the art of boring™

EP87 | Why investors really need to understand the mechanics of Bitcoin

Rob Campbell: 00:00 This is a podcast about Bitcoin. One of our beliefs here at Mawer is that context matters, meaning that opinions based on surface-level knowledge can lead to flawed biases and invite risk.

With that in mind, my colleague Justin Anderson takes us through a granular look at the technology underpinning bitcoin—effectively diving into both the "crypto" and the "currency" sides of cryptocurrency. After which, Justin hands out some grades as to how well he sees bitcoin performing as a currency, as a store of value, and a few other categories.

Since we recorded this podcast in early May, a lot has happened in the crypto world: we've seen large swings in the value of bitcoin and other cryptocurrencies; Elon Musk, of course, has continued to move markets with his tweets; and we've seen a crackdown by China on crypto miners.

00:49 As you'll hear, the reason Justin and some others at Mawer have deepened their understanding of Bitcoin was better situational awareness in making investment decisions. And what I appreciated about this conversation—and fair warning, it does get technical—beyond Justin's curiosity and passion itself, was that it has elevated by own situational awareness. Meaning, that better understanding of the technology itself has allowed me to better understand current events in the crypto-world and evaluate their implications.

I hope you enjoy it as much as I did.

Disclaimer: 01:43 This podcast is for informational purposes only, information relating to investment approaches or individual investments should not be construed as advice or endorsement. Any views expressed in this podcast are based upon the information available at the time and are subject to change.

Rob Campbell: 01:59 Justin, we're here to talk about Bitcoin, and well, I wanted to start just based on our tagline of, "Be Boring. Make Money.TM" Part of that I think means avoiding investment fads or not trying to get caught up in the latest investment craze.

We're talking about Bitcoin; I'm sure there are some of those out there listening thinking, "Is this the next investment craze?" I thought I'd start just by asking, why are you and some others at the firm looking at Bitcoin? The technology itself? Apart from being our technology guru, what has driven your interest into Bitcoin?

Justin Anderson: 02:34 Yeah, thanks, Rob. It's great to be back on the podcast. I think it's a really fair question. Like, "Hey, there's lots of fads, our strategy is Be Boring. Make Money.TM…why are we looking into this?" I mean, I think one of the big ones is just the size of these markets. They're becoming global in scale. Bitcoin [is] roughly—today, if you add up all the bitcoin and the value of that bitcoin— it turns out, that's about the GDP of Spain.

Rob Campbell: 03:00 Wow.

Justin Anderson 03:00 So it's huge.

In context, relative to gold, it's about an eighth right now of the size of the gold markets. It's starting to play with the big boys. We're looking at that and saying, "Hey, we've got to really wrap our head around these markets and understand what's going on here." That's one.

Another element would be—our job as investors, as portfolio managers, is we're managing risk. Managing risk means looking at the different forces that are happening in the world that could impact these businesses that we're investing in. So, a good example would be Visa [and] MasterCard, which would be a couple companies that we own [and] have large positions in, and something like Bitcoin and these alternative payment mechanisms can impact those businesses. We need to understand these risks and opportunities that are out there.

03:46 A couple other points I would say, is Bitcoin's rise is also impacting a lot of the direct holdings we have. Like Square is an example of a company [that are] actively buying bitcoin, they're helping people buy and sell bitcoin, they're running an exchange on their platforms. So, there [are] companies that directly are involved in this as well.

And then I guess the last point would just be coming back to our culture. We talk a lot about curiosity being a key part of what motivates us, and we believe that being curious makes you a better investor. A better, well-rounded investor. So, part of this is just running back to that cultural foundation and getting curious about the world and what's happening in the world.

Rob Campbell: 04:23 Perfect. So, curiosity and then just this situational awareness, being aware of things that are getting bigger, that may impact positions that we already have. So, let's dig into it! I know that you're going to take us on a fairly basic and detailed approach to understanding Bitcoin. Can you start with why you think it's important to understand the mechanics? There's been lots of publications about blockchain and Bitcoin and other cryptocurrencies. What's missing from them that you think is important? The reason that you're going to take us on this journey to really understanding how some of the code, and how you actually go about purchasing bitcoin?

Justin Anderson: 04:56 Fair point. I think one of my learnings is, there's a lot of material out there today on Bitcoin, on blockchains, you can look up podcasts…and what I find often lacking from an investor's perspective, is an investor dive into the actual details of, how do these work? And why is it that people get excited about these technologies?

I think part of it is, if you just stay at the very high level, sometimes you can lose the understanding of what is it that, when people talk about these being "trustless," why is it that they're trustless? What's the mechanism that's driving that?

05:28 So, part of the idea when I reached out to you, Rob, about this podcast was like, "Hey, let's dig a little deeper and open up the Pandora's box a little bit and just help investors understand what's going on here." So, the risk is we might get a little technical for folks, but maybe that'll be valuable for people.

Rob Campbell: 05:45 Okay, so it's worth jumping in at "Crypto 101," you're not going to the advanced courses right away, even though this, I think, will feel like quite an advanced course for many of us.

You mentioned trust, and I thought that would be a good place to start, because it seems like this is a big "why" behind blockchain technology in general. Can you start with the problem of trust? Just…in society that we faced for generations?

Justin Anderson: 06:07 I think it's good to take a step back before we get into the detail and just look at this from the "30,000 feet" perspective, and understand a little bit [of] what gets people so excited, a lot of these Bitcoin visionaries…what is it that's animating all this excitement?

