Interplanetary Educational System (IPES)

Blockchain and Internet of Things School (BIOTS)

ETH Zürich

30. April 2018

Contributors:
David Haldimann (haldavid@student.ethz.ch)
Matthias Untergassmair (untergam@student.ethz.ch)
Nikola Nikolov (nnikolov@student.ethz.ch)
Scott Beckmeyer (scottb@student.ethz.ch)
Stephan Lütolf (luetolfs@student.ethz.ch)
Viktor Charpentier (chviktor@student.ethz.ch)
Jan Bühlmann (janbu@student.ethz.ch)

All contributors contributed equally to this report.

Word count: 4641

The software code which is part of this report is open source and available at
https://github.com/ninikolov/EDUCoin/tree/gh-pages

This project report was written as part of the spring 2018 course 'Blockchain And the Internet of Things (851-0591-01L)' run by M. Dapp, S. Klauser, and D. Helbing.

Abstract: The Interplanetary Educational System (IPES) is a personal, secure and widely recognised blockchain solution for storing international academic achievements and individual educational growth. It enables universal ECTS credits transfer, eliminating fraud and incentivises quality education. In this document, we describe IPES and present our initial prototype. We discuss our findings, and interesting possible directions moving forward.

1. Introduction

Blockchain is a new technology that has the potential to disrupt a number of industries, such as financial, digital identity, Internet of Things (IoT), supply chain or even healthcare records. While the sheer excitement about the future potential seems endless, reality often collides with the technical limitations to scalability, governmental regulations or the developer unfriendly environment of an early-stage technology. Thus, when considering the use of blockchain for a project, it is important to examine the specific problem and use case, and verify the real need for the technology. For example, if the use case requires the implementation of a distributed system that ensures the trust and consensus of multiple participating parties and immutability, that might be a good use case for a blockchain.

1.1. Problem Overview

The focus of our project is on the global educational system, which is an area that, at its core, has seen little technological change over the last 200 years. The system is currently kept rigid by prestigious institutions (rich and influential) and has low internal incentives to change. By definition, mainstream educational certification is local and centralized: it is always associated with a particular institution that issues a certificate to a student. The institution is based in a single country, and typically receives the majority of its funding by the government. Access to courses, receiving credit and a diploma is often tied to a particular institution and a country. In addition to these administrative challenges, there are currently a number of overheads for the individual parties that participate in or benefit from the educational system: **students**, **educators** and **companies**.

For **students**, currently there are various difficulties related to the accessibility, quality and international recognition of education. First, access to courses and receiving credit is often tied to a particular institution. Despite the current trend towards online courses, we are lacking a universally recognised system for enrolment to a course from any university, and for receiving credit on an international level. Second, there are no widely accepted international standards for comparing the quality of a study programme on a global level: what's recognized in one country might not be acceptable in another. This makes changing universities or changing study tracks difficult. Furthermore, the quality of education is often determined by the ranking of the university as a whole, measured as a single number. This is often inaccurate, as in every university there are courses that are taught well and courses that are taught poorly, and the ranking of individual courses is not visible from the outside. This demotivates university **professors** to constantly deliver good courses: they have no incentive to always teach at their best, because they can get away with mediocre performance. Although students can provide feedback, it is only visible to the professor, and currently there is no global system for the public and no open ranking of individual courses, that is accessible to all parties interested in education.

In turn, **industry** is relying upon the educators to supply the right skills to the economy. With today's changing business environment, this is not always the case. Supply and demand does the work fairly well, but most would agree that there is a mismatch between the education of the

students coming out of university and the needs of industry, requiring companies to invest in additional training. Verifying the credentials of a student is difficult, and currently this is done based on the ranking of the university rather than individual courses and specific skills and achievements acquired during the courses. Furthermore, the needs of industry have, arguably, changed a lot in the last 50 years. A vast number of new fields and sciences have been discovered, and new technology is being discovered and adopted faster than ever. This needs to be reflected in the current educational offering. Further, the educators today struggle to receive quality feedback and once again this process is not very transparent.

