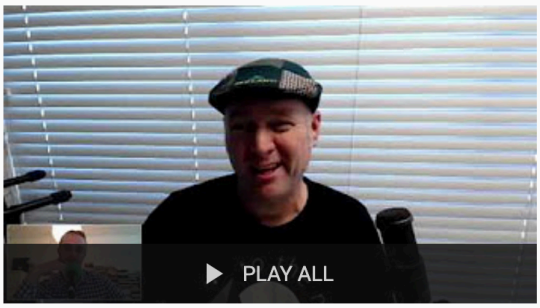
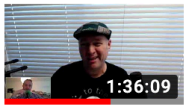
Vitalik Buterin answers r/EthTrader's questions

Wednesday, March 27th 2019

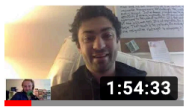


EthTrader's Community Member Spotlight

1 

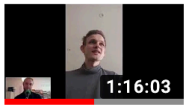
Jeremiah Nichol (/u/jtnichol) @ EthTrader's Community Member Spotlight

Kobe van Reppelen

2 

A talk with Ameen on Spankchain, governance, r/Ethereum discussions, the MolochDAO, and

Kobe van Reppelen

3 

Vitalik Buterin (/u/vbuterin) @ EthTrader's Community Member Spotlight

Kobe van Reppelen

Transcript generously provided by u/NeedzRehab.

Edited for readability by u/krokodilmannchen.

Introduction

K: So we are recording right now. First and foremost Vitalik thank you for coming on. For people that are new to this format, it's a community series. People have posted and voted on questions on Reddit and I have grouped them together and we will go over them today. Thank you to everybody who has submitted the questions. I will say that I couldn't include all questions from everybody, but I tried my best to group them together and have as many questions answered as possible. I will also recommend listeners and viewers to check Vitalik's latest and recent talks with Laura Shin and with Eric from into the Ether and then I particularly liked his talk with Dimitri from Hidden Forces and Tyler from Conversations with Tyler, and I will link to all of that. I'm mentioning this because many questions that were asked were actually answered in one of those conversations, especially the two more recent ones. So, let's just dive in and get started.

V: Sure.

K: So, Vitalik can you, as an introduction, can you share a little about the place where you are sitting right now. And the reason I'm asking this is that we are in this distributed world and it's nice to get a feeling of where you are, right now.

V: Sure, I'm just with my family in Toronto right now.

K: For people who have never heard about you, who are you and what are your interests or what is your background?

V: I'm the founder of the Ethereum project. Before that I was in what was then just the Bitcoin space for a few years. I co-founded Bitcoin Magazine and just generally interested in all of the related things and I get into a lot of software and program related stuff and a lot of math and economics and philosophy and just those kinds of things in general.

K: What did you study and how is that relevant to what you do today?

V: In university I studied Computer Science for one year but then I dropped out. I guess most of my learning has like especially recently has just been on my own from talking to people and reading things on the internet.

K: And if there is somebody, who do you go to for advice or is there somebody you look up to if it's nobody in particular?

V: I don't know. It depends.

K: All right. If, this is the last introductory question, but if people want to learn more about you, where should they go and find out more about you?

V: It depends what you want to know about me I guess. A lot of the things I've written aside from the Reddit and Twitter, I have a blog at (www.vitalik.ca) and wrote a bunch of other things on Medium. Otherwise it depends on what you want to know. The internet is a big place and the internet has a lot of things.

General questions

K: Let's start with the first question from Reddit. Talking about Twitter. You're incredibly gracious on Twitter. How do you manage to stay calm in the face of trolling, ignorance, and tribalism?

V: Hmm. I don't know how to answer that well. I mean I guess you just learn to get used to it after a few years of just dealing with it head on all the time.

K: Alright. Just by the way, I will start with some general questions, then there are some questions on Ethereum in general, and then some technical questions on Ethereum and that's how I group these questions.

V: Okay.

K: Just so you know. Another question: what do you think about the crypto space as a whole? Do you share the opinion that one day there will be a superior coin or blockchain or is there enough space for different blockchains and technologies?

V: I definitely think there is enough space for different kinds of projects. I mean definitely not the all 15000 or whatever crypto coins we have right now are going to succeed. Like I think almost all are going to be completely forgotten over the next few years. But there is definitely room for more than one protocol and I mean even within one blockchain ecosystem there is room for many more protocols.

I think one of the interesting things about having multiple crypto currencies and multiple blockchains is just the ability to explore and have different trade-off's inside of them. So, like for example, like in the case of Ethereum if you look at the approach we are taking for Proof of Stake it tends to be, like, emphasizing things like decentralization heavily. It emphasizes the ability to run a node very cheaply. It emphasizes things like security deposits and penalties if you break rules. Whereas a lot of other proof of stake systems tend to be more explicitly organized around the idea that there should only be a couple dozen or a couple hundred nodes.

Those kinds of systems could be faster and have faster block times, but on the other hand they can fall into centralization

concerns much more easily. So there's a lot of like interesting trade-offs like that so between centralization, efficiency is a big one, also just functionality, performance, and simplicity is probably another one. I mean obviously there is different kinds of Consensus algorithms.

So just as like technical experiments, and also as social experiments, if you start thinking about on chain governance versus immutabilist governance versus Vlad (somethings) governance. You know what other ones you have. I think those things are interesting and it's a good thing that we can have those different communities try out different models. And I obviously have my own opinions about which of those experiments are likely to succeed and I am obviously use those opinions in at least the part of designing the Ethereum protocol that I do myself. But there's room for options.

K: I wanted to, the next questions is about the relation between the Blockchain space and the Real space. This is the question that was asked. You and Glen (something) I don't know how to pronounce his last name correctly, but you and Glen say that the crypto community is a great testing ground for Radical Market ideas such as quadratic voting and Harberger taxes. Blockchain projects are in need of better rules, and the communities are generally more receptive to trying out radical changes and games. If these ideas are successful, how do you see them being transitioned from the blockchain space into the "real world?" Do you foresee incumbents of the current systems rejecting these ideas out of fear of losing their own power and property?

