Demetri Kofinas:	00:00	Today's episode of Hidden Forces is made possible by listeners like you. For more information about this week's episode or for easy access to related programming, visit our website at hiddenforces.io and subscribe to our free email list. If you want access to overtime segments, episode transcripts, and show rundowns full of links and detailed information related to each and every episode check out our premium subscription available through the Hidden Forces website, or through our Patreon page.
Demetri Kofinas:	00:34	And remember, if you listen to the show on your Apple podcast app, you can give us a review. Each review helps more people find the show and join our amazing community. And with that, please enjoy this week's episode.
Demetri Kofinas:	00:50	What's up everybody? I'm Demetri Kofinas and you're listening to Hidden Forces, where each week I speak with experts in the fields of technology, science, finance and culture to help you gain the tools to better navigate an increasingly complex world, so that you're less surprised by tomorrow, and better able to predict what happens next.
Demetri Kofinas:	01:13	My guest this week is Pierre Rochard, a self-ascribed Bitcoin Maximalist, who co-founded the Satoshi Nakamoto institute and who has been a researcher, investor, and software developer in the space since early 2013. In addition to developing bitcoin software, Pierre is an outspoken advocate for bitcoin's decentralized governance, the operator of one of the largest lightning network routing hubs, and the host of the Noded Bitcoin Podcast.
Demetri Kofinas:	01:44	This conversation is broken in to two parts. The first deals with fundamental questions concerning bitcoin's base layer protocol, the supply schedule, governance, decentralization, utility and challenges to layer one scalability. As well as a fascinating conversation about anarchocapitalism and the role of Austrian economics and theories of hard money in the Bitcoin community, including comparisons of bitcoin to gold.
Demetri Kofinas:	02:14	The second part, which is available as a 40 minute overtime segment, which is available to our subscribers, consists of a prolonged series of conversations on hyperbitcoinization, including the mechanics of a speculative attack by bitcoin against the U.S. dollar, and other fiat currencies, as well as the existential threat posed by governments and how Pierre believes that bitcoin will manage to overcome all of them on its path towards becoming the global currency standard in the 21st century.

Demetri Kofinas:	02:47	We also explore monetary theories of value, the Lindy effect, Gresham's law and layer 2 solutions for scaling bitcoin as a viable medium of exchange. I end by asking Pierre for his predictions and forecasts, not only for bitcoin, but for the market more broadly, including a conversation on how he's positioning himself for the start of the next bull phase in crypto.
Demetri Kofinas:	03:15	As a reminder, all information provided in this podcast is for informational purposes only and should not be viewed as financial advice, nor should it be relied upon as the basis for financial decisions. And with that, let's get right in to this week's episode.
Demetri Kofinas:	03:35	Pierre Rochard, welcome to Hidden Forces.
Pierre Rochard:	03:38	Thanks for having me on.
Demetri Kofinas:	03:39	What's the proper way to pronounce that?
Pierre Rochard:	03:40	Pierre Rochard.
Demetri Kofinas:	03:41	It's the name of a hockey player. Are you from Montreal?
Pierre Rochard:	03:44	No I'm not. I'm originally from France.
Demetri Kofinas:	03:45	Oh really? You're actually legitimately from the continent.
Pierre Rochard:	03:48	That's correct.
Demetri Kofinas:	03:49	All right well I'm very excited to have you on Pierre. For those of my audience who don't frequent Twitter, this interview basically came together last Friday, we are recording this Tuesday. It's going to be released the next Tuesday - Tuesday the 15th. I wanted to do an episode on Bitcoin Maximalism. I had been speaking with Murad about having him on the show and he's in Azerbaijan I think.
Pierre Rochard:	04:12	He just got back to New York yesterday. We talk all the time.
Demetri Kofinas:	04:14	Okay amazing. So he was supposed to be on the show. He wasn't able to make it and I Tweeted out "I want to get on a Bitcoin Maximalist," and within, I think, an hour or so, we decided to have you.
Pierre Rochard:	04:24	I'm not going to do as good of a job as Murat. But I'll do my best.

Demetri Kofinas:	04:27	Oh I'm sure you will. I did my research, I'm sure this is going to be a fascinating conversation. So, for my audience to understand, in these rundowns, I always put at the front the question, why do I care? I have to answer that question first before I can expect anyone else to care, right? So what drew me to want to have someone from the Bitcoin Maximalist community on...it's not really something I was aware of, but it was after this, real bear market in crypto, the first thing that really emerged was this maximalism, right? So I find that fascinating because amid the carnage of all these cryptocurrencies, what has emerged is the faith in bitcoin, right?
Demetri Kofinas:	05:01	So I think it's fascinating and I wanted to use it as an opportunity to really explore the culture, the governance, the technology, everything. And the arguments for what you and others call hyperbitcoinization, which I think is a very interesting term. But before we get into any of that, everyone has an initiation story in bitcoin. I'm curious to hear what yours is.
Pierre Rochard:	05:21	Yeah so in 2011 I was one slashdot.org which was a developer's website news site, and I generally read through a lot of things that were posted on there, and one of it was bitcoin and I found it interesting so I downloaded the client and opened it up. The article was about mining. I didn't see a button to mine or anything like that, and I just closed it, because I was like, "All right, well." And at that point I forgot about it, and at the end of 2012 I discovered it through a few friends of mine who are crazy libertarians in Austin, Texas. A dime a dozen there. We were debating fractional reserve banking and-
Demetri Kofinas:	06:02	This is 2013 you said?
Pierre Rochard:	06:03	End of 2012, yeah.
Demetri Kofinas:	06:04	2012.
Pierre Rochard:	06:05	And this was my last year of graduate school. I was getting my master's in accounting at UT Austin, and we had a reading circle for Austrian economics called the Mises Circle and bitcoin naturally came up in the course of that conversation. That's when I found out about the monetary policy of bitcoin - 21 million bitcoins - and that's when I realized that this is something, if the cryptography is good, if the engineering is good, if there's no bugs or anything like that, that would cripple the system, that this would be a highly successful money, and it would be a very competitive money.

Demetri Kofinas: 06:39 That's interesting. I've heard Jimmy Song say something similar, although I think he discovered in 2011. But he said something similar about the supply schedule. This is another thing that's fascinated me. We'll get into it. This focus on the supply schedule. Was it not you, or am I thinking it was somebody else who made the point that the software only ran on Windows and they were-

Pierre Rochard: 06:58 That's correct.

Demetri Kofinas: 06:58 That's you?

Pierre Rochard: 06:59 I mean I've made that point, but that's a well-known [crosstalk 00:07:01]

Demetri Kofinas: 07:01 Someone had made that point, which they discovered it early on but it ran on Windows and they were like, "This has got to be a shitcoin."

Pierre Rochard: 07:08 Yeah, I remember Bryan Bishop saying as much in a recent interview.

Demetri Kofinas: 07:12 Maybe it was Bryan Bishop. So you mentioned Austrian theory, let's get into that, because this is fascinating. I was blown away listening to some of your interviews at how well your fundamental understanding of Austrian economics is. I was similarly influenced by Austrian economics, theories of the business cycle, money and credit, et cetera. I was primarily introduced ... Well initially I was introduced to Austrian economics through the newsletters of Kurt Richebächer and the Daily Reckoning. But in terms of formal thinkers, it was most Rothbard and some Hayek and Mises obviously.

