The blockEDU Protocol

A Peer-to-Peer Education Network

July Xth, 2017

Nathan Ginnever
Dylan Lott

Abstract

BlockEDU is a protocol token built on-top of the Ethereum blockchain and a network of distributed reputation where data is stored in a private and decentralized cloud. BlockEDU implements a consensus mechanism similar to that proposed by backfeed [cite backfeed] called Proof of Affordable Education. It is an alternative education protocol that can host free--and open source--course management systems (CMS) where Distributed Open Collaborative Courses (DOCC), Small Private Online Courses (SPOC), Massive Open Online Courses (MOOC), and institution free traditional universities can be explored. The goal of BlockEDU is to solve some of the apparent issues with current accredited universities as well as online courses in a way that makes quality and reputable education affordable and accessible to all. BlockEDU offers the ability for anyone to create custom courses or structure degree programs that conform to current academic paths without the centralized trust provided by the current system. BlockEDU will remain an uncontrolled non-profit that has no ability to impose any unnecessary fees on students or educators. There are no C-titles that will take unreasonable profits from this organization, and it will remain a community driven project throughout its lifespan.

1 Introduction

The question has been raised as to whether institutional universities are continuing to provide an affordable and quality education for students. The increase of student loan debt to income ratio has caused many students to begin looking for alternatives. Alternative forms of education enabled by the web have become a popular industry in the past decade as students face increasing tuition rates and the inability to afford traditional accredited universities. With MOOCs you do not need to be geographically close to your institution of learning. As long as the academic community has an internet connection and a cursory knowledge of technology they may connect with each other to advance knowledge. Online institutions such as Udacity, edX, and Coursera have seen success as a perhaps viable way of spreading mass education at an affordable price. They promise to offer affordable and accessible information to those who otherwise would not have had a chance to learn. BlockEDU is an attempt to aid in Goal 4 of the 2030 Agenda for Sustainable Development where the UN has envisioned a way to ensure inclusive and quality education for all and promote lifelong learning. It is encouraged that all existing education platforms, online and offline work together to achieve this goal. One can imagine traditional universities such as Harvard and MIT and online systems such as the MOOCs listed previously committing to this consensus and building their governance model on-top of blockEDU.

2 Problem Statement

[research education outside of the united states, it is clear that the industry only cares for profit here, but other countries should receive credit for doing it better]

Education has become a booming industry [pull stats on education industry]. What was once thought to be a service to society has become a system where companies can take profit from a core need. Organizations that once started with a non-profit business model have inevitably moved towards institutionalization, advertising, and profit. These evolutions toward a profit are methods to sustain the organization, whether that be attracting better educators and affording better tools, or sustaining the non-profit business. The industry of education is run just like every other industry, with profit as its only goal.

2.1 The MOOC Profit Model

Every system has a cost to building and maintaining its infrastructure and systems such as the platform provided by edX try to encourage the open source community to do this service to

reduce costs, however their open source system is hard to run, populated by advertisement software, and enables the creation of an entire industry of cloud service providers to take even more profit from students and teachers. These systems are too complicated to set up and it is advertised that these providers are creating a valuable service for educators. edX thus creates a proprietary system that has salaried employees to create a quality platform. Developers and maintainers should be paid fair wages for creating these systems, but online universities and course management systems fall into the same pattern as traditional universities where CEOs and CTOs taking large salaries at the cost of both the student and educator.

2.2 The University Profit Model

Offline Institutions are also failing to keep courses affordable for students and are facilitating the rise of online education. Current institutions have too many auxiliary fees that don't benefit the student such as administrative fees. Higher up positions such as deans and CEOs are taking multimillion dollar salaries [source open information on actual salaries]. The increase in student loan debt discourages students from enrolling in traditional universities. Teachers are incentivised to keep course material proprietary as a way to produce income.

[source student debt information]

2.3 Accreditation

Universities maintain their place in society because there is nowhere else for teachers to have the reputation they need to be trusted. Until recently it has not been understood how trust can be accomplished without a centralized authority to issue it. [more research into the need for accreditation, question why it has to be granted from a university. Trust models will be discussed further down in the rep system. We will be describing how we can offer trust without a central authority. Perhaps create an analogy to CA problems vs web of trust]

2.4 Lack of Personal Interactions and Feedback in MOOC

MOOC lack a flexibility that allows the community to decide how courses should be structured. Some Universities have expressed concern that the massive nature of MOOCs or the need for those involved to understand technology or a lack of a strong sequenced structure makes them unacceptable. They often forget about foreign language speakers and only cater to English as they are not able to coordinate on a local level. These MOOC systems fail to explore the difficulties of relevance and knowledge transfer across borders.