As a result of these issues, external critique towards the educational system has risen in recent years. New technology for online education has opened up for actors which provide free or relatively cheap access to certified education: this includes companies such as Khan Academy, Lynda, Coursera, Udacity, Skillshare and edX. We believe that the next step, which we explore here, is to decentralize the global educational system, and provide a universal platform where individual actors and interested parties, such as students, professors and institutions, can be registered and interact. We imagine a system where (a) the needs of society/industry are reflected in the offering of educators, (b) education is available for all people/students of all skill levels, and (c) records are aligned, secure, visible and transparent for all authorized parties. We believe blockchain technology will be instrumental in achieving this.

In our view, the students of the future will not want to embark on a three- to five- year university programme, for a variety of reasons ranging from financial to opportunity costs. A degree will be deconstructed as an ‘a la carte’ set of courses. Students will also wish to use plug and play models within an international context – studying components in different locations and different contexts, and with some modules being undertaken through face to face tuition and others through blended or completely online means. In this model, the blockchain could serve as a lifelong learning passport that accredits single courses taken over independent time periods and at different institutions. The blockchain’s components could replace a centralized institution’s function of securing and verifying certificates by issuing micro credentials. Those credentials could then be linked to digital CV’s, eliminating fraud and giving the learner full ownership over their qualifications, associated coursework and teacher feedback.

The strategic application of blockchains may dramatically lower administration costs through automation provided by smart contracts and reduce the cost for companies in their search for properly qualified personnel. In addition, it strengthens the link between academia and industry: companies that decide to invest in the educational system can choose to directly influence specific educational trends. They can observe the performance of students, and finance the education of specific good students.

1.2. Previous Work on Blockchain for Education

Among the numerous blockchain-based projects, there have also been a few efforts targeting education. The Japanese tech conglomerate **Sony**[1] just filed a patent that hints the company will be using blockchain technology as part of an education platform. Their blockchain could be used "to store information such as education experiences, certificates and other information" of a user. MIT released their project **blockcerts**[2] as open source code on github. Blockcerts aims to notarize academic records on the Ethereum blockchain, enabling students to hold and share their official records directly with others. A similar approach is followed by another project, **accredible**[3], which hands out certificates on the Bitcoin blockchain, targeting digital education providers such as Rosetta Stone and Google. Another project, **bitdegree**[4], develops an online education platform with token scholarships (dubbed edchain), which is an open-sourced, decentralized library for sharing educational content.

1.3. Overview of our Project and the Rest of this Document

In this project, we propose the **Interplanetary Educational System (IPES)**: a personal, secure and widely recognised blockchain solution for storing international academic achievements and individual educational growth. It enables universal ECTS credits transfer, eliminates fraud and incentivises quality education. It is a private system for securely storing timestamped educational data, associated with an anonymous student ID. At the same time, the information is accessible to all authorised parties, such as universities or companies. In the following chapters we outline the specification, implementation, challenges and outlook for our project.

2. Specification of the IPES

The two key components of IPES are **a)** a token-based architecture that allows efficient educational enrolment as well as feedback mechanism, and **b)** an immutable transparent ledger keeping track of educational credit. There are several stakeholders in the realm of education and the ones considered in this model are: students, educators (and their institutions) and industry. IPES is designed to allow for both, traditional and new ways of achieving educational credit and knowledge acquisition. Traditional educational institutions are basically an aggregate of single educators and can therefore also benefit from the IPES.

Token-based Architecture

Within the field of education, we identify several value streams. The first (and obvious) flow of value is the monetary payment for education. In order for IPES to comply with traditional educational institutions, fiat money will initially be exchanged for institution-bound Priority Coins

[1] https://www.coindesk.com/sony-patent-filing-details-blockchain-use-managing-education-data/
[2] https://www.blockcerts.org/
[3] https://www.accredible.com/
[4] https://www.bitdegree.org/

(PC). The educator (a role which anyone in the IPES network could take) issues a smart contract for each course. A student enrolled at a university, will be given a certain number of PCs that will be used for bidding into being accepted into an educator's course. The one placing the most PCs will get accepted into the course[5]. Upon the completion of a course, PCs will be distributed back to course participants. If, additionally, the redistribution of PCs is done (partly) according to the students' past performance, it renders a system that incentivises good performance and potentially cheap education for top-performers. PCs should not be transferable between individual students.