V: So I guess like first of all there is, you don't need to exit the blockchain world to enter the real world. Like I personally hope that some of these fancy Glen Weylian mechanisms design ideas end up not only succeeding but I also hope that Ethereum and blockchains really end up succeeding and if both end up succeeding then why not continue working with and building on top of each other?

In terms of things that I see as being interesting experiments and the Gitcoin CLR is one of those that I really continue to be interested in. So there is this round of CLR matching that they did last month where you basically had a list of projects and anyone could donate to those projects and then they used Glen's formulas to basically take the amount, the square roots of the amount that every donated, add up those square roots, take the square of the results, that number is always going to be bigger than the total amount that people originally donated and then so use this kind of central point of funding to make up the difference. And that, I was actually really impressed by the results of the first one. It created an outcome that was, just worked really well in general. And now there is round 2 that is happening.

As these experiments get bigger, the one thing that will have to start fighting against or dealing with is that these experiments are going to start getting attacked. One of the things that I've been starting to call attention to is especially the mechanisms

that don't naturally have collusion resistance. Mechanisms where if someone can easily create 10,000 accounts or if someone can easily bribe other people then that ends up breaking the mechanisms. In those kinds of cases, if collusion is extremely easy, then a lot of these mechanisms stop working well. So someone needs to start coming up with ways to make either creating fake accounts or collusion not so easy. This seems like something that a lot of people aren't really appreciating, but it is something that our space will have to deal with.

One of the kind of dark sides of the crypto space is that there is all of these just totally anonymous often smart and well-resourced attackers floating all over the place. So like the one that besieged our blockchain with a denial of service attack for about a month two years ago or whoever hacks the DOW or whatever and these wonderful characters. And I'm sure they will try exploiting the CLR's as well. So if these, if we can come up with ways to make sure these mechanisms survive in that environment, and if the kind of broader society ends up wanting to use them in larger scale context, they could just end up using the same solutions that we will have evolved from directly and why not?

K: How long do you believe it'll be before we have a unique human identity protocol with strong anonymity guarantees and what do you think is the most promising approach to this problem?

V: That's a difficult one. I think creating a unique human identity problem with like an infinite level of security, I'm not even sure if it's possible. Basically because even with government based Human Identity programs, like if we create an international standard for say like giving everyone electronic passports that have digital signing capabilities well what's going to happen? Well North Korea is going to print 30 million of them and they are all going to be sitting in Kim Jung Un's drawer and he's just going to use all 30 million of those passports and collude and grab all of the CLR money and North Korea becomes a world superpower.

So that's like, it's quite difficult to like actually really robustly make these systems in a way that just can't be exploited in some way. Potentially as counterintuitive as it might seem to someone from more traditional backgrounds, decentralized approaches, if they work might work better than centralized ones, because centralized approaches to identity, they do kind of seem to work but you know really they can break. They can be hacked. There was some recent news from a couple of countries where tens of millions of some kind of national ID credentials, I forget the details, like just got hacked. If hostile governments realize they can use these as a way of getting more money for themselves, then they'll definitely end up having secret ORG's that end up doing that.

Making a really really super robust identity thing, I'm not sure if it can ever happen but creating systems that have kind of higher and higher levels of security, and try to work in

situation-specific contexts, that try to instead of making it impossible to fake identities will try to put a lower balance on the cost that it takes to do that. Will try to make it easier for people to kind of work toward having an identity that passes through a filter like a through natural activities that happen every day but make it hard for people to do that artificially. And just have many types of research towards doing that and we might have something that reasonably works in some cases, like in a few years. I don't know.

K: Is there a specific approach or team that is trying to solve this that you look at with special interest?

V: I haven't seen anything... so if we are talking specifically about the kind of unique human identity use case then I haven't seen anything that I'm super impressed with yet. That said, Glen sent me a paper literally two days ago and I haven't read the paper yet but knowing it's from Glen and having seen one of the slides from the presentation, I have a higher probability estimate that it's more legitimate than other stuff. We'll see.

K: All right. How is your relationship with Vlad changing and do you see him continuing to contribute to Ethereum long-term or moving in a different direction?

V: Vlad has always been this wonderful fun character. Like he's... on the one hand he's always just kind of off by himself and like you can't give him orders and like if you try to give him orders he's just not going to listen to you. And we never really did.

On the other hand, he's just going to go off and do random things, and sometimes those are random things I agree with and sometimes those are random things that I don't agree with. On the other hand he has made really significant contributions to Ethereum research. So like for example Casper CBC. So the vision Casper CBC that Vlad has is you have like his own thing Casper and then you have like CBC flavor of sharding and then his own CBC flavor of load balancing and then all those other things. There is a lot of that vision that I don't really find super practical. Like I personally don't believe in sharded systems without a logically centralized beacon chain. I don't believe in in-protocol load balancing because I think that's just too much complexity for layer one. And I don't believe in highly activist governance where the chain ends up like having IETF committee's weekly deciding which smart contracts to burn.

But at the same time, Casper CBC for example, is just brilliant, and it's brilliant on a scale where it's a multi-decade level improvement over the traditional academic VFT space in many ways. I can't find any other algorithm that allows you to avoid having in-protocol enshrined finality thresholds, that allows you to just kind of layer Consensus on top of a majority driven forktuous rule so you can have the same mechanism that

would decide block by block and the same mechanism finalize. So between all of those things, like, no just Casper CBC is amazing and useful and it's something that we hope to switch over to over time. I hope Vlad comes up with more ideas and we end up continuing to help out with each others research.

K: I think /u/carlslarson, who is a moderator on the Ethtrader subreddit asked this. Vitalik, are you aware that you have 82,300 donuts!? And that Reddit recently announced they are supporting a community initiative, r/daonuts, to decentralize the donuts system. Do you think there is value in bringing Ethereum/web3 technologies back into web2 entities like Reddit? What would you like to see change with how Reddit communities operate?

