

基于区块链的学位证书认证

Blockchain-Based Academic Credentials

背景与现状

1. 传统学位证书可信吗？

学校是学生信息的唯一记录保持者。如果学生想要访问或分享他们的官方记录，他们必须进行一个缓慢，复杂，通常是昂贵的过程。

2. 教育正在改变。

在线学习和基于能力的计划越来越受欢迎。这种情况被越来越多的获得认证的教育机构所放大，这些机构远远超过传统学校。这导致难以管理的教育要求的激增，并且在政策和技术方面提出了许多新的问题。



How to build trust in the Internet
of academic credentialing?

我们需要什么样的学位证书？

- 安全 Safe
 - 防篡改 Tamper-proof
 - 可信任 Trusted
 - 保护隐私 Protecting privacy
-
- The diagram shows four requirements listed on the left, each with a line that converges into a single arrow pointing to the text '区块链?' (Blockchain?) on the right. The requirements are: 安全 Safe, 防篡改 Tamper-proof, 可信任 Trusted, and 保护隐私 Protecting privacy. The text '区块链?' is written in red.
- 区块链？

区块链能用于学位证书认证吗？

区块链本身只是一个交易的分类帐。在金钱的情况下，它是记录金融交易：谁发送交易，谁收到交易，交易额是多少。这种模式使它非常适合记录学术资格证书，因为学位证书记录了相同的基本事物：谁发布学位证书，谁收到学位证书，以及内容的单向哈希，以后可以用于验证。学术成就只是另一种价值。

所以，区块链非常适合用于学位证书认证。

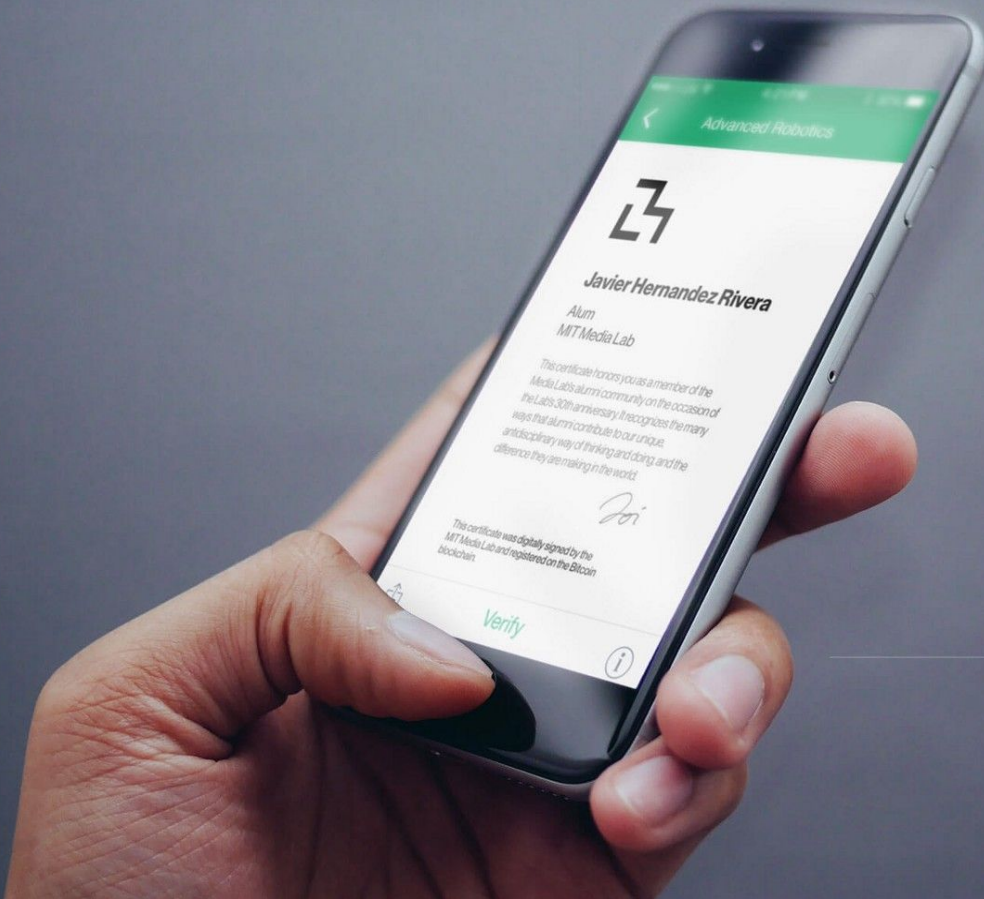
“Using the blockchain and strong cryptography, it is now possible to create a certification infrastructure that puts us in control of the full record of our achievements and accomplishments.”

