Bad News for Bitcoin?
Guest: Erik Voorhees
February 20, 2014

Erik Voorhees is a long-time Bitcoin entrepreneur. Follow him on Twitter @ErikVoorhees.

WOODS: I've got a lot of items to talk to you about, and they're mostly negative, about Bitcoin over the past month or couple of months since we spoke last time. I want to give you a chance to talk to my listeners and explain what's going on and try to make sense of everything. The first thing that has to be talked about, obviously, is: what's going on with the Mt. Gox situation? Can you explain what it is and what's happening there?

VOORHEES: Mt. Gox was the largest Bitcoin exchange for a long time, and it was really the first big Bitcoin exchange in the world and sort of dominated the market. Over the last nine months it has sort of been on a slow decline, but they've, for a long time, had withdrawal problems and mainly these were regarding fiat. So, if you had dollars in the exchange and you were trying to send those back to your bank account, it would often take many weeks or even a few months to get those funds. So that was all very obnoxious and annoying, but people put up with it. A lot of it might have been due to various banking problems in Japan where they're located.

But more recently they've had withdrawal problems of Bitcoins themselves and that was a fairly new issue for them. And once this started cropping up, maybe a month ago, people started noticing that Bitcoin withdrawals were not coming through properly and, of course, a Bitcoin withdrawal should be instant. The whole point of Bitcoin is instant payments anywhere in the world. So as people started noticing this, the story got picked up and more people got a little nervous. And they're like: "Well, let me see if I can withdraw."

They would try it and ultimately it created a sort of run on the bank, so to speak. Lots of people were trying to withdraw Bitcoins and they were all failing. All the transactions were failing, and people couldn't get their coins out.

What this revealed was that Mt. Gox had been vulnerable to a long-known bug—maybe bug is not the right word, an issue with the Bitcoin protocol, which causes transactions to possibly be spoofed if you don't write your wallet software properly. So, apparently Gox had not written their wallet software to handle this properly. And we still don't know many of the details of what's going on behind the scenes there.

But, as of now and for the last seven to ten days people have not been able to get their Bitcoins out. The theories range from they're totally insolvent and this is the beginning of them just disappearing with everyone's money; to maybe they lost a bunch of money from a hacking exploit of this issue; to basically they just had a technical problem and it's taken them a long time to fix it, but it will get fixed and everyone will get their money back. So, we'll have to watch and see what happens.

I guess their next announcement is supposed to be tomorrow.

WOODS: Now, Mt. Gox tried to claim that the problem really was Bitcoin's problem. It was a Bitcoin issue. It was not really their fault. Is that just a smokescreen, you think?

VOORHEES: Well, of course there's a little truth to it. Bitcoin is open-source software that is still in beta and is being built by lots of people all over the world. It's certainly not perfect. There are issues with the various implementations, and there are issues with the code, and deficiencies, and all that sort of stuff. In general, it works very well almost all the time, but there are certain things that are known issues that you should take into consideration when writing software for Bitcoin.

So there was an issue with Bitcoin, I suppose, and Mt. Gox either wasn't aware of it or simply didn't write their software to handle it, whereas everyone else seems to have done so. So them blaming Bitcoin doesn't go very far when all the other exchanges have come out of this without problems and are still processing withdrawals. I don't think people give much credibility to Mt. Gox's argument. They mainly seem focused on putting blame elsewhere instead of focusing on the fact that this bug has been known about for years and they just never took action to resolve it.

WOODS: Let's talk about this distributed denial of service attack, just over the past week or so, I guess, that hit Bitcoin. Blockchain's chief security officer says, "The attack was massive and concerted with parallel transactions being executed to create a 'fog of confusion.'"

Now, can you explain a distributed denial of service attack? I had one of those hit my website. Would you be able to explain, first of all, what that is?

And then, secondly, why is this not something that would make somebody say: "Bitcoin is just too risky for me to be involved in. I mean, look at what's going on here."

VOORHEES: A standard distributed denial of service attack usually refers to a website that is coming under a huge load of traffic, often from bot-nets or various computers around the world, and the intention is to overload it with so much traffic, so many data requests, that it just can't process them all. And legitimate users get blocked out of the site because it just can't handle it. Those happen all the time in the world of the Internet.

