

A Bitcoin Governance Network: The Multi-stakeholder Solution to the Challenges of Cryptocurrency*

Transcript of Interview with Patrick Murck General Counsel, Bitcoin Foundation

Introduction:

Digital currencies, such as bitcoin, are products of the digital revolution and the networked age. As their usage and value have grown, government policymakers have struggled to play catch-up, finding it difficult to comprehend this phenomenon, let alone regulate and govern digital currencies effectively. Incumbent interests, such as large financial institutions, have been similarly caught off guard. Meanwhile, digital currencies march forward. The bitcoin economy has grown to over \$8 billion in value and the bitcoin ecosystem, once composed exclusively of a few hobbyists and technologists, now includes merchants, financial services firms, start-ups, foundations, advocacy groups, investment companies, venture capitalists, government regulators, law enforcement agencies and NGOs. Thought leaders and business innovators, such as Patrick Murck at Bitcoin Foundation, are now pushing forward with bold new applications for the bitcoin protocol. We were fortunate enough to sit down with Mr. Murck for a candid and in-depth interview.



Patrick Murck

We would like to thank Mr. Murck for his time and for his thoughts on this disruptive and fast-changing technology.

Participants:

Guest: Patrick Murck, General Counsel, Bitcoin Foundation

Interviewer: Alex Tapscott, Author, "[A Bitcoin Governance Network](#)"

The Interview:

Tapscott We've launched this program called the Global Solution Networks program which is studying the potential of global web-based networks for cooperation, problem solving and governance and we're looking at this pretty broadly. Any new technology or new application of technology that seems to be doing good in the world, or is at the very least disruptive, is something that we care about. And digital currency we've identified as being one of those technologies and so part of our effort here is to make sure that we understand the viewpoints of all the different stakeholders in what I call the bitcoin ecosystem. I've spoken thus far to people in the private sector, people in government, people in

the legal community, the academic community and, from my perspective, speaking to someone like yourself—an advocate, someone who’s trying to promote the technology from an NGO viewpoint, if that’s a fair characterization—it’s something that we’re very interested in doing. So thank you very much for the time.

Murck Sure, happy to help.

Tapscott I’ve read the website and I know a lot about the Bitcoin Foundation but I’d love to hear it in your own words. What is it that you’re trying to accomplish?

Murck The Bitcoin Foundation was created to promote, protect and standardize the bitcoin protocol. What does that mean in practical terms? We have simply three goals. One is to create a transparent funding mechanism for technical development of the bitcoin protocol. The second is to create a safe public policy framework within which bitcoin and other decentralized currencies can evolve. And the third is educational, to help people understand the benefits of the new digital economy. Those are the three things that we set out to do.

Before the foundation was started, Gavin Andresen, who is our chief scientist, posted on one of the prominent bitcoin forums back when no one was really paying attention to bitcoin, when it was a very, very small community. He said he would like to see a foundation, sort of like the Winnick Foundation, spring up around bitcoin. And a group of us came together to help bring that vision into the world. And the first thing we did was to essentially hire Gavin to work full time on the bitcoin protocol. So he had a funding mechanism to do the work that he’s doing which is extremely important, but also to create transparency so people understood how he was being compensated for the work that he was doing. So there was no conspiracy theory, right, in that matter.

Tapscott So your mission statement is to standardize, protect and promote; can you explain or maybe just elaborate a little bit on how you go about that? Does the work that’s being done at the Bitcoin Foundation happen internally, or are you reaching out to other stakeholders?

Murck Yes, sure thing. So we start with standardize. What we mean by that is supporting the Bitcoin Core reference implementation, so this is the original Satoshi code that was released, and when Satoshi moved out from the project he turned it over to Gavin. And that’s one way, one method by which you can kind of standardize an implementation of bitcoin so people understand, okay, if I want to send outputs from one address to another, this is the way I should do it. If I want to include metadata I can do it this way, if I want to create invoices with unique pay-to addresses, I can do it this way. And it’s not so much in the form of a whitepaper; it’s in the natural implementation, a reference implementation. And so that’s what Bitcoin Core is. My current project, it’s been around for little while and it’s hugely, hugely important and influential, and recently BitPay, a Bitcoin project which is another implementation of bitcoin. It’s good to have diversity of implementation but what we do is try and standardize bitcoin as to fund the development of the Bitcoin Core reference implementation.

