TFTC 451

**Marty:** [00:00:00] All right. We're recording. Steve. Are you there? I'm

**Steve:** here. You're here.

**Marty:** Take two. All right. We just had some technical technical difficulties. Freaks. Steve's mic stopped working as soon as we went live for take one, but we're here. Take two to talk about UTX Oracle. Whenever I say UTXO, I want to say UTXO.

Whenever I say UTX, So getting

**Steve:** like you. It's kind of a hard word to say. Yeah. It's kind of a tricky word to say. Yeah. I mean,

**Marty:** it's a really cool project. Uh, it's got me pretty excited in terms of how we can, well, we'll get into like, is there an Oracle problem? What are like the correct trade offs? But before we dive into UTX Oracle, which is the project that you guys built and launched, uh, this month, I believe.

So [00:01:00] correct me if I'm wrong there. But, um, before we jump into that, we're sitting down with Steve Jeffress and, uh, Daniel Hinton. And, How did you guys meet and why'd you guys decide to tackle this particular program for the problem in the Bitcoin space?

**Steve:** Uh, you want me to do that, Daniel, or you want to, uh, well, we just met at the Raleigh Bitcoin meetup.

We, um, we know we're never going to be like the biggest meetup like Nashville or Austin. So we just try to be the most toxic meetup, try to, uh, name something for ourselves now. Not really. It's, um, kind of lighthearted, but yeah, we met, we have a great meetup scene here in Raleigh, North Carolina. It was started by Jamison Lopp and then, um, I took over organizing it around 2017.

Um, and yeah, me and Daniel met at one of those. Actually, we've met at one when Jameson was still running it, didn't we? Yep. Yep. Yeah. So, [00:02:00] uh, yeah, just became good friends. And, um, I don't know, do you want me to dive into UTX Oracle or

**Marty:** did you want to? Daniel, I think your experience at SFOX and what you're seeing on that side of the market is interesting because I'm sure you guys deal with this particular pricing problem day in and day out.

**Daniel:** Yeah, we definitely do. And that, you know, I started with SFOX back in 2018 when I was living up in Raleigh and, uh, it was, you know, back in the day it was a lot more common. Uh, so at SFOX, we, we aggregate liquidity from a lot of different venues on the exchange and the OTC and the market maker side. So from my perspective, looking at the, at the market, it's always been clear to me that there is no single, the price of Bitcoin, right?

So wherever you go and check the price, that's never going to be the price. And even if, even if, you know, as Fox and Coinbase and Kraken and a bunch of other places had the [00:03:00] same dollar price down to the penny. There's different depth and there's different, there, there's all kinds of things that factor into what a price is or what the price is.

Right. So, um, yeah, this has always been sort of, uh, obvious to me. And that's one reason why people come to S Fox is because we aggregate. Uh, but looking at things from this side of the, the veil from the UTX Oracle perspective, you know, we. We don't have an authoritative stance on what the price is, um, and nor does anybody else.

So from, from Steve and I's perspective, we were just talking about it and Steve can talk some, some about his visualizations and through the process of us over a number of years, just looking at these visualizations and understanding. Um, different pattern sets that appear in the UTXO set, it kind of became more obvious to us that there was a price signal and, uh, and it, it's led to [00:04:00] some pretty interesting findings and hopefully truly decentralized use cases for people to, to operate in the, in the market.

**Marty:** Yeah. And before we jump into UTXO Oracle and how you guys are. discerning these trends on the charts of the chain data. Let's just start with the basics. Pretend like anybody listening to this doesn't understand Bitcoin fully yet. So like, let's start with what is a UTXO and how can people track that throughout the blockchain and then visualize it on charts?

**Steve:** Uh, you want me to do it this time, Daniel? Yeah. Um, I like the analogy of bills in your wallet, like 100 bill, 50 bill. And every time you receive Bitcoin, you receive it in a bill and to spend it, you have to spend the whole bill and then you receive change and other bills. And, um, that's how the Bitcoin [00:05:00] blockchain works.

And another way to think about it is as a database that keeps adding rows. So, I mean, Bitcoin does use a database, um, and you can think of every new transaction as a new row in the database. And when you have Bitcoin, it means you kind of have ownership of one of those rows. And then when you spend Bitcoin, that row kind of like goes gray, uh, because it's spent and then you create.

New unspent transactions. Um, you can think of those as like new rows added to the, uh, uh, database, which are now unspent. So they're kind of like, you know, you can think about it kind of like a white and gray rows and an Excel spreadsheet with the like spent and unspent Bitcoin. And if you add up all the unspent Bitcoin, you'll get the total amount of Bitcoin in the system.

Uh, is that a good one? Is that good?

**Daniel:** Yeah. And just, this is one thing that really. Highlights it to me with why are UTXOs important. It's just like, you know, you take [00:06:00] however many UTXOs there are right now, 115, 120 million or so, um, you take all those UTXOs and just add them up one by one and you come up with the exact amount of Bitcoin that exists in the world at any particular point in time, right?

And this is something that anyone with a full node has full access to and full validation of, right? So you're not trusting anybody. Yeah. Yeah.

**Marty:** UTXO. I mean, yeah. It's a very important part of Bitcoin, particularly understanding that it's like a push system and not a pull system. You have to push. These UTX forward into the network when you're, when you're making economic transactions there, like Steve said, destroying UTXO that you're using to spend.

And then if you're not spending the whole amount within the UTXO, you get changed back, which is in the form of new UTXOs that you can then push back into the network in the future. Right?

**Steve:** Yeah. And it's all, you know, public data. It's all data that everybody [00:07:00] has on their node. Um, it's a lot of data. the full blockchain is what, like half a terabyte now.

Um, and so, you know, I, I part of my like PhD program and did a lot of data visualization. So when I first got into Bitcoin, I knew I was going to like do some cool data visualization stuff. And it's, it's hard to visualize 500 gigabytes of data. Um, But, um, through like a lot of kind of doing, um, histograms, bell curves, simplifying, um, I was able to create really cool ways to visualize both the UTXO set and all transactions.

And, um, so I've been playing around with that for quite a few years now. And the USD price was just kind of one of the things. That I saw that was clearly visible. Um, if you visualize the blockchain the way that I do, so that's kind of where it all came from. [00:08:00] Oh, I was thinking when Daniel was talking about, um, The price problem.

Uh, it might seem like we developed UTX oracle because we wanted to do that. Uh, it didn't really happen like that. It was just kind of like, well, what's that? Oh, that's the price. Oh, wow. That's cool. Like maybe we should just pull that out of there. And this happened like a number of years ago. And I kind of finally got around to writing a program to do it like you can very clearly see by I Um, if there's like something goes wrong, you know, there's a difference between like something going wrong in the program and like not actually being able to see with your eye what the price is, um, in the heat maps.

So, yeah, it's just a very strong signal

**Daniel:** and see that that concept of us just sitting around at the meet up and You know, looking at some of your visuals, visualizations and asking questions about them and zooming in on a particular area [00:09:00] and, you know, finding Satoshi's half pipe and all those kinds of crazy little things we've found over the years.

Uh, it just, it produces interesting conversations and, and findings that. Wouldn't be possible just looking at that database view of things like visualizations are so powerful for synthesizing this tremendous amount of data over this 15 year period and Yeah, it's very cool. Just at the start of the podcast here.

We should definitely recommend people go to utxo. live Um, to, to see, you know, a real visualization of this and a lot of the things we're talking about here. Um, that's great. And

**Steve:** don't everybody get to it at the same time? Cause I pay 40 a month on a digital ocean server. Uh, yeah. Like going to a 1990s style website takes a while to load.

**Daniel:** Well, don't worry. Bitcoin will not break if the, if this website goes down.

**Marty:** [00:10:00] Well, I agree. The visualization is very powerful. I think my first. Sort of run in to understanding the power of visualization, visualizing the blockchain particularly, was back in, I think it was 2017 or 2018. When Laurent, uh, from the OXT team, um, tried to hunt down, he had that, that research series that he called, uh, Bitcoin's Moby Dick, where he sort of identified that there was these spam transactions that were clogging the mem pool and driving transactions fees up.

