A New Academic Certificate Authentication Using Blockchain Technology

better security over Blockcerts V2.0

Student: Rujia Li [1]
Supervisor: David Galindo[1]

([1]University of Birmingham)

August 21, 2017

CONTENTS

Introduction

Scope of work

Methodology

Implementation

Conclusion

Introduction

- ✓ Background
- ✓ Traditional Authentication
- ✓ BlockCerts & Blockchain
- ✓ BlockCerts mechanism

Background

Counterfeit academic certificates have been a longstanding issue in the academic community. Overall, there are two broad types of degree fraud[1].

Bogus institution

Fake certificate which issued by bogus universities and degree mills

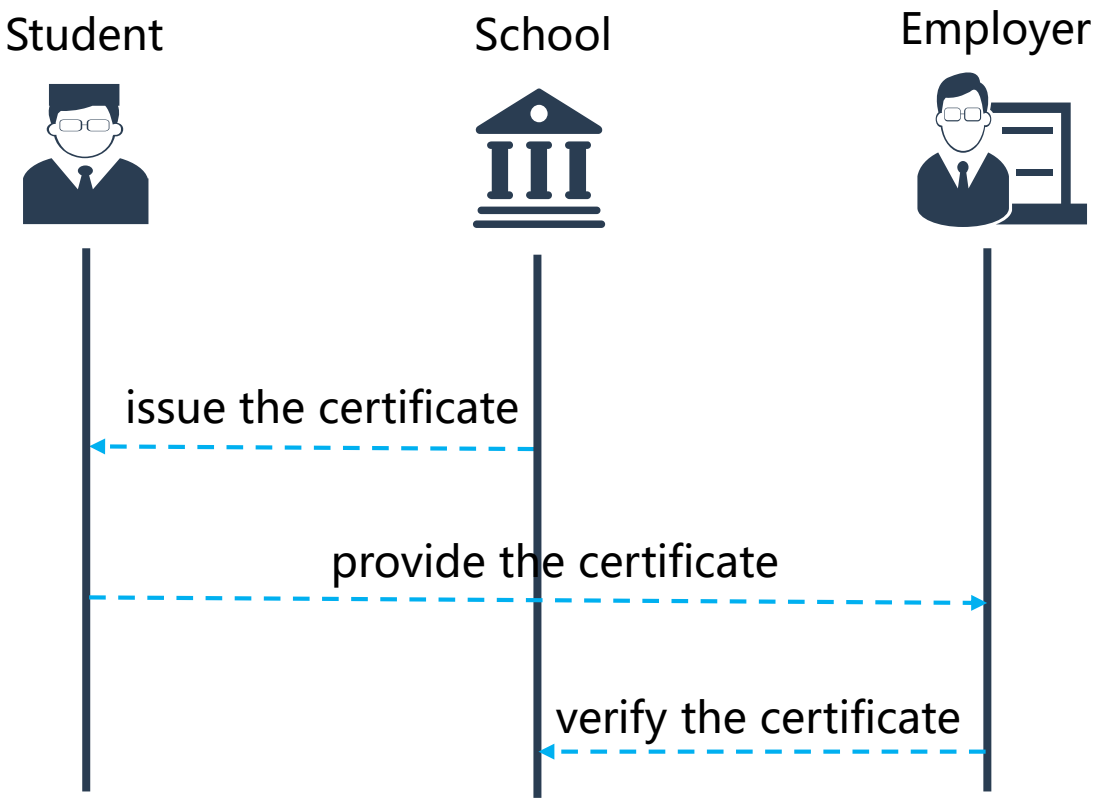
Individuals fraud

Fake certificate on real institution which fraud committed by individuals

Key Words: **Fake certificate, Authentication**

1.http://cdn.prospects.ac.uk/2.0.1/pdf/HEDD%20degree%20fraud.pdf

Traditional Authentication

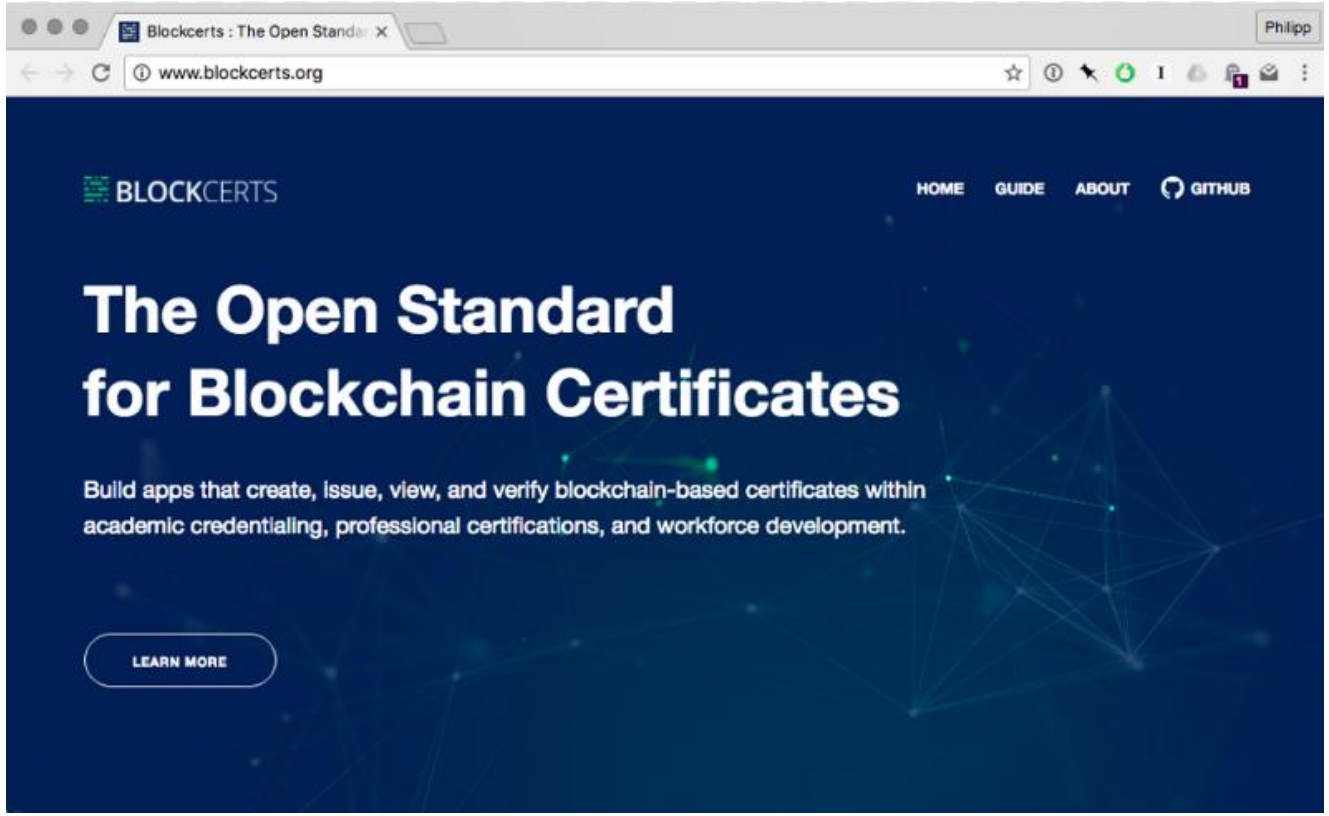


Costly
It is costly to interoperate and collaborate between different business.

Fragile
Completely depend on the school, A single point of failure can cause the whole process to fail.