You hit on it; it's really about this concept of trust. If you think about trust in society, for hundreds and 1000s of years, the amount of money and resources that people have put into trust is just enormous.

06:07 And so, towards the end of last year was when I think NetEase became on our radar, because people in Tencent, people in onshore Chinese game developers—everyone's telling me the same story that, "Hey, this company is very good with innovation. They're best in class." And so, [in] IEF, we decided to take a look at NetEase.

Justin Anderson

06:35 I'm reminded on a holiday that I took a couple years ago now—before the pandemic days—I was in a museum and noticed they have all these old papyrus scrolls. These are these ancient scrolls that people used to write, and it was this long tedious manufacturing process to get the reeds out of the river, and then lay them all out and dry them all out. People just put huge amounts of limited resources into these paper documents.

And if you actually read what was on these documents, it's fascinating. It wasn't some colorful cultural history of kings and queens and what people were doing, it was documentation of these transactions of who was buying what and who owns what and essentially trying to inculcate a certain level of trust using the limited resources they had to encourage trust in interactions and transactions.

07:23 That papyrus of the past...you fast forward to today, and we continue to invest huge amounts of societal resources into trust. If you think of our political system, the laws, and all the effort that goes into creating laws, the bureaucracies, the regulations, the police, the courts, the banks, all of these institutions...a big chunk of what they're really doing is making sure people can trust each other when they're interacting or engaging in some transaction.

There's actually a Nobel Prize winning economist Douglass North—he put out the idea that lowering transaction costs, which is a function of high trust, is one of the core mechanisms that actually created the societies that created the most wealth in history, and makes the case that, "Hey, it's all about low transaction costs."

08:11 So, trust is at the foundation of that. It's at the foundation of our society. And so, coming back to what people get so excited about Bitcoin, it’s like, "Hey, is there a way that we can inject this trust and achieve the same level of trust at a much lower cost?" We'll get into a little bit [more] about that, but I think that's the core mechanism of what excites people about this technology.

Rob Campbell: 08:33 And you're talking about trust at scale, really. At a societal level. I'm just thinking about—I play online risk with a couple of my college buddies, and it's always the same people. We have these side deals with each other, we tend to honour them, because we know we're going to play again, and we don't want to undermine each other. But at scale, you need something to enforce that trust. I think you referred to police departments and courts and property rights—things like that. But these institutions that have developed, leading to these lower transaction costs. Can you just talk about that a little bit?

Justin Anderson: 09:04 You and I and others in these advanced societies—we're swimming in the soup of institutional trust. We take it for granted. It's all around us. If I go and buy a car from a stranger in Canada today, there's a 95 plus percent chance that the person is going to deal with me in an ethical way, and that I can expect that. That's not normal for the history of mankind. I mean, most of history has been people that have not always had trust. As soon as you go down to—I don't know what the number is—but you start ratcheting lower that percentage of how much natural trust is in the society, the transaction start to break down, and people start to revert not to trade, to get what they want, but to war and to fighting to get what they want.

09:45 So, trust is really at the root. I think one thing to understand about trust too, is, there's this tension between centralized trust and decentralized trust. That's where we're getting into Bitcoin a little bit. But the tradeoff there, is a lot of trust today is coming out of centralized patterns. Governments for example, that have a monopoly on force for example, or have that central control of the ability to issue currency or whatnot. There's a lot of advantages to centralized trust, because it comes with cost advantages, scaling effects. A lot of the typical economies of scale that we look at is, if you centralize everything you can achieve economies of scale, and deliver trust at that lower cost.

10:27 The promise of Bitcoin and blockchains more generally, is that, "Hey, we can actually offer a more robust, decentralized mechanism of trust that comes at the same or even more efficient cost of that scalable version that we've lived in the past on."

It doesn't mean all these ideas are necessarily going to come to pass, and it doesn't mean that there's no problem with a lot of them. But this is the kind of vision that is animating people who are excited about these technologies.

Rob Campbell: 10:53 Got it. So it continued lowering in the costs of trust or transaction costs in society?

Justin Anderson: 10:58 Exactly. Yeah, achieving a more robust trust mechanism through decentralized networks, but not sacrificing the low cost of, say, a centralized model.

Rob Campbell: 11:09 Okay. For many people thinking about Bitcoin, it's currency first. As we get into what it is, maybe that's the place to start: what is the link between a currency and this element of trust?

Justin Anderson: 11:22 Well, currency, I mean, it's almost at the very foundation of societal trust. It's the mechanism that we all collectively agree upon like, "Here is the thing we're going to trade, and I'm going to give you this." It's a real psychological phenomenon. We'll get more to that when we talk about the implications of Bitcoin. But people have been using different types of currencies for a very long time. I mean, some of the things you're looking for in a currency is A) is it scarce? You don't want a currency that if it turns out, I can just create or copy instantly a bunch more of them, then that undermines the nature of it. So, people are looking for scarce resources that represent their currency.

12:04 Gold has historically been sort of a “top shelf” currency because it is naturally scarce, and even as the price rises, the production doesn't rise with that price, because it's very difficult to mine more of it.

Rob Campbell: 12:15 Okay, let's get into Bitcoin then. I'm going to buy bitcoin. What do I do, and what does it actually mean when I go to buy bitcoin?

Justin Anderson: 12:23 Ha! So, let's start with digging into the technical side: cryptography 101. Let's actually really understand what technology is underlying this.

