【翻訳版】Web3についての私の第一印象[Translated version] My first impression of Web3

石ころStones
Apr 9Apr 9

Hello, this is a stone.

The article My first impressions of web3 (written in January 2022) written by Moxie Marlinspikees, the founder of the messaging app Signal , was thought-provoking, so I will introduce the translated version.

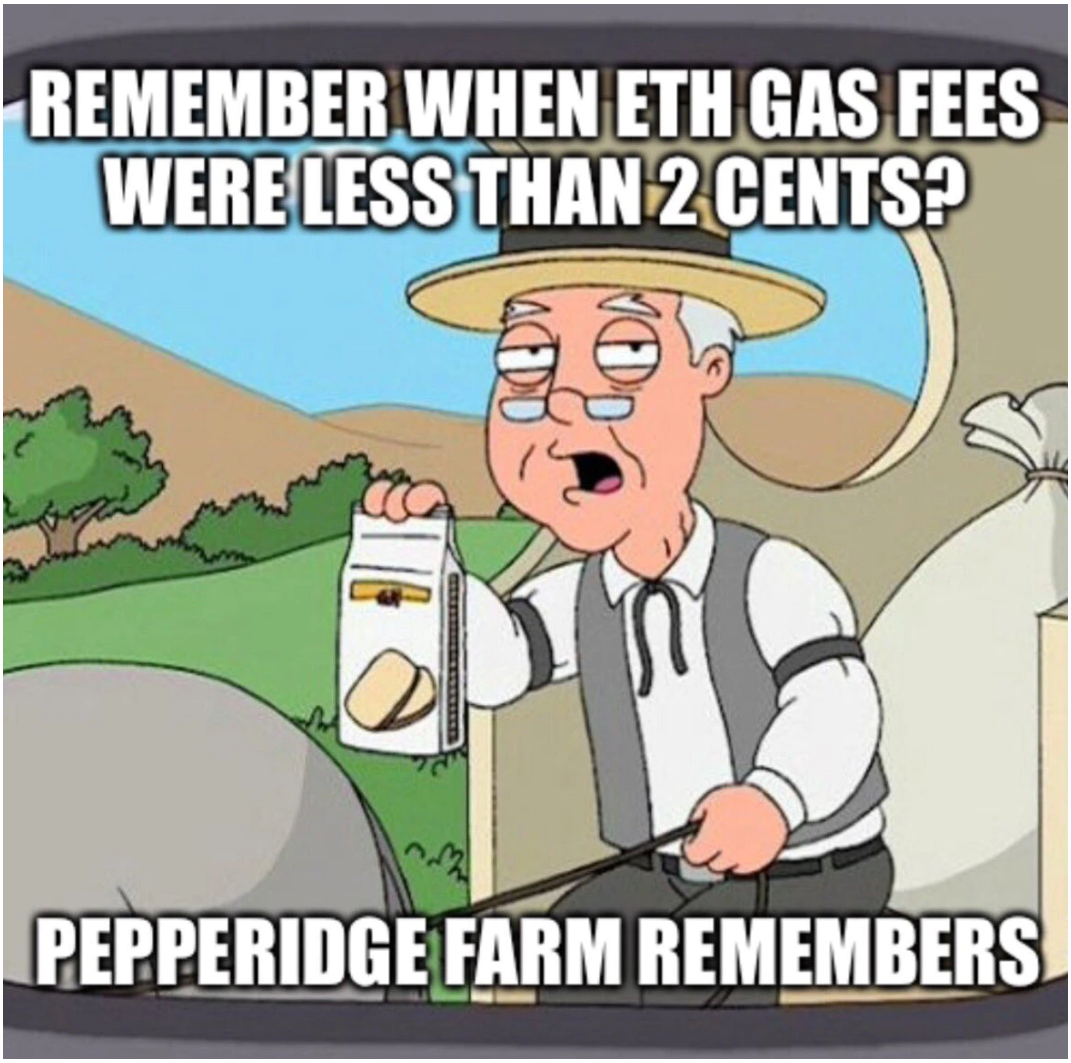
The original tweet that Moxie wrote an article got 30,000 likes, and Ethereum founder Vitalik Buterin and Elon Musk also replied, and it seems that it was controversial in a good way.