—— PHILIPP SCHMIDT, MIT MEDIA LAB

“Own and share your Achievements. With the blockchain, your official records are now yours forever. Receive them once, share and verify them for a lifetime.”

—— BLOCKCERTS WEBSITE





Step 1 of 5
Computing SHA256 digest of local certificate [DONE]

Step 2 of 5
Fetching hash in OP_RETURN field [DONE]

Step 3 of 5
Comparing local and blockchain hashes [PASS]

Step 4 of 5
Checking MIT signature [PASS]

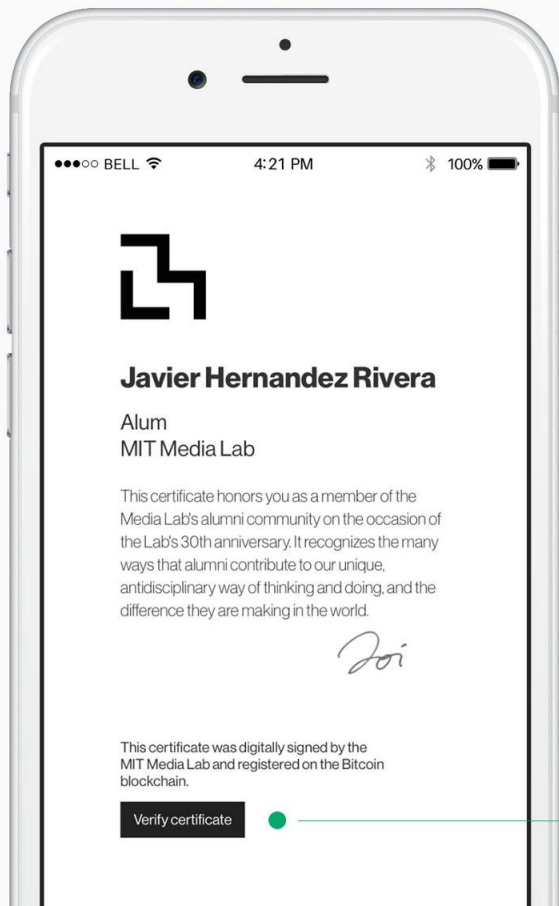
Step 5 of 5
Checking not revoked by issuer [PASS]



VERIFIED

Public Key
1HYPitzbwR83M3Smw6Gws5XeQzBWwJAEes

Blockchain Address
4bf64ff1517554dac3496e9da0a28ca9ae492682b0898e384ea17e7f90ee1295



Step 1 of 5

Computing SHA256 digest of local certificate [DONE]

Step 2 of 5

Fetching hash in OP_RETURN field [DONE]

Step 3 of 5

Comparing local and blockchain hashes [PASS]

Step 4 of 5

Checking MIT signature [PASS]

Step 5 of 5

Checking not revoked by issuer [PASS]

