored By The Guardian For Writing About Israel's War For Gaza's Gas
- Ferguson Reveals Racists In Libertarian Clothing
- USAID: An Imperialist Snare Under The Guise Of Humanitarian Aid
- US Has "Much Left To Do" On Racism: Segregation Worse Now Than In 70s
- Myth Vs. Fact: Breaking Down The Conflict In Gaza
- VIDEO: Is The Crisis In Gaza A Reflection Of Apartheid? Interview With Miko Peled
- VIDEO: Bolivia Declares Israel "Terrorist State", UN Condemns Civilian Deaths
- Leaks: EU Wants "Free Access" To US Fossil Fuels, Lift Ban On Oil Exports In TTIP Agreement
- The Crisis In Gaza, A MintPress Exclusive Timeline and Whitepaper
- What The Media's Getting Wrong About Israel And Palestine -- And Why It Matters

[About Us](#) [Contact Us](#) [Careers & Internships](#) [Terms of Use](#) [Privacy Policy](#) [Archives](#)