Demetri Kofinas: 07:44 I think that the way that you described your initial encounters with Austrian economics, I think parallels many people's experiences. Which is we have this Samuelsonian school that we are taught the neoclassical synthesis in college, and it doesn't make sense, sort of intuitively. But Austrian economics does in so many ways. I'm curious to ask you first, how did you come in contact with it? And what was that experience like for you?

Pierre Rochard: 08:08 Yeah. So I was living in France, in Grenoble, France on the border with Switzerland and my family was originally from France but we moved back and forth between the U.S. and France. At this point I was in high school and it was my summer after sophomore year, before junior year. I was on Wikipedia,

and the featured article on that day was anarchocapitalism and just that title alone struck my interest. I had been interested in political economy. Probably a little bit before that, due to some good teachers I had.

Demetri Kofinas: 08:41 This was 2007?

Pierre Rochard: 08:42 2005, yeah. And then after reading through that article on anarchocapitalism I was like, "Oh wow this is my political ideology." I had just figured it all out. And I ended up going to mises.org that had just a massive treasure trove of Austrian economics for some kid who works or lives and goes to school in a ... It's not Paris, you know so I don't have access to the best libraries or anything. So I could download PDFs all day long. They even had audio podcasts back then I remember listening to on an iPod with a hard drive. Old school style. Yeah, I just became obsessed with Austrian economics for a very long time after that.

Pierre Rochard: 09:26 Simultaneously though, I was getting interested in Linux and open source software and poking around in the command line. My focus on Austrian economics was on monetary economics. That's the part I found to be most fascinating, because of its linkage to the macroeconomic cycle, and that impacting everything else in society. I was already in the mindset long before bitcoin that money is the hidden force, and so-

Demetri Kofinas: 09:51 It certainly is one of them, that's for sure.

Pierre Rochard: 09:52 Yeah. So already I was interested in the Austrian business cycle theory and how fractional reserve banking played a role in that, how central banking played a role in that and in the evolution of our monetary system, it's long history. I think that the general public doesn't know about the history of monetary policy or of monetary economics throughout civilization.

Demetri Kofinas: 10:13 Well I told you, I think it was a tweet or an article, I don't know where it was, or maybe it was an interview of yours, but I tweeted at you about this. But I was surprised that you knew a small fact of history, that Volcker's great insight was not to target the interest rate but to target the money supply. And that caused interest rates to vary wildly, and it created a lot of uncertainty in the banking community around what the rate of interest would be, what the price of money would be, the cost of capital. That perhaps is the biggest contributor to stemming the inflationary crisis that had been unfolding in the late 70s and early 80s.

Demetri Kofinas:	10:47	You mentioned anarchocapitalism, you know Austrian economics functions ideally in a world where there is a gold standard. Without a gold standard, in a fiat world, things like modern monetary theory help tremendously in terms of providing a theoretical framework for how money is generated. If there are no actual reserves, if there is no reserve on which to build fractions, there is something to be desired.
Demetri Kofinas:	11:11	So it's not surprising to me that it has been adopted so vociferously by the bitcoin community. Do you think that it's possible to understand bitcoin without Austrian economics?
Pierre Rochard:	11:22	Yeah absolutely. And sometimes understanding Austrian economics can be a hindrance to understanding bitcoin. I'm familiar with a number of early people who were interested in Austrian economics who took a look at bitcoin and said that it was a bad idea and it was the worst form of fiat possible.
Demetri Kofinas:	11:38	What was their argument?
Pierre Rochard:	11:39	So Mises had this regression theorem, which was basically if you go back to the beginning of the history of a medium of exchange, that at some point it had some kind of production value or utility beyond just being a medium of exchange. So if a money doesn't have that, then my view is that's kind of the straw man reading of regression theorem. So if you apply that to bitcoin you would say, "Well this had no utility at the beginning." Even though I disagree. I think that it had utility from day zero, it's just you didn't think it did.
Demetri Kofinas:	12:10	What as a medium of exchange?
Pierre Rochard:	12:12	Well if you look at it, it's kind of an empirical question of going to people like Hal Finney who was the first person to receive a bitcoin transaction, of "Why do you subjectively value this system and this token? This bitcoin?" Because from there you can kind of deduce, "Okay what is it that was the utility for Hal Finney in particular?" So I think that Austrian's sometimes forget the key tenant of the school is subjectivism, which is that we can't tell from the outside what the utility of bitcoin was to the early adopters.
Pierre Rochard:	12:40	But clearly it existed right? Because at some point it bootstrapped and there were people who were interested in it, and there were people who valued bitcoins before they had a dollar value.

Demetri Kofinas:	12:49	But wasn't it, if I understand the argument, wasn't the argument that they were putting forward ... Or who was it? You said Rockwell was putting that forward?
Pierre Rochard:	12:56	It was people like, I think Gary North has put it forward.
Demetri Kofinas:	12:59	Okay. I'm not familiar with what their argument was, but it sounded to me, the way I assumed it was put forward, was to say that gold has an industrial value and an aesthetic value that's independent of its monetary value. It is fair to say that bitcoin has no value outside of its monetary value, right? And that monetary value is built up entirely based on the network and the protocol.
Pierre Rochard:	13:19	That's what I'm disputing. Because if that were the case, then I don't think it would have ever been able to bootstrap. So for example, some people say that the value was as a collectible, as a digital collectible, so that kind of fits into Nick Szabo's framework for how money bootstraps. So even though 100 bitcoin at the beginning of the system did not have a monetary value, and did not have a dollar price to it, it did have, for some individuals out there, they subjectively projected some value onto it, and they personally valued it enough to at least keep it around and not delete it from their hard drive.
Demetri Kofinas:	13:56	That's an interesting argument. What you're saying is there was a value in the novelty of the item?
Pierre Rochard:	14:02	Right. Right.
Demetri Kofinas:	14:02	But that no longer holds, because it's no longer novel.
Pierre Rochard:	14:05	Well we could say that might reflect .001% of bitcoin's current value, and the rest of it is just purely monetary as a medium of exchange-
Demetri Kofinas:	14:13	Or, it's an expired option.
Pierre Rochard:	14:14	Right.
Demetri Kofinas:	14:15	It no longer holds as a ... So you wouldn't dispute the fact that there is a very big difference between the utility value of gold as an industrial metal or as sort of aesthetic ornament, and bitcoin. Your point is that there's got to be some subjective value outside of, I guess, outside of the monetary value to have even gotten started, because there would have been no one to transact with on day one.

Pierre Rochard:	14:38	Correct.

Demetri Kofinas:	14:39	Well Satoshi Nakamoto saw some value in the design.

Pierre Rochard:	14:42	Well, if no one had joined him at that point, it would have been a system of one.

Demetri Kofinas:	14:46	So one of the things I want to ask you as we continue is - and it's a way of getting into the question of what is bitcoin really? Not just what is bitcoin in technological terms, but was is it really? And I think we can get there by going further down this point about the supply side and the demand side, which deals with utility and with scarcity, right?