Personally, I found it to be the most interesting Web3 related article I read this year.

The translation is based on DeepL and has been modified in various ways.

Even though I consider myself a cryptographer, I'm not particularly attracted to "Crypto". I don't think I've actually said "get out of my lawn", but rather than the new NFT information, it's a *Pepperidge Farm Remembers* -flavored meme that "crypto" meant "cryptography." There are far more clicks.

[Supplementary stones] Refers to the following memes (material images) that are used together with the template sentence "Do you remember when XX was still ◯◯?". (I didn't have a version of the line "Remember when Crypto was still pointing to cryptography?", So I'm substituting it with another pattern.)



[Supplementary end]

And to be honest, I can't share the generational excitement of moving every aspect of life into a mechanized economy.

Even at the technically rigorous level, I haven't become a believer yet. So, in response to the recent focus on what is called Web3, I decided to thoroughly investigate what is happening in this field and whether I have overlooked it. bottom.

What do i think about 1 and 2

The word web3 is a bit vague, so it's hard to rigorously assess the ambitions that web3 has, but the general thesis is that web1 is decentralized, web2 concentrates everything on the platform, and web3 again. It's about decentralizing everything. web3 should give you the richness of web2, but also decentralize it.

It would be nice to clarify why a centralized platform emerged in the first place. In my opinion, the explanation is very simple:

1. **People don't want to run their own servers and will continue to do so.** The premise of web1 was that everyone on the Internet was a producer and consumer of content, as well as a producer and consumer of infrastructure.

   We all have our own web server with our website, our mail server for our emails, our finger server for our status messages, our own character for generating our characters. To have a charged-on server. But-I don't think this can be overemphasized- *people don't want it* . People don't want to run their own server.

   At this point, even geeks don't want to run their own servers. Even organizations that make software full-time don't want to run their own servers at this time. One thing I've learned about this world is that people don't want to run their own servers. Companies that did it for them emerged, succeeded, and based on what was possible with that network, companies that repeatedly improved new features became even more successful.
2. **The protocol runs much slower than the platform** . After more than 30 years, the email is unencrypted. On the other hand, WhatsApp has moved from unencrypted to full e2ee (end to end encryption) in just one year. People are still working on standardization to ensure video sharing on IRC (Internet Relay Chat). On the other hand, Slack allows you to create custom reaction emojis from your face.

   This is not a financial issue. If something is really decentralized, it will be very difficult to change it, and time will often remain stationary. It's a problem for technology. Because other ecosystems are moving very fast and if you can't keep up with them, you'll fail. As a result, there are parallel industries trying to define and improve agile-like methodologies and find ways to organize a huge number of people. Being able to move as quickly as possible is very critical.

   If the technology itself encourages stillness rather than movement, that's a problem. The secret to success was to take a protocol that has been stuck in the 90's, centralize it, and repeat it quickly.

But web3 is intended to be different, so let's take a look. To get to know this area quickly and better understand what's going to happen in the future, I decided to create some dApps (dencentralized apps) and create NFTs.

Let's make some distributed apps

To get to know the world of Web3, I created a dApp called Autonomous Art . This allows anyone to mint tokens by making a visual contribution to the NFT. The cost of making a visual contribution rises over time, and the funds paid by the contributor for mint are distributed to all previous artists (visualizing this financial structure, it resembles a pyramid). Will be). At the time of writing this article, over 38K USD (a little less than 5 million yen) has been spent on producing this collectible art piece.

I also created a dApp called First Derivative that allows you to create, discover, and exchange NFT derivatives that are tied to the underlying NFT, as well as financial derivatives that are tied to the underlying asset .

Both were able to get a feel for how this area works. To be clear, to avoid misunderstandings, the app itself has no particular "distributed" element, it's just a normal reactive website. This "decentralized" dApps means that the state and the logic and permissions to update the state are on the blockchain rather than in a "centralized" database.

What I've always wondered about in the crypto world is that the client / server interface isn't paying attention. When people talk about blockchain, they talk about decentralized trusts, leaderless agreements, and all of those mechanics, but the reality that clients are ultimately unable to join them is often obscured. .. All network diagrams are for the server, trust models are for the servers, and everything is for the server. Although blockchain is designed as a network of peers, it is not designed so that mobile devices and web browsers can actually become one of the peers.

