

Semantic Blockchain: Credential Certification Mechanism

S. Matthew English
english@cs.uni-bonn.de

Héctor Ugarte
s6heugar@uni-bonn.de

Sören Auer
auer@cs.uni-bonn.de

Rheinische Friedrich-Wilhelms-Universität Bonn
Fraunhofer-Institut für Intelligente Analyse und Informationssysteme IAIS
Bonn, Germany

Michelle Bachler

Kevin Quick

John Domingue

{michelle.bachler, kevin.quick, john.domingue}@open.ac.uk
KMi, The Open University
Milton Keynes, UK

ABSTRACT

The “blockchain” is run on a peer-to-peer network. It is a data representation model which constitutes an append-only ledger for time-stamped, freely available information. The best known application of the blockchain is the cryptocurrency Bitcoin however the emerging concept of “blockchain 2.0” applies the same technological underpinnings to a host of different domains. Insofar as this compute paradigm now constitutes a significant, and growing, portion of open data available on the Internet it will be integrated into the Semantic Web. Our initial challenge then is how to describe the blockchain using an ontology that remains applicable under rapidly evolving circumstances. To this end we propose an extensible ontology designed for this purpose. The absence of meaningful semantic content intrinsic to the blockchain provides a further challenge to its interoperability in the web of data. This is a consequence of the pseudo-anonymity that was a cornerstone of the Bitcoin application. Accordingly we propose a methodology for imbuing the blockchain itself with rich semantics. We examine how the decentralized nature of the blockchain network can be exploited to strengthen the persistence of the URI naming scheme of semantic data. Subsequently an assessment is made of the impact of our approach to the efficient handling of educational credentials on the Web. This paper concludes with a use-case scenario of our certification ecosystem built atop blockchain infrastructure.

CCS Concepts

•Information systems → Distributed database transactions; Resource Description Framework (RDF);

Keywords

Blockchain, Semantic Web, Linked Open Data

1. INTRODUCTION

“What is all knowledge except recorded experience” -
Thomas Carlyle (1795 - 1881)

The Semantic Web has been described as heralding the age of “Web 3.0”. Increasingly this accolade is applied to blockchain technologies. The concept of peer-to-peer applications is not new, nor is the concept of distributed hash tables. What emerged in 2008 with the publication of the Bitcoin white paper [10] was an incentive structure that unified these two software paradigms with a set of economic stimuli to motivate the creation of a dedicated computing network orders of magnitude more powerful than the world’s fastest supercomputers. The purpose of which was the creation and continued maintenance of a web-scale distributed database known as the Bitcoin “blockchain”. Apart from the digital currency it enables the concept of a blockchain is a fascinating new computing paradigm with potentially broad implications for the future development of the World Wide Web, and by extension, the further growth of Linked Open Data and the Semantic Web [3].

We commence with a general assessment of the current state-of-the-art in the “semantification” of the blockchain, introducing the ontology we have engineered for this purpose. Subsequently we hone in on the problem of recognizing achievement in the emerging realm of massive open online courses (MOOCs) in addition to other non-traditional educational environments, to demonstrate the practical applicability of our approach.

Having established a grounds for our efforts, we introduce the conceptual framework of a fully functional *Semantic Blockchain*. This system, to the best of our knowledge, constitutes a hitherto unexamined approach towards the unification of the Semantic Web and blockchain technologies as part of a single, mutually beneficial framework.

We start by describing first principles and progress towards demonstrating our fully actionable solution. We evaluate the technical work we have undertaken towards realization of the benchmarks described in the previous section with the introduction of a blockchain-based decentralized application for the certification of academic credentials.

Although blockchain is a relatively recent phenomena it draws on a rich history of pioneering research. Recognizing the achievements of our peers, and the industrial efforts in the domain, we consider the related work and juxtapose it with our own implementation.

SEMANTICS '16, September 12-15th Leipzig, Germany

ACM ISBN 978-1-4503-2138-9.

DOI: 10.1145/1235

The next section briefly touches upon some of the future work we are undertaking that bears a close relation to the sections described above.

With the concluding remarks we recapitulate and set forth our conception of the most likely course of further development at the intersection of blockchain technologies and the Semantic Web.

2. BACKGROUND

The blockchain facilitates a resilient and highly distributed ledger for recording transactions, attributing them to a specific node in a network, and ordering them in time. This is the functionality that undergirds the cryptocurrency Bitcoin (BTC), among others. As Bitcoin was the first and best known instance of an application running on a blockchain we examine it in further detail to shed light on the ideas and processes relevant to this work.

The blockchain is made possible through a process known as “mining” whereby a large number of dedicated high-powered computers running application-specific integrated circuits (ASICs) [4] process the transactions of the Bitcoin network in real time, competing with each other for a small fee associated with a new transfer in BTC in addition to a subsidy in the form of a fixed amount of newly minted Bitcoins. Data is permanently recorded in the Bitcoin network through aggregated transaction instances collected into files called “blocks”. A block is a record of some or all of the recent Bitcoin transactions that have not yet been recorded and mining is the process of adding these transaction records to Bitcoin’s public ledger of past transactions, i.e. the *blockchain*.