Demetri Kofinas:	15:07	Now you've written in a tweet, you said that, "Bitcoin is a medium of exchange with the most legitimate, credible, and sound monetary policy. This is why it has a nine year track record of extraordinary rapid adoption." And then you said, "This is why it makes sense to speculate on it."

Demetri Kofinas:	15:28	bitcoin supply schedule is not immutable, it's not written in stone obviously. But there is this cultural underpinning to it, right? This idea of "code is law." Similarly in the United States, the Constitution isn't what gives us our freedom. It is a piece of paper. You could tear it up, you could burn it. It is ultimately the history and the foundations of American democracy. How much of bitcoin's success in your view is attributable to its supply schedule? How much of it is attributed to its governance? How much to the innovations in its protocol? How much of it is the circumstances around its birth? The culture, the community, etc.? And that's a way of asking, what is bitcoin?

Pierre Rochard:	16:06	We can spend an hour on each one of those points that you brought up.

Demetri Kofinas:	16:09	We will. We won't spend an hour, but I am curious as to your overview answer to that question.

Pierre Rochard:	16:15	So, if I really were to boil it down, I think that most of the value derives from the fact that this is a system whereby a social consensus can be automated using cryptography. And, so, that social consensus is the 21 million bitcoins. Actually a long list of what are called consensus rules, and some of those rules are just kind of arcane technological, you know, aspects of bitcoin. But a lot of them actually directly impact the economics of bitcoin and its ability to remain decentralized into the future.

Pierre Rochard:	16:52	So that, to me is bitcoin in a nutshell, and that's where bitcoin's value comes from, is that these consensus rules are automated. Not only are they just automated, but they're also automated in such a manner where the rules can be validated by a number of people - thousands of people, an indefinite number of people. So if the cost of running a bitcoin node is low enough, for you personally, you can be participating in this consensus and making ... Essentially any time that someone tries to send you value, and they claim it's bitcoin, you're able to independently verify that it meets your personal definition of bitcoin, whatever that may be.
Pierre Rochard:	17:32	Then if your personal definition of bitcoin matches up with other peoples' are, then that socially is an inner-subjective consensus.
Demetri Kofinas:	17:40	Are you describing the open source nature of the protocol?
Pierre Rochard:	17:43	Well this would apply even if it was proprietary software. But it is open source.
Demetri Kofinas:	17:48	But in either case, how does that fit in? Because what you're saying is that people can decide to run the software or not, right?
Pierre Rochard:	17:54	Right.
Demetri Kofinas:	17:55	That the permission list nature of the network.
Pierre Rochard:	17:58	Right. So they're free to join and leave the network as they please, and the main part though that I want to have in place is that the definition of what bitcoin is, is not fixed by a central authority, or by a corporation, or by a government. It's an inter-subjective consensus, in the same way that our definitions of words are.
Demetri Kofinas:	18:15	Neither is Linux, right?
Pierre Rochard:	18:17	Right. Well so-
Demetri Kofinas:	18:17	So what's the difference?
Pierre Rochard:	18:18	Arguably not, because Linux has a Linux foundation with Linus Torvalds' ... But to me, it's the laptop, right? So there's no law that says a laptop is a monitor with a keyboard attached. But if you were to sell a laptop on eBay and send someone a brick, you can't say, "Well my personal definition of a laptop is a

brick." Because you're out of line with the rest of the inter-subjective consensus of what a laptop is, and you'll get sued for fraud.

Demetri Kofinas: 18:45   I am kind of following you. I mean I wouldn't disagree with anything you said, but that's not sufficient to give me a definition of bitcoin.

Pierre Rochard: 18:51   Right.

Demetri Kofinas: 18:51   So let's actually, just for my own clarity, and for the audience's, can you narrow down what you just said so that I can understand it a little bit better and then let's layer on top of it the things that actually make it bitcoin?

Pierre Rochard: 19:02   Yeah. So bitcoin is a piece of software that you are running on your computer. It's node software.

Demetri Kofinas: 19:07   Right. And you can decide to run it, or not run it. And you can join the network, or not join the network.

Pierre Rochard: 19:12   Right.

Demetri Kofinas: 19:12   That's what we talked about so far.

Pierre Rochard: 19:13   Yeah. So from there, what that software is doing, it's automating rules that are put in place in terms of defining, what are the rules for verifying the ledger? So then that way we can construct a shared ledger, and we're all transmitting this data to each other and keeping it in sync. The way we keep it in sync is with this mining process, the proof of work. That's called time stamping function, or a proof of publication function. And basically what that means is that we all agree on the rules for the transactions that we're sending on this network. This time stamping function means that we agree on the ordering of those transactions.

Pierre Rochard: 19:51   So that way we have a temporal ordering of which transaction came before the other, so that you avoid the issue of double spending it.

Demetri Kofinas: 19:57   Well the reordering of blocks, not transactions, right?

Pierre Rochard: 20:00   Of transactions really, because blocks are just a collection of transactions.

Demetri Kofinas:	20:04	Transactions. But you can't order transactions within a block in bitcoin.
Pierre Rochard:	20:06	Not temporally, I mean that wouldn't make sense, because a block is a singular unit of time, essentially.
Demetri Kofinas:	20:12	Right but there are transactions within that block that can't be ordered. My point is you have one megabyte-
Pierre Rochard:	20:16	Oh so you can't spend the same output in one block, so yeah. Correct.
Demetri Kofinas:	20:20	My point is that you can't order transactions over time in the blockchain. It has to be within a block.
Pierre Rochard:	20:25	Right.
Demetri Kofinas:	20:25	So every transaction, within that block, there's no difference in time between those, you don't know. There is a difference, but no one knows what came before what.
Pierre Rochard:	20:33	Right.
Demetri Kofinas:	20:34	Okay fair enough. And probably we'll get into proof of work and some of the mechanisms of the protocol, but still this is an interesting ... I don't know what the theory is in cognitive, in your science, or in theory of mind, but there's the theory or this thought experiment, which is if I copied your brain, your mind, and I erected a duplicate of you on a server ... It's this same argument of uploading your consciousness. If I uploaded my consciousness, I could supposedly replicate it. So if we were to follow this, I think, absurd logic, in a sense, you would end up having multiple copies of me, right? Each thinking that he or she is the same, and indistinguishable, and each thinking that he or she was immutable.
Demetri Kofinas:	21:15	You could replicate bitcoin, it's open source. So let's say we just replicate bitcoin, right? What makes that not bitcoin and bitcoin, bitcoin?
Pierre Rochard:	21:25	Right. So if you were to replicate bitcoin exactly how it is, it would still be bitcoin, because you're still following all the same protocol rules, so you haven't changed any of the protocol rules. So if you copy paste a bitcoin wallet, or if you copy paste-
Demetri Kofinas:	21:38	But if no one uses it, how is it bitcoin?

Pierre Rochard: 21:40   Well I just mean in the sense that the rules in which this is operating on the system are entirely compatible with everyone else's nodes. So you have to change something to make it distinguishable from bitcoin. And then at that point, it's no longer bitcoin.

Demetri Kofinas: 21:54   Right. Well I guess my point was you could replicate the exact same technology and erect it. I guess I was trying to meander into a conversation around the culture and the community.