With the move to mobile, we are living firmly in the client and server world, and it is completely impossible for the former to play the role of the latter. This question seems more important to me than ever. Ethereum, on the other hand, calls the server a "client." This means that there must be a client / server interface without a trust somewhere, but *without that word* , if successful, there will end up billions (!) Of clients over the server. I don't admit.

For example, dApps like Autonomous Art and First Derivative , whether running on mobile or the web, change or render state (collective artwork, its edit history, NFT derivatives, etc.). In

addition, we need to interact with the blockchain in some way. However, the blockchain cannot exist on mobile devices (or, in reality, desktop browsers), so you can't do this from the client. Therefore, there is no choice but to interact with the blockchain via a node running on some server.

server! But as you know, people don't want to run their own servers. That's why companies have emerged that provide API access to Ethereum nodes as a service, providing analytics tools, extended APIs built on top of the default Ethereum API, and access to past transactions. This is ... familiar. At the moment, there are basically two companies. Almost all dApps use either Infura or Alchemy to interact with the blockchain. In fact, even if you connect a wallet like MetaMask to a dApp and that dApp interacts with the blockchain via the wallet, MetaMask is just making a call to Infura.

These client APIs don't use anything to check the state of the blockchain or the authenticity of the response. The result of the call is not even signed. When an app like Autonomous Art says "what's the output of this view function for this smart contract", Alchemy and Infura respond with a JSON blob that says "this is the output" and the app renders it.

I was shocked by this. (People) have spent so much effort, energy and time creating a trustless decentralized consensus mechanism, but virtually every client trying to access it trusts the output from the two companies. Just do it and you're accessing it without further verification. Also, I don't think it's the best situation in terms of privacy. What if every time you interact with a website in Chrome, a request is first sent to Google, then routed to your destination and back. That is the current situation of Ethereum. Of course, all write traffic is already exposed on the blockchain, but these companies can also see almost every read request from almost every user in almost every dApps.

Blockchain followers, even with the emergence of this kind of centralized platform, the state itself is exposed on the blockchain, so if these platforms do something wrong, the client simply goes elsewhere. You might say it's okay because you just have to move. However, I point out that this is a very simplistic view of the dynamics that make up the platform.

Let me give you an example.

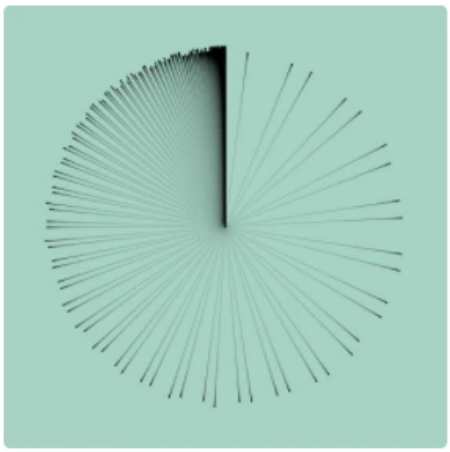
Creating an NFT

I also wanted to make a more traditional NFT. Many people think of NFTs as images and digital art, but NFTs generally do not store that data on-chain. For most image NFTs, that

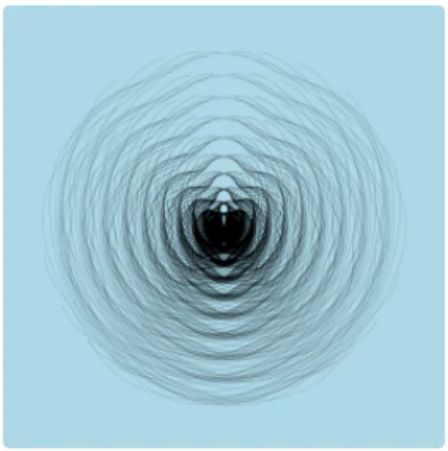
would be too costly.

Instead of storing the data on-chain, NFTs store URLs that *point to the data.* What surprised me with this standard is that the data in the URL has no hash commitment. If you look at many of the NFTs that sell for tens, hundreds, or millions of dollars on popular marketplaces, the URL points to a VPS running some Apache. Often just. Anyone who has access to the machine, who will buy the domain name in the future, or who puts the machine at risk can change the NFT's image, title, description, etc. to whatever they like at any time ("own" the token). Whether or not you are doing it). There is no NFT specification that tells you what an image should be, and you can't even check if something is a "correct" image.