Centralized
The data is centralized and the verification service must expose to outside which increased attack surface.

BlockCerts



MIT Media Lab released a decentralized credentialing system for academic, professional, and workforce credentialing called Blockchain Certificates in Auguste, 2016 [2]

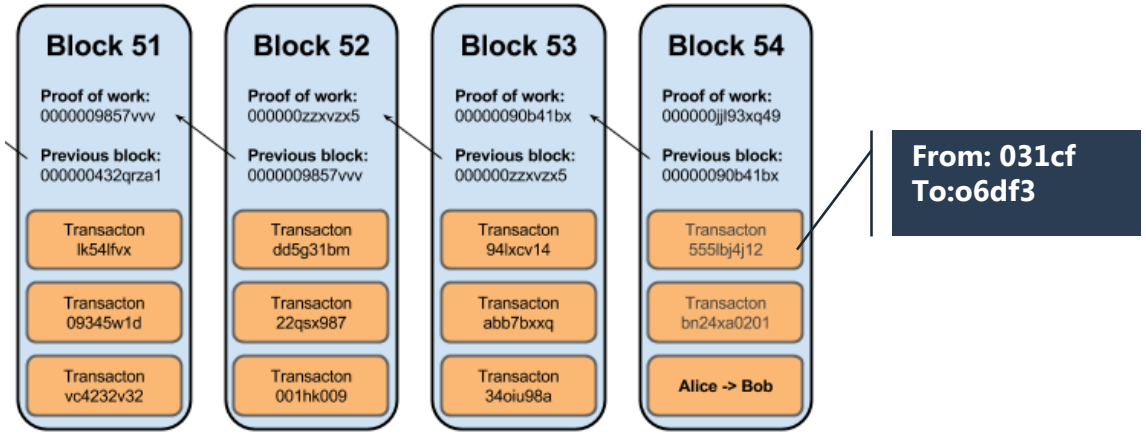
The Bitcoin Blockchain acts as the provider of trust, and credentials are tamper-resistant and verifiable.

2. https://news.bitcoin.com/mit-blockcerts-certification-bitcoin/

Blockchain

A blockchain is a distributed database that maintains a keep-growing list of ordered records called block [3].

Each block contains a header and a list of transactions TX_i . Each header includes a timestamp T_i, a link to a previous block H_{i-1} and nonce N_i . [4]



The blockchain is cryptographically secured, for every round, the miner need find a random number to meet the computing difficulty D_i , and this progress is called the proof of work (POW) [5].

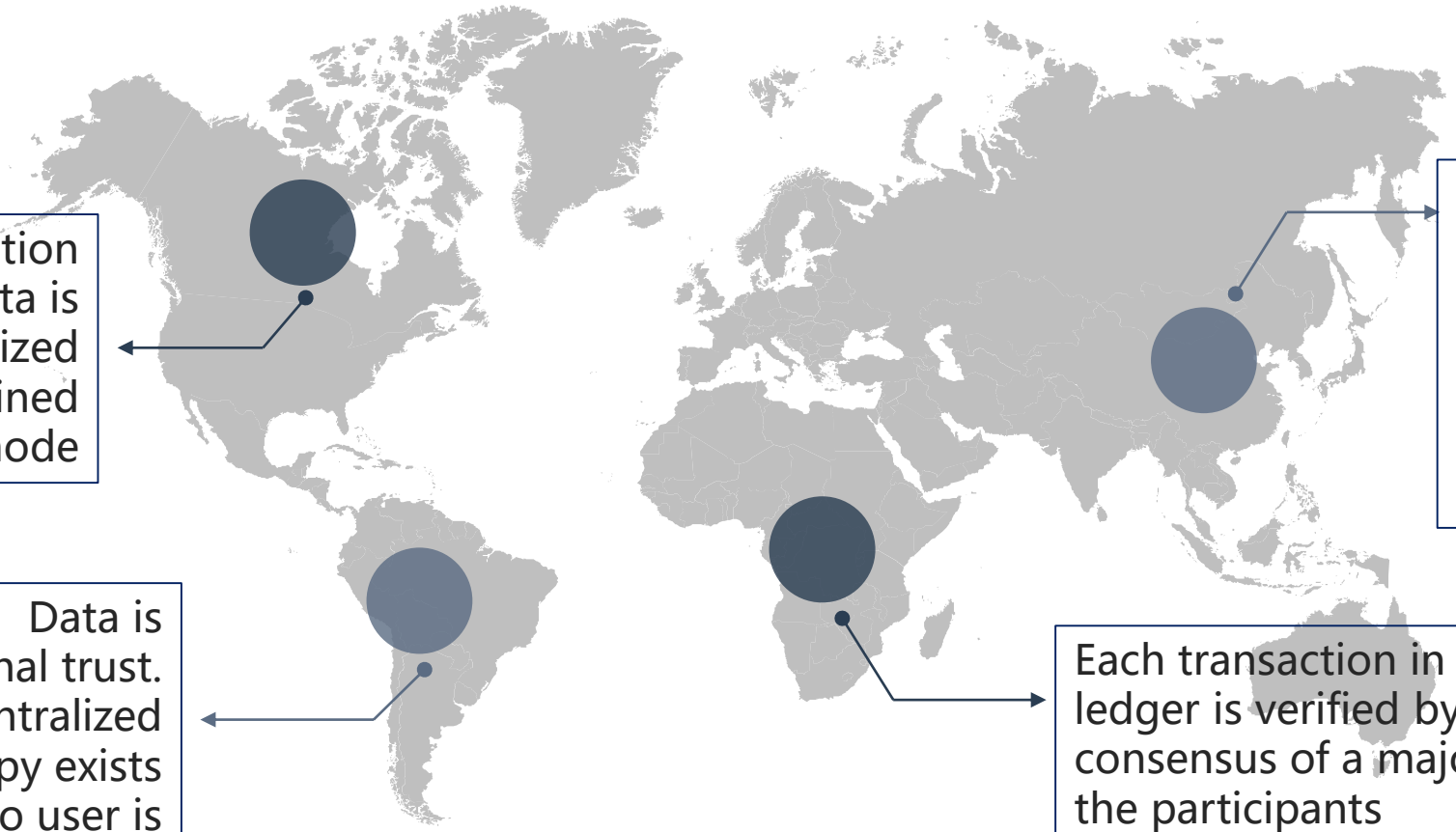
$$f(D_i) > \text{SHA-256}(\text{SHA-256}(H_{i-1} \| T_i \| TX_i \| N_i \|)))$$

