Power and Wealth in Cryptoeconomies

Ryan Watkins

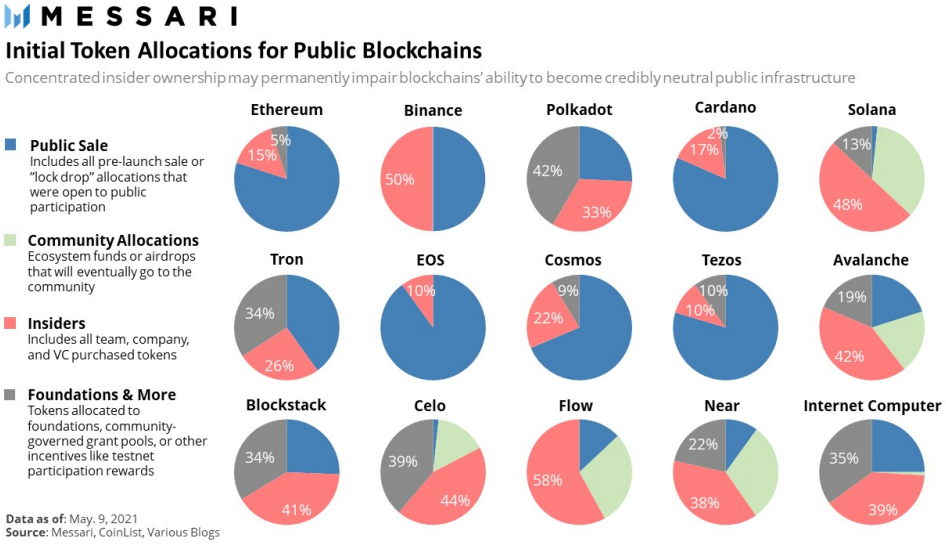
May 17, 2021

Imagine you're designing a new economic system from scratch. You're deciding everything from resource allocation to property rights to how this entire system will ultimately be governed and controlled. How would you design it?

In truth, there's no right answer. This is a question that philosophers, politicians, and economists have struggled with for centuries as they've designed institutions. In any case these architects attempt to satisfy society's shared ideals when doing so, such as freedom, opportunity, fairness, and security.

Whether they know it or not, blockchain architects face similar questions as they design blockchains. Like firms, markets, and governments, blockchains are also an institutional technology. They not only regulate the supply and distribution of scarce digital assets, they also provide a governance system for a wide variety of social, political, and economic activities. Ultimately blockchains may grow to become the foundation of the global economy and usher in a new economic system. But before they fulfill this ambition they must first answer the most basic questions about power and wealth distribution.

With this in mind, how have blockchain architects done so far? Well, the results are mixed.



An Erosion of Values?

The original philosophy underpinning token sales centered around the idea of communities funding open source projects and receiving ownership in return. Many of the older smart contract platforms took this philosophy to heart, allocating the majority of their token supplies to their communities in this fashion. Projects such as Ethereum, Cosmos, Tezos, and

EOS for example allocated more than 70% of their token supplies to their communities for this purpose.

However, something seems to have changed in the years since then and projects skewing newer have had less generous supply distributions. Whether it be the increased presence of venture capitalists who treat blockchains like companies and seek larger ownership allocations, increased regulation, or an erosion of the early egalitarian ideals, many newer entrants to the smart contract arena such as Binance, Solana, Flow, and Avalanche have significantly higher insider allocations. In these cases insiders own more than 40% of each projects' token supply - even more extreme when you also consider foundation allocations.

Power and Wealth in Cryptoeconomies

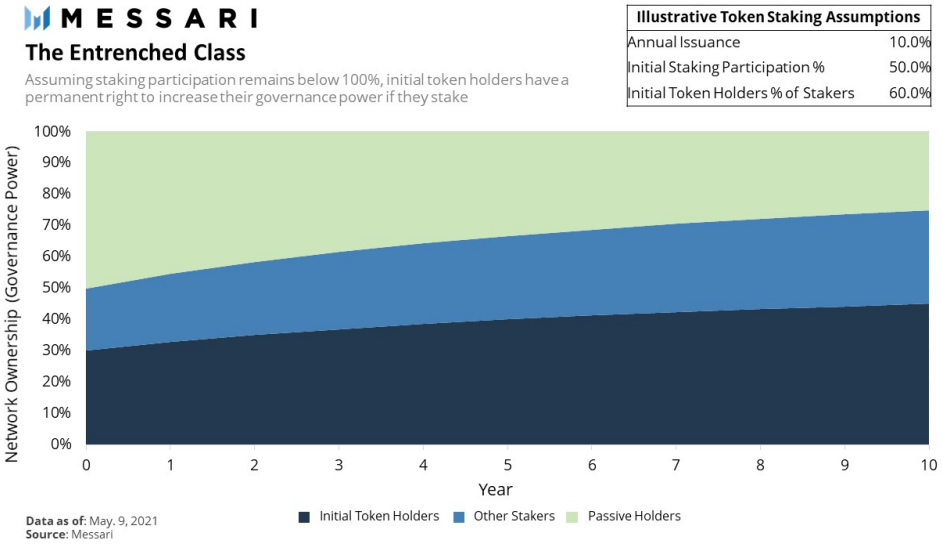
In an ideal world, blockchain architects wouldn't need to decide initial token allocations. They could instead just start the supply at zero and issue new tokens equitably on an ongoing basis to those who contribute resources to it. This is how Bitcoin started, with every single coin that's ever been issued having been distributed to miners for their valuable role in securing the Bitcoin blockchain.

