

Introduction

In 2022, the crypto community is getting wilder than ever, more blockchain-based networks are starting to be released with a purpose - to make blockchain networks scale and cheap-to-use. And today, I'm here to tell you how that is not actually true and often comes at a cost.

This article is expected to have my negative comments, so be calm and feel free to have your own opinion. It will also not be a “your chain” versus “some chain” type of article, so chill.

Problems with modern networks

Centralized, permissioned, not trustless

The one true reason why we all need blockchain networks is that we want to achieve decentralization, without decentralization, even if your network has millions of tps, it is nothing. If you are just going for a centralized network, might as well stick with traditional centralized systems, which are faster, lighter, cheaper, there is absolutely no reason to use blockchain technology if the network is centralized.

Another important factor is “permission”, everyone should have the freedom, a voice in the network. Also, missing this one might also bring centralization but just with extra steps.

Moreover, “trust” is also a really dangerous thing to mess with because when tangling with trust, you might introduce centralization, or it will be permissioned, or it will be insecure, etc. Trust is weak too, relying on trust is fragile, when trust breaks, the whole network will break.

Proof of stake

The first thing that comes in mind when talking about these networks is that it has proof of stake or its variations as a consensus mechanism to replace proof of work, making transaction speed higher and reducing electrical energy consumed. But the thing is, *they are badly implemented*.

But first, let's talk about the “true” proof of stake consensus mechanism. It is basically a system where one stakes their tokens to become a validator, gaining chances to be the block producer. If a validator cheats or goes offline, that individual should be punished by getting portions of his staked tokens lost. But the system is much harder to build than it sounds, so people set off with delegated proof of stake or its variations.

DPoS is basically a consensus model where rather than staking to get chances to be the next block producer, you are delegating others to create blocks, sounds very trust-involved doesn't it? Delegators are now trusting validators that they

delegate, users are now trusting delegators to delegate the right validator, this shouldn't be called proof of stake at all, but more of "proof of other's stake". The system also draws paths to centralization: One validator can basically convince, bribe, or have a solid relationship with delegators and then everything is centralized towards him. To make the matter worse, there is often no slashing system, so a validator can just goof off and he has nothing/nearly nothing to lose, making the network extremely insecure and hard to recover from attacks.

DPOS is one thing, token distribution is another element that really bothers me. Many networks out there give large amounts of their supply to whales, VCs, or to the foundation itself. This, again, makes everything mega-centralized, because not only whales holding too many tokens is bad, but the attacking threshold of many networks is just about ~33%.

Multichain

Multichain is a system where apps have their own smaller chains, and these smaller chains can interact with others easily. This brings scalability and interoperability, but yet again, it comes with a cost. It is often harder to talk about multichain networks because it can be dependent on how that network implements its appchains system, but usually, multichain networks are implemented in a very trust-involved and permissioned way. Appchains usually need to go through a crowdfunding, voting, or whitelisting process to actually be in the main network, thus limiting developers, as they can't just create dapps however they like, but they need to be accepted before being deployed into the main chain. It also favors the rich developers, big teams, and big corporations, as systems like crowdfunding don't give the regular class a chance, but rather the riches, from that, it is somewhat centralized too since apps are all from the rich.

But the sad thing here is that you need this picking system because otherwise the network will break if one child network break :/

Running full nodes

To actually "be in a network", you need to run a full node, but most networks out there require a very hefty node requirement. For example, Solana requires you a CPU with 16 cores, 32 threads, 256 GB of ram and 1 TB of storage, not everyone can afford that. Another problem is staking requirement, if the staking requirement is too high, no one but the riches can participate in block production. For instance, BSC has a ridiculous staking requirement of 10000 BNB (around 3 to 4 million dollars at the time of writing).

If running a full node is expensive, then again, the riches are the ones who take control of the network.

Not enough nodes

This is not that big of a problem (since it can be resolved in a near future) but definitely is still a factor worth saying, because new networks are too young, there haven't been much people running nodes for them, or it is just because the full node requirement is too ridiculous, introducing centralization once again.

Do they actually care?

Depends, many people are serious about the tech, and are aware of the problems and bottlenecks blockchain networks have, but it seems that many just want to create quick cash-grab projects, or just take VCs' money while they are not actually aware of the technology or what it actually solves. (Many projects seem to not understand what they are doing, take Nano for example, they removed gas fees and then got attacked immediately, proving that they hardly know anything).

Good networks

This is my opinion on networks that can be "okay" in the time of writing.

First generation blockchains

Decentralized payment system like Monero or Zcash are actually *pretty good*, they are decentralized, private, and serves what they are meant to do. However, they can not do anything further than send money.

Algorand

Algorand is a *kind of decent* network, as delegations are random, however, the UX is not up to par in my opinion and no one actually develops apps for it, which is probably the main reason why no one actually uses it today. But tech-wise, it is much better than a lot of networks.

Ethereum

Ethereum is decent, it is battle-tested, there are a ton of nodes running already, you can find all sorts of dapp on it.

The main problem currently is that it is slow and expensive. It is slow because PoW is slow (or expected to be slow to bring out the best security), and it is expensive because Ethereum is the most used smart contract platform out there, and the demand for block space sky-rocketed in 2021 with the rise of NFTs and crypto in general.

The performance issue can be solved using the new proof of stake system - Casper that Ethereum is planning to switch to, and the nice thing here is that it will be a true proof of stake system, not a DPoS spin-off. The token distribution

problem and the “gatekeeping problem” of PoS are no longer there also, since tokens are distributed nicely through 7 years of PoW mining, now no one holds that much token distribution shares to actually do anything.

The expensive gas can be lowered when sharding is brought to the network, which people are uncertain of the release date (rumors about Ethereum 2.0 is not real if you are wondering). But if it is released, then Ethereum would be the go-to blockchain network, since it will have fast performance, reliable security, decent decentralization and cheap gas fees.

Of course, there are still many problems to consider even after these 2 big updates are released, but it is definitely way better than most networks out there.

Layer 2 networks

A rising approach is to use layer 2 networks (rollups specifically, and you should probably only use Ethereum l2s), they are independent networks but post data to the main chain. It is secure, fast, and cheap at the same time.

Conclusion

I firmly believe that blockchain and decentralized networks still have a long road to go, not just staying like how current networks do.

I hope you enjoyed the article, once again, no hate or love on any networks, I just want to say the truth, do correct me if I'm wrong, and have your own perspective.