The ability to scale class sizes up is potentially one of the largest weaknesses presented by traditional MOOCs and institutions. There is often a lack of interpersonal connections and diversity in scope that cater to all types of learning. Because of this there are large incompletion rates and only a select few that will succeed from MOOCs. Others will drop off and lose money

to a for-profit institution. Large class sizes also limit the ability of the educator to learn better ways of structuring their courses in the future. Teachers often report that personal feedback is a valuable resource for both educator and student.

[site algebraic reasoning] A case example of the value of personal feedback can be found in teachers and researched beliefs about the development of algebraic reasoning in high school students. In this example the teachers must organize their mathematics testing and problem sets by their predicted difficulty for students. Textbooks sometimes are not a reliable source for this reasoning. "The Symbol Precedence Model of development of algebraic reasoning, in which symbolic problem solving precedes verbal problem solving and arithmetic skills strictly precede algebraic skills, was contrasted with the Verbal Precedence Model of development, which provided a better quantitative fit of students' performance data."

3 Proposed Solutions Overview - Why Decentralize?

[overview of why decentralization is a good idea here]

3.1 Profit Solution

BlockEDU offers an easy to use platform for educators and students such that there is not a need for unnecessary technical installations or cloud data solutions. This reduces the costs burdened to both educators and students that were once forced to pay for services to run CMS.

BlockEDU puts forth an idea that using decentralized technologies can enforce a non-profit model that is self sustaining. The organization is maintained by reserving a portion of the total supply of EDU tokens. Doing so commits the organization to being only worth what the community believes it is worth. As the free market decides to support or not support blockEDU

3.2 Consensus

To encourage that education remain free, we present a consensus model that rewards educators for maintaining a free course. Just as bitcoin [site bitcoin] maintains consensus on the correctness of financial transactions, blockEDU maintains consensus on the idea that education should be affordable. The consensus protocol incentivises educators to not charge students for their service. While giving education and course content away for free is not mandatory, the protocol rewards teachers that maintain this standard, and does not reward those that charge money for their time and content. [backfeed] "These mechanisms ensure a fair distribution of the generated value to each individual, according to the perceived value of their respective contribution to the organization as a whole."

3.3 Accreditation

[write general overview of how distributed systems offer an alternative to centralized trust]

3.3 (a) Educator Reputation

The blockEDU protocol creates the ability to use distributed reputation in a way that provides the accreditation needed for students to trust that they are getting a quality education, and to pass this knowledge forward to future employers or education groups so they may trust that a quality education was provided. Educators can also use this proof as a way to demonstrate their value to other educators and for side organizations that encourage the development of knowledge in their specialty.

3.3 (b) Student Reputation

Each community member has their course records permanently printed in the Ethereum blockchain. Students maintain these records on a distributed cloud storage platform with encryption keys so that they always retain who gets to see their achievements. To prove the accumulation of knowledge to the protocol, smart contracts read course completion registers that allow them to unlock more advanced courses. In this way you could imagine building entire degree paths on-top of the blockEDU protocol.

3.4 Personal Interactions

The possibility of peer-to-peer education will ensure that the community always forms the organization. There will be no centralized authority to dictate how a course should be sized, scheduled, or monetized. Courses are never limited to the constructs of a few, but rather molded by the masses

Privacy and a lack of censorship are built into the systems used by the blockEDU protocol to avoid potential issues with control mechanisms such as authoritative governments outside of the protocol.

Choice is a core tenant of blockEDU and if other organizations are not comfortable creating a decentralized community, they may choose to establish a more traditional centralized and permissioned university role. You may set the permissions on your course contracts to allow anyone to join or only those that you deem fit or that have completed enough prerequisites.

Just as massive course structures are possible so are small localized communities with personal interaction. You can choose the max number of identities that may register in the course contract. If you wish to keep a course small it is as simple as limiting this number and

structuring the course to use the frontend CMS forum application to facilitate personal communications. You may also use the system to advertise local meetup facilities that will happen at predetermined times. Ultimately the members of this community get to determine where they belong and what works best for them.