This recent denial of service attack on Bitcoin, I'm not sure I would call it a denial of service attack. It had that effect, but it was more about an attack trying to exploit this vulnerability. This issue that was brought to light in the Bitcoin code. A lot of people already knew about it, but this Mt. Gox thing popularized it. So I imagine that every hacker around the world is like, "Hey, I'm going to see which Bitcoin services around the world are vulnerable to this."

They started creating all sorts of transactions and just going crazy to try to exploit this problem. Of course, it doesn't seem to have affected anyone other than Gox.

I think the important lesson isn't that Bitcoin is so vulnerable, and doesn't respond to all these problems, and has these issues and therefore you can't trust it. I think the opposite lesson is actually important. It's that as these problems get discovered, attacks happen on the Bitcoin network and through all the various attacks that have happened over the years the Bitcoin community pulls together, figures things out, makes the software better, and the Bitcoin afterward is stronger Bitcoin than the Bitcoin before. So, this is sort of the concept of anti-fragility, where every time these incidents happen, Bitcoin as an ecosystem get stronger than it was prior.

WOODS: Let's just make this clear: this particular attack did not result in anyone losing any actual Bitcoins, is that right?

VOORHEES: As far as I'm aware, there have not been any reports of services that have lost Bitcoins. That doesn't mean some haven't happened, and it's possible that in some cases where coins were lost, the companies or exchanges just can cover it out of their own pocket, so it might not ever be public. We don't know if Gox lost money from this problem that was happening. They haven't been very open in their communications. So that's really the big question: Did Mt. Gox lose a bunch of money from this exploit?

And really we don't know, but there have not been users who have lost their money from various websites, so it seems to have been pretty well handled by people.

WOODS: I was just referring to a quotation from somebody at the Bitcoin Foundation saying, "This is a denial of service attack. Whoever is doing this is not stealing coins, but is succeeding in preventing some transactions from confirming. It's important to note that DOS attacks do not affect people's Bitcoin wallets or funds."

So you think maybe are they perhaps reassuring people too much?

VOORHEES: No, it depends. So if you have your Bitcoins stored in your own Bitcoin software on your computer, this attack was totally irrelevant for you. It doesn't do anything. It's not like someone could pull the coins out of your account and you open your computer the next day and discover the coins are gone because of the attack.

WOODS: I see, I see, I get it, I get it.

VOORHEES: So people don't need to be worried in that way. However, if you have your coins with an exchange or with an online e-wallet and this bug is allowing the attacker to pull Bitcoins out of that exchange. For example, if they're pulling Bitcoins out of Mt. Gox without Mt. Gox understanding that, Mt. Gox might be losing Bitcoins, even though all the user balances would be the same. So then that would put Mt. Gox in the bad situation of having to cover all of those losses or just admit insolvency and disappear.

But we have no idea. Mt. Gox may not have lost anything. They may have lost a bunch of money. We really don't know. One of the important lessons is: as always, if you keep your money with someone else, you are at risk of any vulnerability that that someone else has. So for the convenience you get of keeping your Bitcoins in an e-wallet, you have the risks associated with that e-wallet and that company and all that that implies. Bitcoin users really need to be very careful and responsible with their funds. Large amounts of money—they should not be leaving it with people they don't trust. And certainly Gox has not engendered trust over the last few years of its existence at all.

WOODS: Speaking of the Bitcoin Foundation, tell us a little bit about what happened with Charlie Shrem.

VOORHEES: I'm not going to comment on that case.

WOODS: Okay. There is certain fallout from this. I read in the *New York Times* that they're claiming that this is going to lead to a greater regulation of firms that are involved with Bitcoin and so on and on. Now, you get this argument all the time, right? People saying that governments are going to try to crack down on Bitcoin and then Bitcoin supporters respond by saying: "Well, they can try, but good luck trying."

Couldn't they, nevertheless, though, cause a lot of headaches for Bitcoin exchanges? Isn't there something that governments could do to gum up the works in that way?

VOORHEES: Yeah. And here again it's very important to understand the difference between the Bitcoin network, the Bitcoin protocol and actual Bitcoin companies and then people using it. The key point with Bitcoin is that because there's no one company behind the protocol, the protocol cannot be regulated. So, any rules that come down from politicians in whatever jurisdiction—in the U.S. or otherwise—there's no person in charge of Bitcoin that can comply with those. So Bitcoin does not care about regulations and it cannot be regulated.