Pierre Rochard: 22:03   Yeah, so-

Demetri Kofinas: 22:04   Which is to put a value on the community of miners and developers and everyone else who's actually animating this network.

Pierre Rochard: 22:10   So I was going on a technicality there, but if someone does copy paste the code and change a little variable to make it different, so like Litecoin or a myriad number of other altcoins, the community around bitcoin and the global order book of its liquidity does not get copy pasted into this new coin. So they have to start from scratch and that's one of bitcoin's advantages over all of these other cryptocurrencies, is that because it was first, it's accumulated the most users, the biggest community.

Demetri Kofinas: 22:38   How important is that? How important is size? In other words, if bitcoin launched today, if an analogous version of bitcoin launched today, do you think it would be successful? I mean obviously the answer is no, it wouldn't be successful. I mean bitcoin already exists. But how much of it is the technology and how much of it is when it launched? Would it have been successful if it had launched in 1999? It launched when it launched. It launched in 2008 in the midst of the financial crisis. How important is this community and the faith of the HODLers? Of the people who are willing to hold it?

Pierre Rochard: 23:11   So I think that the timing of its launch is fortuitous, but by no means did it have an impact on its adoption rate. That's my view. And I think that actually bitcoin's behavior price wise, and also just in general, is very indigenous and I don't think that there's been any kind of macro-narrative that's impacted bitcoin. Especially to the extent-

Demetri Kofinas: 23:31   Really? The financial crisis and the Austrian theory and theories of hard money?

Pierre Rochard:	23:34	I'm really skeptical that those have had material impact on bitcoin. I mean aside from obviously Satoshi putting financial crisis related information in the-
Demetri Kofinas:	23:44	You don't think that the anarchocapitalism culture is integral to the success of this? That's where the demand for it comes from.
Pierre Rochard:	23:52	Well so I think that there is niche ideological demand that comes from anarchocapitalist ideologues, but ultimately if it cannot succeed on just the raw economics of it, then I would say that we've reached a point of saturation and adoption and bitcoin will no longer grow. All right? Because we've run out of anarchocapitalists-
Demetri Kofinas:	24:12	Well not yet, clearly. And it's just the community, right? My point in all this was to try and bring up the nuance of the value, right? That it's not just the protocol, it's not just the technology. All these things play a role and the community is in a central part of it.
Pierre Rochard:	24:27	Right so my argument though, is I think the community is a self-selected group that's selected into bitcoin and they selected into bitcoin because of bitcoin's properties. So to that extent I think that community would have grown up around bitcoin at any point in time.
Demetri Kofinas:	24:42	And the supply schedule is a huge part of that, an enormous part of that. You mentioned it before and it's something that I want to get into further. Because I was interested when I started to delve in more deeply, I mean I've sort of skimmed the surface of bitcoin. I never delved in as much as I did with you, preparing for this conversation, so I was surprised to see how important the supply schedule was. It really is its central tenant. Let's kind of shift away from that a little bit and move to the demand side, because I would contend that what gives a currency it's value is not its supply side, it's the demand side. It is people's willingness to hold it. Now would you agree with that?
Pierre Rochard:	25:16	100%.
Demetri Kofinas:	25:16	Okay. So we mentioned utility before, right? What are the determinates of demand? How important is utility in that and where do you ascribe the desire to hold bitcoin? Where does that come from?

Pierre Rochard:	25:30	Yeah so, I think that there's a number of different drivers of utility for bitcoin. One aspect that Tone Vays' emphasizes is, it's unconfiscatable. So that speaks to the difficulty of seizing private keys, versus the difficulty of seizing a bank account or seizing gold.
Demetri Kofinas:	25:47	Why is it more unconfiscatable than gold? Isn't the government able to identify who owns what bitcoins? I mean maybe not all of the owners, but lots of the owners. I know they've been working with chain analysis to do that. Can't they arrest someone and demand their private keys?
Pierre Rochard:	26:01	Yeah. Absolutely. I think that it depends really on the scale of it. So basically, the argument for bitcoin's advantage in confiscatability is that it's more expensive to confiscate at the very least.
Demetri Kofinas:	26:16	Why is it more expensive to confiscate?
Pierre Rochard:	26:18	Because physical gold, if you are moving 100 million dollars' worth of gold, that's going to be very hard to move it geographically. Which nation states operate based on geography. Whereas, moving 100 million dollars' worth of bitcoin is trivial, regardless of geography, as long as you have internet access. So the government already has an issue there, because they're just not as good at the cyber as they are at the land.
Demetri Kofinas:	26:42	But that's confusing. So let me ask you this about that. Because in the case where this matters is, case in point, FDR's 1933 executive order, right? To confiscate gold. That would be a concern for people. In that case, I feel like your argument is turned on its head, which is that the difficulty of moving gold, the fact that I would actually make a point, not the difficulty of moving gold, but the physical nature of gold, in small enough quantities ... obviously you can't hold a tremendous amount of bullion without ... Well I guess you can hold it at your house, sure. But you can certainly dig a hole and throw it in the ground, and there are no keys, and you remember where it was. If you forget, you forget.
Demetri Kofinas:	27:19	But the government can't ... Well I guess it can do the same thing, it can put a gun to your head and ask you where the gold is.
Pierre Rochard:	27:26	You have to assume here that the person accumulating gold doesn't have to do the KYCAML that they would have to do with

bitcoin. So that's a fair analysis, but there are ways of accumulating bitcoin without doing KYCAML. For example, if you're a merchant and you're accepting bitcoin in the course of commerce, you don't have to go on and exchange and reveal your identity to anyone and the government wouldn't have that information reported to them. So it's for you to volunteer that in your IRS tax returns.

Demetri Kofinas: 27:50 So if you've never, ever transacted on an exchange, you're safe.

Pierre Rochard: 27:53 Correct and I think that even people who have transacted on exchanges, especially in modern western liberal democracies, they're safe.

Demetri Kofinas: 28:01 A quick question for you here, because this was a tweet and I didn't know what you meant by it and I wanted to ask you. You said that you don't think that drawing a dichotomy between store value and medium of exchange makes any sense, both in theory and in practice. What does that mean?

Pierre Rochard: 28:13 That means that basically there's different views on what medium of exchange means. One view is that medium of exchange is basically the method of payment. So cash or a check or a credit card. I think that's the wrong analysis of what a medium of exchange is. I see medium of exchange as a property of a money in the abstract sense, not in a concrete terms of what you're physically ... Because you can transact in dollars and all sorts of symbolic ways or accounting ways, and you can have, for example, a business that is selling goods to another business and then the other business is selling goods back to them.

Pierre Rochard: 28:51 So you have accounts payable, accounts receivable and they net out to 0. It's like, okay they used dollars as the medium of exchange because those invoices were denominated in dollars, but ultimately no money changed hands at all, because they just netted out their accounts receivable and their accounts payable. So I think that looking at it just from the method of payment is kind of weird.

Demetri Kofinas: 29:11 Well can I ask you ... I've got a question about that. So during the period of the gold standard, gold was a store of value, but demand deposit certificates were mediums of exchange, right? If I was a bank in Nebraska, I would issue certificates on the deposits that I had and those would function as the medium of exchange, but they would not be the store of value, right? Something similar seems to be the case for layer- solutions.

