‘CredBlock’

A blockchain solution for credential verification

PROJECT DOCUMENTATION

Blockchain Development – T175 (dApp II)
George Brown College
August 15th, 2020

Zakariya Jasat – 101092428

zakariya.jasat@georgebrown.ca

CredBlock

A CREDENTIAL VERIFICATION START-UP.

We are leveraging Distributed Ledger Technology by integrating Blockchain infrastructure in our business model.

We strive to streamline the credential verification process for educational institutions, students, and employers.

Our business will facilitate employers in validating candidate education in minutes, while putting an end to fake credentials.

Contents

Business

Executive Summary

Education is one of the essential elements in any prosperous society. In Canada, over 2 million students have enrolled in post-secondary education each year from 2012 to 2017. Over a period of 10 years from 2006 to 2016, the proportion of Canadians aged 25 to 64 who had either a college or university qualification soared up to 54% from 48% (Statistics Canada, 2017). Meanwhile, an important issue arising is the need for a streamlined process of verifying academic credentials across Canada. While employers and academic institutions are preoccupied with verifying graduate credentials, the number of fraudsters is steadily increasing (CBC Marketplace, 2017). With privacy, security, and an ethically driven organizational culture, CredBlock strives to combat fake credentials by leveraging distributed ledgers through an immutable blockchain. CredBlock will offer solutions that address different aspects of the credential verification process and establish new standards. By investigating business, legal, and technological details that pinpoint CredBlock, this paper explores how blockchain can lead to the achievement of credential verifiability.

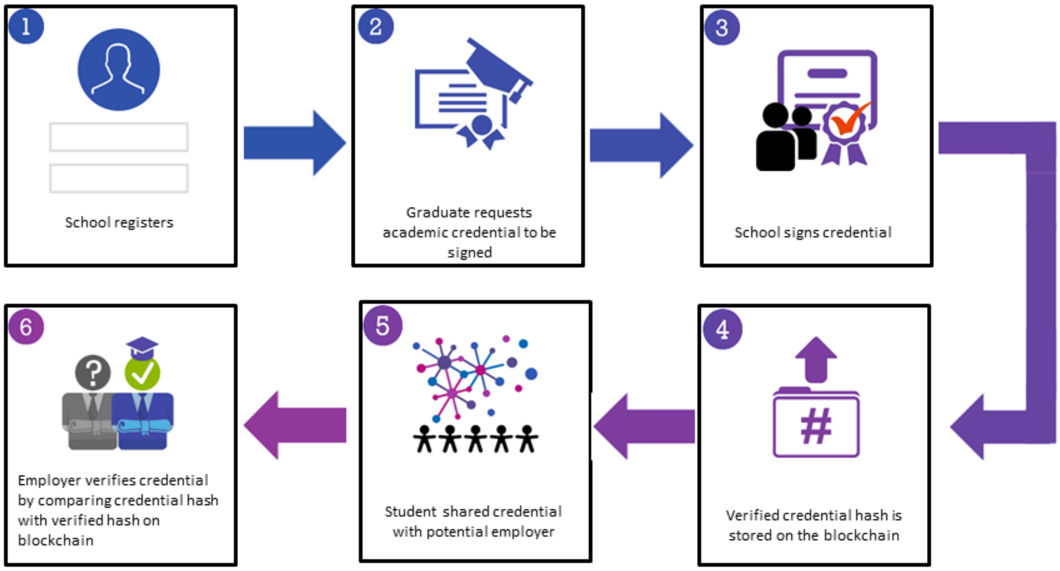

1
School registers
2
Graduate requests academic credential to be signed
3
School signs credential
4
#
Verified credential hash is stored on the blockchain
5
Student shared credential with potential employer
6
Employer verifies credential by comparing credential hash with verified hash on blockchain

Figure 1. CredBlock Process Flow Chart

Problem Statement

In terms of employment, it is not uncommon that candidates submit fake academic credentials to employers during the hiring process. This has become a growing concern for many organizations due to the high cost implications of wrong hires, consumption of human resources, lost work-time, reimbursement of tuition fraud, hiring new employees, and the decline of public trust for the organization. Negative impacts like these can cause ripple effects on many industries and can contribute to a sluggish growth for the Canadian economy.

Background

Fake credentials in the professional atmosphere is of growing concern, with easily purchasable diplomas online for as little as $400 USD from companies such as '*PhonyDiploma'* and *'RealisticDiplomas'* (Crockett, 2015). According to CBC's Marketplace, over 800 people in Canada have purchased a fake credential from the largest fake diploma mill in the world, '*Axact*', located in Pakistan; with disciplines including Medical Professionals, Engineers, and Legal Consultants (CBC Marketplace, 2017).

Employers in Canada go through a tedious process of making manual calls to academic institutions to validate candidate information or hire third-party companies to make the calls, putting strain on company resources like time and money, while also creating a burden on academic institutions who have to allocate some of their resources on liaising with third-parties. The dreariness of the process has resulted in some companies relying on 'candidate-trust' and do not bother verifying credentials at all, giving way for negative impacts on business reputation, resources and creates safety concerns for the public. The average cost of education verification by a third-party vendor can start from $29.95 CAD per check (HireRight Inc, 2020); and requests for academic transcripts can cost upwards of $15 CAD per request (OUAC. 2019), with usually, very long wait times.

Effects of Fraudulent Credentials

During the past few years, falsified educational certifications being used by high level employees of multinational organizations has come to light. Many employers have suffered negative consequences of hiring an individual with a fake credential, one of them involved a legal case, R. v. Rose’s Well Services in Alberta; whereby an employee was convicted of safety offences after causing two coworkers to get badly burnt due to the fact that they were not qualified for the position and were hired through using fake credentials (Silliker, 2019). In a separate incident, Ex-Walmart Vice President David Tovar, who lied about his degree, was forced out from his position. This brought Walmart the high cost to replace him as well as the damage to Walmart’s reputation (Abrams, 2014).

A further example is a case involving Dubravko Zgrablić, who taught thousands of students, at Seneca College, University of Toronto, Centennial College and Ryerson University. It was later discovered that he held a fake computer science master’s degree (Adlakha, 2017). A few more examples include Ex-Yahoo CEO Scott Thompson claimed to have completed a Computer Science Degree while it was in-fact an Accounting Degree (Anand, 2014), and Ex-RadioShack’s CEO David Edmondson falsely claimed that he has two College Degrees while the report shows that he attended the school for only two semesters (Anand, 2014).

