DLG FEATURED ARTICLE

A HUMAN RIGHTS ACTIVIST'S RESPONSE TO BITCOIN CRITICS

Alex Gladstein Feb 19 2019

Bitcoin: a tool of freedom and human rights.

Foreign Policy recently published the latest mainstream media attack on Bitcoin from the London-based author and journalist David Gerard. Gerard's "Forget Bitcoin, Try your Mattress" is the newest in a long line of Bitcoin criticism published everywhere from the Financial Times to The Washington Post. This time, Bitcoin is part of a system "plagued by hacks, fraud, and social engineering." Doesn't sound very appealing, does it? Why, might you ask, would a human rights activist like me be interested in something so universally derided by experts and the world establishment?

This response is my answer. If you read along, we'll cover where the critics are right; why Bitcoin is secure and safe; how it does things that we can't do with our existing financial system; how it will scale and improve; why its monetary system is an improvement for many; why it's not a waste of energy; why

progressives and libertarians should both be fans; why it matters for human rights; how we are at just the beginning of the Bitcoin journey; and why now is the best time to learn more and get involved.

This essay is written from the point of view of someone who believes that mainstream Bitcoin critics don't actually understand how it works (meaning: haven't done their homework and couldn't pass a basic quiz on topics like mining, wallets, or nodes) and are fulfilling the historical role of skeptics of a new technology early in its life cycle. There are two main varieties of Bitcoin critics: establishmentarians like Martin Wolf who write from a place of fear, who don't want to see the existing financial system disrupted; and progressives like Gerard who write from a place of disbelief, who don't believe decentralized money (Bitcoin) could actually improve the world just like decentralized government (democracy) and decentralized knowledge (the Internet).

Bitcoin critics do get many things right, as Gerard does in his Foreign Policy article. Too many actors in the cryptocurrency and blockchain space are actually charlatans or thieves; there is a huge amount of snake oil and hype; and many crypto exchanges are unsafe and wind up being hacked. The sad reality is that with the exception of a few valuable efforts like Monero, ZCash, and MakerDAO (whose teams and core values and driving missions of private money and censorship-resistant stable assets are critical even if they fail), most crypto projects are either intentional scams, unexciting modifications to existing technology, or wolves in sheep's clothing — centralized systems which pretend to be decentralized but still have backdoors. The big mistake of the critics, however, is to conflate this entire mess of an industry with Bitcoin, which, despite what Gerard and friends would have you believe, is the most secure form of money on the planet and our first line of defense against the looming threat of mass social engineering and digital authoritarianism.

Gerard's core Bitcoin critique centers on the Quadriga crisis, where $135 million of cryptocurrency was recently lost when the owner of an exchange died. While right to be alarmed about individuals losing huge sums of money, here is where Gerard makes a puzzling conflation. Losing your bitcoin when it is controlled by someone else (in the Quadriga case, a sketchy company run entirely by one person) is like losing your money when thieves hack your bank account, or losing your jewelry if someone breaks into your security deposit box. In these cases, the security model of your bank is the problem, not the type of assets you own. And Bitcoin is no more responsible for the failure of a crypto exchange than the Internet is responsible for the failure of the latest web startup— and yet this line of attack is one that so many critics take when they try to blame scandals like Quadriga on Bitcoin and fool you into thinking that the project is one big scam.

The community mantra "not your keys, not your Bitcoin" is a constant reminder that you shouldn't allow someone else to control your bitcoin. And Gerard even shares this phrase with his readers, but doesn't seem to appreciate the meaning. Users can have complete financial sovereignty over their bitcoin, which is secured by public key cryptography. Simply put, if you don't have my private key (think: password), you can't steal or spend my bitcoin. This goes for thieves as well as giant companies or even world powers like the Chinese or American governments. No other form of money can boast this kind of security. In the title of his article, Gerard suggests that hiding money in your mattress would be safer. This is a bizarre argument to make when today you could instead store any amount of Bitcoin on a tiny USB stick or even a brain wallet, where you can memorize a back-up phrase to your assets and cross borders with a billion dollars in your head.

