The Future of Bitcoin
Guest: Erik Voorhees
October 11

Erik Voorhees is a longtime Bitcoin entrepreneur. Follow him on Twitter at http://twitter.com/ErikVoorhees.

WOODS: Let's start off with the best you can do in explaining for the layman, in a nutshell and without any nuance, what Bitcoin is.

VOORHEES: Sure. Bitcoin is a digital currency, and it's a payment system through which people send that digital currency. So it's basically a way to send digital units called Bitcoins between any two people that are using the system. And Bitcoins are not tied to any commodity or any government fiat currency. They are their own currency unit and the price of them fluctuates on the open market.

WOODS: Now what's the benefit of Bitcoin? Why would somebody be interested in Bitcoin?

VOORHEES: Well, there are several reasons. One is just that people who prefer an alternative to government money might really like Bitcoin. But practically speaking, you can send any amount of money anywhere in the world instantly with almost no fee. So compare that to any bank or credit card, and it really blows it out of the water. Some people use it for ideological or moral reasons, because they don't like using the government's money, and some people use it because it is a better payment system, much faster, and much cheaper.

WOODS: I think a lot of people are interested in the whole matter of Silk Road and the shutdown of Silk Road and how that happened. I want you to do three things for us. First is tell people what Silk Road is or was. Then secondly, how did it get shut down, and is there any weakness in Bitcoin that's been exposed because of the shutdown of Silk Road? And then thirdly, does this mean there's going to be added surveillance or harassment or spying on of people who are interested in or trading in Bitcoin?

VOORHEES: So what is Silk Road? A lot of people have heard about Silk Road over the last few years. It was one of the things that first got a lot of press attention for Bitcoin. Basically it was a website where users would buy and sell illicit drugs—things that are illegal in almost every country. And this was not a website that you would find in the normal Internet, but it existed over what's called the Tor network, which is sort of like a dark Internet. And the Tor anonymizes internet traffic, so you can't really tell from where a visitor is coming or where a server is hosted.

So Silk Road was a marketplace for drugs that lives in the dark Internet under Tor. Of course you can't buy drugs online with your credit card, because then there is a paper trail of what you've been spending your money on, because credit cards obviously have no privacy whatsoever. So Silk Road instead used Bitcoin, because one of its attributes is that it is pseudonymous or nearly anonymous depending on how careful you are with it. Your Bitcoin account is not attached to any name or address or any identifying information at all. So if you're careful in how you use your Bitcoin accounts, you can do so with a great deal of privacy. And that's what was used on Silk Road.

WOODS: Why didn't Silk Road go on forever?

VOORHEES: Silk Road has been running, I guess, for about three years, but last week the alleged operator of Silk Road was caught by the FBI, and the servers were seized and shut down. So Silk Road is no more. It is gone now. Looking at how the FBI actually carried out this attack, mostly it was due to some careless mistakes made by the operator of Silk Road. So if you're trying to run something purely anonymously for many years you can't mess up, and this guy messed up a few times. And it was enough for the government

to piece some things together and figure out who he was and where he was and ultimately arrest him.

WOODS: I think the way this was spun, at least initially to some people, especially by Bitcoin skeptics, was to say, "Aha, you see, you people thought that with Bitcoin nothing could be tracked, and now look, everybody's transactions in fact are easily visible to everybody." To what extent is Bitcoin anonymous or can it be made anonymous and if so, how?

VOORHEES: When you create a Bitcoin account, it's just a long string of numbers. Think of it like a Swiss bank account number. And it's not attached to any information about you. Now if you go out into the world and post that address in places, if you put your Bitcoin address on your Facebook page, now suddenly it is not anonymous anymore. Now suddenly that address is very much attached to your real-world identity. And so if you want to use it in a way that is actually anonymous, you have to take a great degree of care in how you behave with it. And if you take that care you can achieve a great deal of anonymity, but you just have to be careful.

So the thing to understand about this Silk Road issue is that the government did not find the operator of the site or take him down or seize his servers due to any vulnerability or problem with Bitcoin. They weren't tracking money around. They weren't attaching Bitcoin payments to real-world users. They were going at it from the network security side and just general police work trying to find out who this guy was, and they were able to do so. It really had nothing to do with Bitcoin at all, and Bitcoin was the strongest link in a chain that actually was weak elsewhere, if that makes sense.

WOODS: Well, I wonder if this is related to an item I read a few days ago. Let me just read a few sentences of this to you and to the listeners here. "Closing down Silk Road and arresting its alleged operator has left the FBI in uncharted territory. After shuttering the hidden site, law enforcement went to work confiscating the money and materials belonging to the alleged operator." But they say that they're finding that the more than 600,000 Bitcoins in his personal fortune are still inaccessible to them. And then it goes on to say, "The only way to move Bitcoins out of a private wallet is to have the corresponding private key to authorize the transaction. The FBI has been unable to get through the encryption, leaving all those Bitcoins—amounting to roughly $80 million at current rates—out of reach."

