The Bitcoin FAQ with Bradley Rettler

Hosted by: Mark Stephany

[00:00:00] **Bradley Rettler:** I hope that through this two hours and 40 minutes, or whatever it turns out to be on the podcast, that people have been able to understand Bitcoin in a way that they didn't before – that it's gone beyond headlines, and that they've also been able maybe to put themselves into the position of people who might find this valuable: people who are living in authoritarian regimes, or with devaluing currencies – and see why progressives, who are supposed to care about these people, might find value in the Bitcoin network.

[00:00:39] Welcome to the Progressive Bitcoiner podcast where we explore the intersection of Bitcoin and progressive issues. I'm your host Mark Stephany.

Jump to a Question:

[00:00:52] **Mark Stephany:** This episode is an FAQ about Bitcoin with Bradley Rettler. Bradley is a philosophy professor at the University of Wyoming. When he's not wrangling cattle with his bare hands and welcoming the droves of undergrads to his office hours, he is writing some of the best work on Bitcoin that is out there. I am grateful for the over two hours he spent with me going through all the questions we could think of that not only someone new to Bitcoin would want to know, but also for those who are more familiar with Bitcoin; you will undoubtedly pick up some new things to consider from the wealth of Bitcoin knowledge that is Bradley Rettler.

[00:01:41] Bradley Rettler, thank you so much for joining me on the progressive Bitcoiner podcast. So happy to have you!

[00:01:46] **Bradley Rettler:** Happy to be here. Thank you.

[00:01:49] **Mark Stephany:** So this is going to be a podcast where we go through some of the most frequently asked questions with regard to Bitcoin, both the technical side, as well as questions that people have – concerns with – regarding Bitcoin.

[00:02:03] **What I want to ask you first is: do you have a general approach by which to look at Bitcoin? From a more objective standpoint?**

[00:02:10] **Bradley Rettler:** Yeah, I think a lot of people rush to judgment about things that they don't know too much about based on their experiences and identity. And I think very often we tend to look at just how things affect us and not how they can affect other people.

[00:02:31] And there are a great many people who Bitcoin harms and there are a lot of people that Bitcoin helps. And the question is, is it more important for the people that Bitcoin harms to be helped or is it more important that the people Bitcoin helps to be helped? So that's kind of a long-winded way of saying: the kind of people that Bitcoin helps may not be the kind of people that listen to this podcast.

[00:02:57] It depends on your financial situation. It depends on what country you live in. It depends on who your government is and how much you trust them and how good a care of you they take. And for people who are doing well, Bitcoin may not help you, or it may only help you a little. But for people who are being mistreated by their government, for people who live in countries with hyperinflating, or even just rapidly inflating, local currencies, these are people that Bitcoin helps a lot.

[00:03:31] So when you're thinking about your overall evaluation of Bitcoin, I think it's tempting to just look at how it affects you. But I think the most important thing to do is to try to get inside the mindset of people who aren't very much like you, but who might be helped – like Russian dissidents, for example, or Belarusian protesters, Venezuelan economics professors, Afghan women entrepreneurs, Nigerian feminists, North Korean revolutionaries. These are all people who have used Bitcoin to either evade the control of their authoritarian government or to store their wealth in a currency that's more stable than their local currency. And these are just some of the examples. So as you hear about the features of Bitcoin, try not to just think about how it could fit into your life, but try to think about how it could fit into the lives of people who aren't very much like you.

[00:04:30] **Mark Stephany:** Thank you. So we are going to start off with the simple question of "what is Bitcoin?" and go from there, with increasing complexity of questions. **So let's get right into it. Bradley, what is Bitcoin?**

[00:04:43] **Bradley Rettler:** The word "Bitcoin" can mean at least two things. When you ask someone, "Do you have any bitcoin?", you're referring to a digital asset. When you ask someone, "Do you think Bitcoin is good for the world?", or when I say, "Governments should invest in Bitcoin", I'm referring to the network. The network exists to track the asset – the Bitcoin network tracks

bitcoin, the asset. At its core, the Bitcoin network exists to keep up a ledger, which records where all of the bitcoin (the asset) presently is and where it most recently came from. The records on the ledger go all the way back to the beginning, 2009, and come all the way up to the present.

[00:05:30] And they're organized in blocks with a new block being added every 10 minutes. A new block has been added roughly every 10 minutes since 2009. Each block contains roughly 4,000 transactions, or the data for roughly 4,000 transactions. It takes about two megabytes of space. This might seem a little confusing. We're used to, you know, if someone owes you $5, you give them a $5 bill. There's like this piece of paper and it moves around and it changes hands; it's sent and it's received. So you might try to think of bitcoin like that, like these little digital bits that move around. But that's not how Bitcoin works.

[00:06:14] That's not how the US dollar works anymore! In its modern digital form. When you deposit a check from your employer, the bank doesn't physically take any cash and like put it in a box for you or anything. It just increases the number of your bank account balance. And then your employer's bank decreases the number on their bank account balance.

[00:06:36] And Bitcoin isn't exactly a balance-based or account-based ledger, but it works pretty similar to that. There aren't bitcoins, there aren't fractions of bitcoins. There aren't these discreet little digital things moving around from computer to computer. There's just a record of transactions.

[00:06:55] And from that record of transactions, you can deduce the amount of bitcoin right now at any address in the ledger. So, as I said, Bitcoin exists to keep up a ledger; but more accurately, it exists to keep a bunch of ledgers – a bunch of records of transactions. One reason for the invention of Bitcoin was that the inventor, who went by the pseudonym "Satoshi Nakamoto", didn't trust banks, didn't trust corporations to keep honest ledgers, and didn't think we had to trust them even if they were trustworthy.

[00:07:31] So Satoshi's idea was for everyone to have a copy of the ledger, anyone who has a full copy of the ledger is running what's called a "full node". And anyone who has a computer that has an internet connection and like 325 gigs of hard drive space can run a full node and keep a copy of the ledger.

[00:07:52] Of course, this is no good if everyone has a different ledger – if everyone's ledger has different records of transactions. The copies all have to agree. So Satoshi put in place a system – an ironclad system – for determining

how to update your copy of the ledger with a new block of transactions, such that every ledger would have identical copies of blocks.

[00:08:15] So everyone who wants to publish the next block has to solve a math problem by trial and error. And only one person will be the first to solve that math problem. And when they solve it, they send out the answer to all of the full nodes – all of the people that have copies of the ledger. They send out the answer as well as the next block of transactions.

[00:08:38] It takes trillions and trillions of calculations right now to get the answer to this math problem because you have to do it by trial and error, but it takes only one calculation to verify. So the nodes verify the answer, and then they add that block to their copy of the ledger and the miners – the publishers, the people who want to publish the next block – are off and running on the solution to the next problem.

[00:09:03] So in the end, we have billions potentially (hundreds of thousands, actually) of identical copies of a ledger that's composed of every Bitcoin transaction that's ever occurred. They are identical because nodes are constantly checking with each other to make sure they all have the same copies of the transactions – but no one node has to trust any other one node.

[00:09:27] The trust is distributed across all of the people who are running the nodes and across the protocol itself. So real quick before I move on, because this is all kind of complicated, here's how it works from the user end, assuming that you have the private key, which is basically like a password to an address that has some bitcoin.

[00:09:49] So you decide you want to broadcast a transaction – you want to put some of that bitcoin at another address. You broadcast to the full nodes the public address from which the Bitcoin's going to go, and the private key to that address, and the amount. The nodes check that the private key and the address match, they check that the address has enough bitcoin – at least as much as what you want to send – and that you're not trying to spend the bitcoin twice.

[00:10:18] (So you're not broadcasting two distinct transactions that use up all the balance of the address.) If that all checks out, they forward it to the miners to include it in the next book. When some minor gets the math problem right, assuming that they've been sent your transaction by a node, they broadcast the answer to the math problem and a block that includes your transaction in the block.

[00:10:44] And that's it. Every node updates the ledger, and the bitcoin is at the new address. More practically, probably what you do is you open a wallet app on your phone, you scan a QR code or you copy and paste an address, you specify an amount of bitcoin, you press a big green button or something, and that's it. Everything that I've been describing is what happens under the surface when you do that.

[00:11:08] **Mark Stephany:** we will get into bitcoin the asset a little bit later, but I want to add a few more points here. One, I think a misconception is Bitcoin just popped out of nowhere in 2008, 2009. And that's not necessarily the case, correct? It's based on decades of cryptography work and previous iterations of digital cash. Bitcoin, as I explained to my 72-year-old mom, is simply computer code. It's a protocol just like the internet is based upon, but it is a protocol for a digital cash. And described simply it is open, meaning it is open source. It is permissionless, meaning you don't need a credit score or an identity or a perfect record to be able to use it. It is non-confiscatable, meaning nobody can take it from you. It is portable; you can take it across borders. And it is disinflationary, meaning no more will be created after 21 million.

[00:12:13] These are further details that we get into with additional questions, but for now let's move on to **who created Bitcoin? Who is Satoshi Nakamoto and is his anonymity a problem?**

[00:12:26] **Bradley Rettler:** You've answered the first question with the second, which is nobody knows. There are guesses at who Satoshi Nakamoto might be. It's pretty clearly a pen name. Some overzealous journalists found a person named Satoshi Nakamoto and declared that person *the* Satoshi Nakamoto, which turned out not to be even close to true or well-supported by any kind of evidence and it ruined the guy's life for quite a while. So I don't know who it is.

[00:12:57] I don't even have speculations about who it might be. And I think that's a good thing. I think that if Satoshi were around, it might be the case that too much emphasis is put on Satoshi's opinions over what should happen to the Bitcoin protocol. So even though the Bitcoin protocol was introduced in 2009, there have been updates to it at various times.

[00:13:20] People put in requests for different features and there are upgrades that happen. And the way that they occur is that they have to be accepted by the community, which means that the full nodes – people who are running this entire ledger that we talked about earlier – have to (all or most) agree to run this upgrade. And if they don't, it just doesn't get done. In this sense, Bitcoin is democratic in a way that no other money is. The way to change anything about

it is to convince people who use it that that thing needs to be changed. And there's no voice right now that speaks out any more strongly about it than any other voice.

[00:14:04] The decision about whether to change any parts of it have to be made by people giving good arguments, good reasons. They have to explain what the upgrade is and why it's important and why it's valuable.

[00:14:18] **Mark Stephany:** So the last known communication from this person or persons was in 2011 and is often cited as a potential concern. If Satoshi were to come back, what would happen? Would that cause the price to drop? **If Satoshi were to cash out his thousands or millions of bitcoin, would that be a problem? What is your opinion on that scenario?**

[00:14:41] **Bradley Rettler:** Yeah, right now there are over a million bitcoin that are presumed lost because they're owned by Satoshi and they haven't been moved since, you know, maybe ever. And if any of those bitcoin were to move, it would be presumed that they were moved by Satoshi. And so we would presume that Satoshi has access to all of the bitcoin that are presumed to be lost and owned by Satoshi. And so, although we operate with this idea that there are 18 million (roughly) bitcoin in circulation right now, there'll be a hard cap of 21 million, we also sorta think that there's like one to 3 million less bitcoin than have come into existence because the one to 3 million are on spendable. Were some of them to be spent, we might have to presume that the rest of them could be spent, and the supply grows larger than we think. And I do think that that would have an impact on the price of bitcoin.

[00:15:40] It would go down.

