The Bitcoin network is several innovations wrapped in a single package. Most famously, its proof-of-work fork choice rule solves the Byzantine generals' problem, which allows a decentralized ledger to be produced. The native currency of the Bitcoin network also has novel properties that allow it to be used as "digital gold." But most importantly, Bitcoin's security budget has blazed a new trail for funding non-rivalrous goods. With minimal planning, millions of people have collaborated to fund the Bitcoin network's security. This post will describe circuit tokens

, an approach that generalizes Bitcoin's model for funding its security budget so it can be applied to fund arbitrary non-rivalrous goods using collection mechanisms like EIP 1559's fee market and miner-extractable value auctions, and using distribution mechanisms like quadratic funding.

Block Rewards as Matching

Transaction fees on the Bitcoin network fund a small fraction of Bitcoin's security budget. Over the past two yearsfees have fluctuated between 1% and 2% of the block rewards, with a spike up to 7% in the middle of 2019. As a result, the Bitcoin network typically funds its security at a multiple of over 50x of what network participants contribute on their own. 50x matching for public goods is unheard of.

Individual donations are typically matched at 2x: for every dollar contributed by the public, a benefactor will contribute a dollar to double the funding. These benefactors are capital constrained, so they typically set a cap on the amount that they'll match. Bitcoin's matching seems to have no cap.

In the realm of government funding, the United States federal government matchesstate spending on Medicaid at 2x to 4.5x, and local capital expenditures on mass transit at around 1.66x with a maximum of 5x. The federal government funds this level of matching using coercive taxation. If the voluntary accomplishments of the Bitcoin network can be generalized in any way, we must find a way to do so as soon as possible to avoid leaving untapped potential on the table.

Bitcoin is an incredibly speculative asset by design: it's "digital gold." Perhaps it isn't possible to replicate the network's feat of 50x matching for its security budget that all participants benefit from. If it can be replicated, however, we need a model that relies on utility instead of speculation. To achieve this, we introduce two constraints: 1) like EIP 1559's fee market, we should maximize network control over contributions instead of designing for direct payments like transaction fees, and 2) the tokens should provide some sort of utility to their owners, like staking or governance. These two alterations are the core of the circuit token model.

Circuit Tokens

Circuit tokens are tokens with an identical token sink and token source: the token supply itself. That is, the network's non-rivalrous goods are funded by releasing tokens, and network fees or donations to the network are paid by depositing tokens back into the token supply. When EIP 1559 is implemented, a significant portion of transaction fees will be burned instead of sent directly to miners, which means ETH will become a circuit token. To fund Ethereum's security budget further, fees from layer 2 systems like miner-extractable value auctions could direct the funds they collect back into the ETH supply.

To broaden the types of goods that can be funded beyond just blockchain security, consider a standalone circuit token that does not operate a blockchain of its own. Instead, token holders vote on what to fund, and network participants voluntarily donate tokens back into the supply. If we assume that such a token could never accrue a monetary premium, the only reasons to hold such a token are the utility from influencing what the network funds, and to potentially increase that utility by increasing the flow of donations through the system and its resulting budget.

To model such a token's ability to match donations, we make two simplifying assumptions. First, we define a constant utility factor, the ratio of the expected maximum token supply to the flow of donated tokens. If governing the system's budget is nearly useless, no one will hold the tokens, and both the equilibrium token supply and the utility factor will approach zero. The more useful it is to govern the system's budget, the more tokens will be held, and the utility factor will rise. The second simplifying assumption is to assume that unlike ETH, the maximum token supply is fixed and released with an exponential decay to ensure that the system has a predictable token supply for every scenario. With these assumptions, the utility factor is defined as follows:

$$\text{utility factor} = \frac{\text{expected max token supply}}{\text{annual donation rate}}$$

The utility factor answers, "How many tokens do people actually hold to be able to govern a given flow of donations?" Regardless of the market price of each token, our hypothesis is that the relationship between the tokens held to govern the system and the flow of donated tokens should be relatively stable.

With a given utility factor, the token system's ability to match donations is a function of the current inflation rate of the system. In this Circuit Tokens Worksheet, you can plug in different utility factors into a token with a fixed supply and inflation that decays exponentially and continuously (not with periodic halvings like Bitcoin actually uses). Since 2479.23 BTC were spent on transaction fees in the last three months of 2019, Bitcoin's utility factor is $\frac{21,000,000}{2479.23 \times 4} = 2117.6$

.This suggests that if the Bitcoin network were to adopt a fee model along the lines of EIP 1559 and provide some sort of utility to BTC holders, it would be able to fund a security budget at unusually high matching multipliers (2x or above) for over 20 more years before approaching an equilibrium where fees provide the entire security budget.

Bitcoin’s matching multipliers over time according to the circuit token model

Experimental Data

To prove that the circuit token model is generally applicable outside of the native tokens of blockchain networks, we need to collect experimental data to demonstrate the matching ability of a token that has no other utility than governing its own funding. Panvala is a DAO that was launched by ConsenSys in August 2019, and now operates as a self-sustaining system. It runs on PAN, the circuit token it uses to issue grants, accept donations to the token supply, and vote on quarterly budgets. Panvala has issued 47 grants to teams across the Ethereum ecosystem.

In the thirteen weeks ending on November 1, 2019, Panvala received 53,221 PAN in donations and released 1,910,663 PAN as grants, for a multiplier of 35.9x. In the thirteen weeks ending on January 31, 2020, Panvala received 182,782.9 PAN in donations and released 2,039,959.8 PAN as grants, for a multiplier of 11.2x. These data points allow us to estimate Panvala’s utility factor, which yields projections of matching multipliers into the future. Using the second data point gives us a utility factor of $\frac{100,000,000}{182,782.9 \times 4} = 136.8$

. This is lower than Bitcoin’s value, but still gives us over a decade of matching above 2x with no central benefactor and no cap on the value of donations that will be matched if the model holds.

Panvala’s matching multipliers over time using the latest utility factor estimate

This should be hard to believe—it certainly was for me. But if this model holds, we can create an incredible decade-long window

when any community in the world can have their funding for public goods amplified at attractive rates with no apparent cap. Think about all the Bitcoin mining operations that have sprung up out of nowhere since 2009 to earn rewards from Satoshi’s decision to subsidize security, and imagine that Satoshi had decided to subsidize other public goods instead. Firms would pop up all over the world—not to rack up power bills mining blocks, but to provide public goods that we’ve all wanted but couldn’t coordinate to fund.

How You Can Help

1. Stress test Panvala’s utility factor.

At its core, the utility factor is a measure of how the flow of tokens resists changes as the value of donations flowing through the system changes. To test it, we need more donations. Our first sponsors are Unstoppable Domains, Helium, and MythX. These sponsors have made nonbinding pledges to make monthly donations to Panvala to fund Ethereum infrastructure. If you or your company becomes a sponsor as well, we’ll be able to collect more data to make firm estimates of Panvala’s utility factor.

1. Critique the circuit token model.

This model includes several simplifying assumptions that we think are fair to make. If some of those assumptions are unrealistic, the sooner we know about it, the better.

1. Join Panvala as a voter.

If the circuit token model works, then we have a huge responsibility: a decade of donation matching at these rates will likely be a society-wide

event, especially since there doesn’t seem to be a limit on the amount of donations that can be matched. Help us show the world how to use this tool effectively, and help us build communities that are worth sustaining even when the matching multiplier runs out in a decade or two. https://panvala.com/