**The Father of Web3 Wants You to Trust Less**

**DO YOU EVER** find yourself wondering, “What is Web3?” You’re not alone. The idea is having a moment, whether you’re measuring by [VC funding](https://www.wired.com/story/andreessen-horowitz-new-crypto-fund-iii/), [lobbying blitzes](https://www.nytimes.com/2021/10/29/us/politics/andreessen-horowitz-lobbying-cryptocurrency.html), or [incomprehensible corporate announcements](https://twitter.com/gregisenberg/status/1458832245385580544?s=20). But it can be hard to tell what all the hype is about.

To believers, Web3 represents the next phase of the internet and, perhaps, of organizing society. Web 1.0, the story goes, was the era of decentralized, open protocols, in which most online activity involved navigating to individual static webpages. Web 2.0, which we’re living through now, is the era of centralization, in which a huge share of communication and commerce takes place on closed platforms owned by a handful of super-powerful corporations—think Google, Facebook, Amazon—subject to the nominal control of centralized government regulators. Web3 is supposed to break the world free of that monopolistic control.

At the most basic level, Web3 refers to a decentralized online ecosystem based on the blockchain. Platforms and apps built on Web3 won’t be owned by a central gatekeeper, but rather by users, who will earn their ownership stake by helping to develop and maintain those services.

Gavin Wood coined the term Web3 (originally Web 3.0) in 2014. At the time, he was fresh off of helping develop Ethereum, the cryptocurrency that is second only to Bitcoin in prominence and market size. Today he runs the Web3 Foundation, which supports decentralized technology projects, as well as Parity Technologies, a company focused on building blockchain infrastructure for Web3. Wood, who is based in Switzerland, spoke with me last week over video about where Web 2.0 went wrong, his vision of the future, and why we all need to be less trusting. The following interview is a transcript of our conversation, lightly edited for clarity and length.

**WIRED: As I understand it, the idea of Web3 at its most basic level is that the current setup, Web 2.0, is no good. So before we talk about what Web3 would entail, how would you describe the problems with the status quo?**

Gavin Wood: I think the model for Web 2.0 was much the same as the model for society before the internet existed. If you go back 500 years, people basically just stuck to their little villages and townships. And they traded with people that they knew. And they relied on, broadly speaking, the social fabric, to ensure that expectations were credible, were likely to actually happen: These apples are not rotten, or this horseshoe doesn’t break after three weeks.

And that works reasonably well, because it’s difficult and very time-consuming and expensive to move between towns. So you have a reasonably high level of credibility that someone is going to stick around and they don't want to be exiled.

But as society moved into something larger-scale, and we have cities and countries and international organizations, we moved on to this weird kind of *brand* reputation thing. We've created these powerful but regulated bodies, and the regulators, in principle, ensure that our expectations are met. There are certain statutory requirements that, to operate in a particular industry, you must fulfill.

This is not a great solution, for a few reasons. One of them is, it's very hard to regulate new industries. The government is slow, it takes a while to catch up. Another is that regulators are imperfect. And especially when they work closely with the industry, oftentimes there's a bit of a revolving door relationship between the industry and the regulator.

Another is simply a regulatory body has very limited firepower. It's how much money the government puts into it. And so necessarily, regulation is going to be patchy. They will be able to regulate maybe the biggest offenders but they aren’t able to retain a really strong influence all the time everywhere. And of course, the regulators and the laws differ from jurisdiction to jurisdiction. If you go somewhere in the EU, then Activity X is fine; if you go somewhere else, then it’s not fine. And as we become a very international society, this effectively means that your expectations are still not being met.

So we need to move beyond this. But unfortunately, Web 2.0 very much still exists in this very centralized model.

**Are we really talking about a failure of technology? Or are we talking about a failure of governance and regulation and competition policy? It sounds like you’re saying: Yes, it’s a failure of regulation, but the answer isn’t better regulation; there needs to be a new layer of technology, because regulatory failures are inevitable. Am I characterizing your view correctly?**

Yeah, absolutely. The model is broken.

**So let's talk about what should replace it. We've been talking about why Web 2.0 is not working. What's your handy elevator definition of Web3?**

“Less trust, more truth.”