V: Huh. So the interesting thing with donuts is that they kind of showed one of the limitations of blockchains by themselves and designing many incentive systems. So basically you can have donuts, and you can earn donuts, and you can use donuts to vote in these community polls. And then they made donuts tradeable by basically having this bridge where you could go onto and move them into Ethereum tokens and then trade them on Uniswap and then move them back. And then a lot of people started complaining and it's like "Hey, now you can buy votes!" and then you have people with Eth just coming in and deciding what happens in our community and then going out without having any skin in the game. And I saw that there were a lot of people just very unhappy about this and correct me if I'm wrong but they ended up suspending the convertibility to ERC-20 tokens?

K: Yeah, exactly, exactly.

V: I thought that was kind of very interesting and instructive experiment in many ways. Like first of all, the donuts being connected to the blockchain just sort of enabled them to be used in so many different ways. On the other hand, like this just goes back to some of those collusion resistant issues.

I'm actually in the middle of writing a big blog post about this. Basically if it becomes too easy to kind of prove to the outside world how you kind of behaved in a system, then you can do things like bribing with smart contracts, you can do things like individuals just buying a whole bunch of coins and using them to make votes. You can just do a whole bunch of behaviors that are just much harder to guard against. And there is a result in Game Theory.

You know how like when some people talk about how politics is fundamentally broken and they mention Aro's Theorem? That's the theorem that says if there is a voting system with more than two voters and more than two outcomes or something like that then there is no way to make one that's kind of fair in every way. It's a pretty common thing in sort of rationalist pop culture but I actually think that Aro's Theorem is overrated and the theorem that's underrated is that there is this result from Cooperative Game Theory which is just this branch of game theory that introduces the possibility that if

multiple subsets of agents can sort of collude with each other and act as one sub coalition. And the results basically said that the core, well the formal statement is that the core of the majority game is empty, and what that means is that if you have a game that corresponds to some kind of majority rule system, then there is no stable outcome because whatever the outcome is you can prove that there is always some group of 51%, possible some including existing privileged users, some including those outside of the ruling coalition that can just come together where that 51% gains an advantage over the status quo from kind of overturning the system to a new status quo where they're at the top. That just shows if collusion becomes this trivial then your ability to make a lot of mechanisms for a lot of cool things just end up breaking down.

I know there is just so much enthusiasm in trying to make these mechanisms for like just some sort of point system on top of social media. The Ethtrader experiment is one. There is also this Chinese media thing called Behoo(?) that's recently launched a similar thing and then there is just a bunch of others. I do worry that if they design them in the wrong way, then these problems will just kind of end up eating them and they'll just have to repeatedly solve them with kind of groups of centralized moderation and that would be very sad. But if we can come up with a solution that works, that would just be really great.

K: From my perspective, it was quite interesting to see how quickly the tokenization of the karma or the donuts, how quickly that led to discussions about buying the banner and then about advertising and you just know that implementing one thing technologically or technical solution just introduces a whole bunch of other questions to which there were no answers and it was just quite interesting to follow that from a reader perspective and to see the opinions and the motivations behind that.

V: By the way, I think the Harberger taxing might be broken to. So like if...

K: Can you just explain to people quickly what it means in this context for people who don't know what the Harberger tax is?

V: I'm sorry. So Ethtrader has this mechanism called, well they call it the Hamburger tax, but it's an implementation of the Harberger tax which is basically, you have this billboard at the top of Ethtrader, and there is always a price that you can buy the billboard for. If you buy the billboard at that price, then that amount of money goes to the original owner, but then you have to set the price at what you're selling it, but whatever price you set it to, you have to pay 1% of that amount every day. So that kind of stops you from putting the price up close to infinity and causes the billboard to have to just keep being on the market.

The way that I would attack this if I were more evil is that I would gather up 150,000 donuts. I would buy the billboard. And then I would replace the contents of the billboard with

Bitcoin Maximalist propaganda. Then I would set the price up to 250,000. And then people in the community would basically have no choice but to buy it back to set the content to something more Ethereum friendly and I would walk away with a profit. Then I would just keep on doing this.

K: But you would run out of donuts, right? To pay the tax?

V: No because if they buy it within 40 days then the amount I sell it for minus the amount I buy it minus the taxes I would still profit.

K: I think you just gave some people some ideas.

V: Well good it will be a playground on which the wolves should play and we should like put these things to the test and that way it's both financially and socially beneficial. Yay!

K: How do you manage being productive while having to attend talks and meetings all around the globe. as a person who trots the globe for work, I find it takes a lot of energy beyond the work to do, to be effective. curious on how your routine is.

V: It's definitely a challenge and it also depends a lot on which area I'm trying to be productive in. So for example, if I'm in kind of like research mode and I'm just trying to come up with and develop new ideas, then I find just going around different places and talking about ideas can be a huge and important source of information.

Now if it's something like coding or writing articles then I definitely want to be in one place. Coding is different. With coding, if I'm in the middle of something then I can definitely easily just take out my laptop, sit down on like an Uber or bus or whatever for 19 minutes, code for 19 minutes, and then close it and get 19 minutes of productivity out of it.

For writing, it's definitely not that easy. Writing is challenging. Sometimes you're in the flow, sometimes you're not in the flow, sometimes it's more complicated. It depends. The other thing is that I find my productivity, and by productivity, I don't actually mean like number of lines of code or number of words I write because that's stupid. I mean the impact I have in improving the Ethereum blockchain and ecosystem and wider society. It's often the case where there are periods of 20 minutes where I do more useful things than I've done in the past 3 weeks. And there are periods of entire weeks when I feel like I've done nothing at all. Trying to maximize those high productivity periods, like bursts, and minimize those other areas, I don't think I've fully figured it out yet.

K: Feel free to skip this question because I wasn't sure to include it but the question was what country are you legally a resident of or for tax purposes or where are you a resident?