[00:15:42] **Mark Stephany:** Yeah. Most certainly it would, but arguably temporarily, because it doesn't change anything about the protocol itself. **We often think of bitcoin as just magic internet money. Why is it so special? Why is Bitcoin so innovative? What computer science problem did it solve?**

[00:16:00] **Bradley Rettler:** It solved a couple computer science problems, some more complicated than others and so some I don't want to get into. There's a well-known problem in computer science called the “Byzantine Generals Problem”, which is a question about how to coordinate among people who can't talk face-to-face – can only send messages to and from each other – and where we presume that at least one of the people is going to be dishonest and so pass false messages. Bitcoin, with the way that the ledger works, the nodes and miners are constantly passing messages around about transactions and whether

they're valid or not. Bitcoin is designed to work even if up to 49% of them, maybe 50%, are being dishonest. So you have to solve this problem of how to handle dishonest communication. The result is pretty technical so I don't want to get into that. I think the more interesting problem than it solved was digital cash. So we had, prior to the existence of Bitcoin, several different systems of digital cash. But the base problem with digital cash is pretty easy to see, which is that anything digital can be copied very easily. It's not easy to copy paintings. It's not easy to copy oil. It's perhaps impossible to copy those things. But any digital objects can be copied and recreated with no loss of content whatsoever. So if digital cash was like physical cash and it was, for example, a picture, it would be way too easy to duplicate that picture. You get one $5 bill and all of a sudden you can make as many $5 bills as you want and send them around anywhere. Bitcoin was, I think, largely created to solve the problem of double spending. How do you know that someone who received five digital dollars didn't send that five digital dollars to two people or 10 people or a hundred people? By using this ledger and by using this chain of blocks – by using the procedure that we talked about at the beginning for creating new blocks and adding them to the chain, adding them to the ledger – Bitcoin solved this problem. If you spend bitcoin, you cannot spend it again. And that's kind of the ingenious innovation of Bitcoin in my mind.

[00:18:37] **Mark Stephany:** Bitcoin utilizes something called Proof of Work, which we'll get to later. But the specific iteration of that was designed for the Bitcoin protocol to allow it to become more decentralized. **Why was the decentralized component of Bitcoin so important as an innovation?**

[00:18:56] **Bradley Rettler:** I think for a couple of reasons. One of the reasons was that Satoshi didn't trust huge corporations, didn't trust governments, and didn't want to *have to* trust individuals that they didn't know. So by decentralizing the network and by giving it a system where as long as half of the people were being honest, the system would function, it removed the need to trust any of these people.

[00:19:22]. So you're trusting the network and you're trusting that at least 50% of the network is trying to be honest. Then Satoshi tried to incentivize every participant in the network to be an honest participant. If you don't control at least 51% of the network, you're not really incentivized to try to be dishonest because it's not going to work.

[00:19:47] You're incentivized to be honest, because then you'll gain some rewards from it. So the decentralization prevents any one person or any group of

people or any corporation or any government from being able to manipulate the network dishonestly.

[00:20:06] **Mark Stephany:** One of the things that are specific to digital forms of money are the trade-offs between security, decentralization, and speed. Which variables to maximize is a design choice. It's currently impossible to maximize all three of those. Bitcoin prioritized security and decentralization over speed. The rationale being that if you're going to be a global settlement layer, security and decentralization are more important, arguably, since we already have speed solved by some of the other networks such as Visa, et cetera, available. So that is something to keep in mind when we are talking about Bitcoin, as it relates to other cryptocurrencies out there that may say that they are "better" than Bitcoin. It was a very intentional reason that security and decentralization were chosen as priorities for Bitcoin.

[00:21:16] **Moving on to Bitcoin's distribution, the 21 million bitcoin. How were bitcoin initially distributed out of the gate? And how will they continue to be distributed? Was the initial distribution fair?**

[00:21:21] **Bradley Rettler:** Before Bitcoin came into existence – as a protocol or as a ledger or as an asset – it was an idea, and it was an idea that was discussed on a mailing list of cypherpunks – people who saw the increasing threat to privacy that Big Data offered – and wanted to try to guard against that. And so they were developing a variety of things, like public key cryptography and things like that. Satoshi was in conversation with the people on this mailing list and sent out an email saying "I've developed this thing. It's going to be a digital cash."

[00:22:06] They [sic: Satoshi], sent the white paper around, sent the software beforehand and said, "Anyone who wants to run this can run this. Here's the date where it's going to start." And anyone on that mailing list could have started running Bitcoin from the very first moment that it existed. No bitcoin, as I said before, existed prior to that. Satoshi didn't keep a certain amount for themselves; the very first bitcoin that came into existence came into existence with the very first block that was mined. That block was mined by Sathosi. It had no transactions, because there was no bitcoin to transact with prior to it. And interestingly, it's unspendable. So, not only could anyone have started running it right away and have competed for this, but perhaps by design (perhaps not – Satoshi never talked about this), the block reward for the first Bitcoin block, which was 50 bitcoin, is unspendable.

[00:23:05] It would require a hard fork to the Bitcoin protocol – that is, rules that are incompatible with the current rules – in order for that to become spendable. So Satoshi almost went out of their way to make sure that this was going to be as fair as possible. And Satoshi wasn't the only person running Bitcoin early on.

[00:23:27] Hal Finney, who was another cypher punk at the time, started running Bitcoin very shortly after. The first known Bitcoin transaction was between Satoshi and Hal Finney. So, anyone could have started competing as early as they wanted. You know, a lot of us probably heard the word "Bitcoin" in 2009, 2010 – especially if you were in any way involved with a university or computer games or anything like that. You probably heard something about it and you [00:24:00] could have gone online and downloaded the software. And at that time you could win Bitcoin blocks just by using your desktop or laptop computer to mine.

[00:24:11] This is in stark contrast to a bunch of the cryptocurrencies that have come into existence since then. For example, prior to the first block on the Ethereum blockchain, there were already 72 million ETH, the native asset of the Ethereum blockchain, that were owned, 60 million that were exchanged for bitcoin.

[00:24:36] There was a website that you could go on and you could exchange a certain amount of bitcoin for a certain amount of ETH, at the time, and 60 million ETH were acquired that way. 6 million were set aside for developers and 6 million were set aside for the Ethereum Foundation. Right now there are 120 million.

[00:24:58] So more than half of the current supply of ETH was owned by people prior to the first block of the Ethereum blockchain ever being mined. So, Bitcoin is unique in the way that it was initially distributed, in that people knew about it beforehand and anyone could participate from the beginning.

[00:25:18] **Mark Stephany:** I think it's important to emphasize what you said earlier – that Satoshi was very cognizant of this. And I think went out of his or her, their way to distribute it to as many people as possible early on. Additionally, when you had people involved with this space within a few years, you had things like Bitcoin Faucet come up where you could quite literally get bitcoin for free on a particular website.

[00:25:48] And so a common critique of Bitcoin is that distribution was not fair. But to that concern, I would say: what is fair? Compared to what else?

Compared to Ethereum where there was a pre-mine? Where, there was clearly a withholding of Ethereum for the founders? That's in contrast to how bitcoin was distributed.

[00:26:15] Additionally, I think it's also important to point out that ownership of the bulk of bitcoin in 2012 was approximately 54% as opposed to the distribution of ownership now in 2021, where the main holders only have 21% of bitcoin. So clearly the distribution is widening throughout the world and it's headed in the right direction. And that's primarily the result of the fact that the supply is limited. And at some point these early holders, if they still have the private keys, will be selling. There's always going to be a price [sic: assuming prior to hyperbitcoinization] at which time they will sell. So it goes to reason then that that distribution will continue to spread amongst more and more people.

[00:27:10] Would you agree with that Bradley?

[00:27:11] **Bradley Rettler:** Yes. I think that the, as you said, the supply is constantly becoming more evenly distributed across the world, and it tends to be people who have a lot who are willing to sell and people who don't have much are buying and not selling because they don't have as much to sell – it doesn't help them as much if they do sell.

[00:27:37] **Mark Stephany:** So getting into some of the stickier questions with regard to Bitcoin – **Is Bitcoin for criminals?**

[00:27:45] **Bradley Rettler:** Yes. That's the simple answer. Bitcoin is for anyone, and that includes criminals. So, we have to ask ourselves some questions. What do we mean by this? I hear this criticism a lot. "Bitcoin is for criminals." You could take it in a few different ways. Is Bitcoin exclusively for criminals? No. I have some bitcoin and I'm not a criminal, so Bitcoin is not exclusively for criminals. Another thing we have to ask is: what kind of criminals is Bitcoin for? Alexei Navalny, Russian opposition leader, is a criminal – according to Vladimir Putin. Alexei Navalny uses bitcoin because his bank accounts regularly get frozen by the Russian government, so that's a criminal use of Bitcoin. People within North Korea are using Bitcoin. That's a criminal use of Bitcoin. Another question we might ask is: is Bitcoin providing something that enables criminality in a new and different and better kind of way. Are we letting criminals be more criminal because Bitcoin exists?

[00:28:58] There, I think the answer is no. Bitcoin is digital, so it is easier to transact with bitcoin across space and time (well, at least space) than it is with

other things. But it's also in a way less private than cash. Cash is much more difficult to trace than bitcoin. Just in the last two weeks, we've seen the US government acquire bitcoin that was stolen in a very famous "hack", or theft at least, from a prominent Bitcoin exchange. And because they knew the address that it was taken from, they could follow it as it was sent to other addresses. And then they could sort of triangulate it, based on ways that those addresses behaved and other facts about those addresses. They could follow the bitcoin and eventually acquire it. That's much more difficult with cash.

[00:29:58] So we have data from about 2019 as to what percentage of bitcoin was used for illegal activities. And in 2019, about $2.4 billion worth of bitcoin was used for illegal activities. When we compare that to how many US dollars were used for illegal activities in 2019, – just the US dollars that we know of, and again keeping in mind that it's harder to trace cash – the estimates are between $800 billion and $2 trillion worth of US dollars. So when we ask, "Is Bitcoin for criminals?", one answer could be, "Well, criminals prefer the US dollar about 500 times more than they prefer Bitcoin for their criminal activities", and the difficulty to trace it has a lot to do with that.

[00:30:49] So, the way I've kind of come down on it is that I think Bitcoin is really good for small-time criminals who are trying to evade not-very-powerful governments, but it's not very good for big-time criminals who are trying to avoid governments that have a lot of computing power and a lot of resources. It's really easy to evade the North Korean government or maybe the Belarusian government or maybe the Nigerian government; but it is much more difficult to evade the US government.

[00:31:28] **Mark Stephany:** and something like Silk Road, which we should acknowledge was an early part of the Bitcoin history, happened because the technology was so nascent and law enforcement was not as familiar with it. This allowed it to go on until it eventually was stopped, and it was stopped because again, it was traceable. So I believe the nefarious behavior – criminal activity using Bitcoin – has dropped to all-time lows as of 2021, to less than 1%. And to quote Jennifer Fowler from the US Department of Treasury, she says, "Although virtual currencies are used for illicit transactions, the volume is small compared to the volume of illicit activity through traditional financial services." This is the US Department of Treasury, which I think should put an end to that critique.

[00:32:18] Moving on to the concern that Bitcoin is not backed by anything. **Is Bitcoin backed by anything, Bradley?**

[00:32:39] **Bradley Rettler:** Yes and no, I guess. There is no other thing which Bitcoin is pegged to, such that having a certain amount of bitcoin is sufficient for acquiring a certain amount of something else.

[00:32:56] Listeners may be aware that in the early days of the US dollar, the US dollar was backed by gold in the following way: you could go to a government facility or bank branch or something like that with a certain amount of dollars and you would get a certain amount of gold. You could redeem the dollars for a certain amount of gold and that amount of gold didn't change.

[00:33:23] The US dollar was backed by gold in that sense. The US dollar is no longer backed by gold. But I think it's a mistake when Bitcoin proponents say that the US dollar is not backed by anything – that's a mistake. The US dollar is backed by the US government and the US economy because you can pay your taxes in US dollars and you can use the US dollar to settle debts with the most powerful government in the world. So the combined output of goods and services that the US produces, balanced against the amount of US dollars that are in circulation, gives you a backing relation.

[00:34:10] It's not a particular dollar or dollar amount to a particular bit of the US economy. But I think this is the right way to think about backing of government currencies. It's the economy of the country versus the supply of the money. So is Bitcoin backed in that sense? Well, not in the same way, but yes. There's a certain amount of people that are willing to take bitcoin in exchange for goods and services.