2.1 Blockchain

The database schema known as a “blockchain” is designed for recording transactions in an adversarial environment where uncertainty prevails and truth is not axiomatic. A useful analogy for conceptualizing blockchain technology is peer-to-peer (P2P) computing, wherein a distributed application architecture partitions work loads among equally privileged participants, forming a peer-to-peer network of nodes. Insofar as a blockchain is a globally shared, transactional database which all participants can read, it is similar to the file sharing system BitTorrent. Changes in the blockchain database are performed by means of transactions, and only persist if they are accepted by the majority of network participants. This is known as the “consensus” mechanism, and is the most important feature of the blockchain.

The main difference between the blockchain and the BitTorrent protocol is that the blockchain is specifically engineered for an environment wherein hostile actors are expected to undermine the validity of the network, e.g. spend the same Bitcoins more than once. BitTorrent relies on the beneficent actions of a trusted third party, the blockchain requires no such assumption. The “timestamp” feature asserts that in the case of conflicting transactions, the first one is given precedence and subsequent conflicting ones are discarded. Figure 1 illustrates the blockchain concept.

2.2 Blockchain 2.0

The securing of a cryptocurrency network notwithstanding, there are a multitude of applications that can be run alongside, or in conjunction with the Bitcoin blockchain. Such extensions can take advantage of the large amount of computational effort generated by the dedicated mining machines and the open access afforded to this processing power available to all holders of even nominal amounts of BTC. For example, already a transaction amounting to 0.00000001 BTC (known as 1 Satoshi) is all it takes to have information indefinitely recorded by the vast mining network.

One method of embedding semantics on the blockchain is through

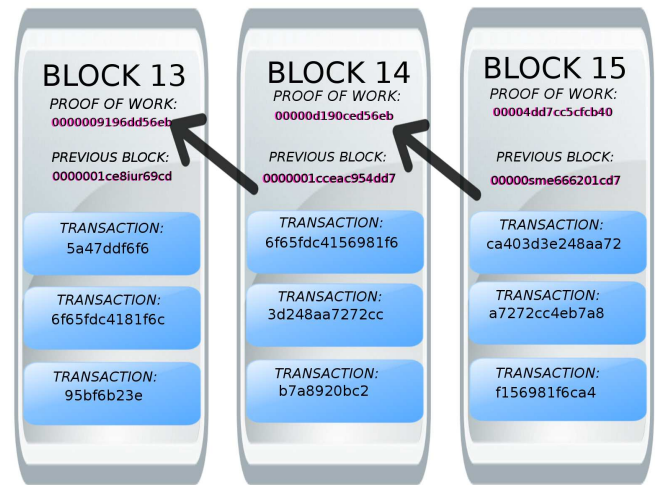


Figure 1: Illustration of a Blockchain

Bitcoin’s scripting language, which allows one to store small amounts of metadata on the blockchain. This can be used to represent transactions more complex than a simple exchange such as asset manipulation, including escrow services that cannot release a transaction without consent from multiple parties. Taken together, these ancillary applications, i.e. blockchain processes not directly related to cryptocurrency, have come to be known collectively as “Blockchain 2.0”.

Moreover there are numerous forks of the original open-source Bitcoin code, known as “altcoins”, the majority of which implement negligible or generally uninteresting modifications. That said, in this paper we explore two of such forks that have extended the original blockchain concept in ways, which can be utilized to provide useful and unique services, extending the semantic capacity of the blockchain concept in powerful ways.

2.3 Ethereum Virtual Machine

Central mediation of services has become a bulwark of the Web. Common functions that are typically in the domain of central authorities include escrow/dispute resolution (e.g. eBay, AirBnB), identity management (e.g. Google+, Facebook).

The *Ethereum project* as created a blockchain with a built-in programming language. It is a platform that creates a virtual machine designed to be run by all participants in the peer-to-peer “mining” network. The purpose of which is to allow people to write decentralized applications (stylized as *Dapps*) using blockchain technology. Although the project is relatively new [15] it holds the promise of affording users the ability to read and write to a blockchain both (quasi-Turing complete) executable code as well as data. The Enigma project from MIT is a related effort [16].

Traditional applications and web portals act mainly as a unified front-end to aggregate clients and provide the services of a particular entity. As conceptualized by the Ethereum project a *Dapp* is a tool for people and organizations to act as counter-parties to an exchange without any such centralized intermediary. A *Dapp* is an application which serves some function for its users, but which has the salient characteristic that the application does not depend on the ongoing existence of any one actor. Some examples of proto-Dapps include BitTorrent for file sharing and of course Bitcoin for currency. The goal of the Ethereum project is to allow developers to generalize peer-to-peer network and blockchain technologies for

a myriad of purposes.

The *Ethereum Virtual Machine* (EVM) is the runtime environment for Dapps. It is completely isolated (sandboxed) such that code running inside the EVM has no access to network, other processes, or the local filesystem. Essentially the EVM is aiming to become a blockchain (viz. large decentralized computing network) with a multiplicity of nodes that collectively have the ability to maintain an internal database, execute code and communicate among one another.

