pS^{3}Chain^2 (Sthree Chain)-The Papros sidechain-its implementation details

Identity, security and the underlying data:

pS^{3}Chain^2 is a hybrid permissionless and permissioned sidechain. Anyone can record a transaction, however those who digitally sign their transactions using their own advanced cryptographic SHA-2 certificate for authentication have that data stored, and thus this offers a means for evaluation of the validity of the document based on the ranking of the identity to the viewer. Similarly, there are varying layers of security. The ground level being anyone can post data and anyone can see the underlying data if it is not protected. However, in higher layers of security, the document may be protected by a password or by more advanced encrypting, however, if the viewer is in possession of the document by other means, he can check against the hashes given the height of the block and thus be able to verify the authenticity of the document. Thus, the approach suits many different scenarios.

Permissioned or permissionless:

The pS^{3}Chain^2 combines the best of both these capabilities. While it offers the advanced needs of business to require permissioning, the Sthree chain allows for participants to decide if their data can be open or requires permission, either in the form of a simple password, or more advanced encrypting. This the pS3Chain2 offers the best of all worlds.

Consensus:

pS^{3}Chain^2 is a sidechain, however, it's a pegged sidechain, in that it can periodically interact with public blockchains to establish periodic time-synchronizations. Thus, it becomes indirectly subject to the consensus. Within its network, pS^{3}Chain^2 allows any number of nodes to fork their registrations but must synchronize with the mother ('mater') node every 24-hours. This ensures that each fork is only for 24 hours-each node is also by extension pegged. Each node also allows for "digitally" identified signatures, by participants are credentialed for their documents by means of their established reputation.

Technology:

This is based on the open source bitcoin technology. The only difference is that the hash is computed a single time and thus is very energy efficient. The computed hash is carried forward. It is a pegged sidechain, meaning it periodically synchronizes with public blockchains to calibrate and establish proof of timestamps. The merkle chains then combine to establish the integrity of the chain, and the chain can only be appended forward.

Private communications are enabled through passwords or encryption. Passwords are enabled for named users in the ownership file, and the default schema for the ownership file is JSON based. The requester passes this as a parameter. On the other hand, encrypted messages are accessible, and using secret cipher only the recipient who has the cipher can decrypt the document.

Identity of creator of the document is well established by showing the public certificate associated with the private key used by that person in signing that document. SHA-2 used in signing the documents.