3.https://en.wikipedia.org/wiki/Blockchain

4 "Bitcoins In Space". 2017. accessed April 2, 2017, Virgin. https://www.virgin.com/richardbranson/bitcoins-in-space.

5 Alex Biryukov, Dmitry Khovratovich and Ivan Pustogarov. 2014. "Deanonymisation Of Clients In Bitcoin P2P Network". 2014 ACM SIGSAC Conference On Computer And Communications Security, 15-29.

Blockchain feature



The transaction data is decentralized and maintained on every node

Transaction history cannot be changed unless redoing all Proof of Work of all blocks in the chain

Data is computational trust. No centralized "official" copy exists and no user is "trusted"

Each transaction in the public ledger is verified by consensus of a majority of the participants

BlockCerts Mechanism

Alice send 5 BTC to Tom with a note "Thank you"

Alice → Tom 5BTC

Merkle root

Certificate hash

LEDGER

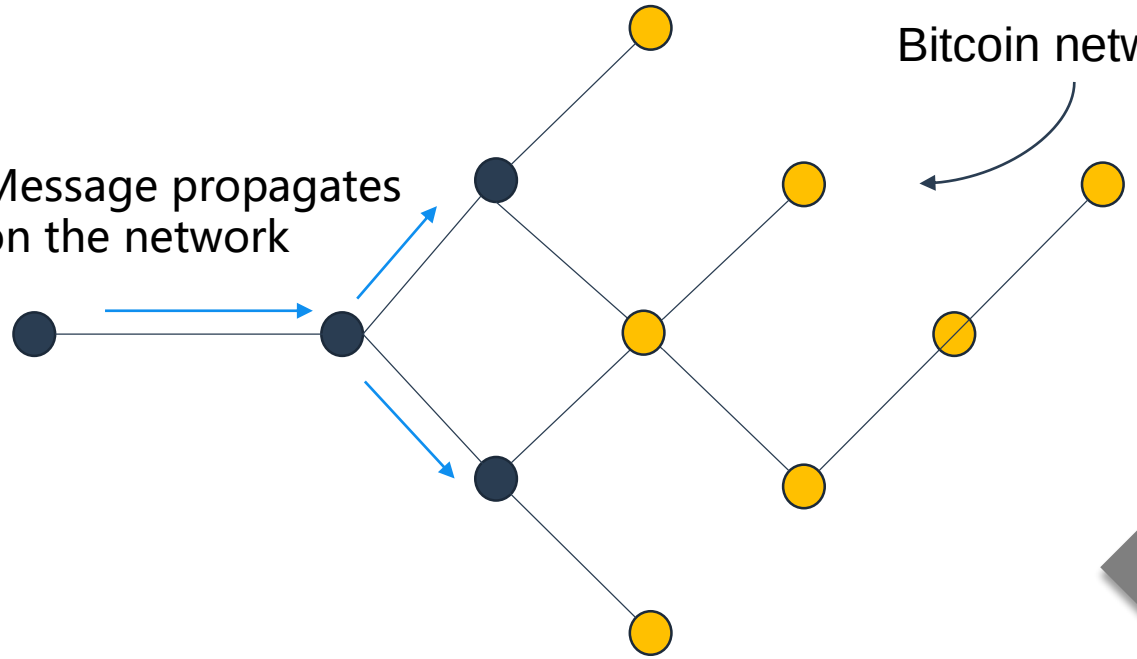
Alice	10
Tom	5
Rujia	4
Alex	8

LEDGER

Alice	5
Tom	10
Rujia	4
Alex	8

Message propagates on the network

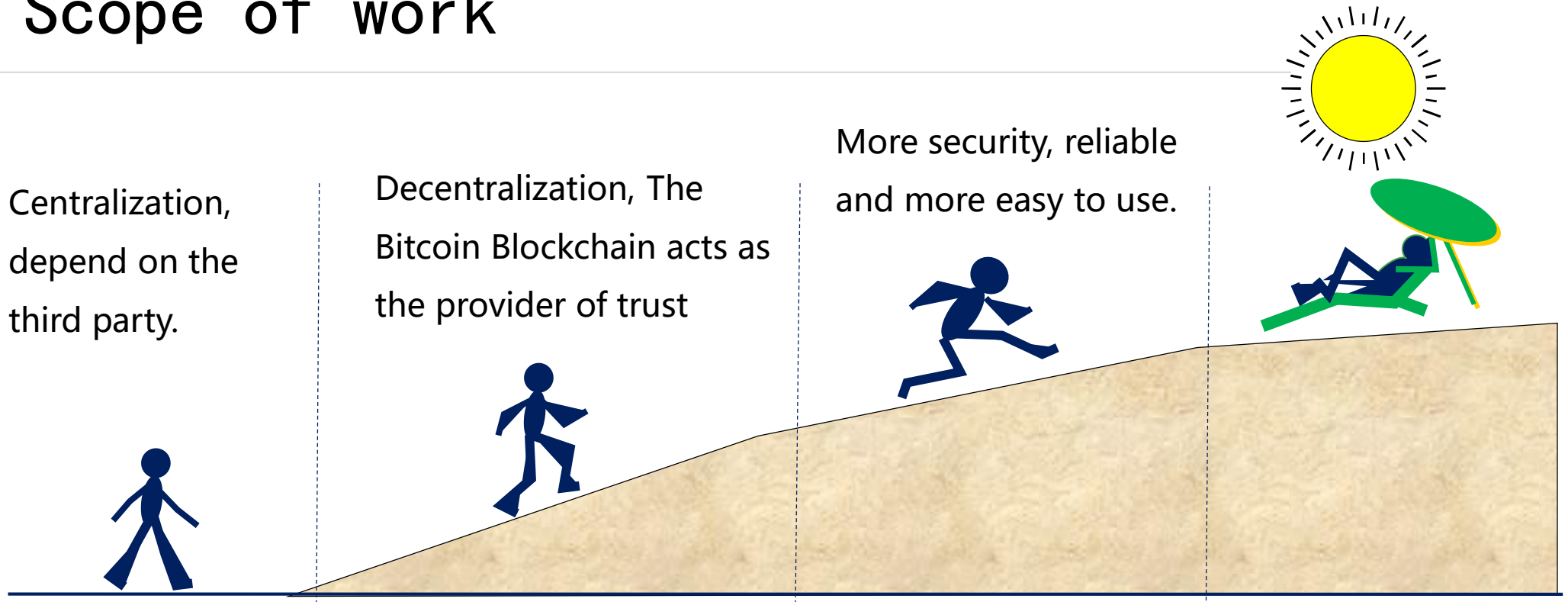
Bitcoin network



Scope of work

- ✓ Scope of work
- ✓ Project stage

Scope of work



Traditional Authentication

BlockCerts Authentication

BlockCerts Authentication
+
Cryptography protocol
+
Extend the standard

Future

Methodology

- ✓ Democratic Multi-signature issuing
- ✓ Security Certificate Revocation
