Roundtable on
"Web3 – Current Trends and Political Implications"
Friedrich-Ebert-Foundation

Thursday, January 19, 2023

Molly White

Thank you for inviting me to speak at today's roundtable discussion. I am Molly White, and I research and write about web3, cryptocurrencies, and blockchain-based technologies. My educational and professional background is in computer science and software engineering, with a particular interest in the web and in web software.

Among other things, I maintain the website *Web3 is Going Just Great*, where I aim to highlight the many issues in the web3 space, but also in the cryptocurrency industry much more broadly. I am a fellow at the Harvard Library Innovation Lab and an affiliate at the Harvard Berkman Klein Center for Internet and Society, though I do not speak on behalf of either group, and the views I will be expressing today are solely my own.

Table of Contents

Summary

As will become apparent, I am very critical of the idea of "web3", and skeptical of its promised potential. The true innovations that have come out of web3 to date have been in enabling various new vectors for fraud, scams, and theft. What really distinguishes it from preexisting models is the lack of regulation, which has among other things allowed wealthy investors and crypto entrepreneurs to access entirely new pools of capital: money belonging to retail investors (that is, the general public: those without access to substantial capital, who are often inexperienced and less knowledgeable about investing or intricate financial instruments). Wealthy venture capitalists have further fattened their purses by investing in web3 companies via closed token presales, and then exiting while in the green when the sale opens to retail investors—profiting at their expense.

Though web3 advocates promise that the technology will someday bring about democratization, decentralization, and other positive changes, those have yet to meaningfully materialize. These advocates will often claim that "it is still early", despite the fact that the actual technological innovation of blockchains occurred fourteen years ago—an eternity in the software world. In reality, web3 advocates are claiming to have a miracle cure for the kinds of messy, human problems that are unlikely to be meaningfully addressed by software alone. Societal and political problems, like the undemocratic nature of much of the web or its centralization in the hands of a few large tech companies, can't be fixed by slapping a blockchain on the problem, but like with miracle cures, it can be very profitable for people to claim that they have the easy fix.

Definitions

To begin, I should first define "web3". "Web3" is intentionally a very nebulous term, with a meaning that tends to shift depending upon who you're talking to and—often—what they are trying to pitch. It is primarily a marketing term, and it has two specific strengths in that respect: for one, it immediately evokes the fear of being left behind in "web2" if one does not get on board; and secondly, it is a relatively new term that does not carry with it the sometimes negative baggage that some people might ascribe to more longstanding terms like "cryptocurrency" or "blockchains".

However, the term "web3" has also come to be used by a broader group of people than just crypto advocates, including—somewhat reluctantly—myself, and it does have some specific meaning. Typically, it is used to describe blockchain-based software projects that crypto advocates believe will be fundamental to the future of the web, or even to society more broadly. Proponents believe that by using public blockchains as a foundational technology in these services, they will be able to move the web in the direction of some specific goals, including decentralization, democratization, trustlessness, self-sovereignty, privacy protection, and censorship-resistance.

It is important to stress that public blockchains and cryptocurrencies are a fundamental part of this envisioned "web3". There exist many software projects pursuing the same goals of decentralization, democratization, etc. that do *not* involve blockchains or cryptocurrencies, and those are not normally considered to be a part of "web3"—although some web3 advocates do try to subsume those projects under the web3 umbrella.

The name "web3" is a nod to the web 1.0 and web 2.0 eras, which were retroactively named when it became clear that there had been a major shift in the character of much of the web sometime between the late 1990s and the mid-2000s. The term "web3" differs critically in that it was named preemptively, and refers to a *predicted* major shift that may or may not come to be. In fact, the blockchain definition of web3 that we discuss today is not even the first proposal of what might define the next major shift in the web. In 2001, web pioneer Tim Berners-Lee predicted that Web 3.0 would be the semantic web, referring to a much more machine-readable web that would bring about far more interoperability. So far, that too has largely not been realized.

