Truth and Beauty Bux: Towards Sane Uses of Cryptocurrency

Eric Purdy
Your Name Here (contributions welcome!)

May 26, 2018

In this document, we briefly lay out a variety of schemes for using cryptocurrency that alleviate a number of the drawbacks of all existing cryptocurrencies. We intend to implement these schemes on top of the upcoming Thunder Token cryptocurrency, as Thunder Token seems to be provably secure, easy to develop on (as it is planned to be interoperable with Ethereum) and as environmentally friendly as any cryptocurrency can be.

1 Introduction: What is Wrong with Cryptocurrency Today?

First, we lay out a number of objections to cryptocurrency, and note briefly how we think they are best addressed.

1.1 Cryptocurrencies Encourage Speculation

Existing cryptocurrencies have largely benefited technically savvy people with the mathematical and programming expertise required to take advantage of less savvy participants, all while creating little to nothing of real value. Large-scale price swings have enriched some and devestated others, largely with no rhyme or reason. Clearly, the root of the price swings is that cryptocurrencies have historically sought to separate themselves from traditional, stable fiat currencies that have widespread adoption and a clear value proposition.

The only obvious solution to these problems is to tether cryptocurrencies to a stable fiat currency whenever possible, which brings us to our second point:

1.2 Tethered Cryptocurrencies Are Bullshit

The existing tethered cryptocurrencies rely (supposedly!) on a promise to bank vast quantities of the fiat currency and produce it upon demand. These promises have proven to be a lie. The market may not care that these promises are a lie, but it is clear that the temptation to lie about such a thing is too great to resist.

Fundamentally, the promise to bank large quantites of fiat currency and then produce them upon demand is insane and counterproductive. It removes capital from the traditional economy while fueling the cryptocurrency bubble. It is much wiser to invest fiat currency backing tethered cryptocurrency in the traditional economy through traditional avenues of investment such as mutual funds that are subject to traditional regulation via e.g. the SEC.

We should not create any powerful institutions that are liable to become corrupt (this was in our estimation the failure mode of the Tether (USDT) cryptocurrency); rather, we should create an ecosystem of institutions that are at most as powerful as is required to do their job, and incentive structures that encourage such necessary institutions to be transparent, honest, and straightforward, both by designing incentives into the software of the cryptocurrency, but more importantly, by invoking existing legal and regulatory structures and institutions where appropriate.

Fundamentally, we believe that Tether (USDT) failed because it tried to do something for which the incentives to be honest were too low, and the incentives to be dishonest were too high. A USD-backed cryptocurrency that people can withdraw from at will requires the backing institution to either lie to investors (morally bankrupt!) or maintain an enormous bank account which it does not use for any investment purpose (financially unsound!).

A much wiser approach is to create an ecosystem of USD-denominated mutual funds that accept deposits in Truth and Beauty Bux tethers, and which has waiting periods to withdraw the tethers. This allows the mutual funds to invest the money in a completely traditional way (in the traditional, legal economy, and subject to traditional legal and regulatory structures and institutions), without worrying too much that the vagaries of the cryptocurrency markets will force them to liquidate their investments on an unprofitable time scale; rather, they can use the waiting period (say, 72 hours, or 168 hours) to liquidate their investments in a sound way. Such mutual funds could choose to waive the waiting period when the cryptocurrency markets were not losing their minds, in order to compete for the loyalty of their customers by providing added convenience.

1.3 Cryptocurrencies Facilitate Illegal Transactions

Cryptocurrencies routinely facilitate illegal transactions. This is their primary value proposition to date.

We believe that routine, voluntary transparency in dealings will enable the government to do its job more easily without curtailing civil liberties, by creating a sort of social contract between users of the cryptocurrency. People will know that non-transparent transactions will be subject to higher scrutiny by the government, but the government will still have a fairly difficult time tracking down the real participants in non-transparent transactions. Ultimately, such efforts will probably require state-level actors with state-level computational budgets and state-level access to traditional financial data. It is hoped that state-level actors will be circumspect in enforcing laws they know to be unjust, in exchange for the trust that users place in the network by using the cryptocurrency at all, and in exchange for the voluntary, routine transparency that this particular cryptocurrency encourages. Ultimately, if the state-level actors choose to enforce unjust laws (such as the prohibition of sales of non-addictive drugs with religious or therapeutic uses, such as hallucinogens or MDMA), and the voluntary, routine transparency becomes less routine, the state-level actors will have only themselves to blame.

In practical terms, this is simply an argument for signing some transactions with cryptographic keys registered with the government under a particular citizen's name and tax identification information.

1.4 Cryptocurrency Has No Use Case

This is a commonly cited argument, but we find it to be uncompelling. If we want a use case for cryptocurrency, we need look no further than file-sharing protocols such as BitTorrent:

Specifically, we hope to do the following:

- Augment the BitTorrent protocol with extensions that make it possible to safeguard artist's rights to be paid for the work they create
- Do so without enforcing odious Digital Rights Management restrictions on what computations people are allowed to run on their own computers
- Solve the free-rider problem that plagues existing BitTorrent networks by incorporating micropayments for serving files

We anticipate transposing the current illegal BitTorrent networks to a completely legal and honorable method for distributing artistic content that does not require the odious restrictions on personal computation that were generally considered to be necessary for Digital Rights Management.