And I think his thesis was that it was part of like the B cash. Sort of propaganda, uh, war to, to incite this problem of high fees when it really was the product of this, this fee spamming attack or whether or not you want to define it

**Steve:** as an attack. And he found that basically by doing the visualization and, and [00:11:00] wondering what was up with what he

**Marty:** saw.

Yeah, you could see all these like equal dust transaction UTXOs. I believe it was right at the dust limit of 564 or 546, whatever it is. I think the first,

**Steve:** I mean, there's so many things. Yeah.

**Daniel:** Good. I was going to say that I'm thinking back to my earlier Bitcoin days, there was a pretty early website that had, you know, the size of the transaction sort of denominated as a circle and it would fall and it would like hit the keyboard or something.

It would make a sound based on the size of the UTXO being spent and it would make funny little musical themes. And yeah, visualizations are very powerful for educational purposes.

**Marty:** Yeah. And I mean, I guess. Jumping into UTX Oracle, like how long did you guys have to stare at the visualizations that you created, Steve, before you're like, oh.

There's something here. We can, we can glean the price outta this.

**Steve:** I'm not, I mean, I stare at these things every [00:12:00] day. Like some people wake up and check the price. I just, I just wake up and like, I look at like the cool patterns and all the ut x's that were spent last night. Um, I've, I don't want to even, I you probably an hour a day for the past eight years, , however long that is.

Um, it's probably underestimated.

Yeah. Um, but I mean the, the price was in there, you know, I probably first saw it. And 2017, um, and I saw the price start to pop out of there around 2013. And, um, cause as you know, there wasn't really a price of Bitcoin before that. And then the, because people spend these round amounts of Bitcoin, um, they just got stronger and stronger.

Sorry, I meant round amounts of dollars. Really interesting that back in the day, it was [00:13:00] mostly round amounts of Bitcoin. Like if you look at what's spent on chain. You know, it's kind of like a normal distribution, like just kind of random, kind of small. And then there's these giant, massive transactions that are at rounds amounts of Bitcoin.

I mean, massive number of them. Um, it's like not even close. You know, it's not like there's a lot of transactions at random amounts. It's like, like yesterday, there was 4000 transactions right at 0. 01 Bitcoin. Um, which is usually the most common round amount of Bitcoin point zero one. And there was like 20, 000 transactions at exactly a hundred dollars.

Um, so this people spending round amounts of dollars is like massively overwhelmed the round amounts of Bitcoin. And that switched around 2019, 2020. Before that, everybody sent each other around amount of Bitcoin. [00:14:00] After about 2020, it around amounts of dollars kind of took over.

**Marty:** And, I mean, you guys mentioned it in the Bitcoin Magazine article that you guys co wrote.

But what is driving these round dollar amounts of people spending on Bitcoin? You mentioned ATMs, are services like BitRefill contributing to that as well?

**Daniel:** Yeah. Yeah, definitely on the upright. Yeah. Yeah, I mean on the utilization side, we just to talk about a few of those use cases. You know, Bitcoin ATMs are, are a big one.

Uh, but there are a lot of other types just to help people who've never used a bitcoin, a t m, you know, it's gonna work that it's almost always gonna be a buy, right? So you're almost always buying Bitcoin at an a t m like this. And you take your money, you put in your a hundred dollars or $500, you get quoted a price there on the spot.

And you show them your Bitcoin wallet and they immediately send you the Bitcoin. Right. So this is, this is one of the good [00:15:00] things that contributes to, um, These dollar denominated Bitcoin signals is that a lot of the dollar denominated activity is more real time, right? So it's you sending to a friend to get them set up on their first Bitcoin wallet and you send them 50 bucks or you're buying it an ATM or you're buying a t shirt or a gift card or something with refill or a bunch of other services or buying a gift card, right?

So these are, they're more real time. And that really helps us looking at the blockchain to know. That these groupings all relate to about the same timeframe, even if their mind is a slightly different block height, you know, so it's, it's all real time, mostly transaction related use. And, uh, and just peer to peer activity, right.

Paying for dinner for a friend or just getting someone onboarded onto Bitcoin. And, uh, you know, it's. It's cheaper to give somebody a hundred dollars than 0. 01 [00:16:00] Bitcoin today. So people might've just switched to dollars. Yeah. And

**Marty:** on the ATM example, particularly like, do you guys have to factor in? Like fees, whether it's network fees or the, the, the fee that the ATM provider is taking out of each transaction.

**Steve:** Yeah. You know, one thing that Daniel said to me, I think, and you might not even remember it a couple of years ago. Um, we were talking about how ATM fees are kind of ridiculous or whatever, like 10, 15%. And then I think Daniel, I think it was you, you said to me, yeah, but that's the price of getting Bitcoin now.

You know, it's not the price of buying something on Coinbase and withdrawing it in a week. And it's like, Oh, well then what's spot price. You know, it shouldn't be the price of Bitcoin now, so it's kind of, it kind of blurs, um, but, you know, I mean, one of the, that's one of the positive [00:17:00] aspects of using UTX Oracle is that like, these aren't people that bought Bitcoin and then withdrew their Bitcoin later.

These are all people that got their Bitcoin on that day. So it's, it's kind of a, I don't know. And

**Daniel:** it's just the scale of the, the dollar denominated sins makes it to where, um, like the average signal, you know, versus a centralized venue price. It does skew higher by like 50 to 60 basis points. So half a percent, you know, or a little bit more.

Um, and. That makes total sense because when you see the price on CoinMarketCap or Coinbase or wherever you look, you know, that price does not include exchange fees, right? That doesn't include the spread that or fees that you're gonna get. It also doesn't include the withdrawal fee if you get charged a withdrawal fee, right?

So the the quoted, you know, centralized spot price is always going to be [00:18:00] lower Then the on chain price, just because there are more things that go into getting those transactions finalized on chain and actually getting it in your possession. So it, we didn't really have to account for fees. They ended up not being very meaningful in the, in the analysis, but it does sort of intuitively make sense why.

The UTX oracle price would skew a little bit higher than the centralized price.

**Marty:** And

**Steve:** centralized price. We're just going to start calling them the centralized price now.

**Daniel:** Yeah, we got it. We got to, Bitcoiners love terminology, you know, you got to create a bunch of new confusing terms.

**Marty:** The cucked price.

**Steve:** Yeah.

**Marty:** Well, with all this in mind, like how. Like, obviously people are sending round dollar amounts of Bitcoin through the network, but how do you actually begin to tease out the price at any given [00:19:00] point in time using, uh, the inference of those dollar spends, dollar amount spends?

**Steve:** Yeah, this is something that's, um, it's very easy to explain if you're looking at one of the heat maps or do you want to pull it up again?

Can you like zoom in to the price level? Um, I don't know if you, if you can't, that's fine. But yeah, like I said, like, so yeah, that if you're looking this on video, that yellow area on the right, there's a little like wavy lines on the right, those, that's the us dollar price line right there. Those are people sending even amounts of bitcoin.

You can see that, like the bottom one is clearly visible back to when, like. 2012 or something like that. That's the 1 line. So people used to send each other 1 very commonly. Um, and but now the most common amount is [00:20:00] 100 and I expect that to just keep going up as Bitcoin. goes up in price. And all you have to do to just, you know, get, you know, a rough estimate of which is the 1 line.

You don't even have to be close to be like, just go one day where you knew Bitcoin was 10, 000. And this isn't how the algorithm works. But, you know, we know that Bitcoin was around 10, 000 on July 26, July 27. So, um, 0. 01 one. Bitcoin. If Bitcoin is 10, 000 is 100. Um, so you know that that's the 100 line. So then you just follow that line.

And the first version of the algorithm, this is what we did. We were like, okay, this is the line. This line crosses 0. 01 Bitcoin on July 26. So we know this is the 100 transaction line and we just followed that line and we're [00:21:00] like, okay, whatever, however this line goes up or down, you know, that's how we're going to calculate what the price is now because 100 is a different amount of Bitcoin every day.

And then, and then kind of version two or three, we're like, Oh, let's not just use the 100 line. Let's use the 10 and the, okay. 50 and you know, all of them. And then in the version we released, um, which is version six, it not, it uses 17 different round amounts of bitcoin and you actually don't have to start it from that peg day either because it, it pretty much just, it's kind of like You know, sliding one fingerprint over top of another fingerprint, we just made this thing called the stencil, which is kind of like a, um, a bell curve just with spikes, um, right at, um, all the round amounts of U.

