There is an economic problem at the heart of decentralized economies that has caught my attention for some time. This is an attempt to articulate it. My apologies if this is self-evident or redundant. I myself believe it to contain many self-evident truths, but still to present a novel problem.

Capitalist economy is based on the assumption that the players in an economy will optimize their profits. The reason why a firm creates a product is in order to generate as much profit as possible from it. Consumers will strive to pay less in order to maximize their own profit (in technical terms, to maximize their utility per unit paid).

In such an economy open-source software presents a bit of a problem. The problem is not just merely that open-source generally does not produce much by way of profit, especially when compared to proprietary code (compare Red Hat and Windows). It is also that open-source code is often of higher quality and therefore more desirable. There are two technical reasons for this: the code can be reviewed by more experts, and also there is more access to professional and specialist contribution. We therefore arise at a bit of a paradox. The public wants open-source, but will pay more for proprietary.

We're not going to discuss why

the public doesn't pay for open-source. I'm not qualified, for one. It may simply be a tragedy of the commons, for another.

This problem is particularly poignant in blockchain/cryptocurrency. One is the poignancy of this paradox on any cryptography software. Software that secures money and other liberties is of a more mission-critical nature, and we need it to be of the highest quality possible. But we still don't want to pay for it. If a firm develops a cryptographic algorithm and implementation, they should want to keep it proprietary to maximize profit, but then we'd lose community review. Of equal importance, two new attack vectors open up. One is that the firm may be malicious, and the other is that the firm can be bribed. Since no one sees the code, no one is the wiser.

(Recommended reading: Matthew Green on the NSA probably bribing a backdoor into RSA.)

Another cause for concern in the blockchain space in general is the ease with which the need to profit can enter at the protocol level. If we were to conceive of a blockchain voting platform (without debating if it's a good idea to put voting on the blockchain), we would likely abstract a system in which accounts (likely verified accounts) can transfer a valueless token or signal some data or the like. Who will create this platform, though? How are they providing for themselves while they write it? The second the writer needs or wants to generate revenue by writing this software (which is a basic capitalist economic theory), instead of charging for the platform (and needing to make the code proprietary or creating a SaaS model), he could insert a token into the system which can have value, and then speculate on the value.

It is my personal opinion that this is a devil's deal. The devil sells it by saying that the code remains open-source and reviewed, and therefore maintains the quality of open-source software. This is the devil talking, though. It's true that the code is open-source, but the protocol has been perverted. Instead of the protocol being optimized for efficiency, usability and security, it will now be also optimized for speculation.

This is true not only of applications on the blockchain, but also of the actual blockchains themselves. Ethereum is supposed to be part of a larger system including Whisper and Swarm, two amazingly important projects. They don't move as quickly as Ethereum, though, and it could very will stand to reason that it is because they do not carry the same economic incentives. How are we supposed to incentivize their development without compromising their quality?

(As a side note, one of the common models that's emerged from very successful open-source projects is that they're developed by firms that don't need revenue from them. Open sourcing these frameworks, such as Kubernetes or React, allows them to grow in quality, assuring that their producers benefit from a higher-quality product while in turn paying less for their development, and also help their image.)

The general model in macroeconomics these days is that the government acts as a non-profit entity that stimulates the economy. The government pays for public works and can create subsidies and/or tax breaks to halt recessions. There has been talk around a portion of block rewards going to the Ethereum Foundation for development purposes. I would argue that this is the same concept of government funding for public works. (I've daydreamed that an IRL government policy of budgeting contributions to open-source would be very beneficial to privacy, security, and the efficiency of programming at large.) This brings its own problems, though. Who decides where this money is going? Well, the Foundation. This introduces and attack vector of gaming the Foundation for unearned money. It is this author's very strong opinion that putting the money in a DAO won't help. Instead of gaming the humans in the Foundation, the attack vector becomes gaming either the user accounts of the DAO or the code of the DAO itself. In other words, creating a public-works fund for developing the platform or developing on it necessarily creates a governance bottleneck. Someone or something is deciding who and what gets how much funding. Is this the decentralized utopia we want?

In summary: If we want quality, quick progress on blockchain platforms and dApps, they should be well-funded and/or profitable, and open-source, and it's not clear how to accomplish that.

I wanted to ask the community their thoughts on this. Are there funding models that I've ignored? Are there any other thoughts about how to otherwise fund the decentralization of the web?