Vitalik Buterin - What Excites Me About the Next Decade - TOKEN2049 Singapore 2024

(0:07 - 0:50)

A lot of the time when people talk about some of the challenges with crypto, one of the answers that people tend to give is people tend to say, you know, this is still early days, right? We're still building, we're still building out the basic infrastructure, you know, look how long something like the internet took to come into fruition, right? And this is something that I think people have been saying since, like, basically almost since Bitcoin itself launched. And one of the challenges with saying this, of course, is that today, you know, we are not in early days anymore, right? Bitcoin has existed for 15 years. Ethereum as a project has existed for more than 10 years.

(0:51 - 1:25)

And, you know, we see things like chat GPT rising up from not even existing as companies to suddenly completely changing everyone's understanding of what intelligence even is. And so you have to ask the question of, like, well, how do we actually even think about this, right? Are we actually early? And the way that I answer this question is I think we are not early to crypto, but we are early to crypto actually being usable. So let me explain what I mean by going a little bit into history.

(1:26 - 2:02)

So who here remembers back in 2013 when we were all excited about Bitcoin and Bitcoin was the next big thing, Bitcoin was the next big revolution for payments, and people were making these really amazing and really earnest efforts to try to just get regular merchants all around the world to start accepting Bitcoin? Who here remembers Room 77 in Berlin? Anyone here ate there? Yeah, so the one on the right, this is Boston. It's a restaurant called Thelonious Monkfish. That's actually the first Bitcoin restaurant that I went to.

(2:02 - 2:21)

So back in 2013, you could be a proud Bitcoin-accepted-here restaurant and also be a proud LGBT-friendly restaurant at the same time. And, you know, crypto Twitter would not think that there is any contradiction. So back at the time, there was, like, real genuine excitement about this.

(2:21 - 2:54)

So what happened? Well, one way to answer this is we can look a little bit further, and the memory that comes to me is this visit to Argentina that I made in 2021. So this was my first time in Argentina, and the first thing that I noticed was that there was this population countrywide that was not just incredibly excited about crypto, but that was actively using it on a massive scale. Like, literally, I was walking around on Christmas Day, and the first coffee shop that I noticed was open.

(2:54 - 3:17)

I walked in, the owner knew who I was, and the owner let me pay in ETH for the coffee and some dessert that I had with my friends. Now, they were using crypto, but they were not using decentralized technology. What were they using? It turns out the Argentinian locals were all using Binance-to-Binance transfers.

(3:18 - 3:35)

Why? Binance-to-Binance transfers are instant, and Binance-to-Binance transfers are free. And this is ultimately the same problem that I think ended up killing at least the original wave of exploration into getting everyone to adopt Bitcoin as a currency. It was the fees.

(3:36 - 3:52)

If you remember the marketing at the very beginning, why Bitcoin is great, it talks a lot about how Western Union, PayPal, credit card companies, they all just horribly gouge you on fees. They charge, like, incredibly high fees. Like, they're awful, right? But then, Bitcoin itself, the fees went up to $50.

(3:53 - 4:14)

Ethereum, the fees went up, too. The highest-ever fee that I paid on Ethereum was actually for a privacy-preserving transaction, so admittedly, the gas went up. And, you know, like, basically, like, big parts of Twitter comment every time I do things, so privacy protocols have a really good product-to-market fit.

(4:15 - 4:28)

And so the transaction fee was about $800. So basically, the reason why a lot of this stuff failed is fees. What's new in 2024? Well, this is a chart of fees on Ethereum Layer 2s.

(4:29 - 4:58)

They have gone down from being somewhere between $0.10 and $0.50 to being under $0.01, basically zero. At the same time, Optimism and Arbitrum, two major Ethereum Layer 1s, have hit this important security milestone that's called Stage 1, and multiple ZK EVM rollups have also told me that they plan to hit Stage 1 very soon. So rollups are rapidly becoming safer, and rollups actually are finally affordable.