4 Protocol

Here we present an in depth look at how the blockEDU protocol is structured. The protocol is inspired by the blockchain system and the work done by backfeed. BlockEDU can be seen as a subset of the backfeed protocol in that it is not generalized to distributed governance but instead localized to education specifically.

4.1 Consensus - Proof of Affordable Education

Analogous to bitcoin's proof of work scheme (PoW), proof of affordable education (PoAE) will be the burden of proof placed upon educators to receive financial incentives. Similar to the work done by backfeed [cite backfeed paper], blockEDU will use a distributed reputation system to provide proof to the Ethereum smart contracts that courses were taught in a valuable way. Educators will be rewarded from the total reserves of EDU tokens created much in the same that mining occurs in other cryptocurrencies. Proof must be supplied in reputation that course was of value to the students. A monetary reputation is assigned to the educator as a separate unit to decide that it was done for free by the students. This of course can not be enforced in any digital protocol as teachers are free to charge in any fiat currency they like outside of the system. However students do have a course of action to ensure that teachers are not paid twice in EDU by lowering the PoEA reputation at the end of the course. A student may get a good education from a teacher, but still assess a false monetary flag for the course. If either of those conditions is broken, the teacher will not be paid out from the reserve token.

A special choice is uploaded to the course contracts once completion of the course has happened. The choice is whether or not to reward the educator for mining the course. This gives students the ability to give a reputation to each individual course taught so that there is a mechanism for deciding if the course was of quality and affordable. This decision is uploaded by the context area agent for that course and determined locally by assessing the recommendations given by the students in the reputation system and assigned as a binary value [0,1] upon course completion. This binary decision is not recorded by the agent in the reputation system but it is derived from it.

4.2 EDU Tokens

EDU represents the unit of consensus that education should be affordable. EDU is an ERC20 standard token. The total supply is held in reserve on the Ethereum blockchain. The tokens provide a method for rewarding the educators after completing the proof scheme and maintaining the consensus that education should be free. The tokens will work as method for students to provide a fee for entering the courses. These tokens also provide a way to unlock the data storage needed to hold course material and student records permanently and securely.

4.2 (a) zEDU Tokens

To continue with the objective that any users in the protocol may remain private, we offer a mechanism for converting traceable Ethereum tokens to [ZKSNARK] protected Zcash tokens. While still in the early stages of development during the time of writing this, blockEDU will provide a method for atomically swapping the ERC20 token for a future standard Zcash token. This is done by [cite sapling, read method]... This will give private payment methods to both students and educators in the unlikely event that education becomes oppressed or deemed illegal by certain authorities.

4.2 (a) Mining Tokens

While there is no computational methods of mining or stake to ensure the network reaches consensus, a loose analogy to bitcoins [site bitcoin] mining can be made in the sense that tokens are still distributed from a total supply when a proof has been established. As stated in 4.1 the proof here is the reputation score of the course after completion.

4.2 (b) EDU Blocks

A course in the protocol is like a block. This is similar to bitcoin mining where miners create blocks of transactions to be rewarded but instead teachers are creating courses filled with knowledge. The proof attached to each block, or course, in this sense is the reputation ratings derived by the students, and the ability for the system to check that the course was provided in an affordable way. During the mining process in bitcoin, mining hardware computes hash values until it hits a certain target. In blockEDU, teachers will produce informative education until the course duration runs out as their mechanism of work.

4.2 (c) EDU Transactions

Transactions in the protocol are represented by passing information to students. If a block is a course then you could imagine filling the block with information. These units could be homework assignments, lecture slides, or any other method of educating a student. The correctness of these transactions will be judged by the student at the end of the course. (Perhaps explore a

test at the end of the course that could determine the understanding students have gained through the course of transactions. We do want to avoid standardized tests if possible but this could be an interesting proof mechanism in addition to the rating from students. This would need some overseeing authority in the field of knowledge to determine what tests would satisfy that a student learned information).

4.2 (d) Token Fees

Fees are an optional parameter set by the student before entering a course. Instructors may choose to pick up students that provide a higher fee for entering the course. This is analogous to a bitcoin transaction fee, where a miner is rewarded an extra amount for picking up this transaction into their block. When the total reserve of EDU runs out in [calculate time it runs out] this will be the only remaining reward for educators.