[00:34:39] And so the amount of bitcoin that there is compared to the amount of people that are willing to exchange it for things – that could be things like pizzas or lawn mowing, or it could be things like US dollars or British pounds – there is an exchange rate with other things because people think that bitcoin has value based on the protocol and the features that it provides. And so those features, I think, are ultimately what give it backing and what give it an exchange rate with other currencies and with goods and services.

[00:35:18] **Mark Stephany:** The question of what kind of asset bitcoin is, I think is delineated in a piece by Fidelity in their Digital Assets group, which also acknowledges the question of it being backed by anything.

[00:35:35] I'm actually going to read that verbatim here, because I think it's rather important and concise. So, they look at this paper written in the nineties by an analyst, Robert Greer, who described certain asset classes, and Fidelity believes that bitcoin best fits into this "store of value" superclass and they

acknowledge that it's “not backed by cash flows, nor is it backed by industrial utility or by government decree. It is distinctly backed by code.” And I will insert here that that code is a form of decree that we all agree upon. Continuing: “that is brought to life by a social contract that exists among its key stakeholders. These stakeholder groups exist in an equilibrium with no one group having outsized power.”

[00:36:28] So you have the users that transact on the network and pay for transaction finality. You have miners that choose to incur costs to process transactions and provide finality. You have nodes that choose to run Bitcoin software to validate transactions. And lastly, you have developers that choose to maintain Bitcoin software.

[00:36:47] So those players all are the backing for the Bitcoin network, ensuring that bitcoin (the asset) as a store of value is maintained. That leads us to our next question. Some people have concerns that bitcoin is not a currency. **Can you expand upon what it means to say that bitcoin is a currency?**

[00:37:16] **Bradley Rettler:** A currency is something like a generally accepted form of payment, and you could have currencies within certain domains. Generally, if something is a generally accepted form of currency in a big enough domain, then we consider it a currency – even if it's not generally accepted in our own domain.

[00:37:40] For example, I think the British pound is a currency, even though I can't pay for anything here with it. If that's right – if a currency is any generally accepted form of payment – then obviously there's some vagueness there with “general acceptance”. Is bitcoin generally accepted enough to be a currency? I don't care so much about that. I think more interesting questions are: “could bitcoin be a currency?” And “would it be good for bitcoin to be a currency?” Or “*is* it good?”, if you say “yes, it's generally accepted enough to be a currency”. So there the question is, “does it have the right kinds of features to be generally accepted?” And here it's interesting because bitcoin in some ways behaves more like a commodity than a currency, as you were talking about with the store of value feature. But it's an interesting kind of commodity in that it has no use outside of being money. So, a commodity like gold… or… let's take oil. Oil is not a very good money. It's messy and heavy and hard to transport and things like that.

[00:39:03] So, it's a commodity that would be a terrible money. Gold is a commodity that is an okay money. It's heavy, so if you want to buy something from far away you probably don't want to have to send gold. It's hard to use for

small amounts. But gold, interestingly, has this non-monetary use as well, in electronics and things like that.

[00:39:29] bitcoin doesn't have a non-monetary, a non-currency, or a non-store-of-value use, but it mimics a lot of the features that gold has. Gold's value doesn't come from its use in electronics. It comes from its value as a store of value. And what gives gold value as a store of value is things like: it takes energy to dig it out of the ground. It takes energy to refine it. It's easy to recognize and hard to fake. It's portable to a certain degree. Bitcoin has these features. It takes work to produce. It's easy to transport. It's impossible to counterfeit. And so bitcoin has the non-utility features of gold that give gold its non-utility value. And, I would argue, bitcoin has them much better, because it's easier to transport. It's easier to recognize. It's easier to divide.

[00:40:32] **Mark Stephany:** It's hard to pigeonhole bitcoin into any one thing. It's hard to say that it's solely a store of value. It's hard to say that it's solely a means of payment. It is really all of these things and we're seeing the evolution of that, right?

[00:40:48] So for you and I, alluding to your very first statement about what value Bitcoin may provide people – that value is dependent upon who you are, where you live, how old you are, your other financial assets. And so for you and I, it may serve more as a store of value than, say, individuals in Ethiopia or the Congo, where their native currency is much more inflationary, they're much more subject to confiscation, and therefore they are using it more as a medium of exchange. So, I try not to get lost in these almost academic nuances of, "is it X, Y, or Z?". It is really all of those things. And we're seeing that play out on a world stage.

[00:41:45] It's merely dependent upon, again, the individual, and how they view Bitcoin and how it is most beneficial for that individual. My next question, one that is again frequently cited as a concern for Bitcoin, is its volatility. Bradley, **why is bitcoin so volatile?**

[00:42:06] **Bradley Rettler:** Two reasons. One is that people are still learning about it, and it's relatively new. It's been around for 13 years now. Gold has been around for thousands of years. We're relatively familiar with gold. We know kind of how it behaves as a market. We know how it behaves as a commodity. And so you wouldn't expect to learn many new things about it. You wouldn't expect there to be a lot of people who all of a sudden discover it and get really into it and try to buy a bunch of it.

[00:42:45] With bitcoin, we're seeing a gradual understanding and desire for it that is at times quickly moving and at times slowly moving, but always increasing. So there's a price discovery mode that we're in right now. We're trying to figure out, what is this new thing? What can it do? Should I care about it? Who else cares about it? Should I get some of it? Why would I want it? What would I use it for? These are difficult questions to answer, in no small part because of the difficulty of answering the first question of this podcast, which is "what is Bitcoin?" Bitcoin is not an easy thing to understand.

[00:43:35] And so it's not an easy thing to decide whether or not you want to acquire some. It takes most people multiple times of hearing about it – and hearing about the features that it has and hearing about use cases for it – to come to a decision about whether they want to invest. And even then they might not. They might invest small at first and then increase. They might invest small and keep investing small. I think right now something like 60 million people own bitcoin in a world population of 7 billion. Some of those 7 billion undoubtedly will never get bitcoin. But I think probably the number of people that own bitcoin will end up being quite a bit higher than 60 million.

[00:44:26] So there's people who are still learning about it, who are still deciding whether to buy it or not, and that's one reason why the volatility. That's a reason that you might think goes away in maybe 15 years, maybe 30, maybe a hundred. The other reason is that Bitcoin has a completely inflexible supply. If demand goes down, supply stays the same. If demand goes up, supply stays the same. Right now, there are 6.25 bitcoin added to the supply every 10 minutes. And if nobody wanted it, but there was one person who kept mining – who kept running the mining software – there would be 6.25 new bitcoin every 10 minutes.

[00:45:12] If all of a sudden everyone in the world was trying to buy it, there'd be 6.25 new bitcoin every 10 minutes. So because of the completely inflexible supply, but the variable demand, bitcoin is volatile. That's an aspect of bitcoin that I don't expect to go away. Originally, I had thought that once the first problem – once we were out of price discovery mode – then the demand for bitcoin would be relatively stable.

[00:45:44] But then my friend, economist Will Luther, convinced me that since the demand for money goes up and down, so the demand for bitcoin will always go up and down. So, in that sense, it might always be volatile – probably not as volatile, but I don't know. I mean, right now we're seeing drops in a week or two of 50%. I'd be surprised if that happens a hundred years in the future, but I suppose it could.

[00:46:19] **Mark Stephany:** Again, to summarize, volatility is a product of a nascent technology with less adoption worldwide. It's a product of demand since the supply is fixed. But what we've seen already in these 13 years is that volatility has declined. To your point, to what degree it minimizes and finds some sense of equilibrium, we don't know – we don't know what timeframe that will be. The assumption is that it will occur, and what degree of volatility we'll have is uncertain. But it's also important to think about volatility in comparison to what else? – the US dollar or the S&P 500, et cetera. As it relates to how somebody might see bitcoin as a part of their portfolio or use as a medium of exchange, I think that's important to acknowledge, as it relates to the topic of volatility.

[00:47:17] And I think it was Lyn Alden who says that it's simply a position size in managing risk. And so clearly the volatility is gonna be much more troublesome to an individual if 50% of your portfolio is made up of bitcoin. But if it's three, five, 10%, that volatility is much less of a concern. So, you mitigate the risks, the downside risks of volatility, by simply managing the percent size of your portfolio.

[00:47:47] **Bradley Rettler:** I don't care nearly as much about bitcoin for people who have portfolios as I do about bitcoin for people who don't – people who lack access to the stock market or to other kinds of long-term stable stores of value.

[00:48:10] So, the volatility concerns me when I'm thinking about, say, someone who lives in Venezuela and makes enough money that they don't need to spend it all right away to provide food and shelter for themselves. But if they hold on to the bolivar, then it just decreases. But they don't have access to the S&P 500 or things like that.

[00:48:34] There, I think bitcoin has a lot to offer as a store of value for them; but then I wonder, is it ever going to get to a point where it just sort of steadily and slowly creeps up like the S&P 500, but it's easier to acquire for them? And I had been hopeful that that would be the case. But now I'm not so sure. That's all I want to say – I mean, I think this is a serious concern.

[00:49:02] I've published a lot of stuff on how bitcoin can help people who aren't so poor that they need to spend every dollar that they make immediately to provide food for themselves but also aren't accredited investors or don't have portfolios. And I still think it's long-term good for them to invest in it.

[00:49:21] I still think it's, long-term, a good store of value because of the fact that it can't be manipulated in the supply. But if they have an emergency and all of a sudden they need to draw on it, it might be worth half of what it will be worth the next month, and they'll get half of what they need. And that's distressing, but perhaps unavoidable.

[00:49:45] **Mark Stephany:** Absolutely. Those are all fair questions and concerns to be focused on with regard to bitcoin. And to that end we've kind of discussed this already, but **does its volatility undermine its potential as a future world reserve currency or otherwise?**

[00:50:02] **Bradley Rettler:** Yes, to some degree. Most currencies right now are inflationary and predictably (to some degree) inflationary – or at least governments are attempting to make them predictably inflationary.

[00:50:17] I think right now in the US we're seeing year-over-year inflation at levels that weren't predicted – in fact, levels where people predicted they would decrease and in fact they've increased. So, in that sense, even a currency that has supply controls in the hands of people who are supposed to know a lot about how to respond to various market and geopolitical and etc. forces aren't responding in ways that keep inflation at the desired 2% rate. Bitcoin can't respond to supply this way. And so one big question is, "Why would I ever spend bitcoin?" Well, I think there are two responses to that. The flat-footed quick response is, "because you need food. You can't get by without food."

[00:51:11] Even if you could buy more food with your bitcoin next week than you can today, you have to eat food this week. And so if all you have is bitcoin, then you have to pay. You need to live somewhere. So, if your landlord is demanding rent, you can't convince them "you know, if you just let me wait a month, then I'll be able to give you even more rent."

[00:51:35] The landlord is going to say "No, just give me the bitcoin now and I'll hold on to it." The landlord is going to have to pay back bank loans or whatever. The landlord also needs to eat. So, there's a certain amount of spending of bitcoin that is unavoidable. Right now, people have money that they don't put into bitcoin. If they really thought that bitcoin was just going to keep going up forever, just because they have US dollars instead of bitcoin doesn't mean that this concern doesn't rear its head. "Why did you buy a car instead of buying bitcoin?" is just as good of a question as "Why would you spend your bitcoin on a car?"

[00:52:14] In that sense, I don't think it's a super compelling objection that nobody will ever spend any bitcoin. But maybe a more interesting question is: what kind of spending that currently occurs, won't occur? If, say, bitcoin is a more widely accepted medium of exchange, more commonly held store value… I think it's maybe discretionary spending of things that you don't really need. The calculation of whether to exchange your US dollars for something that you don't really need is a different calculation than whether to exchange your bitcoin for something that you don't really need – given these background facts about the US dollar and about bitcoin.