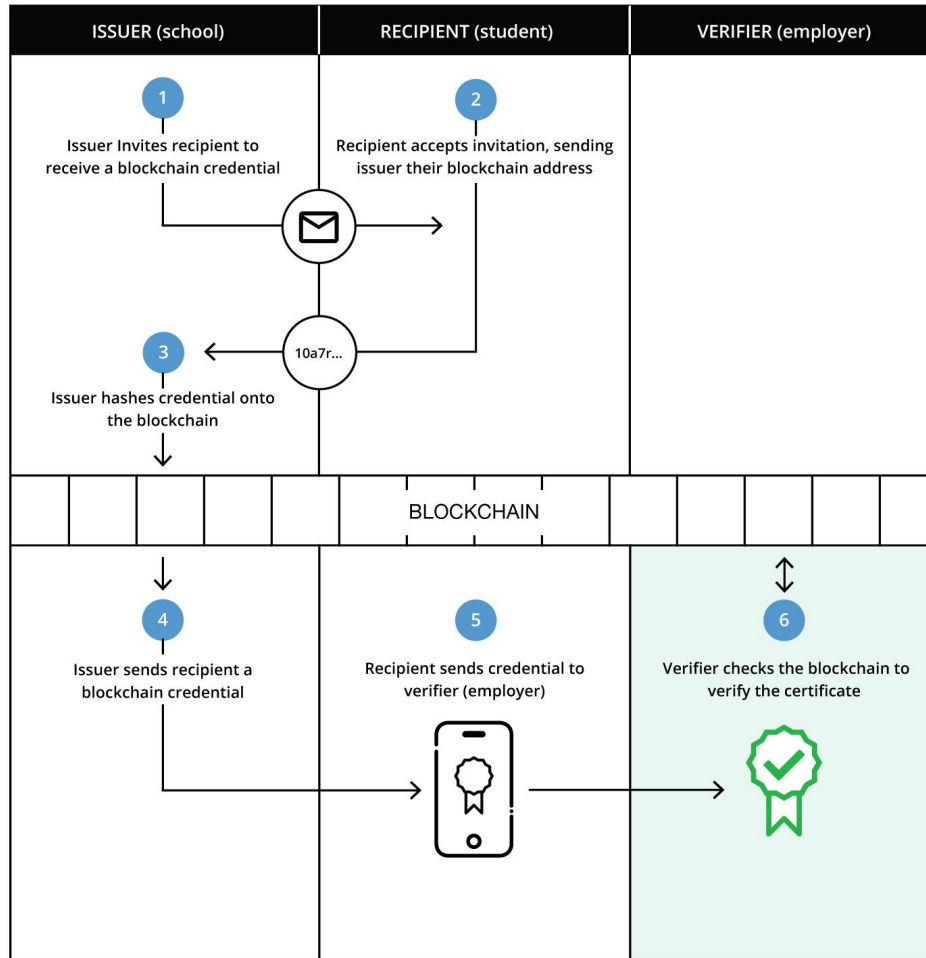


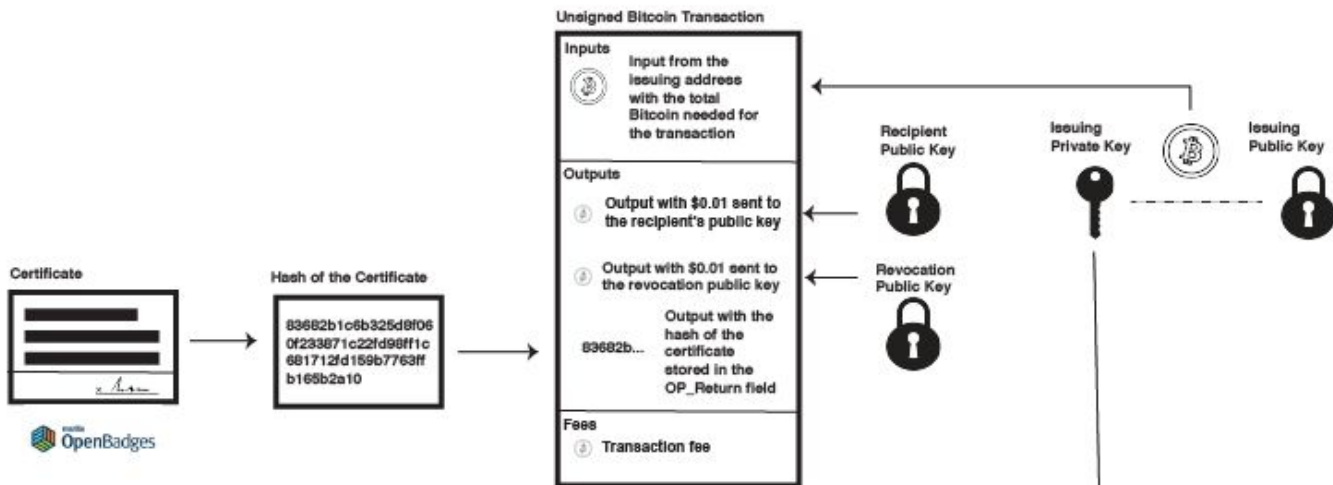
Public Key

1HYPitzbwR83M3Smw6GWs5XeQzBW0JAEeS

Blockchain Address

48f64ff1517554dac3496e9da0a28ca0ae492682b0898e38a4e17e7f90ee1295






Blockchain



Unsigned Bitcoin Transaction

Inputs	
	Input from the issuing address with the total Bitcoin needed for the transaction
Outputs	
①	Output with \$0.01 sent to the recipient's public key
②	Output with \$0.01 sent to the revocation public key
③	Output with the hash of the certificate stored in the OP_Return field 83682b...
Fees	
④	Transaction fee

Input:

Minimal amount of bitcoin (currently ~\$.80 USD) from Issuer's Bitcoin address

Outputs:

OP_RETURN field, storing a hash of the batch of certificates

Optional: change to an issuer address

OP_RETURN code :

The OP_RETURN code was introduced by the Bitcoin core developers to address the increasing desire of people to store non-financial data.

证书能撤销吗？

Revocation in current system (version 1) is **not actually a deletion** (no information can ever be deleted from the blockchain) but it is a flag that either the issuer or the recipient can set to signal that they don't acknowledge the certificate to be valid. In more technical terms, we create two outputs containing \$0.01, with one assigned to the recipient and the other to the issuer. To revoke a certificate, either party just spends the output they control.

for version 2 the system is exploring other revocation approaches, which could reduce the ability for viewers to show or validate revoked certificates.

我的隐私会被公开吗？

Users should be able to disclose this information to one employer, without having to also share it with every other employer.