**What does “less trust” mean?**

I have a particular meaning of trust that’s essentially faith. It's the belief that something will happen, that the world will work in a certain way, without any real evidence or rational arguments as to why it will do that. So we want less of that, and we want more truth—which what I really mean is a greater reason to believe that our expectations will be met.

It sounds like you're saying “less blind faith, more credible trustworthiness.”

Yes and no. I think trust in itself is actually just a bad thing all around. Trust implies that you are you're placing some sort of authority in somebody else, or in some organization, and they will be able to use this authority in some arbitrary way. As soon as it becomes *credible* trust, it's not really trust anymore. There is a mechanism, a rationale, an argument, a logical mechanism—whatever— but in my mind, it's not trust.

**You've written that Web3 will bust platform monopolies like Google and Facebook. Can you explain how it will do that?**

Yeah, I guess the thing is, I don't know if it's going to—I mean, I think it's a logical improvement. And I think in the grander scheme, it’s inevitable. Either it’s inevitable or society’s going down the pan. But in terms of concrete, it’s a much more difficult question to answer.

But, OK. In terms of technology, what do we have? We have cryptography. Cryptography, at its basic level, allows me to talk to my friend but for the communication channel to be public or go through a third party with me still having a good level of expectation, credible expectation, that it will be a private conversation. It will be as private as if we were in a field and chatting to each other and could see there was nobody around.

**Just taking encrypted communication as an example, that so far seems very compatible with corporate monopoly. Like, WhatsApp offers encrypted communication. There’s some controversy over the degree to which that is truly satisfying your desire for privacy, but I would still argue that that’s an example of encrypted communication that’s controlled by one of the most powerful companies in the world and has billions of users.**

It's an interesting one, and on the face of it, sure. But there are a few important differences. One of them is, what if WhatsApp introduced into their service a key that allowed them to decrypt all conversations? How do we know that it’s not there? You have to *trust*. We can't see the code, we can't see how their service runs, we can't see their key structure. So all we have is the blind trust that they are telling the truth. Now, OK, maybe they tell the truth because they're scared that their reputation will take a big hit if they don't. But then, as we saw with some of the Snowden revelations, sometimes companies don't get an opportunity to tell the truth. Sometimes, security services can just install a box in their back office, and they're told, “You don't need to look at this box, you're not allowed to say or do anything about this box, you just have to sit quietly.”

**It sounds like open source software would accomplish what you’re talking about, but you’re not just describing open source software. When we talk about Web3, we're talking about the blockchain, which is a completely different way of architecting the internet. So how, technologically, do you achieve this lack of dependence on trust?**

I think a degree of truth is necessary. And by this I mean openness, transparency. Blockchain technology uses both cryptography and certain game theory economics to deliver its service. We need to understand the node infrastructure of the network; is it really peer-to-peer or is it actually run from one data center by a company that manufactures and sells hardware and is required to be consulted before a new node can come online? The details make the difference as to whether it's basically just Web 2.0 in disguise or whether it is actually legitimately open, transparent, decentralized, peer-to-peer.

**Let's drill down on the idea of “decentralized.” I mean, the internet already is decentralized, right? Internet protocols are not owned by a company. While on a practical level, people tend to route their behavior through gatekeeper platforms, they don't necessarily have to. You don't** ***have*** **to message on Facebook, it's just convenient. So when we talk about centralization and decentralization, what does that mean?**

In essence, it means I personally can become a provider or a co-provider of this overall service just as easily as anybody else in the world.

**How realistic is that, though? From where I sit, it’s hard to imagine anyone outside of a small subset of people with high technical literacy actually exercising that right to participate in providing the service. And in that scenario, it sounds like you would have a different kind of centralization. Perhaps it would be more than just, you know, a handful of all-powerful CEOs, but it would still be a small subset of people for whom that's a meaningful freedom.**

There's a big difference between having a right or a freedom that you could execute if you had bothered educating yourself well enough, and the inability at a very basic and fundamental level of doing something because you lack the inclusion in an exclusive group. If I educate myself well enough on material that is freely available, and that's all that is required to become a co-provider of the service, then that is a free service.