V: Yeah, umm. So I guess like...

K: I wasn't sure to include this so I dunno feel free to answer it or not.

V: Mhm. I mean I spend a lot of time in Singapore. I also just spend realistically the big bulk of my time just traveling everywhere around the world. Probably Canada and the US quite a bit. Germany in Berlin some of the time. Just like different Asian countries some of the time. It's like really distributed. I don't think any one country takes up more of my time over the last two years.

General Ethereum Questions

K: Switching over to general Ethereum questions. Over a year ago you suggested that prices had outpaced development, but I'm curious if your opinion has changed given the current prices and the latest developments.

V: I'm actually much more optimistic about development than I was a year ago. I mean, I was always optimistic, but I feel like progress has just kept on getting better every three months. Like maybe about 9 months ago we were really happy that we had a spec. And after that we were really happy that we had a couple of implementations. And after that we were happy that we had a feature complete spec for phase 0. And now we're really happy that we have a feature complete spec for phase 1. And we have testing, and we have implementations, and the implementations themselves are starting to have testing, and people were tweeting out validator nodes on a testnet with 50,000 slots and processing state transitions and it's getting greater and greater. I'm definitely really excited about that side of things.

I'm also happy about that development in Plasma is really starting to pick up. Like I feel like there was this big lull just this last year where we were just expecting some team will come up with something but not that much really came out. And now there is Plasma Group, and Plasma Group has published this test version of their Plasma server and their Plasma client. There's these other projects, like Loom has Plasma Cash. I think OMSIGO is releasing theirs soon, among others. So Plasma is finally moving somewhere. I'm excited about ZK Rollup. I made a presentation about this recently. This is this approach where you do computation off chain then you put a snark of the computation on chain and you put data on chain and...

K: Sorry, can I interrupt you for a moment? The reason I'm interrupting you is there are some questions about the snarks and about the more technological side, and if it's okay for you, I would like to stick to these questions now and ask those later so that it's easier for people who are just going to tune in for a few questions so that they have their answers there and so I avoid having to ask you duplicate questions later on. Is that okay for you?

V: Mhm.

K: So would you say that earlier price has outpaced development and that that's reversed right now? So that development just keeps on going and the price are lacking behind.

V: Development is definitely keeping on going and prices are definitely flat so we'll see how it goes from here. It's really interesting.

K: Almost 18 months after the ICO euphoria, which, in your opinion, are the successful examples of dapps, utility tokens, and so, as it comes to real adoption.

V: In terms of things that people are using, Maker(DAO), Augur, and Uniswap are kind of would be the top three in a lot of people's minds I think. People are making trades on Augur. People are using DAI and Uniswap are being used for exchanging all sorts of things.

K: Are you still worried about MakerDAO? I remember, it might not be the words you used, but I remember seeing a tweet of yours where you mention some concerns.

V: I was worried about the fact that there are 2 million Eth locked up in this thing and like "Hmm, when was the last time we had more than 2 million Eth locked up in a smart contract?". I feel like MakerDAO team has taken a more methodical approach to this. That was much less reckless in a bunch of ways, which is good. But at the same time I think it's important for the community to have some kind of skepticism about just going all in head first in this like defy thing just because it seems like cool and fancy.

So the one example I brought up in the Laura Shin interview last week was that I think it's important. There was this one Twitter discussion that I remember having where someone pointed out that you could get I think it was 6% interest rates on Compound and I think you can get 2.5% on Maker or something like that. The person was saying "Hey, everyone should put a bit of their Eth in Compound because it's like an extra 3.5% returns and it's basically free. Why aren't you doing it?" and I'm like "Uhh, dude, you do realize that smart contracts have risks and if you're making that claim you're implying that Compound has less than a 3.5% chance of breaking in the next year and how much are you really willing to stake behind that claim?" and the reply to this was "Oh sure, that's reasonable, but you can start putting in a little." and I pointed out that "Well, you can put in a little but then only put in a little and that's fine but that's how I lost 2 Bitcoins to BitScalper back in 2012." I definitely support experimentation but I think people should be clear-eyed and realistic about these kinds of risks.

K: Do you have a vision for what comes after Eth 2.0? Does Ethereum become a very reliable and somewhat stagnant base layer, with most of the innovation happening on Layer 2? Or do you expect that the base layer should continue to evolve in dramatic fashion to keep up with the latest technology?

V: I've definitely become more recently in favor of more and more stabilized base layer. Maybe earlier on, we had these plans that oh, we have Ethereum 2.0 that does quadratic sharding, we have Ethereum 3.0 which is super quadratic sharding. It would be even more complicated and more fancy. I feel like more recently that what's changed in my thinking is that I do believe that we will have Ethereum 2.x or 3.0 or whatever but it will be more kind of incremental and marginal so adding starks for security for example. Adding data availability proofs. Adding post-quantum security. Adding more and more security upgrades over time. Eventually increasing the shard count, bumping it possibly past 1024, maybe bumping it all the way up to 10,000 and things like that.

I don't think we ever need to do super quadratic sharding for example. Super quadratic sharding basically means that you have your beacon chain. Your beacon chain keeps track of all the shards, and each shard has a bunch of data. And the reason why it's called quadratic is because if you take like C as being the amount of computing power that a node can process then each block and each shard has a size of C. And then C is the size of a beacon block and then C is the total number of shards that it can handle so you have like C2 total scalability. Super quadratic would say that you have shards inside of shards inside of shards and so it could go up to C3 or C4 or C to pretty much any power. The reason I'm skeptical about this is that first of all it just adds a huge amount of complexity. And second, ultimately when we talk about C2 there is a denominator like C is measured in something. And it's measured kind of per unit time. You can actually make quadratic scaling have as much scalability as you want by basically just increasing the block time.