Objective

CredBlock is determined to streamline the process of credential verification in Canada with the use of ‘*Blockchain Technology*’. CredBlock will empower graduates in having access to their proof of accomplishments all the time. Therefore, enabling third parties who are concerned with graduate credential authenticity in being confident that they are viewing a genuine academic certification. CredBlock’s solution also unlocks more time for academic institutions to work on strategic objectives, rather than spending their resources liaising with third parties verifying graduate credentials.

Blockchain Solution

We are working on providing a blockchain-based system for education verification that provides only true and immutable information. In the case of credential verification, such technology is perfect for recording proofs academic qualifications, in-that it records verified necessary and unchangeable information including the owners, the signers, and a one-way hash of the credential that will be used for verification. It serves various parties such as employers, agencies, universities, and allows graduates to retrieve and share their official records (degrees, transcripts, certifications) directly with others in a secure, timely and tamper-resistant way.

With the help of the Ethereum Blockchain and leveraging their Solidity based Smart Contracts, CredBlock will help combat the issue of fake academic credentials being used to defraud employers. CredBlock's decentralized application will facilitate a process by which academic credentials can verified using cryptographic hashes. While the actual credential is stored on a database, crucial information about the credential is hashed and stored on the blockchain using the secure SHA-256 algorithm, which will help us save space and costs (Whittle, 2018). Credential verification will be carried out by third parties being able to use CredBlock's services to get a real time hash of the credential shared with them by the applicant and compare it with the immutable hash of the original document on the blockchain, thus creating an almost instantaneous solution for verifying academic credentials.

CredBlock's decentralized application will enable educational institutions to 'sign' specific credentials belonging to graduates to go on to the blockchain. CredBlock will ensure the institutions are certified in Canada with the help of the public Oracle 'Certified Educational Institutions Master List' provided by the Canadian Government (MCL, 2018).

Structure:

Each block consists of the following segments:

Hash of credential data: The academic certifications and credential information.

Credential Owner: Address of the student who owns the credential.

Credential Signer: Address of the academic institution that verified the credential.

Timestamp: Block creation time.

Privacy:

Considering clients' privacy and the nature of our business, confidential information stored on the blockchain will be always be hashed. Access to the data on the database will only be given to the individual who is the owner of the data. CredBlock will not access any confidential data without prior consent from the owner unless legally required to do so.

Oracle:

The Oracle for this project will be the '*Certified Educational Institutions Master List*' provided by the Canadian Government (MCL, 2018). This will provide the means to assure legitimacy and certification of each educational institution in Canada. Only after the institution has been deemed as authentic, will we accept any academic transcript from them.

Security:

The Ethereum blockchain network is maintained by thousands of nodes competing to complete transactions through the Proof of Work (PoW) consensus mechanism, making it almost impossible to be compromised (Tar, 2018).

Smart Contracts:

CredBlock will utilize multiple Solidity based smart contracts to make the decentralised application functional, including:

- One for the states – which will outline the structure of what a credential will have and what the institution will have.
- One for interacting with the states – which will have functions to add new institutions, add new credentials, retrieve institution information, and retrieve credential information.
- One for credential verification – which will have the logic for how a credential can be verified by matching the new document hash with the verified hash.

- One as a main contract – which will inherit the other contracts' logic to make the decentralised application run smoothly.

Business Model

CredBlock's decentralized application will be designed to be extremely user friendly, with considerations of the various stakeholders who will interact with the service. The process of onboarding new academic institutions, signing transactions, and verifying credentials will be done through just a few clicks, making it time efficient for all parties involved.

Third party verifiers will not have any immediate costs associated with the service as they will only be reading from the blockchain and not creating any new transactions. However, later on in the process of completing the service and enough traction with many users already on the service, CredBlock's solution can be 'software as a service', whereas third party verifiers would pay a subscription fee to CredBlock, in order to be able to instantaneously verify graduate credentials and save on lengthy verification processes. Academic institutions will have to pay the *'Gas'* costs for deploying the smart contracts on the Ethereum main net. Graduates will have no associated costs with owning their credentials.

The use of a database will be adopted to store the actual credential, which will save costs of transacting heavy loads on to the blockchain and will also make the application much faster. Critical operations including the registration of new institutions, adding new credentials, and verifying the credentials will be handled on-chain.

Laws and Regulations

Financing Considerations

From an investment perspective, there are seven types of financing for a start-up: personal, family, venture capitals, angels, incubators & accelerators, government grants and bank loans. Commonly known that venture capitals and angels are high risk equity investors, who in return want to be involved in the ownership of a company by keeping shares. *Alexandra Kaschuta* said the main difference between them is that "venture capitals are usually bound by stricter operating procedures and formalities, angels have more free-rein to negotiate customised arrangements." Loans are another type of financing source that attribute to liabilities without third-party involvement in ownership.

Building User Privacy Trust Through Legislative Compliance

It is important to note that in Canada the '*Personal Information Protection and Electronic Documents Act*' (PIPEDA) provides a framework that guides the private sector on how to collect, store and transfer 'personal information' of members of the public. Under *section 8* of the *Canadian Charter of Rights and Freedoms,* "Everyone has the right to be secure against unreasonable search or seizure". (The Constitution Act – UK, 1982). Personal information is defined as any information that that allows the identification of an individual and that the information is also about an individual. Where information does not involve subject matter that engages an individual's privacy rights, the information is not personal information, even if it may identify an individual. However, this determination can make difficulties in some cases, particularly where it is unclear whether the information affects an individual in a personal capacity.

Also determining how to resolve disputes in the event of a breach of information is crucial for businesses that collect personal information. Resolving disputes may take two forms. The first would be to present the case to the Office of the Privacy Commissioner of Canada and the second would be litigation in the court of law.

Decisions reached by the Office of the Privacy Commissioner are only binding between the parties involved while decisions made by the court set legal precedence and can extend beyond the parties involved.