[00:53:00] Of course, we still have the same thing. Right now, if I have US dollars and I'm deciding, say, whether to add guacamole to my burrito, I could not do it and buy bitcoin. So, I think the calculation is still the same in the end: there's a lot of things that I could do with this asset that I have, whether it's bitcoin or the US dollar – one of the things I can do is buy a consumable good, one of the things I can do is buy a store of value – and my decision about what to do should be one that takes into account the future of the thing that I'm exchanging. What could this be in the future if I don't spend it right now? For bitcoin, it could be worth more. For the US dollar, it could be exchanged for bitcoin, which would then be worth more. So, the mere existence of bitcoin forces us to reckon with our spending habits, spending patterns, the things we spend money on… and decide whether they're worth what they could be.

[00:54:11] **Mark Stephany:** Which gives us pause to reflect on our consumer behaviors, which obviously is top of mind for all of us at this juncture, knowing the downstream externalities of doing so. One thing that I think should be acknowledged is that currently bitcoin is taxed when you spend it. So that is most certainly a limiting factor for people to want to spend it. I have heard proposals that this will change under certain amounts, but even if people wanted to spend it, it being taxed as property or a commodity by the IRS limits one's desire – let alone ability – to spend their bitcoin at least within the United States.

[00:54:59] So my next question for you, Bradley, is **does bitcoin have intrinsic value?**

[00:55:03] **Bradley Rettler:** The phrase "intrinsic value" is said in many ways. The way that it's usually said in investments is kind of the opposite of the way that it's usually talked about in philosophy. Investments have intrinsic value when they have cash flow, which is a paradigmatically extrinsic kind of thing –"extrinsic" meaning "outside of the thing itself" and "intrinsic" meaning "within that thing itself". I think what gives bitcoin value are the features that it

has within itself. We talked about many of them already, but: it's private, it's censorship-resistant, its supply isn't flexible, it's portable, it's divisible, it's digital. These are features of it that give it value – but not a value in itself. They give it value for the way that it's used. Depending on how people want to use it, it may or may not give value to them – people who don't have a computer or a phone or anything like that might find no value in bitcoin. People who have those things but are wealthy and own lots of real estate and are accredited investors and have access to seed rounds of funding and things like that – they might not find much value in bitcoin. But people who need these various features – people who want to be able to spend money on things that their government doesn't want them to spend money on, like for example, Taiwanese flags or something like that – might find a lot of value in bitcoin. People who need to flee their country because it's being attacked by an autocrat and want to be able to gather up all their wealth in their mind and flee with it might find a lot of value in bitcoin.

[00:57:15] So I think the value in bitcoin comes from these features that it has and how much value it has depends on how much people need those features for the things that they want to do.

[00:57:27] **Mark Stephany:** **The probably most cited question or concern rather, for Bitcoin is that eventually, if it gets big enough, the US will ban Bitcoin. What are your thoughts surrounding that concern?**

[00:57:42] **Bradley Rettler:** I think that's unlikely. There was maybe a time at which the attempt to do that might've been successful. Bitcoin runs on the internet and it's difficult to distinguish Bitcoin from any other aspects of the internet; that is, the Bitcoin protocol. So the government can't ban it in the sense that they can't shut down all of the Bitcoin full nodes that are in existence, nor can they shut down the Bitcoin miners – the people that are competing to publish the blocks of Bitcoin transactions. What they could do is make a law that says that it's illegal to own any bitcoin. But there are now millions of Americans who own bitcoin and a large percentage of Bitcoin mining is done in the United States. So, it seems unlikely to me that the government would take this kind of step, knowing that it would decrease the wealth of the aggregate of Americans.

[00:58:48] **Mark Stephany:** Absolutely. I would agree. It's already considered property by the US government. It's taxed as a commodity by the IRS and that's a significant revenue stream that would be lost. You've got the political donor class that's already using it. And we have seen the pushback that unfavorable laws have resulted in. So I would agree an outright ban seems highly unlikely,

but it certainly would appear that they would want to regulate it to a greater degree.

[00:59:19] What that regulation means is yet to be determined. But we shall see. People often cite the confiscation – or banning rather – of the owning of gold from 1933 to 1975. But the history and the circumstances surrounding that are different than they are today, which we don't need to get into, but outright confiscation as was desired with gold back then is simply impossible as it relates to Bitcoin given its cryptographic protection. So, the only way that it could be accessed, would be through knocking on your door and legal interventions. Any final thoughts on the US banning Bitcoin?

[01:00:07] **Bradley Rettler:** Yeah. Two things on that. One is that when the United States did that with gold, the price of gold in the US skyrocketed right away, because of the second reason, which is: when a government bans something, that's usually a really good indication that people need to be paying attention to that thing. When authoritarian governments ban Bitcoin, it tells people, "This is a thing that can be used to evade authoritarian governments," which is great. The United States is not an authoritarian government, but to ban something like this would get people talking about it and why the US felt the need to ban it.

[01:00:49] And it would, I think, draw a lot of people's attention to it. I think this is called the "Barbara Streisand Principle" or the "Streisand Effect", where the banning of it would create more demand for it than already exists.

[01:01:05] **Mark Stephany:** Since it's a peer-to-peer network, it's going to continue to exist and command that premium. We've seen China try to ban it and backtrack. We've seen India try to ban it and backtrack. And several other countries. And there's always the backtracking, because it's clearly of value for both citizens as well as eventually the government themselves. Let's get into a little bit more of the technical side of Bitcoin.

[01:01:36] **Mark Stephany: One of the concerns is that Bitcoin won't be able to scale given its extremely limited transaction throughput. What are your thoughts on this concern?**

[01:01:46] **Bradley Rettler:** Yes, I agree that the Bitcoin blockchain is not big enough to contain as many transactions as would be necessary for bitcoin to be a currency. Block size is limited in Bitcoin and transactions take up space because they require a certain amount of data to be included in the transaction. And it works out, given that a block comes out every 10 minutes and it's one

megabyte roughly per block, that you can do about seven transactions per second.

[01:02:30] The Visa payment processing network can do about 1700 transactions per second – so about 250 times more. It's impractical to think that people could transact on the Bitcoin blockchain for everything that they're buying – coffee and all that kind of stuff. That being said, Bitcoin is a final settlement layer.

[01:02:58] So when a transaction is broadcast and included in a block, that transaction is irreversible – it's impossible to go back and change anything about it. Visa isn't like that. If you've ever had your Visa number stolen and used for nefarious purposes, as I have on more than one occasion, you know that Visa does not charge you for that. I don't know exactly what Visa does with respect to the merchants that accepted the fraudulent transaction, but it's not the final say when you swipe your card at a coffee shop; that's not final settlement. Final settlement is like FedWire, the wire transfer service that banks use to communicate with the Federal Reserve.

[01:03:51] And then we have layers on top of FedWire layers, layers like cashier's checks and money orders. And then we have layers on top of that, like Visa. We have layers on top of Visa, like PayPal and things like that. So, our monetary system is not all happening at the base layer. If Bitcoin becomes more popular… Even now there are layers being built on top of Bitcoin.

[01:04:19] One of those layers, for example, is the Lightning Network, where you can open channels between people. You open the channels using bitcoin [on the blockchain] and you close the channels using bitcoin [on the blockchain]. But in the meantime, you can route your payments through a bunch of these different Lightning Network nodes and they happen nearly instantaneously.

[01:04:41] They don't settle on the Bitcoin blockchain until the channel is closed. And in the meantime, they can transfer a lot of value back and forth. It happens nearly instantaneously, and it's nearly free. And it has just as much, if not more, of a possible transaction per second throughput than the Visa network does.

[01:05:02] So when we think about using bitcoin to do things like buy a cup of coffee or things like that, we shouldn't think about this as happening on the base layer. That's where big, expensive transactions will happen and people will be willing to pay for that base settlement – this final settlement idea. But it's only

practical to pay that if the amount that you're settling is enough to make it worth it.

[01:05:30] So if you're going to buy a cup of coffee, you'll probably use a layer two or layer three system. If you're going to buy a house or a car, you might want to use the Bitcoin base layer. FedWire takes days to settle at the base layer. Bitcoin takes 10 minutes. So even there, if you're willing to pay for the block space, which varies between 40 cents and $40 depending on how much competition there is for block space at the time, if you're willing to pay for it you'll have final settlement much more quickly than you could have within the traditional financial system.

[01:06:09] **Mark Stephany:** So again, Bitcoin is optimizing for security and decentralization. These second and third layers like the Lightning Network are optimizing for speed and have already achieved speeds – transaction throughput – equivalent to Visa. Another technical question, **what is Proof of Work? And then we will contrast that with Proof of Stake.**

[01:06:34] **Bradley Rettler:** Proof of work and Proof of Stake are two consensus mechanisms for maintaining distributed ledgers that are blockchains. Recall from earlier, the way that the Bitcoin ledger works is that every 10 minutes a new block is added, and you just keep adding to the front end. So, one of the questions is, "who can add to this" and "how do we decide who can add to it?"

[01:07:07] "Who's going to be the next person to add to it?" Importantly, we need to all agree whose edition to the blockchain was the correct one – the canonical one. Imagine we were co-authoring a story, and it got to the end of the fourth page and then two different people wrote page five, and they were both co-authors; but only one of those can be page five. We need a way of deciding whose is the canonical page five. So the way that it works in Bitcoin is the Proof of Work system. You have all of these miners who are running a computer program that is working to solve a math problem by trial and error. It's working to basically multiply a number from the previous block times an unknown number to get a number that starts with a certain number of zeros.

[01:08:09] So it's gotta be like .000000. And the only way to do this is to take that first number from the previous block and multiply it by as many numbers as fast as you can to try to get this new number by trial and error. This takes a lot of computing power. And when you get that and you broadcast it, you say, "look, here's the answer." Everyone can immediately check it with one calculation. You can check it by hand if you want to – some people have done

this just for fun. But you take the value from the previous block, you multiply it by the number that the miner says is the winning number, and you can immediately verify it.

[01:08:49] So it takes trillions and trillions of calculations at the current power levels to come up with this number by trial and error, but it takes one calculation to check it. So, everyone checks it. And by providing the correct answer, you are proving that you spent a probable amount of energy on getting the answer.

[01:09:18] So you've exchanged energy for new bitcoin and the difficulty of the problem, that is, the number of calculations that will probabilistically lead to finding the answer, varies depending on how many people are working on it. That number changes every two weeks. Early on when you could mine Bitcoin with your computer, it was very low – the difficulty was very low. Now the difficulty is obviously much higher – it takes specialized hardware. But in any case, you're proving that you spent energy. You're proving that it took work to come up with it, and because of that, you are given the right to publish the next block of transactions. Let me say a little bit about how this works in the incentive structure before I contrast it with Proof of Stake.

[01:10:08] So one of the important things, as we were talking about with Satoshi's design of how Bitcoin worked, was to incentivize honesty. Satoshi didn't want to trust people to be honest; Satoshi wanted us to assume that people would try to be dishonest if it would benefit them. And so we needed to make sure that it *didn't* benefit them. If you have a lot of computing power at your disposal, you have two choices: you can use it to try to attack the network, which is to broadcast dishonest transactions that benefit you, or you can use it to support the network, which is to broadcast honest transactions. And if you have, let's say, a quarter of the computing power on the network (that's a lot, nobody has that much, but suppose you did), you have a quarter of the computing power of the network, and you say, “I'm going to try to use this to attack the network.”

[01:11:12] There's a 25% chance that you'll succeed at being the first person to solve the next math problem and so to broadcast the next block. If you fail in that first instance, then you have to go back and…you’re trying to presumably undo some spending that you did to give yourself back the bitcoin. So, you have to start with the block that contains the transaction that you're trying to undo. So, everyone else is working on the next math problem. If you try to work on that, you'd be twenty-five percent likely to succeed. But now you have to go back and somehow redo the block that's already done, *plus* the next block, *plus* the next block.

[01:12:01] Every Bitcoin full node is set up to accept the longest chain as the valid one. So, you have to undo a transaction, go back one block, do that block and do the next block before any miners do just the next block. If you only have 25% of the network hash power, the likelihood that you're going to be able to do *that* is *significantly* lower than 25%.

[01:12:29] So you have a 25% chance at winning the block reward versus a super-small chance of succeeding and doing two blocks before anyone else can do one block. So, you're just not incentivized in the Proof of Work system to try to cheat the network by undoing a spend and catching up.