Tapscott My understanding here is that a lot of participants, entrepreneurs, technologists etc. have been finding a wide array of uses for the bitcoin architecture and are applying it in a variety of very innovative ways. So you mentioned, for example, like BitPay’s Bitcoin, that’s something that was developed or the standard was set outside of the Bitcoin Foundation.

Murck Well, it's an implementation. So they could set different standards if they chose to. They tend to implement things that have gone through the Bitcoin Core process. But then some other things too; like they have their own version of multi-signature transactions called Copay which they're able to implement and put out into the wild and without having to go through the bit process which is the process which changes the name to Bitcoin Core, so it allows for more experimentation. If they are successful experiments, people love Copay or they love, say, CoinJoin or some of these other techniques for kind of pre-mixing coins, then they can create a bit that says okay, here, not only do I think this is a good idea, I've tried it in this implementation, it works really well, people love it, go ahead and add this into the next version of Bitcoin Core which is kind of the standard. So that's a great reason to have multiple implementations out there.

It should be noted that Bitcore, which is BitPay's implementation, is a project team led by Jeff Garzik who is also one of the core developers for Bitcoin Core. Jeff and Gavin work together. It's still a small community of developers working on all of these things. And just to give you some insight, and I'm not trying to stay on this conversation too much, but when somebody says, "I'm a Bitcoin Core developer," there's a technical implication to that which is sometimes lost in common conversation. So there are only a handful of Bitcoin Core developers and those are people who have what's called "commit" access to the Bitcoin Core repository, that's the original Futoshi code. Gavin, Peter, Vladimir, Jeff, Greg and then somebody like Mike Hearn who is hugely influential, is not technically a Bitcoin Core developer because he doesn't have commit access on the repo. Now, that's his own choice to not have that because he has his own project but he would certainly be offered that any time he wanted it. But he's technically not a Core developer. You do see that term bandied around a bit where people claim to be Core developers because they contribute code. But contributing code technically isn't what makes you a Core developer.

Tapscott Why is that so few people have access to the original code?

Murck I think it's just a matter of managing the process. You certainly want to trust the people who have commit access to the code. You don't want any random person to be able to push a new version out into the community or create a million competing versions of something called Bitcoin Core. You can fork the code and create whatever version you like but the one that has the brand association, Bitcoin Core, that has a few people who maintain that repository and who are in charge of it. Gavin actually handed down the kind of day-to-day duty for maintaining that, in other words going through all the commits and looking at the codes that have been submitted and managing the bit process to Vladimir van der Laan who's also employed by the Bitcoin Foundation to create again the transparency and the funding. So that's why; you want to make sure that you keep the integrity of the process.

Tapscott And then anything that a developer might want to use the original code to, as you say, fork in some other direction...it's open source, right, people can...?

Murck It's open source. Anybody can take and do whatever they want but...

Tapscott But they can't change the underlying fundamental code, right?

Murck Yes, well... Right, exactly. There's one reference repository that's managed by the six individuals, the access, and then the seventh is Futoshi but he or she or they have kind of disappeared from the scene.

Tapscott Okay. Can we go onto the second aspect, the protection?

Murck Sure. So protect, so for example if there is a legal challenge to bitcoin's legitimacy or use of bitcoin in a peer-to-peer environment, something like that, that's an issue where we will extend resources to protect the free and open permission of use of the protocol. A good example of that is in Florida there is a criminal case brought against two defendants for selling bitcoin to undercover agents, who claimed to want to do some criminal activity. They caught two guys doing it [selling bitcoin]. One of the charges was unlicensed money transmission, and while we in the trial didn't make any, we filed an amicus brief contesting the application of Florida's money transfer laws in peer to peer transactions like the one that was being applied against one of the defendants. The rest of the issues we left alone.