Gerard asks, what use is there for a money where you have to control your own password? Think about that for a second. He's telling you that the only form of digital money that could possibly be useful is one where you have to rely on a third party. Human rights advocates should be wary of this kind of corporate mindset. Consider what is happening right now in China where the Communist Party has loaded nearly the entire population onto systems like WeChat or Alipay where they not only exert easy surveillance and control over your money and payments, but also steer you with powerful incentives and disincentives as part of the largest social engineering project in human history. Control over our data and money will be an increasingly important part of keeping the Internet and our societies free and open as we enter the age of mass surveillance and the cashless world.

While it's true that you probably need to spend days or even weeks (think: a bootcamp or crash course) learning how to use Bitcoin before you can use it safely and properly, the fact is that this knowledge is available to anyone in the world, online, for free. If you would like to sacrifice the opportunity to personally control your bitcoin for convenience, and you opt to use a third party to store your bitcoin, then you can make that decision. But anyone now can choose to *be their own bank*: a game-changer for the billions of people who don't control their own money. This is especially relevant outside of the advanced economies where nearly all professional Bitcoin critics live.

Gerard claims that Bitcoin takes us to the past, where you could "lose your savings if your banker ran off with your money." The sad part is, this is not the past but the dire present for people living in countries ranging from Iran to Zimbabwe to Venezuela, where governments recklessly print fiat currency, stealing from the hard-earned savings of the average person. In other places, including China, Saudi Arabia, and Russia, the government exerts total dictatorial control over the banking system. Meaning: your banker can and often does run off with your money, whenever he wants. This is even true to an extent in advanced economies, where the value of the dollar (inflated to pay for, among other things, global wars) has plummeted over the last few decades against other assets like oil and gold. Bitcoin doesn't take us backwards, but instead into the future into a world where it will be much more difficult for governments and companies to control us.

As far as Bitcoin's value proposition, one can certainly say that after its first decade, it's still a nascent technology, with a long way to go. It is not as private, fast, accessible, or approachable as it could and will be. But it's a considerable improvement already on at least one key function of our society — the wire or ACH. Bitcoin is a big upgrade here, where, for the first time, one can send money to someone else across the globe within minutes and without worry. Compare this to the existing model, where after sending a wire, we sometimes have to wait days, pay big fees to third parties, and even wonder if the transaction will go through.

Contrary to what the critics would have you believe with all of their scary language about fraud and risk, when I send an on-chain Bitcoin transaction to you, it will get to you, no matter what. There is no point of censorship, seizure, or control. Critics like to paint Bitcoin as a broken system, but actually, unlike Visa or MasterCard, which do "break" and go down from time to time, your access to Bitcoin can't be broken or censored, even if your government shuts down the internet. One of the most exciting developments in Bitcoin recently is the rise of satellite, mesh networking, and even radio infrastructure. Whether with a small satellite device, or even over radio waves, you can send and receive bitcoin from anywhere on earth, and beyond. And people are catching on. Already today, it is estimated that at least $6 trillion dollars

moved across the Bitcoin network in 2018 — $3.2 trillion over exchanges, and two to three times that amount via OTC transfers. Compare that to $62 billion for Venmo, or $8 trillion for Visa.*

Gerard says that the Bitcoin protocol is "incredibly slow, anti-efficient, and hard to scale up." What he may not realize is that these are features, not bugs. Bitcoin's architects and ongoing community made an engineering trade off at the base layer, choosing security and censorship-resistance over speed. The good news is that there are second layer technologies that people are building today that will allow large numbers of bitcoin transactions to be batched together, potentially allowing bitcoin to surpass our current financial system by orders of magnitude when it comes to speed and scaling.