Lightning networks seems to be a bitcoin certificate network, for packet switching.

Pierre Rochard:	29:40	Those are fighting words.

Demetri Kofinas:	29:41	Oh really? Is that right?

Pierre Rochard:	29:43	Oh yeah. Absolutely. That's really opening up a really-

Demetri Kofinas:	29:46	Okay so hold up. So if we're going to get there, because I'm very excited to be educated on lightning network. I told you I knew very little about it on a superficial level. I'm happy that this elicited such a passionate response. I'm looking forward to that, but I want to make sure that we get to it in the proper place, but go ahead.

Pierre Rochard:	30:01	So what you talked about is medium of exchange of bank bills, to me those are like money substitutes. Whereas if the certificate is denominated in gold, I still consider gold to be the medium of exchange in that regard.

Demetri Kofinas:	30:13	I see. So derivatives are still the store of value.

Pierre Rochard:	30:15	Well in the sense that you're adding on counter-party risk for sure, and credit risk and that was a problem with cold certificates, and that's what eventually led to the current system. But more broadly speaking, I think that the medium of exchange is about people accepting that value to themselves. As a way of settling a liability. So if someone is not willing to accept that value, then it's a bad medium of exchange. Now why is it that someone would accept that value to settle liability? It's because they think that it's going to keep its value. It's going to be a store of value.

Pierre Rochard:	30:51	So I really see it as that parable of the blind man feeling the elephant. I see unit of account, medium of exchange, store of value as just three different parts of the elephant that people are touching, but ultimately the elephant is money.

Demetri Kofinas:	31:05	Was this a response to what argument?

Pierre Rochard:	31:07	So there's often the view that bitcoin is a bad medium of exchange and a good store of value. I think that what they mean is that sometimes as a method of payment, bitcoin is subpar. It's not as good as methods of payment that ... Where, a credit card, there's no reason why your credit card couldn't be bitcoin

denominated. So you could use a credit card as a method of payment and use bitcoins as the medium of exchange.

Demetri Kofinas:	31:31	So it's a layer-2 solution.
Pierre Rochard:	31:32	Right.
Demetri Kofinas:	31:32	It's a layer 2, 3, 4. Which goes back to the point about lightning network.
Pierre Rochard:	31:36	So we can get into lightning network.
Demetri Kofinas:	31:38	No we will, we will.
Pierre Rochard:	31:38	Okay. You keep bringing it up.
Demetri Kofinas:	31:39	By the way this is super hardcore. I'm really happy about this. I haven't had an opportunity to get this nerdy in a very long time. I know we're delighting a certain subsection of my listeners, but I don't want to go down this rabbit hole too far, because I'm not sure where it's going and I don't know where we're going to end up and I want to make sure that we end up in certain good places. You wrote this post titled, "Bitcoin Investment Thesis". I read it. It's from the summer of 2018, and you wrote in part of it, "The strengths associated with openness could be a head wind for cryptoassets as they attempt to become long-term stores of value. The fact that current mainstream crypto-assets are freely available to copy limits their ability to establish uniqueness, a possible precursor for value permanence."
Demetri Kofinas:	32:25	I found this to be a very interesting statement. I want to ask you, is your point that in an open source development environment that without any type of legal protection that first mover advantage is inordinately important and that bitcoin can simply borrow innovations made by anyone else to maintain its advantage? Which by the way brings us to back to why I asked you at the top, what is bitcoin, really? Right? Because is it just the protocol, which can change? Or is it, again, how important do we value the community of developers and miners and HODLers?
Pierre Rochard:	33:03	So yeah. I think the words I use are social consensus, and by that I do mean the community. But also when I think of the community I actually think of a relatively limited number of individuals compared to what the wider social consensus is. And I actually think the wider social consensus of the lambda viewer of CNBC, their perception of what bitcoin is, that's actually even

more important than what the inside baseball people within the bitcoin community think of as bitcoin being.

Demetri Kofinas: 33:31 Well of course, but you're putting the cart before the horse. I mean if those people agreed with the community then there would already be hyperbitcoinization.

Pierre Rochard: 33:39 No, no, no. By that I mean that the layperson who is not intimately familiar with the technology has just an important view of what the social consensus is than the technical developer person. By that, I mean that if you're going on Coinbase to buy bitcoins from Coinbase, it's very important to Coinbase that they sell you bitcoins and that they don't sell you accidentally ... and same for Ethereum, right? They want to sell you ethers, not some knockoff of bitcoin that-

Demetri Kofinas: 34:07 Well that also brings us back to one of the concerns around bitcoin cash and bitcoin when it forked. There are probably people that bought bitcoin cash, in fact I heard about this. People bought bitcoin cash and got together over Christmas and thanksgiving and turned out they thought they owned bitcoin, but they didn't. Right?

Pierre Rochard: 34:22 Right.

Demetri Kofinas: 34:23 But let me stick on this point because it's an important point. It may be important to deal with this impression of culture, but in this open source development even isn't the most important thing the fact that bitcoin has a certain fundamental architecture that works? It's essential, because without that they wouldn't be where they are. But now that they're there, it's not like it's a static piece of code. It can change, it can evolve, right?

Pierre Rochard: 34:48 Yeah. Well and some parts more than others but-

Demetri Kofinas: 34:51 Was that your argument in that? Was that the reason that you made that point? What did you mean by that?

Pierre Rochard: 34:55 On paper bitcoin can take innovations from other coins, and it's open source or not, but that just hasn't happened in practice. In practice we've seen the opposite, where other coins take features that are added to bitcoin and sometimes they get there first because bitcoin's consensus is harder to change that their centralized altcoin is. So the number one aspect of money is liquidity, right? And one of the important features of liquidity is liquidity begets liquidity.

Demetri Kofinas: 35:22 When you say the number one aspect of money is liquidity, what do you mean?

Pierre Rochard: 35:26 It's monetary premium, it's value as a medium of exchange, all of these are synonyms with liquidity.

Demetri Kofinas: 35:33 Right. Because with no liquidity, you can't exchange anything.

Pierre Rochard: 35:36 Right. Right.

Demetri Kofinas: 35:36 Right.

Pierre Rochard: 35:37 So if you kind of rank order all goods and services in society by what is their relative liquidity, from a pack of cigarettes to a U.S. dollar, I see bitcoin as working its way up that totem pole of liquidity. So if we put it back in the context of cryptocurrencies, all these other cryptocurrencies are also claiming that same totem pole of liquidity. And they have been increasing in liquidity and sometimes at a faster rate than bitcoin and sometimes at a slower rate than bitcoin.

Demetri Kofinas: 36:05 The specific point, just to re-emphasize, my question is what did you mean by that openness, which is an asset could also become a headwind for liability?