However, such fair launches may no longer be possible with the amount of attention this asset class commands and the profit expectations people have for new projects. A Bitcoin-like launch today would attract tens if not hundreds of millions of dollars in capital seeking to get in early on a new project, eliminating the ability of early contributors to accrue upside in the project and be motivated to continue contributing to it.

As a result many projects have elected to mint some, if not all, of their token supply at genesis, in order to set aside a portion of the supply for core contributors as well as early backers in the project. This is how Ethereum started when it pre-mined its supply and launched a public sale for early supporters to fund the project.

This launch model has important consequences when considering consensus algorithms. Projects that use Proof of Work (PoW) distribute new coins more widely than projects that use Proof of Stake (PoS). Miners in PoW require both significant upfront and ongoing investment in their mining operations to stay competitive. This competition naturally compresses margins over time and causes many miners to be forced sellers over time to stay profitable. As a result most new coins that are mined end up being distributed to the market, rather than accruing to the balance sheets of miners.

PoS functions differently. In PoS systems there is little on-going investment needed to capture new issuance. Once a staker has acquired their coins and staked it in a PoS system, they have a proportional right to all future issuance of a network. This locks in their percentage ownership of the network into perpetuity and eliminates the distributive effects of the new issuance process seen in PoW.



This phenomena is critical to how power and wealth accrues over time in cryptoeconomies when you consider that most tokens in PoS systems not only have a claim on new issuance, but also network fees and voting power. Projects that start off as PoS allow those initially allocated tokens the ability to permanently lock in their ownership stake in the network, with important consequences for power and wealth distribution into perpetuity.

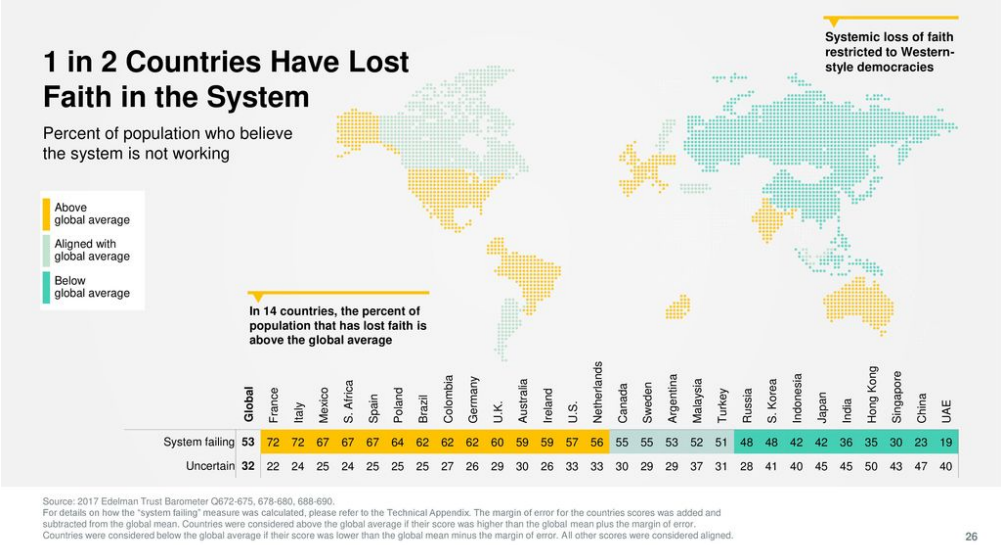
Control in a Decentralized World

"We are working to build permissionless, open tech. Most of the process is open, but the part that remains the most closed and shrouded in secrecy is the early-stage financing… Under the veil of this opacity the same norms and structures that have imbalanced past wealth and power distributions are at play. If we don't openly address what's going on at the inception of cryptonetworks, then we are bound to repeat the same past societal mistakes… Where the capital accrues, so too will the power." - Chris Burniske

In many ways blockchains are more like governments than companies. Like governments, blockchains manage property rights, enforce contracts, and even have social contracts and systems of governance. The promise is that we may be able to use these blockchains in the future as reliable public infrastructure for the global economy.

This vision is compromised when wealth and power becomes concentrated into the hands of a limited number of insiders. Token holders in PoS systems have direct control over blockchains such as which votes get passed, which upgrades get pushed through, what transactions get included, and how much transactions ultimately cost. It's the equivalent of the richest people in the United States having direct and formal control over the United States Government and the Federal Reserve just because they hold the most USD.

When a concentrated group of people ultimately control a blockchain, we lose everything interesting about them. Blockchains that can be shut down, manipulated, compromised, and restricted, are useless. People across the globe have already lost trust in many institutions that govern our lives today. Why would they want to adopt a new system that is even more unfair?



Source: Edelman Trust Barometer 2017

It's Not Just Ideological

The desire for more distributed power and wealth in blockchains is not just an ideological appeal, it is practical. Blockchains that are credibly neutral (do not favor any one group of stakeholders over any other) are more likely to scale globally and as a consequence, attract a larger amount of capital and high value transactions. The more concentrated power and wealth are in a blockchain, the more users need to trust that those in power will behave in their favor, and the less they'll ultimately use it. Projects that concentrate power and wealth from inception, and provide token holders the ability to lock in their ownership through staking, may find it difficult to escape this fate.

But perhaps only time will tell.