Summary Alternative Consensus 1 Alexander Wandrup

Snow is an alternative consensus protocol. This system works by sampling the network at random to steer correct nodes towards a common outcome. This protocol have several goals. One goal is to ensure safety trough a probabilistic guarantee. They claim this is as good as traditional safety guarantees as appropriately small choices of probability will render consensus failure negligible. The protocols also provide a non-zero probability guarantee of termination within a bounded amount of time. This work similar to protocols like longest-chain protocols. In order for the protocol to achieve liveness it is synchronous and not asynchronous. This is because the system works by subsampling and it is possible for a sample to select a majority of adversarial nodes and can therefore get stuck waiting for responses. To ensure liveness a node should be able to wait some time without a timeout. The adversarial nodes execute on their own with their own internal scheduler. They can execute at any time unlike correct nodes. The adversary can also view the state of every hones node at all time. It cannot schedule or modify communications between correct nodes.

The slush protocol works by having a node at first in an uncoloured state. When it receives a transaction it will update its colour to the one carried in the transaction. It will then initiate a query. A query works works by making the node pick up a small constant sized sample of the network uniformly at random and then sends a query message. Any uncoloured node will adopt the colour in the query and respond with that colour and then send out another query, while an already coloured node will respond with it's own colour. Once the querying node gets a certain amount of responses it will check if big enough fraction of the responses are of the same colour. If the threshold is met and the sampled colour is different from its own colour it will change its own colour. It will then query again. This will go on for a predetermined amount of time. When the time is up the node will decide its colour.

Snowflake changes this by adding a counter that shows the nodes conviction of its own colour. The counter stores how many consecutive queries have yielded the same colour. A node accepts it current colour when it reaccess β a security parameter.