A second stream of value within the realm of education is the feedback mechanism. It is essential, as quality feedback ensures that a course remains relevant and attractive in a world becoming more and more transparent. In IPES this is implemented by the fact that after completion of a training course, a certain amount of Feedback Coins (FC) are distributed to course participants. The FCs are then used to rate the educator and the course according to some criteria. As the grading of a participant only happens he or she has completed the rating, it is mandatory to do the rating. Of course, the lecturer does only see the feedback before grading is completed, and only in an aggregate form. Course rating will be clearly readable in the course smart contract and tamper proof because of the transparent and immutable nature of the ledger. FCs are only transferable between individuals and course smart contracts.

Educational Credit Ledger

After the feedback mechanism through FCs, grades are distributed to students in the form of Credit Coins. Credit Coins are basically a reference to the course smart contract and a receipt that the student has passed the education and, acquired a certain skill set. The CCs will be added to the students' academic record and therefore readable for all those participants in the IPES to whom he or she provides it. This allows for a more standardized and efficient method of checking the prerequisites when taking courses at different institutions. It also allows the industry to screen the public blockchain for a certain skill set, much like the way LinkedIn is working today.

3. Prototype Implementation during BIOTS

As part of the two-day hackathon during the BIOTS week, we implemented a first prototype of IPES. Due to the time constraint of the hackathon, only a subset of the IPES vision was implemented. The implemented subset was tested with a web interface we created (see next chapter "IPES Platform for Education") and proved to work on the Ropsten test blockchain. All

[5] Fun fact: The idea of an auction-based course assignment mechanism actually originated from a real problem at our university ETH: The courses with limited places available, are assigned according to the first-come-first-served principle. This leads to the paradoxical situation that every student simply greedily subscribes to all the restricted courses, and only later, in a quiet minute, decides which courses to drop again. This makes it even harder for those students missing the initial time window shortly after the opening of the registration: Within 30 minutes most of the courses at e.g. the MTEC department are typically overbooked! The resulting inconveniences, planning uncertainties and strong negative emotions led to the idea of this project.

the source code is openly available and can be found at: https://github.com/ninikolov/EDUCoin/tree/gh-pages.

IPES Smart Contract

The main piece of the implemented functionality is the smart contract[6] `Course`. Figure 1 illustrates its relations to the other auxiliary smart contracts and lists their most important methods and attributes.