Building User Privacy Trust Through Compliance with Regulatory Bodies

Building trust through compliance with regulatory bodies would be extremely beneficial for new businesses as it expresses an ethical organizational climate. Some of these regulatory bodies include *'Canada's Association of I.T. Processionals, 'Associate Information Technology Professional', 'Informational Systems Professional',* and *'Information Technology Certified Professional'*. While membership to these organizations is not law, they strive to create accountability and guides I.T professionals to maintain the highest level of ethical conduct, standards of practice and integrity with respect. Of these, only the Informational Systems Professional (ISP) designation is recognized by Canadian law as a self-regulating designation in six provinces. The Associate Information Technology Professional (AITP) is considered a pre-professional designation for individuals who have recently graduated from an IT program with limited industry experience. Whereas the Information Technology Certified Professional (ITCP) is a designation attained by senior IT practitioners and academics (Givergis, 2018). These designations while not a requirement, demonstrate to industry participants that the holder is competent and upholds a high standard of ethical conduct in handling their commercial activities.

Solution

Reducing the Verification Cost to Users

CredBlock have designed their business model to be extremely user friendly – in that, it will be easy for new participants to join their network. To use CredBlock's services, graduates will make a personal account on CredBlock's website by going through a secure KYC (know you client) process to ensure valid user information. Once users have been verified, they can make a request to their corresponding certified academic institution to sign a copy a verified copy of their credential to add on to the blockchain. The institution will only have to pay the Gas fees associated with deploying the smart contract transactions on the Ethereum main net. Once the hash of the credential is received by the graduate, they can easily share copies of their credential with employers, who can then verify the credential using CredBlock's services in an efficient manner.

Oracles and the Safe and Efficient Storage of Verified Credentials

Considering the deleterious impacts of fake credentials on the Canadian economy and the deteriorating reputation of Canadian businesses, CredBlock's solution will empower graduates in permitting CredBlock to upload their certified academic credentials from verified educational institutions on to an immutable distributed ledger, verifiable through secure '*hashes'* any time. Third parties given the credential by the user will be able to instantaneously verify genuine academic qualifications through CredBlock's website. In order to verify if an educational institution is legitimate in Canada, CredBlock will leverage and utilise the open-sourced oracles, '*Certified Educational Institutions Master List'* and '*List of Eligible Post-secondary Education Institutions in Canada'*, provided by the Government of Canada (Social Development Canada 2019; Northern Affairs Canada, 2019).

Investor Relations

CredBlock will adopt a corporate business structure as it will permit more flexibility in dealing with negotiation on the matter of ownership between shareholders, whereby, shareholders can easily sell or buy shares of the company. With the selected corporate structure, CredBlock will be able to take advantage of raising larger investments and having lower tax rates. CredBlock will require starting capital to operate the business, and therefore strive to secure investments from various sources like venture capitals and bank loans. Venture capitals will be chosen over angel investors as it will ensure CredBlock's ownership of equity. With CredBlock's ethical organizational culture and underlining disruptive technology utilization, CredBlock has significant potential of success, which will persuade investors in helping CredBlock reach its required starting capital. Bank loans will be a good solution for CredBlock as it will proportionately distribute liability of the loans based on the shares of owners.

Privacy and Ethical Codes of Conduct

CredBlock's collection, storage, transfer and verification of an individual's certification(s) will affect that individual in a personal capacity and therefore, to build trust, the treatment of the certifications and other documents of personal information will need to be in compliance with the Privacy Act, PIPEDA and their strictest interpretations. CredBlock intends to store an individual's credential on a database that can be used as a reference for the verified hash on the blockchain. While hashes are relatively recent, using the *Privacy Commissioner of Canada's* approach towards IP addresses, the Commissioner outlined that while IP addresses do not only constitute the technical base for electronic communication but also provide a potential starting point to unlock additional information about the individual who used the electronic device which identified itself via the IP address in question (Wagner, 2018).

To instill trust among users of the credential verification, CredBlock will have a Privacy Policy document that users can agree or disagree with, which:

- Expressly lets them know why CredBlock is collecting their documents and how they intend to use and transfer their personal information.
- Expressly inform them that CredBlock will use the information for the same purposes they consented to.
- Expressly identify who at CredBlock is responsible for protecting their personal information.
- Reinforces to the user that CredBlock will hold their personal information in an accurate, complete, and up-to-date manner.
- Expressly inform the user that they always have the right to request for corrections or even to complain about how CredBlock handles their personal information if necessary.
- Users can know that CredBlock will strive to ensure to set safeguards or codes of conduct for third parties in place for protecting their personal information. (PIPEDA, Safeguards.)

- If a breach does occur, that CredBlock will inform the user, the police, and take steps to enhance safeguards to ensure the breach does not happen again.

Affiliation with I.T Industry Regulatory Bodies

CredBlock will also require all employees to attain certifications from regulatory bodies like *'Canada's Association of I.T. Processionals', 'Associate Information Technology Professional', 'Informational Systems Professional' and 'Information Technology Certified Professional'*; which will maintain CredBlock's reputation of being ethically driven. CredBlock will create working partnerships with established and trusted organizations such as *the Canadian Council of Ministers of Education*, *certified post-secondary institutions,* and *other government organisations,* ensuring watertight safeguards to user information, further improving their reputation of being ethically driven.

Conclusion

The ever-increasing expenditure of organizational and institutional resources in validating graduate credentials, compiled with the ease of obtaining fake credentials by malicious individuals has become a rebarbative burden on the Canadian economy and diminishes safety of Canadians. Through proper credential verification and authenticity proof, CredBlock challenges the status-quo of credential fraudsters by eliminating their opportunity to deceive. CredBlock will empower graduates in always owning a verified digital copy of their academic credentials, facilitating employers in validating candidate education instantaneously thus eradicating occurrences of hiring people with fake credentials, and streamlining the process of receiving certified credentials from academic institutions thus encouraging resource reallocation towards other strategic objectives. CredBlock's Ethereum blockchain choice implements an effective technique to validate transactions through an already proven Proof of Work consensus mechanism. With the simplification of credential verification, CredBlock will accelerate current frameworks being used by educational institutions, employers, third-party verifiers, and graduates.

