Fairness and Inclusion in Blockchain

A consensus is a mechanism through which all the members of a network reach a common agreement about the current distributed ledger. Now, distributed consensus refers to a procedure to reach a common agreement in a de-centralized multi-membered platform. There are various promises which need to be followed to form a distributed consensus in any environment including but not limited to a common agreement among all members, the decision of non-faulty processes, and integrity among members. There are various distributed consensus protocols such as Proof of Work, Proof of Stake (newly formulated), Proof of Burn, etc. These are used in validating crypto transactions in decentralized blockchains to reduce false transactions by fraudsters. They make sure that all the members of a chain have supplied resources to the network in some way.

Now, talking about proof of work, this algorithm uses some hard trial and error puzzles for the miners to solve using high-computing computers. The first miner to crack the puzzle is authorized to add new blocks to the blockchain network for transactional purposes. When some piece of the block is approved by a member the coins are provided to the miner in the Blockchain network. For validation, a random member is chosen using an algorithm that takes care of the stake of the miner and experience in the hierarchy. If the authentication process is not completed somehow, it may even result in a stake being lost by the person solving the puzzle. One thing to note about this algorithm is that the computers used in this algorithm are very advanced and require a lot of care and resources and this implies that expansion of the network will cost us even more concerning time and energy. Now, to take down proof of work a fraudster need to take down more than 50% of the network and its energy. There is also a possibility of Blockchain duplication to prevent the history of our original transactions is moved in a new direction also. Miners have the option to remain in the original network or move to the duplicate network. This up to some point prevents the takedown of 50% or more resources because now the computing resources need to be divided into both sides of the networks. Now, let’s move to proof of stake as, after authentication of the blocks, the miner receives the digital currency added to their starting stake. Proof of stake is recently designed because it takes care of the various problems, we have in proof of work i.e. resource consumption, and scalability. Adding this stake putting also helps in reducing the fake commits and thus makes our system extra secure. Now, there are some problems with proof of stake also including but not limited to a large amount of investment miner makes to take out his/her stake. Thus miners with a large amount of money have the most power also and have a big say on the authenticator. Now, the problem in the case of proof of work i.e. the duplication of the Blockchain network is also taken care bu the fact that now the authenticator gets the copy of the stake as there was no record. Hence, he/she will end up paying double the amount (both in blockchain and duplicate blockchain world).

The major difference Between proof of work and proof of stake is the power consumption (used very much more in case of proof of work because of the usage of high-frequency computers). The power consumption is less in the power of stake because in this algorithm the authenticator is used by random chance instead of complex puzzles solved in the case of proof of work using high-frequency computers. There is also a case of double spending in case of proof of work when more than 50% of the stakes are held by some false/fake miners. This may lead trustworthy miners to suffer. Proof of stake takes care of this because it asks the miner to add a stake before validating any block and thus the stake of the miner is a kind of security added to the network which will then reduce the false miners because they will not try unfair means on the risk of losing their stake.

Now, talking about proof of burn (another consensus algorithm to ensure agreement among the states of our blockchain network), it is mainly used to avoid double spending and high resource consumption problem. It allows the miners to burn the coins held in form of a stake by the miner during the right of addition of blocks. The more the number of virtual coins/ native currency destroyed by a miner the more will be the rig of the miner because instead of them now the miner is getting a new reward of the native currency of that particular Blockchain network i.e. all the members are rewarded with native currency both for burning their coins as well as other people’s coins in the network. Now, there can be an unwanted advantage to a miner who has adopted the network earlier compared to another one joining later and to tackle this unfair advantage in proof of work a periodic burning of coins is implemented. The effect of the burned currency dulls with every addition of a new block.

Now, we need fairness i.e. equal opportunity to win in the consensus round because the rewards we get are only fetched after winning the consensus round the thing is that both proof of work and proof of stake are unfair. The rich miner gets richer as they have most of the say and the poor miner has too less to say. This implies that if one is poor and has no chance of winning the consensus round then that person will have no chance of mining new bitcoins also. But algorithms like weighted proofs and proof of burn are more fair compared to proof of work and proof of stake. In proof of burn, the winner loses the coins and the winner will have coins of less burn value in the next round thus his probability of winning the next round is too less because his/her currency is too new. Burn value is defined in such a way that it is too less for the new coins and comparatively more for the same value of the old currency. So, this algorithm ensures somewhat fairness without decreasing/cutting short the value of the currency we have and just by considering the age of the coins and there are some other parameters also. Now, even after considering all these things, there is still some unfairness going on in some other parameters.

Fairness and Inclusion in Blockchain Systems

The term "consensus" refers to the process by which all of the participants in a network come to a decision or judgement regarding the state of the distributed ledger. Now, when we talk about reaching a shared agreement in a decentralised environment with several members, we're referring to a process called distributed consensus. A common agreement among all members, the decision of non-faulty processes, and integrity among members are some of the many promises that need to be followed in order to form a distributed consensus in any environment. These promises must be followed in order for a distributed consensus to be formed. There are many other protocols for reaching a distributed consensus, such as Proof of Work, Proof of Stake (a freshly developed version), Proof of Burn, and many others. In order to limit the number of fraudulent transactions caused by scammers, they are utilised in the process of validating cryptographic transactions that take place on decentralised blockchains. They check to see that every node in a chain has contributed resources to the network in some form before moving on to the next.

