Please name 2 more other than the 4 types of certificates mentioned above.
Please provide examples of blockchain applications other than certificates
Why do we need trust of the Certificate?
Who should be trusted?
What certificates in education can be implemented with blockchain technology?
Mention other advantages and disadvantages, apart from those described on the previous Blockchain Certificates!

Jawab :
-Achievement of learning outcomes, irrespective of the form learning
- The Competence of teacher
- A learning Process undertaken by a learner, irrespective of the form of the learning
- An educational organization or course meeting certain quality criteria
- An accreditation body being authorized to issue certifications.
- Single Domain SSL Certificates
- Wildcard SSL Certificates.
- Multi-Domain SSL Certificates (MDC)
- Domain Validation SSL Certificates.
- Organization Validation SSL Certificates.
- Extended Validation SSL Certificates.

A. Blockchain in Healthcare industry
B. Blockchain in Goverment Organizations
C. Blockchain in trade finance Industry
D. Blockchain in other industries worldwide

A Certification of Trust is a legal document that can be used to certify both the existence of a Trust, as well as to prove a Trustee's legal authority to act. It's shorter than the actual Trust document, and it can offer pertinent information without making every aspect of the Trust public.

4. The Claim, the issuer, Evidence, a recipient, a certificate, Signature

5. Certificate for learners, Certificate for accreditation, Certificate for tracking intellectual property, Certificate for financial matters.

6. Blockchain Certificate advantages :
They need fewer resources for their issuance and maintenance.
They can be revoked by the issuing institution.
They are more difficult to modify or insert false data.
Blockchain Certificate disadvantages:
Without the use of digital signatures, they are easy to forge;
The use of digital signatures requires 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.