Project Plan

Project Decomposition

EPIC 1

- Create Project Documentation
    - Business plan
        - Architecture
        - Needs analysis
        - Legal considerations

EPIC 2

- Writing Smart Contracts with Truffle
    - States smart contract
        - Data types
    - Interacting with states smart contract
        - Data types
    - Credential verification smart contract
        - Data types
    - Main smart contract
        - Data types
- Writing Test Cases for Smart Contracts

EPIC 3

- Web Application
    - Building backend
        - Web server
        - Node.js, Express, & Web3
    - Front End
        - Designing user interface with React.js
- Database
    - Store data
        - Connect MongoDB

Time Estimates

Work Breakdown Structure	Estimated Hours	Actual Hours	Assigned	% complete
1 Project Documentation	**55**	**45**	**ZJ**	**100%**
1.1 Business plan	50			
1.1.1 Architecture	20			
1.1.2 Needs analysis	15			
1.1.3 Legal considerations	20			
2 Smart Contract	**35**			
2.1 States smart contract	5			
2.1.1 List different data types used	4			
2.2 Interacting with states smart contract	5			
2.2.1 List different data types used	4			
2.3 Credential verification smart contract	5			
2.3.1 List different data types used	4			
2.4 Main smart contract	4			
2.4.1 List different data types used	4			
3 Build Web Application	**35**			
3.1 Build Backend	20			
3.1.1 Implement Web server	4			
3.1.2 List the routes	4			
3.1.3 Integrate Smart Contracts	6			
3.2 Build Frontend	15			
3.2.1 Design user interface	5			
3.2.2 Integrate React.js	4			
3.3 Create Tests	12			
4 Connect Database	**10**			
4.1 Connect Web Server to the Database	6			
4.1.1 Build schemas to store history	4			

Staffing

ROLES

Project Manager	**Zakariya**
SCRUM Master	**Zakariya**
Fullstack Developer	**Zakariya**
Blockchain Developer	**Zakariya**
Human Resource Manager	**Zakariya**
Industry Researcher	**Zakariya**
Blockchain Analyst	**Zakariya**
Marketing Manager	**Zakariya**
Technical Support Manager	**Zakariya**

Task	Responsibilities	Status	Year 1
1 Business Tasks			
1.1 Create Business Plan	Project Manager	Completed	✓
1.2 Survey the market	Industry Researcher	Completed	✓
1.3 Collect data	Industry Researcher	Completed	✓
1.4 Develop marketing campaign	Marketing Manager	Active	
2 Technical Tasks			
2.1 Build Website	Fullstack Developer	Active	
2.2 Develop blockchain solution / Smart Contracts	Blockchain Developer	Active	

Needs Analysis

Goals

What is the client trying to achieve?

- Create process for academic institutions to share academic credentials in a secure and efficient manner.
- Enable graduates to own verified copies of their credentials all the time.
- Empower third parties in being confident that they are viewing an authentic academic credential.

How do we measure that?

- Verifying status of all academic institutions using the service as certified in Canada, by leveraging access to the Master List provided by the Government of Canada.
- Storing the required verification information on blockchain including credential hash, time stamp, owner, and signer.
- Create interface for third parties to get real time hash of credential to compare with verified hash on the blockchain.

Problem statement

- Battling fake credentials in the Canadian economy.
- Creating confidence in job market and easing time burdens in new hire costs.
- Enabling graduates to own their authentic credential proofs all the time.

Stakeholders

Who is involved?

- Academic Institutions.
- Graduates.
- Third-Party Verifiers.

What are the roles that they play?

- Academic Institutions:
    - ○ Ensure they are acknowledged as a certified academic institution by the Government of Canada.

        - Submit verified copies of graduate academic credentials to be signed.
- Graduates:
    - Only share verified copies of their academic credentials with third parties like employers.
- Third-Party Verifiers:
    - Verify credential provided by graduate by comparing with verified version.

What are their restrictions?

- Academic Institutions:
    - Must follow legal requirements of staying as a certified academic institution in Canada.
- Graduates:
    - Can not alter their credentials, otherwise will be deemed as unverified.
- Third-Party Verifiers:
    - Must abide by legal requirements to protect graduate information privacy.
    - Must make sure they do not alter the credential provided by the student.

State Data

What is the system tracking?

- Cryptographic Signature.

What needs to be captured?

- Owner of the credential.
- Signer of the credential.
- Credential information.
- Date & time of transaction creation.

What is generated?

- Verified hash including:
    - Credential information
    - Owner
    - Signer
    - Time stamp

Architecture

Goals of the Architecture

Smart Contract

We will create our smart contracts using Ethereum's blockchain, in their Solidity language. The smart contracts will facilitate the process by which new academic institutions will be able to join CredBlock, graduates will be able to own their verified credentials, and third parties can confidently verify credential authenticity. In our smart contracts we will be able to store information like:

- The signers ID, which will be the address of the academic institution.
- The owners ID, which will be the address of the graduate.
- The credential hash, which will be a SHA-256 of required JSON data from the original credential, later used by third parties to compare with the hash they get from the credential the graduate gives them.
- The time stamp, which will help us determine when the credential was posted.