- ✓ Security Federated Identity

Blockcerts & BTCert (Multi-Signature)

Pay to Public Key

One public key, combined with one private key pairs, is utilized to authenticate the identity of an issuer. Thus, anyone who possesses the private key can publish legitimate digital certificates

problem: key physical secure

problem: democracy issued

problem: single point of failure

problem: corruption and fraud

VS

Multi-signature

It is the multi-signature scripts that set a criterion where N public keys are recorded in the scripts and at least M of them have to provide signatures to release the encumbrance

solution : distributed storage

solution: the majority of key owner signed

solution : more than one person agreed

Multi-Signature

the Signature generating Algorithm

Algorithm: Generating the Signature Stack

Input: The condition we defined in Initialization Phase

Input: An empty Stack S

Output: The Signature List Stack

1: κ = the prefix OP_0
2: for i ← [1,M] do
3: $K_i = K_i < n$
4: $R \leftarrow (r_1, r_2) = kG$
5: $r \leftarrow r1 \bmod n$
6: $s \leftarrow k^{-1}(F(m)+dr)$
7: $o_i \leftarrow (r, s)$
8: end for

Return: S = push ($\kappa + o_i$)

After this progress, any combination of M signatures from the private keys corresponding to the N listed public keys will generate in a signature stack as follow.