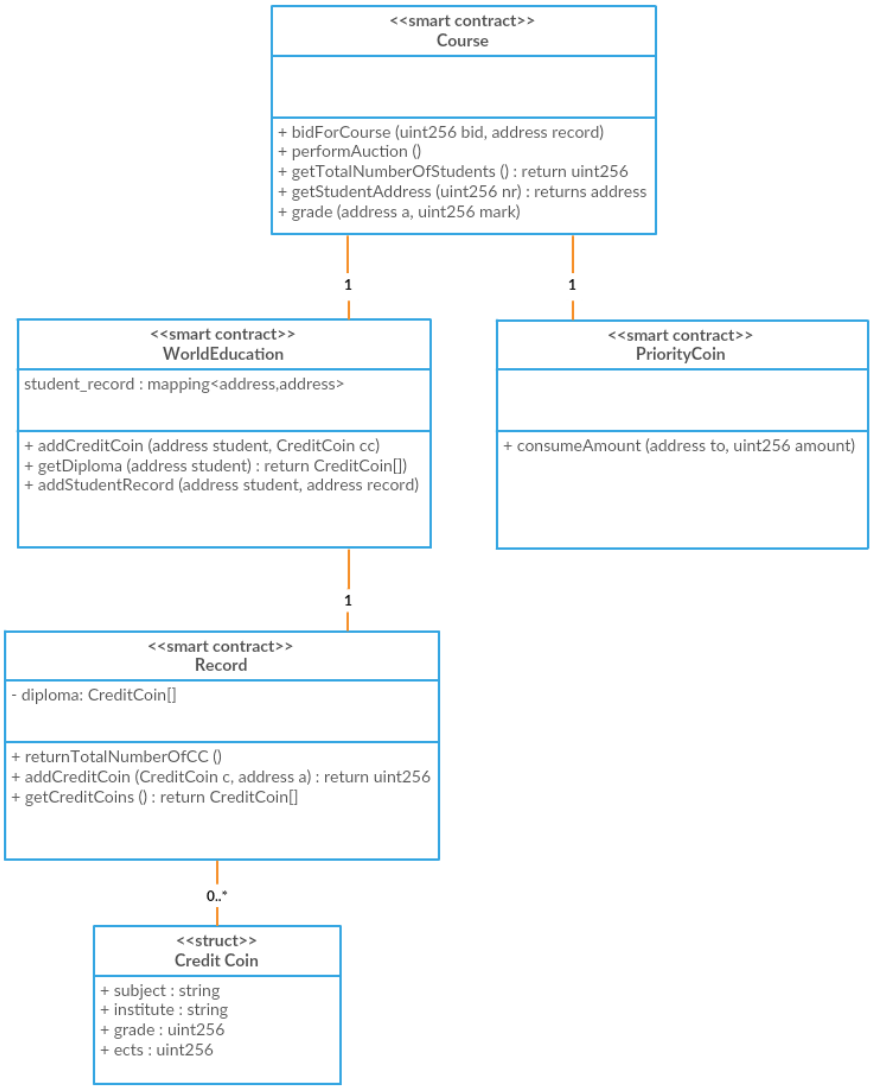

Figure 1. *Simplified class diagram showing the relations between the different smart contracts*

The common data type `CreditCoin` is not implemented as a smart contract, but as a struct. (Implementation note: To make `CreditCoin` globally accessible to all the smart contracts, we

[6] Our smart contract file is located at https://github.com/ninikolov/EDUCoin/blob/master/scCourse.sol.

made them inherit from a common base class called `EduBase` wherein we defined the struct. For better readability `EduBase` is not shown in the figure)

The smart contract `Course` offers functionality...

- ...for the students to bid for a course of their preference
- ...for the administration to perform the auction, and
- ...for the professors to grade their students.

Each of the three functionalities is described in the following sections in more detail.

Bidding for Courses

The student identifies himselfs to the smart contract `Course` by providing the address of his academic record and offers a priority bid ranging from 0% to 100%. The smart contract `PriorityCoin` makes sure that the total sum of biddings does not exceed 100% for any student. Let's assume a certain student intends on taking two courses next semester. She absolutely wants to participate in a certain course, say "BIOTS2019". Therefore, she bets 90% on this lecture and 10% on a course on Politics. If, on the other hand, she was quite ambivalent about which course she prefers, she might have bet 50% on both of them.

Starting the Auction

Once the time window of the registration period is over, someone from the administration office will call the function `performAuction()` on the smart contract `Course`. This will then start the auction process and depending on the algorithm pick, e.g. the top 25 students who bid most on this course and are thus most interested in the subject. One can think of other possible rules and algorithms. Due to technical difficulties we encountered with the handling of data collections (e.g. sorting) in Solidity and due to the time restriction of the hackathon, we implemented a first-come-first-serve algorithm as a placeholder.

Grading

After completion of the course, the professor can grade the performance of the course participants by calling the function `grade (...)` on the smart contract `Course` and providing the students address and the grade (on a unified scale from 0 to 100). This creates a `CreditCoin` with information on the course subject, the educational institute, the achieved grade and the number of earned ECTS points. The `CreditCoin` is added to the smart contract called `WorldEducation` which holds a map of all the world's student's academic records. The academic records of a student are stored in a smart contract called `Record`, which holds basically a list of all the earned `CreditCoins`.