You may have noticed that I keep using the term "public blockchain", which I also ought to briefly touch upon before I go on. With this, I am distinguishing public blockchains from their counterparts: permissioned, and sometimes private, blockchains. Permissioned blockchains are controlled by a central entity who allows only authorized users to write to the chain. Private permissioned blockchains additionally limit who may access the data stored on the chain. Permissioned or private permissioned blockchains are dramatically different from the public blockchains that are used in web3, and are primarily used in various enterprise proofs-of-concept, though are rarely deployed due to technological shortfalls that are typically better addressed with other forms of database. Although many web3 advocates will point to various press releases about major banks or large corporations "adopting" blockchain as evidence of some sort of buy-in to web3 as a concept, these quite often refer to permissioned or private permissioned blockchains, and even then usually refer to projects in very early exploratory stages. Going forward I will just use the term "blockchain" for brevity, but I will be referring to public blockchains throughout.

Web3's appeal

Web3 has been compelling to some because the issues it claims to tackle are very real and important. For example, much of the web has coalesced under a fairly small number of platforms controlled by massive tech companies who seek to extract as much profit as possible. Many of these business models revolve around extracting as much data as possible from users while maximizing engagement with advertising, leading companies to design software that can be actively detrimental to their users' well-being.

While some might argue that those who have a problem with them should simply choose not to use those platforms, they are becoming more and more difficult to avoid as these companies build monopolies by edging out or acquiring smaller competitors. Furthermore, these tech companies are broadening their reach far outside of what we might think of as the realm of the web, and now those who seek employment in a wide variety of fields ranging from drivers to dog walkers to freelance creatives may find themselves working for these very companies, and those who need these types of services may find these companies to be the cheapest option, and may be unable to afford pricier alternatives.

Financial inequality is another major problem identified by web3 advocates, who see wealthy people who are able to become ever wealthier thanks to credit scoring that favors those who are already wealthy when evaluating suitability for loans, and the existence of financial instruments and investments available only to accredited investors (who I believe are referred to as "experienced" or "sophisticated" investors outside of the US), a status determined based on net worth and/or income. Meanwhile, others are unbanked or underbanked, and face systemic barriers to accessing banking services and accumulating wealth.

When someone comes to you offering a solution to problems like monopolization by tech giants who prioritize profits over their users' or employees' well-being, it's hard to say no. But when that solution has yet to meaningfully address tech monopolies, financial inequality, or any of the other major issues it claims to solve, and has in fact created *new*, exploitative monopolies and further financial inequality, it must be evaluated critically.

Implications of widespread adoption

Before I begin to address the implications of widespread adoption of web3 technology, I want to address one challenge that arises when having these kinds of conversations.

Rather than talking about the widespread adoption of something that resembles today's web3, many web3 advocates prefer to talk of the widespread adoption of some as-yet unimagined version of web3. These often rely on assuming either that humanity will have somehow made some technologically infeasible achievements, or that there will have been major societal changes for which there is not a clear path (for example, "cryptocurrency will have been widely adopted and used day-to-day as a currency"). These make for challenging conversations, because one generally can't prove that an unlikely scenario will *never* happen. These are often unfalsifiable scenarios.

On the topic of technological infeasibility: there are some technological advances that are fairly safe to assume—for example, as time progresses, computers tend to get faster and storage tends to get cheaper. I have no problem with assuming that pattern will continue in a reasonable fashion. But many crypto advocates will argue various other hypotheticals—often ones that require you to assume that not only will humanity at some point in the future solve as-yet unsolved problems in computer science, but *also* that solving those problems will not result in the very likely outcome that the blockchains themselves will be rendered useless.

All that said, I will limit my preliminary statement to discussion of the implications of widespread adoption of web3 projects somewhat like ones we've seen to date, to avoid jumping down the rabbit hole of evaluating infinite hypothetical scenarios. If it would be useful to delve into broader hypotheticals during the discussion, I am however happy to do so.

Economic

If we envision a world in which cryptocurrencies enjoy broad adoption, and an average person uses them as either currency or an investment vehicle, then there are some implications to consider.

Volatility

Many cryptocurrencies tend to be enormously volatile, and so not particularly useful as currency. A world in which a cryptocurrency like Bitcoin is widely used as currency is not terribly likely, since its value fluctuates wildly, and there is no mechanism that would cause it to stabilize. However, it is possible to envision a world where the more volatile cryptocurrencies like Bitcoin continue to be used as speculative assets, while more stable cryptocurrencies are used as currency.