The approach here would be that we have recently been coming up with these kind of layer 2 approaches for increasing cross shard communication capacity. If you look up I think Layer 2 Fast Cross Transactions or something like that on EthResearch then basically what you'll find is that we've come up with a way to support very fast cross shard transactions as a higher level language on top of some low cross shard transactions. That's really nice because it means that the base layer can be slow and most of the time transactions can happen pretty quickly.

Then what you can do is the base layer can kind of become slower and slower as the scalability goes up and up but from a user level point of view things will still appear like they are all very fast. I think approaches like that and then approaches like doing privacy as a layer 2 and doing things like CK Rollup for more scalability as a layer 2. And I think doing asynchronous cross transaction as a layer 2, I really do think that we can do basically anything that you could do on a blockchain as these layer 2's on top of a scalable data layer.

K: I think it's fair to say an initial shared vision/gameplan involved the EF funding development of a technology trifecta (blockchain, swarm, whisper) + a browser to use it all. Has that plan been lost and if so is that a good outcome?

V: Hmm. I think the plan of the Ethereum Foundation kind of being the sponsor of the 3 has been lost, and I think the outcome is good, because the outcome isn't that those 3 things have been lost, the outcome is that those things are being worked on by other members of the community. Like for example, you have Ethereum integration into Opera. You have MetaMask. You have Ethereum integration into Brave. You have integration into the HTC blockchain phone. You have the Samsung blockchain phone. You have all of these different environments where people can Ethereum and more and more are just popping up quickly. I think all of those things are good things. I think on the user-interfaced browser side things are moving along well. On the Whisper side, that's something that's definitely happening slower than expected and that's definitely something that I hope can happen more quickly. As for Swarm, I think it seems multiple file storage protocols are actively proceeding forward so I'm fairly happy there.

K: How do you feel about the progress OmiseGO has made with their MoreViable Plasma release?

V: How do I feel about who?

K: How do you feel about the progress OmiseGO has made with their MoreViable Plasma release?

V: I think it's definitely great that they are making a lot of progress. And I think technologically, and I've told them this, that these flavors of Plasma that require users to download everything in the Plasma chain aren't really the best approach to take, and I think flavors like Plasma Cash and Cash Flow are better because instead of being O of N for users they are O of Login so you can have users run like Bug browser extensions to verify Plasma blocks. And I've talked to them about this and they seem like interested in upgrading to those other flavors of Plasma over time which is, I think, great.

K: Recently someone did some in-depth investigation into Ethereum holdings and your personal wealth. In my mind, that's really nobody's business but yours. So my question is how do we protect identities on the Ethereum? What is the current status of privacy mechanisms like ZK Snarks? When can we expect to see more accessible privacy options?

V: Technologically, it's very possible to make privacy preserving systems on Ethereum. The main obstacle to them actually being privacy-preserving that I see so far is that there is this really subtle issue in the Ethereum blockchain that because you need to have Ether to pay gas for transactions, you need to like basically the transaction that includes the cryptographic zero-knowledge proof that lets you claim Ether that you put into one of these privacy preserving mixing systems. That itself basically links your output to Ether that

you already had in the clear and that itself basically unanonymous you.

So this is something that account extraction is definitely going to fix, and it's something that we could theoretically fix with a layer 2 network as well. It just hasn't been done yet, but I definitely encourage people working on it. Aside from just privacy of money the other big reason why I support people working on it is that there is just a lot of non-financial applications on Ethereum.

You don't want every single piece of a persons activity to be linked to every other piece of a persons activity. I think the best default is if people, just by default, automatically use a different account for each application that they log into. But if you do that, then you do need to have some way to move Ether between those accounts without that looking like you're just clearly sending money to yourself and then linking all those accounts together. So that's a really good initial use case for a privacy solution. I definitely support things like that happening.

K: There is a lot of talk about the "failures" of Ethereum governance from some in the community, but what do you see as the primary advantages of Ethereum's somewhat unique governance structure, and what role can/should the broader community of non-devs play in this structure?

V: I honestly don't think that it's failed.

K: It's a loaded question. It makes certain assumptions, I guess.

V: I think that if you look at kind of outcomes that people in the community broadly wanted, so like for example technical upgrades, frontier to homestead, homestead to Byzantium, Byzantium to Constantinople, they all happened.

In those times when kind of centralization and rapid development was needed because there were security emergencies like DOS attacks about 2.5 years ago, the community came together, it happened. Hardforks were successfully rolled out in 3-6 days. The issuance reduction from 5 to 3 was successfully done. The issuance reduction from 3 to 2 was successfully done. Serenity and Eth 2.0 are moving forward. Eth 1.x is moving forward. ProgPOW is moving forward slowly but it's definitely itching forward and there is audits happening. In terms of outcomes that at least as far as I can tell the majority of the community is broadly aligned and wants to see happen have happened.

I guess ultimately in the long run performance is the best judge of a governance system because if it doesn't perform than what's the point? And everyone who is not ideological will end up migrating to systems that do perform better.

So I feel like we've done pretty well on that front. In terms of things that I think are still not perfect, I think that the main challenge right now is that there are these kind of wedge

issues where the main kind of failure mode seems to be that they can just cause the participants of the governance process to just lose a lot of time bikeshedding(?). If you look at the All Core Dev's calls, ProgPOW ends up taking half an hour every call.

And then there is this fund recovery stuff that just keeps on popping up in almost the same format at least every couple of months and there is just issues that keep on repeating ad nauseam and that clearly takes a lot of load on people.

Part of the reason why seems to be that there aren't sources of polling the community that people kind of trust and that have common knowledge that they are legitimate. For example, right now you have carbon votes. You have votes on GitHub with like thumbs up and thumbs down. You have votes on Reddit. You have votes on Ethtrader.

I personally do take those signals seriously especially when there is multiple signals that say the same thing. For example, one of the things that I found interesting was this recent poll on inflation funding and it was really preliminary and only 90 people participated but there was a bunch of people in favor of it. I didn't see strong condemnation of it like I saw strong condemnation of like, EIP 867, the general purpose fund recovery one. I found that interesting because you might not have guessed that people who are against fund recovery might still be in favor of inflation funding. But hey! It turns out that the way that a lot of people are.