4.2 (e) Reserves

[formulate exact details on the reserves and the deflation of issuance]

4.2 (e) Block Rewards

An issuer contract holds the reserve of all tokens that will be issued to educators. When a course contract is completed, an agent responsible for storing the reputation will call the [create function name] function that sets a boolean value for each the monetary reputation [was this course provided affordably or free?, decide on that] and sets the course value integer in the range [0,1]. The course instructor may then call the finalize function on the issuer contract to be awarded iff the course boolean is true, in the proportional amount to course value integer between [0,1]. For example, if Alice completes a math course with an affordable boolean of true, and value integer of 0255 (solidity does not have floating points so we represent them as ints) then Alice will receive 2.55 EDU for her course. Fees are not included in the boolean reputation rating.

5 Trust

Trust plays an important role in the blockEDU protocol since there is no central authority to disseminate trust to the participants. Here we present some definitions of trust as presented by research [cite research].

5.1

6 Distributed Reputation System

The distributed reputation system deployed in the blockEDU protocol is based on the research done in the UniTEC system [cite UniTEC]

6.1 Overview

[summarize general how the system works]

6.1 (a) Identity

Identity in our system is in the same format as Ethereum [source the format, 160 bits, encoding details]. This gives our reputation system the ability to sign transactions on the blockchain that correspond one-to-one with the signatures in the reputation system.

Other forms of identity are required to work with the Orc Network and Zcash tokens (should privacy in token be required). These identities work the same way with slightly different formats [discuss orc / zcash format].

As to not burden each user of the system and fulfill the requirement that the protocol is as easy to use and easier to set up than current systems, blockEDU provides a service on the network that is entrusted to manage the private keys. In this way, students and teachers can simply remember a username and password, however, it is encouraged that those who are willing to store their own private keys do so.

6.1 (b) Agents

Unlike users that solely interact with the CMS on-top of the blockEDU protoco, and subsequently interact with agents. Agents are full nodes on our reputation network that provide a service to the user community. They report the reputation records, they maintain the reputation database, and find trust paths so that the ease of use requirement can be fulfilled.

Each agent/s is responsible for managing a context area in the network. It is encouraged that these agents are selected by the community for having some interest in promoting the health of their academic area. As they are responsible for connecting each user to the reputation system, and the reputation system is the proof scheme responsible for maintaining consensus, it is essential that these node be trusted and transparent to the community. Any user may decide to run a full node and advertise themselves as an agent. Ideally the entire network would be made up of agents and not user.

6.2 Modeling

Below we describe the models of the distributed reputation system as formed by UniTEC, the trust, knowledge, and system models.

6.2 (a) Trust Model

Trust Context Areas

As the UniTEC paper describes, trust is not all-encompassing. Instead people's trust is relevant to a certain context. Someone who is trusted to repair your car should not have this trust translated over to another context area of say babysitting your children. The context areas in the blockEDU protocol are partitioned by knowledge areas i.e. Mathematics, Physics, or Literature. We also have to superset context areas to differentiate students and teachers.

Due to the complex nature of trust, the system will be comprises of interdependent context areas. Each context area has a trust value in the range from [0,1] and a given confidence vector in that user for giving the recommendation of that value. In this representation, 0 indicates that there is either no previous experiences with the user in the given context area while a 1 represents maximum trust in the user for either teaching a course, or being an experienced student. I may trust Alice with a value of 1 meaning that I believe she is a capable English teacher.

The confidence vectors store metadata that defines the quality of trust in the entity and contains the following entries:

- Number of direct experiences in that context area
- Number of indirect experiences (from context areas influencing the one in question)
- The last N direct experiences
- A blacklist (set by the user to prevent recommendations from certain identities)

Keeping track of the number of experiences with another user's gives the system a way to calculate trust on the fly. It is a parameter to the trust update algorithm as discussed further in [get section number].

6.2 (b) Knowledge Model

The UniTEC system develops the knowledge model as a "local profile stored for each user to create a view of "who knows what" including the user's own knowledge. Hence it is used to communicate one's own expertise as well as to learn about other's expertise."

The cardinality of the set of personal recommendations is stored to build the *own expertise* indicator for a certain context area. Figure 6.2 shows an example of how these recommendations are stored to build this expertise. We do not currently explore pseudonyms for each participant where a user could have a different name for each context area they have knowledge in, but this has been done in the original UniTEC design.

To evaluate the *expertise of others*, we store the number of recommendation requests a user gets for each context area. This is also how we express each user's understanding of a context area.

