Cryptography and its applications in Blockchain (StudentChain)

Abirami Ravishankar

Abstract

This paper aims to show the interconnection between cryptography, how cryptocurrencies were formed, blockchain and application of blockchain through time and improving tech-nology. Cryptography is used to solve codes. Cryptocurrency is a digital currency with encryption techniques used to regulate the generation currency and verification of transfer of funds, operating independently of a central bank. A blockchain is a digital ledger in which transactions are made. A cryptocurrency and are recorded chronologically and publicly. A blockchain is also a secure way to store data as every message is converted to a hash and is then stored. Till date it's been impossible to hack into a blockchain. StudentChain is a blockchain model with distributed ledgers with peer-to-peer verification of student IDs to prevent the misuse of student discounts. SHA-256 is the algorithm using python language used in StudentChain.

1) Introduction

The current market is a cash strapped market. Companies are now looking to attract student population as there are 21 million college students in the United States. Student discounts are now extremely popular. Currently, .edu email addresses and student IDs are methods of verification. StudentChain is a prototype of a distributed ledger system with peer-to-peer verification of students currently enrolled in universities in the United States. The universities listed are stored as blocks and the students enrolled in them are stored as nodes.

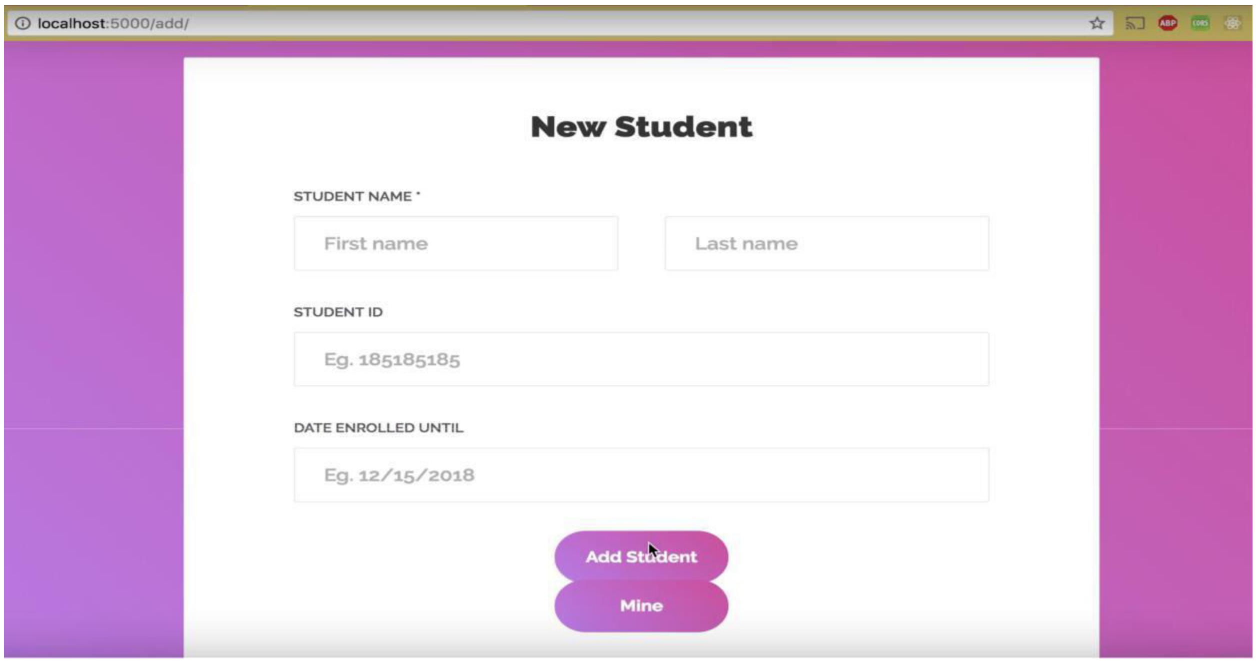
2. StudentChain

Student chain is a platform created to prevent the misuse of student discounts in the United States. Every student enrolled in a university (let's say University of California, Berkeley) is a node on the blockchain and every recognised university is a node. Blockchain is immutable and reliable for verification. Asymmetric encryption allows institutions to sign a student cer-tificate that anyone can verify. Ensures only institutions can add students to the blockchain. A company that has a policy of offering student discounts can verify the identity of students applying for the discount instantly. Companies can check if a student has a valid record in the blockchain and that it is signed by their institution. Using the language Python to produce a hash using the SHA-256 algorithm for every student enrolled. SHA-256 generates a unique 256-bit (32-byte) signature for a text. Peer to peer verification happens within a few seconds and it shows if the verification was successful or if it failed. The companies are also nodes on the blockchain.