I think coming up with ways of measuring the community better that aren't just votes where a few rich people vote or Reddit votes where pretty much anyone can come in and vote. Those are things that could really be useful. Like even the Ethtrader polls I think are interesting because of how they are governed by donuts, so you have to be an actual participant in the community in order to be able to have a vote that makes a big difference. More experiments like that.

One experiment that I have been in favor of recently is that I think people should just independently come up with lists either GitHub accounts or Ethereum addresses or something that likely correspond with unique humans who are active members of the Ethereum community with some level of security. Jeff Goldman recently made the suggestion and I retweeted it and he retweeted my retweeting of him which was wonderful.

The idea behind that is once you have those lists you can use them as kind of a higher security source of input for things like CLR's, for community polls, for quadratic votes, for just all sorts of different kinds of votes and that might be kind of an improvement over both kinds of carbon votes that just favor rich people versus Reddit votes that can just get brigaded easily.

But those things are problematic too because if you start making judgments about who is part of a community then that

itself is just a horribly subjective exercise that's incredibly prone to bias and might fail in different ways but I'm generally of the view that having more indicators is better than having fewer indicators.

K: As we begin to possibly enter a more robust multi-chain world, what do you believe is the unique value proposition of Ethereum, in comparison to the value propositions articulated by many competing chains (often focused upon scalability, interoperability, on-chain governance, etc.)?

V: I think Ethereum does have an opportunity to continue to position itself very uniquely in the space. And I mentioned some of this briefly when I had that interview with Eric Connor with EthHub last week but the basic idea is that you have all of these other chains that are going to this on chain governance and on chain voting, and highly activist layer 1 fund recovery, like blockchain central nervous system whatever whatever direction. Those things have some advantages, but I think Ethereum should avoid falling into the trap of trying to compete with those things. Even though those things have their genuine fans, I would actually favor the Ethereum community just explicitly saying "No, we're not doing that." and instead going this direction of relatively at least post 2.0 and after 2.0 is rolled out valuing more conservatism, this more kind of decentralization and more technical decentralization, more of this kind of distributed approach to governance, more of this approach to doing things only if they satisfy multiple communities of stakeholders and things like that.

So basically, having some similarities with how Bitcoin governance works, but definitely not going all the way in that direction. In terms of decentralization, for example, one example of the kind of differences that I've noticed, a lot of the proof of stake chains that I see, like I've seen launched so far, they tend to take the easy route and say "Oh, we're only going to have 20 nodes or we're only going to have 100 or 500 nodes. And then we're going to have this small but we're going to assume everyone is part of a stake pool and we're not going to do sharding we're just going to do maybe kind of internal sharding within each node. We're going to require stake pools to have data centers. And we're going to try to improve our stake like that." On the one hand, that has general kind of speed benefits, and that allows you to have wait and sees of one second and that allows you to process transactions per second without having to do the hard work of having to figure out how to shard anything.

But it does come at a high cost, which is that those systems seem to be much more prone to centralization. Like basically because even if the cost of running a validator node is non-prohibitive, if that cost is even high, like if it's even high enough to be annoying, then that creates this kind of inexcusable centralization pressure where smaller pools just aren't able to offer competitive rates of return. Larger pools are. And so people might migrate from smaller pools to larger pools over time and then the system centralizes, and that's something that I would really like to try and avoid.

Another example of this is that I think a lot of these newer projects are just fundamentally not able to have a diverse set of coinholders to the same extent that Ethereum and Bitcoin are.

The reason is a lot of these projects, and first of all because the kind of legal environment has become more restrictive recently, and they can't do crowd sales and ICO's, and these projects also end up wanting to get money so they get VC investments and so we have a bunch of VC's that have this very large portion of protocol tokens early on. And I think that's something that harms the perceived legitimacy of the projects when the set of coinholders is that concentrated. It also means that it's just going to have a harder time trying to get a decentralized set of stakeholders for proof of stake, whereas in Ethereum's case the coinholder set seems to be pretty diverse and pretty distributed as far as coins go which I think is a major advantage.

K: I know I have heard you mention implementing a supply cap and the benefits of doing so; I think many people really want to see one because to most people, finite supply triggers a value mechanism in our brains. Do you think a supply cap will be implemented? and if so when and what number?

V: So here's an interesting tension. So supply caps seem to be popular. Issuance funding for protocol public goods seems to like, and it's definitely too early to be able to tell if it will be popular but it also doesn't seem to be getting huge condemnation. If you have ongoing issuance funding then you can't have a supply cap. This is one of the examples of a trade-off between two nice things that the community will have to navigate. Another thing about a supply cap that I think it would be personally irresponsible to try and move toward a supply cap until the proof of stake system has been running for some amount of time and we have evidence that the proof of stake can run reasonably well with low levels of issuance.

K: Just wondering, when you say for some amount of time, is that months? Years? How long is that? Just to get a perspective.

V: I'm inclined to say a couple of years. It does take time for economic equilibrium to start setting in stone. Like even if you look at Bitcoin, it took five years for centralization pressures to really start hitting them on the mining side. These days the community is much larger and the centralization pressures will start happening more quickly but it's still something that we need to watch out for.

K: Would you, I think I saw that 140 million Ether number thrown out. Would you still stick to that as a number to achieve or is that something that we should completely forget and see how proof of stake runs for a few years?

V: I think if people want a supply cap, then 140 million is a totally achievable number. Right now, the supply is 105 million, and when proof of stake launches, maybe the supply will be 110 million. Then at some point, we will be able to cut down the proof of work mining reward. Then at some point the proof of work chain will be retired entirely. Maybe at that point the supply will be somewhere in the high 110 millions to 120. Then when that happens, you could totally just follow the same formula I added in EIP 960 and have the issuance just taper off to 140. I think that is something that totally could be done.