[01:12:50] **Mark Stephany:** The importance of Proof of Work – and in turn, the amount of energy that goes into that system – is so that it deters the manipulation of data going into it. Meaning Bitcoin – the base layer, the protocol, as we said before – needs to be trusted and secure. It is this immutable truth of data that we all need to trust in. In order to maintain that, it requires a lot of energy. So, the point of all of that is to be able to obviously solve these puzzles, but in doing so that deters any manipulation of that ledger at any given moment. And so that you don't have to worry about some other party changing the data or manipulating it.

[01:13:48] Would you agree with that framing?

[01:13:51] **Bradley Rettler:** Yeah. Yeah. I think that's exactly right. The starting point was, "how do we incentivize honesty?" And the solution was to require people to expend energy to do this. So, if you expend energy in an attack and you fail, all that energy is wasted. But if you expend energy to help secure the network, you're more likely to succeed and you're more likely to be rewarded.

[01:14:15] **Perfect. So what is Proof of Stake?**

Bradley Rettler: What some people have thought is a problem of Proof of Work, which I assume we'll talk about at some point towards the end, is how much energy it expends. Given the value of bitcoin and the block reward of Bitcoin, getting the right answer to the math problem is worth something like a quarter of a million dollars at the time that we're recording this. So, 6.25 bitcoin times $43,000 is a quarter of a million dollars. So, every 10 minutes, a quarter of a million dollars is being created. So, it's worth spending a lot of money and expending a lot of energy to try to get that block reward – and that thereby uses a lot of energy. So, some people then thought, "Well, we like this blockchain idea, we like this immutable ledger thing. But we don't want to use Proof of Work for two reasons. One, it uses a lot of energy, and two, if people are going

to expend energy, they're probably going to do it on Bitcoin and not on this other project – whatever that other project is. So, we need something else." Proof of Stake is an alternative consensus mechanism.

[01:15:27] It's an alternative way of determining who gets the right to publish the next official block. And it does it by taking people who already own the native asset on the blockchain. And what they do is put a certain amount of it up as their stake. They prove that they own it. And then there's a probabilistic function that rewards the blocks based on the percentage of the native asset that you have staked.

[01:16:07] Just for simple terms, if you have 25% of the native asset staked – a hundred percent is the total amount that anyone has staked and you have 25% of that – then probabilistically, you'll win the right to publish one out of every four blocks. And then that's the official one – the network recognizes that that's the official one – and then we move on.

[01:16:32] So, nobody has had to solve a math problem or anything like that. You just have to put up as collateral the native asset. And the idea is that you're going to be incentivized to act honestly because you have a lot of the native asset. And if you do dishonest things, then that will, once it becomes known, make the value of the asset go down, which decreases the value of your holdings.

[01:17:02] There's two questions of Proof of Stake versus Proof of Work. One is, "does it provide as strong of an incentive not to cheat – not to act dishonestly?" And question two is, "is it as fair or just of a consensus mechanism?" In answer to the first question, I think the answer to the first question is, "probably not." Although I'm not sure. Proof of work means that you have *wasted* something if you try to attack the network and you fail. In Proof of Stake, you haven't wasted anything – you still have your stake. It relies on external forces to make the value go down. So, it's not at least quite as built into the system that it's bound to result in you losing money or capital or something.

[01:18:03] And then with regard to question two, I think the answer is a clear "No." I don't think it's as fair. Go back to the beginning of Bitcoin versus the beginning of Ethereum. Anyone could participate in mining Bitcoin and they could expend any amount that they wanted on energy and owning computers just to mine Bitcoin.

[01:18:26] With Ethereum, you had to own some Ethereum. (Let's imagine Ethereum was Proof of Stake, as it's supposed to be – as has been promised for the last five years or so.) If Ethereum had been Proof of Stake from the beginning, the only people who could have mined Ethereum – who could have published the next block – are the people who already owned it through buying it or through being gifted it by the Ethereum Foundation.

[01:18:56] So, the developers had some, the Foundation had some, and then people who bought it with bitcoin had some. Only those people could do it. If you believed in it and you wanted to participate, you were out of luck. You couldn't just use energy to get more of it. I should stress that's not how Ethereum started. It's been designed to switch to that eventually, and that switch has been promised for the last five years or so. There's still no evidence that it will actually happen. But you can see how the cryptocurrencies that use Proof of Stake have to give out some of that or sell some of that beforehand in order for anyone to be able to stake any of it – and it usually goes to insiders, it usually goes to friends, it usually goes to developers… And that just seems to me fundamentally unjust.

[01:19:52] **Mark Stephany:** One of the comparisons that I like to make is that Proof of Stake, in essence, is just a different name for equity ownership. And if you're an individual – if you're a founder – and you have X percent of equity of a company (presumably the most), you have the ability to make decisions based upon that – as opposed to your average citizen who may have stock in your company and has voting rights; but those voting rights are likely very minimal.

[01:20:28] The majority owners could increase shares should they desire; they could split the stock should they desire. They can make changes to the company that they desire that you may not agree with, but you don't have enough equity, i.e., "stake", to do anything about it. That contrasts with Proof of Work where the user is guaranteed certain specific rights under the protocol.

[01:20:59] And I will steal this from Pete Rizzo in saying that we know the rights that Bitcoin promises you are the following: the irrevocable right to your money, the ability to write and review code, the ability to post and validate transactions, the right to a known money supply that will not change, and most importantly the right to, as he says, dissent – you don't have to run certain upgrades to the protocol. You can run the original, should you desire. So that is the ability to dissent, whereas in Proof of Stake if you dissent you're essentially cut out of the network and any network effects that it may already have, such as the case was Ethereum and Ethereum Classic.

[01:21:59] [01:22:00] In my opinion, Proof of Stake is just another name for our current market dynamics between equity ownership and stock ownership. If you do not have a controlling stake, your voice is greatly minimized. Would you agree with that framing as well?

[01:22:23] **Bradley Rettler:** Yes. And I think it's important to stress, too, that one of the things that I like about Bitcoin is that it is inclusive. It allows people who don't have access to equity markets and things like that to own it. All you need is a smartphone. And for people who like Bitcoin for these reasons – that it offers a way to maybe store value, even for people who can't get stores of value like equity markets – you might wonder, "What kind of system would I want these other people to be able to opt into?" The equity market and the US financial system have harmed a lot of people by keeping them out, and Proof of Stake systems (given the similarity) are doing the same thing.

[01:23:21] **Mark Stephany:** One of the things about these other cryptocurrencies that concerns me, in my opinion, is the emperor with no clothes. It's the fact that these other cryptocurrencies have any monetary value at all – that Ethereum has value, that it's going up in price, or that Cardano is going up in price. Setting aside SEC chair Gensler's concern that the majority are unregistered securities, one of the things that I lovingly call "The Rettler Dilemma" touches on this concern: I cannot for the life of me understand why these tokens go up in price. When in fact, it would appear that they were primarily used as fees to pay for the network. And we know that fees are a race to the bottom, meaning the network that has the cheapest fees will eventually win. It's much like an ATM fee.

[01:24:31] ATMs aren't going to flourish if you're paying five or ten bucks for every transaction, rather, the one that is the cheapest is going to be most utilized. So again, I know there's pushback about this metaphor as for banking fees, but I still have not found a good fair critique. And so I would like for you to describe to the listeners what the Rettler Dilemma is and how you see it affecting the prices of these other cryptocurrencies.

[01:25:02] **Bradley Rettler:** I called this "The Non-Monetary Blockchain Dilemma", but I'm happy to have it named after me! As we talked about earlier, when Satoshi was designing the Bitcoin blockchain, they desired for it to be money. And so you hold onto it, you store value in it, you spend it to have space on the blockchain when you want to transact with it, and everything seems to incentivize the same thing; everyone who owns it wants the value of it to go up.

[01:25:32] That's good for everyone who's participating in the network; it's good for the miners, it's good for the users. There are other blockchains, something like 17,000 of them at the time of recording.

[01:25:58] And they all have, at least as far as I know, native assets on them. They're tracking the movement of some synthetic digital commodity. But they aren't all trying to be money, because that's Bitcoin's thing and Bitcoin was around first, so anyone that tries to compete with Bitcoin along purely this dimension – is a better digital money – is probably going to lose.

[01:26:26] So, they try to do other things. They try to be software platforms or smart contract platforms. So, there's a native asset on these blockchains, but the point of the whole blockchain isn't to track this native asset and the distribution of it, but it's rather to do this other thing. And to do that other thing, you need to use the native asset – whether that's ETH or ADA or whatever. So, then you have some things: you have the miners or stakers or in some way publishers of additions to the blockchain, you have the users. The miners or stakers are rewarded with the native asset of the blockchain, so they want it to go *up*. The users own the native asset so that they can do whatever the blockchain is supposed to do – smart contracts or whatever. As you pointed out, they want the value to go *down*. The miners and the users – or the publishers and the users, because they don't all use mining – are at cross purposes. One of them wants the price to go up, and one of them wants the price to go down. Because these things are digital, it’s very easy to move from one to the other. I think the ATM analogy is great. Let's expand it this way. You might know the cheapest ATM in your city. It might be at your bank, because your bank's not going to charge you fees to use it.

[01:28:12] So imagine that literally you had a hundred ATM's right in front of you and you could pick any one of them just by walking a few steps. Nobody is going to use the most expensive ATM. Here’s where the analogy starts to come apart a little. The publishers of the blockchain are staking the native asset, or they're expending energy to mine blocks, or they're somehow trading something for security of the blockchain. If fees go down too much, then they're not going to provide security for the blockchain – whether by staking or mining or otherwise. So, if fees start to go down, users love that, but then miners leave; so, the network becomes less secure. Fees start to go up, miners love that, so they flood over to the network. Then users abandon it because fees have gone up. So, it seems like the stable equilibrium for all of these things is to just keep inventing new ones that do it for cheap. And then everyone floods over there. The users flood over there first, because of the cheap fees. The fees start to go up because of the competition, miners go over there to get the high fees, but

then users leave to go somewhere else. And it's just going to be this hopping from one to another.

[01:29:40] **Mark Stephany:** Yeah. If Gensler had a magic switch and just said, "These are all securities. Treat them as such.", you could understand why ETH might go up in price, because then it's essentially a stock right and you are investing in that platform.

[01:29:56] But as a token, its utility in the network would plummet because as you said, it would need to be the cheapest. I just don't see that happening. And in turn, we're left with this dilemma. I find it troubling to say the least, but we shall see what happens.

[01:30:19] **Bradley Rettler:** Yeah. What we're seeing right now is that this phenomenon of NFTs – non-fungible tokens, which are often pieces of digital art – whole families of these are being transacted on specific blockchains and sometimes it takes more to mint your NFT – that is, to get block space on a certain blockchain to declare that you have ownership of it – than you think your NFT is going to be worth. And so people are leaving to other platforms. They're [01:31:00] abandoning; whole families of NFTs are going from one platform to another so that people can trade them around cheaper. And then of course that network needs security because you don't want someone to be able to come and steal your NFT by attacking the network with computing power. So, the network needs computing power. But then the people who are providing that computing power are hoping that the fees are going to go up… So yeah, there's no stability, I think, long-term in these kinds of non-monetary blockchain networks.

[01:31:36] **Mark Stephany:** Another big one – they're all big ones, aren't they? **I thought Bitcoin was a pyramid scheme or a Ponzi scheme. Can you tell me why it is not?**

[01:31:45] **Bradley Rettler:** Ponzi schemes were famously investment opportunities that did two things. One, they paid out earlier investors with later investors' money to make the early investors think that they were getting a great return. But ultimately this was not sustainable because it needs a constant influx of new people in order to pay the old people back. And there's only so many people in the world, so you can't constantly keep getting new people. And famously, that fact was hidden from everyone. So it's not that Charles Ponzi said, "Here's what I'm going to do. You give me a hundred bucks and then I'll convince a bunch of other people to give me a hundred bucks. I'll give you their

hundred bucks and then I'll convince a bunch of others…" He wasn't forthcoming with the features of his "investment opportunity."

