LEARNING MACHINE

Frequently Asked Questions

1. Are there reasons to use Blockchain as opposed to just hashing and encryption?

The main reason to use blockchain technology is the independent verification it provides. By "independent verification," I mean that a document can be verified instantly without needing to check with the issuing institution or with a software vendor. Currently, most digital document verification, even using hashing or encryption, is still hosted by the issuer or vendor--you have to check with them or visit their website to verify the documents. But if the verification website goes down or stops working, or the issuer or vendor goes out of business, you lose the ability to verify the digital documents they have issued. With Blockcerts, you can simply visit blockcerts.org and upload any document issued by any institution anywhere in the world and have it instantly verified in a manner you know you can trust.

2. What is the importance of on-chain vs. off-chain data?

On-chain data is stored directly on the blockchain; off-chain data is store off of the blockchain (for example, on your hard drive or in the cloud) but can be verified using a blockchain. A Blockcert is a document that is stored off-chain but can be verified using a blockchain because of how it is issued. You can store a Blockcert off-chain by saving the file or hosting it at a link that can be accessed by others for easy viewing, sharing, and verification.

When using a public blockchain like Bitcoin or Ethereum, no documents or personally-identifiable information are stored on chain. All that is stored on chain is a one-way cryptographic hash (digital fingerprint) of the document, which cannot be used to reconstruct the document contents. Other data stored on-chain are the public keys of issuer and recipients (these serve as identifiers when linked to a known identity) and the date and time of the transaction. None of this data can be altered. This makes blockchains useful for decentralized verification by a system, like Blockcerts, which can use the Blockcert document to reference the blockchain transaction. Immutability is also why blockchains make it very difficult to fraudulently issue certificates.

3. Can private data be deleted forever?

Yes. If a recipient or issuer wants to delete the off-chain Blockcert, they can simply delete the file and take down the link. It is impossible to recover the certificate or any data from the blockchain. Remember: the Blockcert references the blockchain, but the blockchain does not reference the Blockcert.

4. How do you verify the identity of a Blockcert issuer?

There are three ways to verify the identity of a Blockcert issuer:

> **1. Check their public key.**
> The issuer's public key is stored both on chain and in the Blockcert file. It is in the interest of the issuing institution to publicize their public key, so everyone can know what records legitimately were issued by them. This is why Learning Machine builds public key registries for our customers--registries allow you to easily verify that, for example, this is the University of X's public key and no one else's.
>
> **2. Check their digital signature.**
> In addition to checking an issuer's public key, the Blockcerts Universal Verifier always checks the issuer signature on a credential to make sure that the private key used by the issuing institution's to digitally sign the credential corresponds to the public key in the credential and on the chain. There is a unique cryptographic relationship between public and private key which identifies the issuer and makes sure no one is forging credentials with someone else's public key.
>
> **3. Check the domain hosting the certificate.**
> Finally, institutions may host the Blockcerts they have issued on their own domains. A verifier can immediately see whether the Blockcert is hosted at the issuing institution's official domain or on some other domain.

Note that you can include written issuer signatures in a Blockcert as well to preserve the traditional look and feel of a paper certificate. Blockcerts are JSON files, meaning they store all the image data, including signature data, inside. However, Blockcerts issuer identity verification doesn't rely on a written signature, since that can be easily forged. Instead, issuer identity verification happens cryptographically, through verifying the "digital signature:" the public/ private keypair unique to the issuer.

5. How do you verify the identity of a Blockcert recipient?

In the recipient’s case, the recipient has a different public key for each issuing institution from which they receive documents. The recipient can choose whether or not to publicize their public keys, linking them to a known identity. (Either way, public keys cannot be used to access any private documents or data.) A recipient can also use their Blockcerts Wallet to countersign any credential they have received with their private key, thus proving that they are the individual to whom this credential was issued.

6. Can Learning Machine access user data, since it flows in and out of the service layer you provide?

Learning Machine is a software application institutions can use to issue Blockcerts at scale. Institutions using Learning Machine upload student data to their private Learning Machine account either via CSV or API. Under GDPR, this makes Learning Machine a Data Processor. Like any Software as a Service (SaaS) company, Learning Machine has data privacy protections in place to safeguard customers’ data. This data can also be permanently deleted either after a specified time period or upon request.

