**Digital Certificates (Digi Locker) Vs BlockChain Based Certificates**

**Digital Certificates**

* Digital Certificates are stored in a centralized database, prone to failure.
* Digital Certificates without digital signatures are extremely easy to forge
* Registries of digital certificates are prone to large scale data leaks
* Keeping digital records safe requires sophisticated and multi-tier backup systems which are prone to failure
* The use of digital signatures requires the participation of third-party providers that guarantee the integrity of the transaction; they exert control on every aspect of the certification and verification processes, which can lead to abuses.
* There is no universally accepted open standard for digital signatures, leading to certificates that can only be verified within the context of proprietary software.
* It is easy to erase electronic records unless very sophisticated security and backup systems are established.
* If the digital record fails, the certificate loses its value because of the lack of intrinsic value.
* Digital certificates are liable to be downloaded in bulk.
* Maintaining IT infrastructure for Digital Certificates is very expensive and ever-increasing.
* Verifying the digital records are not instant, takes considerable time up to 24 hours, and may increase.
* Verifying the digital records requires authorization from the stack holder(s), prone to failures, less reliable.
* Verifying the digital records may not be possible if issuing organization is no more available or stack holders not willing.

**Blockchain Certificates**

* Blockchain Certificates are stored in a decentralized database over the cloud infrastructure.
* Impossible to change the records (immutable) as not stored in a single place.
* Validation and Verification are possible even if the issuing organization is no longer exists.
* Verification is very easy, anyone having access to Blockchain can verify the certificates.
* They are verified instantly, using a QR Code
* Option not to publish the certificate itself, preserving its privacy
* Each certificate will contain a unique digital signature (Hash, which can't be tampered with and is unique).
* Which is stored in a public database (the blockchain) and identical in thousands of computers around the world.
* The digital signature is linked with a blockchain address. In any case, the original document is tampered with and regenerated, the certificate fails during the verification process.
* No chance of forging.
* The registry of certificates issued and received in a blockchain can only be destroyed if each and every one of the existing copies are destroyed in thousands of computers that host this technology.