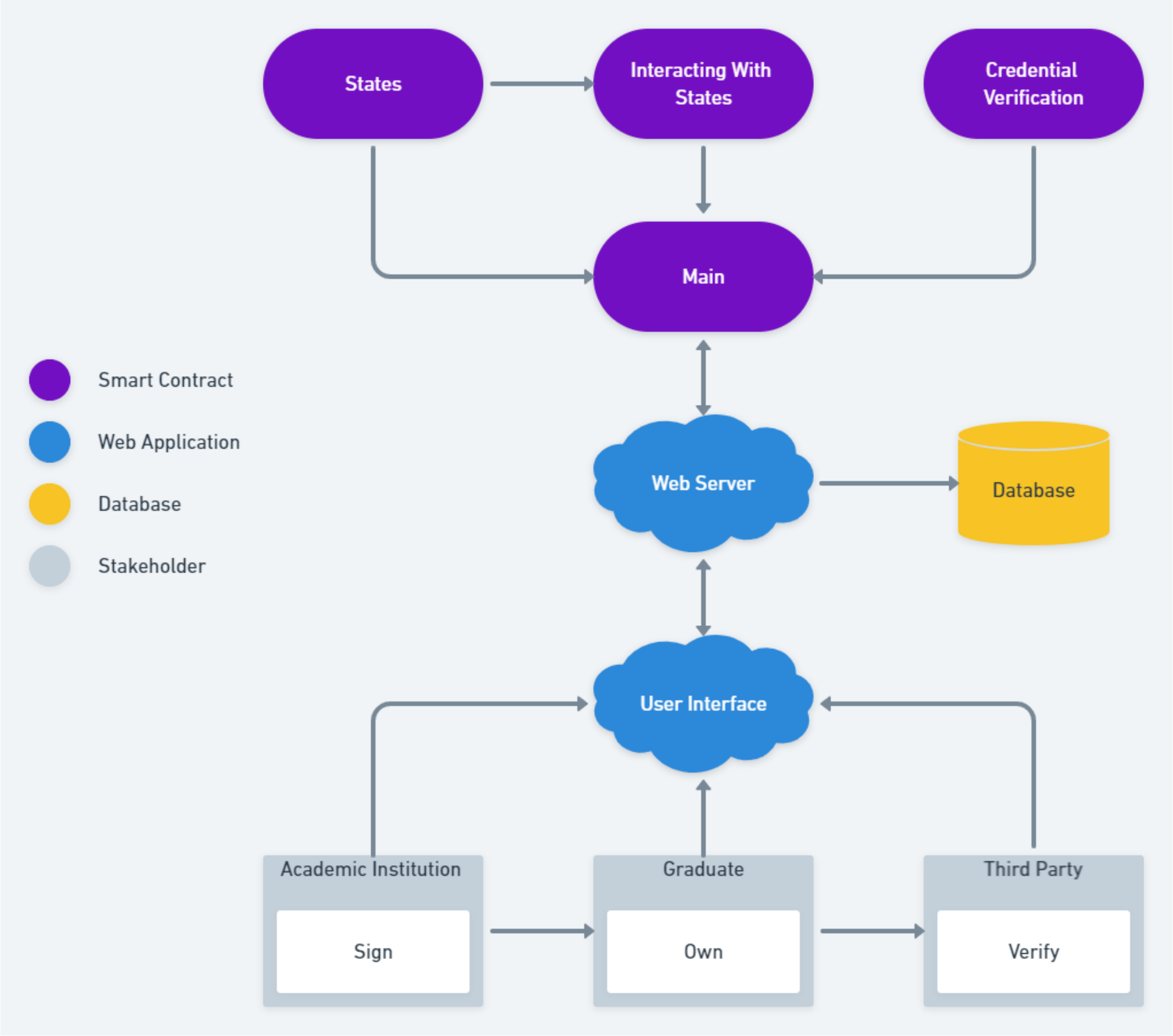
Frontend

Our frontend solution leverages the information provided from our web servers, to create a friendly user interface specifically designed for the stakeholders. Academic institutions will be able to register and sign academic credentials. Graduates will be able to own a digital copy of their credential that they can prove as authentic anytime they want. Third part verifiers like employers can instantaneously verify graduate academic credentials.

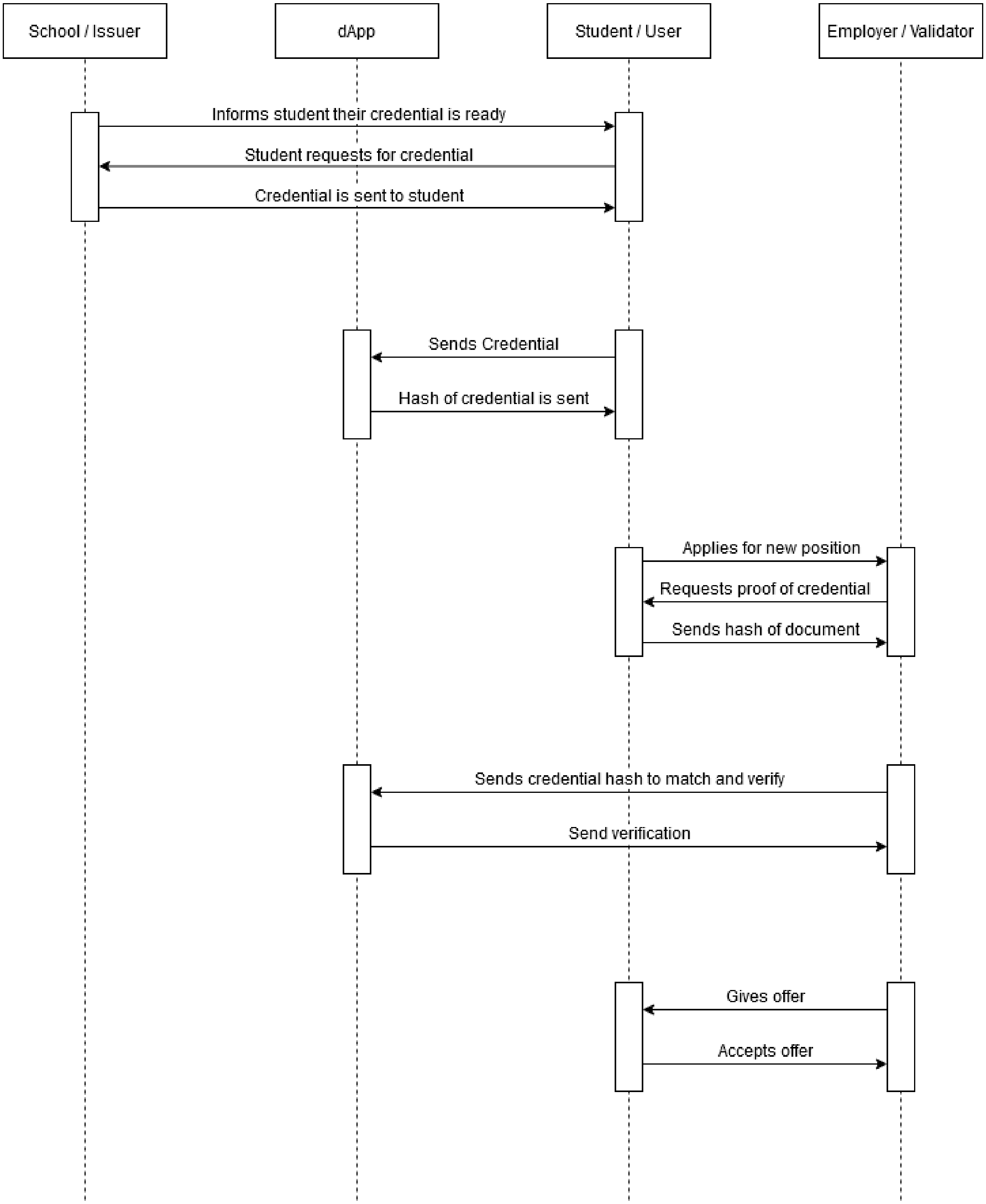
Backend

The backend creates the bigger picture by connecting the dots between the smart contracts, the database, and the front end. The backend will be built as an API which creates more efficient and flexible communication between the frontend, backend, database, and smart contracts.