(4:58 - 5:27)

But this is not the only thing that's improved. One of the other annoyances that I distinctly remember suffering on my trip to Argentina was I tried paying one of these people in ETH on Layer 1. The transaction fee was about $4, and the transaction took about five minutes to confirm. Now, this was after EIP-1559 had come on-chain, but this particular wallet, it had not actually upgraded to EIP-1559 yet.

(5:27 - 5:48)

So on Bitcoin, blocks come every 10 minutes, and so you have to wait 10 minutes, potentially an hour, for transactions to confirm. Ethereum, theoretically, the block time is 13 seconds, but because of the way that the gas market used to be really inefficient, sometimes you'd have to wait a totally random amount. If you get unlucky, five minutes, maybe even longer for a transaction to get included.

(5:49 - 6:12)

EIP-1559 actually basically fixed this, and if you add on the merge, one of the things that the merge did is it also cut in half the average waiting time until the next block. And so with both of those things, actually, these days, I reliably have my own transactions confirmed in 5 to 15 seconds. Then, if you use Layer 2s that have fast pre-confirmations, often this gets down to one second.

(6:12 - 6:39)

And so basically, the two big problems that are the biggest things that made centralized UX much better than decentralized UX in 2021, today, decentralized UX has them too. But also, we can look at the general user experience quality of applications. So on the left here, you have EtherTweet from 2015, and it clearly looks like a hackathon demo.

(6:39 - 7:00)

Now, on the right here, you can look at Firefly, which is a client for Forecaster and Twitter and Lens. And if you look at the quality of the UI, this looks like a Web 2.0 level of quality, but it's a decentralized application under the hood. But also, this year, we saw progress in account abstraction.

(7:00 - 7:11)

We saw more and more people using Safe. We saw ZK email, EIP-7702. We're starting to see mainstreaming in ZK-SNARKs, all kinds of different applications.

(7:11 - 7:33)

So we have new and better privacy protocols, Railway, Oxbow, ZooPass, which we'll talk about a bit later, Raremo, which can prove in zero knowledge that you have a passport, and then you can do voting on top of that. Also, even existing ease-of-use improvements between Layer 2s. Two years ago, everyone was complaining about having to manually switch networks.

(7:33 - 8:00)

Today, I think for at least the last year, I actually haven't yet manually had to switch networks. So before, the limitations of the technology were a stopping factor. I even remember that moment where CryptoKitties looked like it might become this really big breakout app, but then what happened? CryptoKitties' own success pushed the Ethereum gas price all the way up to 50 guay, Ethereum became basically unusable, and that by itself put a ceiling on the growth.

(8:00 - 8:17)

This is no longer true. But this basically means that the reasons not to use crypto are no longer here. What about the reasons to come in the first place? One of the mistakes that I think people sometimes make is talking about crypto as being an efficiency technology.

(8:18 - 8:53)

This is something that a lot of people talked about even back in 10 years ago. So this is a random page from 2013 that was just listing the benefits of accepting Bitcoin, right? So payments made easy, security and control over your money, zero or low fees, protect your identity, right? So two of the four are, I think, things that are features that are very unique to crypto. The other two, well, they were unique to crypto then, but are they now, right? Today, we have Venmo, we have much better SIPA payments, there's WeChat Pay, the centralized systems keep getting better and better.

(8:54 - 9:09)

But yet, in some places, payments and access to finance remain durably difficult. Why do they remain difficult? It's not because of access to technology. It's basically because of limitations in global politics.

(9:09 - 9:36)

So I think it's important to remember, right, that the kinds of benefits that crypto brings to the world, they don't have to do with technological improvements of the same type as switching from a regular jet to a supersonic jet is a technological improvement. It's a different type of technology. What kind of type? So one way to look at this is this blog post that Josh Stark from the Ethereum Foundation wrote about two years ago.

(9:36 - 10:27)

And the title here is Atoms, Institutions, and Blockchains. And the thesis is that blockchains allow us to create a kind of digital hardness and a kind of social hardness, basically that lets us create persistent digital structures that are hard and that can resist being broken in the same way that you can make hard physical structures out of something like concrete. And if you think about how blockchains differ from some of the previous cypherpunk technologies that they came from, things like Mixnet, things like Tor, things like BitTorrent, the thing that you realize is that blockchains are all about creating persistent structures that are extremely robust, right? So a file-sharing network, well, if your file-sharing network blows up, that's fine.