OP_0 <Signature 0> <Signature 1>···<Signature M-1><Signature M>

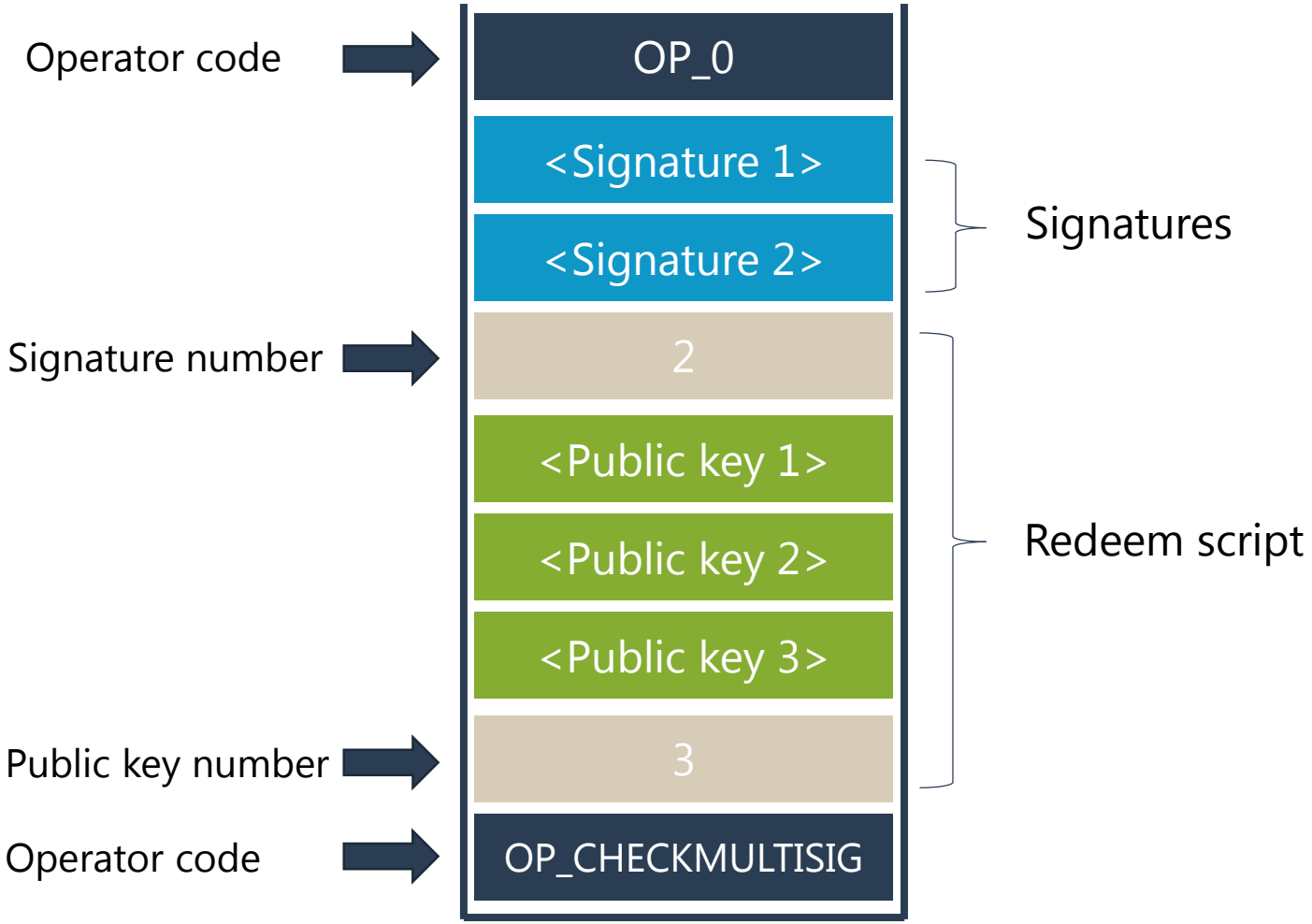
The multi-signature script is stack-based, and processed from left to right. It is purposefully not Turing-complete, with no loops. [6]

This signature scheme uses a standard ECDSA signature but put all the signed result in one stack

6 M. Antonopoulos, Andreas. 2017. Mastering Bitcoin. 1st ed. O'Reilly Media.

Multi-Signature

The signature verifying algorithm



The validation script is a combination of signature lists and the redeem script, which allows being split as an independent unit to verify.

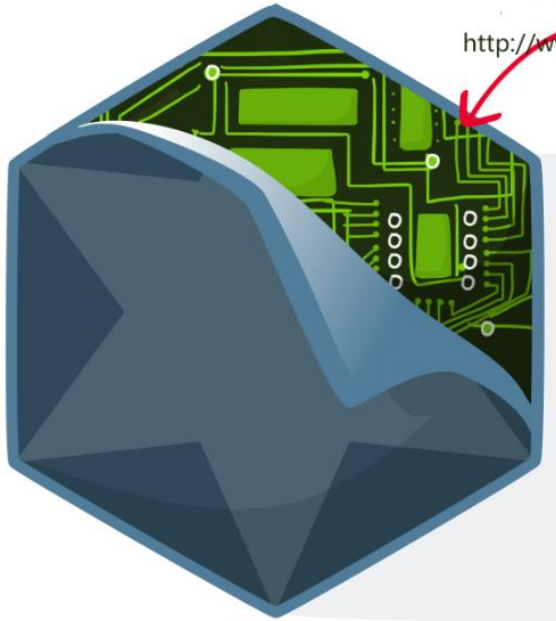
Each independent unit holds a standard ECDSA signature validation

https://en.bitcoin.it/wiki/Script

Blockcerts & BTCert (Certificate Revocation)

Revocation list(URL)

http://www.bham.ac.uk/revocation_list.html



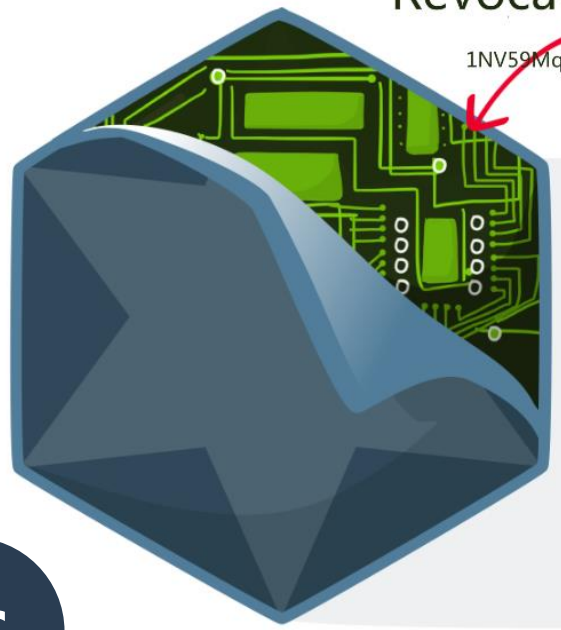
```
badge name
badge URL (description)
badge criteria
badge image
issuer
issue date
recipient
tags
alignment (standards)
expiration date
evidence URL
```

The revocation list is merged in the certificate, when verify the certificate, the revocation list needs to check, which represent a single point of failure

VS

Revocation Address(BTC)