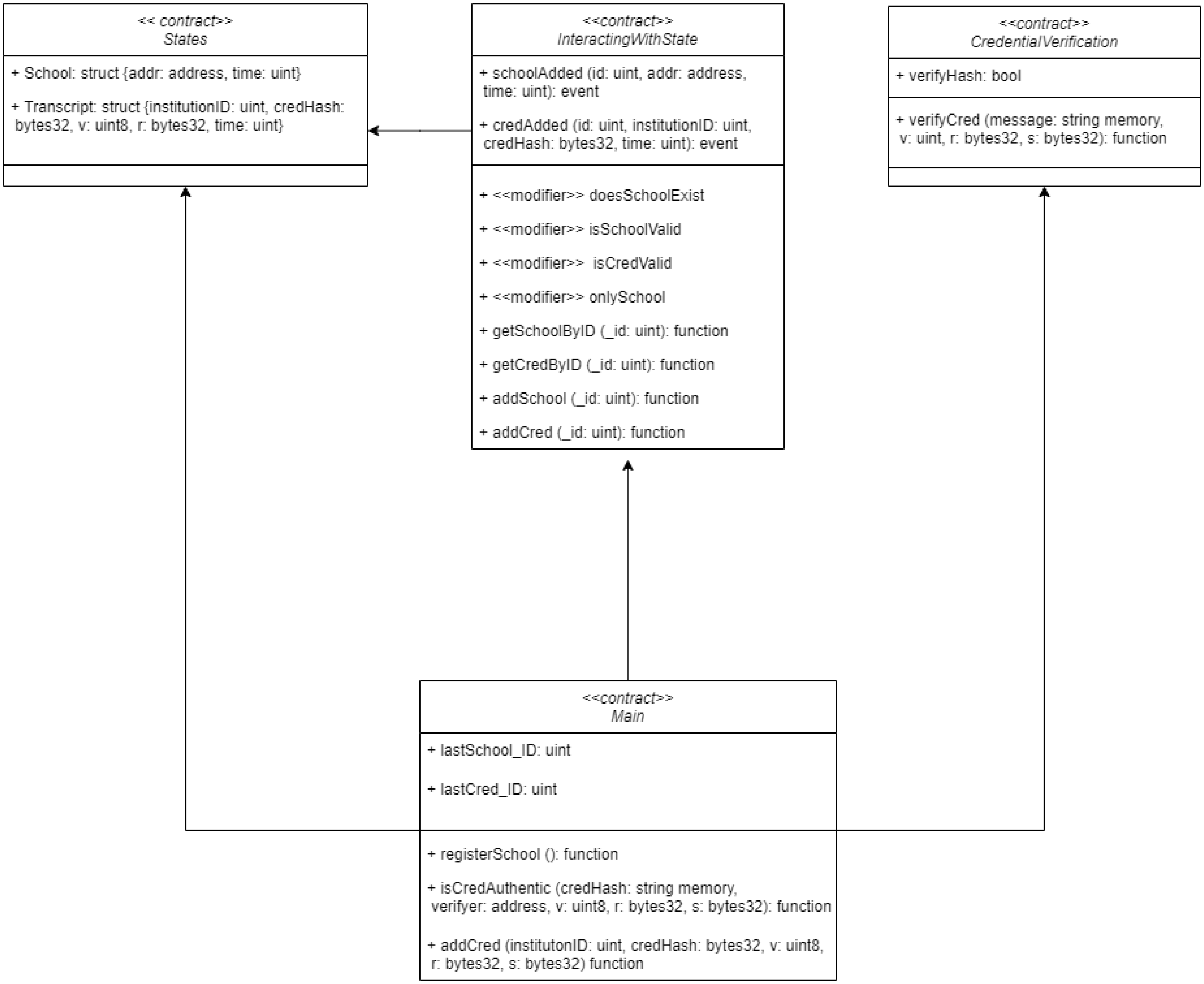
Architecture Diagram



Sequence Diagram


School / Issuer
dApp
Student / User
Employer / Validator
Informs student their credential is ready
Student requests for credential
Credential is sent to student
Sends Credential
Hash of credential is sent
Applies for new position
Requests proof of credential
Sends hash of document
Sends credential hash to match and verify
Send verification
Gives offer
Accepts offer

Class Diagram



<< contract>>
States
+ School: struct {addr: address, time: uint}
+ Transcript: struct {institutionID: uint, credHash: bytes32, v: uint8, r: bytes32, time: uint}
<<contract>>
InteractingWithState
+ schoolAdded (id: uint, addr: address, time: uint): event
+ credAdded (id: uint, institutionID: uint, credHash: bytes32, time: uint): event
+ <<modifier>> doesSchoolExist
+ <<modifier>> isSchoolValid
+ <<modifier>> isCredValid
+ <<modifier>> onlySchool
+ getSchoolByID (_id: uint): function
+ getCredByID (_id: uint): function
+ addSchool (_id: uint): function
+ addCred (_id: uint): function
<<contract>>
CredentialVerification
+ verifyHash: bool
+ verifyCred (message: string memory, v: uint, r: bytes32, s: bytes32): function
<<contract>>
Main
+ lastSchool_ID: uint
+ lastCred_ID: uint
+ registerSchool (): function
+ isCredAuthentic (credHash: string memory, verifyer: address, v: uint8, r: bytes32, s: bytes32): function
+ addCred (institutonID: uint, credHash: bytes32, v: uint8, r: bytes32, s: bytes32) function

