The fundamental values of the crypto community

When it comes to good conversations about crypto, it's getting harder and harder to have conversation not only about the future, but the history of crypto as well. Who knows where Satoshi is, Vitalik is always with so many people and other founders are really hard to get with. Except Emin Gun Sirer, whom with I had a lot of conversation of the past couple years.
But one of the founders who I never thought I would meet is Zooko Wilcox, founder of ZCash.

Back in 2017, when I was a few months in my crypto journey, the Zcash one was the first whitepaper I thoroughly studied before making the decision to buy ZEC. It was a few weeks before JPMorgan announced he'd use that same zk tech in some of their projects - and it was also the time when institutions tech adoption news made the coins pump, quite old times now if you ask me.

I had the chance to sit down with Zooko after a panel at the Shielding Summit in Brussels, and I just wanted to say hi and listen what he had to say about the future of Zcash, but the conversation became much more.

I can't tell everything, and most things are quite chaothic, so I'll need to still think about it for a while. But of all the things we talked about - his work on the Electric Coin Company, cryptography and lately wallets - I grasped that there really are different generations of blockchains.

First gen: the monetary freedom

That's because the way Zooko talks, and the things he did, those are part of the fundamental values of the *bitcoin dogma*, if I can call it like this. The bitcoin dogma is the need for a truly distributed, global and permissionless payment system that puts money in the hands of anyone, in any country.

Bitcoin was born to give a 'bank account' to the unbanked, and to free from the chains (no pun intended) of the traditional banking system that controls and decides who owns what. That is still the ethos of bitcoin, and it was transferred as is to zcash and a number of other, let's say, first generation coins like Litecoin, Dogecoin, Namecoin (who remembers that?) and many more, including Zcash. I'd say that this ethos was predominant until 2016, when Ethereum broke out.

Second gen: the libertarian community

When Ethereum launched in 2015, it launched with a very specific narrative, and it was not monetary freedom. That narrative was kind of implicit, but the explicit one was *The World Computer*. Technically speaking, Ethereum expanded some bytes reserved to arbitrary execution (I think it was an 80 bytes space) to enable Turing-complete computation on the blockchain, on which only coin transfers were possible before.
Associated to this narrative was another, very futuristic, related to Decentralized Autonomous Organizations. I remember reading on the Ethereum website, back in 2017, that on the blockchain you could build DAOs, a new way of organizing consensus and interests and recording the value it produces, or something like that.
I thought that this new 'DAO' thing would take *decades* to be built effectively, and I still think like that: what we're seeing right now are experiments, of which 90% end up bad.
DAOs *could* be businesses, but not only: the whole Ethereum brand, even look & feel, is very close to libertarianism and queer values.
So Ethereum not only expanded on technical restrictions from bitcoin, but went beyond and expanded to apply and aim for freedom at every level of society.

So when people, on Crypto Twitter, say that they're *Ethereum-aligned*, they

So when people, on Crypto Twitter, say that they're Ethereum-aligned, they could mean that they inherit security from Ethereum (L2s, L3s, restaking protocols, whatever), but I bet the original meaning of it is that you are aligned to the high ideals of complete freedom, total inclusiveness and 'auto-enforced democracy'.

I honestly wasn't getting all this until I met the OP Labs team IRL at EthCC: for who doesn't know, OP Labs came from the Plasma Group, the first group working on Ethereum scaling back in 2018/2019.

The OP Labs team really doesn't want to talk on private chats - they do as much as possible in the open, and they put *a lot* of effort on it.

They don't want to give advantage to any one over any one else. At first, it was really hard to digest, but now I get it. And they're driven by the Ether's Phoenix vision (impact = profit) which really aligns with the Ethereum vision.

I connected the dots and realized that, for example, the Ethereum Foundation funds open source projects much mure than closed source ones. They incentivize openness.

(This is one other reason why I don't like the way Etherscan works: they have a closed source product, take a lot of money and rarely give something back to the community and industry as a whole, apart from the direct impact of their product which they earn a lot of money from. Etherscan is not Ethereum-aligned, and I don't know when someone will notice this.

We (Routescan) also have a closed source product, but we contribute to a ton of open source initiatives, make donations and support any way we can, without discrimination as much as we can)

That's why Ethereum and its ecosystem (L2s, mostly) are surrounded by social and political projects. We donated to the Regen Village at EthCC, an initiative supported by Regen, a tokenized community involved in regenerative projects. And I met PhDs, students and all kinds of people interested in making contributions ranging from governance to social impact and economics - to contribute to *The World Computer*. I was impressed by the vibes.

Third gen: the new value system

For about a year, I've been presenting some slides in my talks about *A multichain seamless future.* In one of the slides, I wrote this:

> *"In order to use blockchain technology as a ledger for any type of value transfer and information recording, it is necessary to build high throughput systems."*

The third generation of blockchains were born with this exact problem in mind. Ethereum was the place where you would pay 200$ in fees to buy a 150$ cryptokitty in late 2017, and entrepreneurs spun up new companies with blockchains from scratch to solve this problem).

That's why we have Avalanche and Cosmos (horizontal scaling and high throughput custom VMs), Solana and NEAR (super high throughput computation) and the likes. These blockchain platforms, and the teams behind it, became particularly sensitive to banks, institutions and large companies that wanted to initiate a 'blockchain transformation' and that could never use bitcoin or Ethereum to process their data.

They're pragmatic, driven more by metrics than values. They focus heavily on enterprise business development and incentivize projects that can make the goal easier to achieve. And that's okay, because that's how blockchain system will power every value transfer throughout the world.

So that's also why we have segmented security guarantees, higher throughputs and a decentralization achieved on cloud services in data centers instead of on personal computers.

But that's also okay. True mainstream adoption won't come if we fixate on our obsessions, but if we listen to everyone. And compromises will always be there.

Three-way future

Three-way future

Each of these blockchain generations have a specific goal, and even though it doesn't seem like it, they all contribute to make *onchain* more prominent, either visibly (1st and 2nd gen) or invisibly (3rd gen).
And we're all gonna profit from that, both in cash (less relevant) and in a better society.

Date: 2024-07-10
Words: 1306
Time to read: 6 mins

Jaack © 2022-2025

Made with Montaigne and bigmission 🇺🇦