S. Dollars. And we just see where that stencil fits over the day's worth of transactions the stencil kind of locks in. Um, [00:22:00] that's how we estimate the price. And, um, Yes, it was. I was very surprised. I mean, I knew the, uh, following, you know, from a peg today would work well because easy. It's just like, where did this line go tomorrow?

Um, but I was really surprised that stencil method without, um, Any peg day at all just seems to lock in it really. Yeah, it's fair to say that this was back tested. I heard you and marty talking on rabbit hole recap yesterday. By the way, huge fan of you guys. I've been listening to you since bar tools are still sportsman.

Um, huge fan of rabbit hole recap. Uh, but yeah, I heard marty, um, definitely a fair point. Like, or yeah, sorry, Matt, I heard Matt say definitely a fair point that, It was back tested and kind of fit to the data. Uh, that's for sure. But I was surprised, like, as soon as I created that stencil, there was only a couple of days, um, where it didn't [00:23:00] work immediately.

And those couple of days were days where. Bitcoin just jumps or crashes like a lot. And so I just, I just had to tweak the stencil a little bit. Um, just kind of handcrafted it a tiny bit, like made some bars a little higher and some bars a little wider. Um, and then it, then it worked. And, um, so, and yeah, and untested data since about June.

So that's why we decided, you know, we got to. We got to release this some point because, you know, people are going to say it's been back tested to fit the data, no matter when you release it. So you got to release it at some point so people can see that it works on untested data.

**Marty:** Yeah. And to better understand how, like how these lines extend, maybe like when you go back to like July, when the price was 10k and you sort of identified, all right, 0.

spends and then extending that into the future. Is that extension [00:24:00] essentially determined by like. amount of equal spend? Like do you just aggregate all the UTXOs and just do that bell curve distribution of like particular SATs spends, and then use that to extend the line. That makes sense.

**Steve:** Um, so I, I don't make sense until you said, extend the line.

Do you want to answer that?

**Daniel:** Well I, I think I understand where Marty's coming from. So yeah, just take, And this, this is another thing that people need to understand about it is this is not a single blocks worth of UTXOs, you know, 4, 000 transactions or so. This is a full day's worth of transactions, anywhere from, you know, 2 to 500, 000 transactions.

So it's, it's a full day's worth of data. So you, you cut out, you know, a lot of the, the, the minutia with, oh, it wasn't perfect in this one block. You need a, a, you need a decent size. Set of data for this to work because [00:25:00] not every single block has has a good signature, but over a day you essentially always do So Steve when you have that full day's worth of transaction data Talk about how you kind of remove some of the things from that to really highlight the USD amounts I think that that helps explain it a bit better.

**Steve:** Sure. Um, yeah. So if you just think of, uh, you know, like you said, you have thousands of transactions during the day. Um, and transactions have multiple outputs. So you have this collection of outputs. And so you, you just make a, or we just make a bell curve out of that. So we have these bins and you know, uh, you see a aran, uh, output that's between 0.01 and 0.015.

Then you just increment that bin and you just build this bell curve of transactions that happened that day and that bell curve, if. [00:26:00] If there weren't round amounts of Bitcoin and weren't round amounts of U. S. dollars and you did it over a long time, that bell curve would be like very smooth. It'd be like a very nice, smooth, even, you know, the peak would be at around 0.

01 Bitcoin and it would, you know, start going down on either side, looking nice. But because most people do round amounts of Bitcoin and U. S. dollars, there's these like giant whiskers sticking up. At just a few spots. Um, and so it's very obvious. It's like, okay, here's the round amount of Bitcoin I can remove the round amount of Bitcoin and then what's left is just the round amounts of dollars and it's very clear that the only spikes on this otherwise smooth bell curve are U.

S. dollars. So you just see like, where are those U. S. dollars like, and which one is the 100? Which one is the 50? The 100 line is just, um. It's always the most popular followed by [00:27:00] 50 and then like 10 and 25. And then on the other side, um, what, 1, 000, 5, 000. Those are all kind of like a quarter of what the hundred dollar and 50 is in terms of

**Daniel:** popularity.

Marty sends to his friends when he, he gets him a new wallet. Yeah. Right. Whatever. Yeah, on.

**Marty:** Stop gifting.

**Daniel:** No more friends and family gifts. I used to, I used to

**Marty:** do 20 bucks back in the day. I still have this one friend, Tim. Every Christmas when I'm home, he pulls up his Coinbase account. He's like, look how much it's worth now. Hold on to it.

**Steve:** Back in like 2013, when I was sending my friends like 10 for Christmas, Coinbase had a feature where it would return it to you if the person didn't log in and create an account.

I got so much Bitcoin returned [00:28:00] to me. Which is great in a way.

**Daniel:** You like intentionally put a typo in their email just so it comes back to you in six months.

**Marty:** I tried. I tried,

**Steve:** but yeah, but you know, like, yeah, all right, so I got, Hey, you got it. Oh, just say, you know how it is kind of a problem gifting people with Bitcoin.

Sometimes it's a good thing. Sometimes it's a bad thing. Sometimes you lose it. It is nice. You know, there's a system there that's like, okay, if this person gets interested in Bitcoin, they get it. If they are like, whatever, then that it comes back to me. It doesn't get lost.

**Daniel:** I think it's probably better to gift people the knowledge about Bitcoin rather than the Bitcoin because they're going to lose it if they don't know what's going on.

This is what I've

**Marty:** learned over the last decade. Like coming back to UTX oracle, like you've created the system where you can tease out the price data at any given point in time. Um, but now [00:29:00] using this, this oracle feature in actual applications, like how viable do you see this tool being, uh, as an actual oracle for business functions or smart contract functions?

**Daniel:** Yeah. Yeah. I'll talk, I'll talk a little bit about that. Um, I mean, with, with the code that, that Steve has produced already, it's just a very simple Python script. You can just download it at UTXO dot live slash Oracle and run it. You just need to have a full node running on your local computer and you can just, uh, query your node and it'll.

You'll put in a day's worth of, uh, you'll put in the particular day where you want the price and it'll go to your node, download the blocks for that day, and then verify it and you get the price for that day, according to this version of the model. And that's a, that's a very cool thing that I think everybody should do.

And we've already had a good number of people doing that and. Uh, some people have even spun up their first full node [00:30:00] in this process, which is very cool to see, um, because it's a lot of people really don't see the incentive of running a full node and, uh, it's, it's, it's a very important thing for the Bitcoin ecosystem to have.

People not only running nodes, but using them for various things. So yeah, we definitely want to encourage that. Um, but as far as, um, using it, uh, like we, you know, you've got your block clock back behind you there. And like, this could be a very easy thing where if, if, uh, you know, the block clock folks didn't want to subscribe to an exchange price feed, they could just.

Either embed that into the clock themselves or just run the script without having to reference any centralized venue. Right. And this would be, uh, a quite accurate price that they would end up with. Um, and this is another thing that Steve and I get a kick out of is who's to say which is right and which is wrong, you know, so it, it might be, it might be 75 basis [00:31:00] points different from fill in the blank central venue, but.

I mean, we're looking at the Bitcoin blockchain of settlement activity. This happened, so maybe this is right and they're wrong. So there's, this is one of those things with Bitcoin. There is no authoritative, um, you know, reference for the Bitcoin price. And I think this version. Within reason is, is just as, it's just as good as any other.

So as far as how you can use it in, uh, let's talk about, you know, kind of the DLC application, which is the one that I'm kind of most excited about. So in the, in this kind of project, there's phase one, which is just get a working prototype that people can run and verify independently to produce a price signal, which they can do today with the code that exists.

Um, you know, phase two is use that. In some way where you can actually settle [00:32:00] decentralized trading or, or other DLC type activities. Um, with the way that, uh, the way that most all DLCs work today is that you and your trade counterparty enter into an agreement. And then you agree to have either one or multiple oracles involved that will At the resolution of the contract, sign a statement as to either the price on that day or the outcome of the event that you're betting on or trading on, right?

So it could be Biden wins or Trump wins, or the price on this day was, was this value. So. Uh, the way that this could work with that type of setup is that instead of just flat out trusting this central oracle to quote you the price that's going to settle your contract, uh, you would just agree that the oracle uses this [00:33:00] version of the UTX oracle, um, price methodology.