Specifically, we envision a version of BitTorrent that exchanges *encrypted* chunks of files. These are only usable as media files if the owner has the decryption key of the file in question. Such keys are themselves of course perfectly copyable and perfectly transferable, as is any digital information, and thus are themselves subject to appearing on BitTorrent and other such platforms. It is hoped that by cutting out such obvious rent-seekers as scientific publishers like Elsevier, or industry groups such as the MPAA and the RIAA, and allowing everyone together to act as a distribution mechanism for artistic and informational content, while funneling payments directly to artists, journalists, and other producers of such content, it will become morally untenable for individual programmers to circumvent such protections, and there will be little or no political will opposing network interference with such protocols when they are identified. Ultimately, it seems unlikely that illegal file-sharing can ever be stamped out without violating civil liberties, but it seems quite straightforward to make it so that it is primarily the domain of scoundrels and scofflaws.

How do we use content distribution as a proof-of-work? This is actually a fairly interesting thing. We postulate that nodes participating in the modified BitTorrent protocol will receive an encrypted file block and a nonce called the "challenge" that is associated with the blockchain nodes that they are extending. They will then publish a new tangle node that includes a hash of *the concatenation of the content of the encrypted file block with the challenge.* It is therefore not super useful to counterfeit such blockchain nodes, because anyone who has a copy of the encrypted file block in question and copies of the relevant global tangle nodes can check your work. Presumably large actors with financial interests in the integrity of the blockchain would simply mirror vast swathes of encrypted content and check all nodes in the global tangle.

1.5 Cryptocurrency Does Not Take Advantage of Existing Financial Infrastructure

This is a valid criticism. Fundamentally, it makes more sense for existing large financial institutions to be considered untrustworthy but potentially valuable allies rather than enemies or competitors.

We propose to allow some blockchain verification to be done off the global blockchain as a proof-of-work; this enables the blockchain protocol to scale almost indefinitely, cuts down on storage needs, and also helps to address environmental concerns.

We note that a tangle-based cryptocurrency can be made more efficient by hosting the majority of nodes off of the global tangle. The idea here is that network actors who have built up some level of trust can choose to publish digests of large subtangles at regular intervals. I.e., a large traditional financial institution such as Goldman Sachs or the NYSE could build their own tangle, based off a large number of nodes in the global tangle, extend with a large number of transactions desired by their customers, then publish some number of tips to the global tangle, along with pointers to a cryptographically signed unencrypted content block that is available to all network participants via the modified BitTorrent protocol. The content block contains the tangle nodes of the transactions that e.g. Goldman Sachs is verifying for its customers, and can be independently verified by other institutions and by network participants who choose to run such a computation. This can act as an auxiliary proof-of-work, while ensuring public trust in the integrity of the blockchain.

2 The Automated Market-Making Problem

We envision using an untethered host cryptocurrency (probably Thunder Toekn) to power Truth and Beauty Bux. This necesitates conversions between the fiat currency we are tethering to (presumably USD) and the host cryptocurrency. Such situations have generally been taken advantage of by savvy actors such as large financial institutions, in a way that is essentially rent-seeking. (That is, providing liquidity is a useful service, worthy of compensation, but in most situations, more value has been extracted by market makers than was truly required in order for them to make a healthy profit while serving their customers honorably.)

We envision a distributed market-maker, in which everyone who has a Truth and Beauty Bux wallet containing a minimum amount of both the host cryptocurrency and Truth and Beauty Bux, and whose wallet has had the minimum amount for more than some minimum length of time (say, one week) will provide liquidity to the market at an automatically determined rate. (For the sake of a very simple example protocol, say that every blockchain node provides a bid and ask price that the publisher of the tip must buy and sell at, and everyone else buys and sells at the average of prices quoted on nodes that have been verified in the past minute, or five minutes, or maybe a Gaussian-smoothed average over the past hour (this would discourage quick price swings).)

The effect of all this should be that people who leave amounts of Truth and Beauty Bux above the required minimum receive compound interest on their wallet amounts that are deposited directly into their wallets. Thus, everyone participating in the network who provides liquidity receives fair compensation for the service they provide, and no network participant can take unfair advantage of their mathematical expertise or greater market knowledge to cheat the other network participants out of their rightful due. This seems superior in every respect to the current situation in the cryptocurrency markets.

2.1 Theoretical Desiderata

In this section, we lay out a research program whereby passive market participants (who are assumed to be less informed and less savvy) can get a fair share of the returns that have traditionally accrued to hedge funds and other financially savvy actors. Our general project will be to try to construct a market-making game where the Nash equilibrium is Pareto-optimal, and where there is no incentive for uninformed market participants to take an active role. If we can describe such a system and prove that it has the requisite properties, this means that we will have achieved our goal of automated market-making for the masses.

3 Acknowledgments

We thank Dr. Jesse Raber for valuable discussions related to the intersection of the blockchain and public policy. We thank Austin Stone for many, many valuable discussions related to the market-making problem.