The value of cryptocurrencies is somewhat uniquely difficult to evaluate. Many cryptocurrencies have no inherent value, and are tied to no real-world good or service (for example, Bitcoin). Some crypto assets are more closely tied to something that could be more traditionally valued—for example, native tokens of crypto businesses tend to behave more like a stock, tracking perceived value of the business. However, these tokens lack the transparency requirements of stocks listed on public stock exchanges, leaving investors unable to make properly informed decisions when deciding which tokens to purchase. We recently observed the collapse of $FTT, the native token of the FTX cryptocurrency exchange—a company that was not publicly traded and almost certainly could not have ever *become* publicly traded due to the transparency requirements that would have exposed the alleged massive fraud that was happening there.

Stablecoins

The most stably-valued crypto assets today are stablecoins, which are designed to maintain a consistent "peg" to some other value—often a fiat currency like the euro or the dollar. In the case of asset-backed stablecoins, their peg is maintained either by maintaining a basket of assets—fiat currency, short-term debt, or even other cryptocurrencies—that could theoretically be redeemed for the stablecoin at a 1:1 value. In the case of algorithmic stablecoins, their value is maintained by an algorithm that encourages market movements that result in the peg being maintained. There are also stablecoins that combine the two techniques. Stablecoins pose a unique threat to the economy.

They tend to be very centralized, particularly in the case of asset-backed stablecoins where there is a single company that maintains control over the assets. Auditing and transparency are practically non-existent, and the entire system relies on blind trust that the entity maintaining the assets is operating honestly. There have already been numerous occasions in which we have seen operators of various major stablecoins act *dis*honestly: in 2021, the operators of the largest stablecoin (Tether) agreed to pay millions in fines and cease operating in New York after it was revealed that they had made false statements that Tether was fully backed. Furthermore, even a properly backed stablecoin that holds assets less liquid than cash are prone to bank runs, and there are no capital requirements, deposit insurance, or central bank lenders to help stabilize them.

In the case of algorithmic stablecoins, they are prone to failure. In May 2022 we saw the largest algorithmic stablecoin, Terra, collapse in sudden and dramatic fashion, wiping out billions of dollars in assets in a devastating blow to many investors who expected their stablecoin to be stable. Other smaller algorithmic stablecoins, such as Titan, have collapsed in similarly unexpected crashes.

Custody

Moving beyond the assets themselves, there is also the question of how people would hold on to their crypto assets in a world where they had achieved widespread adoption. Cryptocurrencies are comparatively difficult to buy and hold, with crypto wallets being notoriously user unfriendly. Cryptocurrency purists will say that the only proper way to store one's cryptocurrency is by self-custody, meaning that the user is the only one who has access to their keys, rather than third-party platforms. In addition to being more technically challenging than custodial cryptocurrency wallets, there is the matter of securely storing crypto private keys in a way where they are not susceptible to loss or theft. Self-custodying one's cryptocurrency is not entirely unlike holding all of one's assets in cash, in that it is far more prone to accidents, theft, and loss. It's why the Bitcoin faithful talk about stamping their seed phrases into blocks of metal and burying them in their backyards, and it's why there's a person currently lobbying the government of a town in Wales to allow him to spend millions of dollars to excavate a landfill in the hopes of finding a ten-year-old hard drive that might contain €170 million in crypto, assuming it still works.

For those who reasonably don't wish to try to self-custody their cryptocurrencies, they have to choose a crypto exchange, wallet provider, or other bank-like company to trust with their money. These entities are poorly regulated if regulated at all, and the past year alone has shown us the fragility of keeping one's crypto in systems like these. Any person who chose Celsius, Voyager, or FTX has lost access to their crypto assets and is awaiting the outcome of potentially lengthy and complex bankruptcy cases before learning if they will receive their assets back, and more likely what small percentage of those assets they'll actually receive. The list of other companies who have suspended withdrawals indefinitely but have not entered any formal bankruptcy proceedings is even longer. In some cases, the executives of those companies have disappeared.

Contagion

One could reasonably counter some of these concerns I have laid out by arguing that in the future, regulations will have changed such that there *are* consumer protections in place for the cryptocurrency industry, and so there will be the equivalent of bank deposit insurance and other safeguards to allow users to more confidently invest.

This, however, implies government intervention of the kind that is antithetical to the cryptocurrency ethos. Part of the whole goal of cryptocurrency is to create a world in which people don't have to trust banks. If we end up in a world where banks are backstopping cryptocurrency, then we have simply recreated the existing system, but with a more volatile asset class that is not tied to real world economic value.