Pierre Rochard: 36:14 So what we see with other cryptocurrencies is that they take liquidity away from each other. And new ones spring up that promise X, Y, Z feature or A, B, C technology and it means that they are essentially in a dog-eat-dog crab bucket where they never get the critical mass of liquidity needed to challenge bitcoin's dominance in the cryptocurrency space. Meanwhile, bitcoin is, I think, growing the market dramatically, and growing the pie, and some altcoins have grown the pie, but that's really been at the margin compared to the-

Demetri Kofinas: 36:44 But couldn't you also argue that what you would call them as ... I think you would call them shitcoins, right? Couldn't you also make the argument that the proliferation of shitcoins ... I mean case in point, the reason why you're on the show right now is because I see it first hand in the crypto space. You've had a complete blowup of all these "shitcoins" and what have people done? They've clung to the cross. By the way I want to make certain religious allusions, certain religious metaphors about bitcoin, because I think they're meaningful and relevant, and I don't mean them to poke fun. Or I could be poking fun, but I'm not trying to be derisive. I actually genuinely believe that there is an element of faith, and in fact to go back to this point about

demand side, I actually think that bitcoin's value is a significant amount, if not the majority of that, is the faith of its HODLers.

Pierre Rochard: 37:32   I 100% agree with you, and I use religion all the time because religion is also a social consensus. We actually see some of the same kind of ... So if you look at Protestants and Catholics, you can say, "Well that's bitcoin and bitcoin cash." You see the similar kinds of splinterings and the antagonism between each other as they have different visions of what respectively ... yeah.

Demetri Kofinas: 37:53   So a bitcoin is the church. The founding church.

Pierre Rochard: 37:57   A dogma.

Demetri Kofinas: 37:57   And there are these little cults that spring up, and when the flood comes and these cults disappear, it only strengthens the religious fervor in the community and people come back to clutch the cross, right? I mean that is in a sense what I have seen. There is a clutching of the cross, and I think the Bitcoin Maximalist movement, much of the conversations, it's made me laugh, and again, I don't mean this in a disparaging way, I listened to a conversation that had me cracking up with you and the Lebanese economist-

Pierre Rochard: 38:23   Saifedean Ammous? Yeah.

Demetri Kofinas: 38:24   And I laughed so hard when he would talk so disparagingly about these altcoins as shitcoiners. Shitcoiners. And he's like, "Shitcoiners, nocoiners." And the conversations for me sound very much about redundancy around the faith, reminding people to hold on to their coins and ... Again, I don't mean it derisively, there is a type of indoctrination, but that may be something that's necessarily for something like this to actually succeed. So again, I don't mean it derisively, I just want to point that out.

Pierre Rochard: 38:54   So you mentioned that there has been a resurgence of Bitcoin Maximalism due to the bare market and I think that it's because when the market is going down, that's when you really test the true liquidity of these coins. So if you can't market sell 50 thousand dollars' worth of this altcoin without driving it down 50% in value, you know massive slippage, then it's extremely liquid and you realize the folly of what you were trying to do by participating in that market for that shitcoin. So that's where I think the people realize that bitcoin really is far more liquid than these altcoins. Because it's easy to get carried away in the bull market and look at your portfolio and say, "Here's a highly liquid

		portfolio of altcoins." It's not until the bare market that you see what actually has liquidity.
Demetri Kofinas:	39:44	Yeah. I'm also blow away by a lot of ... I think there were over 4000 of those things, right? And we actually did an episode, a special episode that I released for the audience over the weekend on the ETC, the 51% and I just don't understand why anyone would hold that. Why anyone would want that. It's just confusing. Again, we have limited amount of time so I don't want to go too far down the turtle shell, rabbit hole fractal.
Demetri Kofinas:	40:11	Let's go to another term which I think is used so much and overused by almost everyone, which is decentralization. What is decentralization and more importantly, how do you measure the extent of something's decentralization?
Pierre Rochard:	40:27	So to me, decentralization is are you able to verify that payments being sent to you are following the rules for the consensus that you are signed up for. So essentially, that means having the ability to run a full node, a node that is verifying that transactions that you are receiving are valid, and then that they are getting included in valid blocks. Whether that means for bitcoin or of Litecoin, or for bitcoin cash or for Ethereum. It means that you can run a full node that is verifying all the rules that are part of that coin's consensus.
Demetri Kofinas:	41:00	And anyone can run a full node?
Pierre Rochard:	41:03	Right. So then we run into the empirical question of how many people are running a full node, and how many people are using it to verify their transactions that they're receiving, and that to me is the theoretical measure of decentralization would be, you know, if we take a rough heuristic of what percentage of the holders of cryptocurrency actually verified that they're holdings were in the blockchain?
Demetri Kofinas:	41:28	So one element of this is the ability for anyone to join the network? That's one aspect of the decentralization, right? How much computing power is required to run a node?
Pierre Rochard:	41:36	Very little. It's like opening a web browser.
Demetri Kofinas:	41:39	Okay. Point being, how many people are actually engaged in the function of mining, right?
Pierre Rochard:	41:45	Well so there's two different things, so-

Demetri Kofinas:	41:47	And this is specific to bitcoin because you guys use proof of work.
Pierre Rochard:	41:51	Right, right. Although there aren't any major proof of state coins and, well, the ones that are --
Demetri Kofinas:	41:57	Ethereum wants to and I think EOS also uses proof of state.
Pierre Rochard:	42:01	Yeah. XRP uses neither really and it's just centralized shitcoin.
Demetri Kofinas:	42:05	But it's more of a permissioned network.
Pierre Rochard:	42:06	Yeah. You know, you're going to get a lot of hate from the XRP army on Twitter over this. Yes.
Demetri Kofinas:	42:12	I've heard there's something out there. Who is it Ryan Selkis usually catches a lot of heat for saying stuff about XRP.
Pierre Rochard:	42:17	Yeah. A lot of controversy there.
Demetri Kofinas:	42:18	I don't know much about it.
Pierre Rochard:	42:18	But I do want to get to the distinction between a node and mining, but before that I actually want to amend an answer I had for you as to the cost of running a node, the computational power. There is a process by which you catch up to the current state of the system. So you start with block 0 and then you verify all the blocks, I think we're up to block ... we're at like 555 thousand blocks, so that part is computationally intensive, but really if you've got a good computer it will only take you six hours. And at that point, as each block comes in every 10 minutes, it only takes up very little computational power.
Demetri Kofinas:	42:51	Before we go there to the thing about node and computational power, I want to actually go a little further out in this notion of decentralization. Because I think about decentralization in terms of power, in terms of the dispersion of power across a network, right?
Pierre Rochard:	43:07	Right.
Demetri Kofinas:	43:07	That's how I think of it. Do you not think of it that way?
Pierre Rochard:	43:09	Well I think that using a node is exercising power, and it's the only effective form of power in these systems is-

Demetri Kofinas: 43:16 But you can be an individual working as part of a collective, in which case you've centralized, right? Because if I cooperate with another million people to attack the network, that's a centralization, right? Even though we're all individuals, that may be very practically different to do, but my point is, isn't it about coordination and coordination and accumulation and centralization of power, and purpose? I mean this is a philosophical point I want to try and make, because it's something I don't have an answer to and I want to free think it with you.

Pierre Rochard: 43:51 Yeah, I mean if that happened, I wouldn't really consider that an attack, it's bitcoin changing. So if there's a bunch of-

Demetri Kofinas: 43:58 That's an interesting point.

Pierre Rochard: 43:58 Right? Because if you convince all of the bitcoiners to change the rules in bitcoin and you persuade them one by one, I don't see that as an attack, I see that as that's just how we upgrade bitcoin.