The academic records of a student can then be read from the blockchain and represented as a digital diploma. A possible implementation of a such a (web) interface is presented in the following section.

IPES Platform for Education

In this section, we briefly present the graphical user interface of the IPES: First, we explain how the prototype user interface was implemented during the BIOTS week. Second, we share our vision on how a complete IPES interface could look like, which also gives hints on how to include functionality that is not present in the existing implementation. In both cases, we will provide visual examples in terms of screenshots and wireframes respectively.

Basic Implementation

In order to provide a convenient and intuitive way to interact with the Ethereum powered back end, we chose to implement a browser-based GUI that is powered by the popular *web3* API. *web3*[7] is a simple to use programming interface between conventional JavaScript and the Ethereum blockchain.

Technical Details

In a first step, we specified the signatures of the provided functions as JSON interface objects[8]. After encoding these function signatures into ABI (Application Binary Interface) signatures, they could then be called directly from JavaScript. In this way, it is possible to call Solidity functions right from JavaScript code running in the browser, but they will be executed on the Ethereum Virtual Machine. In general, it takes a little while until functions are executed on the blockchain and the results are returned. Therefore, when invoking functions that run on the blockchain, web3 allows to provide callback functions which process the returned results, update the front end or handle potential errors.

Screens

We implemented two basic screens, the **student view** and the **educator view**. From the student view (see Figure 2), students can provide the address of the smart contract that represents their digital CV. The courses they enrol for will be appended to this CV upon completion. After identifying using the address of their digital CV, on the left-hand side of the interface, students can see the academic achievements that have been registered on their account in the form of `CreditCoins`. On the right-hand side, students see a list of all available courses, and they can bid for their courses of interest using `PriorityCoins`. To see a brief live demo of the current state of our system in action, we composed a short video clip at https://youtu.be/2BY7hbi31YY. The video illustrates the process of bidding for a course on our system using our user interface and the MetaMask[9] extension.

[7] https://github.com/ethereum/web3.js
[8] https://web3js.readthedocs.io/en/1.0/web3-eth-abi.html
[9] https://metamask.io/