7. If, unfortunately, Learning Machine doesn't exist anymore, how do learners and issuers access their data on Blockchain?

Every Blockcert is issued as a digital document and sent directly to the recipient. Issuers also keep a copy of every Blockcert they issue. The Blockcert document references the blockchain transaction which anchored its fingerprint to the blockchain. The Blockcert file can be stored anywhere the issuer and recipient choose, even printed out as a PDF with a QR code. The document can be independently verified using the open source Blockcerts Universal Verifier even if Learning Machine or any other software vendor issuing Blockcerts ceases to exist. You can try out the Blockcerts Universal Verifier at blockcerts.org.

8. When a learner shares his or her credential on social media or with an employer, do others need a private key to see it?

No. Issuers can host their issued Blockcerts as a public link. If the recipient chooses to share this link, the person with the link can verify the Blockcert with no additional software needed.

9. For users of the Learning Machine Issuing System, what does training include?

The first training session is a one-hour workshop to walk you and your team — as many people as you choose to invite on your end — through every step of the account setup process. A Learning Machine implementation specialist will guide you through the process of test issuing credentials to everyone who provides an email address for the workshop. Subsequent training sessions can also be arranged virtually.

10. Do you do the workspace configuration or do we do the configuration ourselves?

Learning Machine configures customer issuing workspaces. We will, however, need a liaison in your IT department to work with during the setup process and on occasional account maintenance tasks. You also have the flexibility to configure many of your account settings on your own, should you choose to do so.

11. How long does account configuration usually take?

About 30 days, but it can go faster.

12. How many people do we need to service our account?

You will need to identify a few account administrators who will help with different aspects of the setup and maintenance process. They are:

> **Domain Administrator & SMTP Administrator.**
> Often these are the same person, your IT Department lead. They should have access to your institution's DNS service and to your email provider.
>
> **Organization Administrator & Recipient Contact.**
> Oversees all account issuing activity. Can also design credentials and manage recipient data. Determines who has access to the system and what permissions they have. This can also be the person recipients reach out to if they have questions or run into any issues (you may choose to delegate this role to someone else).

Communications Lead.
This person will work with us to raise awareness about Blockcerts with your student body and internal stakeholders. Will will send them a booklet of resources they can use to design email campaigns, website content, FAQ's, videos, and other materials.

13. Is there technical documentation about Learning Machine?

Yes! Please reference the following document:

Learning Machine Technical Requirements and User Guide (https://www.learningmachine.com/user-guide/)

14. Do we need specialized people to use Learning Machine?

No. The Learning Machine Issuing System is a web-based application and can be used by anyone with basic administrative skills. Anyone with a smartphone can receive Blockcerts through the free Blockcerts Wallet (available for both iOS and Android). Verifiers of credentials just need to click a link to access the Blockcert through any web browser. To verify the Blockcert, they can click the "Verify" button on the hosted credential or upload the Blockcert file to the Universal Verifier at Blockcerts.org. Verification is instant and free.

15. Do we need to know how to program Blockchain to use Blockcerts?

Not at all! You don't need to buy any tokens, run a node, or even need to know what the blockchain is to immediately see the value. It's super easy to use for issuers, recipients, and verifiers.

16. How long does issuing a credential take?

Issuing a high-stakes certificate to a blockchain can be very fast or take significant time depending on the institution's process for issuing credentials. The issuing process involves the following steps:

1. Designing your certificate
2. Importing your recipient data and mapping it to the certificate
3. Reviewing and approving the certificate template
4. Reviewing and approving the certificate data
5. Scheduling a date and time for certificate issuance
6. Issuing the certificate

Once issuing is initiated, the amount of time it takes depends on the block confirmation times and network traffic of the blockchain being used. Network traffic and block confirmation times are different for different blockchains (Bitcoin, Ethereum, Litecoin, Hyperledger, etc.), but virtually all transactions are processed within the same day, usually within an hour.