[figure 6.2 Sample Knowledge model entry]

Definition (Authority): *Someone that is expected to have a direct knowledge of the given context area and can provide helpful recommendation in that area.*

Definition (Hub): *Someone that does not have a high level expertise in any one particular context area, but knows many Authorities that do.*

Recording both of these pieces of information allows us to to discern information about each user's expertise as an authority (likely a teacher or advanced student themselves) or a hub (perhaps a dean of a university or a teacher's assistant).

6.2 (c) System Model

Our system will be comprised of both light clients (end users) and full nodes. Full nodes will be responsible for storing both the trust and knowledge models described in section 6.2 (a) and 6.2 (b).

[create a graphic here showing the two top level context areas (student and teachers) as a well as the subsets for each (the different academic areas of interest). This will give an idea of how neighborhoods are formed and how trust will be built by what is relevant to each individual user]

6.2 (d) Recommendations

6.3 Interactions

6.3 (a) Publishing recommendations

6.3 (b) Handling Requests

6.3 (c) Collecting Responses

6.3 (d) Handling Feedback

6.4 System Architecture

The UniTEC research uses a CORAL DHT as a method for distributed communicating and storing the reputation information that has been laid out previously. blockEDU uses a pubsub DHT for communicating, however we diverge from UniTEC here by storing reputation data directly in the blockchain.

7 Distributed Cloud Storage - Orc Network

[cite Orc]

A persistent data storage network is needed for both educators and students to store course content and reputation records. The Orc Network offers [Have at it Gordon]

8 Ethereum Contracts

Ethereum is a decentralized network of nodes that process transactions and maintains consensus on general state. [give better def and cite Ethereum]. Ethereum is used in the blockEDU protocol to maintain the state of reward system in place for educators. It will provide a mechanism for unlocking courses / course content, it maintains the identities of the users in the system, it provides the registries that provide pointers to the current state of the applications running on the protocol,

8.1 Ethereum Shortcomings

Storing data in the ethereum network is expensive. [gather details on op storage costs per byte of hex data]. Ethereum is used as the network to provide a decentralized point of authority on the state of the blockEDU protocol. There will be a large amount of transactions to this state machine and as a method for offsetting the costs we propose two solutions.

8.1 a State Channels

[state channel research here]

8.1 b Linked Data pointers

The Orc Network provides meta information as to the location of uploaded data in the distributed network. This meta information is updated in the state of the contracts as a way to offset the data storage costs of large data such as written recommendations on the blockchain.

The meta information needed to locate a file on the Orc Network is as follows.

```
* @param {String} id - Unique bucket ID
* @param {String} file - Unique file ID
```

Each string is a X bytes of X hash algorithm. The maximum registry size for the Ethereum VM is 32 bytes so concatenation of these two fields fits into one register with an MLOAD instruction. The total cost for a X byte MLOAD instruction is X units of gas. [fill in the Xs]

```
pragma solidity ^0.4.11;

contract OrcDataPointer {

    address owner;
    bytes32 pointer;

    modifier onlyOwner() {
        if (msg.sender != owner) throw;
        _;
    }

    /// Create ownership of this pointer to data.
    function OrcDataPointer() {
        owner = msg.sender;
    }

    /// resets the pointer.
    function removePointer(address to) onlyOwner {
        pointer = 0x0;
    }

    /// Update the given pointer to a new state of the data.
    function updatePointer(bytes32 _pointer) onlyOwner{
        assembly {
            pointer := mload(add(_pointer, 24))
        }
    }
}
```

Figure 8.1 Simple contract to store pointers to the orc network.

As shown in Figure 8.1 a simple method in a contract can be used to load pointers to Orc data onto the Ethereum blockchain to reduce the cost of storing actual data. The above example uses a permissioned modifier to ensure the community is not able to destroy data pointers, and thus the data itself, if they do not own it. It should be noted that the above example does not give an accessor function to the loaded data.

8.2 Issuer Contract

The issuer contract is the mechanism in which educators are paid for mining and maintaining consensus.

8.3 Course Contracts

8.4 Registry Contract

9 [create a name] - The first CMS

The first CMS is built by blockEDU on-top of the protocol token, reputation system, and Orc Network It is not necessarily the only system that can be built. Other organization that are currently in existence are welcome to replace their backend with the blockEDU protocol and auxiliary systems like the Orc Network distributed storage method presented here. [enter name] serves as an example of this may be done.

[description of the CMS we are building, similar to udemy]

9.1 Client Application Features and Scope

9.2 Requirements Analysis