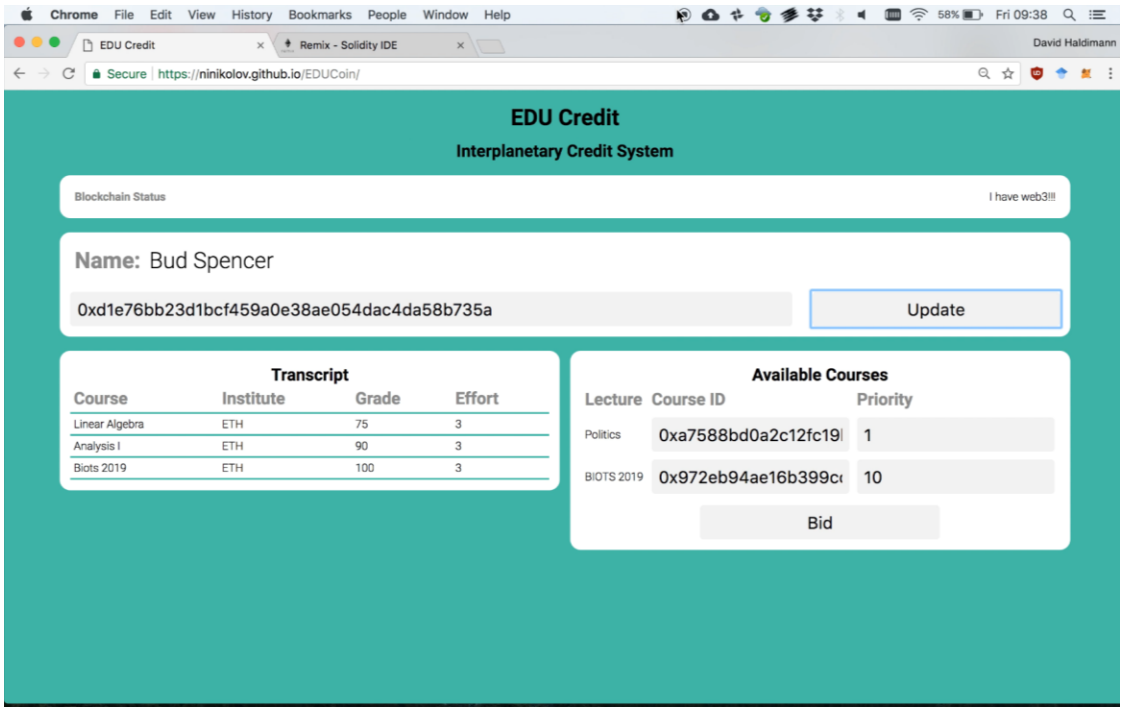

Figure 2: *Student view that presents the prototype user interface for student users. The current transcript is shown on the left-hand side, the available courses are on the right. The student needs to manually insert the address of the smart contract that is associated with his academic record, i.e. his CV.*

The most tedious and error prone step in the current workflow is the insertion of the smart contract address. This step could be easily circumvented by using a third-party service that links the identity of the student to his academic record (and is potentially based on blockchain as well, see efforts to create digital IDs[10] on the blockchain). With this modification, the user would just simply login by proving his identity at the device he is using, and the system would automatically understand what is the academic record that is associated with this user.

The educator view is implemented in a similar way, with the difference that the educator needs to provide the course code (via the address of the associated smart contract) and he can then administer his course on the web page by letting students enrol for it, closing the bidding period and starting the class, requesting feedback and submitting grades to each of the students.

Future Vision for the User Interface

In Figure 3, we present an illustration depicting how the user interface of IPES could look like in the future. Our vision is that IPES will show a single, combined academic record to each student, enlisting the courses he has completed from multiple academic institutions. In this way, achievements from universities, internships, online classes or from any other educator can all be viewed in one place. When applying for a job, the student can give direct access to his

[10] https://themerkle.com/6-blockchain-based-digital-id-management-platforms-to-keep-an-eye-on/

achievements to the hiring manager which - in turn - can fully trust the information on this blockchain-based platform.