3. Using StudentChain

Student chain was entirely done on a local host as the traffic in the prototype was less. Python 3, flask web framework and requests library must be installed. If you run ‘python3 unicode2.py’ then you are now a university node on the blockchain. A spectator node can be set up in a similar manner but they cannot add or delete data on the blockchain and can simply view/ verify. http://localhost:5000/add/ is where the form for adding a student in a university node is. After adding the student, clock on ‘mine’ to mine a new block in the blockchain. Students would be sorted accordingly. http://localhost:5000/check to verify someone’s student status and click on ‘check student’ to verify. Peer-to-peer verification happens in this stage. http://localhost:5000/chain to view the entire blockchain. To add more university nodes, click ‘resolve’ in http://localhost:5000/check and repeat the above steps.

The user interface.


localhost:5000/add/

New Student

STUDENT NAME *

First name | Last name

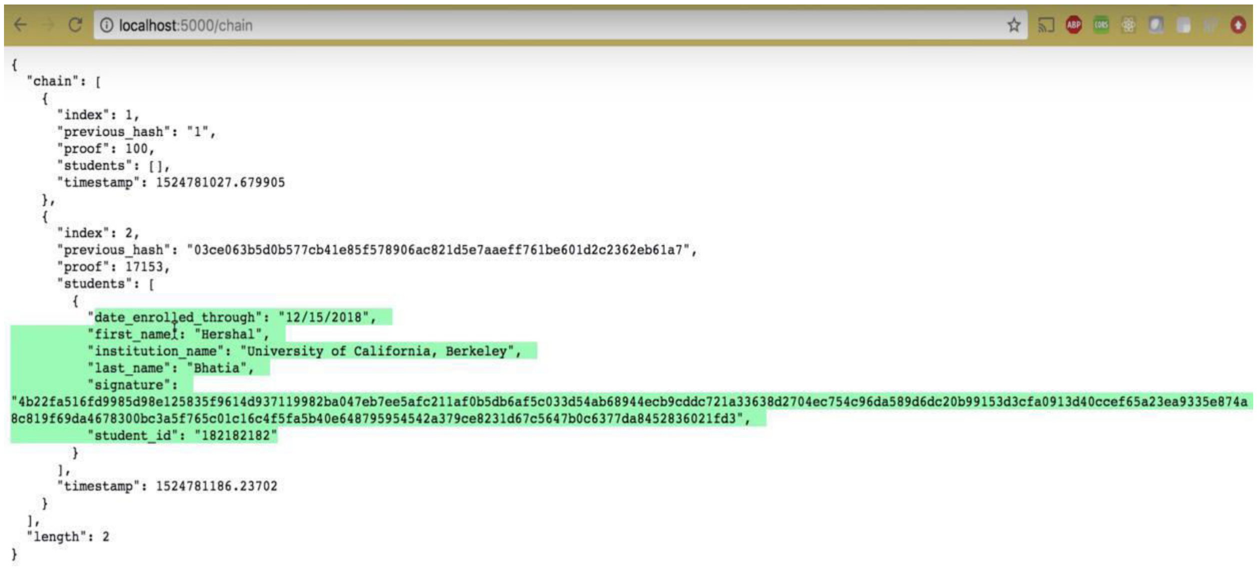
STUDENT ID

Eg. 185185185

DATE ENROLLED UNTIL

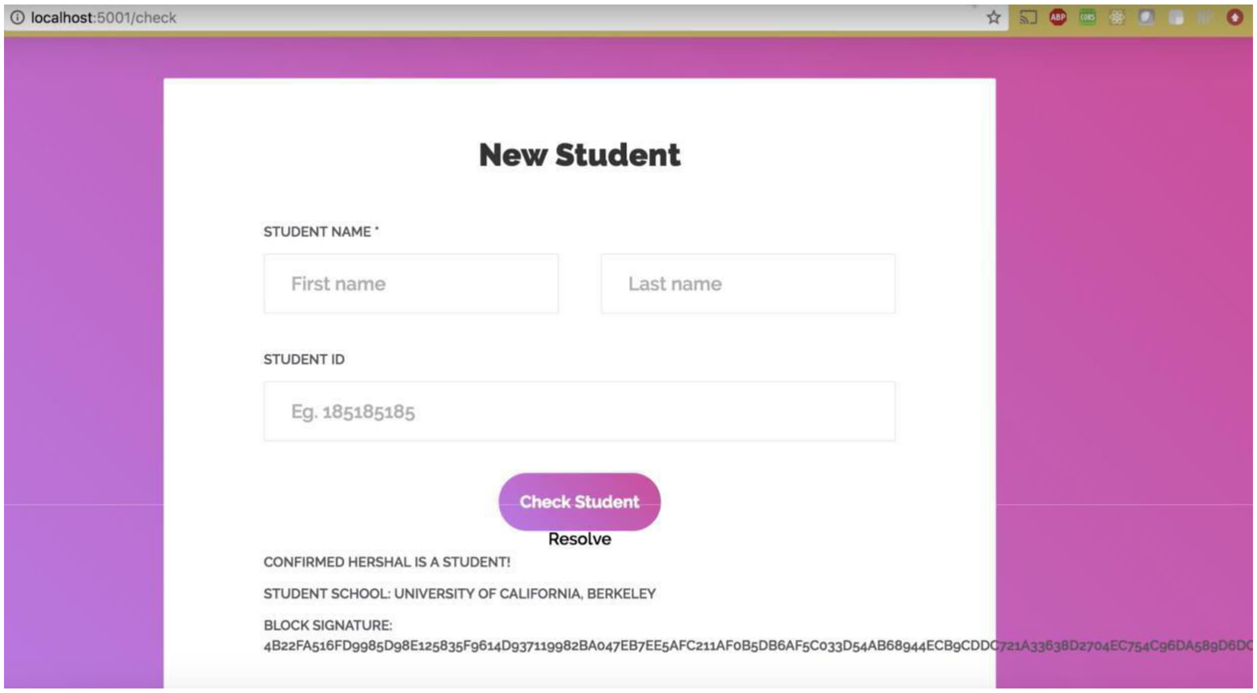
Eg. 12/15/2018

A unique hash is generated.


localhost:5000/chain

```
{
  "chain": [
    {
      "index": 1,
      "previous_hash": "1",
      "proof": 100,
      "students": [],
      "timestamp": 1524781027.679905
    },
    {
      "index": 2,
      "previous_hash": "03ce063b5d0b577cb41e85f578906ac821d5e7aaeff761be601d2c2362eb61a7",
      "proof": 17153,
      "students": [
        {
          "date_enrolled_through": "12/15/2018",
          "first_name": "Hershal",
          "institution_name": "University of California, Berkeley",
          "last_name": "Bhatia",
          "signature":
"4b22fa516fd9985d98e125835f9614d937119982ba047eb7ee5afc211af0b5db6af5c033d54ab68944ecb9cddc721a33638d2704ec754c96da589d6dc20b99153d3cfa0913d40ccef65a23ea9335e874a