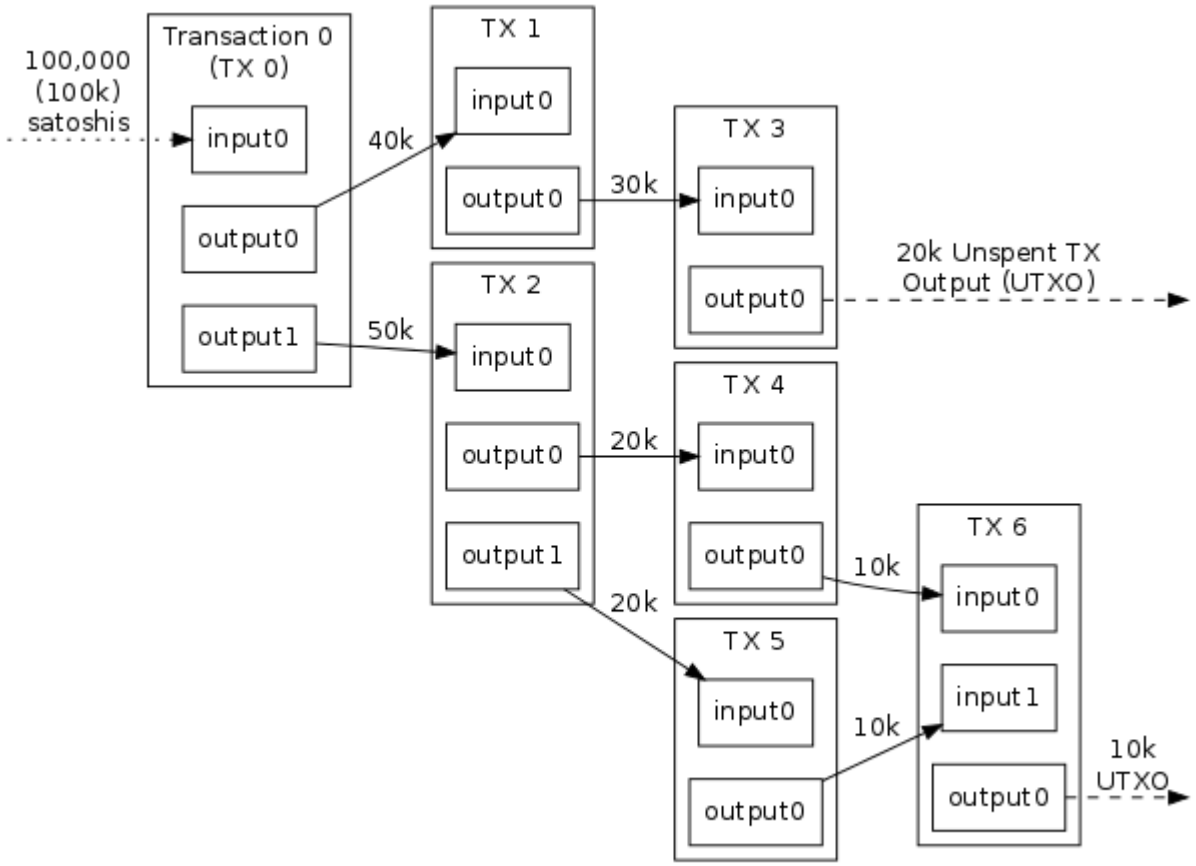
1NV59Mqq7MPksatVJHmJ8jepKQnGbCPKb7



```
badge name
badge URL (description)
badge criteria
badge image
issuer
issue date
recipient
tags
alignment (standards)
expiration date
evidence URL
```

The revocation address is merged in the certificate, when verify the certificate, the BTC address needs to check.

Security Certificate Revocation



Triple-Entry Bookkeeping (Transaction-To-Transaction Payments) As Used By Bitcoin

Every transaction has input and output.

Each input refers to the previous output it's spending by the txid of the transaction

The input address is public and verifiable.

Image source: https://21.co/learn/the-blockchain/

Security Certificate Revocation

Students	Revoke_address	Batch_revoke_address	Private key	State
Rujia	1GS7diwCc7SywyaUYgynd1bbMUdoh1PShx	1JuGXZ7imBaB2zYceogSYnJmnRpTm4v3A3	*******	valid
Tom	18H4xq3jFfhis7Jn91c1vieXFYKx3LsPnJ	1JuGXZ7imBaB2zYceogSYnJmnRpTm4v3A3	*******	revoked

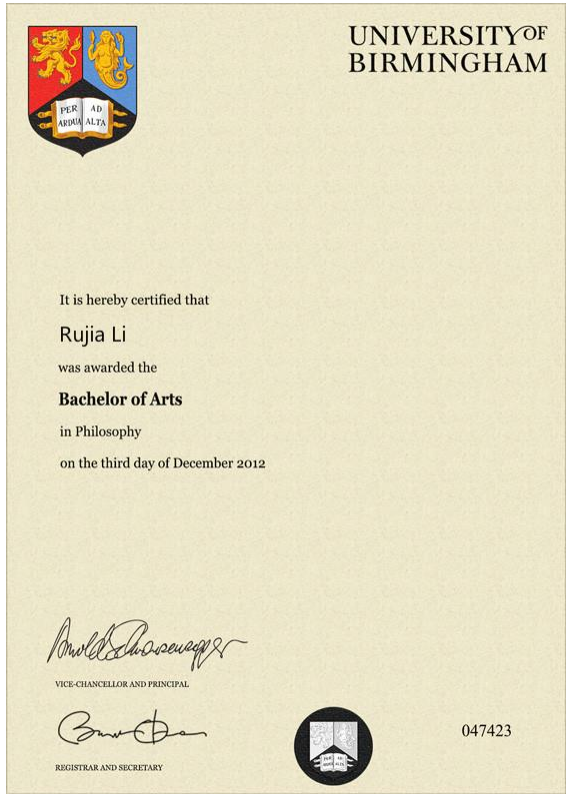

```
- badge: {
      created: "2017-01-01",
      description: "good",
      expires: "2100-01-01",
    + fileClaim: { … },
      id: https://example.org/robotics-badge.json,
    + identityClaim: { … },
      image: "good",
    + issuer: { … },
      name: "Bachelor of Arts",
    - revocationClaim: {
          batchRevocationAddress: "1JuGXZ7imBaB2zYceogSYnJmnRpTm4v3A3",
          revocationAddress: "1GS7diwCc7SywyaUYgynd1bbMUdoh1PShx",
        + type: [ … ]
      },
      type: "Certifacte"
  },
```


Revocation is performed by checking the transaction's input from the embedded bitcoin address.