I think going toward 120 million as the number would be aggressive but 140 million could be achievable if people want a cap. The other thing to keep in mind though is that one of the intuitive arguments I have against caps is that I feel like projects that institute caps early on, there is something dishonest to this decreasing reward schedule concept. And the reason why I feel it's kind of dishonest is that you're basically claiming two contradictory things at once. You're using the present level of issuance of the system and the systems ability to operate under the present level of issuance as a proof that the system is safe. But then you're using the fact that it has this baked in decreasing reward schedule as a proof that it's finite supply. But then if it's finite supply then the reward schedule is going to decrease and we have no evidence that the system is going to be safe under the decreased rewards.

If we want a practical example of this it would be current Bitcoin fees today are about $140,000 a day and the current Bitcoin block reward is 12.5 BTC multiplied by 144 blocks which goes up to 1800 bitcoins a day which multiplied by $4,000 which is $7.2 million dollars a day. So Bitcoin going to a fees only model would decrease rewards by a factor of 50. But if you take Bitcoins mining power and divide it by a factor of 50, that's not much stronger than what ETC has, and ETC got 51% attacked. So I think in general people should view promises of supply caps, even if they are backed by angry and ideologically excited people that are extremely attached to their selling points. I think people should view them as less credible than people generally view them now. But at the same time there is this argument that Proof of Stake can achieve the same level of security much more cheaply than proof of work, and so maybe if proof of work with a supply cap can't work, proof of stake with a supply cap can work. And if he wants to do the number on that, Ethereums current transaction fees per day are something like I think 500 Ether so if you take 500 Ether multiplied by 365 days a year, you get 180,000 Ether ever year. And 180,000 Ether every year basically means like the equivalent of 0.15% annual issuance. 0.15% annual issuance with 10% of the staking, that means 10% of the staking can get 1.5% annual reward. So it's definitely not out of the question, but it's an unproven hypothesis that 10% of Eth

stakers will be willing to stake, in exchange for a 1.5% annual reward. So we'll see. I think it's almost counter-productive to argue about this too much before we have clearer numbers of how many proof of stake participants are willing to participate. Then after we have those numbers, things will get a lot more interesting.

Technical Ethereum questions

K: Regarding beacon chain. You've been thinking about on chain randomness for a long time, from Randao around 2016 to now VDF (verifiable delay functions) and threshold signatures etc etc. Besides protocol security, how else do you think having cheaply available provable randomness on the web will change the world? What will the world do differently with this randomness in the future?

V: Sure. So I think aside from increasing protocol security, having this easily available randomness can definitely be useful to just many kinds of applications. The really obvious one is just on chain lottery. Like if you even think about these multi-million dollar national government lotteries that people do, the randomness is kind of opaque and it's hard for people to really be convinced that it works. I think if we have a robust VDF ecosystem with reasonable updated VDF hardware running then that's an example of something that could run on a blockchain and possibly even should run on a blockchain.

In general, lotteries and any kind of game that involves randomization. There is also other types of protocols that rely pretty heavily on randomization. There is games that have some kind of hybrid between relying on randomness and relying on skill. There is a lot of different kinds of mechanisms where you just end up needing some sort of randomness because it can't be perfectly deterministic. There is definitely just this big long tail of use cases for things that want random numbers of some kind.

Even proof of stake algorithms that are used on layer 2 of Ethereum possibly. Oh here's another one! Increasing the efficiency of Starks. Starks currently have a size of 50 to 150 kilobytes and a big part of the reason why is because they need to use this (something) protocol where they basically create a Merkle tree of all of this extended computation trace, then you use the Merkle group as a source of randomness. Based on the Merkle group, you randomly pick some branches, you check that those branches are correct. And the reason why you use this protocol is so you can't create data that's mostly incorrect and just selectively pick the branches that you think are correct.

You basically just have to keep trying to create a bad proof over and over again until eventually, you find one that works. The advantage of moving from fiatamirror(?) to using a VDF for randomness, is that if you use a VDF for randomness, there is no ability to try over and over again. So instead of a stark having, say, 80 branches, a stark might have, say, 20 branches. And with 20 branches, the stark would potentially,

the size of it, go down by a factor of 4, and starks for anything would be able to comfortably fit inside of one block, which would be really interesting. So there is really a big bunch of use cases for randomness that would be really interesting to unlock.

K: I interrupted you earlier, and now we got to the question, and I'm happy you starting talking about Starks, because somebody asked a question about this. Do you think Stark proofs will eventually become small enough to use in place of Snarks in schemes such as roll-up? Do you eventually forsee transaction aggregation using Starks at Layer 1 of the protocol rather than Layer 2? So those are 2 questions.

V: Yeah so I think transaction aggregation using starks at layer 1 is definitely useful when we want it to have a post-quantumable sort of less aggregation (couldn't really understand that last part). So that's one major use case. Another use case would be just for verifying the correctness of state transition function but that's like very far away because if we want to do that then we have to have starks that are powerful enough to execute over a virtual machine and that's just something that has a huge amount of overhead in so many ways.

I think starks for layer 2 protocols is definitely something that's more achievable in the near term. I do think that they are going to be small enough for use inside of blocks, and one of the things that encourages me is that we've done some recent studies of what causes the Ethereum network to not work well. Like right now, what causes high uncle rates? And it turns out that currently we're underpricing data, or sorry we're overpricing data and underpricing computation. So actually the Ethereum blockchain could handle blocks that are maybe 3 or 4 times bigger or maybe more as long as they don't have more computation than they do right now. So even if a stark is 100 kilobytes or whatever, that's something that could eventually fit into an Ethereum block in the future.

K: With the switch over to Proof of Stake and the need for stakers to maintain uptime will the security requirements be a barrier to entry for an average user who wishes to stake?

V: I don't think so. So we've actually tried really hard to make staking amateur friendly.

K: Even I'll be able to stake, hopefully.

V: Yes. So the two ways that we've done this. One way you don't literally have to be online all of the time. So you as a staker can be profitable as long as you are online 2/3 of the time. You can literally go offline for days at a time and as long as you come back online and are online most of the time you are still earning a profit.

