Hard forks, soft forks, and choices.

Recent events surrounding Bitcoin had been a matter of dispute, arising from the difference in views of how scalability is to be addressed – Either through SegWit (subsequently off-chain transactions) or increased block sizes facilitating more on-chain transactions (with tx malleability fixes). Each implementation is done quite differently: The Core developers pushed through SegWit with a soft fork, whereas others proposing for an increase in block sizes requires a consensus protocol change resulting in a hard fork. The purpose of this write up is not to scrutinise the technical underlying of each implementation, but to lay out views that in a decentralised setting where a contentious protocol upgrade is to be introduced, a hard fork is not necessarily more forceful than a soft fork, and could be a better method to preserve network participants' freedom of choice.

Some quick definitions:

Hard fork – A hard fork introduces protocol changes which requires what would *previously be considered invalid to be accepted as valid*. This will require the network participants to upgrade their clients to continue accepting and build on these new set of consensus rules. In terms of technical implementation, a hard fork provides developers with more flexibility, as they do not need to strictly ensure the new protocol fits into the old protocol. Participants (miners, nodes, and users) will need to explicitly show support and opt-in to the hard forked chain for it to be a success, and due to that there is a higher likelihood of a chain split.

A hard fork could be made *bilateral*, i.e. where new consensus rules do not agree entirely with previous consensus rules; or *expanding*, i.e. where new consensus rules are built on top existing rules thereby the non-forked chain is valid under the new set of rules.

Soft fork – A soft fork introduces protocol changes by *limiting or reducing the transactions* that would be valid moving forward, therefore network participants on the old rules could still participate on the new chain, assuming that the new chain has majority hash rate support. In this case network participants do not need to upgrade the client to stay on the new chain, possibly with some minor caveats, and the upgrade could be delivered implicitly without participants explicitly opting in. This results in a lower likelihood of a chain split, and in the event the fork is successful there will not be an unforked chain. In terms of technical implementation, more work has to be done as to not introduce an incompatibility with old consensus rules.

The key point which I would like to highlight is this – *A soft fork could be delivered implicitly without needing participants explicitly opting in*. The soft forked chain is backwards compatible, and users do not need to even realise an upgrade to the network was rolled out. In addition, the nature of not having an unforked chain also means that a participant would not have a venue to opt-out for an introduced protocol when it is entirely against the participant's view.

Therefore a soft fork is either all (or vast majority) or none at all, creating a situation where participants of a network do not get to choose for themselves – either for good or for bad – for a proposal to be carried out on the network without having everyone else agreeing to their views, ala *liberum veto*. For a signalling requiring vast majority (80%, 95%, etc) support,

the minority then gets side-lined. Non-upgraded blocks are being censored, and majoritarianism made apparent when there is a requirement of a majority hash rate signalling for a soft fork (hence tyranny of the majority). For the case of SegWit, choosing not to upgrade meaning having your blocks potentially rejected as a miner, transaction drop offs, and delayed transaction appearance.

From this perspective, a hard fork provides more freedom to the participants of a network, in the sense that the participants are given choices and they could exercise the right to choose from the options provided. Miners make their own decision on which chain to provide hashing power towards, nodes maintain the chain they'd want to, and users send transactions on the chain of their choice. There would not exist a majoritarianism nor minoritarianism dictating how the rest should play along a set rules; Rather each individual is empowered with the ability to make a choice and to work on the choice they have made.

Admittedly hard fork chain splits risk splitting asset price backing the chain (and subsequently hashing power and users), but whichever chain with the most active development providing mass acceptance has shown to be fairly resilient and able to sort itself out over time. Furthermore since a vast majority of hash rate is expected to carry out the soft fork, that would imply a confidence of having users, miners and nodes to be on the updated chain, thereby invalidating reasons to expect otherwise on a hard fork chain.