In subsequent sections we explore how Dapps can facilitate a series of novel methods for the symbiotic development of blockchain technologies and the Semantic Web as applied to contemporary education methodologies.

3. BLOCKCHAIN ONTOLOGY WITH DYNAMIC EXTENSIBILITY (BLONDIE)

To date there has been some progressive work on the creation of a standard ontology for blockchain processes [6]¹. However, the rapid development of the field has rendered some of these efforts incomplete. To address this situation we have engineered an open source collaborative ontology which we have published on GitHub².

BLONDIE represents a comprehensive information model that covers the structure of various blockchain components (e.g. Wallets, Transactions, Blocks, Accounts, etc.). At this time BLONDIE is specifically focused on Bitcoin and Ethereum although the extensibility to cover other altcoins was part of the engineering focus of this effort.

In its current instantiation it is one of the initial steps towards the envisaged melding of semantic and blockchain technologies. The first application of this tool will be the implementation of a Semantic “blockchain explorer”.

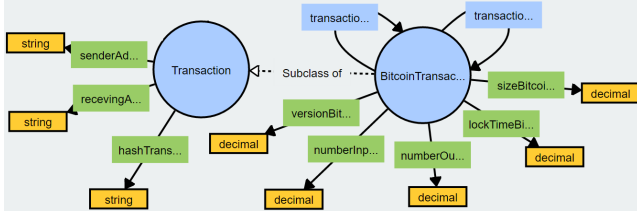


Figure 2: BLONDIE classes and properties for representing Bitcoin transactions.

Using the Visual Notation for OWL Ontologies [9] Figure 2 shows the classes and properties related to Transactions. Three fundamental properties in transactions are: Receiver Address, Sender Address and value.

Figure 3 shows the two types of accounts that Ethereum supports:

1. *Externally owned accounts (EOA)*, that are controlled by private keys, and
2. *Contract accounts (CA)*, that are controlled by their contract code (also called smart contract) and can only be activated by an EOA.

Since the blockchain serves as a public ledger of transactions, extracted content identified using BLONDIE will serve as an effective mechanism for the publication of Bitcoin and Ethereum data as part of the Linked Open Data cloud [2].

¹<http://cc.rww.io/vocab>

²<https://github.com/EIS-Bonn/BLONDIE/>

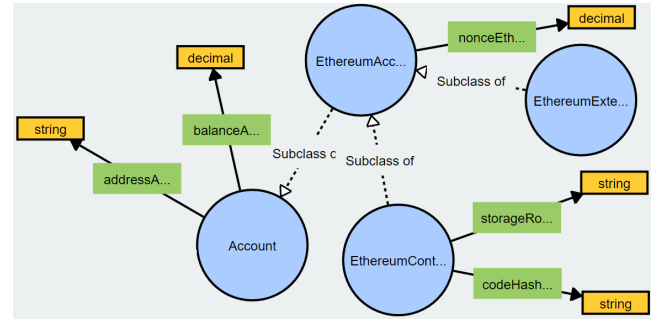


Figure 3: BLONDIE classes and properties for representing Ethereum accounts.

4. USE CASE SCENARIO

One of the defining characteristics of the 21st century has been the proliferation of highly novel mediums by which people all over the world are empowered to share and consume information. This paradigm has given rise to new industries and is having a profound impact on well established ones. In this environment new opportunities are created for individuals with the appropriate proficiencies and accordingly the process of skill acquisition is one of the strongest indicators of societal change.

4.1 Recognition of Credentials

Massive Open Online Courses (MOOCs) typically comprise a lecture series including accompanying material, focused on a particular subject, created for broad distribution across the Internet with largely unrestricted access for interested participants.

Since their inception MOOCs have consistently attracted staggering numbers of students, typically in the hundreds of thousands. What is the reason for this popularity?

The increasing sophistication of statistical models that drive automation processes and machine learning are having a substantive impact on the economic landscape and are projected to make large numbers of jobs redundant in the coming years. This situation is merely one example in a cadre of changes that reflect a larger trend which might be described as something approaching a tectonic shift in the fundamental factors that drive the global economy.

The rapid growth and demise of platforms and frameworks, the tools that support the dynamic response of industry to the increasingly mercurial needs of consumers, fuels a demand for educational resources that can keep abreast of the core competencies needed to distinguish oneself in the highly competitive job market.

4.2 Impetus to Success

The New York Times labeled 2012 “the year of the MOOC” [11] with the emergence of a number of successful online education platforms backed by large industry actors and top universities. In the intervening years there has been a diminution in the amount of media attention surrounding MOOCs, due (in no small part) to the low numbers of students that remain involved with the course through to successful completion. It has been strongly conjectured that one of the primary causes behind these disappointing statistics is the fact that there is considerable uncertainty as to how exactly the achievements benchmarked in MOOCs should be recognized.

