Fair Decentralised Consensus Is Impossible

Ben Laurie
ben@links.org

November 19, 2017

1 Introduction

I wrote this proof not because it proves anything that is not obvious, but because I am tired of descending the cryptocurrency rabbit hole.

If you want to claim that you have a fair decentralised consensus mechanism, then you have to tell me which of my assumptions is incorrect for your system. Thay can't all be correct. I have proof.

Enjoy.

2 Definitions

Informally, decentralised means that there is no central authority. But what does this mean formally? I propose that we can model a general "decentralised" system as a set of participants, P, of unknown size. In other words, no member of P can enumerate P. Also, all members of P are not special in any way.

By decentralised consensus I mean a deterministic algorithm, C which, given a set of possible outcomes (which are also not special), O and a vote by every member p of P for some outcome $o_p \in O$, $C(Q) \in O$ where $Q \subseteq P$, and $\exists P' \subset P$ s.t. $C(P') = C(P)$ (in other words, it is possible to determine the consensus without enumerating P).

C is also allowed to fail - i.e. to indicate there is no consensus.

A consensus algorithm C is said to be *fair* if $C(Q) \in \{o_q : q \in Q\}$ where $Q \subseteq P$ (that is, the consensus for any subset is voted for by at least one member of that subset). Note that this is a very weak definition of "fair" but is sufficient for the proof.

3 Proof

Consider the point of view of some particular participant, let's say $q \in Q$ where $Q \subseteq P$.

q must assume[1] that $\exists R \subset P$, $Q \cap R = \emptyset$ (that is, a disjoint subset of P), $C(Q) \neq C(R)$. This is because of fairness and the unknowability of P: q must assume R exists where all members have voted for an outcome other than $C(Q)$, which means that $C(R) \neq C(Q)$, because of fairness. And because no-one is special, R could also meet the consensus rules, whatever they are.

Since no participant is special, q must assume that either $C(Q)$ or $C(R)$ could be the same as $C(P)$ (note that $C(P)$ could be neither!), because choosing one would make q special, and hence, q cannot know what $C(P)$ is.

This argument applies to all members of P, which implies that no participant can ever know $C(P)$.

So, in other words, there cannot be fair decentralised consensus.

4 Afternote

Actually, there is one: C always fails.

[1] By which I mean that I can construct R and there's no way for q to know that R does not exist.