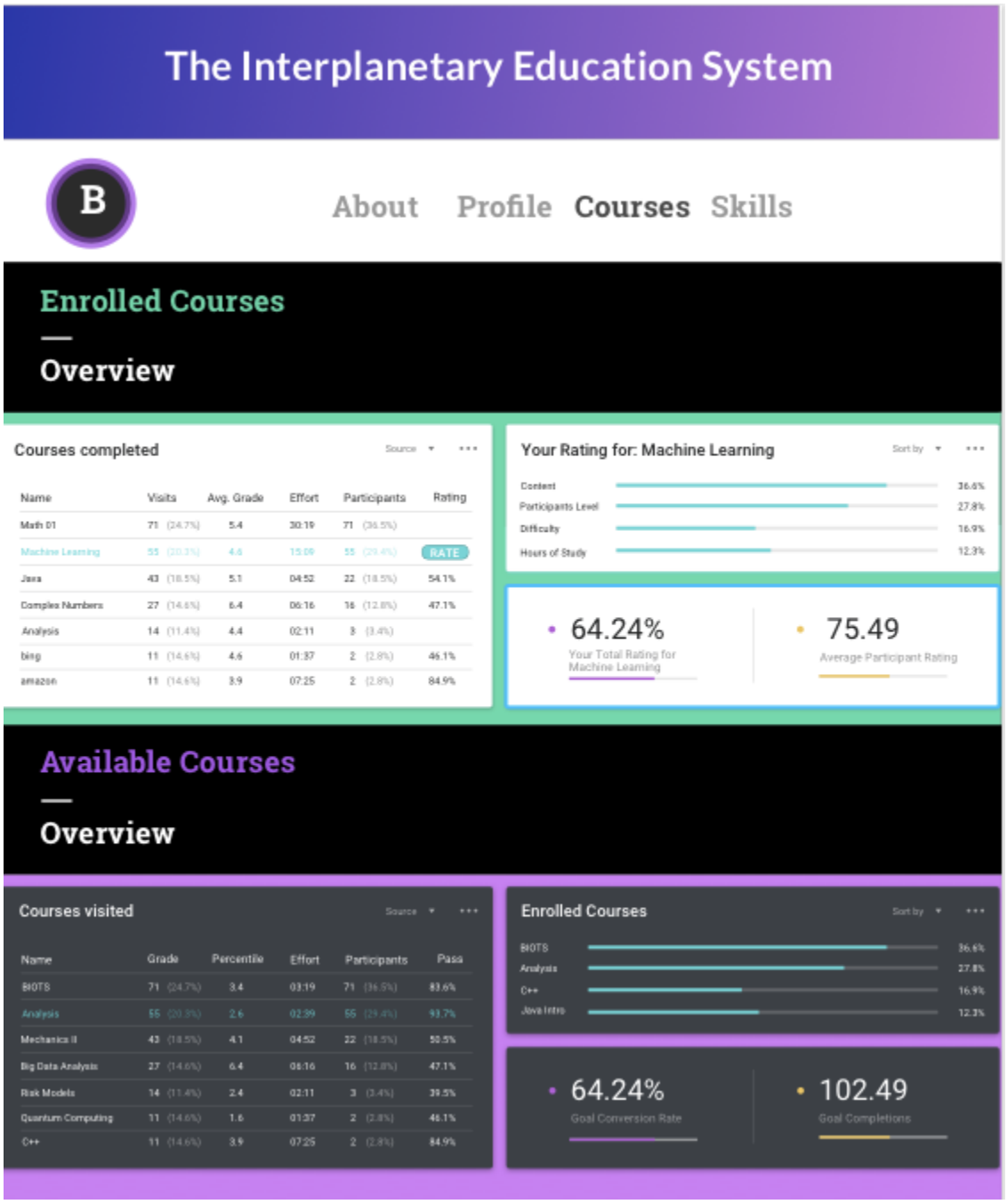

Figure 3: *Illustration of our vision for the platform. In addition to the lists of completed and available courses, the student can also view statistics on the courses of interest, provide feedback, and more.*

4. Evaluation and Future Work

Most of the core functionality that was originally envisioned for this first prototype was implemented, although there is still work to be done. For example, none of the permissions were dealt with, such that anyone could create multiple courses and fill up their own record with `CreditCoins` or a new malicious smart contract could be written that directly accesses `WorldEducation`. On the other hand, this opens up our platform to any educator that gives classes, online or offline, and with the feedback system only the well rated classes would generate meaningful `CreditCoins`.

One security feature was implemented that prevented students to complete courses on behalf of other students by requiring the students that complete the class, also to be the owner of their `Record`.

As mentioned previously, the evaluation of the bids was not implemented as planned. It should be considered whether that should be computed off-chain. The `PriorityCoin` implementation is missing a function where `PriorityCoins` are returned, when a student fails to sign up for a course. The `Course` smart contract contains most of the functions implemented. When submitting a bid for a course, the students user ID is linked to his record. This is necessary later on, when the `CreditCoin` are passed on to `WorldEducation` along with the student's user ID. Only then the `CreditCoin` is added into the student's record. Also, another security measure should be put in place that makes sure that a `CreditCoin` is granted multiple times for the same student. This could be easily solved by having a list of all the students which gets updated when the `CreditCoin` is sent to the student record.

One feature that wasn't implemented was the feedback system and the integration of such a system to incentivise students to give feedback on courses. Lastly, a point that requires further elaboration is the hard-coded name of the institute and the hard-coded number of ECTS a course gives. This could be changed quickly, such that this information is provided in the constructor when a course is created.

