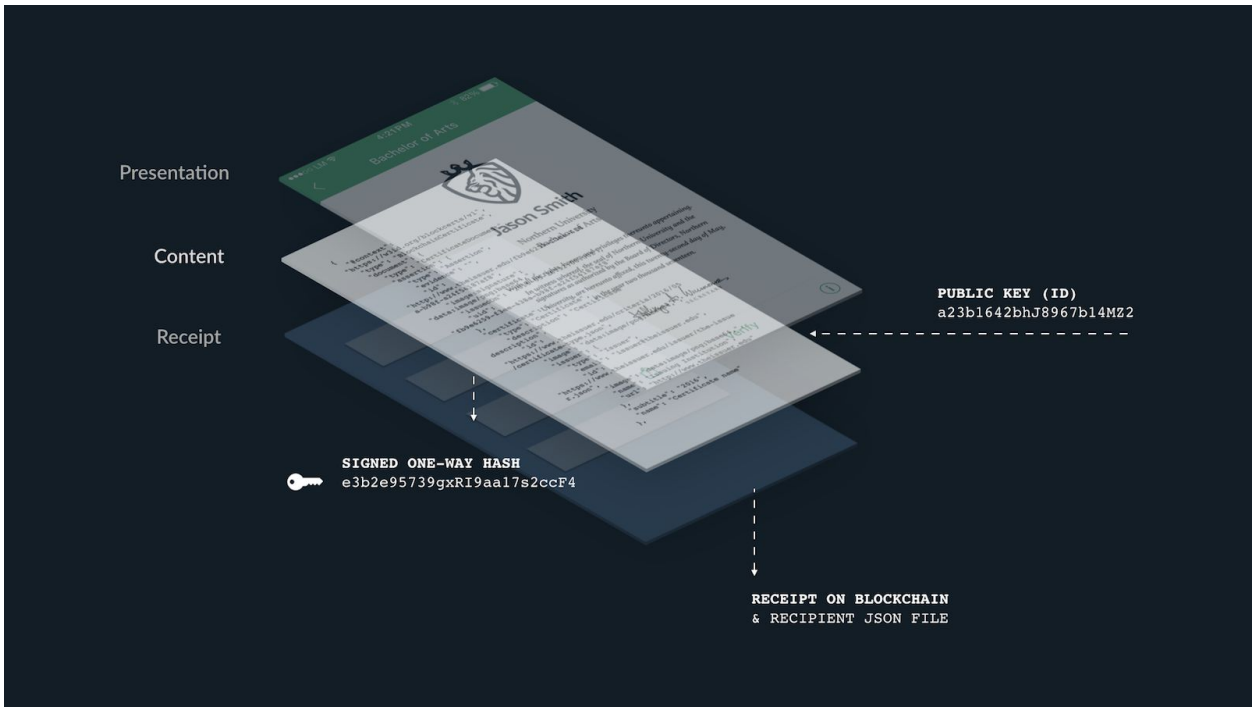
LEARN ING MA CHINE

Tamper-proof Records

Tamper-proof records are digital files that have been cryptographically signed by an issuer and registered on the blockchain. Each record contains a recipient's public key, they can demonstrate ownership of the record without any dependence upon a certificate authority.

- The **Presentation** layer can be styled to mimic the look of traditional records.
- The **Content** layer is code that contains all of the data and images.
- The **Receipt** contains proof of the transaction, which includes a signed hash of the content.



The verification process compares information on the recipient's record to the receipt stored on the blockchain. When everything matches, that record is verified.

Efficiency

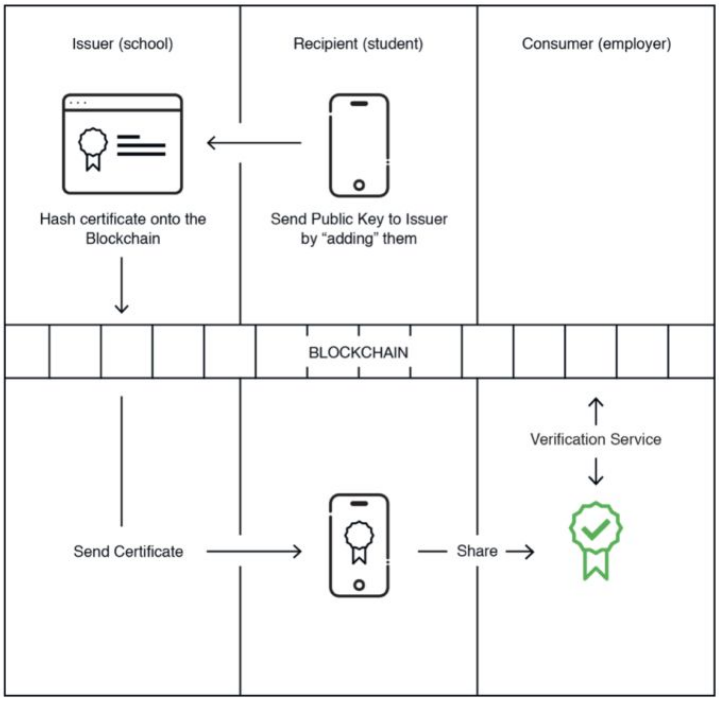
Issuance is executed in batches via a merkle tree to preserve computational efficiency and cost effectiveness. Think of this as an email campaign — you can design templates with variables which are filled in with data from thousands of recipients when you "send." Each issuing event creates a single transaction on the blockchain, regardless of the number records, via the merkle root.

Verification

The blockchain acts as a notary because it logs the transaction of you giving recipients official records on a certain date and time. A record of this transaction can be checked at any time to ensure nothing has been altered since that date. An independent blockchain lookup service will find the transaction ID and then verify the issuer keys, the recipient keys, and that the record is still valid.

Transmission

Once an institution has retrieved a recipient's public key(s), they encode it into a record issued to that person. The end result is simply a digital file (json) that has all the necessary information to check it against the transaction information stored on the blockchain. This record can be shared as an attachment, or as a link if issuers choose to provide hosting for the record.



Advantages Over Traditional PKI Techniques

Using the blockchain as a notary creates several benefits beyond traditional PKI. Beyond removing the dependence upon any certificate authority or trusted third party, the blockchain provides independent time stamping, which creates significant security benefits. A reliable timestamp is clearly important in cases where credentials expire, but it is also critical for a practical reason — the issuer must be able to rotate issuing keys on a regular basis, both as part of security best practices, but more critically in response to a key leak.

> **To determine that a record was issued by a specific issuer *when* the issuing key was valid requires knowledge of an independent timestamp.**

If a private key is leaked, there is nothing to prevent an attacker from issuing fake records and backdating content. Even if an issuer publicly revokes those records, an independent verifier would not know the difference between a valid and invalid record unless there were some additional authority attesting to when the transaction took place.

What about the possibility of an attack?

On the Bitcoin blockchain, there is no incentive for such an attack to take place and very limited power if it indeed occurred. An attacker who established control with over 50% of network computing would not be able to edit the past; they would gain a limited amount of power over a small segment of current transactions. However, attempting this attack would destroy the value of their mining equipment, since it would result in protocol changes that make their equipment useless. Finally, the number of copies make it's history easy to reconstitute if ever needed.

--