(10:27 - 10:40)

You just switch to a different one, and after a week, everyone forgets. If a blockchain blows up and you switch to a different one, everyone loses all of their money. This is a fundamental difference between what technologies before blockchains did and what blockchains do.

(10:41 - 11:16)

And so blockchains, because of this, enable the internet to not just route around weaknesses in old-world structures, but also do an actually better job of building better alternatives that can solve similar kinds of problems. So blockchains are digital concrete, and what is digital concrete for? Digital concrete is for building digital castles in the sky. So who here has seen this movie, Laputa Castle in the Sky? Come on, raise your hand if you've seen it.

(11:17 - 12:09)

Raise your hand if you know the opening theme song. Okay, let's do a sing-along. あの地平線　輝くのは　どこかに君を隠しているから　たくさんの日が懐かしいのは　あのどれかひとつに君がいるから So this is one of the... Actually, so the reason why this movie is fun is, I mean, first of all, I actually think it's great, and I think Studio Ghibli is absolutely top-tier, and you can probably tell I've seen this five times at least.

(12:09 - 12:49)

But it turns out that it was also somehow accidentally the inspiration for Ethereum without me even realizing it. Basically what happened was, in 2013, I was browsing a Wikipedia list of fictional elements, and I came upon Ethereum in that list, and in that list I saw, okay, this looks like a really nice name, and it reminds me of this 19th century scientific theory, this idea that there's this medium that permeates everything, and so, okay, fine, I picked the name. Then two months later, one of the Ethereum Foundation designers, back before it was even called the Ethereum Foundation, decided to use this diamond as the Ethereum logo.

(12:50 - 13:02)

I thought, okay, this is a really cool diamond. I like the logo, it's beautiful. Seven years later, I watched this movie for the first time, and then I saw, wait, they have Ethereum crystals, and Ethereum crystals actually look like diamonds.

(13:02 - 13:21)

And so it turns out that actually, basically, a whole bunch of Ethereum art was inspired by this without even realizing it. So, the other thing about that song is that the song, it actually sounds nice. I think in crypto, we actually need better songs.

(13:22 - 13:49)

It's like, a lot of the time, if you ask someone to come up with an anthem for a project, they come up with something that's totally cringe. It's like, decentralized, we stand united, a hash confirmed, a new block invited. And like, okay, if you like rap, then that's good, but do you really want that to be your anthem forever? Okay, so, back in 2013, there was this other song that I remember.

(13:50 - 14:14)

There was this artist named Kryptina. It's, QE said and done, all your fiat inflate to be on the sun, but no more because now there's a better one, and its properties perform better than all the rest of them, it's mathematical. No more double spend, it's encryptable.

(14:15 - 14:26)

Put your cash in your brain or it's wearable. A new form of wealth begins. Who here actually remembers that one? Okay, I do.

(14:27 - 14:45)

So, see, like, digital castles in the sky, I think, are the unifying theme that combines the serious and the fun aspects of crypto together. This is what I want people to remember. A castle is something that can protect you and keep your family and keep your tribe safe.

(14:46 - 15:01)

A castle can also be a castle in Disneyland that lets your community have fun. A castle can also be a museum that preserves all of the entire thousand year history of your culture. And a digital castle, similarly, can be all of these things.

(15:01 - 15:25)

And digital castles of all types are something that we can build on top of Ethereum. So, done with digital castles. What should our key goal be? So, this is my view that I've said the whole time, right? We need to satisfy the needs of mainstream adoption and we need to hold on to open source and decentralization values at the same time.

(15:25 - 15:41)

What does this mean? So, example one, wallet security. Historically, there's basically two ways to hold your money. One of those ways is you basically, you do the crazy self-sovereignty maximalist thing.