8c819f69da4678300bc3a5f765c01c16c4f5fa5b40e648795954542a379ce8231d67c5647b0c6377da8452836021fd3",
          "student_id": "182182182"
        }
      ],
      "timestamp": 1524781186.23702
    }
  ],
  "length": 2
}
```

Peer-to-peer verification-


localhost:5001/check

New Student

STUDENT NAME *

First name	Last name

STUDENT ID

Eg. 185185185

CONFIRMED HERSHAL IS A STUDENT!

STUDENT SCHOOL: UNIVERSITY OF CALIFORNIA, BERKELEY

BLOCK SIGNATURE:
4B22FA516FD9985D98E125835F9614D937119982BA047EB7EE5AFC211AF0B5DB6AF5C033D54AB68944ECB9CDDC721A33638D2704EC754C96DA589D6DC

4. Conclusion:

The prototype - StudentChain produced a unique hash for every student and is a unique example of a blockchain project. The user interface was easy to use and made the whole concept of verifying using blockchain simpler. It is highly unlikely that StudentChain is misused as it is stored on a blockchain and only the The StudentChain takes about 3-4 seconds to verify a particular student and with high volume of traffic may prove to be extremely time consuming and expensive with the significant increase in the number of servers required to regulate the traffic. Further to verifying for student discounts, it can be used to verify birth and death certificates, verification of degree certificates, criminal records and many more.

5. References:

[1] Satoshi Nakomoto https://bitcoin.org/bitcoin.pdf , 2008

[2] Brian Ho, Gillian Chu, Gloria Zhaohttps://blockchain.berkeley.edu/decal/fa18/fund/ , 2013

[3] Akash Khosla and Nicolas Zoghb https://blockchain.berkeley.edu/decal/fa17/dev/ , 2013

[4] Nowak Kowalski https://en.wikipedia.org/wiki/Theory_of_computation , 2018

[5] Peaceray https://en.wikipedia.org/wiki/Cryptography , 2018

My sincere thanks to Blockchain Challenge Lab at the University of California, Berkeley; the Sutardja Center for Technology and Entrepreneurship, UC Berkeley for the semester abroad. My fellow teammates for this project, Pal Makkar and Hershal Bhatia.