We focus particularly on MOOCs as an application scenario for using blockchain technology to certify learning achievements. Learning today takes place in a context of new interactions between formal and informal learning. This is characterized by the changing role of teachers, the impact of social media and the students ac-

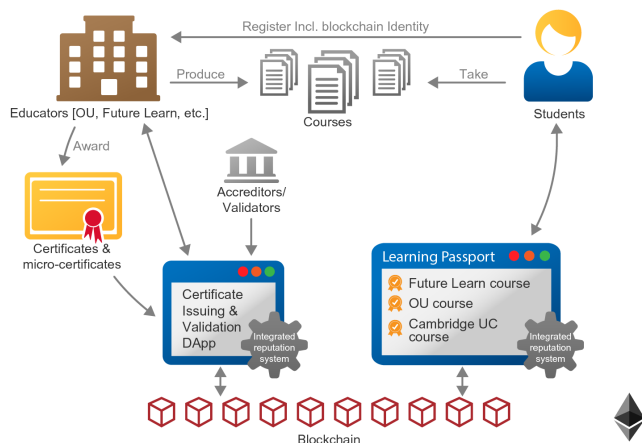


Figure 4: A scenario of how blockchains and smart contracts can support accreditation and certification in higher education.

tive participation in the design of learning activities. Expertise in a domain might be gained through participation in a Meetup event, continued involvement in a question answering platform, thoughtful contemplation of recorded video content, or through a multiplicity of channels. All of these non-traditional educational mediums are marginalized by our current system of honouring credentials.

4.3 Learning passport

Figure 4 shows a scenario of how a smart contract platform such as Ethereum could support micro and standard accreditation within a higher educational setting. Educational establishments including universities and MOOC providers such as *FutureLearn*³ develop and deploy courses and award recognition of student achievement through certificates, micro-certificates and badges.

Students take courses and gain recognition after registering for and completing courses through certification. In an era of re-skilling and lifelong learning⁴ students will increasingly take a variety of courses from a variety of providers over a longer period of time. There is a need in this context for students to be able to collect and store all their informal and formal qualifications in a fashion that makes these easily accessible to relevant parties such as potential employers and educational organisations. The above process can be supported by two decentralized blockchain based applications (DApps) running on the Ethereum network. A *Certificate Issuing and Validation* DApp would handle the publication of signed certificates within a blockchain. Secure signatures would tie all certificates to the specific issuing educational institution and the receiving student. Because of the nature of blockchains the certificates would remain valid even if the issuing organisation ceased to exist. Recently, the University of Nicosia has placed all the certificates for its free introductory MOOC “*An Introduction to Digital Currencies*” within the Bitcoin blockchain⁵.

A *Learning Passport* DApp would enable learners to easily view and manage all recognition of their learning no matter if informal or formal. These might include badges collected for course completion from MOOCs and formal degree course certificates. Each

³<http://www.futurelearn.com/>

⁴No 21 year old on completion of a bachelor’s degree will have gained all the skills he or she requires for the rest of his/her life

⁵<http://digitalcurrency.unic.ac.cy/certificates>

of these two DApps would incorporate evaluation and reputation services. Certificates can be verified partly through reputation, but also be stored as credentials on the platform. For example, a verified credential proving certain prerequisites at one institution can allow a student to easily enroll in a higher level course at another. This allows the platform to operate with little overhead. Evaluation and reputation services would allow teachers and students to match their learning styles effectively. It will also set the stage for self-regulation of the system. Semantics can help in supporting interoperability issues in the above scenario, namely:

- Mapping from university and educational establishment data structures into the data structures as required by blockchain transactions and for the smart contracts.
- Semantically, indexing template smart contracts and transactions for re-use.
- Mapping between the Learning Passport data format into arbitrary certification and badging systems.

5. SEMANTIC BLOCKCHAIN

The methodology for semantifying blockchain technology presented in this section is generic and easily generalizable to multiple application domains. However, we will restrict ourselves in our characterization to the learning achievement certification use case.

5.1 Data Representation Framework

A common definition of a transaction is an occurrence in which goods, services, or money are passed from one person, account, etc., to another. Accordingly we understand a transaction to be an interchange of information between three entities: a buyer, a seller, and the commodity exchanged. RDF is conceptualized as, and serves in practice to be an effective method for expressing information structured as subject-predicate-object triples. The natural correlation between these two paradigms gives rise to the concept of the “Semantic Blockchain”, a mechanism to imbue simple blockchain transactions with multifaceted meaning, facilitating demonstrable utility in the dissemination of credentials between widely dispersed counterparties in a trustful, persistent, universally accessible ecosystem.

Ultimately what we are working towards is a blockchain that is itself semantic, insofar as rich meaningful content will be an intrinsic feature of the transaction as opposed to a “bolted on” appendage.

1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2

Figure 5: Sample address hash

At present the assignment of public and private keys in the Bitcoin blockchain network incorporates random noise into the generation process to yield a unique identifier of the form depicted in Figure 5.

In cryptography this noise component is known as a seed. If one is optimizing a network for the transference of value across extra-legal marketplaces, e.g. the infamous Silk Road, then random seeds and pseudoanonymity are desirable characteristics. However, as blockchain finds uses in mainstream society a model whereby responsible actors can rightfully gain recognition for hard-won achievements is of utility.