If a embedded bitcoin address is never used, It means that the certificate is valid.

If the embedded bitcoin address is used and the transaction's input address is belonged to institution. It represents that the certificate is revoked.

Certificate Authenticity in Blockcert Version 1.0



There is a signature and a url-based public key embedded in the certificate. The recipient-owned public key embedded in the record allows the recipient to prove ownership.

```
- issuer: {
      name: "University of Birmingham",
      email: "uob@bham.ac.uk",
      url: http://www.birmingham.ac.uk,
      type: "Issuer",
      signer_pub_key: http://www.birmingham.ac.uk/keys/bham_public_key.asc,
      id: "001"
  },
```

Perfect forward secrecy (PFS) ✗

If the private key was leaked, there is nothing to prevent an attacker from issuing fake records and backdating the content.

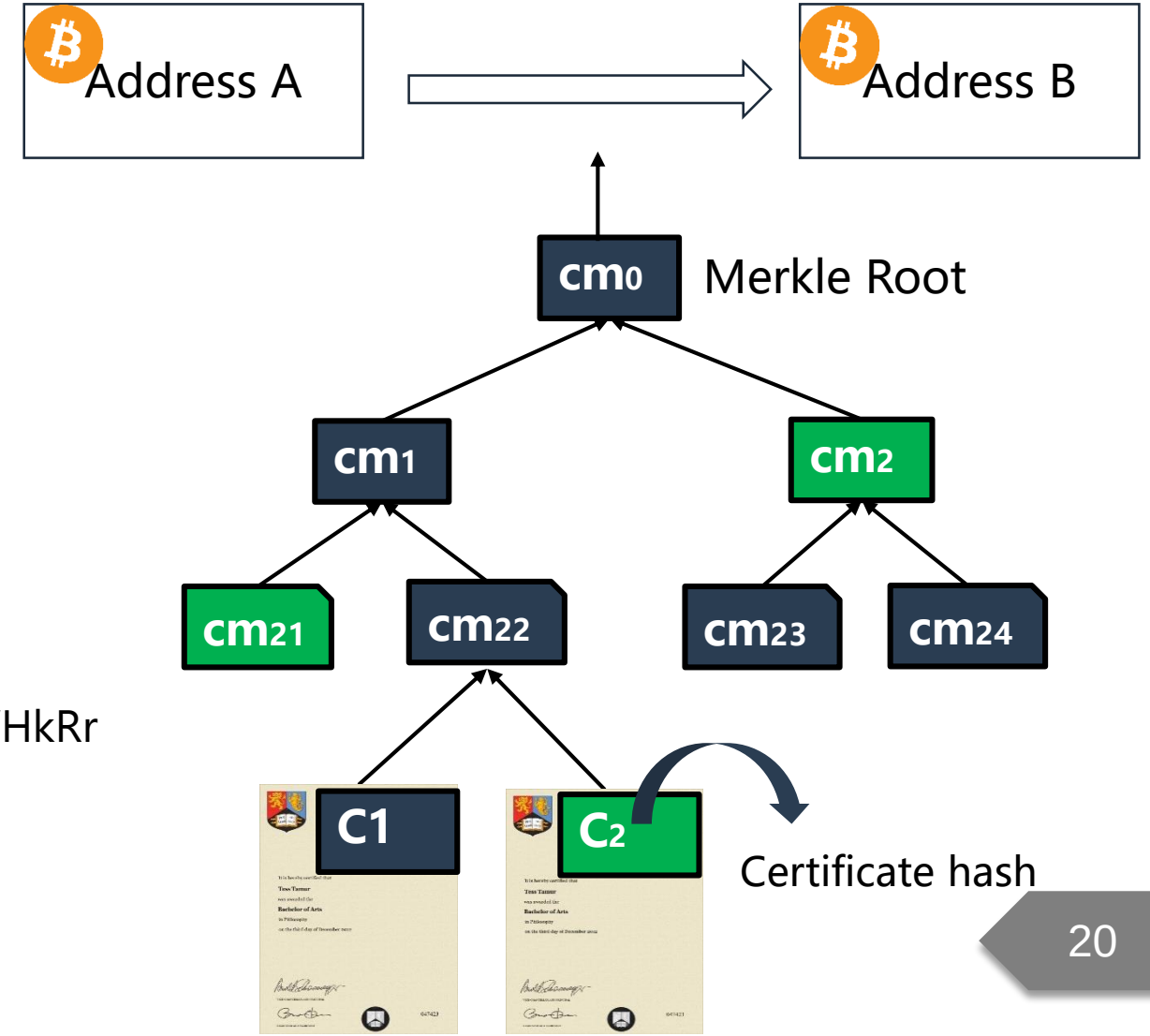
Certificate Authenticity in Blockcert Version 1.0

To determine that a record was issued by a specific issuer when the issuing key was valid requires knowledge of the timestamp beyond anything written into the credential itself.