Demetri Kofinas: 44:09 That's an interesting point. So it really is about agency, individual participation in the network.

Pierre Rochard: 44:15 Right exactly. So there's a very strong tension there though, because there's the social consensus, right? Which is like you were saying joining a bigger group, and then there's the individualism and your ability to express your own views on things. So if you step outside of the consensus of what bitcoin is, you create an altcoin. So that's what happened with bitcoin cash. And if you stay within it, you're limiting your own ability to change the protocol rules, and I kind of see it the same way that statists view the social contract, is that you avoid the state of nature of being on an island where there's no division of labor, and you agree to follow specific rules of the bitcoin protocol so that you can participate in this wider community.

Demetri Kofinas: 45:01 Let me ask you something else. There is a distinction in the United States between a republic and democracy, right? Ancient Athens was direct democracy, of course you couldn't be a slave and you have to be a man. But there is a distinction between the two, and in the United States there's this idea that we have a Bill of Rights and the majority cannot take those away, right? So I want to go back again, to that point which is that now were defining decentralization as the disbursement across the network in a very democratic way. But then what does that mean in terms of the rights of the users on the network, and the

security of those users. Is security, in your view, synonymous with decentralization?

Demetri Kofinas: 45:41 The more decentralized the network, the more secure the property?

Pierre Rochard: 45:45 It is, when I think of security- Well when I think of security, I think of you being able to secure your private keys. So that's kind of a different issue than if you think of it more at the network level. And then the network level I think of security as issues like denial of service attacks and attempts to sabotage nodes and to take [crosstalk 00:46:05]

Demetri Kofinas: 46:03 And immutability is what I'm getting at also.

Pierre Rochard: 46:05 Well the immutability, there you get into what's written into the code, right? And what the specific code says. The code has had bugs in the past that meant that the social consensus rules were out of line with the code that was actually being run on the network. So at that point, it's kind of on the code to be congruent with the social consensus. I think that if we go back to our comparison to republican democracy, the challenge here is that we're dealing with a different form of governance entirely, is network governance. So if we were to apply it to real life, it's like if you were able to live in a world where at the drop of a hat, you can remove all of the assault rifles in the United States, and you can live in that country, but that actually does not disturb the guy in Texas who loves assault rifles. He actually lives in a parallel country that still has assault rifles. So you can exist in both countries.

Pierre Rochard: 46:57 So that's kind of how network governance works, where when bitcoin split into bitcoin and bitcoin cash, everyone still owned bitcoin and everyone still owned bitcoin cash, and they were just on two parallel networks with different rules. So it's not like in a democracy where the majority can impose its will on the minority, the minority can always leave, and there's a very low cost to leaving. The biggest cost to leaving is the liquidity hit, right? Which is the ... you can be splitting the liquidity between these two networks.

Demetri Kofinas: 47:27 It's almost kind of like punishment or the-

Pierre Rochard: 47:30 A voice in exit.

Demetri Kofinas: 47:31 Yeah. Exactly. What's that called? Exile.

Pierre Rochard:	47:34	Yeah.
Demetri Kofinas:	47:34	There's exile from the city.
Pierre Rochard:	47:36	Self-inflicted. There's no one kicking you out, it's you kicking yourself out.
Demetri Kofinas:	47:40	Right. I was going to use the example and then I pulled back when you said that, I was going to use the example, the tyranny of the majority of the murder of Socrates in Athens, right? But actually that doesn't hold. They would have had to banish him from the city. Actually they gave him that choice and he chose death over exile.
Pierre Rochard:	47:54	Well all the Athenians could have lived in a city that had him, then all the Athenians could also have lived in a city that didn't have him.
Demetri Kofinas:	48:00	See now you're taking [crosstalk 00:48:04]
Pierre Rochard:	48:01	That's quantum parallel [crosstalk 00:48:04]
Demetri Kofinas:	48:03	I was trying to make it more workable.
Pierre Rochard:	48:05	And that's the difficulty of this network governance, and that's why it's been so hard for people to wrap their minds around it.
Demetri Kofinas:	48:09	You know that reminds me of a conversation I had with Bruce Schneider where I was trying to create a metaphor to talk about cyber war, and I was using world war one and the Schlieffen Plan and he said, well you know ... How did he say it? I love the way he said it. He said, "Metaphors are hard because computers are different." I love that. I mean that really has stuck with me and it's true, and this is the challenge of trying to explain this, and also, I'm trying to do my best here and also to understand certain things. There's this meme, I don't know if you would call that a meme, it's a phrase that travels in the-
Pierre Rochard:	48:39	No I love memes.
Demetri Kofinas:	48:40	Yeah. There's this phrase that travels around in the crypto space which I really love and I think it's borrowed from entrepreneurship, which is failing to scale versus scaling to fail. I think this is one of the best phrases that I've come across. To highlight the problem or this challenge, right? This challenge between scaling the network, but also making it secure as a store of value. So I understand it, transaction throughput on the

bitcoin network is limited by two things, block size and the difficulty of solving reverse hash for the purposes of leader election and civil resistance.

Pierre Rochard: 49:20 Yes.

Demetri Kofinas: 49:21 Right? Which is the proof of work. One of the advantages and the limitations of the current protocol, and how bitcoin's technology works.

Pierre Rochard: 49:30 Yeah so, the main limitation is that it's a global broadcast system, and it has to maintain global consensus. So by that I mean, we just discussed running your own node and that giving you sovereignty over the system, and a system where no one is sovereign and everyone is sovereign at the same time. So that aspect of it, it gets increasingly expensive to run your own node the more transactions are going through the system. So that's why we have this box size limit. But really if we step back and look at the macro economics of bitcoin, the biggest danger to bitcoin is that it's long-term hash-rate is too low. Let's get into the 21 million bitcoins.

Pierre Rochard: 50:12 Currently every new bitcoin goes to a miner, and that miner is performing this proof of work function, this time stamping function, so that's how they're getting rewarded for that today. That's why you have statistical finality after six blocks or so that your-

Demetri Kofinas: 50:27 Probabilistic consensus.

Pierre Rochard: 50:28 Yeah exactly. And so, right now the rule of thumb is six confirmations, but really there's a number of variables that go into whether six is an appropriate number for you or not. The lower the value, the fewer confirmations you need. So for lightning for example, you-

Demetri Kofinas: 50:42 It's a qualitative.

Pierre Rochard: 50:43 Yeah.

Demetri Kofinas: 50:43 It's subjective.

Pierre Rochard: 50:44 It is. And it also would depend on how much you trust the other person. But as the inflation of bitcoin decreases, as we approach that 21 million total bitcoins, that the amount-

Demetri Kofinas: 50:56 How many did you say we're at now?