Our proposal is to move to a model wherein the random noise is replaced by a specific URI, such as the FOAF identifier of a person, the DBpedia index of an institution or the hash of a document certifying a particular accomplishment. Thus wallets on the network

Figure 6: Example address seed

employing the hash of a semantic resource as address will be fully dereferenceable.

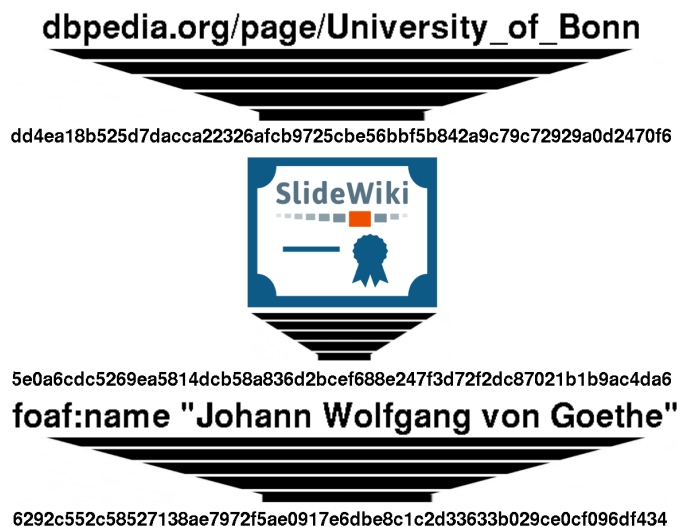


Figure 7: Hash Generator: Triple Structure

At present this involves the creation of a fork from the original Bitcoin code, available under the terms of the MIT license to construct a “testnet”. Essentially a testnet is an alternative Bitcoin block chain, to be used for experimentation. Testnet coins are distinct from “real-world” bitcoins, and are not intended to have any monetary value. This allows developers to freely conduct tests without the expense of using real BTC or causing damage to the main Bitcoin blockchain.

To validate the efficacy of this approach we are organizing a large scale analysis, and pending the successful result are planning to roll it out for the certification of credentials as part of the *SlideWiki*⁶ platform.

5.2 DNS management

On the Semantic Web, all information is expressed in statements about resources. Resources are identified by International or Uniform Resource Identifiers (IRI/URIs). While URIs are very beneficial, they also have some inherent weaknesses:

- *Centralization.* While individual URIs can be minted in a distributed fashion, the identifier generation relies on the centralized DNS system, which poses a single point of failure or attack.
- *Persistence.* In case of intentional (e.g. a merger or acquisition of a legal entity) or unintentional (e.g. bankruptcy) events, the persistence of identifiers can not be guaranteed.

There are three key requirements which an ideal identifier system should fulfill:

1. *Secure:* dereferencing identifiers should not be prone to attacks, i.e. when retrieving the content of a website or resource the authenticity of the content should be ensured.
2. *Human-readable:* it should be possible to give identifiers intuitive names, which can be easily remembered by humans.
3. *Decentralized:* no central authority should control identifier creation and pose a single point of failure or attack.

Aaron Swartz [14] described a naming system based on Bitcoin, employing the distributed block chain as a proof-of-work to establish consensus of domain name ownership. Namecoin implements the concept.

Namecoin is a decentralized open source information registration and transfer system based on the Bitcoin block chain itself. It enables users to dis-intermediate the Domain Name System (DNS) providers, one of the last bastions of centralization in the architecture of the modern web.

Practically speaking the issues identified above have afflicted the Semantic Web community in the past, e.g. the shuttering of Freebase by acquirer Google [1]. Consider the semantic machine learning system NELL (Never-Ending Language Learning) [5], which aims at remaining operational indefinitely. For such an ambition as this to be credible we must rely on a naming convention system that will not disappear as Freebase did.

Consequently we have commenced the implementation of a fully functional mirror site to *dbpedia.org* under the top-level domain *dbpedia.bit*. Top-level *.bit* domains cannot be found through a “normal” browser unless one stores the full Namecoin blockchain locally. At this stage the solution might be described as unstable, however we remain confident that going forward this will be a credible remedy to the problem posed by hyper long-term projects such as NELL.

6. DECENTRALIZED APPLICATION (ÐAPP) FOR EDUCATION

As stated above Ethereum is a platform intended to facilitate the development of decentralized applications (Ðapps) using blockchain technology. A foundational ingredient in the efficient operation of programs on this distributed application platform is “Ether”. This is a form of payment made by the users of the network to the machines executing their code. Ether is the incentive ensuring that developers write applications that do not waste resources, e.g. running endless loops on the platform, it also ensures that users are compensated for the contribution of their computation time and/or memory space.

Recent work at The Knowledge Media Institute (KMi), research and development arm of The Open University, has been centered around the implementation of a decentralized application, which enables crowd-based recognition of educational activity on the *FutureLearn* and *OpenLearn*⁷ platforms.

The Ðapps provides students the ability to enroll in courses using Ether funds, receive certifications of achievement, called “awards” and aggregate the awards in a sharable common interface. In this ecosystem the users, viz. students and administrators, manage enrollment, and remuneration (using Ether), in addition to the assignment of credentials all on the blockchain.