If you look at the Liberty Reserve's notice of proposed rulemaking, when the Treasury Department since then have taken special measures against Liberty Reserve, some of the language in that MTRN, even though Liberty is a specialized currency, it has nothing to do with bitcoin. Between you and me, frankly they're criminals and there was a criminal enterprise; it's pretty obvious, we still had to step in and file a comment in that MTRN proceeding because some of the language in the special measure was too broad and it would have implicated or it could have implicated very legitimate uses of digital currencies like bitcoin. So we wanted to clarify things. And we're seeing that play out in New York right now as well where you have a regulator who's proposed rules that are sweeping and would stifle innovation for the industry. So we're trying to protect the freedom of people to use the protocol and open permission this way.

Tapscott I had a call earlier today actually with Jeremy Allaire of Circle...

Murck Yes, I know Jeremy.

Tapscott And he had written what I thought was a really eloquent rebuttal to the rules or the initial proposal that was made in New York. His view was interesting because it was quite balanced. You know, on one hand I think he's someone who welcomes government's role but doesn't want them overstepping and, as you said, stifling innovation. His view is when it comes to organizations that are simply the on- and off-ramp for transferring other currencies, companies need to abide by AML standards that have been set at the federal level, and ones that maybe are set at the state level. He doesn't want those kinds of requirements for compliance being set for companies that are using the bitcoin protocol for something else. And I thought that was quite interesting.

I want to wrap up just the third goal, promote, and then I want to talk more broadly about governance. So why don't you just run through what you mean by promote and then we can move on...

Murck Sure. Protect and promote sometimes overlap because generally it's a policy issue. But promote is also kind of like what we did in the US senate. When the Senate had hearings we worked very closely with both committees to make sure that there was a positive message that came out about bitcoin and digital currency. So that's an example of promoting and educating—there's educating lawmakers but there's also this example: I was at CYBOS—the Swiss Correspondent Banking Conference—to promote digital currency and bitcoin to that audience. If you know ACAMS, the Anti-money laundering specialists certification body, I've been to their conference, their international conference and I do webinars to educate the compliance officers and BSA officers on such practices and the positive aspect of bitcoin, things like that, so it's fortuitous I suppose.

Tapscott I'm learning that a lot of the people that are part of your organization have been there from very close to the beginning of this phenomenon. That's fair, right? I mean the original app of the developers who posted this to a forum board before it exploded into mainstream. And what I find, you know, reading online in the forum board is that a lot of the earlier adopters of the technology had a really anti-government bent, sort of this was an opportunity to wrestle exchange and the free flow of money away from government monopolies and that government intervention, by definition, categorically had to be something bad and had to be something that had to be forestalled or prevented. But at the same time it sounds to me like you're now in communication with regulators, with legislators to help examine policies, which brings me to my next question which is, what's the role of government regulators in fostering the growth of this industry or helping to legitimize it?

Murck The foundation has been pretty controversial since its inception and some of that is shooting ourselves in the foot and things like that as a group, and some of it is just distrust of government and this idea that even engaging in a conversation with the government or regulators or something like that is either foolhardy or kind of tacit like surrender.

Lawrence Lessig wrote about this in *Code 2.0* – if you read it – but he called it libertarian failure, so it's market failure, government failure and the third one is libertarian failure. That would be a kind of dogmatic insistence that you should never sit at the table with a regulator because the only people who sit at the table are the people who don't agree with you. And then rules inevitably come out looking like something you wouldn't like. I'm actually a libertarian. I worked on the Obama campaign so I'm kind of a weird guy in bitcoin I guess. But I don't buy into that, the argument that you shouldn't engage on these issues or that government or regulators don't have a role in it. And as a group we took a lot of heat, I personally took a lot of heat late 2012 and then early 2013 for proactively engaging with the regulatory community to start the conversation and to set the terms of the debate as best we could. At the time, the message was "there's a thing called bitcoin and it's basically used to buy drugs and it's for criminals."

Tapscott Yes, I remember that.