K: But is that 2/3 calculated within a specific timeframe or within the total staking timeframe?

V: Within the total staking time.

K: Okay.

V: The one exception is that if many other people are offline and the system stops finalizing, then the penalties for being offline go up quadratically. The way that I interpret staking is that staking is kind of like being part of the reserve army. You don't have to go to battle, you can stay at home, but if a war happens then you have to get drafted and go to the field but normally wars don't happen. So it's that kind of relationship where if an emergency happens you have to really make sure that you're online to defend against it but otherwise, eh, online 2/3 of the time and you'll be okay.

The other thing we do is we have this anti-correlation mechanism which basically says if you get slashed, so if you get slashed for misbehavior, then you only lose a percentage of a deposit, which is three times the percentage of the other validators that have been slashed around the same time period. And what that means is, once again, that if there is a big attack, and there is lots of people misbehaving, then you stand to lose a huge amount.

But if you're just the only one who misbehaves and you cause a little tiny fault that doesn't really affect the blockchain, then you lose like only one Eth out of your total stake. So that also just means that you don't have to put armed guards in front of your validator node and run 7 crazy layers of firewalls to make sure we don't get hacked. It's all about safety in numbers rather than safety in making individual nodes super robust.

K: There are two questions that I will ask at the same time. One is what is your biggest concern in transitioning to proof of stake and another question is: in an ideal world, what are 3 things that could happen that would allow Serenity Phase 2 to be deployed quicker? Is there anything members of the wider community can do to make these things more likely to happen?

V: So what kind of things can make Phase 2 happen more quickly? I think right now it's just mostly this long research and development slog.

If you're a technical person, and you're interested in participating in like testing, reviewing the spec, adding tests, checking compliance of tests, writing code for one of the clients, like all of those things. Any of those things can make things go faster. If you are a dapp developer, then I would encourage people to comment on some of the things that we are looking to do for phase 2.

We're in the process of gathering comments around like what should smart contract execution layers look like? What should cross-shard transactions look like? What would abstraction

look like? And what would the Eth 2.0 ERC-20 standard look like? If people have opinions on things we have posted on that then I would definitely highly encourage sharing them. If you're someone with money that you're willing to donate, you can donate it to the Eth 2.0 development teams. Right now actually GitCoin is running their second round of their CLR experiment so if you go to www.GitCoin.co/grants if you make like even a tiny donation then it will probably get multiplied by like 5 or 10 or even more from the CLR so I would encourage supporting Prismatic Lighthouse, Pegasus, ChainSafe, any of these other wonderful 2.0 teams.

If there's anything, if you're just like a community member, there's also things like education, things like supporting developers. There is a lot of little things that people can do to help make Eth 2.0 happen faster. Also, the other probably related question to answer is what you can do to make layer 2 development happen faster because layer 2 is like plasma and ZK Rollup and those things are also really important, and in that case, just using them and giving feedback is a big part of it because there are tests that are available already. Another thing that needs to be done is just helping to standardize them and help to make sure that we don't have like 15 different protocols that are totally incompatible with each other. Just generally help these projects along to usability.

Closing questions

K: Vitalik, do you have a few more minutes for 3 closing questions?

V: Sure.

K: So a question that was asked by a few people is outside of crypto what fascinates you or what do you daydream about in the abstract or concretely aside from crypto?

V: I guess out of my bigger interests, one is that I follow Glen Weyl's radical mechanism design stuff pretty closely and I find that interesting. The economic space and also this rationalist space in general. Longevity and anti-aging research, I care about that a lot as you can probably tell.

K: I wonder, by the way, is that something that came from the Peter Thiel influence or was that prior to that or...?

V: I actually read Aubry's book when I was 13 so I've been a huge fan of his since like before I knew I had the ability to do anything about it.

K: How much do you actually work a week, was a question?
V: That's actually impossible to calculate because I'm not actually sure what counts as work and what doesn't.

K: What books strongly shaped your world view?

V: Honestly, like more recently, I've been doing books less. I've been just reading things on the internet more. And in that

case just the entire Soidster Codex(?) blog is probably a big one. Like there's just so much there you can probably just think of it as a book or a trilogy at this point, and that ended up influencing my thinking a lot. Obviously like radical markets and the other things that Glen have written. Economics and cryptography textbooks. And sometimes that just a more technical thing but then sometimes, especially on the economics side, you kind of mathematically form a version of important real-world insights as well. Also like just various things written by blogs by the various different people and intellectuals I end up following. Rob Hanson and his work on signaling is another significant one that has helped me understand how communities and discussions end up failing and not leading to the best outcomes sometimes.

K: Is his blog Melting Asphalt or is that his?

V: No Rob Hanson is Overcoming Bias.

K: Okay, because I read the Elephant and the Brain which I would really recommend everybody but I was wondering Hanson or someone's blog... but anyway, didn't want to interrupt. But there was a good blog that I wanted to refer to that I can't remember. What do you do to relax when you're not working and do you have a favorite t-shirt?

V: I like going on walks. I try to do that as much as I can. Do I have a favorite t-shirt? Maybe. I like the Alpaca corner or the buffalo corner you know one of those unicorn ones?

K: Last question. Where do you see yourself in 10 years time and do you ever think about early retirement?

V: Retirement? Definitely not. I don't know where I'll be in 10 years time. There are definitely times when I feel like I would just get tired and I want to go away but then I realize that first of all that would be a big loss in many ways but also I would get bored in three weeks and want to come back in some form.
K: Is there anything you would like to mention or some closing thoughts to the people listening to this, which will be mostly people on Ethtrader. Anything you didn't talk about or you would like to say?

V: I don't know. I mean like just keep being a great community.

K: Alright, then, Vitalik, thank you very much for answering the questions and good luck with everything you do and I think many people on Ethtrader will be on the front line seeing where this all leads to so thank you very much.

V: Thank you.