Bitcoin—people refer to it as a cryptocurrency. What does that mean? When people use the word “crypto,” they're really referring to cryptography.

And the concept in cryptography—if you remember from your World War II movies… I’m sure you’re educated on [that], Rob—is there's the Enigma machine that the German army used to send messages to each other. The Enigma machine was a kind of cryptography device. So what it was, was, you would run a message through it, so you'd have your message, you'd run it through the machine, and it would create a garbled message that only someone who had a machine could decipher and untangle that message.

13:07 So in the terms of cryptography, what we can think of is, in this case, you're sharing the private key; the Enigma device is acting as a private key or way to unlock this message.

Justin Anderson

13:19 But the problem is, you need to get together with the person that you want to send the message to before you send them the message. For example, I need to go to the submarine, install the Enigma device on it, and now I can send the sub out into the ocean. Now I can send them crypted messages.

But in the world of the internet, there's a different problem, which is oftentimes we don't have the luxury of getting together and trading that device and ensuring that, "Hey, I know that it's you Rob, here's the device, and now we're going to talk." We don't have that luxury.

13:45 So, this was a real problem for a long time for the internet. And some mathematicians—I just want to remember their names: there's [Ronald L.] Rivest, [Adi] Shamir and [Leonard M.] Adleman—they came up with this algorithm, essentially, or this encryption mechanism to allow people who didn't have to meet to be able to still send safe messages towards each other.

So, the concept—we'll dig into it a little bit, it's a little detailed—but the basic idea is that, think of each of us in a node. So, each of us are individuals acting in a network, and we need to send each other messages, and we don't want other people in the network to be able to hear those messages and decipher what we're saying. So, we want to send secure messages to each other.

14:28 The first thing you do is, each of us, we assign each of us essentially a lock. It's our unique lock that only you or I on our individual nodes can open with our own private key.

And then the concept is, if I want to send you a message, I take my message, I encrypt it using your lock. So essentially, I borrow your lock, which is unlocked, I put the message inside the box, I then lock it, and you're the only one who actually has the key. So, everybody can see each other's unlocked locks—those are the public keys in the network—and we can grab whichever unlocked lock we want. But once you lock that lock, only the holder of the private key for that lock can actually open it.

15:10 But at the foundation, that's the standard that Bitcoin uses in order to send secure messages to each other, is this concept of encryption, of me being able to take your public key, encrypt an amount of bitcoin that I want to transfer over to you, and then only you are able to provide the private key to unlock that and therefore send it to somebody else.

Rob Campbell: 15:32 Okay, so Bitcoin is then based off of fairly standard encryption technology that's developed with the internet over time.

Justin Anderson: 15:39 That's a great point. To build on that point, when you're actually talking to someone on the internet, you oftentimes, if you look in your browser, you'll see a little lock in the top left of the browser, if you're on like a bank website, or if you're on some website. And that's actually a sign that you've got an encrypted connection to that website. These website technologies are using the exact same or similar principles, which is when you first try to talk to a website, you want to verify that it is the true website that you are intending to talk to—it's not some third party that's corrupted. So, they'll use similar technologies where they'll start by trading public keys, validate each other's identity through the private key, and now once we have validated the identity, we can trade a private key and start to interact securely.

16:26 So, a lot of this stuff is actually leveraging the similar kinds of technologies. What makes Bitcoin quite unique from that is, we start to have a global blockchain that everybody agrees—a single ledger—that everybody is agreeing upon. And that's the concept of the miners, which we'll get into in a second when we get into the mining side of Bitcoin.

Rob Campbell: 16:42 So encryption is pretty standard—usually used to pass information from one to another. The difference with Bitcoin, I guess, is that the information that we're passing is Bitcoin, so it's ownership over a digital asset. The other difference being that the validity of that transaction is being rated by others on this network.

Justin Anderson: 17:02 That's right. You can think of the problem that, sure I can send you a message that says, "Hey, I'm going to send Rob 10 bitcoin." I can send you that message, but we also have this other problem that, everybody on the network has to agree that I indeed, sent that message. It's one thing for you and me to agree to that, and it's another thing for the entire network to accept that that happened.

It's this sort of communal problem, this communal ledger problem, that makes it a much more difficult problem than just securely transferring a message between you and me.

Rob Campbell: 17:34 Okay. I'm just thinking about banking, when I'm trying to send information via an e-Transfer—the one that validates the transaction—there is my bank, RBC effectively, and that's the centralized approach. The decentralized approach would be to say, "Hey, let's make these transactions completely public and everybody can see all the transactions that are going on." And the way that a transaction gets validated is by everybody saying, "Yep, looks like a valid transaction."

Justin Anderson: 17:59 Yeah, that's right. I mean, at the core of it, RBC would be the only holder of the ledger in that case, versus Bitcoin, where that copy of that ledger would exist on hundreds or thousands of nodes that are all checking each other and achieving consensus that this is indeed the state of the blockchain today.

So, rather than one copy being controlled by a single central authority, it's a decentralized architecture. And you had asked the first question about, "Okay, well, how do we now actually sign up for Bitcoin?" So, you might think, "Oh, maybe there's a sign-up form or something. I go to some website, and there's a sign-up form." No, that doesn't exist! [Laughs] If you want to sign up for Bitcoin, you can do that almost instantaneously by just generating a private key for yourself. What is a private key? A private key is just a 256-Bit number. So, think of 256 ones and zeros in a row, and you can represent that in different formats. But that essentially is a private key.