VOORHEES: Correct.

WOODS: Now, I don't know. Maybe that's changed over the past few days, and they figured something out. But can you comment on this?

VOORHEES: Yeah, I'll clarify a few things. First of all, they were able to seize some coins. They seized coins that were basically held on the live Silk Road server. These were coins that were in what's called a hot wallet, meaning a big coin wallet that is very much online, not necessarily encrypted, not stored safely. The reason that you would have a hot wallet is that it can be used for live transactions very quickly. So most Bitcoin businesses have a hot wallet where money is going in and out quickly, and it's not super secure. And then they keep their savings in a much more secure form called a cold wallet or cold storage.

So the FBI got the hot wallet. 26,000 Bitcoins from the Silk Road website. Most of those belonged to users of the site who had Bitcoins deposited in their Silk Road account. But the government has not been able to get the 600,000 Bitcoins that apparently belong to the operator of Silk Road. They have his wallet that has all these Bitcoins in it, but they can't break the encryption. And this is quite funny actually, because they spend billions of dollars building these research facilities and have all the supercomputer power in the world, and yet they can't get into the Bitcoin wallet of this guy, because it was secured properly. So this is a strong testament to the fact that Bitcoin, when used properly, is really quite bulletproof.

WOODS: So in other words, let me make sure I'm clear on this. You're saying that not only can they not get access to those Bitcoins now, but unless, I don't know, he buckles and spills the beans or something and

gives them the information they need, they'll never be able to access them?

VOORHEES: Correct. They would have to torture him into providing the password, and depending on how he set it up, he might not even know his own password. He may have, you know, set something up in such a way that he doesn't even know it. There are certain ways to do that, but basically if they don't get his password, they can't get those Bitcoins ever.

WOODS: All right.

VOORHEES: And what's further actually entertaining about this is that Bitcoin wallets can be copied, so even though they have his wallet, it's likely that that wallet exists in other places. Maybe he had copies with friends or trusted partners who he worked with. Maybe there's one buried in his backyard. But anyone who has a different copy of the wallet and had the password can still spend those coins. So even though the government has the 600,000 coins, they can't spend them, and anyone else who has a password still can. So they could at any moment vanish from under the FBI's fingers.

WOODS: Well, what do you think about this thing called Zerocoin, which is sort of suggesting that there isn't enough built into Bitcoin to guarantee anonymity, and so if you have Zerocoin this makes you better off? Do you think this is overkill? Is this a misunderstanding? How do we understand something like Zerocoin?

VOORHEES: Bitcoin is a very diverse ecosystem of developers and interests and software. And I as I mentioned before, it's not automatically anonymous. You have to be careful with how you use it. So there are some people out there who think the anonymity is extremely important, and so they spend their time writing more software to improve the anonymity aspects of Bitcoin. Other people don't care about anonymity at all. They build software that doesn't care about that type of thing. So you really have people working in all different directions in this ecosystem. Zerocoin—I'm not an expert on it, but in general, anything that improves privacy without causing other problems is typically a good thing. I tend to think that the privacy afforded by just the standard Bitcoin is extremely good. It's mostly a case of knowing how to use it properly.

WOODS: Now, I think of myself as being very much a sympathizer of Bitcoin. At some point I want to have my LibertyClassroom.com accept Bitcoins [TW note: it now does], and I just haven't gotten around to it. And I'm sure it's easy, and I can hire somebody to do it for me. I've just been a lazy bum, and I haven't. I'm more or less in your corner. But for the sake of devil's advocate here: I walked into Panera Bread for lunch not long ago, and there on the front page of *USA Today* was the Silk Road story. Now the guy I was having lunch with had never heard of Bitcoin before, and the story was zooming right over his head. But there it was on the front page.

So it seems to me that at a time like this if you're going to go to a Bitcoin conference, and you're going to be out there and be very vocally and openly associated with Bitcoin, you have to expect that there are going to be people that you don't like, namely the authorities, so-called, who are going to be very interested in you, who may be tracking you. Is there anything to be concerned about, and what are your thoughts about this?

VOORHEES: Yeah, that's a really good question. The authorities have obviously been aware about Bitcoin for a few years. Being involved in a number of Bitcoin businesses, something that's very important is how the government will react to Bitcoin and Bitcoin companies. It's very important to understand that Bitcoin is not just this underground currency that's used for drugs. It is used for everything that money is used for. People buy the most innocent things online with it. They use it to pay each other for beers at bars. It's used just as any money, and I think most government people that are interested in this understand that point. They know that only a small percentage of Bitcoin users are involved in illegal activities. They see it as something that's innovative. They don't quite understand it. They don't know how they should regulate it, but they don't see it as this terrible technology that they need to shut down.

