CHAPTER 4
TRUST-BASED ALTERNATIVES

One way of doing this is by replacing the seminal trustless proof-of-work algorithm with trust-based substitutes such as proof-of-stake, proof-of-consensus, proof-of-activity and others. Let us now briefly touch on these alternatives and find out more about it. However, we do not support this approach because it lacks sound cryptographic encoding and is trust-based, which in our opinion is less secure and open to manipulation.

So, let's begin with the Ethereum network, which is most likely to transition from its current trustless proof-of-work algorithm to a proof-of-stake[11] algorithm. The proof-of-stake is a trust-based alternative.

As can be seen in the article cited below that they intend to abandon the seminal proof-of-work approach in favor of a to-be-designed proof-of-stake system. That's due to the Byzantine fault tolerance and high computational costs involved in a trustless system. It does not matter which flaw they point at, the fact remains that due to the high costs involved in running a trustless proof-of-work algorithm, they will abandon it and move on to a proof-of-stake system.

Although we agree with some of the aforementioned arguments and assumptions, there are others that we strongly disagree with. To begin with, we agree that proof-of-stake is more complex, less proven, and in dire need of improvement. We also agree that proof-of-stake is prone to Byzantine fault complexity[12], inability to handle network latency[13], partly asynchronous operational difficulties[14], and the inability to remain consistent. Also, implementing various mitigations and workarounds to the above can make it prone to bugs.

Coming to disagreements, we strongly refute the claim that the problem lies in the excessive simplicity of the seminal Bitcoin protocol, on which Ethereum is based. We also disagree with the remedial recommendation to "fix" it by exponentially increasing its complexity. That misses the point entirely: the root problem is complexity, not simplicity and that cannot be "improved" by increasing its complexity.

Thus, the solution to the network cost problem has nothing to do with weak subjectivity, Byzantine fault tolerance, pseudo-random validator

[11] See https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ . Cost estimate at top of 2nd point, remainder provides arguments in favor of P.o.S. systems.
[12] Lamport, Shostak & Pease "The Byzantine Generals Problem". http://www-inst.eecs.berkeley.edu/~cs162/fa12/hand-outs/Original_Byzantine.pdf
[13] Fischer, Lynch & Patterson "The Impossibility of Distributed Consensus with one Faulty Process" https://groups.csail.mit.edu/tds/papers/Lynch/jacm85.pdf
[14] Dwork, Lynch & Stockmeyer "Consensus in the Presence of Partial Synchrony" https://groups.csail.mit.edu/tds/papers/Lynch/jacm88.pdf