Murck And that's pretty much what the thought pattern was in DC. And so we made a decision to go at that headlong, take that on and change the perception. And we were very successful at that and I think it culminated in the senate hearing. So now we have a different conversation happening which is not "should there be a regulatory framework, should the government be involved" but "to what degree and what's the best way," with an understanding that we're all on the same page, that there are significant benefits with technology.

Tapscott That in and of itself I think was a big shift in perception that people in government were willing to acknowledge that this technology could have benefits to their constituents and to the economy. How responsible do you think the Bitcoin Foundation was in helping to change that conversation? Was it something that you believe you spearheaded on your own or was it something that came about from multiple stakeholders?

Murck I think without the foundation it wouldn't have happened. I'm usually a very humble guy, but in this case that was something that no one else was willing to do.

Tapscott So looking forward, if...

Murck It wasn't just all me by the way. I had a lot of people who helped me do that obviously. It's not a one-person thing.

Tapscott So here's another question for you: If bitcoin grows to what you think it could be in terms of its potential, inevitably there are going to be other advocacy groups, other—to reuse the word, other stakeholders—that are going to be trying to perform a lot of the same tasks that you're doing. Do you welcome that and do you plan on cooperating, or is it something where the goal of standardizing, protecting and promoting is something that you view as being the domain exclusively of the Bitcoin Foundation?

Murck No, I don't. That's not in the spirit of community. I mean the spirit of the community is open source so the idea is we set a standard, in some places we set a very high standard and in some places we set a very low standard and if somebody can come in and do it better than us then kudos to them. In any aspect of what we're doing, or the totality, it's not about creating roadblocks that other people get stuck on. Every time I see another association announced I think it's good news. It means more people are active and engaged and involved. For me it was always so difficult in the early days to get anybody's attention on policy issues that to see today that it's the new hot trendy thing is pretty great. I think it's very cool and I'm glad to see that there are other groups out there. I know there are at least half a dozen, some announced, some not announced. I think it's all great. And some of them are going to be higher quality than others but... Yes. It's much like how Bitcoin Core is a reference implementation of bitcoin but the bitcoin ecosystem is more robust, more diverse and a better ecosystem overall when there are more implementations allowed. I would say it's the same thing when you're talking about policy, policy organizations as well.

Tapscott So part of our project, the GSN project, is to identify ten different types of global solution networks, and these are broad categories used to describe organizations that are effecting changes in technology and doing so in a multi-stakeholder fashion. So things like a standards network, for example, is one of them and we've seen standardization networks in different technologies before. Policy networks is another one, watchdog networks is a third example. So I'd just like to touch on a couple of those – policy and watchdog. Do you think we need policy networks to create international guidance on issues such as crime, fraud, consumer protection, anti-money laundering, etc., or do you think that's something that's going to come from the top-down from government? Is there any role for you or for any other organization to have a seat at the table when discussing issues like crime, fraud and anti-money laundering, etc.?

Murck I've been very active in that discussion. There's a difference between helping law enforcement understand the technology so that they can develop new methodologies and do a better job, the same for anti-money laundering professionals; there's a difference between that and, say, like what FNIC does where they're actually engaging and stopping illicit activity. So the foundation isn't an SRO, we're not a certification body. We've made a conscious decision not to even attempt to be that or try to do those things. But I've been very involved in the conversation with law enforcement and regulators and anti-money laundering specialists. I've had many conversations with the FBI, Secret Service. There was a conference up in Montreal just last year talking about shady operators and consumer fraud and all these different things. So the better educated those agencies are, the better they're able to root out illicit activity, the better the overall bitcoin ecosystem is going to be and the more useful it will be for people.

Tapscott Who are those law enforcement agencies and governments reaching out to learn more about this? Are they reaching out to developers in the private sector?

Murck I don't know if they're reaching out to software developers, not that I'm aware of. I think there's some outreach to companies operating in this space. I think right now for the most part a lot of the agencies have a pretty good handle on the technology, the underlying technology and they're more interested in how people operate in the space, there's operationalized protection around this, this is how they harden their systems against illicit activity and any trends in the data that they're seeing at an operational level. I think that's where the interest is right now. So it's not so much the developers as it is businesses. There is probably a great deal of interest in cooperating with people who are active in this space to understand the trend.