And, uh, if for some reason the price that they produce on that day is different. Then the price that's produced from this V six version, then you could have some kind of punishment mechanism for that. Right. So you're not, you're not just blatantly trusting that your Oracle is going to, um, is going to do the right thing and not try to exit scam you or something.

Right. So this is, it just gives the individual more, more say so in, uh, yeah. And the ability to independently verify the outcome that the Oracle is attesting to. Which, you know, given the right, given the right setup, I think could be a really compelling use case. The, the example that I like the best is say you're, you're, you're a little, you're a little skittish and you don't trust centralized venues.

And you enter into a, a three of five Oracle setup to where five Oracles are gonna produce [00:34:00] the price on January 1st, 2024. And, um, and you're gonna use that to settle your contract. Right? The five oracles that you chose were. We're FTX and BlockFi and Celsius and Voyager and somebody else. Right. And, and now you thought you had five oracles and you thought, okay, I'm, I'm safe.

And it turns out you're not safe because there are no bailouts in Bitcoin and things happen, especially over long timeframes. So in this type of setup, even if you wanted to use that, that three of five oracle setup, you could maybe just have UTX oracle be a backup for that. Or if these five oracles don't produce a valid signature when they're supposed to, you just default back to this price.

That's going to get you close enough for, for government

**Marty:** work. Yeah, I've actually never thought about that particular aspect of the Oracle problem. What happens if the Oracles go bunk and they can't attest to [00:35:00] an event and then you don't have anything to sign the closing transaction signature with? And it

**Daniel:** doesn't even have to be a catastrophic blow up.

It could just be that they've changed their direction of the business and they don't want to do this anymore. And they're going to wind it down at some point and somehow you didn't get the memo and so you're relying on it. And, you know, the, the company's still there, but they're not, they don't have this division anymore.

**Marty:** Yeah, and you're sitting there with a transaction that can't be spent because you don't have the attestation. Yeah, right. Attestation.

**Daniel:** Um, so that's, that's like, that's a version that could work today. You know, given the right people participated, the, what I see as, as the, the true goal would be for Marty.

You and I, we want to, we want to do a trade about the price on January 1st, 2024, what would be fantastic. And what would be more of more of like a lightning style set up with sort of a punishment mechanism that's built [00:36:00] into the protocol would be if you and I could agree to use the V six price and you and I could just.

Run the V six code ourselves, and then somehow produce a valid signature at that time to settle. So it would still be a two of three, but I would produce my own signature. And then I would use the V six code to produce the second signature for the two of three. Um, and then you and I, you and I can just do it ourselves without having to rely on any external trusted third party.

So that in my mind, that would be like the gold standard. For, for usability here, but, uh, there's some technical challenges in that, that I have not worked out yet. And I would, I would really love it. If people could, uh, could opine, uh, to, to us in the telegram channel or on Twitter about ideas you have about that.

Cause. If that were possible in some way, that would be very, very cool and would, would really open up a lot of [00:37:00] avenues for expansion of this.

**Marty:** What are some of the hurdles that are in the way?

**Daniel:** Well, it just, there's, uh, there's no obvious way to prevent you Marty. So, so January 1st comes around and you think, well, this is, this is ridiculous.

Like I want the trade settled at the price I wanted, not the, not the true price within a Bitcoin transaction today. I don't know how to. Make it so that the, your signing software knows that that was a fake V6 price that you input. Right? So it's kind of like, there's not a good punishment mechanism in the game, the system.

**Steve:** You could maybe like do some kind of like hash of the code that you used hash of the Python script itself, maybe.

**Daniel:** And I think that something like that would be possible, but, um, yeah, I just haven't put the pieces together for how it could work in reality. But. That would be phenomenally cool if we can figure [00:38:00] that out.

**Marty:** Yeah, because you have to think, and coming back to the Oracle problem more broadly, like, you can't fake, I mean, the problem you just described would be me faking some data, but at the end of the day, really, like, if you're actually running the full node, and you're verifying against your counterparty, you really can't fake that data.

**Daniel:** Yeah, and you, in this, in this example, it's kind of more like a man in the middle attack, because... You who are signing up an inaccurate price, but you didn't change the blockchain, you just changed your wallet software to force it to sign something that's not true. So that's that that's the area where I would love some feedback from people.

Um, cause it, it really would be very cool if that were possible.

**Marty:** And going back to UTX Oracle right now, you're doing the price at the end of the day. Um, once a day, but could you have like a rolling per [00:39:00] block price? Just doing like a trailing 144 block look back, just have a price

**Steve:** per block. Yeah, that's definitely possible.

Um, I just decided to release the daily average just as kind of a simple thing. Uh, you definitely need a number of blocks, you know, cause you know, some of these blocks just have one. You know, wizard ordinal in them. You couldn't just look at one block and be very confident about finding the price, but yeah, trailing 144 blocks should work fine.

Um, you know, I, I have a little robot on my server that runs this thing every night and publishes it every night. I don't really want to use my servers just running that 24 seven. Um, but yeah, it's certainly possible.

**Daniel:** Come on, man. You got to do it, do it for the

**Steve:** digital ocean's going to go up to 40 bucks to 45 bucks a month, [00:40:00] man.

Need it. Yeah. Not stacking hard enough.

**Marty:** Well, that gets to an interesting, like, should there be dedicated services and companies built around providing this type of data? Or is that to feed the whole purpose? Is the whole purpose that individuals should be doing it themselves? Yeah,

**Steve:** I mean, yeah,

**Daniel:** this is something that Steve and I have joked about for years as far as, you know, it's very difficult to start a company in the Bitcoin space that doesn't artificially insert yourself as a trusted third party.

So, I mean, one of the nice things about UTX Oracle is that, you know, I have it on my computer, Steve has on his, and several other people have it on theirs already, and you really don't, it's not a very computationally intensive thing, like, on a, on a normal, you know, MacBook, you can run it in a minute or two.

And it, it'll give you the price for the day. Right. So it's not, not overly complicated. And Steve's made, he made the program very user friendly for non technical people as well. So [00:41:00] it's just follow a few instructions and you'll end up where you should be.

**Marty:** That seems like highly.

**Steve:** Yeah, it does seem like, I mean, me and Daniel have been talking about this forever, like there's gotta be some kind of business case, um, to be made from this, but just like everything else in Bitcoin is just so hard to, um. To make a, a, you know, ethical, virtuous business on Bitcoin. I mean, you got wallets, you got exchanges, you got mixers, maybe.

But, um, other than those, you know, I'm sure you know, Marty, it's hard to think of one. Yeah,

**Marty:** well, that's, I mean, but that's always been one of the business cases that makes sense to me. It's like an Oracle provider just getting paid for providing an attestation. But again, with what you guys are building, it's like

**Daniel:** the individual should be able to provide it themselves.

More of like a value add within a Fetiment setup, you know, to where that [00:42:00] Fetiment just has either a dedicated member or a dedicated server. And it's like, Hey, this is, this is the price according to the Raleigh Fetiment, you know, server or something like, um, yeah, yeah. But it, I agree with you. We, yeah, it, there's a lot of thought that's gone into that.

And, um, it's, it's kind of, you don't, you don't know what to hope for. Right. So it's, you, you want it to be available to the public and freely accessible and usable. Um, But yeah, I think that there could be, this could be a nice thing for existing businesses to layer into their offering. Yeah,

**Marty:** and it's something, I can't really grasp what I'm trying to articulate, but there's just something beautiful about being able to pull this data from the chain and using the chain to get this instead of depending on a centralized third party, like an exchange.

Yeah. Like it highlights that there's new ways to do things with Bitcoin, whether it's multi sig custody, it's like a new way to [00:43:00] secure an asset, and then using the chain data. To get Yeah. Information about It's very, the purchasing power at any given point in time. Yeah. We,

**Steve:** we, yeah. There's something, there's just something very cool about it and yeah, that's, that's essentially why I did it.

I was like, dude, this is awesome. We gotta, we gotta release this. We're not really sure we, it's so cool, but there's just something very cool about it.

**Daniel:** I think it's so cool because nobody forced this to happen, right? There wasn't some committee meeting then we said, okay, let's all send around. You know, around USD amounts and sizes that are big enough to where we can find it on chain and, and make a model around it.

