Essay: Propose a mining method for a public blockchain that avoids double-spend (for currency blockchains) or alteration of the past (DLT), such that the incentive structure and integrity mining methods do not lead to centralization?

Before proposing a different consensus method I will start by describing and mentioning some of the benefits of current popular algorithms (most of the information in this section was taken from '' What are the Alternative Strategies for Proof-of-Work?' online article):

- Proof-of-Work (PoW): It has been proven that the Proof of Work mining method works. The protocol of investing significant effort (computer power and electricity) to solve the mathematical puzzle that can be proven very easily is a great way to reach consensus. Since the odds of being able to write several consecutive blocks are slim, the method discourages 'bad' nodes of trying to double spend or modify transactions. PoW consensus algorithms has two main purposes: validity of information and avoid manipulation. Miners collect transactions fees and 'create' new currency which they pay to themselves every time they write a new block.
- Proof-of-Burn (PoB). In this algorithm, the miners are required to 'burn' crypto or fiat currency to earn the right of processing the transactions and getting the fees. The 'burning' process stabilizes and increases the price of the cryptocurrency. The more money or crypto coins you burn the probability of getting selected increases. This method is used by Slimcoin and Counterparty.
- Proof-of-Stake (PoS): is a good alternative to PoW since it doesn't require a lot of computational power thus saving electricity and resources. In this consensus algorithm 'miners' called forgers, get randomly selected to process transactions and charge their respective fee. In order to participate they need to make a deposit once they get selected. Their chances of being selected increases by having more stake (number of coins in a wallet). In this consensus methodology there is no coin creation only transaction fees. Peercoin, Nxt, Blackcoin and Shadowcoin are using PoS.

- Proof-of-Capacity (PoC): is based on hard drive space (more space equals the more is the probability of mining the next block). The algorithm here generates large data sets that would then be stored on the hard drive. This method is used in Burstcoin.

After describing the main characteristics of some of the best-known consensus mechanisms it is easy to spot their benefits. Each method has a way to deter the bad actors of messing up with the system. The method I propose has some of these characteristics.

The method I propose, which I would call Penalty-Agreement (or for keeping with the same structure as other methods would call it Proof-of-Penalty) would be a pay and play mechanism. Miner would have to meet only 2 requirements to participate: first, they have to own a stake of coins and second, they have to be the owner of a public database which everyone would be able to see but only them would have the writing privileges.

In a sense it is very similar to the Proof-of-Stake algorithm. The way it differs from the PoS method is that instead of assigning the transaction randomly to one miner it will be a process which I would call 'splitting' that will broadcast the transaction to all registered miners but will randomly assign a penalty to each miner in case they decide not to record the transaction in their own database.
The miner would belong to the 'system' but won't be able to participate in the transactions if they don't have enough funds to cover the randomly assigned penalty.
The penalty would contain 2 parts: one part we would call the 'base' which would consist in the transaction value divided by the total 'active' miners. The other part would be a 'spread' which would be randomly generated percentage that could be up to 25% of the base amount. For example, if the transaction value is 200 and there are 100 miners the assigned penalty would be 200/100=1 (base) plus a randomly generated percentage that can be of up to 25%. So worst case scenario someone would be assigned a penalty of 1.25. In order to participate the miner would have to own at least the worst-case scenario amount which in this case is 1.25.

In the case that one rogue miner doesn't want to write the transaction in their database (ledger) and it is published by more than 50% of the miners the bad node would be charged the penalty. In order to be considered a valid transaction, it would have to be confirmed by more than 50% of the miners.

The way to incentivize miners to participate would be through the charge of transaction fees. Transaction fee would be a percentage of the total transaction, in this case I would start in around 2-3% which is an average fee in credit card transactions. This fee would be divided in equal amounts for all participating miners that confirm the transaction in their ledger.

Another difference with the transactions is that since everyone would have to write the transaction at the same time there would be a way to record the time stamp.

The way all the ledgers would be processing the transactions would be a little bit different than other methods: the ledgers would be recording amounts and balances so 'change' transactions won't be needed. It would be recommended that users own at least 2 different 'accounts'. One or more to keep their funds and one or more to process transactions. For example, if you want to pay someone 5 coins you will have the option of transferring this 5 directly from your account A where you keep most of your funds or transferring those 5 to your account B (where you always keep a balance close to cero) and then making the payment.

This distributed ledger technology would continue to have the 5 positive traits or strengths mentioned in previous module:

- Visibility: everyone would have the ability to see transactions in any of the public ledgers
- Aggregation: transaction could be generated by anyone (person, exchange, etc.)
- Validation: information would be difficult to tamper with since it will be recorded in all databases
- Automation: ability to execute transactions automatically in response to prespecified conditions
- Resiliency: it will be able to withstand certain shocks (some nodes disappearing from the network). As long as at least there is more than 50% of the nodes working.

Conclusion

There are pros and cons of all consensus methods. It is important to find a way to make the system easy for everyone to use, validate and 'mine'. The system has to keep in mind that security and integrity are the most important characteristics of every distributed ledger.

A method such as the one I propose would look more like an actual ledger where you will be able to see the transactions main information such as the date and balance of accounts.

Reference

1. Kumar Sharma, Toshendra. "What are the Alternative Strategies for Proof-of-Work?". January 25, 2018. https://www.blockchain-council.org/blockchain/what-are-the-alternative-strategies-for-proof-of-work/
2. Walters, Steve. "Proof of Burn Explained – An Alternative Crypto Consensus Algorithm". March 28, 2018. https://www.coinbureau.com/education/proof-of-burn-explained/
3. Blockgeeks. "Proof of work vs. proof of stake: Basic mining guide". 2017. https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/