Pierre Rochard:	50:57	We're at 18 million or so.
Demetri Kofinas:	50:58	Okay.
Pierre Rochard:	51:00	And it's about 4%, 3% increase per year right now. Then the next halving is in 2020. So at that point we go, I think it's from 6.5 to 3.25 or 12 to ... anyway. So as the halving's keep happening, then less and less revenue is going to miners and so the hash rate, you know, in equilibrium would be falling and that means that we have to wait longer and longer, so that six-
Demetri Kofinas:	51:22	Latency increases.
Pierre Rochard:	51:24	Right. So the six confirmations rule of thumb would become 60, would become 600, become 6000. So a danger for the system in a sense that it actually impacts the reliability of layer 2 solutions, and it impacts the usability of the system.
Demetri Kofinas:	51:36	Because the layer 2 solutions will have to go longer before reconciling on the main chain.
Pierre Rochard:	51:39	Right.
Demetri Kofinas:	51:40	Is that the reason?
Pierre Rochard:	51:40	Exactly. So the solution to that, and Satoshi talked about this in the white paper, is to replace the inflationary mining award with a mining reward from transaction fees. So every transaction would contribute a certain amount in fees to rewarding the miner for mining a block. So from there you can kind of think about, "All right well we want to maximize transaction fee revenue if we want to maintain the properties of bitcoin, otherwise it won't be enough to make up for the lack of new bitcoin creation." Right? So there's two ways of doing that. One is by having a lot of transactions with a very low transaction fee, and then the alternative is to have very few transactions with a very high transaction fee, or some mix.
Demetri Kofinas:	52:25	So that has to do with block size?
Pierre Rochard:	52:27	Right.
Demetri Kofinas:	52:27	Is that right?
Pierre Rochard:	52:28	So I think that the solution of having a lot of transactions with a low transaction fee doesn't work because it causes the system

		to centralize. So we have to with the alternative of having very high transaction fees with very few-
Demetri Kofinas:	52:41	Can you explain why it causes the system to centralize?
Pierre Rochard:	52:43	Because you're dramatically increasing the cost of running a full node and so at some point you only have miners running full nodes, and even they don't need to be running full nodes, so it becomes easy for governments to identify, what are the 12 nodes that define the-
Demetri Kofinas:	52:58	Isn't there also an issue, the way I'm imagining, correct me if I'm wrong, isn't there also an issue about the software being able to actually identify which chain to build on if your blocks are too small?
Pierre Rochard:	53:09	No. That wouldn't be impacted.
Demetri Kofinas:	53:10	Okay. All right so there are limits to scale. Regardless, I think the main interesting thing I've taken away from this conversation is the acknowledgement by the bitcoin community that there are limits to scale, but that's not the point. The point isn't that layer 1, that this space layer protocol has scaling limitations, the point is that ... What matters is, the hard money aspects of this, and that you can build multiple layers on top of it, just like we have in the modern banking system, but that you have this base layer, which is immutable, and which has, again to bring us back to this point, a supply schedule that is deflationary, which is what is so unique about bitcoin and that you can build a system on top of it that does the same things that the current financial system does. Right?
Pierre Rochard:	54:00	That's right.
Demetri Kofinas:	54:01	It's basically digital gold. I mean the bottom line is that the thing that I've taken away from the arguments in the bitcoin community is that ultimately all bitcoin really is, is it is gold for a digital economy and a digital universe.
Pierre Rochard:	54:18	It's programmable, it's scarce, yeah.
Demetri Kofinas:	54:20	That's what it is right?
Pierre Rochard:	54:21	Yeah.
Demetri Kofinas:	54:21	Except the difference being that unlike gold, you actually know what the supply is.

Pierre Rochard:	54:25	And I think it has a better supply schedule than gold does. Gold continues to get mined at a steady clip out of the earth. So I think that bitcoin actually has an advantage there as well.
Demetri Kofinas:	54:35	It's a really interesting argument. Anyway, we can spend a lot of time on it. It's interesting. That a lot of aspects that are fascinating to explore as well as ... You know, we could bring it back to the gold argument, you know we are analog creatures. We're in this world where everyone is kind of obsessed with futurism, the singularity, and a lot of people think they're going to live forever, but you know, are we getting a little ahead of ourselves? Gold has a 5000 year history. This actually brings us forward to something else, which is the Lindy effect, which is used a lot in this community. But before we get there, maybe I want to ask you quickly, what do you think about some of these alternatives solutions to scale like proof of stake and also implementations like EOS and Ethereum's Casper? Which they haven't implemented yet, but we've done, I think you might have heard it with Vlad and Vitalik on the Friendly Finality Gadget (FFG) and Correct by Consensus (CBC).
Pierre Rochard:	55:25	So I don't see those as scaling technologies. They really are about different consensus mechanisms, and so-
Demetri Kofinas:	55:32	Doesn't the consensus mechanism enable the system to scale in a way they wouldn't otherwise?
Pierre Rochard:	55:36	Well, no because you still have to verifying all of the rules and be transmitting all of this data. So when I say that bitcoin doesn't scale, by that I mean that our broadband internet connections are not increasing in speed enough for bitcoin to scale. It's kind of a shorthand way ... When people say bitcoin doesn't scale, it's entirely due to our internet speeds. So if we get fiber optic connections to every single human being in the world, then-
Demetri Kofinas:	56:02	Would it still take 10 minutes to add a one megabyte block?
Pierre Rochard:	56:05	But you could add a one gigabyte block every 10 minutes. You've just dramatically increased the throughput on the base layer.
Demetri Kofinas:	56:13	What are the disadvantages of expanding block size?
Pierre Rochard:	56:16	For an increasing number of people it becomes impossible to run a full node because their internet connection is not fast enough, or their computer hardware is too slow. In practice, it's

generally the internet connection that's an issue. So I think that we'll be able to increase the block size limit significantly as the propagation of fiber and of 5G LTE increases.

Demetri Kofinas: 56:37 What type of performance would you get at a one gigabyte block size?

Pierre Rochard: 56:43 Well I mean it's kind of linear, so if we have eight transactions per second today with one megabyte block size, then you know, multiply that by 1000, 8000 transactions per second. But really, I wouldn't necessarily see that as being particularly interesting, especially compared to other ways of sending value using layer 2 with lightning.

Demetri Kofinas: 57:02 So Pierre, I want you to stick around, we're going to do the second half for our subscribers. We're going to get into hyperbitcoinization, the Lindy effect. We're going to get into survivability gold, questions of governance, the lightning network, and I also want to get your predictions for the cryptomarket as well as the broader markets. And for you listeners, you can subscribe to our overtime feed, as well as our rundowns and transcripts either through the website in the actual individual episode page, where you can click on the tabs for overtime, rundown, and transcripts. Or directly through Patreon at patreon.com/hiddenforces. We integrate Patreon's backend into our site so that content is available both on our website and through Patreon. So we'll hope to see you there.

Demetri Kofinas: 57:52 And that was my episode with Pierre Rochard. I want to thank Pierre for being on my program. Today's episode of Hidden Forces was recorded at Edge studio in New York City. For more information about this week's episode, or if you want easy access to related programming, visit our website at hiddenforces.io and subscribe to our free email list. If you want access to overtime segments, episode transcripts and show rundowns, full of links and detailed information related to each and every episode, check out our premium subscription available through the Hidden Forces website, or through our Patreon page.

Demetri Kofinas: 58:34 Today's episode was produced by me and edited by Stylianos Nicolaou. For more episodes you can check out our website at hiddenforces.io. Join the conversation at Facebook, Twitter, and Instagram at @Hiddenforcespod or send me an email.

Demetri Kofinas: 58:55 As always, thanks for listening. We'll see you next week.