That is not the same as saying that various companies that are involved in Bitcoin services cannot be regulated. They certainly can. And indeed, you see the companies in the U.S. that are involved with Bitcoin are going to have to comply with the various laws of the U.S. government or else they risk prosecution.

You have to sort of see it in this dual light where the protocol can't be regulated and doesn't answer to anyone, but individual companies in whatever jurisdiction they're in will have to.

WOODS: Erik, I want to run by you a story that appeared in Business Insider and I'm sorry it's also negative. I'm not doing this on purpose, but I want to know how a Bitcoin expert like you responds to some of these news items that a lot of us are reading about. You are the best person I know of to deal with all of this and I just want to throw at you everything there is and see what comes back.

And so there was an article in Business Insider, which I always take with a grain of salt, but the suggestion of the article was that what's going on here is that there's a kind of civil war emerging between the earliest Bitcoin adopters, who tended to be hardcore libertarian in their political views, and now what he's calling "a more moneyed wing"—relative latecomers to Bitcoin that see that there's money to be made here and what they want, above all, is respectability. And if that comes at the price of agreeing to various types of regulation, etc., then that is a price they are willing to pay. And frankly, they are not interested in and are kind of amused by the sort of anarcho-capitalist, libertarian wing of Bitcoin.

Have you encountered any of this and do you have any comment on that?

VOORHEES: Of course, as Bitcoin grows from a little niche thing carried out by anarchists in their basements to the dominant global financial system that many of us think it's destined to become, it will necessarily start including larger and larger swaths of the population. And that means the sort of early ideology of many people who got involved will not be present in the later adopters. So, there's nothing strange or unusual about that; indeed, it should be expected. This is not a currency for libertarians. It is a currency for everyone on the planet. And it is used by all sorts of different people for all sorts of different purposes.

So, of course, in that context you're going to have people with differing goals and views trying to use Bitcoin for their own purposes, and often they'll be at odds with each other. And that's fine; this is part of a decentralized system. Ultimately, the people who want Bitcoin to be regulated, they don't have any magic wand either. They can't make the protocol regulated any more than anyone else can.

And also, I think it's important to know that there are people who are much more Machiavellian about these sorts of things. They may be very anti-regulation and they may be sort of hardcore anarcho-capitalists at heart, but they also know how to play the game. And they know what kind of face they need to put on in order to operate in the kind of world that we live in. So people's motives and intentions are not always clear.

WOODS: Interesting, yeah.

VOORHEES: Yeah…. I'll just leave it at that.

WOODS: I hear you loud and clear.

Let's turn to something that is maybe a little bit more positive—it's almost old news about Overstock.com accepting Bitcoin. Are you familiar with the website Fiverr.com?

VOORHEES: I read that they recently started doing some Bitcoin stuff.

WOODS: Yeah. Here I was thinking I was going to tell you something you didn't know already. So much for that. I've used Fiverr, I've used it repeatedly. It's a neat website. It's a neat site where people offer all kinds of interesting services in five-dollar units. For five dollars, I'll do some crazy thing, I'll transcribe ten minutes of audio, or whatever. It is an extremely valuable website. I absolutely love it. I use it for all kinds of neat things. I had people all over the world wishing my wife a Merry Christmas in the most bizarre ways imaginable. I paid a guy five bucks to eat his way through a watermelon and then in the center of it was a Merry Christmas note to my wife. That cost me five bucks. I would love to be able to use Bitcoin for that. I've got these Bitcoins; I'd like to use them.

Now, I can't speak for a company like Fiverr, the CEO of Overstock has made clear that they don't want to be in Bitcoin. They don't want to hold on to the Bitcoins. They want to cash them out into cash. This raises the question that a lot of critics have raised: is Bitcoin in fact being used as money when the people on the other end of the transaction want to get out of it right away?

VOORHEES: First of all, with Overstock they've actually come back and said they are actually interested in keeping some of it in Bitcoin.

WOODS: Oh, okay.