Furthermore, the kind of consumer protections that would allow consumers to confidently invest in crypto would also open up the enormous potential for financial contagion from the cryptocurrency ecosystem. If there has been one blessing in the past year of crypto collapses and complete devastation, it has been that there was fairly little contagion into the world of traditional finance, and those who chose to steer clear of cryptocurrency did not suffer due to having to help absorb the losses for those who did. That would not have been the case if the government had found itself in the position of having to bail out floundering cryptocurrency companies.

Social

There are social concerns when it comes to the widespread adoption of cryptocurrency, as well.

Privacy

A crypto wallet is identified by a string of characters, and there is nothing that inherently ties one to a given individual. All transactions to and from that cryptocurrency wallet are completely public, at least in the case of most widely-used cryptocurrencies. This means that once a wallet is tied to a specific person, either due to them intentionally or accidentally disclosing it, or due to some detective work on the part of a third-party, all of their transactions can be inspected as well.

Today, the implications of this are worrying, but often somewhat limited in their scope. People transacting with cryptocurrencies are not typically using them for day-to-day transactions. But in a future world where cryptocurrencies have achieved widespread adoption, this would be tantamount to my credit card transaction history being publicly visible to anyone who wished to see it. People could trivially deduce a person's location by looking at where they shopped, or to whom they paid their rent—information that would be extremely useful to stalkers and abusers.

The same types of surveillance that web3 advocates and others complain about in the current web, with large social networks collecting enormous amounts of data to use for ad targeting or to resell, would become even more pronounced with added access to detailed public financial data that could be mined.

Immutability

Blockchains are also immutable, meaning that once data has been stored to the chain, it can't be edited or deleted. With blockchains like Bitcoin, this is mostly simple financial data—the number of coins being sent or received. But blockchains like the ones used by web3 applications involve far more data, and some web3 projects are beginning to store user-generated data to the chain.

This opens up enormous risks as far as user safety, and content moderation is impossible *by design.* With systems that store user-generated content to a blockchain or immutable storage, if someone uploads revenge porn or child sexual abuse material, it is there forever and cannot be removed. Individual platforms built on that blockchain can implement content moderation systems on top of the chain that would not display it, but the data would still be there and could still be accessed by anyone, either by querying the chain directly or by just choosing to use a different platform built on the same chain. This means that if someone is a victim of revenge porn, the best they can do is reach out to individual platforms and petition them to hide the content—this could be many, many platforms, and even still, the content remains available on the chain to those who wish to look for it. Layering on content moderation in this way is not an adequate solution.

Legislation like the GDPR and various "right to be forgotten" laws are fundamentally incompatible with blockchain technology. Attempts to design systems that could comply with such legislation typically involve storing any personal data off-chain in centralized, secure, and modifiable databases, completely nullifying the goals of web3 to create decentralized, trustless software.

Wealth inequality

One major characteristic of web3 is financialization. In order to engage with any web3 project, you typically have to own tokens—either general-purpose tokens like Ethereum, or the specific token of a given blockchain-based project.

If we look at the example of *Axie Infinity*, a popular Pokémon-like web3 game where players acquired monsters which they then battled against others, we can see this in action: users first had to create a crypto wallet on the game's dedicated blockchain, buy Ethereum tokens, use those Ethereum to buy three monsters (currently priced at a few euros apiece, but once priced at more than €100 apiece), and then begin playing. High Axie prices resulted in the emergence of a completely secondary ecosystem of "scholarships", which was really a system in which users rented monsters to users who couldn't afford to buy them, in exchange for a cut of the tokens they earned while playing the game. This created a system in which wealthier individuals, and even venture-capital-backed startups, hired players in low-income countries like the Philippines to play *Axie Infinity* for them, while they skimmed a cut of the earnings. For a very brief period this was a way for those players to make substantially more than they could in other jobs, but that didn't last.

Axie Infinity presented a useful tangible illustration of the wealth inequality that often emerges in web3. The initial buy-in to play a game, post on a social network, vote in a decentralized autonomous organization (DAO), or do just about anything is often non-trivial. Even the fees to perform a simple transaction, like exchanging one type of cryptocurrency token for another, costs several euros. That relatively small amount still renders the ecosystem completely inaccessible to people who don't have a few euros to spare, particularly those in parts of the world where wages are lower. It creates a system that by design is simply not accessible to all.