Gerard actually mentions one of these technologies — the Lightning Network — but calls it a "toy" that is "already centralized." I would offer an alternative definition. Simply put, Lightning will allow hundreds, thousands, or, one day, millions of payments to get batched together into one transaction on the underlying blockchain. Lightning payments are globally instantaneous (watch this demonstration done by CoinCenter in U.S. Congress) and, in good news for privacy advocates, protected by onion routing, a robust encryption technology. So while today, with enough resources, a government can surveil bitcoin transactions by analyzing the blockchain, and potentially hunt down dissidents, doing so on Lightning will be much more difficult, as payments will occur off-chain, routed in a way where the owners of the network's payment hubs don't know the origin or final destination of the payments which pass through them. As for whether or not Lightning is centralized, the answer is easy. It's not. There is no single point of failure. You may have heard about Lightning in the news lately as Twitter and Square CEO Jack Dorsey has said it is a matter of when, not if, Square will implement the network into its popular Cash App. This is an exciting step in the right direction for advocates of privacy and human rights.

Gerard also attacks Bitcoin for having a limited supply cap. Meaning: there won't be more than 21 million Bitcoin, ever, and more than 17 million are already in circulation, with the rest to be slowly released as rewards for those who provide network security over the next 120 years. This means Bitcoin is a deflationary system, with a transparent and known monetary policy, where no dictator or CEO can decide to print more and devalue everyone else's money. Bitcoin's anonymous creator, Satoshi Nakamoto, was quite clear that Bitcoin was supposed to be an alternative to central banking and absolute government control of money, even inserting a critique of quantitative easing into the first "genesis" block of the Bitcoin blockchain to prove the point. And what's wrong with that? Monopolized control of money may seem "normal" to you today, but in reality, the practice causes misery for billions of people around the world who are caught under hyperinflation, currency crises, financial surveillance, sanctions, and capital controls. It also makes it easy for governments to print money to go to war and commit violence. We can do better.

Not wanting to miss the most common line of attack against Bitcoin, Gerard mentions that it's a waste of energy. But here he, and all the rest of the critics who blindly repeat an argument sourced mainly from a non-expert's blog, are missing the big picture. Today, more than 75% of Bitcoin's energy usage is estimated to come from renewable resources, a number projected to only increase into the future. Nearly half of all mining is done in a part of China where power is almost exclusively hydroelectric. So while yes, Bitcoin does use a lot of energy — in the same way, as Saifedean Ammous has pointed out, that the car uses more energy than the horse carriage, and the refrigerator more than an ice bucket, and a washing machine more than arduous hand labor, and a modern hospital more than a medieval field tent — it is

already unlocking new sources of hydro, geothermal, solar, and wind power that go otherwise unused or unreachable, hopefully helping us toward the end of the hydrocarbon age.

Gerard characterizes Bitcoin as a project promoting "libertarianism." While it's certainly true that you can have a libertarian appreciation for Bitcoin, given that it gives one financial sovereignty and liberates you from government control, one can also have a progressive appreciation. In my view, Bitcoin is a similar phenomenon to democracy and the Internet, technologies which respectively smashed the tyranny of political power and corporate control of knowledge. Through democracy, citizens are able to check the power of kings and dictators, and through the internet, citizens outside of the government and the richest classes are now able to have a strong public voice and have unfettered access to all of the world's knowledge. In the same way, Bitcoin will break the government and corporate monopoly on money. In 100 years, humans will likely look back at today and see a time when a small handful of elites controlled money as a backwards idea, just like the idea of political tyranny or state-controlled news.

Gerard saves his favorite argument for last, that bitcoin is a shadowy network that will surely be used by criminals and drug dealers. But remember, the same types of fear-based arguments were made by kings and elites and dictators when the people demanded that they step down and share power, or by big telephone companies and news organizations and propaganda regimes at the dawn of the internet. But instead of bringing instability and terror and crime to our societies, democracy has empowered half our world and sparked historic advances in innovation, prosperity, peace, and social welfare. And instead of becoming a criminal domain, the Internet has put the sum of human knowledge into anyone's hand, giving a global megaphone to investigative journalists and a world encyclopedia to aspiring students. And while Gerard tries to tie Bitcoin to evil doers, he fails to mention that virtually all financial crime and drug trafficking is committed inside the existing "official" financial system, where trillions of dollars of corruption occur, aided and abetted by banks like HSBC and Wells Fargo. Watch "Escaping the Global Banking Cartel," a stand-out talk by Andreas Antonopolous, and you'll learn more about why Bitcoin is a way out of our current system, which is exclusionary and unjust, and tends to prey on the weak and disenfranchised while letting the corrupt Davos crowd walk free.