Tapscott And on the subject of watchdogs, do you need watchdogs to watch the watchdog? If governments are setting standards, setting rules and if the private sector is self-regulating to a degree, is there some other entity whose role is necessary in keeping a tab on what powerful stakeholders in the ecosystem are doing?

Murck Yes. This is kind of a cornerstone of our advocacy and why we always advocate for things like user-defined privacy on the network and open permission on protocol and things like that. The idea around bitcoin is that you can operate directly with the bitcoin protocol without having any regulatory overhead, without having to submit to any kind of surveillance of your activity. That is within your rights to do. If you choose to do something that's more convenient, like go through some third party operator, one, you assume the consumer risk of storing your bitcoin there potentially, or whatever counterparty risk you're taking on using a third party operator, and of course you're going to have to turn over identity information, you're going to have some surveillance on your transactions, things like that, so giving consumers the option of choosing between different levels of service and with the understanding that those different levels of choice can come at a price in terms of privacy and security. But that balance should be preserved, the ability for people to use the protocol and to transact in a completely peer-to-peer manner, that I think is what's going to protect them and create that watchdog effect to check any sort of abuse of the system. I don't know if there's a specific organization that needs to be formed to do that or if it's inherent in the protocol as open.

Tapscott Okay.

Murck Does that make sense or is that too abstract?

Tapscott Can you give a practical example, like how would the fact that it's open and that users determine things like anonymity etc. lead to...

Murck So say you're concerned that... what would be an abuse? I suppose surveillance of your transactions or something like that, right?

Tapscott Sure, so a corporation is trying to use that information against you, government is surveilling you without all the necessary legal rationale for doing so, that kind of stuff.

Murck Exactly. So if this is your concern, you should always have the option of downloading a bitcoin wallet onto your hard-drive, storing your bitcoins locally yourself without anybody else involved in that

process and transacting on a purely peer-to-peer basis without ever interfacing with a third party intermediary. Now that's going to be difficult when it comes to exchanging bitcoin for fiat currency, making certain types of transactions, right? That's why there's a market for commercializing aspects of that flow. But at the same time, if people always have the ability to interact directly with the network on a peer-to-peer basis without any intermediaries, then who are we worried about? As long as there aren't any sort of back doors or anything like that in the protocol, as long as the protocol is unaffected by regulation then that serves as the check. So am I there?

Tapscott That was extremely helpful.

Murck I will say on that point there is this constant struggle that has been ongoing since bitcoin was first introduced in the world between, you know, privacy on the network and surveillance of the network. And I'm not just talking about the on-ramps and off-ramps where we all agree that some level of regulation is appropriate and in the actual data mining of the blockchain and clustering and tying identities to addresses and things like that and then privacy enhancing technology like CoinJoin and mixing services. The more pressure there is to surveil and data mine the blockchain, the more of a response you're going to see from privacy advocates to obscure transactions on the network. And that's been something that's played out time and time again.

Tapscott It sounds like your role is needed more than ever.

Murck Yes, well it keeps things interesting for me that's for sure.

Tapscott My view is that something like this should never be in the hands of, or I guess its fate shouldn't be in the hands of one interest group or one organization. It shouldn't be government, it shouldn't be exclusively developers, it shouldn't be, sort of, you know, technology freedom fighters and libertarians, whatever you want to call it. Like in order for this to thrive it's going to require balance and it might be messy but the more voices, the better.

Murck I think that's right. When you get down to... Have you had a talk yet with someone about how government works within the bitcoin ecosystem itself?

Tapscott No, I'd love to do that.