18:54 And then what Bitcoin does is, you "hash" that, which is a one-way function. You take that private key, you hash it, and that eventually becomes your public key, and that's the thing that you send. Remember we talked about unlocked locks that you're sharing with the network? That's that public key that you expose to everybody. And if anybody wants to send you bitcoin, they take that public key, they encrypt the message that they want to send you bitcoin [with], and then only you, the holder of the associated private key, are able to unlock that. That's really the sign-up mechanism: [to] randomly choose a key. And now you can send transactions.

Rob Campbell: 19:30 Got it. I want to go back to the bit you were talking about before, though, which is that, well, originally, we'd stated that, part of the excitement around this technology was that it would lower transaction costs. But it strikes me in that example, with RBC, isn't it a lot more expensive for all these different participants on this decentralized network to maintain their own ledgers? Versus a single central authority? Help square that for me. Where is the reduction in cost coming?

Justin Anderson: **19:56** It's a really good point. I think a lot of blockchain technologies today...it's very application-dependent on whether you're actually achieving a lower cost architecture. It does depend on the application. A good example would be payments. So, today using bitcoin to make daily payments—like you go to buy your coffee or you pay your rent—it's not at scale, it's not set up for that. One of the main problems for that is just the size of the individual transactions or blocks that you can actually append to the blockchain, they're limited. And that limitation basically means that you can only handle a certain number of transactions per second on the network.

20:36 And that essentially means as a currency of exchange, as it is today, it's not feasible to use bitcoin at scale for that. It would be too costly, essentially. And essentially impossible in this case, because of the size limitation. So, there's no question that in certain applications, the cost is either prohibitive or not efficient. So, it's very, very application specific. But the general answer to your point is that, there's always been this tradeoff between the low cost of a centralized approach versus the high cost, but the robustness of a decentralized approach.

21:12 The robustness is very important when you're talking about trust and security, because if I can trust in the system being secure, that adds a lot of value for me, and I'm willing to pay a premium for that. Whereas in your RBC model, yes RBC itself today you might trust. But you can imagine that over time, central holders of truth or central authorities—governments for that matter—essentially inevitably become corrupted at some point. Whereas the idea of blockchain is like, "No, this won't get corrupted. It's by its nature, it's too robust to get corrupted." So that often does come with higher cost, but the idea is that the blockchain is reducing the cost significantly, so that tradeoff is becoming more attractive to the decentralized side of the equation.

Rob Campbell: **21:55** Okay. In that model, every time that there's a bitcoin transaction, a block effectively gets added to the ledger. This ledger is validated by the participants on the decentralized network. What's actually incentivizing people to participate in this, or the various nodes of this ledger? What's in it for them?

Justin Anderson: 22:15 The nodes in the ledger are called the miners. You've probably heard about miners “mining” blocks on the blockchain. Think about if you're a miner, what are you really doing? What's the perspective from the miner? The first thing you're doing is, you're taking all the proposed transactions that are out there. So, if you wanted to send me bitcoin, you would create a transaction, and what that transaction would be, is a key, essentially a key that would show that, "Hey, I can unlock a transaction that had been sent to me, Rob.” So I'm unlocking that transaction showing that I'm the valid holder of the private key associated with that public address that was sent to me, and I am now addressing and taking Justin's public key and I'm encrypting a new transaction that has me sending coin to him.

Justin Anderson: 23:00 That's the proposed transaction that you've created; you now put that out there into the world. How do you do that? Well, there's various—they're called mempools—but they're places where, essentially memory pools where you can dump these proposed transactions. And that's where the miners are going and collecting and aggregating all those proposed transactions, and they're picking up these transactions, putting them together into the block.

23:24 And part of that aggregation of putting everything into the block is they're also trying to solve a complex problem—essentially, doing a brute force hashing process, where they're guessing what's called a “nonce,” which is a random number, putting it into this hashing function, and then generating a hash from that. They keep doing that over and over again trillions of times to randomly generate a hash that is lower than a work threshold. Basically, a target hash threshold.

23:52 Once they achieve that, the first miner that successfully finds a hash that does meet that criteria, they are then given the right to mint new coin. It's sort of the reward that they get for providing all this verification process. Then when they get that reward, they can mint those coins into their own public address. They then show the rest of the network, "Hey, here's the nonce, here's the hash that generated, all the other nodes can now validate that indeed, this miner was successful at finding a hash that was below the target hash." So they validate it, everybody updates their copy of the blockchain with that new block that gets added, and then the process repeats itself.

24:34 So essentially, the miners’ function is twofold. One is—the whole reason we're giving them and minting this coin is we want them to validate all the transactions; the mempool full of transactions. We want them to go through, gather those up, and run essentially the unlocking script that validates that you are indeed the holder of the private key associated with the cryptography side of it. That's one aspect of it. The other aspect of it is recreating over time a difficult, very expensive to replicate blockchain. Because of all the work that is going into generating these hashes, you cannot just go back and replicate.

Justin Anderson: 25:12 This is actually a really important point, because what it means is the moment that you...let's say, you wanted to go and manipulate the ledger, you're like, "Okay, I'm a bad actor, I want to go back and change the transaction that happened three years ago.” You sent me 10 bitcoin, and you're going to erase that transaction so that you can send that bitcoin to someone else now. You go and try to erase it, well, you can't really do that, because you'd have to recreate all the hashes—subsequent hashes—from three years ago until today, and each of those would require an enormous amount of computational power just for each of those 10 minute blocks to achieve.