One exploitability mentioned during the week was the "reentrancy attack". This kind of attack manages to exploit smart contracts by recursively withdrawing currency from the smart contract before the smart contract is able to set the updated balance. Attacks of this kind would not affect this kind of platform as there are no smart contracts that return any kind of currency. Also, the `CreditCoin` objects are issued by courses where only the educator can send them out after the students have completed the course with a passing grade. This means, it should not be possible to create such a malicious recursion.

Overall this prototype contained most of the core functionalities:

- The `Course` smart contract can be created by an educator
- Students can sign up by bidding for courses
- Student's `Record` are linked in `WorldEducation`

- Educators can grade and send `CreditCoins`
- Students can receive `CreditCoins` for completing the course

These features form the basis of our platform. The next step necessary would be the implementation of the feedback system. Courses would receive a rating, quantifying the value of the generated `CreditCoins`.

Overall, we also did not consider in depth the management body that would oversee the IPES or if there would be formalized management of the system at all. Many of the current platforms or environments enabled by blockchain technology struggle with their correct and appropriate management. The great value that is provided by such a technology is that it is truly decentralized. This allows for more pure economies to play out regarding supply, demand and pricing of the overall assets (in our case education and learning). Yet there is also a need to facilitate the system, make updates to the code underlying the system, settle disputes and agree on standards. Additionally, we would need to determine who would make the initial effort to convince educators and students on the platform. This is a topic that should be considered independently but is equally important to the potential success.

5. Conclusion and Outlook

It is clear that education will look very different in the future. Education is now being seen as a lifelong journey rather than a singular time in life. A connected digital world is democratizing our access to information. Our world is changing at an unprecedented pace and those that are able to adapt, learn new skills and clearly demonstrate their knowledge will be the most valued. Likewise, educators will be valued in direct proportion to the value that they bring to their students rather than the “prestige” of their background.

In order to build for this future, we have envisioned the IPES as a decentralized, secure, and open education ecosystem. Through a decentralized platform, we create an economy of performance for both students and educators, where those that perform will be equally rewarded. Likewise, the education that is offered will be better matched with the needs of industry and the greater public by allowing them to incentivise students and educators with Priority Coins. By disintermediating the role of educational institutions as brand, and better matching education offered with the types of skills demanded, we also hope to decrease the cost of education to the student and hold academic institutions accountable (e.g. universities in the United States).

In just two days in the BIOTS 2018 hackathon, we developed a model for the vision we assigned the working title “EDUCoin” that we believe can have a profound impact on the educational system if implemented. Our diverse team has a background of Computer Science, Engineering, Artificial Intelligence, Business and Innovation coming from both academia and industry. All of us have experienced the mismatch between education and industry, expected and actual educational quality and the lack of transparency of courses and institutions. EDUCoin is however still in its infancy and will need the support and motivation of students, institutions and industry to become

fully realized. With this paper and our code base which we have licensed under creative commons, we hope to light a spark that others can carry forward. We believe that open source is the best model for the application of EDUCoin and encourage others to contribute to a better future.

To conclude, let us take the example of the journey of one student, Anna, in the IPES ecosystem. Anna logs in and searches from a countless number of courses provided from institutions like ETH or Harvard, online platforms like udacity or even individual educators. Each course on the marketplace is assigned a score based on the previous feedback and a price that is competitively bid on by students using Priority Coins. Anna then bids on a number of courses using the Priority Coin that was given to her as a scholarship from a company that she is interested in and who found her from her IPES profile. After winning and successfully completing her courses for the semester, she receives EDUcoins which will be held securely in her personal digital wallet. As Anna collects more EDUcoins her profile will become more and more attractive to potential employers, research institutions and donors which will help fund her continuing education and get a job. Throughout her career, Anna can continue to learn and adapt to her interests and needs by proactively building her education. With the IPES, Anna, like many future students would have better access to quality education, that is adaptable and competitively matched to industry and that she has full control over.