Environmental

Finally, there are environmental ramifications that must be considered when talking about cryptocurrency. These primarily manifest in Bitcoin, which uses a consensus algorithm called proof-of-work. Proof-of-work is enormously energy intensive. Based on recent estimates of Bitcoin energy consumption, the network was consuming 77 Terawatt hours of electricity per year. If it was a country, it would rank slightly above Bangladesh in terms of annual electricity consumption and just below that of Chile, Finland, and Belgium—somewhere around #40 in the list of countries by electricity consumption. This is actually an improvement from past numbers, because the crash in Bitcoin price has caused a lot of Bitcoin miners to go out of business or to power off machines that were no longer profitable. Until June 2022, Bitcoin was consuming more than 200 TWh, which would place it somewhere around #23 in the list of countries by electricity usage—above Egypt and Thailand but below South Africa and Vietnam.

Some claim that Bitcoin mining is largely done using renewables, and so the environmental impact is lessened. This is a somewhat faulty argument, given that in many cases the renewable energy could go toward other productive uses if it was not mining Bitcoin, but also because it's simply not true: more than half of Bitcoin mining is powered by natural gas, oil, and coal.

Some blockchains use consensus algorithms besides proof-of-work, and those tend to be much less energy intensive. Ethereum notably switched from proof-of-work to a system called proof-of-stake last autumn, and reduced its electricity consumption by more than 99%. Unfortunately, such a migration is quite unlikely to happen with Bitcoin, which remains the largest cryptocurrency by market cap by quite a substantial margin.

Political approach

As far as the political approach to web3 and crypto more broadly, I will caveat my statements by saying that I am not an expert in European regulations—or in US regulations, for that matter. However, I believe it is critical to take great care in not introducing contagion risk to the financial system, and to ensure that consumers are protected to the best extent possible while also avoiding contagion risk.

Laws against fraud, money laundering, and plain theft can be applied to crypto just as they can be applied to crimes committed with traditional currency, and the rampant fraud in the web3 space needs to be addressed.

Another action that would go a long way towards consumer protection would be to treat cryptocurrencies similarly to other investments, and requiring the organizations behind cryptocurrencies to comply with auditing and transparency requirements. This would enable consumers to make more informed decisions if they do choose to engage with cryptocurrency assets, while also reducing the degree of fraud that can occur behind closed doors.

Separations between traditional banking institutions and cryptocurrency companies should be maintained or strengthened, in the interests of reducing the degree to which collapse in the cryptocurrency ecosystem could impact traditional finance.

The state of user privacy and data stewardship in web3 must be treated with extreme suspicion. Although many web3 projects like to claim that they are inherently more privacy-conscious because they use blockchains, the opposite is often true. Although a cryptocurrency wallet may pseudonymize a user behind the wallet address, as soon as that wallet address is connected to the individual it can reveal an enormous amount about them, including who they're transacting with, when, and in what amounts, what products they use, and what data has been connected to their cryptocurrency address. More products are emerging seeking to store more and more identity data on blockchains, such as professional credentials, identification documents, or even highly personal data like medical records. Although some of these projects encrypt the data, publicly storing it on an immutable ledger is a privacy risk that is simply not worth taking.

Web3's goals

Although web3 has not shown much promise in achieving its various stated goals, including decentralization, democratization, and user privacy protection, it is critical that we remember that web3 is not synonymous with these ideals.

There are many groups and organizations pursuing these same goals who have not tied themselves to using blockchains and cryptocurrencies. Fairmondo, for example, is a democratic, user- and employee-owned alternative to major e-commerce websites like Amazon. The decentralized web movement has pushed for years for decentralization, and there are many non-blockchain, decentralized web projects including BitTorrent, the Tor network, and the Mastodon federated social network.

The centralization, lack of democracy, and lack of user privacy on the web is not a technological problem. We have technologies to enable all of these things. Instead, it is a societal, economic, and political problem. It is extremely lucrative to be a tech monopoly, and to mistreat users and employees in search of higher profits. I think solutions to this problem will come not from some cure-all technological fix, as easy and convenient as that might be, but rather through societal change, including pressure from users and employees, regulation and legislation, and an environment that allows alternatives and competitors to thrive.