Zack Hess

proof of stake

This is a weaker kind of consensus than POW consensus. If you you leave your computer off longer than 2 weeks, your money will get deleted.
It is recommended to sell all your money for bitcoin before turning off your computer, every time.

==========response to andytoshi========

Andrew Poelstra wrote a paper about how POS is impossible:
https://download.wpsoftware.net/bitcoin/pos.pdf

His arguments rest upon a false assumption. He assumes that consensus can only be achieved if the longest blockchain is also the correct one.

If you take the assumption to be true, it is easy to show that long-range attack is always possible. Because it does not cost anything to build a longer blockchain. This is known as "costless-simulation argument".

A simple counter-example to the assumption that costless-simulation arguments depend upon is the relationship between litecoin and bitcoin. Even if litecoin was longer than bitcoin, the bitcoin nodes would still only download bitcoin blocks, and would not start downloading litecoin blocks.

In my proposal, long-range attack forks are distinguishable altcoins. Commiting a long-range attack is identical to forking the code, and launching an altcoin.

==========implementation details==========

I start with this https://blog.ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm/
Slasher is safe against any forks where were created within the last 3000 blocks. I do the following upgrades, to make slasher secure against forks from longer ago:

1) The reward for mining a block should be negative. Usually, no one makes blocks until there are enough transaction fees to pay for a new block. It is impossible to use money to get more money.

2) The POW for each block should be far lower. 5 seconds on a core 2 DUO doing CPU mining.

I deviate from Vitalik's Slasher in a couple more ways, but to explain them, I need to explain how Vitalik's Slasher is broken. This is called a "long-range attack". There is no incentive to protect old private keys after you spend the money. It is possible that someone could collect a lot of old private keys, and that person would own more than 50% of money at a time in history. With this they can build a fork which is longer than the real fork. When new people download a client and join the network, they will download the wrong fork, and will be unable to receive funds.

To make this type of attack impossible, I make the following changes.

1) Everyone must periodically pledge to a fork, your money gets deleted in every other fork.

2) If anyone simultaneously pledges to completing forks, their money is erased in both forks.

3) Each node needs a list of public keys that have money, it can look at valid blocks with signatures from these pubkeys. When a node boots up, it downloads the longest blockchain where at least one of the public keys from the list still has money. If some forks have less than 1/2 as much money as the biggest fork, they are ignored.

==========If you are too lazy to read Vitalik's blog entry on slasher, but are still curious of what slasher does==========

----jury
*the jury is selected randomly from coin-holders.
*jurors have the potential to collect a reward, if they successfully broadcast 2 txs at the right times.
*the first is called 'signature tx' the second is 'reveal tx'

----signature tx
*it has a 10-block window where it can be broadcast.
*This tx can only be put onto a single fork.
*If a juror tries to sign multiple forks, they lose money and their signatures are erased on both forks.
*This tx contains HASH(secret)

----reveal tx
-*it has a 900-block window where it can be broadcast.
-*reveals secret
-*gives the juror a reward.

-----random number generator
*the random number generator's seed is made up of revealed secrets from jurors from over 3000 blocks ago.
*the random number generator selects who will be on jury for the next block.

----punitive tx
*you have to prove that a juror signed on multiple forks.
*the juror is punished, and you recieve a reward.

It is impossible to do a long-range attack within the last 3000 blocks because the seed to the random number generator is already set, and the people who were elected as juror are

========attack vectors==========

A majority of coin-holders decide to stop a minority from pledging to the real fork.
The minority can try to purchase blocks too, and they are willing to spend ALL of their money rather than have it destroyed. The attackers will have to spend even more money than that the victims, and they have to spend it on every single block till the victims die. That is 1000 blocks.

A large number of coin-holders do not pledge to any blockchain, and let their amount of money=M get burned in the same moment.
This creates a vulnerability in our armour, but the vulnerability wont be a problem till decades or centuries in the future. Once the blockchain has less than 2.3*M total coins, we need to copy/paste how

much money everyone has and make a new genesis block.