This is just some weird emergent behavior that Bitcoin just happens to have. Right. It's like nobody, there's no committee meeting that said that, you know, miners have to go out and, uh, and create these phenomenally, you know, capable. New ASIC [00:44:00] chips either. It's like, it just happens. And it's, it's just bizarre.

All these incentives that align in Bitcoin to create these outcomes that, that seem to make Bitcoin stronger. Yeah.

**Steve:** Yeah. And because there wasn't some initiating thing, it was, it, that makes it a lot harder to game too. Um, Daniel can talk about that more than I can, but I was just talking to my mom on the phone earlier today, actually.

And I was like, yeah, mom. I mean. You can't stop everybody around the world from sending each other a hundred dollars. You can't just like make an announcement and just say, Hey, stop doing that. Like, that's just not going to happen. You know, it's like a rumor going around to high school. Like, you can't stop that.

I mean, you could pay to have all the block space. You know, you could just pay enormous transaction fees to crowd out everybody. Sure, that's very costly, but I don't think you can stop this signal in the chain. [00:45:00] I think it's kind of unstoppable.

**Marty:** Yeah. I mean, it's just, you know, action, you can't stop human action.

**Steve:** Yeah. Cause yeah, there's no, there was no central place that started it. So, and this is, and there's just something very cool. Or so I got,

**Daniel:** well, I was just gonna say about the, the sort of the attack factor is people, people are very quick to say, Oh, well at, you know, how many transactions would it cost to produce a, you know, a.

A derivative or a fake signal or a duplicate signal. And you can do some quick mental math on that. It's it's, you know, it, it essentially starts at costing you like seven Bitcoin a day, and then it would go up a lot from there. Once it, once it actually started happening, um, but it's like, what could you do with, with seven Bitcoin a day at a central venue, like if you needed the, if you needed the closing price on a particular day to show a value, like.

Maybe you, you could do that a lot cheaper than [00:46:00] manipulating the Bitcoin blockchain on some other venue. Yeah. Just use

**Marty:** like futures or something

**Daniel:** like that. Yeah. Or just get some, get a database guy to, to change a number on the screen. Yeah,

**Marty:** yeah. Uh, did, uh, um, Oh, go ahead,

**Steve:** Steve. I was just, I had never thought about it the way Daniel just said it right there.

Like instead of just, yeah, just compare it to someone manipulating the price on an exchange. Yeah. Like it's probably about the same. Yeah.

**Marty:** And the cost of that is zero. It's just convincing somebody to do it where seven Bitcoin a day right now is more than 150 grand. Yeah. Rather expensive.

**Daniel:** Quite quickly.

You can't, you can't blackmail the Bitcoin blockchain. Yeah,

**Marty:** something I'm curious about since you guys have been looking at this data in visualizations, obviously, ordinales and inscriptions have been a big thing. This year, did the emergence of [00:47:00] that phenomena, like, change the visualizations?

**Steve:** Well, those transactions are, uh, usually very low Satoshi amounts.

Um, they're kind of near the dust limit. Um, they're like less than a dollar, all those transactions. So those transactions didn't really affect, uh, the, or the Oracle that much. And, uh, the, uh, the Oracle is affected more by the, the price changing a huge amount on a day because in the morning, a hundred dollars is a lot different than it was at night.

So there's, there's no clear spike. Um, but now the, the one off transactions didn't really affect it too much.

**Daniel:** Yeah. And just for, for round numbers, for people listening, you know, at the beginning of the year, there were, it's not, it's not a. A requirement that the number of UTXOs go up over time, because it can go down when you consolidate UTXOs into larger amounts, but in general, it does go up over time and at the beginning of the year, it was [00:48:00] about 70 million UTXOs.

And now it's, you know, 120 million or so. So a lot of that. UTXO proliferation has been the inscription stuff. But, uh, yeah, Steve has a, has a nice chart showing, you know, the entire history of blockchain, uh, the entire history of the blockchain. And there's just one little tiny piece down at the bottom, right.

For this year's values. And it's very, very low on the, on the Y axis. It's like, those are the inscriptions, right? It's like pretty. It doesn't really matter much when you look at the entire Bitcoin blockchain. It's pretty inconsequential. Interesting.

**Steve:** Yeah. People have been doing very strange things on chain for a long time.

Um, and inscriptions is just one of them. She's like, Oh, what's that? And I'm just like, well, what's all those other like crazy things that people have done over the years? Like, yeah, Ren BTC was had a 10, 000 BTC [00:49:00] hot wallet that they would do 100 transactions a day out of. It's just like, what in the world?

I changed the wild place, man. Wild place. Well, on that

**Marty:** note, like what are some of the, I'm sure you guys have some insights. Into broad UTXO mismanagement, like, do you guys have ideas around, I mean, Daniel, you mentioned consolidation, I'm a big believer that people don't have proper UTXO management, even some of the most popular companies in the space, like, what lessons have you learned from looking at these visualizations day in and day out?

Is there anything that, like, sticks out to you? Like, what are these people doing? Like, there's a better way to do this. Yeah.

**Steve:** Um, well, you know, don't send yourself like a ton of really small ones, that's for sure. Uh, because you're gonna have a hard time getting those out. I, I think I, I was on spaces some [00:50:00] Twitter spaces where somebody disagreed with me on this, but I would recommend sending yourself not just one large one either.

Um, but something in the middle, you know, if you're kind of, if you're going out to the strip club at night, you know, you don't want all ones. You don't want all twenties either. You know, you kind of want something in the middle there. Uh, so I recommend a distribution and I also recommend labeling them especially, I mean, maybe not on your kind of phone wallet, not on your everyday wallet, but on like your cold stash, you know, use one of those good wallets like Sparrow or Specter and uh, cause they let you label.

You're gonna be like, Oh yeah, this is the one that I got from here. This is the one that I got from here. And then you can also see if you, if you're, if you keep up with labeling them, you can also see if somebody's trying to dust attack you, you know, you're like, Oh, where did that one come from? You know, if you get a UTXO, you don't know where it came from.

Don't spend it. Do not spend it. [00:51:00] Um, but that's mostly from personal experience. I would love to see

**Daniel:** you. I feel like you got, you have some wild labels in there, Steve. I I'm dying to see now. Um, no, I think the, just the, the things that you see people doing on chain is just really cool. The, the Ren BTC one was very interesting and it took.

It took you a while to figure that one out. Um, but it's just this, this massive single UTXO that just gets just, it just gets, it's like, it's a working Bitcoin stash, you know, it's like, there's some Bitcoin that are like lazy on the beach somewhere. And there's some that are like out in the field working all day long.

Like they get turned over dozens and dozens of times a day, just because it's a, it's a hot wallet and it's just, just churning through transactions constantly, those types of things are interesting to me. Like these are your. Your, your UTXOs of leisure and your hard work and UTXOs, you know, out in the mines.[00:52:00]

So

**Marty:** you're saying Ren BTC was churning over 10, 000 Bitcoin a hundred times a day. Is that what they

**Steve:** were doing? Yeah, they were destroying their 10, 000 BTC UTXO completely destroyed every day. Multiple times a day, like a hundred times a day. So, you know, it'd be like an exchange or something. If you pay, let's say you're withdrawing from Ren BTC, they would just send you, they would destroy their whole stash, send you one output and then send the change of their stash back to a new UTXO.

Every time somebody would draw. Yeah. Every time somebody would draw, they destroyed their stash and send themselves the change. That was amazing. Like one time I was very confident. Yeah, yeah, yeah.

**Marty:** Reckless.

**Steve:** It was crazy reckless. I can't believe, but they rent BTC made it for like three years. What was

**Marty:** written?

BTC better.

**Steve:** I don't even know some defy stuff. Yeah, I'm [00:53:00] not sure. Yeah,

**Marty:** that seems terribly risky. Like if your change address, you fuck that up.

**Steve:** Some of the other cool things that you can see are these kind of frequencies, these oscillations, so you can definitely see the weekly cycle. Um, Saturday and Sunday.

Very small, noticeable kind of, you know, sign wave kind of in the weekly cycle of outputs. Um, also back a while ago, it was pretty common for all the exchanges or sorry, all the mining pools to pay out on a certain day. Marty, you probably know more about that than we do, but like you could see that like, okay, this, this mining pool pays out on Sundays.