25:48 So, it's functionally impossible for you to recreate it. The best you can do, even if you did take over 51% of the network (as people talk about the 51% attack), is you could only manipulate stuff going forward. There's the sort of staying power to the blockchain that happens with all this proof of work or this computational effort that goes into it.

Rob Campbell: 26:07 I want to come back to the 51% a little bit later, but effectively, the miners are validating transactions; they're getting rewarded through the ability to mint coins.

And this is where the system is just so elegantly set up, isn't it? In the sense that depending on how quickly new coins are being minted, there's almost an equilibrium going back to the point you made before with regards to the scarcity. There are only a certain number of bitcoins that will ever be. Can you talk a little bit more about that and how the system calibrates itself?

Justin Anderson: 26:36 We talked about this a little bit at the intro, but the hardness of a currency is really a function of how supply and price are linked. So, if the price goes up, to what extent are you able to increase the supply? Because obviously, the motivation to increase supply goes up as the price goes up. Traditionally, why gold was such a successful currency or store of value, was that as much as the price went up, it still was very hard to find more gold. That supply made it a hard currency.

27:03 Bitcoin is essentially perfectly hard, in the sense that there is no relationship between the price and the supply. So, it doesn't matter if the price is a million or $1, the rate of supply is going to be the same.

And that's a fascinating technological achievement that makes it a perfectly hard currency. That has to do with, for example, if the bitcoin price tomorrow dropped to $1 or crashed, what would happen is a bunch of miners would stop mining and a lot of the computational power that they're putting to bear right now on mining, they would just pull that off, because it wouldn't be economically worth it.

Justin Anderson: 26:16 And what would happen is the target hash that you have to solve in order to mine new blocks, would become much simpler. The complexity would require a lot fewer hashes in order to generate or find that target hash.

And vice versa: if the computational power ramped up, then the hash would get more difficult to crack. So, it's got this mechanism that is always floating that makes it impossible to connect the price to the supply. That is really the core beauty of what makes it such an effective store of value.

Rob Campbell: 28:07 That's amazing. Let's go back to the 51%. I know you mentioned it, but important to understand with regards to the trust in this decentralized network—effectively with this democratized approach to validating transactions, a risk is that, a single actor just becomes really large and controls outright or indirectly a number of the nodes that validate these transactions.

Can you just talk a little bit about that, and whether you see that as a real risk for blockchain?

Justin Anderson: 28:35 Let's take a step back and talk a little bit about the problems with proof of work. So, we've talked about this mining issue and how there's all these miners, and they're spending all these resources. A lot of folks are looking at this and saying, "Hey, why are we wasting all this electricity on this mining process? It seems ridiculous and bad for the environment." And these kinds of criticisms.

There's an alternative approach that people in blockchain are talking about, which is "Proof of Stake," and what that amounts to is saying, "Hey, instead of cracking all these difficult-to-crack hashes, why don't we just make all the nodes in our network, put up whoever wants to validate and win and mine coin, let's make them ante up some coin that is at risk if they ever engage in fraud," essentially.

They put up a certain amount of value, and they randomly get chosen based on how much they've put up to be chosen to be the winning miner, essentially, for that block creation. And if it turns out that the majority of the network feels like one node has engaged in fraud in some way, then they can vote them off the island, their coin gets absolved and distributed to the rest. And that is essentially the proof of stake concept. The idea is that you would require a lot less computational power.

Justin Anderson: 29:49 There's a lot of debate within the Bitcoin and the cryptocurrencies in general about Proof of Work (POW) versus Proof of Stake (PoS) and advantages and disadvantages of both. But I just wanted to start with that just to tell you that there are people who are worried about that, and they're coming up with different ways to solve that problem of all the computational energy.

The 51% attack—one of the arguments that the Proof of Work people say is that the Proof of Stake is a lot more exposed to the 51% attack problem than the POW. And that is partly because of the history that I've talked about—of how you're creating a very difficult to replicate problem over time.

30:23 Every time you add a block, you're actually making it more and more difficult to cheat back in time. Whereas PoS—the argument goes that it's more doable under a 51% attack to go back and recreate the past in a fraudulent way. So, that's just a long way to say that the main risk factor, I think, to these protocols, is the 51% attack.

Basically, you take over more than half of the network, and then you can start to manipulate it. I think one of the things that counters that risk as well is, you would be winning a prize of no value. The moment that you successfully took over 51% of the network, everybody would say, "Oh, it's now corrupted, I'm not going to deal in bitcoin." And it would be the end of it. So, wouldn't be much of a prize to win. I think that's another mitigant on that risk.

Rob Campbell: 31:08 Interesting. Can we just shift towards...we've been talking specifically about Bitcoin; I'm sure listeners have heard of broader applications of this blockchain technology. Can you talk, first I guess, about other cryptocurrencies? How they're different and what some of their applications might be? And then beyond that, beyond currencies?

Justin Anderson: 32:28 I think most people in blockchain...they get really excited that, "Hey, it's not so much Bitcoin that we're excited about, it's this idea of decentralized ability to manage information." That's where the most notable, not necessarily competing blockchain, but protocol that is comparable—is Ethereum. The idea there is, imagine the same protocol as Bitcoin, but let's inject flexibility on what we actually put inside the individual transaction. So rather than being limited to moving bitcoin back and forth, we can put inside a transaction almost anything we want. We can spin up a smart contract that says, "Pay Rob, if the Oilers win the game, and pay Justin if the Flames win the game."