VOORHEES: Let's ignore that for now because certainly it's true that most companies will not want to keep their Bitcoin revenue in Bitcoins. And that's completely understandable, right, because the currency is so volatile. It can go down 20 percent in a day. It would be imprudent for a company that wants to accept Bitcoin and to handle its accounting normally to be taking on that exchange-rate risk.

So, to the extent the companies are just cashing out Bitcoin into normal money—there's nothing wrong with that, that's just using Bitcoin as a payment network instead of as a currency itself. Bitcoin is both things. It is the currency units and it is a payment network. The currency units ultimately get their value from the payment network itself. There are some purists, I guess, who think it's wrong or sacrilegious to be cashing out your Bitcoins for dollars. I think that's nonsense. However people find to use this technology in a useful and productive way, they should do it.

And you'll start to see, maybe it'll take a number of years, as the Bitcoin price stabilizes, which it will at some point, as it stabilizes people will feel more and more comfortable with holding, at the margins, some portion of their earnings in Bitcoins. And this comes from the stability. This comes from when they realize there's other places they can spend it directly, but that's something that happens right away. This is a spontaneous market-based process that is ugly, that has ups and downs, and mistakes, and problems, and all sorts of roundabout ways of getting to its goal, but we'll see it come to that over the years.

WOODS: Erik, you are, of course, very plugged into the Bitcoin community. Can you tell us how people's spirits have been over the past month? I mean, we had the Charlie Shrem arrest, we've had the Mt. Gox situation, and we had that, whether we want to call it a denial of service attack or not, we had that go on. We've had items like this and then this alleged civil war going on with Bitcoin. Have people thought, "Well, this was really a bad month for Bitcoin"? Or are people thinking, "The mainstream media is just missing it here. They're being distracted by issues in the long run that are just not going to matter"?

VOORHEES: Ultimately, there's lots of noise in Bitcoin. Individual people and the press love a salacious story that will just get people interested for various reasons. And yeah, I mean, when the Bitcoin price is going up people are going to be optimistic and positive and everyone is glowing about it. And when the price has been going down people spout doom and gloom and all that stuff. You know, you can go in the Bitcoin reddit forum and you can tell who's new and who's been around a while. New people—

WOODS: They're all panicked?

VOORHEES: --when prices are going up they're just euphoric and they just think, "Wow, this is amazing." And when things go sour for a little while they completely turn around and they get all depressed and everything. And it just seems very childish. And it's something that I've come to not enjoy dealing with that every time there's a down trend.

You know this stuff is going to be volatile. Volatile means up and down and crazy movements in price and sentiment all the time. And certainly, different sentiment in different places around the world. So what might be going well in the U.S. for a while is not necessarily going well in China or something. This is going to be a bumpy ride, and people who are really interested in this technology are going to have to get the stomach for it and grow up and put their big-boy pants on and deal with it.

WOODS: Erik, is there a central place on the Internet where somebody can get Bitcoin-related news on a daily basis? Is there one center that everybody goes to?

VOORHEES: If you want written article news, the best source is coindesk.com. They are just getting better and better. I mean, they put out new pieces every day now about various things that are relevant in Bitcoin. So, that's like written articles.

The reddit forum, reddit.com/r/bitcoin, is probably the biggest community and the most active, so if you just want news all the time, real quick, some of it worthless, some of it valuable, that's the place to hang out.

Between those two places if you observe them you'll probably have a good idea of what's going on.

WOODS: And finally, Erik, let me take the last minute or two to turn it over to say anything you want to say to the listeners out there, including for those who are curious about Bitcoin and want to get started, what you would advise them to do.

VOORHEES: Well, for anyone who is still curious about Bitcoin all you can really do is start learning about it. Don't put money in that you can't lose. Understand how risky and crazy this stuff is. But understand how if it works it will absolutely change the world, and it's probably a good idea to at least understand what this is.

So just educate yourself and spend an afternoon learning about it and you'll probably get hooked and fall down the rabbit hole.

WOODS: You know, Erik, I don't want people to think that I'm not promoting you adequately. I always promote the guests and I direct people to websites and books that they've done. But I know that you just want to represent yourself and not any affiliation you have with anything. If there's anything you want me to plug, I'll do it; otherwise we'll say goodbye until next time.

VOORHEES: I think we should be good. I'd rather not promote anything right now. I'm happy to be on the show and talking with you.