Issued Key + Timestamp

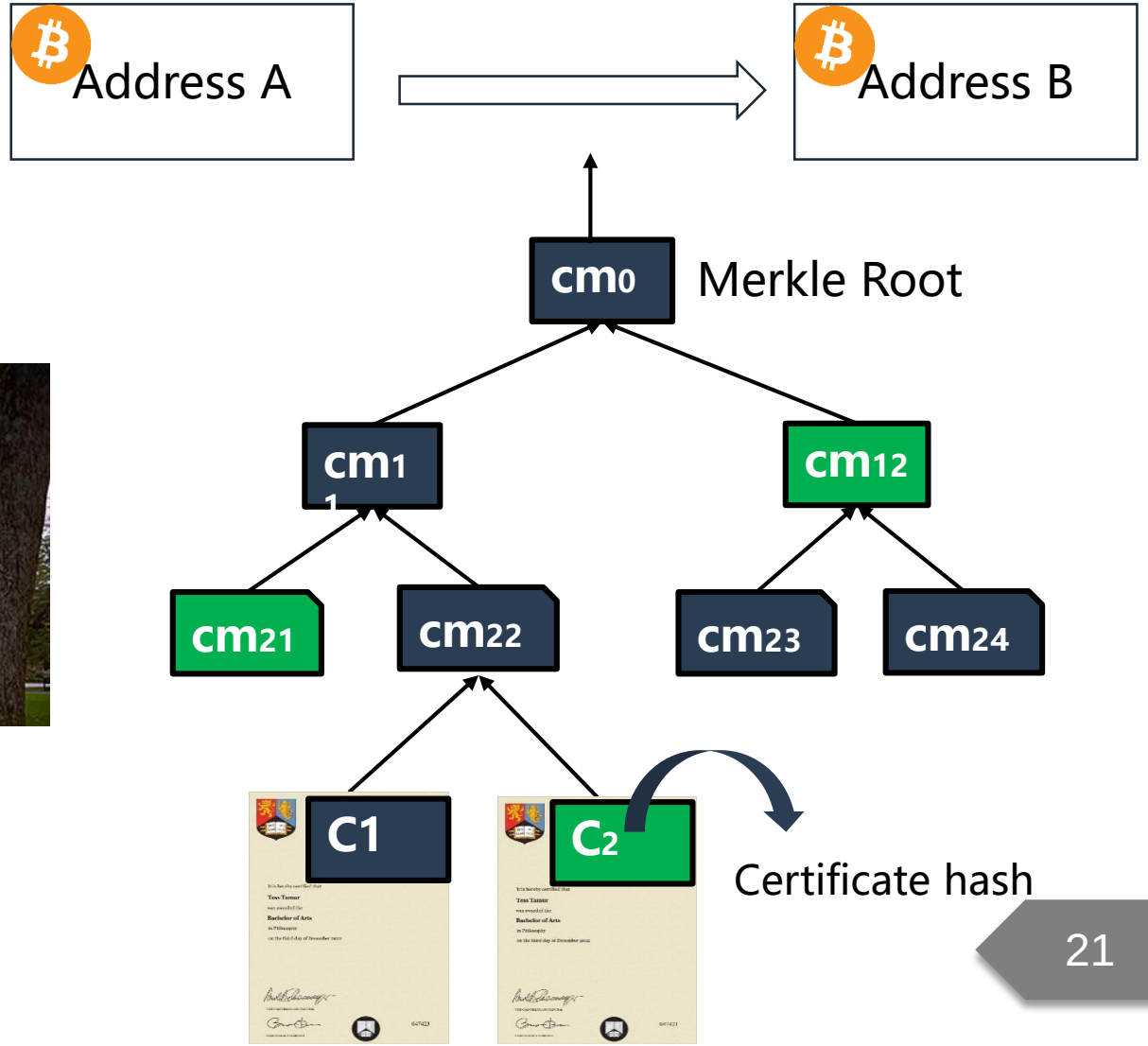
Address:
1Jw1qkMvP7tp2RuErFoSbxMwfyrnFVHkRr

Timestamp:
15- August - 2017



Security Federated Identity

How to prove the address is belonged to this institution(school) ?



Security Federated Identity

WitnessURL2: **Well-Known URLs** + Organization abbreviation

WitnessURL2: **Well-Known URLs** + Organization abbreviation

+

Random Number

+

Trapdoor

Address A

Authentication Code

Official website

Implementation

- ✓ Framework and tech stack
- ✓ Standard blockchain certificate
- ✓ Demonstration page

Framework and tech stack

Development	Deployment
spring BOOT	docker
mongoDB	git
Bootstrap	amazon web services EC2

Standard blockchain certificate


```
{
  - badge: {
      created: "2017-01-01",
      description: "good",
      expires: "2100-01-01",
    + fileClaim: { … },
      id: https://example.org/robotics-badge.json,
    + identityClaim: { … },
      image: "good",
    + issuer: { … },
      name: "Bachelor of Arts",
    + revocationClaim: { … },
      type: "Certifacte"
    },
  + context: [ … ],
    id: "1a08a38afe7f4a848d8f6e7609350814",
    issuedOn: "2017-08-15 00:20:26",
  + recipient: { … },
  - signature: {
    + anchors: [ … ],
      context: https://w3id.org/chainpoint/v2,
      merkleRoot: "1cf7ec6048c93cb3710b274a714ff5e7312b496f7cf79bd27881feed69c122eb",
    - proof: [
        - {
            left: "68a7d9a8e1f47d23e28e57e15fdbbc3206764363a93db32705aa8ceddfb96116"
          },
        - {
            right: "7a1337ce6ce66b6114b7828f82d8a20477d9db37cef76c7841f2b10365f45508"
          }
      ],
      targetHash: "4ec37c5ab0595ca0ba0f5cb80526ed7dbee0da13636ee3c15e47dc953089d4e9",
    + typelist: [ … ]
    },
    type: "badgeClass",
  + verification: { … }
}
```


Certificate

Receipt


https://btcert.com
BTcert.com
University of Birmingham 2017 BTCert
Overview
User Manage
Registered User Manage
Config Manage
Student RevoInfo Manage
School Identity Manage
School Configure Manage
Transaction
Transaction address
UnBroadcasted Transaction
Broadcasted Transaction
Latest Confirmed Transaction
Overview / Home
Certificate & Transaction
SN: 32901
TCN: 32900
VCN: 20004
RCN: 20
RTF:0.0001
TTN:10
TA:204
Tags
Bitcoin price & Bitcoin fee
Live Bitcoin price and market cap
$4319.49
MktCap $71.3B
High $4319.49
Low $952.68
Supply 16.5M
Blocks 480796
Aug 16, 2017 1:00 AM
Predicting Bitcoin fee and confirmed time
X: fee/byte, Y: confirm time/mins

Admin page

Student Page

Conclusion

- ✓ Contribution

Contribution

MIT

Certificates based on blockchain
+
Python Implementation

UOB

Democratic Multi-signature issuing
+
Security Certificate Revocation
+
Security Federated Identity

W3C

Verifiable Claims Data Model and Representations
+
Data format standard

THANKS!