There are many companies in the U.S., venture-backed companies, that have raised millions of dollars from prominent tech investors, that are explicitly Bitcoin companies. They use their real names. They have offices. They have employees. They're not hiding from anyone, and they don't need to be shy about being involved in Bitcoin. And what's really, I think, important about this Silk Road lesson is that a lot of people I think incorrectly assume that Bitcoin existed because Silk Road was there. That the only real use of Bitcoin was that people bought drugs online. Those of us who've been involved with this for a few years know that that's not true at all, but it's hard to prove that.

So now that Silk Road is gone, people are going to see that the Bitcoin value doesn't drop to zero, the transactions aren't falling off the cliff. It's still being used just as much as it was before. The prices actually were covered all the way since the drop last week. So there's been almost no effect on the price, and people will realize that Bitcoin is much bigger than the Silk Road. It wasn't Bitcoin that relied on Silk Road. It was actually Silk Road that relied on Bitcoin.

WOODS: I was just about to ask you to tell us about what kind of value fluctuation occurred, but it's interesting to note that it did recover. Now the average person who maybe doesn't know a whole lot about Bitcoin but follows financial headlines—it does seem that we've been seeing an increase in headlines about this or that aspect of Bitcoin, or there's this firm or this person having either more government oversight or regulation or harassment. I mean, doesn't there seem like there's been a cluster of stories like that? And if that's the case, is there any reason for concern by people using it, or is the thing just so bulletproof that this is just like trying to take Superman down with a machine gun?

VOORHEES: It's fairly correct to use that Superman and the machine gun analogy. Not everyone that's involved in Bitcoin is an extreme libertarian who doesn't want government around at all. There are people who think governments are great, and they just need to regulate in a smart way. And so a lot of them will advocate that governments, whether in the U.S. or elsewhere, need to create regulation and to control Bitcoin in a prudent manner. And so they go about doing that. But if you really understand Bitcoin, and you realize how the distributed payment network works, you don't need to fear the regulation, because the people who don't wish to participate in that system can use Bitcoin in whatever way they want. It is a tool that no one controls, and so it doesn't matter what Washington says about it or does to it. It is something that anyone can use for any purpose whatsoever.

WOODS: Now, I'm sure people's appetites have been whetted a bit by this, and again, we've been a bit cryptic, because we haven't answered a lot of the objections or explained the nuts and bolts of how it works, what a wallet is, and so on. Are there online resources where the absolute newbie can go?

VOORHEES: Yeah, I think one thing that's important is that you're not going to understand Bitcoin from just a ten-minute read through a Wikipedia article. It is a new world of technology. It would be like trying to learn all the things that the Internet was in the early days of the Internet. And so if you're actually interested in Bitcoin, spend an afternoon and learn about it. Spend a few hours really understanding it, because just like myself when I first heard about it, I was extremely skeptical and thought it was really stupid, but then after a few hours of educating myself on it, once it clicked, then it clicked. But people need to spend a little time doing that. I'm not going to recommend one place to get started. I would just say, dedicate some time and treat this as an important tool that you should learn about just as every important tool you use from your car to your computer, and spend some time educating yourself.

WOODS: Eric, before I let you go, do you mind if I ask you a personal question?

VOORHEES: Sure.

WOODS: You've relocated to Panama. Can you shed some light on what motivated that decision and what life has been like for you down there?

VOORHEES: I've lived abroad a couple of times. I think there's a lot of value in getting outside of the U.S. bubble, but one of the companies I'm involved with had started up in the U.S., but things are expensive in the U.S., tax rates are high, and because Bitcoin is a global ecosystem, most of our customers will be outside of the U.S. So we didn't want to hamstring ourselves to the U.S. regulatory apparatus if we're going to be working with rural farmers in Kenya. So we chose to leave, and we went to Panama City, because it is a financial center. It has low taxes, and it's not too far from the U.S. when we need to travel to conferences and to see our families. We're not super remote.

WOODS: Well, Erik I appreciate your time. I thought of you first of all as the guy to talk to. It's hard to deal with Bitcoin in layman's terms, because it depends on the level at which you want to understand. I guess it's sort of like the Internet.

VOORHEES: Yeah.

WOODS: I don't need to really understand fully how the Internet works in order to benefit from it.

VOORHEES: Or like a car, right?

WOODS: Exactly. I have no idea how a car works. Yeah, I have not the slightest idea, and when I hear people talk about cars and the Internet at a very high level, I just think this is hopeless. I'll never understand this. But you can talk about it at both levels, and I really appreciate that. And I hope you can be my Bitcoin go-to guy when there are items in the news.