On the Ethereum network a Ðapp consists of two parts: a frontend, written in HTML, and a backend, essentially the database of the application. We have developed a fully functional prototype of such a system, demonstrated in Figure 8.

⁶<http://slidewiki.org/>

⁷<http://www.open.edu/openlearn/>






OpenLearn					
Institute	Course Title	Price	View	Action	
	OpenLearn	Succeed with learning	0.06	Details	Enroll
	OpenLearn	Taking your first steps into higher education	0.06	Details	Enroll
	OpenLearn	Succeed with maths - Part 2	0.06	Details	Enroll
	OpenLearn	English: Skills for learning	0.07	Details	Enroll
	OpenLearn	Succeed with maths - Part 1	0.06	Details	Enroll

Figure 8: Platform view.

Create New Wallet

Accounts for: Wallet 0

Account	Balance (ETH)	Trans. Count
02b8515602138c9264c54a57fa754eb55b8c526b	4.16529826	8
51f7934930e502a1a8381e9fec9d933cf7350285	4.90313134	16
c78ae2432b67cbd351c9b6c2eccadda60401cc72	4.143372375041768	12

Transfer ether

From: To:
 Ether:

Figure 9: Prototype of “Student Browser” frontend.

From the main element “My Wallets” view students manage their Ether (available funds) account. Users create one or more wallets, and use them to transfer funds between different actors, e.g. a transmission of their Ether to an online learning platform such as *FutureLearn*.

There is a profile area wherein users can establish their identity by associating it with a known public key. Accordingly an individual wallet account is bound to a name and an icon. Subsequently this account can be indicated as the “current account” and used to enroll in a course.




Student Profiles				
<input type="button" value="Create New Student Profile"/> <input type="button" value="Edit Student Profile"/> <input type="button" value="Clear Current Profile"/>				
Image	First Name	Last Name	Account	Default
	Anon2	Anonymous	0xc78ae2432b67cbd351c9b6c2eccadda60401cc72	Set As Current
	Anon	Anonymous	0x51f7934930e502a1a8381e9fec9d933cf7350285	Set As Current
	Anon3	AnonymousAgain	0x02b8515602138c9264c54a57fa754eb55b8c526b	Set As Current


Figure 10: Dashboard view of multiple different user accounts.

The embedded Dapp Store contains course selections from multiple sources, among them both *FutureLearn* and *OpenLearn* and are anticipating content from *Fraunhofer Academy*⁸ and *SlideWiki*.

To register for a course in the system a user must initiate the process with a click-through of the “Register” button, this will prompt

⁸<http://www.academy.fraunhofer.de/en.html>

a pop-up box with a password input screen, since subsequently a monetary transaction (using Ether) will take place.



Anon3 AnonymousAgain

Account:

0x02b8515602138c9264c54a57fa754eb55b8c526b

Balance:

4.16429794

My Courses








	OpenLearn	Anon Anonymous	Taking your first steps into higher education	0.06	Completed
	OpenLearn	Anon2 Anonymous	Succeed with maths - Part 1	0.06	Completed
	OpenLearn	Anon2 Anonymous	Taking your first steps into higher education	0.06	Completed
	OpenLearn	Anon Anonymous	Succeed with learning	0.06	Completed
	OpenLearn	Anon Anonymous	English: Skills for learning	0.07	Completed
	FutureLearn	Anon Anonymous	Big Data: Measuring and Predicting Human Behaviour	0.09	Completed
	OpenLearn	Anon3 AnonymousAgain	English: Skills for learning	0.07	Completed


Figure 11: Course Dashboard.

Concurrently with this interchange we can see a transaction which is generated on the blockchain, it will remain pending until it is mined, this is viewable in a partition of the browser window depicted in Figure 12.

				
Pending Transactions: Hash: <input type="text"/> From: <input type="text"/> To: <input type="text"/> Value: <input type="text"/> Gas: <input type="text"/> Gas Price: <input type="text"/> 84c17				

Figure 12: Blockchain transaction.

Mined (confirmed) blocks are represented by the numbered green ovals, unconfirmed blocks will appear as red. There is a transaction hash, and the two hashes representing sender (From) and receiver (To). Once the block has been successfully mined it will be added to the list of courses pending. One additional exchange (separate from the transactions that pay for enrollment in the course) facilitates its delivery to the course dashboard of the user. On the current environment this process is instantaneous, on a larger network, e.g. the web-scale Bitcoin blockchain, as currently implemented, to confirm with certainty might take the amount of time required to process a new block, i.e. not more than 10 minutes.