[01:32:48] In my opinion, all Ponzi schemes share both of these features. So, you can't just have a Ponzi scheme where the money from later investors accrues to earlier investors. There has to be this element of deception. One of the reasons I think that is because then things like gold would be a Ponzi scheme. Anyone who's buying gold now is giving money to someone who has bought gold earlier. Or real estate, or literally anything – baseball cards would be a Ponzi scheme. So, there has to be this element of deception – of unawareness of how it works.

And I don't see that feature in gold, I don't see it in baseball cards, and I don't see it in Bitcoin. People who are buying bitcoin now are giving money to people who bought bitcoin earlier. First of all, there's nobody "representing" Bitcoin in the way that Charles Ponzi was "representing" his company.

[01:34:02] This is a decentralized purchasing network. You can buy bitcoin from anyone who's willing to sell it, and there's no deception about what's going on. We have this synthetic digital commodity. We have these protocols. We have miners. Everyone knows how the situation works. A lot of people don't think that bitcoin has any value because of these features, and they don't buy bitcoin.

[01:34:23] A lot of people think it does, and maybe they do or maybe they don't buy bitcoin; but the facts about what's going on are out there for everyone to see. And you, if you buy bitcoin, you buy it knowing – at least you can know – all of these things.

[01:34:40] **Mark Stephany:** Right, exactly. I push back as well because by definition a "Ponzi scheme" is a central source of deception. As you said, Ponzi is a person – Charles Ponzi – or Madoff… There's these central authorities who do the deception. Bitcoin simply does not have that. It is a transparent ledger. There is no hiding the numbers or cooking the books to any degree. **The other critique that Bitcoin faces is this idea of a greater fool** and I'd like your thoughts on that. I will say initially, though, that the idea of a greater fool is that you are assuming somebody in the future will buy your asset, or whatever it is, for a higher price. And again, you go down the list with baseball cards, real estate gold, et cetera, et cetera. I find that argument still fairly weak as it relates to Bitcoin, especially when you tack on all the benefits that we believe the network that is Bitcoin does provide. **So what is your response to the idea of Bitcoin being a greater fool scenario?**

[01:35:53] **Bradley Rettler:** I think that there are a lot of people who buy bitcoin because they think that they will be able to sell it for more later on. That is one of the premises behind it. But the reason isn't because some greater fool will be stupid enough to buy it in the future. It's because the supply is capped and compared to other currencies whose supplies aren't capped, you'd expect bitcoin to go up against those currencies or things. So there are fundamental reasons based on the rules of the protocol to think that you will be able to sell it for more later on. But a lot of people who invest in bitcoin, or who own bitcoin, I should say, don't intend to sell it for something for some other currency later on; they intend to exchange it for goods and services.

[01:36:44] They believe in the technology and they want to use it as money because they think it's a better money than the other kinds of money that they have. So I mean, people who own US dollars expect to exchange them later on for something else, whether it's food or rent or something like that. That doesn't seem to be greater fool theory.

[01:37:07] Is it merely because the value of the US dollar is expected to go down, such that if you expect the value to go up, then it would be? That doesn't seem like the point of the greater fool theory. The point of the greater fool theory is that people who are purchasing it don't understand it. I don't think Bitcoin is premised on people not understanding it. I mean, here we are recording a however-many-hour-long podcast trying to help people to understand it. I think a lot of Bitcoin educators are trying to do the same thing. I'm certainly not trying to be deceptive about anything. I'm not trying to create fools who then will buy bitcoin or something like that.

[01:37:50] So, yeah, I don't see that the necessary deception or the necessary thinking of future bitcoin purchasers as somehow unintelligent or missing the point. I think the more you understand about Bitcoin, the more you see why it's valuable to other people.

[01:38:09] **Mark Stephany:** **Bradley, isn't bitcoin controlled by only 0.1% of its holders?**

[01:38:13] **Bradley Rettler:** I don't think so. I've seen this statistic bandied about by certain analytic firms and at least every time that I've looked at it, they don't seem to have distinguished between users and exchanges. They sometimes have marked out some wallets that are known to be owned by exchanges. But there are a lot of Bitcoin exchanges in the world that hold a lot of bitcoin because they constantly are buying.

[01:38:48] One could get the impression, looking at the huge balance of bitcoin in those wallets, that bitcoin is owned by a small group of people – that the vast majority of bitcoins are owned by a small group of people. But for one Bitcoin wallet, say, held by Coinbase, there could be 3 million people who own that bitcoin, and Coinbase just stores it all in one wallet.

[01:39:13] If you, say, have an account on Coinbase, and you haven't withdrawn bitcoin from Coinbase, then the bitcoin isn't yours in the sense that you don't control the private key to the address that the bitcoin resides at – Coinbase does. And so they put it in one of their wallets. Of course, early on all of the bitcoin was owned by Satoshi, and then all of the bitcoin was owned by Satoshi and Hal Finney… We see this constant spreading out of the bitcoin, and I think we'll expect that to continue.

[01:39:52] **Mark Stephany:** Additionally, it's also important to note what people mean by "control", because clearly you can have a significant amount of bitcoin, but you don't control anything per se; you've just got a lot of bitcoin. You're not controlling the network. You're not able to change the network. This is not a Proof of Stake system. You don't control the miners. You don't control the nodes. You just have a ton of bitcoin.

[01:40:13] **Bradley Rettler:** Yeah, you control where some bitcoin can go to.

[01:40:20] **Mark Stephany:** Exactly. And as we mentioned earlier, this distribution is only spreading to more and more people, so that concentration is diminishing. Additionally again, it's also important to ask, "In comparison to what?" If we look at the trend of equity ownership in the United States, it is becoming more concentrated over time. The top 1% now own 53% of total equities. Compared to that, bitcoin is headed in the right direction, and that should be acknowledged.

[01:40:58] This gets us back to my next question: **How do you view bitcoin as an asset class? Do you see speculating on cryptocurrency or bitcoin different from speculating on collectibles like beanie babies or art?**

[01:41:13] **Bradley Rettler:** In some ways, yes. And in some ways, no. I'm not an investment advisor, but some people are clearly speculating on cryptocurrencies. I think the rise of certain kinds of cryptocurrencies can tell you that. So, when I think about Bitcoin, I think about the fundamental features that it has, that we've talked about it at some length: privacy and censorship-resistance and things like that. Those are the value propositions for Bitcoin.

[01:41:48] These are the reasons why bitcoin is valuable. And ideally people would be investing or not investing in bitcoin based on whether they think those features are important or unimportant. There are a lot of other cryptocurrencies that people exchange dollars or bitcoin for, and the value proposition is quite different.

[01:42:10] For example, one of them is “this is funny.” That's the value proposition of Dogecoin. “This is even funnier than Dogecoin” is the value proposition of the Shiba Inu coin. All these different cryptocurrencies have different reasons that people who own them tell you that you should invest in them.

[01:42:34] They have different reasons that those people find them valuable. When you think about beanie babies, I don't know exactly what the value proposition for beanie babies was. It was something like, “These are reasonably rare, they’re a big part of people's childhood, they're cool, and people will want to buy them in the future.”

[01:42:56] Baseball cards are something like, “Our grandparents' generation invented these, and then when they grew up and had money, they wanted to buy back a piece of their childhood.” Maybe it's the same thing with Beanie Babies. Okay, these are the value propositions of these various asset classes, and the value propositions of baseball cards and Beanie Babies both have something to do with nostalgia, I guess, plus that people will give you more money for them in the future. The value proposition for Bitcoin is, I think, twofold. One of them is, “This is a stable store of value because of the fixed supply.” And the other is, “This technology will constantly be in demand by people in authoritarian regimes who want to buy things without their government knowing about it.” And these seem like really different reasons to me than the Beanie Baby reason or the baseball card reason.

[01:43:56] **Mark Stephany:** The next question has to do with the **concentration of mining** or lack thereof and peoples’ concern that if that becomes too concentrated, then **how can Bitcoin claim to be truly democratizing finance?**

[01:44:13] **Bradley Rettler:** I think here there's two key things to think about. As you said before, the word “control.” You control some bitcoin, or you control the private keys, and you pointed out that you don't thereby control *anything* about the Bitcoin network. The same is true with mining. Even if you have a huge mining operation, you don't get to change any rules about Bitcoin.

[01:44:39] You don't get to change any facts about how the difficulty adjustment works, or how much energy it takes to mine the next block, or anything like that. You play by the rules, and if you play by the rules, you get bitcoin – as a miner, who's getting the block rewards. So, in that sense Bitcoin is not under the control of any even sufficiently wealthy person or group of miners or anything. Bitcoin is under the control of the people who are running the nodes. They get to decide which software to run or not. And you can do that with any – basically any – computer that has enough storage capacity and RAM and stuff to run a full node and have a complete copy of the ledger and affirm the rules. Furthermore, we're seeing a lot more publicly traded companies who are doing Bitcoin mining, so they might have CEOs and officers and things like that; but they're owned by groups of people and those groups of people are in a sense controlling that company. And so we're seeing democratization in that kind of way.

[01:46:00] **Mark Stephany: The next question has to do with people's concern that Bitcoin can be forked, or that somebody can make simply a better Bitcoin – that it is the MySpace of cryptocurrencies. What is your response to that concern?**

[01:46:17] **Bradley Rettler:** Bitcoin has been hard-forked a lot of times, but perhaps the two most well-known hard forks occurred as a desire to increase the block size of Bitcoin so that it could do more transactions per second. But of course, that comes at the cost of security. The more transactions per second, the bigger the blockchain gets in terms of storage capacity – the bigger of a computer or hard drive you need to have in order to have a copy of the ledger. And so the fewer full nodes there will be that are providing network security.

[01:47:02] Anyone can fork Bitcoin at any time. It's really easy to do. You just download a copy of the open-source source code, change some parameters that make it incompatible with the current version, and then start running it. The difficulty is getting other people to run it with you! In order to do that, you have to convince them that your version is better than the former version. This is what the hard forks of Bitcoin have been unable to do; they've been unable to convince the vast majority of users and full nodes that their version is a better version of Bitcoin. That's not to say that they haven't convinced anyone. These hard forks do have some, you know… So, anyone can fork Bitcoin at any time; there's an exchange rate, so there are people who are willing to purchase those things with US dollars or with bitcoin. But they don't have the kind of belief in them – as expressed by a market cap – that Bitcoin does. So, it's trivially easy to change the rules, but it's very difficult to convince other people that the new rules are better than the old.

[01:48:13] **Mark Stephany:** Two additional thoughts. One, I'm going to quote directly here from Lynn Alden, who is a prominent analyst in this space. She says, “Bitcoin’s open-source software may be forked; its community and network cannot. So, as it forks, what makes the 21 million units in Bitcoin's network more valuable than the 21 million units in a Bitcoin fork like Bitcoin Cash? Equating the value of Bitcoin Cash to the value of Bitcoin would be equivalent to assuming that Facebook's source code could “fork" and automatically duplicate the value of its 2.6 billion users and its 50,000 employees. Their value stems from Bitcoin’s and Facebook's network effects, not just their existence." This also begs the question: what would you change? How would you improve upon Bitcoin to “make it better”? And I think what we've seen is attempts at that, but clear failures. So what Bitcoin is, is, in turn, what is most desired by its users. Additionally, it's important to point out that Adam Back, one of the core developers and an individual who's been around since the beginning, has often stated that if there is an additional feature that would be beneficial, Bitcoin can take that on. It can be developed on a second or a third layer, but it has to be a consensus among users to adopt it. So all these other things try to be “better”; if in fact enough users do deem that feature to be better, then that's something that Bitcoin can simply adopt. And that's what we've seen with the lightning network. **So your thoughts?**

[01:50:07] **Bradley Rettler:** Absolutely. Not only can it be adopted at a second or third layer, but if the community is convinced that it should be adopted at the base layer, there's a protocol for doing that. And we call these “soft forks”, and they’re upgrades to allow Bitcoin to do more interesting things. What it takes there is the same as before -- it's convincing the community that it's a good thing, that it won't ruin any of the good things about Bitcoin, but that it will add another good thing. There've been lots of soft forks in Bitcoin; we had one just a few months ago now, called Taproot, that upgraded some privacy aspects of Bitcoin and also condensed the block space required to do certain kinds of transactions. So, there's two pieces of good news, right? The one piece of good news is that Bitcoin is going to survive attempts to hard-fork because the community will stick with it, as it has in previous attempted hard forks. And the other good news is there is a mechanism for introducing better-making features for Bitcoin – for upgrading it. What it takes is democracy. It takes convincing a large group of people that they should vote with their full nodes for the upgrade.