Justin Anderson: 32:08 It would be a smart contract that we could use all the same technology, the same cryptography to send messages; the same transaction process that we've been talking about today. But instead of moving coins around, we're putting different sub transactions into that transaction piece of the block.

So, that's really what Ethereum is all about. You can imagine you release that degree of freedom, you introduce a lot of complexity, because now you've got to specify, "Okay, how do different transactions look?" And then it opens up the Pandora's box on the different types of applications that people are potentially going to put on here.

32:39 One of the more recent ones that is pretty hot in the news is these NFTs, non-fungible tokens. Just think of this as one of the long tail of potential applications that people can use blockchains for. This case, an NFT—what you're doing is in that transaction part of the blockchain, you're putting a token in there, a unique token that can still be transacted across—so I can send you my token—and now you own the token.

But it introduces this other really fascinating problem called the "Oracle Problem," which I guess I'll introduce right now, since I just introduced it [laughs], which is this idea that...one of the beauties of Bitcoin is that all of the data relating to the architecture is on the blockchain.

33:19 So, there's nothing outside, external to the ledger that you need to worry about. Whereas in a lot of these new applications, like NFTs, that token is actually pointing to something off of the blockchain. It might be pointing to, like an image and saying, "Hey, there's a website that has this image, and this is the image." Smart contract. I just talked about Flames and Oilers game. So, in that case, if we put that into the blockchain, we would have to have a rule that says, "Okay, who's actually going to decide if the Flames won or if the Oilers won?" So, we might say, "Okay, we agree that the NHL is going to be the arbiter."

33:53 So, pretty soon you'll see that you're actually pointing to some external authority to decide truth and decide what's the outcome. Then that sends it back to the question—

Rob Campbell: 34:03 Takes you right back to the beginning.

Justin Anderson: 34:04 —what are we doing? If we're just going to use a central authority, why won't we just go to the centralized approach? Why are we dealing with all this decentralized complexity? That in a nutshell, when you're reaching off chain, is essentially the Oracle Problem. And it undermines a lot of the applications, but not all of them.

I think people do have ideas on how you can manage that issue, because the idea is that you're decentralizing the transaction piece of it, and you could still have central authorities that you farm out, maybe you have multiple people who have the right to. There are ideas of how you manage that risk, but it's one of the challenges that faces blockchains that are reaching off chain.

Rob Campbell: 34:40 Justin, having done all this work, and understanding the real mechanics behind Bitcoin, I'm wondering if you can score for us your story, your assessment, of Bitcoin specifically, first, as a currency. We touched on this a little bit, but maybe just to summarize your thoughts on Bitcoin as a currency.

Justin Anderson: 34:58 The grade I gave it was a failing grade as a currency, and [there are] some reasons for that. One is the transaction friction is very significant. So, if you do want to use this to do a transaction, you've got to spin up a transaction, you got to put that out onto the blockchain, you got to wait 10 minutes. Fact, in Bitcoin, you might actually have to wait a little bit longer than 10 minutes to ensure it goes through for another problem, which is as the miners are trying to solve this problem, you may have the case where two miners crack separate sets of transactions at the same time; they both solve the problem, and you now have two competing chains that are starting to emerge.

35:36 So the way they get around that problem is they just say, "Okay, we'll keep going, it's okay to have two chains." One half of the network might be trying to solve this chain, and then building on this on chain A, and the other half on chain B, and then as soon as the next block is mined, whichever one happened to do it first—that would essentially, the longest one, would become the official one the rest of the nodes would switch over to. So it uses this longest chain mechanism. But the implication of that is that it might take 30 minutes, 40 minutes, an hour until you're really confident that your transaction is complete.

Justin Anderson: 36:06 If you're purchasing something, the requirement to wait an hour to get a process transaction is going to make it very difficult to use as a currency. Another problem is the irreversibility of it. Our credit card networks for example, they're very sophisticated in that there's a third party involved and they're basically giving people a dispute mechanism that allows them to dispute a transaction and add that third-party person into the relationship. In Bitcoin, you don't have that. Once you've sent the bitcoin, it's done, it's gone to that other person. So, there's no way, you just have to depend on their good graces to switch it.

36:40 I think the most fundamental problem is the size. So, there's the megabyte limit on individual blocks of just how big these blocks are allowed to be. That limits how many transactions you can shove on an individual block, which limits how many transactions you can do, and that makes it, as a currency, basically impossible to be used. It's interesting because folks have [seen] that problem and you may have heard of Bitcoin Cash, which is a bit of a competitor to Bitcoin—it was a major debate in the community where the Bitcoin Cash people, they wanted to increase the megabyte limit from one megabyte to eight megabytes on the blockchain in order to facilitate as more of a currency, to say, "Look, we need a bigger block in order to facilitate more transactions."

37:21 So there was a real fundamental debate within the community and Bitcoin Cash actually was a fork that took essentially the Bitcoin protocol, but just changed some minor things such as the blockchain size, or the block size, and went off on its own.

So, I think the fact that Bitcoin has stuck to the one-megabyte limit, really is the final nail in the coffin—at least for the protocol as it is for Bitcoin as a currency.