Smart Contracts Breakdown

Function Name	Function Visibility	Function Type	Modifiers	Paramaters	Action - Notes
InteractingWithState.sol					
getSchoolByID	public	view	doesSchoolExist	(uint _id)	-It returns the information about the school -By passing the ID of the school, user can get the address of the school
getCredByID	public	view	doesCredExist	(uint _id)	-It returns the information about cred -By passing the ID of the cred, user can get the schools ID and the cred hash
addSchool	public	-	isSchoolValid	(uint _id)	-Adds a new school to the system -Before adding the school, user must make sure the school is valid
addCred	public	-	doesSchoolExist, onlySchool, isCredValid	(uint _id, uint _instituteId, bytes32 transcriptHash, uint8 v, bytes32 r, bytes32 s)	-The login of the function from main is here -Must make sure the school exists, only the school can do this, and the cred is valid
CredentialVerification.sol					
verifyCred	public	pure	-	(string memory message, uint8 v, bytes32 r, bytes32 s)	-This is where all the logic of the cred verification goes -It will take inputs and create hash
Main.sol					
registerSchool	public	-	-	()	-Add 1 to last instutues ID passes new ID into addSchool
isCredAuthentic	public	pure	-	(string memory transcriptHash, address signer, uint8 v, bytes32 r, bytes32 s)	-Returns bool about cred status -It matches the hash of the uploaded credential to the hash on the blockchain
addCred	public	-	-	(uint instituteId, bytes32 transcriptHash, uint8 v, bytes32 r, bytes32 s)	-Add 1 to last cred ID -Passes required information what will be in the credential

Cost Estimates

Ethereum: (Low Estimate – $650 CAD || High Estimate – $1,000 CAD)

Costs associated –>

- Deploying to main net
  - Gas costs per transaction
    - Cost varies based on how much information needs to be deployed, however, we predict 1 ETH (currently around $520CAD) should be enough to cover expenses related to deploying to the main net for a POC or MVP.
- Smart Contracts
  - Security Audit
    - MythX has a Developer subscription tailored for small teams that would give us 500 quick and standard scans for $49 USD a month ($98 USD for 2 months).

***Notes**: The additional costs in this section may arise from either a need for a professional security audit subscription, an additional Ether for deployment to the main net, or price fluctuations for Ether.*

Hosting: (Low Estimate – $250 CAD || High Estimate – $750 CAD)

Costs associated –>

- Templates
  - Front-end template would cost a one-time fee of $20USD.
- Off-chain data
  - Digital Ocean rent would cost around $40USD per month ($160USD for 4 months).
  - MongoDB would be free to use if we rent a server to host to the information (would be covered under Digital Ocean).

***Notes**: The additional costs in this section may arise from a requirement for additional storage space on the server.*

Additional Software: (Low Estimate – Free || High Estimate – $250 CAD)

Costs associated –>

- VM Ware
  - We have student access for 1 year which would cover costs for the project
- Office 365
  - We have student access for 1 year which would cover costs for the project

***Notes**: The additional costs in this section may arise from a requirement of any additional software which may be required that we have not accounted for thus far.*

TOTAL COST ESTIMATES – Ethereum:

Low End: $900 CAD ***High End: $2,000 CAD***

References

Abrams, R. (2014). Walmart Vice President Forced Out for Lying About Degree. Nytimes.com. Retrieved 11 August 2020, from https://www.nytimes.com/2014/09/17/business/17tovar.html.

Adlakha, A. (2017). Former University of Toronto instructor found to have fake degree – The Varsity. Thevarsity.ca. Retrieved 11 August 2020, from https://thevarsity.ca/2017/10/02/former-university-of-toronto-professor-with-fake-degree-exposed/.

Anand, P. (2014). 5 big-shots who lied on their resumes. MarketWatch. Retrieved 11 August 2020, from https://www.marketwatch.com/story/5-big-shots-who-lied-on-their-resumes-2014-09-18.

Canada, E. (2019). List of designated educational institutions - Canada.ca. Canada.ca. Retrieved 11 August 2020, from https://www.canada.ca/en/employment-social-development/programs/designated-schools.html.

CanLII. (1982). The Constitution Act, 1982, Schedule B to the Canada Act 1982 (UK), 1982, c 11. Canadian Legal Information Institute. Retrieved 11 August 2020, from https://www.canlii.org/en/ca/laws/stat/schedule-b-to-the-canada-act-1982-uk-1982-c-11/latest/schedule-b-to-the-canada-act-1982-uk-1982-c-11.html#sec8_smooth.

CBC. (2017). Fake Degrees - Exposing Canadians with phoney credentials. Cbc.ca. Retrieved 11 August 2020, from https://www.cbc.ca/marketplace/episodes/2017-2018/fake-degrees-exposing-canadians-with-phoney-credentials.

CICIC. (2020). Do an advanced search in the Directory of Educational Institutions in Canada. Cicic.ca. Retrieved 11 August 2020, from https://www.cicic.ca/869/results.canada?search=&p=2.

CIPS. (2018). Code of Ethics and Standards of Conduct.. Cips.ca. Retrieved 11 August 2020, from http://www.cips.ca/sites/default/files/CIPS%20Code%20of%20Ethics%20and%20Standards%20of%20Conduct%20-%20June%202018.pdf.

Columbus, L. (2018). Three Ways Machine Learning Is Revolutionizing Zero Trust Security - Enterprise Irregulars. Enterprise Irregulars. Retrieved 12 August 2020, from https://www.enterpriseirregulars.com/127644/three-ways-machine-learning-is-revolutionizing-zero-trust-security/.

Corporations Canada. (2016). Share structure and shareholders - Corporations Canada. Ic.gc.ca. Retrieved 11 August 2020, from https://www.ic.gc.ca/eic/site/cd-dgc.nsf/eng/cs06644.html.

Creative Common. (2020). Attribution 3.0 Unported — CC BY 3.0. Creativecommons.org. Retrieved 11 August 2020, from https://creativecommons.org/licenses/by/3.0/.

Crockett, Z. (2015). The Business of Fake Diplomas. Price Economics. Retrieved 11 August 2020, from https://priceonomics.com/the-business-of-fake- diplomas/.

Givergis, K. (2018). Becoming an IT Professional in Canada - World Education Services. World Education Services. Retrieved 11 August 2020, from https://www.wes.org/advisor-blog/becoming-an-it-professional-in-canada/.

Government of Canada. (2019). List of eligible post-secondary education institutions in Canada. Sac-isc.gc.ca. Retrieved 11 August 2020, from https://www.sac-isc.gc.ca/eng/1429541743524/1531402273996.