(15:42 - 16:03)

You write down a seed phrase, you do everything offline, you take your seed phrase, you engrave it on a piece of titanium, you put your titanium inside of a lockbox that's made out of even more titanium, and then you put that lockbox 10 meters underground and then your coins are safe, right? So, that's one approach. The other approach is to say, bro, I'm like a normie. I'm not going to do all that.

(16:03 - 16:12)

And so, instead, you basically go and you take your coins and you go off to give them to some trustworthy guy. You know, there's this nice guy. His name is Sam.

(16:12 - 16:23)

He goes on panels with Bill Clinton. He's got to be trustworthy. And, you know, two years later, it turns out that your assessment of who's trustworthy and who's not was a little bit wrong.

(16:24 - 16:42)

So, I think these are not the only two alternatives, right? So, basically, if you want to be protected against centralized bad actors, then you do the traditional self-custody thing. And if you really want, you can put it in titanium and put it 10 meters underground. If you want to be protected from your own mistakes, you do a centralized exchange.

(16:43 - 16:57)

What if you want both? This is what smart wallets with multisig let you do. Multisig means you have multiple keys, so you might have, for example, six keys, out of which you need four to send a transaction. And you could even have a rule that for small transactions, you only need one.

(16:57 - 17:28)

And those keys can be any combination of keys that you control, friends and family, ZK wrappers of existing services. So, you could even make a ZK wrapper of an email. You can literally today make an Ethereum account, which is a smart contract wallet, from which you can only send transactions if you generate a proof that you control a particular email address, right? So, you could basically take Web2 trust anchors and you can pull them into the Web3 world.

(17:29 - 17:51)

And in the Web3 world, you could even diversify your trust, right? So, you can ZK wrap a Gmail account, which is a U.S. company. Then you could combine that to make another one of your guardians be a ZK wrapper of an Indian government ID. And then you make a third key be a hardware wallet that was made by a company in China, right? You can maximally diversify everything.

(17:52 - 18:08)

And so, you could actually get the benefits of institutional trust without a lot of the weaknesses. So, example 1.5, decentralized social media UX. Farcaster, it's user experience-wise, Warpcast is a Web2 quality app.

(18:08 - 18:20)

But you could set your recovery address, the thing that has ultimate control over your account, to be your multisig. And I personally trust my multisig way more than any one of my centralized accounts. Example 2, payments.

(18:20 - 18:30)

So, this is Daimo. It's a wallet that is meant to be entirely Ethereum-based, but it has the same UX quality as Venmo. Example 3, privacy pools.

(18:30 - 18:56)

Privacy pools uses a mechanism where users can prove that their withdrawal came from some deposit without revealing which one, but revealing that their deposit did not come from one of the bad guys. And so, this is a way that allows you to have a very high degree of privacy for regular users and meet a lot of important compliance needs, but without actually having backdoors. Example 4, ZK social media.

(18:56 - 19:19)

This is a Zoom poll which uses ZooPaths, and so we can prove that you're a human, prove that you're a member of a community, solve the proof-of-personhood problems, solve reputation problems, while still preserving your privacy. It's not about either you're a non and nobody trusts you, or your KYC verified and you have no privacy. It's like, no, you can have privacy and you can have trust at the same time.

(19:19 - 19:48)

Example 5, Ethereum layer 1. A lot of technological improvements that are happening that make the layer 1 both more performant in terms of reducing finality time, increasing capacity, and at the same time, more decentralized and easy to verify. And a lot of these things are already happening. These are all directions that the Ethereum ecosystem, and I think crypto in general, are going to be going over the next 10 years.

(19:51 - 20:21)

Basically, the two wrong paths are, one is to sacrifice practicality for decentralization and forever be an ecosystem that's just appealing to itself and only has 691 users. The other bad path is to sacrifice decentralization for practicality and to say, okay, well, we're trying to get mass adoption, and so guess what? The next great crypto application, you have to log into it with a frigging Gmail account, right? What do we do best? Well, no. We do not have to take either of these dark choices.

(20:22 - 20:29)

We have decentralization and we have practicality at the same time. Eat both pills, be purple, take both. Thank you.