Rob Campbell: 37:44 Okay. I'm just trying to imagine—I ordered sushi last night, we got some takeout. I paid with my Visa, it took a second for it to get approved. If I had to sit and wait there for 10 minutes, it wouldn't be very pleasant, if not more to get those transactions through.

Justin Anderson: 37:57 [Laughs] Exactly.

Rob Campbell: 37:58 I can get that, but I guess my curiosity then is that your degrade is really specific to Bitcoin. Other cryptocurrencies like Bitcoin Cash or others that might come along and get widely adopted, those concerns might go away.

Justin Anderson: 38:11 That's true. There's no question that maybe an Ethereum-based blockchain or some other cryptocurrency could rise.

I think, for the landscape that I see today, I don't see any of these cryptocurrencies that are in a position that they're really playing this role. I think it's quite a difficult competition to compete with the Visas and the Mastercards of the world that do have these incredibly scaled, sophisticated platforms for exchange. And so on the currency issue, I mean, obviously, the future is impossible to predict and we have no idea where this is going to go. And these technologies...someone could come up with an application that could do it, but I certainly don't see it out there today.

Rob Campbell: 38:47 Second grade—an attribute that many people assign to currencies as well—but just as a store of value, Bitcoin as a store of value. How do you grade it there?

Justin Anderson: 38:57 Yeah, I mean, it's a very different story. I think as a store of value, I give it an A grade. I think it's really got a lot of these attributes that you look for in a store of value. The most important one of all is psychology [laughs]. The thing with psychology, if you think about currency, if you take a step back, and [think], "Okay, well, why do you value the American dollar, or why do you value the Canadian dollar, or why do you value gold?" A lot of it, what percentage of it I don't know, but a huge piece of that is just [the] why you value it—because other people value it. And that's it.

39:25 I mean, if you look at the U.S. dollar, it's just a piece of paper. And it's not even backed by anything today. I mean, it's backed by the U.S. government, which is significant, but it's not like it's tied to gold like it once was.

So, that psychology is partly why we're talking about Bitcoin today, because Bitcoin has reached a level of prominence in the wider society, that if you look at surveys, people are increasingly saying, "Yes, I do give that value. Yes, I am willing to assign that value."

39:50 I think there was a survey we were looking at [that said] something like 55% of people said they are planning to buy bitcoin in the U.S. sometime in the next couple of years. That's quite an achievement: 55% for some digital cryptocurrency. I think that's number one; just the value that others are giving it actually really does matter.

Rob Campbell: 40:06 Can I interject? Just because I think it's one thing that I've wrapped my head around more recently—is this is not unique to currencies, this is not unique to digital assets... this is true of lots of things. I mean, just think about art. It's pretty subjective; there's no intrinsic value. Maybe you could do something with the art if you weren't using it as art, but we give it value because we all agree that the Mona Lisa, or whatever piece of art, has value. That's a subjective, collective psychological commitment that gives those things value.

Justin Anderson: 40:34 I completely agree with you. I think one of the biggest strikes against it—if I was going to say, give it an A instead of an A+, for example—is the argument you just mentioned. Which is, what's the potential value of it independent of the psychological value? So, real estate is a good example of a store of value that does have obvious use outside of a store of value.

Rob Campbell: 40:57 You can farm it.

Justin Anderson: 40:57 You can farm it, you can build a house on it. People make the same case for gold, but it's definitely more limited. It does have some industrial uses, but certainly not in line with the value that it's priced at. There's a huge premium for psychology there, and so on down the line. Like, paper currency certainly is pure psychology.

I think the use of the thing does matter. Or, some people can argue that it matters, and that's probably the biggest strike against Bitcoin. But outside of that, I think it really checks the boxes; we already talked about the hardness quality that it has, which for a currency is probably the most fundamental thing—or sorry, for a store of value—storage costs, transfer costs...I mean, compare that to gold.

41:36 I think that the right peer that people use for Bitcoin is gold. It's like digital gold. If you stack it up against gold, it really does look pretty good. It's like, "Okay, I can transfer it, way lower cost, I can store it for lower cost, it's more auditable, I can see the train all the way back to the first transaction." So, you can audit it completely. It doesn't degrade over time like other physical stores, it's permanent. It's got a lot of these really nice values that you say, "Look, if I'm doing the checkbox +/- equation," this really checks out as taking gold to the next level.

Rob Campbell: 42:07 The next question is related, though—if something is a reliable store of value, presumably I can have some sense of what it might be worth with some degree of reliability down the road. Just given the intense swings in price that Bitcoin has seen...I mean, yes, gold and precious metals do exhibit changes in price as well, but I got to ask you the “B” question. Can you give it a grade with respect to: are we in a bubble? With respect to Bitcoin and just the sheer incredible increases that we've seen in its prices—at least measured in U.S. dollars [laughs]?

Justin Anderson: 42:37 The “B” question [laughs], I like that. It's interesting. I was reading a tweet by Nassim Taleb, who I follow, and he was making essentially the same criticism about Bitcoin saying, "Hey, if it's this great store of value, how the heck do you explain this volatility? This is ridiculous. It's not a store of value, store of values can't be that volatile."

And I think the answer to that, and I would argue—I think everyone's going to have their own opinion, it's hard to argue with Nassim Taleb, he's pretty smart guy—but the story I would say is, there's a de-risking that's happening here. And there's a psychological effect that's happening here that, once you achieve universal agreement that this is a valuable thing, then I would expect the volatility would go down dramatically.