[01:51:33] **Mark Stephany:** All right. You ready for a softball? **Is bitcoin expensive? Do I have to buy one full bitcoin at a time?** This obviously is with the premise that you are buying bitcoin solely for its investment function, but is it too expensive? Did I miss the boat here?

[01:51:52] **Bradley Rettler:** Yeah, sorry. Bad news. Right now you need exactly $44,000. No, bitcoin is divisible into 100 million units. That was a design choice – all it would take to extend that to further units is a soft fork; it would not require a hard fork. 1/100,000,000th of a bitcoin is called a "satoshi", and a satoshi right now costs you less than half a penny. For $1, you can have some thousands of Satoshis. Now, in order to buy $1 worth of bitcoin, you're probably gonna want to do that on the lightning network because using block space for that small of a transfer from someone else's wallet to yours would cost as much or perhaps more than you would actually get.

[01:52:58] But yeah, you can invest trivially small amounts, or you can exchange trivially small amounts of dollars for bitcoin. You can acquire trivially small amounts. So you can ask a friend, "Hey, I've been hearing about Bitcoin. I'm kind of interested in just playing around with it. I know you have some bitcoin. How much are you willing to send me for free?" And if they're a good friend, they'll say, "Oh, I'll send you like 5,000 Satoshis just to try it out", and that's a dollar or so.

[01:53:30] **Mark Stephany:** So, again – with the preface that this is a statement based upon people who are looking at bitcoin solely as an investment opportunity, which we've discussed previously is not the only benefit to Bitcoin nor why the majority of its users find it beneficial – but with regard to that, I think it's important to acknowledge what kind of asset classes and market cap we are talking about with regard to Bitcoin. So the obvious comparison is to gold, and the market cap of gold is somewhere between $10 trillion and $12 trillion. But then there are obviously economists and financial pundits who believe bitcoin will start absorbing money from other asset classes, such as art and real estate and the bond market, et cetera, et cetera, which then carries that market cap even higher. You take that, divided by 21 million, and then you get a price per bitcoin. And you can do that math. So to people's concern about being "too late to the party", that is most certainly not the case. And that's enough said on that. The next question that I want to get to is with regard to privacy. **A blockchain is, by definition, public – a public ledger. How could that be considered good for privacy?**

[01:55:00] **Bradley Rettler:** There's multiple ways of understanding privacy. What the Bitcoin blockchain has is addresses and amounts. The addresses are numbers and letters, the amounts are numbers, and that's it in terms of the information about transactions that are made public.

[01:55:23] In that sense, Bitcoin is not private with respect to what addresses have what amount of bitcoin, and what addresses have sent what amount of

bitcoin to what other addresses. But it is private with respect to who any of those addresses belong to – any real-world identities of any people. However, a lot of ways of acquiring bitcoin involve disclosing aspects of a person's real-world identity.

[01:55:56] When new bitcoin is mined, the miners provide an address for bitcoin to go to – anyone can generate an address online easily. And if a miner was to provide that address, nobody would know who that miner was. In that sense, there's a way to have bitcoin where there's no identity knowledge at all.

[01:56:26] Most people who acquire bitcoin buy bitcoin from an exchange. And pretty much every exchange – certainly exchanges in the US and I believe in most other countries – are required to verify the identities of people who are buying. These are "know your customer" laws. So, if you buy bitcoin in the US from an exchange, they know who you are and the government can ask them, "Do you have this address on file? If so, who has sent any bitcoin to it?" The exchange will have to tell them. In that sense, Bitcoin is not private. So, it kind of goes back to the question about criminals using bitcoin. What governments have the power and authority to go to exchanges and compel information about customers? And about which customers are those exchanges willing to divulge this information? For the vast majority of people, if a government tried hard enough, they could find out how much bitcoin that person owns. But again, there are ways around that, and it depends on how powerful the government is in terms of this data-tracking.

[01:57:44] **Mark Stephany:** With regard to Bitcoin being technologically complicated and requiring certain software, such as hardware wallets, **aren't users just being asked to place all their trust into whatever or whomever made the wallet software? How can we call Bitcoin a "zero-trust" environment as such?**

[01:58:05] **Bradley Rettler:** I don't like calling Bitcoin a zero-trust environment. The main reason is because I've read the Bitcoin code and I don't understand it. I'm not a computer scientist. I'm not a programmer. I have a PhD in philosophy. I don't know what the Bitcoin protocol says – despite the fact that it's open source. What I do think, though, is that open-source software in general allows you to *distribute* trust across a range of people. So, what I trust is that people who are knowledgeable about software and programming and things like that – I trust that they know what they're looking at when they read it, and that if there were something in there that would be a problem, that they'll raise an alarm about it and explain to people like me what it means. I think the same is true with wallet software. There are closed-source or ask-for-the-source wallets,

and I would not use those. There are open-source wallets, though, and there I think you're distributing trust across every person who you think is competent enough to have looked at the source code of the wallet and evaluated it and given their okay. And so you could do this by finding one person who you think you align with morally and philosophically and that you trust and just see what wallets they recommend. Or you can pick the most popular wallet and say, "Well, if there was a problem with this one, surely someone would've pointed it out." But unless you're going to learn computer science yourself and look at the source code of all these wallets, you're going to have to have to trust someone or some group. There's a way of minimizing that individual trust that you have to place in any particular person by sort of spreading it out in this way.

[02:00:08] **Mark Stephany:** Bradley, we're coming to our last few questions here, believe it or not. And I think in order to address the question of Bitcoin's environmental impact and whether or not it "wastes energy," we must first clearly state why we believe Bitcoin to be a force for good. Because if you do not believe that it is, then no amount of energy will be rational. So the question becomes, "Is it worth the amount of energy to secure the Bitcoin network and process these transactions?" **And so, Bradley and I want to make the claim that it is. And I will let you take the floor here to make that case as to why you believe Bitcoin is good and why it is able to accomplish certain things that no other asset class – let alone centralized entity – would be able to do.**

[02:01:21] **Bradley Rettler:** We've talked now a lot about the various features of Bitcoin and how it works. And I think we can see that for some people, Bitcoin is valuable.

Everything in the world (pretty much) takes energy of some kind, right? Watching a YouTube video takes energy. Driving a car takes energy. And we can question whether the value of the thing that the energy takes is worth the energy that's expended on it. Sometimes we do this, more often than not we don't. In my circles right now, there's a huge question of whether philosophy conferences are worth the energy that it takes for all the people who would attend them to fly there – the carbon footprint of philosophy conferences is of a certain size, and then there are certain goods that come about as the result of a philosophy conference. And some people think the goods that you get from a conference aren't worth the carbon footprint of the conference, and we should move them off to Zoom, which takes some energy, of course, as well, but less energy. And there are less goods – you don't get to, like, have dinner with your friends. But maybe there the goods outweigh the carbon footprint, whereas for in-person conferences, maybe they don't. So, the way to evaluate all of these is the balance for energy cost versus the benefit. I think when we talk more about

the energy, we might see the energy use as a benefit; but let's hold off on that for a second and talk about the other benefits.

[02:03:05] I said at the beginning that we should evaluate Bitcoin not just for ourselves but for other people – some of whom are not very much like us at all. I think we can see from the way Bitcoin works – its inclusivity, its fixed supply, its censorship-resistance and relative anonymity on a small-scale at least – that it shouldn't be too hard to think of the kind of people for whom this is good. This is a good thing for people who are living in authoritarian regimes. This is a good thing for women who are living in patriarchal societies. This is a good thing for LGBTQ people in societies that want to deny their existence and want to prevent them from finding community and expressing themselves in their purchases. This is a good thing for people who live in countries where their local currency is devaluing. This is a good thing for people who are protesting injustice and are fearful of the government that they are protesting. That's a lot of people in the world that could find great utility in bitcoin as a medium of exchange or as a store of value.

[02:04:26] So, when we consider the energy that it takes to do this, we need to consider all these goods. We also need to consider the alternatives, right? If there's no Bitcoin, the US dollar still takes energy. Maybe you only want to consider the energy that the US treasury and the Federal Reserve computers and the commercial bank computers use. But a large portion of the US dollar gets its value from the US military – in the fact that the US can't be invaded and the US dollar stolen. How much energy does the US military take? And how does that compare to Bitcoin? The main goal, I think, of discussing Bitcoin and energy should be twofold. One, it should be to put the goods in perspective with the costs. And the other thing is to consider the alternatives and the energy costs and the goods of those as well.

[02:05:24] **Mark Stephany:** So, I will take the stage here and do my best to describe why I believe Bitcoin to be good before moving on to the question of Bitcoin and its environmental impact. I believe Bitcoin to be good – again the reason depends upon where you live, how old you are, your other investments (should you have them)… Since the majority of the audience listening to this podcast is from the US, we'll start there – while certainly it stands to reason that individuals in underdeveloped countries and marginalized communities can benefit more from Bitcoin, there's certainly still a strong reason why the average American should consider holding it. One is historical. Aside from the British pound, there is no fiat regime in history that has not been debased out of existence. The monetary and fiscal policies that we are currently living under are, in fact, an experiment that all started back in 1971. So, it's certainly possible

that it's just a matter of time before the US dollar faces the same consequences. And we are certainly starting to see some of that play out. Bitcoin is a hedge against that inflation – maybe not in our lifetime, but certainly the possibility is greater for our children's and our grandchildren's.

[02:06:54] So that's a reason why one may consider Bitcoin to be important – as a hedge against that possibility. The second point that I'll make is that I personally view bitcoin not only as an investment (and I say it's an investment because that's a position that I find myself in my life and the privilege that I have), but I also view it as philanthropy, meaning it is like no other asset class in the world – that rewards greed, not only for the individual user, but for users worldwide. And that's the key – worldwide. I know that when I am holding bitcoin, that that in turn is stabilizing the price, augmenting the price for somebody in an underdeveloped country who is living in an authoritarian regime, who's facing higher inflation rates – that I am in turn benefiting that person.

[02:07:52] Lastly, there are characteristics that we can find beneficial no matter who we are. We can find benefit in an open-source network that is inflation resistant, that is non confiscatable, that is permissionless, that most certainly would appear to be incentivizing renewable energy (as we will get to)… Each one of those elements of Bitcoin – each one of those characteristics – you can examine personally to see where you may benefit from those characteristics. In addition, as Bradley discussed early on in the podcast, we ask that you not only look at it yourself and what it can do for you, but how those characteristics can also apply to others in your family, your community, your state, your country, and worldwide. And again, there's no other asset class like it; there is no other network like it that can provide those same characteristics and benefits.

[02:08:58] I will step off the stage now and hope to get to our final question with regard to Bitcoin's environmental impact. **How do you like to look at that, Bradley? How do you like to frame Bitcoin's environmental impact?**

[02:09:15] **Bradley Rettler:** We talked earlier about Proof of Work and Proof of Stake and why Satoshi chose Proof of Work as the consensus mechanism that incentivizes honest behavior; people have to exchange a different asset—energy—in order to win the right to publish the next block in the Bitcoin blockchain.

