How OpenCerts Works

OpenCerts is a blockchain-based[1] platform developed by SkillsFuture Singapore (SSG), Government Technology Agency (GovTech), Ngee Ann Polytechnic (NP), and the Ministry of Education (MOE). The platform offers an easy and reliable way to issue and validate certificates that are tamper-resistant.

Certificates issued by OpenCerts contain the following information:

   I.   Certificate Name: Name of completed education course
   II. Issuer's Identity: Name of institution that published the digital certificate
   III. Transcript: Modules and results achieved
   IV. Recipient's Identity: Name of student who received the digital certificate
   V.   Tamper-proof Signature: A means of verifying the authenticity of the certificate
   VI. Metadata: Additional data that do not fit into the standard categories of Information

When an OpenCerts certificate is issued, a unique code is published onto the blockchain. A cryptographic proof[2] is appended onto the certificate data and sent to the individual recipient. During verification, the certificate data is checked against its proof for signs of tampering and against the code on the blockchain for validity.

Built on open source and standards, educational institutions can easily create digital versions of every certificate that has been or will be issued, and publish them on a public ledger[3].

Scan the QR code or visit opencerts.io to find out more about the technology and process behind OpenCerts.

---

[1] Blockchain is a tool for digitally recording transactions, be it between a buyer and seller, or in this case an educational institution and its graduates. A public blockchain is neither owned nor maintained by an individual, and instead decentralised. This ensures that records made on it cannot be altered or destroyed by a single person.

[2] A cryptographic proof is a method by which one party can prove to another party that they know a value of the proof without being aware of any other details within the documentation.

[3] Public ledger is a database that is consensually shared and synced across multiple parties.