43:15 But I think until you reach that place where it's universally accepted as a store of value, it's going to be extremely volatile because it's battling between essentially, the "B" question—people who think of it as a bubble, versus people who think of it like, "No, no, this is a long term store of value." So, you're going to have that tension in the market, you're going to see that through lots of volatility. I would expect the volatility to continue as it battles for its place as a legitimate currency. It either will be a bubble or won't be [laughs]. If it falls to zero, it's a bubble, and if it becomes another mainstay currency, then it's not a bubble. So it's an impossible one to predict, because it could go both ways, and both ways are valid.

Rob Campbell: 43:54 Got it. My last one…and I don't even know we're grading anymore with this one, but just coming back to governments and centralized institutions—most of the notes that…I don't know if I have any in my wallet today, I don't carry around a lot of cash [laughs], but there's a legal tender associated with currency. Presumably these cryptocurrencies are a threat to governments, centralized institutions, who basically benefit from the system in its current state. What are your thoughts there in terms of how that might evolve?

Justin Anderson: 44:21 Well that's a fascinating question. A lot of the research into this, one of the first things I came across was, in 1914 when the government first came off of the gold standard, a big reason they did that was to be able to wage war. It was World War I at the time, and they were very limited because fiat currencies were tied to the gold standard and they couldn't, essentially, raise enough money in order to pay people to go fight in a four-year blood-fest in Europe. And some people make the case—and I think this is pretty persuasive—that if they had stayed on the gold standard, they would all [have run] out of money, and the war would have ended in a year [laughs]. That would have been a much better outcome for the world.

Justin Anderson: 44:58 So, the argument is that sort of used the manipulation of the monetary system in order to fight a war. That's an example of how a central authority, if it's done right, it can be great for society. But if it goes off the rails and doesn't have a goal that may be aligned with the greater good, it can do something that maybe is horrible. And it ties back to the vision behind this whole thing.

So, I absolutely agree that I think that governments will definitely see something like Bitcoin potentially as a threat, but the offset is, they may not be able to do too much about it; [it’s decentralized by its nature] it's quite secure, very difficult to tamper with.

45:35 But governments are also going to pursue...I think there's ways for them to leverage this technology. You hear about Stablecoin, and central banks are exploring ways that they can capture a lot of the transaction beauty that these blockchains are leveraging to be more efficient in how they manage the monetary system. So, there's definitely the possibility that they jump into that. But I think Bitcoin itself...I think overall, it probably is a threat. It's one of the...maybe the number one knocks against it; that it might be fighting an uphill battle if it gets too prominent, and government start to see it as a threat to its ability to mint money.

Rob Campbell: 46:09 Fascinating. Thinking back to the beginning, and just the reasons to look into Bitcoin and the technology itself; coming at this from situational awareness... In our existing portfolios, the way that we're investing, how has your work influenced the way you've looked at portfolio's or specific holdings? In other words, what has been the result of this analysis?

Justin Anderson: 46:31 We spend a lot of time in the payments world. So, we own Visa [and] MasterCard, we have a lot of other [payments companies], like Adyen is another portfolio holding. We really want to have our head around where payments is going and the different risks and opportunities that they face.

So, I think a big part of this was not just digging into Bitcoin, but just blockchain more generally, and understanding the risks and opportunities that these represent to these incumbent companies. I don't want to give too much away of our thoughts on those individual holdings [laugh], and what way we think that goes, but ultimately, that's the rationale why we went into it.

47:04 The other thing is, if you look at a company that we hold—Square, in our Global Equity Fund—that's one that's, I would say, is the most actively prosecuting the case for Bitcoin [laughs] in our holdings. Really, they're buying hundreds of millions worth of bitcoin, they're enabling transactions of bitcoin. So, part of this analysis was trying to get our heads around, "Hey, is this a good capital allocation decision? Does this make sense?" Because that's what we're doing; we're constantly trying to assess our managers’ capital allocation decisions. To do that, we need to dig into Bitcoin to understand what this is, to get our head around whether or not we think these guys are wasting shareholder money. So yeah, that would be a couple of the reasons, kind of the specific implications that this work has had for our portfolios.

Rob Campbell: 47:47 Great. Then, well, just recognizing that your last comments were very specific or bottom-up based, are there any more macro insights as you think about portfolios that this work has elicited for you?

Justin Anderson: 48:00 For a long time we've lived in a world where we believe gold has a significant store of value. It doesn't necessarily translate into us investing in gold companies or buying gold for our portfolios, because our strategy is to buy wealth-creating businesses, run by good managers, at reasonable valuations. Just because something checks the box as a store of value, doesn't necessarily mean, "Oh, hey, we're going to go buy those companies." If anything, I would say that we would start very neutrally on the subject of whether or not this is a valuable business. We'd want to look at each individual company bottom-up, assess—just like in the case of Square—what's their wealth creation? What's the return on capital? And so on.

48:40 I think what it does is it just gives us a little more confidence on the future role that Bitcoin may have, and also still understanding that, there's a lot of uncertainty as to how the story is going to play out.

Rob Campbell: 48:51 Well, Justin, this has been fascinating. I'll probably have to listen to this two or three times to begin to wrap my head around some of the details, but I agree—I think it's easy to draw conclusions from surface-level knowledge, and we certainly believe that context matters. So, thanks for coming on today and helping our listeners learn a little bit more about Bitcoin.

Justin Anderson: 49:09 Great being with you today, Rob.