Therefore, the web server that provides the image can choose to provide different images depending on the IP of the request source and the user agent, so as an experiment, we created an NFT that changes depending on who sees it. For example, it looked like it was in OpenSea and different in Rarible, but when I bought it and looked at it from my crypto wallet, it always looked like a big 💩 emoji. You don't get what you bid. There is nothing different about this NFT, and the NFT specifications are made that way in the first place. Many of the best NFTs can turn into 💩 emojis at any time, and I just made it explicit.



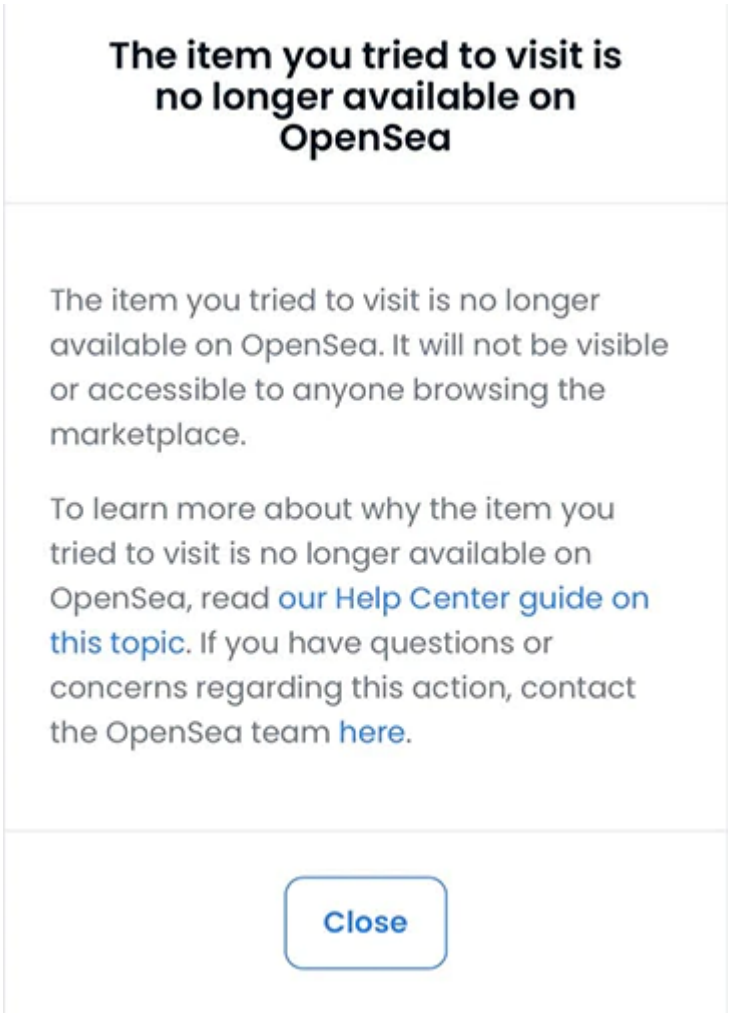
NFT on OpenSea



Same NFT on Rarible

Same NFT in a wallet

A few days later, without warning or explanation, my NFT was removed from OpenSea.



This deletion alleges that I violated some terms of use, but when I read the terms, I don't see anything banning NFTs that change depending on where they are seen, and I openly do so. I was writing.

But most interestingly, after OpenSea removed my NFT, **I no longer see the NFT in any crypto wallet on my device.** This is web3, but why is that possible?

Crypto wallets such as MetaMask and Rainbow are "Non-Custodial" (keys are stored by the user), but they have the same problem as the dApps I made above: wallets on mobile devices and browsers. Must work with. Ethereum and other blockchains, on the other hand, are designed with the idea of being a network of peers, but not so that mobile devices and browsers can really be one of those peers. It is.

Wallets like MetaMask need to do basic things like balances, recent transactions, displaying NFTs, to more complex things like building transactions, interacting with smart contracts, and so on. In short, MetaMask needs to interact with the blockchain, but the blockchain is

designed to prevent clients like MetaMask from interacting with it. So, like my dApps, MetaMask does this by making API calls to three companies that integrate this area.

