By: Nguyen Phu Minh Written in April 2022

Introduction

Blockchain is probably one of the most mentioned technology in two recent decades, it first leaded way to achieve a decentralized payment system/decentralized currency, now, it is moving forward to bringing a new decentralized application platform, or even bigger - a new, decentralized internet.

However, while I believe that a decentralized payment system can be achievable, I can guarantee that blockchain-powered networks are not ready at all to accomplish such a mission of bringing a new internet or something like that, and that we should think of better, more impressive technologies rather than just being comfortable with what we have already had. I believe this article will receive mixed opinions, and probably a lot of hate, but be open-minded because I can be right and wrong at the same time.

(Note: With that said, in this article, I will just focus on smart contract supported networks, not payment systems like Bitcoin, Litecoin, Monero, etc).

Performance and scalability

The first problem in blockchain networks that pretty much everybody in the field know is performance and scalability.

With old, existing, yet widely used networks like Ethereum, it is expected to only have below 50 tps, which is really, really slow, with new, modern networks like Solana, Polkadot, Fantom or rollup networks like Arbitrum, you would expect to see 1000-10000 tps, that's still nothing compared to centralized systems where 1000000 tps can be achieved without a hassle. A thing that's commonly seen with blockchain networks is that all apps (contracts) are run on a single network. That's absolutely awful because with centralized systems, which can roll out 1-10 million tps, and only has a few apps running on those servers, it is still slow sometimes. Here, you have a 10-10000 tps system that has thousands of contracts (can be more in the future) running, with thousands of people using those contracts. It is like carrying an elephant while riding a bike.

And the problem is not easy to solve, since it is well-expected that peer-to-peer networks would be slow, due to consensus and many rounds of communication between nodes, or you will be met with the blockchain trilemma of scalability, security, and decentralization.

UX

It would be safe to say that the UX with blockchain dapps is not as good compared to traditional applications.

Gas fee

The first bottleneck is definitely gas fee, you would never want to pay a dollar or even a cent to like your girlfriend's photos right? Yeah, me too. And if you do the math, you will see that even compared to paid system, you would normally spend a couple thousand times more money.

I think if gas fees still exist, blockchain will hardly ever be adopted in normal use cases, but rather still in the DeFi world.

This problem is absolutely hard to fix though, probably way harder than the scalability problem, because gas fee is there to prevent spamming attacks and incentivizes nodes to keep the blockchain's data.

Payment system involvement

Another thing that seems extremely terrifying is the act of opening a wallet app every time you want to do something data-related, I mean, again, if you are there for DeFi, then it is okay, but what's not okay is the fact that every time you just want to save your game or post an article, the app is frozen, the wallet just popped out, it's really annoying.

Slow

As mentioned earlier in the Performance and scalability section, blockchain networks are slow.

You wouldn't want to wait from 30 seconds to a few minutes to do anything, would you?

Decentralized, trustless, permissionless? Not really

Now, the whole reasons why we use blockchain-based networks are decentralization, trustlessness, and permissionlessness, but they actually aren't.

Take PoW networks, those that are considered top-notch in these elements, actually all suffered from mining pools. Miners are *trusting* mining pools, and they are also *centralized to* those pools, and individual nodes can never win against pools with hundreds of nodes joining in. Furthermore, to have *somewhat of a voice*, you must afford extremely expensive mining hardware, not really "decentralization" nor "permissionless". These networks are more like "decentralized, permissionless and trustless across different parties" rather than "across anyone".

In modern networks' case, it is much worse. There are not many nodes, many networks' full node requirements are terrible and centralized, like BSC where the staking requirement is 10000 BNB (about 4 million dollars in the time of writing), or Solana where the hardware needed is too high, or Internet Computer where you even need to submit a ticket to join in. Tokens are mostly distributed terribly (this matters a lot because they mostly use a PoS system), and they all use DPoS or its variants which are trust-involved by design and can lead to centralization. Other trust-involved networks are multichain networks, which is not okay.

A somewhat "okay" solution to this would probably be the new PoS Ethereum, since it is not trust-involved like DPoS, the staking requirement is capped so it should be harder to form pools, tokens are distributed evenly after 7 years of PoW mining so problems with PoS shouldn't be there anymore, there are already >300k nodes running, the full node requirements are not that ridiculous. But still, it still has some drawbacks, but at least it should be better.

How we use blockchain ourselves

Blockchains can be centralized in how we use them ourselves, most people in the field just use wallets in their default setting, which should target Infura or some node providers, and that is centralized, to be decentralized you must run your own node.

Privacy

This is kind of an arguable topic, but here are my reasons why blockchain is bad for privacy.

You see, since data is viewable by everyone in the network, so to be private, you would need to encrypt that data. However, what if the encryption algorithm is broken in the future? All data will be public to anyone and you can't do anything about it since blockchains are immutable, you just can't change old data. Centralized systems are worse at first since they can be exploitable, but they can delete the data or change it later on, making data private again, which blockchain networks can not do.

Decentralized networks without blockchain

There are cases where we don't need blockchains at all, things like decentralized file storing have already existed since a long time ago, through torrenting and ipfs, and they don't cost you gas fees. You should only use blockchain when a thing must be publicly agreed by everyone, like finance or automated rules perhaps.

Conclusion

I have just mentioned all the drawbacks that I think are the most important in blockchain networks. I definitely saw blockchain's accomplishments, but I also hope that blockchain networks and decentralized networks in general can be pushed further in the future.