Anon3 AnonymousAgain

Account: 0x02b8515602138c9264c54a57fa754eb55b8c526b
Balance: 4.16429794

My Awards







Issuer	Student	Award title	Description	Date
	FutureLearn Anon Anonymous	Big Data: Measuring and Predicting Human Behaviour Award	An award for completing the Big Data: Measuring and Predicting Human Behaviour course	14 Mar 2016
	OpenLearn Anon Anonymous	English: Skills for learning Award	An award for completing the English: Skills for learning course	22 Mar 2016
	OpenLearn Anon Anonymous	Succeed with learning Award	An award for completing the Succeed with learning course	22 Mar 2016
	OpenLearn Anon2 Anonymous	Succeed with maths - Part 1 Award	An award for completing the Succeed with maths - Part 1 course	17 Mar 2016
	OpenLearn Anon Anonymous	Taking your first steps into higher education Award	An award for completing the Taking your first steps into higher education course	14 Mar 2016
	OpenLearn Anon2 Anonymous	Taking your first steps into higher education Award	An award for completing the Taking your first steps into higher education course	24 Mar 2016
	OpenLearn Anon3 AnonymousAgain	English: Skills for learning Award	An award for completing the English: Skills for learning course	13 Apr 2016

Figure 13: Awards view.

Once the course has been completed the administrator can log-on to issue the award. After the block containing the award has been mined it can be found in the “Awards List” of the associated student.

The following code snippet represents a component of an Ethereum “smart contract” for an educational institute to offer courses.

Note that no students are using this course demo for enrolment as it is currently merely a proof of concept.

```
function getCourses() public returns (address[]
    availablecourses){
    availablecourses = courses;
    return availablecourses;
}

function addCourse(address course) public onlyOwner
    returns (bool success){
    bool exists = false;
    success = false;
    uint i=0;
    uint count = courses.length;
    address next;
    for (i=0; i<count;i++) {
        next = courses[i];
        if (next == course) {
            exists = true;
        }
    }
    if (exists == false) {
        success = true;
        courses.push(course);
    }
}
```

Figure 14: Ethereum “smart contract” snippet

7. RELATED WORK

The work we have carried out thus far in the domain of the Semantic Blockchain is largely a continuation of the achievements recorded by the initiatives described in this section.

7.1 Open Badges

The Mozilla Foundation and Peer2Peer University, in collaboration with The MacArthur Foundation, contributed significantly to the field of credential assignment in the context of non-traditional education through the publication of a well known white paper on the subject of modular accreditation [12]. The initiative is known under the name “Open Badges for Lifelong Learning”. The purpose of which is to support skill development and lifelong learning for “real results”, e.g. job placement and advancement [8].

The essence of a digital open badge is a standardized way to conveniently demonstrate that one has achieved a given degree of competency in a particular domain. Through close cooperation with credible organizations Open Badges facilitates the process of skill, interest and achievement verification.

The system is based on an open standard, such that one is free to combine multiple badges from different issuers in a comprehensive accomplishment narrative. The aim of this platform is not restricted to the Web and should transcend the digital medium to be applicable to work performed online as well as offline.

Through the shared technical standard Open Badges facilitates a process of garnering recognition for the things one learns as well as the things one is able to teach. Anyone who satisfies the standard can award badges. There is a vibrant community of contributors and partners supporting this effort, such as NASA, the Smithsonian, Intel, and the American Girl Scouts.

Originally the badges infrastructure envisioned a decentralized server structure, but the incentives for providers to run these servers

were never strong enough to maintain such an environment. For this reason it appears that the blockchain is a better foundation, as it is run by self-interested entities but can openly be utilized for broad community-based initiatives [13].

7.2 Blockchain Certificate Issuance

We have alluded to the fact that a blockchain database is durable, time-stamped, transparent, and decentralized. These characteristics are useful attributes in the management of a reputation system. We can consider reputation as a type of currency that enables access to social capital, as opposed to financial capital.

The MIT Media Lab is currently issuing blockchain certificates in accordance with the following procedure:

1. Create a digital file that contains basic information such as:
 - (a) the name of the recipient
 - (b) the name of the issuer
 - (c) an issue date
2. Subsequently the contents of the certificates are signed using a private key to which only the Media Lab has access
 - (a) append that signature to the certificate itself
3. Next create a hash, which is a short string that can be used to verify that nobody has tampered with the content of the certificate.
4. Finally use the private key once again to create a record on the Bitcoin blockchain which states that a certain certificate was issued to a certain person on a certain date

This system makes it possible to verify who a certificate was issued to, by whom, and validate the content of the certificate itself. Currently it uses the Bitcoin blockchain by way of the OP_RETURN field. OP_RETURN is a script operation code used to mark a transaction output as invalid. Since the data after OP_RETURN are irrelevant to Bitcoin payments, arbitrary data can be added into the output after an OP_RETURN. The hash value of the MIT Media Lab is stored in this OP_RETURN segment.

The current version creates a separate transaction for each certificate. Future versions of the software could store all hashes in one Merkle tree and only the Merkle root might be stored in the OP_RETURN, referring back into the blockchain approximately once every day.

7.3 Industry Interest

Sony Global Education, Inc. a division of the multinational conglomerate company Sony Corporation is the foremost industry actor to announce an interest in the adaptation of blockchain technology to the field of education [7].

They are pioneering an effort to realize a solution to enable open and secure sharing of academic proficiency and progress records by leveraging the security properties inherent in the blockchain to facilitate the encrypted transmission of data, such as an individual’s academic proficiency records and measures of progress, between two specified parties.