For example, MetaMask displays recent transactions by making an API call to etherscan.

```
GET https://api.etherscan.io/api?
module=account&address=0x0208376c899fdaEbA530570c008C4323803AA9E8&offset=40
&order=desc&action=txlist&tag=latest&page=1 HTTP/2.0
```

... Display your account balance by making an API call to Infura.

```
POST https://mainnet.infura.io/v3/d039103314584a379e33c21fbe89b6cb HTTP/2.0

{
    "id": 2628746552039525,
    "jsonrpc": "2.0",
    "method": "eth_getBalance",
    "params": [
        "0x0208376c899fdaEbA530570c008C4323803AA9E8",
        "latest"
    ]
}
```

... Display the NFT by making an API call to OpenSea.

```
GET https://api.opensea.io/api/v1/assets?
owner=0x0208376c899fdaEbA530570c008C4323803AA9E8&offset=0&limit=50 HTTP/2.0
```

Again, like my dApp, these responses aren't somehow authenticated. It hasn't even been signed to prove that they are lying later. It reuses the same connection, TLS session ticket, etc. for all accounts in the wallet, so if you manage multiple accounts in the wallet and separate identities, these companies will link them. You will know what you are doing.

MetaMask doesn't really do much work, it's just a view of the data provided by these centralized APIs. This is not a MetaMask-specific issue. What other options do you have? Rainbow etc. are made in exactly the same way. (Interestingly, Rainbow has its own data for the social features built into the wallet (social graph, showcase, etc.) and has opted to build everything on top of Firebase rather than the blockchain. increase).

These things mean that if your NFT is removed from OpenSea, it will disappear from your wallet as well. It's functionally irrelevant that my NFT remains somewhere on the blockchain. Because the wallet (and more and more everything else in the crypto ecosystem) *is only using*

the OpenSea API to display NFTs , 304 for NFT queries owned by my address Because I started returning No Content!

Reproduce this world

Given the history of why web1 became web2, what makes me wonder about web3 is that technologies like Ethereum are made with many traps implicitly, just like web1. .. To make these technologies available, this area is ... being centralized around the platform. again. People who run servers for you and iterate over new features. Infura, OpenSea, Coinbase, Etherscan and more.

Similarly, the evolution of the Web3 protocol is slow. When creating the First Derivative, it would have been great if we could price the derivative as a percentage of the underlying asset value. That data isn't on the chain, but it's in the API provided by OpenSea. NFT royalties are attracting attention as being beneficial to creators, but ERC-721 does not specify royalties and it is too late to change them, so OpenSea has its own royalties that exist in the Web2 space. There is a setting method of. Rapid iteration on a centralized platform has already surpassed distributed protocols and is concentrating on the platform.

Given this dynamic, I don't think it's surprising that the Crypto Wallet NFT view (view / screen) has already come to the point of being an OpenSea NFT view (view / screen). It is. We shouldn't be surprised that OpenSea isn't a pure, replaceable "view." Because OpenSea has been busy improving and iterating the platform beyond what is possible within the framework of standards that are inherently impossible / difficult to change (blockchain).

I think this is very similar to the email situation. I can run my own mail server, but it doesn't make sense for privacy, resistance to censorship, or control (by myself). ——Because all the emails I send and receive will have (centralized) Gmail anyway. Once the decentralized ecosystem is platform-centric for convenience, it's the worst thing for both: centralized yet decentralized enough to stop (slowly) time. .. I can create my own NFT marketplace, but if OpenSea mediates all NFT views of the wallet (and all other apps in the ecosystem) people use, it brings additional control. not.

This is not a complaint about OpenSea or a blame for what they have built. On the contrary, they are trying to make something that works. We should expect such platform integration to occur, and given that it is unavoidable, if things are such a mechanism, give us what we want. I think we should design a system that will give us. But my feeling and concern is that the web3 community expects results that are different from what we're already seeing.

It's just getting started

When Web3 officials discuss this, the most common phrase is "it's just getting started and it's in its infancy." Objectively, it's been 10 years or more, so in a sense, it's "still early" that cryptocurrencies have failed to reach a scale beyond relatively immature engineering. Will make it possible.