In fact, for all of his do-gooder, consumer protection positioning, Gerard misses the key human rights aspects of bitcoin completely. Whether you are trapped under centralized payment schemes like WeChat used to microtrack your lives, or whether your newspaper's bank account has been frozen by a dictator, or whether the US government has unfairly put broad sanctions on your country, punishing you for crimes your rulers committed — Bitcoin is a way out. The greatest potential that Bitcoin has is to help the most vulnerable on this planet, those without bank accounts, identities, or access to the financial system. Now, with just a phone and an internet connection, anyone can receive bitcoin from anyone else in the world, in minutes, for a small fee, with no possibility of censorship or seizure, without needing to ask permission from anyone, and without needing to prove an identity.

In the coming years, as infrastructure and local liquidity and exchange points grow, Bitcoin will have a major impact on foreign and humanitarian aid. Individuals, charities, and democratic governments will no longer need to comply or even deal with the dictators who rule over most of the world's poorest people. As Coinbase realizes with its GiveCrypto program, we'll be able to side-step this old infrastructure completely and transact with aid recipients directly. We can already analyze local exchange data to see that despite Bitcoin's declining price in the past year, usage has increased in authoritarian societies like Belarus, Venezuela, Kazakhstan, and Egypt.

Perhaps the most shocking thing about Bitcoin is that so few know about it. 10 years since the project began, it is estimated that less than 1% of the global population has ever interacted with Bitcoin. Unlike the modern financial system, which is run by a kind of aristocracy, and only permits selective access, Bitcoin is completely open to everyone. It cannot discriminate. Literally anyone can use free online tools to learn how Bitcoin works, send and receive bitcoin, and even learn to code and contribute to the Bitcoin software itself, helping to steer the direction of the future economy. Here's the best part: you don't need to go to Harvard or be a VC in Silicon Valley or have a thirty-year career in economics or central banking to help lead the next financial revolution.

Most world-changing technologies are dismissed by the crowd at first. Consider the telephone, which no one wanted to buy; the car, which surely couldn't work on our horse roads; the plane, which couldn't possibly be safe; or the internet, which was destined to fail. Remember the words of Paul Krugman who said that "by 2005, it will become clear that the Internet's impact on the economy has been no greater than the fax machine." Any fundamental technology, from the fridge to the credit card, follows an adoption S-curve, and at the beginning of the S, there are always plenty of luddites and skeptics. Eventually, the curve goes exponential and the technology spreads throughout humanity. It's hard to imagine a more fair or democratic idea than the fact that anyone today — regardless of their location, gender, language, age, level of education, or wealth — can get meaningfully involved at the ground level of Bitcoin, an exponential technology that is still at the bottom of its adoption S-curve. The only thing stopping you, is you.

Perhaps it's too much for Gerard to grasp this, as he writes from the cozy confines of London. But whether it's in the Philippines, Nigeria, Turkey, Venezuela, or Palestine, there are people who don't have his rights, freedoms, and trust in their financial system. And they are increasingly using Bitcoin, the most secure and sovereign form of money on earth.

Thanks to Dan Held and Misir Mahmudov for their feedback.

**Coinmetrics has more conservative data, stating that $2.16 trillion was moved across the network in 2018, with $601 billion in "meaningful volume."*

Alex Gladstein Medium member since Feb 2019

I'm the Chief Strategy Officer at @HRF and a guest lecturer at @SingularityU. Follow me @gladstein for thoughts on freedom and decentralization.