Regarding the initiative Sony Global Education has released a public statement to the effect that,

“The technology has the potential to realize an entirely new infrastructure system for sharing records securely over the network in any number of ways, opening new doors of possibility for academic records and how they

are assessed. For example, after taking an examination to demonstrate his or her academic proficiency level, an individual could direct the testing organization to share the test results with one or more third-party evaluating organizations. This would be a first if implemented on a system-wide basis”

while notably vague as to the details of the implementation, from this statement we can clearly discern the strong motivation for a solution that under-girds such efforts.

It enables network users to freely and securely transfer permissions, without the need for an established relationship of trust between network participants, and in such a way that damaging or tampering with programs and data is prohibitively difficult.

8. CONCLUSION

This paper represents a first statement on the relationship between blockchains and the Semantic Web, and accordingly we sought to encompass a comprehensive overview that includes all pertinent activity we have thus far undertaken in the space such that it might serve as a catalyst for further development. We strongly feel that many lessons on how semantics has been aligned with the Web infrastructure could be applied to blockchains. We also feel that there is a timing issue here. Now is the time for the Semantic Web community to explore how our work can be reused by the blockchain community and vice versa before too many wheels are re-invented. The two communities have much to offer each other.

The proposed application scenario of MOOCs was selected not for the extraordinary utility that this paradigm provides but to illustrate the concept that the ability to trace an exchange or transaction through the blockchain can provide a social benefit, alleviating the need for holders of credentials to verify their accomplishments ad infinitum— a common problem for those who have obtained degrees abroad. We had contemplated highlighting the analogous example of musician Imogen Heap using blockchain technology to license music, but finally determined MOOCs to be more immediately relatable to the larger SEMANTiCs audience. Moreover, it seems clear that online learning and the need for new methods to fill existing skills gaps will continue to develop going forward.

As briefly touched on above we have commenced work on a Semantic Blockchain explorer along the lines of `blockchain.info`. However, where this service exports the raw blockchain data to a relational database we are exporting the data to RDF, using the BLONDiE ontology, in an effort to facilitate interaction with the Linked Open Data (LOD) cloud.

9. ACKNOWLEDGEMENTS

We are grateful to Aeron Buchanan, Vinay Gupta, & Vitalik Buterin of Ethereum, Philipp Schmidt of the MIT Media Lab, Dr. Christopher Brewster of TNO, Jessi Baker of Provenance, Ulrich Atz of The Open Data Institute and finally Simon Scerri, Steffen Lohmann & Prof. Dr. Maria-Esther Vidal of Fraunhofer IAIS/The University of Bonn for their valuable contributions in helping to bring this work to fruition.

10. ADDITIONAL AUTHORS

Fabrizio Orlandi (Rheinische Friedrich-Wilhelms-Universität Bonn & Fraunhofer-Institut für Intelligente Analyse und Informationssysteme IAIS, email: `orlandi@iai.uni-bonn.de`)

11. REFERENCES

- [1] Freebase is read-only and will be shut-down., May 2015.
- [2] S. Auer and J. Lehmann. Creating knowledge out of interlinked data. *Semantic Web*, 1(1, 2):97–104, 2010.
- [3] T. Berners-Lee, J. Hendler, O. Lassila, et al. The semantic web. *Scientific american*, 284(5):28–37, 2001.
- [4] G. Brunner. The bitcoin network outperforms the top 500 supercomputers combined, may 2013.
- [5] A. Carlson, J. Betteridge, B. Kisiel, B. Settles, E. R. Hruschka Jr, and T. M. Mitchell. Toward an architecture for never-ending language learning. In *AAAI*, volume 5, page 3, 2010.
- [6] M. Carvalho. Ontology for crypto currencies. <https://cc.rww.io/vocab>, oct 2013.
- [7] S. G. Education. Sony global education develops technology using blockchain for open sharing of academic proficiency and progress records, feb 2016.
- [8] T. M. Foundation and i. c. w. T. M. F. Peer 2 Peer University. Open badges for lifelong learning. *Working Document*, sep 2011.
- [9] S. Lohmann, S. Negru, F. Haag, and T. Ertl. VOWL 2: User-oriented visualization of ontologies. In *19th Int. Conf. on Knowledge Engineering and Knowledge Management (EKAW '14)*, volume 8876 of *LNAI*, pages 266–281. Springer, 2014.
- [10] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.
- [11] L. Pappano. The year of the mooc, Nov. 2012.
- [12] P. Schmidt. (how) can badges replace degrees? In *OCWC Global 2011: Celebrating 10 years of OpenCourseWare*, 2011.
- [13] P. Schmidt. Certificates, reputation, and the blockchain, oct 2015.
- [14] A. Swartz. Squaring the triangle: Secure, decentralized, human-readable names, jan 2011.
- [15] G. Wood. Ethereum: A secure decentralised generalised transaction ledger, 2014.
- [16] G. Zyskind, O. Nathan, and A. Pentland. Enigma: Decentralized computation platform with guaranteed privacy. *arXiv preprint arXiv:1506.03471*, 2015.