On the Scalability of Blockchains

Nick Tomaino · Follow
Published in The Control
5 min read · Mar 23, 2018

Bitcoin and Ethereum, the most widely used blockchains, cannot currently support mainstream transaction usage. They are both supporting mainstream investment usage today, but if blockchains ever become useful for anything beyond investment, solutions that allow them to maintain performance as throughput increases must exist. $300B+ worth of speculative value is a big number for a category of technologies that can't yet support transaction usage at any scale, but the good news is **there are various approaches attempting to allow blockchains to support mainstream transactional usage.**

> Use cases are fun to talk about, but use cases beyond investment can't work well unless scalability is solved

What is the problem?

Creating a centralized network that supports transaction scalability is not difficult from a technical perspective. Paypal, Visa, and Mastercard and many others have done that before. What is difficult is creating a blockchain system that offers users the optimal combination of scalability, decentralization, and security. Vitalik coined the scalability trilemma here, which states that blockchain systems fundamentally can only have two out of the three following properties:

- **Decentralization:** defined as the system being able to run in a scenario where each participant only has access to O(c) resources, ie. a regular laptop or small VPS
- **Scalability:** defined as being able to process O(n) > O(c) transactions
- **Security:** defined as being secure against attackers with up to O(n) resources

Bitcoin and Ethereum were built first and foremost to be decentralized and secure, but sacrificed scalability (Bitcoin supports ~3 transactions per second and Ethereum supports ~12 transactions per second). That has proven to be an effective way to bootstrap a network to date, but also has limitations as the network grows (which we are now starting to see).

There are a variety of newer blockchains sacrificing decentralization or security for scalability and trying to bootstrap a network that way. It remains to be seen how effective that approach will be. But to date, no one has found the combination of decentralization, scalability, and security necessary to create a fully functioning cryptocurrency network at scale.

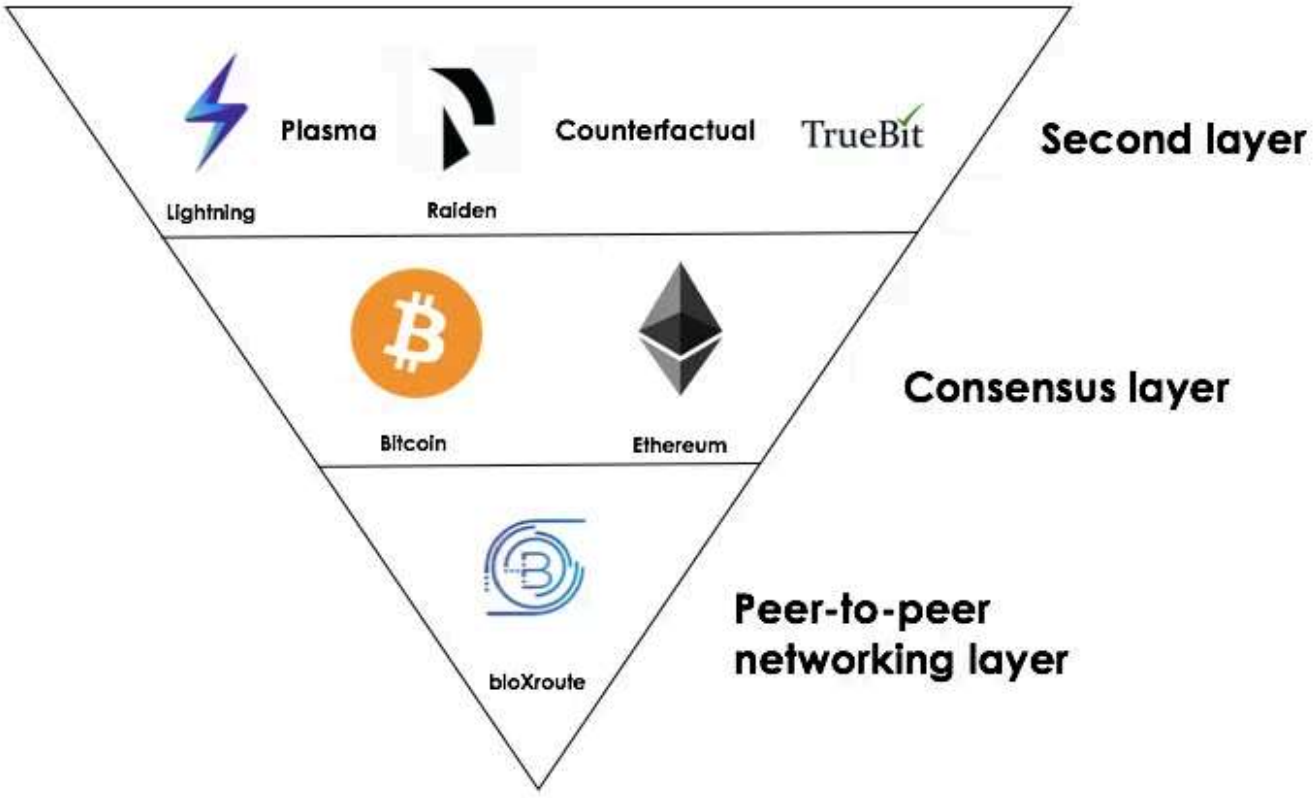
How to create a network that generates transaction demand at scale and is also capable of supporting that demand?