**I went to law school, and I could say, look, anybody could learn the law. Anybody could study, get into law school, and then study for the bar. But in fact, at least in the US, it is a guild with very high barriers to entry, most notably cost. Even if the barriers to entry in the legal profession are higher than in programming, that doesn't necessarily mean that the barriers to entry in the world that you come from are not meaningfully high. I understand the distinction you’re drawing, but I wonder if that's sort of a naive—forgive me—reading of social arrangements to think that everybody just kind of has the choice to go become an expert Web3 programmer?**

No, of course. In principle, this isn't about being a Web3 programmer. You should be able to enjoy most of the ability to evaluate something without being an in-depth core developer. But there are an awful lot more programmers in the world than there are lawyers. And there's a good reason for that. Programming a machine actually only requires knowledge of a language that is reasonably straightforward to learn. You can be in a random little village in India, that just happens to have an internet point, and you can learn JavaScript in a week. You can't do that with American law.

I’m not going to try and persuade you that literally every person in the world could do this. But the point is that the more people that can do this, the lower the barrier, the better.

**This still feels a little abstract. Someone who's reading this might be thinking, “What would I be** ***doing*** **in a Web3 world?”** **Can you sketch out what that might look like? A certain a certain kind of activity or app interface or transaction?**

I think I think the initial breed of Web3 applications will probably be mostly small iterations on Web 2.0 applications. But one thing that Web3 brings that Web 2.0 cannot easily service is financial obligations or economically strong applications. This is where individuals in a peer to peer fashion can have economic services between themselves.

This isn't about sending money per se, but it's about sending things that are or can be credibly rare, or credibly difficult, or credibly expensive in some way. So we can imagine, for example, dating apps where you can send virtual flowers, but we can only send one bunch of virtual flowers per day, regardless of how much you pay. And one could imagine, therefore, that sending a bunch of flowers every day to the same person is a very strong signal that they're into you. And this is a signal that you can’t game—that's the whole point. You can't pay to send more flowers.

**I don't mean to be a killjoy, but I feel like Tinder could just add that functionality to Tinder.**

They *could,* right. They sort of do—there’s the star thing that you can only do once per day. But guess what? They're a profit-motivated company. So if you pay Tinder enough, you can just send as many stars as you want.

**But won’t companies built on Web3 still have the same market incentives as Web 2.0 companies? I could be missing something obvious, but it's hard to think of technological developments throughout history that didn’t allow for more concentration of political or economic power. So why should we expect this blockchain-based, decentralized Web3 to break the mold?**

I've always been into technology, since being a youth. I learned to code when I was like eight years old. I've never seen a technology that existed to limit one’s power. As you've said, every technology that I can think of has served to make the user more powerful. They can do more stuff. They can be richer, they can fulfill the service that they provide faster or better or to more people. Blockchain doesn't do that. It's fundamentally different. It's effectively a social construct. It's a set of rules. And the only thing that these rules have going for themselves is that there is no one with arbitrary power within the system. You can be reasonably certain, especially if you're a coder, then you can you can look at the code and know that it's doing the right thing. But you can also be reasonably certain just on the basis of the fact that so many people have joined the network on the back of this expectation. And if this expectation were not met, they would just leave the network.

**A lot of people have gravitated toward crypto because they see it as a way to overthrow the existing political order or the power of central banks. But you've suggested that Web3 will help support the liberal, postwar order. How do you see it doing that?**

I think the services and the expectations that we have are under threat because of the centralization of power that the technology allows. It's just a fact. There's not much that has come along before Facebook and Google that allowed that level of power for such few people. It's not that I don’t think Facebook and Google and all the rest of it deserve to be displaced, but that's not exactly the crux of Web3. For me, Web3 is actually much more of a larger sociopolitical movement that is moving away from arbitrary authorities into a much more rationally based liberal model. And this is the only way I can see of safeguarding the liberal world, the life that we have come to enjoy over the last 70 years. It's the only way that we can actually keep it going 70 more years into the future. And at the moment, I think we are very much flirting with quite a different direction.