Government of Canada. (2020). List of Certified Institutions. Certification.esdc.gc.ca. Retrieved 11 August 2020, from http://certification.esdc.gc.ca/lea-mcl/h.4m.2@-eng.jsp.

HireRight. (2020). HireRight Inc. Retrieved 11 August 2020, from https://www.hireright.com/contact-us/find-the-right-solution?utm_source=solutions&utm_campaign=contact_sales&utm_medium=right-navi.

Hook, M. (2013). How do I structure my business?. Small Business Law Blog. Retrieved 11 August 2020, from https://mikehooklaw.wordpress.com/2013/09/05/how-do-i-structure-my-business/.

Jagers, C. (2016). Verifiable Credentials on the Blockchain. Medium. Retrieved 11 August 2020, from https://medium.com/learning-machine-blog/blockchain-credentials-b4cf5d02bbb7#.ycqark4w7.

Jimi, S. (2018). Blockchain: What are nodes and masternodes?. Medium. Retrieved 11 August 2020, from https://medium.com/coinmonks/blockchain-what-is-a-node-or-masternode-and-what-does-it-do-4d9a4200938f.

Johnson, E. (2017). 'He turned his fake degree into a weapon': Man posing as a lawyer tricks clients out of thousands. CBC. Retrieved 11 August 2020, from https://www.cbc.ca/news/business/fake-toronto-lawyer-defrauds-clients-1.4276157.

Kaschuta, A. (2019). The Complete Guide to Startup Funding Canada (The 2020 Guide!). Fundsquire Canada. Retrieved 11 August 2020, from https://fundsquire.ca/the-complete-guide-to-startup-scaleup-funding-in-canada/.

Li, K. (2019). The Blockchain Scalability Problem & the Race for Visa-Like Transaction Speed | Hacker Noon. Hackernoon.com. Retrieved 11 August 2020, from https://hackernoon.com/the-blockchain-scalability-problem-the-race-for-visa-like-transaction-speed-5cce48f9d44.

Link, A. (2018). Rotating AWS IAM Keys—Finally Made Easy and Automated. Medium. Retrieved 12 August 2020, from https://medium.com/fluidity/rotating-aws-iam-keys-finally-made-easy-and-automated-4cb4ec8a4e20.

Ministry of Government and Consumer Services. (2020). Freedom of Information and Protection of Privacy Manual. Ontario.ca. Retrieved 11 August 2020, from https://www.ontario.ca/document/freedom-information-and-protection-privacy-manual.

Office of the Privacy Commissioner of Canada. (2013). Interpretation Bulletin: Accuracy. Priv.gc.ca. Retrieved 11 August 2020, from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_04_accuracy/.

Office of the Privacy Commissioner of Canada. (2013). Interpretation Bulletin: Personal Information. Priv.gc.ca. Retrieved 11 August 2020, from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_02/.

Office of the Privacy Commissioner of Canada. (2015). Interpretation Bulletin: Form of Consent. Priv.gc.ca. Retrieved 11 August 2020, from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_07_consent/.

Office of the Privacy Commissioner of Canada. (2015). Interpretation Bulletin: Safeguards. Priv.gc.ca. Retrieved 11 August 2020, from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_08_sg/.

Office of the Privacy Commissioner of Canada. (2020). Interpretation Bulletin: Access to Personal Information. Priv.gc.ca. Retrieved 11 August 2020, from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_05_access/.

OPC. (2018). Summary of privacy laws in Canada - Office of the Privacy Commissioner of Canada. Priv.gc.ca. Retrieved 11 August 2020, from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/#heading-0-0-2-2.

OUAC. (2019). Transcript Request Fees | Ontario Universities' Application Centre. Ontario Universities' Application Centre. Retrieved 11 August 2020, from https://www.ouac.on.ca/transcript-request-fees/.

OUAC. (2020). How to Submit and Pay for your 105 Application (Transcript - Text Only) | Ontario Universities' Application Centre. Ontario Universities' Application Centre. Retrieved 11 August 2020, from https://www.ouac.on.ca/105-tutorials/submit-pay-105-application-transcript/.

Rhodes, D. (2019). Blockchain Security Issues and Legislative Challenges. CoinCentral. Retrieved 11 August 2020, from https://coincentral.com/blockchain-security-issues/.

Robyn, K. (2018). How Much Does It Cost to Run a Background Check?. Trusted Employees. Retrieved 11 August 2020, from https://www.trustedemployees.com/learning-center/articles-news/how-much-does-it-usually-cost-to-run-a-background-check/.

Silliker, A. (2019). Can you spot the fake credentials?. Thesafetymag.com. Retrieved 11 August 2020, from https://www.thesafetymag.com/ca/topics/technology/can-you-spot-the-fake-credentials/184131.

Statistics Canada. (2020). Postsecondary enrolments, by registration status, institution type, status of student in Canada and gender. Www150.statcan.gc.ca. Retrieved 11 August 2020, from https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=3710001801.

Tar, A. (2018). Proof-of-Work, Explained. Cointelegraph. Retrieved 11 August 2020, from https://cointelegraph.com/explained/proof-of-work-explained.

University of Toronto. (2020). Ordering A Transcript. Transcript Centre. Retrieved 11 August 2020, from https://transcripts.utoronto.ca/.

Vukolic, M. (2016). The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. Allquantor.at. Retrieved 11 August 2020, from https://allquantor.at/blockchainbib/pdf/vukolic2015quest.pdf.

Whittle, B. (2018). Storing Documents on the Blockchain | Why, How, and Where. CoinCentral. Retrieved 11 August 2020, from https://coincentral.com/storing-documents-on-the-blockchain-why-how-and-where/.

Witzleb, N., & Wagner, J. (2018). When is Personal Data “About” or “Relating to” an Individual? A Comparison of Australian, Canadian, and EU Data Protection and Privacy Laws. Commentary.canlii.org. Retrieved 11 August 2020, from https://commentary.canlii.org/w/canlii/2018CanLIIDocs120?zoupio-debug#!fragment/zoupio-_Toc3Page2/(hash:(chunk:(anchorText:zoupio-_Toc3Page2),notesQuery:'',scrollChunk:!n,searchQuery:'Personal%20information%20privacy%20I.T%20',searchSortBy:RELEVANCE,tab:search)).