There are several ways that cryptocurrency network scalability could end up playing out:

1.) The communities with the largest network effects and developer mindshare (Bitcoin and Ethereum) will solve scalability

The most widely known projects that are seeking to increase the scalability of Bitcoin and Ethereum are Lightning Network (Bitcoin), Plasma (Ethereum), and Casper (Ethereum). Lightning and Plasma are both Layer 2 solutions that allow transactions to occur off-chain and then ultimately settle on-chain, while Casper seeks to implement sharding to increase on-chain scalability at the consensus layer.

There are other projects that are less well-known building at the second layer of Ethereum (Truebit, Raiden, and Counterfactual) and one that is building at the peer-to-peer networking layer for all blockchains (bloXroute, announced this week). These efforts are early but also promising.



Core scalability solutions for Bitcoin and Ethereum

The solutions described above seek to achieve scalability at various layers of the stack for the largest networks with the most mindshare and the most passionate communities. The BTC and ETH communities have a strong belief in the cryptocurrencies native to their respective networks and the strongest inherent demand to scale now.

They also have the strongest technical minds working on these problems. In my view, the most likely path forward is that a variety of solutions end up enabling Ethereum and Bitcoin to scale on-chain and off-chain and Bitcoin and Ethereum end up being the core networks the masses converge on.

2.) New networks emerge that are fundamentally built to be scalable and users gravitate to them

Scalability-first blockchains. Several new scalability-first blokchains have emerged to serve users and developers as more scalable payment networks (i.e. Bitcoin Cash, Algorand) and dApp platforms (i.e. Cosmos, Dfinity, EOS, etc). There's likely a few quality projects I'm missing, but for the most part there are a lot of low quality projects making big claims about scalability and raising massive amounts of money from unsophisticated investors on these claims. I'm skeptical of most of these, but there are some diamonds in the rough led by teams that have deep historical context

and knowledge and have made compromises on security or decentralization, which could pay off.

Scalability-first blockchains

While these scalability-first projects generally lack the passionate, grassroots communities that have the strong inherent demand to use these platforms for transactions today, they have constructed blockchains that are fundamentally more scalable than Bitcoin and Ethereum now. If solutions don't emerge to help scale Bitcoin and Ethereum before the demand for transactions increases significantly, it's quite possible that users shift to these next-generation blockchains.

New consensus constructs. There's another category of scalability-first projects that is even earlier and less proven than the projects listed above that seek to achieve consensus via mechanisms that lie outside the construct of a blockchain (gossip protocols, directed acyclic graphs, etc). Projects like Hashgraph and DAG Labs are championing these ideas. I think they are worthwhile initiatives but early and highly speculative.

3.) Cryptocurrency networks don't scale

As bullish as I am about the future of blockchains, I do recognize that there is a small probability that they don't scale for transactions, either because the tech is not figured out or users demand just doesn't increase to the scale we hope.

What to expect?

My view is that the network effects and mindshare of Bitcoin and Ethereum, and the caliber of the teams working on scalability solutions for these networks make it

highly likely that solutions on Bitcoin and Ethereum enable widespread transaction usage of the networks.

It's also possible (albeit much less likely) that a critical mass of developers and users will shift to next-generation networks that fundamentally support more throughput (Cosmos, Dfinity, EOS, or something else). If we see demand for transactions increase significantly (i.e. we see a few more Cryptokitties-like apps) before better solutions exist on Bitcoin and Ethreum, that could happen.

It's also possible (albeit even less likely) that cryptocurrency networks don't scale. I'd put that probability at less than 5% because of all the momentum and talent currently focused on solving the problem. But it's not a foregone conclusion that people will want to use cryptocurrency networks for transactions at scale and the right combination of decentralization, security and scalability will be found. The industry has a lot more work to do on both fronts.

Learn more

- Vitalik On Sharding Blockchains: https://github.com/ethereum/wiki/wiki/Sharding-FAQ
- The Bitcoin Lightning Network Whitepaper
- The Plasma Whitepaper
- The bloXroute Whitepaper
- Join the bloXroute subreddit to discuss scalability
- Token Summit SF Panel with Joseph Poon (Plasma), Jason Teutsch (Truebit), and Jae Kwon (Cosmos)