You know, this mining pool pays out on Tuesdays, Or once a month or something like that. So those things are pretty striking in the heat maps as well. Yeah, I imagine

**Marty:** BitMEX where they do every Monday morning. [00:54:00] Yeah, something like that, yeah. They would

**Steve:** do withdrawals. But I, yeah, I mean, I love what OXT. me has done and like, what was the other one?

KYCP. org, I think, the related one. I mean, I love that they're trying to give people some kind of open source way to do some kind of chain analysis. People have asked me to do that. I, I don't know. I can't make myself do that for some reason. People are like, who is that? And I'm just like, I cannot make myself try to dox this person.

Yeah. It just goes against my nature to do that.

**Daniel:** Aside from tc, no doxxing, Steve ,

**Marty:** tc. No, it is, but it really is a fascinating conundrum, if you will. 'cause the data's there, somebody's gonna look at it. And that's why I do really love what Lauren, um, samurai now are doing with O xt, me and Ergo um, yeah, sort of.

You need our chain analysis experts to be on the front [00:55:00] lines to sort of tell chain analysis and elliptic and Point out when they're egregiously wrong if somebody isn't watching the watchmen You get these weird situations with like the the bit fog Situation where this dude could go to jail on some bunk chain so

**Steve:** bad Yeah, man, I hope it turns out like the Ross Ulbrich thing and it ends up like chain analysis.

People go to jail because that, that Bitcoin fog story is so bad. Yeah. I mean, chain analysis, getting all that money funding and needing to like prove that they're great. So they go after somebody. I mean, I shouldn't talk about it because I just know what I heard, but it sounds terrible. It sounds a lot like the corrupt FBI agents going after Russell.

**Marty:** Yeah. And then they're trying to claim that Brian Bishop isn't an expert on this stuff. And,

**Daniel:** Oh yeah. Okay. Anybody can have anything knows that's not true. Yeah. Um, [00:56:00] Hey Steve, just, uh, talking about kind of the, the routine of what the, what the daily Bitcoin utilization looks like. Um, just talk about how Like what a normal day's use looks like when you look at the, you know, that, that one visualization, it looks like the rocket, you know, shooting out stuff.

And then like how frequently seemingly rare UTXOs show up being spent. Cause this is, I think, a source of kind of confusion and angst for some people. If they see like, Oh, wow, there was a big, a big spin from 2010 or something. It's like. How often does that happen?

**Steve:** Oh yeah. Yeah. So when like you hear a news story, that's like, Oh my God, someone just sent a coin from 10 years ago.

The news story kind of makes it sound like this never happened. And some old guys sold something and this is going to be a big deal. Every day people [00:57:00] send spend Bitcoin from like 2011, 2012, 2013. I mean, it's, that happens every day. You know, someone will send one from, you know, a little bit earlier in 2010 or something, and it'll make the news and be a big headline.

But this is just it's a very consistent distribution. If you look at the age of coins that are spent, you'll see it's very consistent. It's just this bell curve. Um, it's actually like a bell curve and log space. So I don't know, log normal distribution or whatever. But, you know, it starts at the dust limit.

And then at about 0. 01 Bitcoin, you'll see the top of that curve. And when you look at the age of that, that 0. 01 Bitcoin will go back to roughly like 2017 or something. Because there's a lot of people still holding on from spikes. So whenever the all time highs were, you'll see [00:58:00] people spending from those a lot.

Um, but then after 0. 01 Bitcoin, you know, it just goes. Back down normally on the other side of the bell curve. And it's very, um, it's very satisfying just looking at that every day and just seeing how, how consistent it is. Um, I guess, you know, people like Glassnode are more interested in the changes in those things.

Like, do we have a lot of OGs, um, selling right now? A lot of OGs buying. Um, I, I think the opposite's cooler. Just how, how stable that distribution is.

**Marty:** Yeah, are you like tank in the matrix? You're like, I see a woman in a red dress. I see

**Steve:** Can't help it man did his world's most beautiful data. This is so interesting.

Somebody just uh reproduced My stuff on ethereum just yesterday started making the heat maps in ethereum And you know do that even a few people [00:59:00] that run a full node

**Marty:** is what's that? You can do that with, since they don't use UTXO, they use, they use state, um, Account. Account. Yeah. Account based system. So you can do that with account based systems.

**Steve:** Well, it's been a long time since I've run an Ethereum node. Um, apparently the geth node, if you run the full, which they call archive in Ethereum language, full node means archive node. Um, full node in Ethereum means pruned node, just to mess with us, I think. Uh, but that geth node is now 12 terabytes.

Apparently there's this node called Aragon, which does the archive node. A little bit more efficiently, and it's like two or three terabytes. So this person was using that node and, um Yeah, I mean, even though it's a state based or whatever, you can still look back in history and see what transactions took place and it's kind of eerie how similar [01:00:00] the Ethereum blockchain looked to the Bitcoin blockchain.

Um, did not think I was going to be talking about Ethereum on this podcast.

**Daniel:** You got baited into it, man.

**Marty:** Well, another thing I'm curious about too is the updating of the address structure. Like so from like legacy to wrap segwit to segwit to pin to tap root. Does that introduce any changes to the visualizations?

**Steve:** Um, not really. Yeah, we talked about that before.

**Daniel:** I had, I had not seen the data on that and I don't know if you've looked at it on that axis, Steve, but that I would, it'd be interesting to see.

**Steve:** Yeah. Um, I mean, but I just look at amounts, so doesn't really matter what type of transaction it was. Yeah, it doesn't really matter that I just, I mean, if somebody was doing some, you know, one of those fancy tap script things where people [01:01:00] own little pieces of the tap, you know, and one of those multi sig thing that might mess it up.

Uh, yeah. If it is in there, it's not significant.

**Marty:** Yeah. Well, that gets to like an interesting point to just something that many Bitcoiners don't like to talk about, but it's like, Hey, we got to talk about it. Like not everybody's going to be able to own a UTXO. In the future we may need these tap script like solutions that allow multiple people to own partial parts of individual UTXOs and that gets into like the broader question is like adoption picks up like how How consistent do you expect these trends to continue into the future, like 10 years from now, Bitcoin is multi deca trillion dollars worth of the economic value of the world.

Like, do you see this sort of evolving?

**Daniel:** I mean, my, my [01:02:00] thesis has been that The signal's going away at some point, you know, for better or worse, but it, I don't think that this will be something that's around, you know, 20 years from now, 10 years, whatever, but, but yeah, it's just, it's very difficult to estimate timescales in Bitcoin because you just, it's, it's also hard to imagine beyond, you know, our line of sight, like what's going to happen because these, these are truly like.

Global geopolitical things. If these types of things happen, like a lot is going to change. So if, if, if we're talking in, uh, you know, in 30 years and the, the USD price is still visible in the same way it is today, I would be very surprised. Disappointed, probably

**Steve:** disappointed. Yeah. I've, I've called it a, a dating app, you know, it's designed to be [01:03:00] deleted.

You know, it's designed just to work until. Bitcoin totally takes over USD price isn't there anymore. Um, but in terms of other things, like you're talking about the UTXO growth and stuff like that, I think it's I think it's funny how people will, um, worry about a problem that's like so long away, like so far away, but they won't worry about a problem like the 2106 bug, which is much more clearly a problem and much more like, well, I want to talk about that.

I mean, I'm not on this podcast, but I'm, I've kind of been working on that a little bit quietly. I love Adam. Um,

**Marty:** But Baltic honey badger, I believe it was 2018. Like I asked about the 2106 bug. He's like, yeah, we'll worry about an 80 year. So I was like, I don't know if that's like the best way to attack this problem.

**Steve:** Right. It's like, yeah, freak out about too many UTXOs [01:04:00] 500 years from now, but don't worry about 2106 bug.

It's like, I mean, like Andres love Andres Antonopoulos. I know, you know, some people don't really follow him very much anymore, but he was very wise about scaling. Like there is not just one way to scale. You know, if you look at the history of technology and UTXO management, I think, is in this world of like, how are we going to scale?

And there are so many creative ways to scale that we haven't discovered yet. Um, 2106 bug where it. It's very clear what the problem is and it's not very clear what to do. Um, well, I have idea of what to do, but the, the, in terms of the scaling problem, it's just like, no, there's going to be thousands of creative scaling solutions in the next hundred years.

