Hello,

Here is my contribution about scalability improvement.

Let's notice that scalability requires high speed validation, whereas block chain formation is a security measure (with merkle roots and tree), which slows down everything.

So the idea is to delay a little bit the block chain formation, in order to allow nodes to focus on real time high speed validation.

1st step : reaching a consensus among nodes in a decentralized network :

Let's assume we have a network of a few hundreds or thousands nodes. This can be achieved by requiring the nodes to stake or deposit a huge quantity of coins, in order to limit the number of nodes (masternodes, Casper nodes, …).

In the first phase, this network would try to make a consensus, meaning to decide whereas an incoming transaction is true or false.

When a client sends a transaction to the network, each node would consider the transaction as valid if he checks the transaction, or, in case there are too many transactions, in case enough other nodes tell that the transaction is valid.

Each node would have an internal database evaluating the reliability of other nodes, and ultimately giving penalties or blacklisting the other nodes who have a different assessment of transactions, since these nodes may be corrupted.

If the majority of nodes share the same software, there should be a wide consensus on valid and invalid transactions proposed by clients.

So I think a consensus could be achieved inside the network within a few seconds or minutes.

Of course, this network could manage hundreds or thousands of transactions per second. For each transaction, a consensus would be reached within a few seconds or minutes.

2nd step : once the consensus is achieved, making a new block into the chain

Once the consensus is achieved inside the network of nodes, and the transaction is considered as valid, this transaction could be marked as "ready for blockchain inclusion".

Then a node, or a group of nodes, could be chosen (randomly or with a deterministic process), in order to make a new block with several transactions marked as "ready for blockchain inclusion" (it could be thousands validated transactions for each new block).

It means a transaction would be included in a new block only after a consensus is reached inside the decentralized network.

This is different from current POW or POS, where there is a competition for making new blocks with incoming transactions.

Incoming transactions would first have to be validated inside the network of nodes, then, only once a consensus is achieved, included in a new block.

After the block is built, other nodes would check the validity of the new block made, and the chain would be processed this way.