Murck It's not so much the developers that you need to think about. They're more front-facing. But it's really kind of tripartite, so you have the users themselves, anybody using the network can accept or reject any change; you don't have to upgrade your bitcoin wallet. If you're running a company you don't have to implement the latest version, so there's the consumer choice. You can always walk away. That's one leg. There are the developers, in particular the core heads who say okay, this is what we're adding to the reference implementation, so the last big change was 0.9, the payment protocol which allowed you a structured way to insert metadata, to issue invoices and things like that. And usually people focus on the developers and say well, they're the guys who are pushing code, they update software so therefore they have the control. But really none of their changes ever get implemented or accepted unless the miners, the payment processors, the transaction processors on the network upgrade their version. So if the developers push out a controversial version of bitcoin through Bitcoin Core and none of the miners accept it, the network doesn't change. Or the miners can turn to another development group and accept those changes. So there has to be coordination between the developers who are

writing the code, the miners who are essentially implementing the software and running the network and then the users who choose not to just simply walk away.

Tapscott Is it coordination or is it just rough consensus? I mean if the developer's modification of the code has the backing of the miners then it will be implemented, and if users want to use it, they'll use it? This isn't a democracy right, it all just happens organically. Or am I misunderstanding what we're talking about here?

Murck It's messier in practice. Practically speaking that's right. In practice it's messier of course and so it does require some level of coordination between the developers and the miners to say, you know... Basically there's no point in pushing an update to Bitcoin Core if the miners are going to reject it. That's just simply a waste of everybody's time and effort and it can create other problems. So there is coordination there. And then also, you know, there have been incidents for some things, like that where it's been pretty critical for the developers to issue an alert for the miners to roll back to a previous version to correct an error and that's happened too. So there is some coordination that happens practically speaking.

Tapscott Which area, this is more for my own sake, I'm just curious; which area of growth within bitcoin do you think holds the most long term practical private sector potential?

Murck I don't think anybody has the answer to that. I mean, to be honest, I'm not trying to dodge the question. I think that no one knows.

Tapscott I look at all these different people approaching it from so many different angles, wallets, exchanges, you know, big commercial sized miners; I just want to know which of these is sustainable and which aren't? How important are they to the long term success of the technology?

Murck The way I generally look at the ecosystem, I have a slide I usually use to map this out, but thinking about waves of innovation, the first wave is the pioneering wave and it's all about peer-to-peer interaction with the protocol. Those are the really, really early adopters. The next wave, and we're kind of in the middle to tail end of the infrastructure phase, and that's building liquid performance exchanges, building wallet services that make sense, mining equipment, scaling to process lots and lots of transactions, investor services, merchant services. That's the infrastructure that's happening.

On top of that is where you're going to see the real innovation and that's the stuff that's on the horizon. And so it's hard to predict what that will be but certainly this idea of structured payment flows, you know, you can correlate any type of data to any type of payment essentially on a skewed level, you can attach all sorts of interesting payment flows to purchases so that if I'm a manufacturer and I want to pay my suppliers, I can just, instead of getting a loan or paying them, I just cut them into my revenue stream in a completely transparent way so that every time a customer buys something online it's dispersed to all the stakeholders or rights holders. This is especially important for digital content. There's certainly this idea of, like, a passive payment layer for, you know, to throw out another buzzword, for the Internet of Things, right? I talk about the idea that, when I have a three-and-a-half-year-old and when he's old enough to have a phone he might think the idea of paying for phones is crazy, like we would think of stenographs or something, right? You don't pay for phones but you just pick one up and it pays for itself. It shows you context-relevant advertising and there are bandwidth matters that are all accepting payments passively on the payment network. You don't need any human interaction to create a

payment flow, things like that. And then of course capital markets; I think there's a huge opportunity through what are called "smart contracts" to disrupt some capital markets, particularly for trading markets. I would not be surprised that within the next decade you see a move in that direction.

Tapscott Wow, pretty exciting stuff.

Murck Yes. But all of my guesses may be wrong.

Tapscott It's like that old line, a kid goes to medical school and they say 50% of what you learn here today is wrong, I just can't tell you what 50%. Maybe not an exact metaphor but...

Murck Yes, that doesn't really give me confidence when I go to the doctor but yes.

Tapscott Well, you know, the kids are 20 years old so they probably figured out which half was wrong. Anyway Patrick, I've used up a lot of your time. Thank you very much for your help and for your insights.

Murck Great. Thanks a lot.

* ["A Bitcoin Governance Network"](#) is a research project of the [Global Solution Networks](#) program.