Like I'm not worried about somebody coming up with a clever way to deal with UTXO growth. I'm not worried about that at all.

**Marty:** I completely agree with you [01:05:00] there. And for those of you who are listening, you're like, what the hell is this 2106 bug? Uh, when Satoshi launched Bitcoin, he used Unix timestamping and that has a sort of end date.

It's called the 2106 bug, or is it the 2064 bug, but it won't affect Bitcoin until 2106,

**Steve:** correct? Yeah, 2106, yeah. Um,

**Marty:** if blocks are produced as they have been historically and particular increment, which the difficulty adjustment

**Steve:** modulates, it's kind of just take like two minutes and talk about that, Daniel.

**Daniel:** Yeah. I would love for, I think you have a really good point and it's

**Marty:** so it's, it's the reason why we definitely need a hard fork in Bitcoin soft fork. But you don't understand. We Bitcoin at some point.

**Steve:** Right. But I, I. I worry about that language a little bit because it makes it seem in [01:06:00] somebody's mind that like everybody has to change their node version at the same time, like in between the same two blocks.

Like when you it it unnecessary because I think I know a way to make a two versions of Bitcoin run together in sync with one another, like one version that's protected from 2106 and one version that's not. And if you can get Transcribed These two versions running together with each other for several decades.

Then when somebody gets a new computer, they have to, they have to install a version of Bitcoin. And then they, once it gets widely known that you can either install the version that forks off. Or not install the version that forks off, then, in my view, it will become a, well, you kind of chose to fork off.

Um, but that's all dependent upon getting a version of Bitcoin core that [01:07:00] can run with, you know, the patched and the unpatched version running together and sync, um, for several decades. And I, I think that's possible. I mean, Greg Maxwell and like a couple other people have been like, well, we could just keep 32 bits in the block header.

And then in the node software, we just kind of do something to detect the overflow. And then when you go back to publish the new block header, like a minor or whatever, just publish the 32 bits with the overflow. Because the patched versions of the node can detect the overflow. And um, I think that version can run together, just keep 32 bits in the block header.

Like, then we never have to do that crazy hard fork that people have in their mind when you say, we have to hard fork eventually.

**Marty:** You know, yeah, no, no, I completely agree. And, um, I will admit, like, I'm not technically competent enough to understand, like, the interaction between the block header and the overflow, but [01:08:00] it always has intuitively made sense to me.

Stop and decrypt. And I used to talk about this a lot and a few years ago, and he's been making the point, like, yeah, like you just said, like, get, get the software that will protect you from 2106 in the future. Uh, introduced as early as possible. So you have like the snake shedding skin thing where it's just like, yeah, like you just mentioned over time, people are going to need new computers are gonna have to pick, um,

**Steve:** when you get a new computer, you don't install 20 year old software on it.

I mean, if you got a new computer and installed the first version of Bitcoin today, you'd fork off, but nobody would care because that's not what we mean by hard fork. What we mean by hard fork is like somebody has a modern, you know, last few years version of Bitcoin and they got kicked off the network against their will, not like somebody chose to install software that they knew was going to hard fork.

Um, so yeah,

**Daniel:** just [01:09:00] people have a lot of just because of how previous soft forks have been activated, we think, okay, that's how we do it now. And I just think that this is a type of thing where there the rules are, there are no rules and that each time we need a soft fork, it's going to be some different mechanism.

And, you know, the participants in the Bitcoin system change a lot over time and the incentives somewhat change and. The thing that worked last time is not going to be the thing that works this time. And we just have to keep an open mind and, you know, not push things like this off, but also not feel like it's an excuse to get a bunch of other goodie bag things that might give us things that would be nice to have, but there, those are not the point of the 2106 issue.

So it's not like we have, we have to do this hard for it. So let's just do what Congress does and cram a bunch of other stuff in there just to get what you want.

**Marty:** Yeah, that's bad politics for this distributed network. [01:10:00] Yeah, like 21, I completely agree with you, Steve, like, I'm completely of the purview that we are going to find creative ways to scale Bitcoin, whether it's on chain, UTXO consolidation, um, multiple individuals owning a piece of an individual UTXO.

Second layer solutions. Like, and that's what a lot of the focus is right now. But 2106 is somewhat existential. Like if something doesn't happen between now and then like Bitcoin will just stop working.

**Steve:** Yeah. It feels like just the right thing to work on, you know. So I've been working on it a little bit.

We're

**Marty:** gonna get some headlines out there in New York Times Discuss how bitcoins gonna fail in 2106. Yeah,

**Steve:** exactly

**Marty:** That's the other reason like you need to front run those narratives Which will definitely pick up once people realize the energy stuff is all bullshit Once they realize the transaction per second is all bullshit.

[01:11:00] Like they'll go for the next thing. It's like, oh, it's got this critical issue Yeah.

**Steve:** Yeah. Yeah. Can't stop the fudsters

**Daniel:** I've had to think about this proposed solution for a bit and it, it, it sort of does make sense to me that for a, for a real world example that just happened today, you know, we all had it on our calendars to do this, uh, next week and then it hadn't happened yet, so it's okay that we changed it to not be the original time, you know?

And this

**Marty:** was the original time and then I messed up on the counter. That was my fault.

**Daniel:** And then nobody's, nobody's the wiser that there was this alternative plan. It's like, no, this is what happened. Then this is the plan.

**Marty:** Fascinating stuff. What other, what other things within Bitcoin are you guys interested in right now?

**Daniel:** Um, I would, I would love to just bring up another concept that, uh, is near and dear to my heart of smelting, [01:12:00] which was another kind of Raleigh Bitcoin meetup, uh, concept. And it's just a concept that you could coordinate with a miner to pay a very high transaction fee with the, with the UTXO that has any type of history, good or bad, and then have that minor, you know, essentially do a coin join swap with you for their newly minted coinbase transaction.

So you end up burning a historied UTXO. And get issued a new Coinbase transaction or a near Coinbase transaction without any history in the, and essentially the same size. And this was something that was possible with, uh, some more complex ECDSA work back before Schnorr, but it's, it's, it's much more possible today.

And this is just one of those things where I feel that there is a lot that can be done with Bitcoin today. That we [01:13:00] just have scratched the surface on that really changes the dynamic of blockchain surveillance and chain analysis and other things. And this, this is more of a, a privacy minded topic, but there are scalability things and other things that I just think we need to have more conversation about these possibly interesting new ways of, Bitcoin that, that really changed the narrative around like, Oh, Bitcoin doesn't have privacy.

It's like, okay, well, if you could have a UTXO. With, you know, whatever history you can imagine that would be unsavory. And if you can just enter into a trustless coin swap with someone and end up with a fresh near coin base output, that seems pretty private to me. So that's a pretty, yeah,

**Steve:** mixing, mixing has always been kind of a problem.

Mixing through coinbase [01:14:00] outputs is like the holy grail of mixing and me and Daniel and a few others have been like trying to figure out how this would work. Actually, I saw that super test net was starting to do stuff on this too recently, so I'm super interested what he ends up doing. Um, but yeah. If you could swap a very history UTXO for a clean UTXO for a small fee, um, that would be end the privacy conversation.

**Marty:** Well, that's very interesting too. Once you consider the economic incentives of these pools, mining pools are notoriously cutthroat. I think they're not very profitable businesses at the end of the day. So you have them forced to create value added services when there's firmware futures markets, which is trying to develop basic brokerage, whatever it may be.

Farm management. Um, yeah, this seems like a way that they could get quote unquote yield on their inventory. [01:15:00] Um,

**Daniel:** revenue stream. Just, just, uh, to steel man a bit here, the, this idea in particular has one major downside in that Um, if there's a block reorg where one of these super high fee transactions happens, um, it ends up the minor who loses their, their coin, not the participant in this melt.

So, you know, reorgs do happen occasionally and who knows how, if they'll happen more frequently in the future. Um, but that's the main, the main downside of this, that the minor does take actual risk in a reorg that they would lose their, you know, lose their coin, so. What if you just

**Marty:** sort of tied it to the actual UTXO of the block, the transaction gets mined in, but you'd have to make sure that the pool mines the block and then you really get a piece of the Coinbase transaction that's released a hundred blocks later.