[02:09:39] So then we might wonder, “How much energy does Bitcoin take?”, and “Is it worth the energy that it takes?” Bitcoin takes a lot of energy. It uses the same amount of energy as a country like Norway. That’s a lot. It's not as

much as, say, US air conditioners, or US laundry dryers, or even US Christmas lights – but it's still a lot of energy. Some people like to break down the energy into a per-transaction cost to make it sound even higher. But as I hope people who have listened this far realize, the point of adding these new blocks isn't just to add the new transactions, but it's also to keep the blockchain growing so that nobody can go back and double-spend the old transactions.

[02:10:40] So when a new block is published, it doesn't just include the new transactions, but it provides yet another layer of work that someone who's trying to attack the network would have to go through in order to unspend. So, it's really securing all the past transactions as well. So, every new block that's created embeds all the other blocks one more block further back.

[02:11:07] And so it would require an attacker with that much more energy. So, really, we need to look at the energy costs combined with the entire value of all of the bitcoin in the world in order to come up with an evaluation.

That's how much energy Bitcoin uses. But another important question is to ask, “What kind of energy does Bitcoin use?” Here's where things start to get interesting. Each Bitcoin block is about one megabyte worth of data, and those occur every 10 minutes. And to broadcast the solution for a miner is a fraction of that. So, you don't need a very strong internet connection to be able to mine Bitcoin; the very low 3G data is enough. This means that you can mine Bitcoin pretty much anywhere on the planet.

Bitcoin is, then, highly responsive to where the energy is. If you have a source of energy that's out in the middle of nowhere – like a waterfall or a volcano or a desert – you can mine Bitcoin in those places, and you just have to have some way of connecting to a very slow internet in order to successfully do that.

[02:12:39] Because of this, Bitcoin has the highest renewable energy mixture of any major industry, in large part due to this non-geographically-limited ability to be able to be mined anywhere. Not only that, but even the non-renewable energy of Bitcoin is, you might think, benefiting the world. Here's an example. Because Bitcoin can be mined anywhere, some of the non-renewable energy comes from methane that is flared when oil fields are in operation. There are companies that go around and find methane that's being either vented just straight up into the atmosphere, or flared where they vent it into the atmosphere but light it on fire. They will build Bitcoin mining facilities on top of that, and they'll capture the methane, and they'll use it. The resulting waste product [CO2] is much less damaging to the environment than the methane was.

[02:13:54] **Mark Stephany:** I'll provide a quick statistic on that very thing: "America's two biggest oil fields flared and vented almost 500 billion cubic feet of gas in 2019, which would have had the climate impact of seven coal-fired plants if released directly into the air. Crusoe energy systems announced it had plans to set up 70 Bitcoin mining units that year, preventing the flaring of 10 million cubic feet of gas per day." And as Bradley said, what that is doing is essentially preventing methane from being leaked into the atmosphere, which is more potent of a greenhouse gas than carbon dioxide.

[02:14:36] So please, I interrupted.

[02:14:38] **Bradley Rettler:** Thank you. I love the statistic. So, it used to be methane, and now they're using the methane to produce instead carbon dioxide – and to secure a monetary network for all the people that we talked about beforehand.

Bitcoin incentivizes using as cheap and energy as possible. Every little bit of energy goes into calculating the result of these math problems by trial and error. And so the cheaper you can get your energy, the better profits you can make as a Bitcoin miner. The cheapest energy is things like renewable energy, because the wind is free and the sun is free and moving water is free and volcanoes are free. Harnessing costs some money. But the other cheapest energy is waste energy, like flared methane or vented methane. So Bitcoin is incentivizing people to clean up oil fields and there are companies that are doing that. Bitcoin may also…here's where I get a little bit more speculative, but I have big dreams…

[02:15:52] Bitcoin may also incentivize renewable energy production and development. I live in a city of 30,000 people. We have a ton of wind. We have a ton of sun. But we don't have a ton of people. And so creating a huge, renewable energy facility here would be cost prohibitive. This is the same in most cities and towns in America; it just doesn't make sense to build a renewable energy operation there because the capacity for using the energy just isn't there.

[02:16:28] But if the excess energy that's produced can be used to mine Bitcoin, then the renewable energy facility can help to pay for itself, making it a lot more cost-effective.

Another aspect is what we are seeing in places like Texas – that the demand for energy is very up and down. What's happening is during some times of the year, they need a lot of energy. During other times they need less. Sometimes it's unpredictable how much energy they'll need; and it takes some time to bring

energy facilities up to a certain level of production that they weren't the day or the week before.

[02:17:15] Ideally what you'd want is these facilities running at max levels all the time, but not producing any waste energy. You could do that if you're using the excess energy to mine Bitcoin. It's very easy in a matter of a few minutes to turn off Bitcoin miners if you need the energy that they're consuming. What might be able to happen is that energy facilities produce enough energy all the time to run the cities and states and stuff that need it *when they're at their highest level*, but then just vary the amount of Bitcoin mining. So when energy needs are greatest, mine no Bitcoin. When energy needs are least, mine a lot of Bitcoin. Just always be producing as much as we are using so we're not wasting anything, but we're using that excess to secure the Bitcoin network.

[02:18:11] **Mark Stephany:** I don't want to overstep my expertise here, but recently heard an excellent description of renewables – that they are both time and geography dependent, meaning whether that's wind solar or hydro, it's sometimes not sunny, it is sometimes not windy. And those locations are not spread universally throughout any particular geography. So that makes it challenging to utilize renewables reliably. That's the key word – "reliably" – for energy usage. So what Bitcoin does – what Bitcoin mining does – is go into those areas and smooth out those peaks and troughs of energy, meaning Bitcoin mining can be turned on when there's excess energy and turned off when there's not so that the grid can remain functional. What that does is provide a level of financial stability for those renewables to function in time- and geography-dependent scenarios where otherwise they would be less likely to function properly.

[02:19:31] **Bradley Rettler:** Yeah, that seems exactly right.

[02:19:33] **Mark Stephany:** I think we should also acknowledge a common misconception based upon a paper written a few years ago that has in fact made its way to Congress and has resulted in claims that Bitcoin would have raised the global temperature by two degrees by 2020. Clearly that did not happen. **So what went wrong? Why was that paper or problem?**

[02:20:03] **Bradley Rettler:** Yeah, there were a couple that made dire predictions about 2020. I think another one said that Bitcoin was on track to consume all of the world's energy by 2020. And by 2020, Bitcoin was not even consuming the amount of energy that the world had been consuming in the year 2000.

One of the reasons is that there's a diminishing rate of return for each additional energy that's being used, both because of the competition from other miners and because of the cost of that energy. Once you're using all the free energy in the world to mine Bitcoin, that provides a certain number of mathematical calculations per second. When you're deciding whether to pay for energy, you then have to decide how, given the current level of computing power and the amount that I'm going to add: how likely is it that I'm going to win any of these competitions? And how likely is it that I'm going to be able to pay off my energy costs by doing that?

[02:21:15] At a certain price point, it becomes prohibitively expensive. Now, the price of Bitcoin going up means that the cost of the bitcoin will offset that increased cost of electricity. So it could be that at $30,000 per bitcoin, it doesn't make sense to pay 5 cents per kilowatt of electricity, but at $40,000 it does; and so you'll see more miners come on. But in the end, it's always a function of how much bitcoin is worth versus how much the energy is costing; and renewables will always be the cheapest and waste energy will always be essentially free. I don't know exactly what went wrong, because these places didn't provide their argument for this, but I think they assumed the hash rate was static and that the bitcoin price would be at a certain level and a bunch of other assumptions that didn't turn out to be true.

[02:22:26] **Mark Stephany:** I want to list off a couple more statistics here that I think are important for our listeners to know. One is from Cambridge Center for Alternative Finance that estimates the total carbon dioxide emissions from Bitcoin mining would not exceed 58 million tons – or 0.17% of total global carbon dioxide emissions – even if Bitcoin mining was *exclusively* powered by coal. I found that to be quite telling.

Additionally, as we've discussed throughout this podcast, it's always important to compare Bitcoin's features to the status quo. To that end, the Bitcoin network is a much more efficient monetary network than traditional banking and gold mining on a global scale.

[02:23:16] Traditional banking emits 1,368 megatons of carbon per year, and gold mining emits 144 megatons. Bitcoin emits 61 – less than 5% and 45% of traditional banking and gold mining, respectively. So, very telling numbers. I think those should be taken into account when examining the functions of Bitcoin and the good that we have described.

[02:23:48] **Bradley Rettler:** I also think it's important. Someone might be tempted to think, “Well, bitcoin has 1/10th of the market cap of gold. And so if

bitcoin went up in value 10x, then the emissions would go up 10x." That would be a mistake, because if bitcoin went up that much, it would incentivize perhaps a lot more renewable energy production. It would incentivize more creation of Bitcoin miners on rivers and at the bases of volcanoes for geothermal energy, which increases the competition, which makes it harder for people who are, say, using coal or natural gas or things like that to win these mining competitions. So I don't think that there's a linear progression of Bitcoin's carbon footprint along with its price.

[02:24:45] **Mark Stephany:** Lastly, I want to say with regard to the specific question, that there is certainly a strong cohort of Bitcoiners – myself and Bradley included – who are concerned about any environmental impact that Bitcoin may have. We are concerned about climate change. And in turn, everything we do going forward is with that in mind. There are very, very strong initiatives being put forward with regard to how to best study this, how to best address this. And to Bradley's point hopefully – it would certainly appear to be – how can Bitcoin incentivize the build out of a renewable infrastructure for our future?

[02:25:36] Bradley, we did it! Over two hours of incredible content here. I want to get any final thoughts that you have at this point.

[02:25:41] **Bradley Rettler:** Yeah. I want to say one more thing about renewable energy. In my view, limiting carbon emissions and carbon capture and all these things are great. But what the US really needs is to go fully renewable as soon as possible to the degree that that's possible. I think the way to do that is to incentivize renewable energy production as much as possible, and renewable energy techniques. And because of this interesting feature of Bitcoin – it's not geographically limited – there's huge promise for Bitcoin to aid in this endeavor. There's also huge promise because of what the energy can be used to do – namely create wealth – there's an incentive for new techniques to be developed. So I think that climate change is real. I think it's one of the most existential threats that we're facing in the world. And I think going 100% renewable as soon as possible for every country in the world is the best thing that we can do to combat it. And I think Bitcoin has a huge role to play in that.

[02:27:03] **Mark Stephany:** Excellent. Any final thoughts?

[02:27:05] **Bradley Rettler:** I hope that through this two hours and 40 minutes, or whatever it turns out to be on the podcast, that people have been able to understand Bitcoin in a way that they didn't before. That it's gone beyond headlines. And that they've also been able maybe to put themselves into the

position of people who might find this valuable – people who are living in authoritarian regimes or with devaluing currencies – and see why progressives, who are supposed to care about these people, might find value in the Bitcoin network.

[02:27:41] **Mark Stephany:** Absolutely. I couldn't agree more. We'll leave it at that. Thank you so much for your time. This was incredibly generous. I appreciate it. I know this will be very well-received. Thank you so much, Bradley.

[02:27:51] **Bradley Rettler:** Thanks for having me.

[02:27:54] **Mark Stephany:** Lastly, tell the listeners where they can find you and please tell them about your forthcoming book.

[02:28:00] **Bradley Rettler:** I'm on Twitter at @rettlerb and I, along with two of my close friends, have a Bitcoin research collective called Resistance Money, which you can find at resistance dot money, which contains links to all our podcast appearances and all of our written work on Bitcoin. They are Andrew Bailey and Craig Warmke. They're also both on Twitter @resistancemoney and @craigwarmke.

Also, if you feel like you didn't get *your* question answered, email Mark! And when he gets enough for another episode, we can do it again.

[02:28:46] **Mark Stephany:** Do you want to mention your book?

[02:28:47] **Bradley Rettler:** Yeah. The book is under contract with Routledge press and it's called *Resistance Money: A Philosophical Defense of Bitcoin*, where we'll tackle moral issues like censorship, privacy, and end with a cumulative evaluation of the cost and benefits of Bitcoin in determining whether it's a net overall good for the world.

[02:29:14] **Mark Stephany:** Bradley. Thanks again.

[02:29:16] **Bradley Rettler:** Thank you.