But even if this is just the beginning (it's quite possible!), I'm not sure if it should be considered as comfort. Rather, I think the opposite may be true. You should pay attention from the very beginning. These technologies tend to quickly centralize through the platform for realization, which has no negative impact on the speed of the ecosystem, and most participants are unaware or unaware of this. To. This is because decentralization itself does not really have immediate practical and imminent importance to the majority of people downstream, because there is something about the amount of decentralization that people want. It may suggest that it is the minimum required, and if not consciously explained, over time, these forces will move us further away, rather than closer to the ideal result. Maybe.

But the gold rush cannot be stopped

Come to think of it, OpenSea will actually be much better at your feet if all the elements of Web3 are gone. It should be faster, cheaper for everyone, and easier to use. For example, to accept my NFT bid, I would have had to pay $ 80 to over $ 150 for Ethereum transaction fees alone. There is an artificial lower limit for all bids, as you will lose money by accepting bids at a lower price than the gas bill. Credit card payment fees usually seem coerced, but they look cheaper than that. OpenSea can also publish a simple transparency log for anyone who needs public records of transactions, offers, bids, etc. to validate their accounting.

But if they had created a platform for buying and selling images that didn't claim to be crypto, I think it wouldn't be widespread. Much of what is needed for crypto to work is no longer decentralized, so the reason it wouldn't have been popular isn't because it's not decentralized. The reason it wouldn't have been popular is because (the current popular pattern) is the *gold rush* . Those who make money from cryptocurrency speculation want to use it in a way that supports their investment and gets more returns, which defines the market setting of wealth transfer. It is.

The end people who trade NFTs are basically not interested in decentralized trust models and payment mechanisms, but they are interested in where the money is. So money attracts people to OpenSea, which improves the user experience by building a platform in the Web2 space

that iteratively improves on the basis of the Web3 protocol, and ultimately NFTs through OpenSea itself rather than its own contracts. And ultimately, Coinbase will open the door to providing access to the validated NFT market through your debit card on its own platform. This opens the way for Coinbase to manage the tokens themselves, eliminate transaction fees, and eliminate any interaction with smart contracts through Coinbase's dark pool. Eventually, all the web3 parts will be gone and you will have a site for buying and selling JPEGs with your debit card. This project cannot start as a web2 platform because of market dynamics, but it is likely that it will eventually end up with the same market dynamics and the fundamental power of centralization.

For NFT artists, these advances are gratifying because they mean more speculation and investment in their art. But if the point of web3 is to avoid web2 traps, we need to be concerned that these new protocols, which should offer a different future, are already heading naturally in this direction.

I think this market principle will probably continue. In my opinion, the question of how long it will last is whether the huge amount of cryptocurrency that has accumulated is ultimately in the engine or in the leaked bucket. If the money flowing through the NFT eventually returns to the crypto space, it could continue to accelerate forever (whether it's just web2x2 or not). If it leaks (outside the crypto space), this will be transient. Personally, I think at this point enough money has been created and there are enough faucets to sustain it, which will not be just transient. If so, it seems worth urgently thinking about how to prevent web3 from becoming web2x2 (web2 but with no more privacy).

Creativity alone may not be enough

I'm just getting into the world of web3, but looking through the lenses of these small projects, it's easy to see why so many people find the web3 ecosystem so nice. I don't think web3 is on track to free us from a centralized platform, I don't think it will radically change our relationship with technology, and the privacy story is for the Internet. I think it's already below average (which is a pretty low hurdle!), But I also understand why nerds like me are so excited to build in Web3. At least at the geek level, it's new. And it creates a space for creativity / quest and is somewhat reminiscent of the early Internet era. Ironically, part of that creativity comes from the constraints that make Web3 so inconvenient. I hope the creativity and quest we see will have positive consequences, but I'm not sure if the same dynamics as the Internet are enough to prevent them from re-evolving.

If we want to change our relationship with technology, we need to do so intentionally. My basic idea is roughly as follows.