**Daniel:** Yeah. And there's, there's some implications [01:16:00] with Stratum V2 on this about, you know, how do you actually make a system like this? And I think that that could be a more. Yeah, a more workable approach to having something like this work, but it's a, it's a pretty complicated idea, but it is pretty fun to think about though.

Yeah,

**Marty:** yeah. Because if you make a deal with a particular pool and another pool minds your transaction. Or maybe something like mempools transaction accelerator can help this and you just pull the mining pool Inventory via market like that. I don't know. I'm getting a little heady here. Just thinking about this idea.

I haven't done. Yeah. No,

**Steve:** I mean welcome Welcome to the conversation. We've been having for years now It's like how do we get around that Daniel was even thinking about an insurance company? Like you just have like a you know, a company that just provides insurance against orphan blocks. Maybe [01:17:00] it's like a third layer Solution though.

**Daniel:** Just, just more complex. I don't know.

**Marty:** These are fun ideas to think about though. It

**Daniel:** is. And just getting together with the pointers to talk about this stuff is awesome. And if you don't have a group to meet up with and talk about these things, you should, you should start one or get one or join one. Cause it's, it really makes it so much more fun.

Yeah.

**Marty:** God, now you got my mind running. I do feel like this is, I think maybe the accelerator model. I haven't thought about that like the accelerator aggregated, accelerate the men pools trying to launch or has launched. Oh, okay. Yeah. But like applying that model to this

**Daniel:** thing. And so what did they do? They just, they just have a separate transaction.

That's like a higher fee just to, to, to drag yours along with it.

**Marty:** They, well, they don't do it. So like if you want to get your transaction accelerated, you'd [01:18:00] pay men. Pool has deals with all the mining pools. Um, and then they create the market book for transactions that need to be accelerated. The person that needs their transaction accelerated pays men pool, and then men pool pays the pool that actually mines the transaction.

Um, so you have this sort of gotcha aggregate men pool's like this aggregate market, um, so's instead, depending on one pool to mine your transaction men pool, uh, aggregates all the transactions that need to be accelerated. And then the pool that actually mines it. It's paid for doing that by mempool. So like, similarly, could you apply that to like mining pool, UTXO inventory with the smelting idea, just to have like a market aggregator of that inventory.

And then the pool that actually mines the transaction. With the higher fee that you're paying, it gets the Bitcoin, but I don't know

**Daniel:** if that's true. know that in employees? [01:19:00] They're like 98 percent perfect and then there's some critical shift.

**Steve:** That accelerator, do you know if they're also including, um, transactions that aren't broadcasted?

What are we calling them these days? Non standard transactions or non, uh. Um, out of band or whatever, uh, because I mean, I

**Marty:** mean, these are out of band payments cause you could have a transaction men pull, then you pay out of band to get a pool to include it in the block and then they get paid for that service.

That's cool. But the nonstandard, I think that's different. Um, where you're going behind, behind the men pool to pull the company.

**Daniel:** This is also one of those ideas where like you, you kind of hope that it's not necessary because if it, If there really is a big market for this, it means that the chain analysis is having an impact on the fungibility of Bitcoin.

And, you know, you kind of don't know [01:20:00] what to hope for if this is necessary. It's maybe not the best, the best for Bitcoin that it is necessary.

**Marty:** Now that's hard. I know Lisa, Lisa Nugget, um, hits the comments when mempool announced that accelerator people are for that particular reason, the nonstandard transactions where you're not actually introducing a transaction to a mempool, um, but you're sending it straight to an accelerator or an individual pool.

Mining pool. How does that perturb the incentives? Is it introduce something like MEV? Yeah, but again all this stuff is possible You have to assume that people are gonna do it and how do you just work around that framework like? Transaction accelerators have been around for almost 10 years now or[01:21:00]

We that. Uh, and we raise 50k a month, uh, pocket withdrawal,

**Steve:** a couple of hundred grand

**Marty:** a month.

**Daniel:** We expect tomorrow,

**Marty:** two hundred grand. That's pretty cheap. But we do it. We, we have hiring this, this year.

**Steve:** Yeah, I'm going to have to go in here in a little bit. Um, but, uh, I, I do want people to, uh, if you're one of those people that has a node and you're just bored, you're like, oh, I thought I was going to have something to do with my node.

Uh, give my program a shot, like go to utxolive. oracle and just like, look at the Python script, you don't have to go to GitHub, uh, you know, GitHub can be a terrifying place for non technical people. You can look at the Python code on the website. And, um, I think you'll understand it more than you think you will.

It's [01:22:00] very well documented. Like, here's how you connect to your node. Here's how Python asks for the blocks that it needs. Here's how, once you have a block, You go through all the transactions. You can see all the outputs in the transactions. It's kind of cool. Like you can see the package structure that Bitcoin core puts the blocks in.

I mean, it's a great way to learn. I mean, some people can read Mastering Bitcoin by Andreas and and figure it out. Um, but you know, the real way to learn like exactly how does Bitcoin worse is just do something cool technically with it. And so I think somebody that doesn't consider themselves very technical could actually like run this python script pretty easily and understand.

More about how their node works. And, you know, so, yeah, I want to encourage everybody to and give me feedback, too. I mean, part part of you takes Oracle is like, [01:23:00] you know, I didn't want to write in a I black box where you didn't know how the Oracle is getting this price. I think. Part of if it's successful, U T X, Oracle will be because a lot of people understand how it worked because that's where you can kind of like get that trustless element.

It's not just the decentralized, it's not just the decentralization of the code itself, it's the decentralization of the understanding of the code. Um, I'm probably be too hopeful here. So the three people out there that might do this , let me know.

**Marty:** Well, I have to imagine like the umbrellas and start nines of the world would make this available pretty easily on there.

Yeah.

**Daniel:** Yeah. We actually already had some, yeah, they, they already put it into their umbrel. So, um, with the right app setup, it's, yeah, it's possible today. Yeah. Like if

**Marty:** they just add it to their app store, I could see this getting [01:24:00] downloaded pretty quickly because who wouldn't, if you're running this anyway, like, Oh, I want my own sovereign price Oracle as well.

**Daniel:** Yeah. It's very fun. There, there are several things that happen when you run a Bitcoin node that are just, Mind blowing and taking your latest block hash and then comparing it with a friend's latest block hash and you, you see that they're the exact same or you count up, you know, all the, all the coins that are out there down to eight decimal points and you ask your friend and it's like, Oh, that's the exact same number that I have too.

This is one of those really fun, uh, educational moments that you can have with somebody to say like, the price that you come up with will be the exact same price at block 809, 000. And that's crazy that you don't have to trust anybody to do that. It seems like it could be really powerful. Yeah.

**Marty:** People don't understand the gravity of that reality yet.

We're

**Steve:** still learning. [01:25:00] It's so crazy. Yeah. Just that we all have these identical databases in our house and there's no central authority given us the identical database. We just all have identical databases on our computer that are updating with each other. And.

Sometimes I think there's something so much more powerful, I mean, not like there is anything more powerful than money, but I think, yeah, there could be something else just with that fact that we all have identical databases, like some other kind of communication could happen

**Marty:** with that. Yeah, I completely agree.

I don't think we've even scratched the surface of understanding what this, how this is going to affect humanity in the long run, obviously money. It's very most important aspect of it, but I do agree, Steve, that there's like just again, like I said, I can't really grasp what I'm trying to articulate, but you can just feel that there's something there.

**Steve:** So fortunate to [01:26:00] be born into this era. Yeah, it

**Marty:** really is. It's crazy. And we get to hop on podcasts and talk about all these crazy ideas. Just wish everybody

**Steve:** could see it.

**Marty:** Yeah, they will. They will. They will at the price they deserve.

Uh, gentlemen, this has been fascinating. Thank you for, uh, for coming on and walking through UTX Oracle with me and thank you for building it and getting it out there in more people's hands. I think it's a really cool project and like we've been alluding to at the end of this conversation, throughout the conversation, there's, uh, unknown unknowns that could come from this that could, that could be massively beneficial moving forward.

Yeah, for sure.

**Daniel:** Thanks for having us on. Yeah, man. Appreciate all you do. And, uh, it's great to be here.

**Marty:** Well, it's great to be on the front lines with you gentlemen. Keep crushing it. Thanks, man. Thanks, buddy. Peace and love.[01:27:00]