The system does this by **hashing the certificate** (which contains a learner's personal information) and only placing the hash on the blockchain. If someone wants to verify the validity of a certificate, they need the learner to disclose both the certificate itself and where the hash of the certificate is located on the blockchain.

真的能百分百保密吗？其实并不是！
It needs to make traceability much harder.

认证一张证书的成本是多少？

A Bitcoin transaction is determined by the size of the transaction and the transaction fee.

Blockcerts transaction sizes are static and small – they add a single fixed-size OP_RETURN output on top of a standard single-input, single-output transaction. This is true no matter the number of certificates in a batch.

So the cost to issue a batch of Blockcerts is largely influenced by the transaction fee, which is a fee paid to miners to ensure timely mining of transactions. In the cert-issuer project, the transaction fee is configurable. The default value was selected as a higher value to reduce wait time. This setting can be overridden in the config file to reduce the cost, but it may result in long waits.

证书认证的效率真的可靠吗？

The idea was clear, but this prototype had barriers preventing much use in the real world. For instance, it didn't take into account how to efficiently issue thousands of certificates at the same time in a manner that was computationally efficient or cost effective.

区块链面临**效率瓶颈**，处理能力低是目前区块链的一个致命问题，也是以区块链为底层技术的BLOCKCERTS必须要面对的问题。

除了上述缺陷，我们还需要哪些改进？

1. each certificate corresponds to a transaction on the Bitcoin blockchain. It is unnecessarily wasteful.
2. Selective disclosure of information is needed.

Merkle tree!