1. **You should accept the premise that people will not run their own servers by designing a system that can distribute trust without distributing the infrastructure.** This means an architecture that uses cryptography (rather than infrastructure) to distribute trust, anticipating and accepting the inevitable relatively centralized client / server relationships. One of the things that surprised me about web3 is that it looks like cryptography is rarely used, even though it's built on top of "crypts"!
2. **We should strive to reduce the burden of building software.** At the moment, software projects require a huge amount of human effort. Even relatively simple apps require many people to sit in front of a computer for eight hours each day. This wasn't always the case, and there were times when the 50 people involved in a software project weren't considered a "small team." As long as the software requires such intensive energy and highly specialized human concentration, it tends to serve the benefit of the people sitting in the room every day, rather than the broad goals we think of. I think there is. To change our relationship with technology, I think we probably need to make software easier to write, but I've seen the opposite happen so far. Unfortunately, I think distributed systems tend to exacerbate this trend by making things more complicated and difficult.

gm!

(End of translation)

Although the article was skeptical of Web3, the one stone thrown by Moxie (as far as I read tweets and various blogs around Web3) is very constructive and quite favorable in the industry. Seems to be accepted by. Instead of arguing about the pros and cons, I thought that a person like him who can think while actually moving his hands is really cool.

↓ I think it will be useful to read the reaction of this celebrity.

Reaction of Ethereum founder Vitalik Buterin

Reaction of MetaMask founder Dan Finlay

reaction of a16z (VC) Chris Dixon

(Promotion)

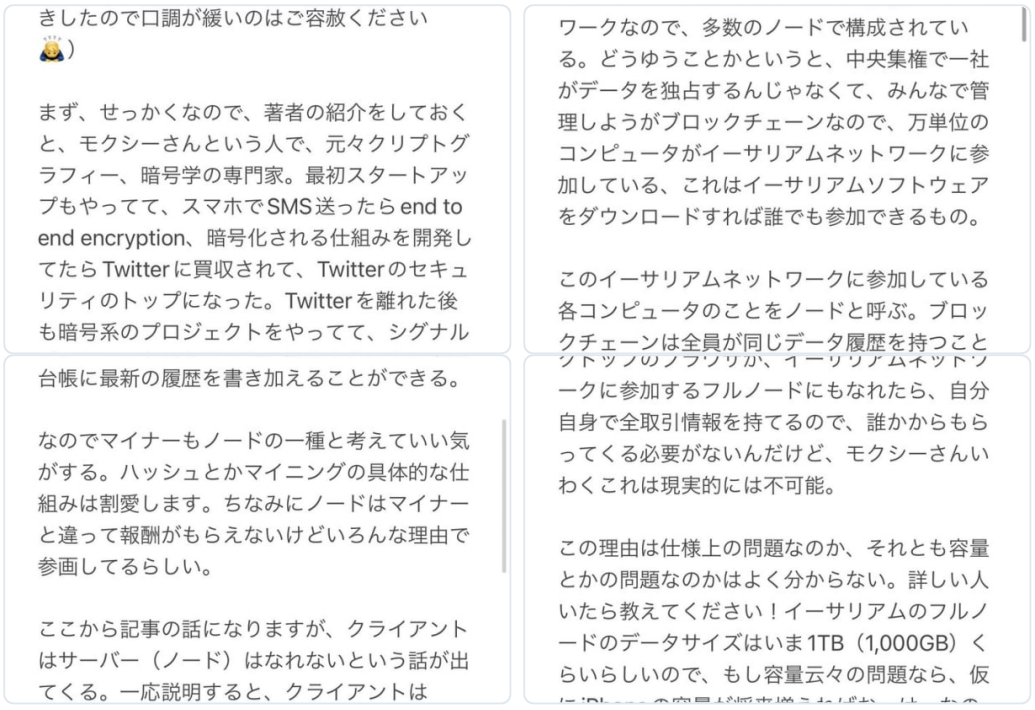
I hope this e-mail newsletter and my Twitter will be able to share my research on Web3, so if you are interested, please do.

unicornlaunching@gmail.com ✓✓

(↓ Addendum: I wrote it so that even beginners of blockchain can understand it.

Stones
@ishicorodayo

As for the above article, I got a lot of individual opinions such as "I read it, but it was difficult because it was a lot of technical terms!", So what is it delicious about blockchain? I tried to chew it so that even those who say that can read it! 🙇



April 10th 2022

1 Retweet **27** Likes

unicornlaunching@gmail.com ✓✓