Now, with regard to proof of work, this method makes use of some challenging trial and error puzzles that the miners must answer by employing high-performance computing devices. The first miner to solve the riddle will be given permission to add new blocks to the blockchain network, which can then be used for conducting transactions. When a member of the Blockchain network gives their stamp of approval to a certain portion of the block, the coins are distributed to the miner in the network. An method that takes into account the miner's stake as well as their level of experience in the hierarchy is used to select a member at random for the validation process. If for whatever reason the verification process is not finished, the individual who solves the problem could end up with less of a reward than they were expecting. It is important to keep in mind that the computers employed in this algorithm are quite sophisticated. As a result, they call for a great deal of attention and resources, which means that the extension of the network will be even more expensive in terms of both our time and our resources. Now, in order to destroy evidence of work, a fraudster will need to destroy more than fifty percent of the network's energy. There is also the potential of duplicating the Blockchain, which would prevent the history of our initial transactions from being altered and moved in a different direction. Miners have the option of staying in the first network or moving to the second network, which is a clone of the first. Because of this, the computational resources now need to be split between both sides of the networks, which prevents the takeover of at least fifty percent of the available resources up to a certain point. Now, let's move on to the proof of stake because, once the blocks have been authenticated, the miner will receive the digital money, which will then be added to their initial stake. Proof of stake is a newer form of cryptocurrency verification that was developed because it solves a number of issues related to proof of work, including resource consumption and scalability. The addition of this stake placing helps to reduce the number of fraudulent commits, which in turn helps to make our system even more safe. Now, there are some issues with proof of stake, and these issues include, but are not limited to, the fact that a miner must make a significant financial commitment in order to withdraw his or her ownership. Miners who control the most money also control the greatest power, and they have a significant degree of influence over the authenticator. Because there was no record previously, the problem that arose in the case of proof of work, which is the duplication of the Blockchain network, has now been resolved. This was made possible by the fact that the authenticator now receives a copy of the stake. As a result, he or she will wind up paying twice as much as they originally owed (both in blockchain and duplicate blockchain world).

The most important distinction The power consumption comes in between the proof of work and the proof of stake (used very much more in case of proof of work because of the usage of high-frequency computers). Because the authenticator in this algorithm is determined by random chance as opposed to the difficult riddles that must be solved in the case of proof of work employing high-frequency computers, the power consumption of the power of stake approach is significantly lower. When more over fifty percent of the stakes are held by some phoney or fake miners, there is also the possibility of double spending occurring within the proof of work system. It's possible that this will cause trustworthy miners to suffer. Because it requires the miner to contribute a stake prior to validating any block, proof of stake solves this problem. The miner's stake functions as a form of network security, which will lead to a reduction in the number of fraudulent miners. This is because fraudulent miners are unlikely to engage in unethical mining practises if they run the risk of losing their stake.

Proof of burn is an additional consensus mechanism that ensures agreement among the states of our blockchain network. Its primary purpose is to prevent double spending and solve the issue of excessive resource usage. It gives the miners the ability to burn the currencies that they have stored in the form of a stake during the time that they have the right to add blocks. Because the miner is now getting a new reward of the native currency of that particular Blockchain network in place of them, the rig of the miner will increase in proportion to the number of virtual coins or native currency that have been destroyed. This is because all of the members of the Blockchain network are rewarded with native currency both for burning their own coins and for burning the coins of other people in the network. Now, a miner who has embraced the network earlier than another miner who joins later could have an unfair edge in the proof of work, thus in order to combat this unfair advantage, a periodic burning of coins is established. This helps to level the playing field. With each new block that is added, the effect of the burned cash will become less noticeable.

Because the benefits we obtain are only fetched after winning the consensus round, we require there to be fairness, which means equal opportunity to win in that round. The problem is that proof of effort and proof of stake are both unfair. The miner who is already affluent gets even richer since they have the most say in the matter, whereas the miner who is already impoverished has very little input. This suggests that if a person is impoverished and does not have a chance of winning the consensus round, then that person will also not have a chance of mining additional bitcoins because there is a direct correlation between the two factors. However, proof-of-burn algorithms and weighted proofs are more equitable than proof-of-work and proof-of-stake systems. The winner of a round of proof of burn forfeits the coins, and going into the following round, that winner will have coins with a lower burn value. As a result, the winner's chances of winning the next round are significantly reduced because his or her currency is too fresh. Burn value is specified in such a way that it is too low for the new coins and relatively high for the same value of the old currency. This makes the new coins worth less than the old currency. By taking into consideration the age of the coins in addition to a number of other parameters, this algorithm ensures that some degree of fairness is maintained without lowering or otherwise diminishing the value of the cash that we now possess. Now, even after taking all of these factors into consideration, there is still some unfairness happening in some of the other metrics.