31 January 2022

Frontier Talk

Memo by Marco Almada

Leveraging Blockchain in Education

Speaker: Primavera De Filippi (EUI)

This event has been organised by the Technological Change and Society Interdisciplinary Research Cluster

Primavera De Filippi is currently a research director at CERSA/CNRS/University Paris II, Faculty Associate at the Berkman Klein Center (Harvard Law School) and Visiting Fellow at the Robert Schuman Centre for Advanced Studies (and EUI Alumna). Her research focuses on blockchain and the new governance opportunities it affords. With Aaron Wright, she authored Blockchain and the Law (Harvard University Press, 2018).

In this talk, the Speaker focuses on the application of blockchain technologies to the education sector. She begins with an introduction to blockchain technologies. This conceptual overview is followed by an overview of the various applications of these technologies, with special attention to applications in the education sector, before concluding with an assessment of the pitfalls and potential shortcomings of the technology. These pitfalls notwithstanding, the overall message of the talk is that blockchain can be used to allow students to exercise better control over their information and their educational pathways.

After the initial discussion, there were about forty-five minutes of discussions between the Speaker and the audience, moderated by a PhD researcher in Economics (henceforth **Moderator**). The participants raised questions about the governance of blockchain arrangements, their relationship with Web 3.0, and the power dynamics reflected in the architecture of blockchain solutions. According to the Speaker, these points have considerable implications for Web 3.0 and blockchain in general. However, they become less salient in the educational context, in which the goal is not to replace existing institutions but to see how they can benefit from blockchain technologies to deliver better and more trustworthy services.

The sections below provide a more extensive overview of the points discussed during the Frontier Talk.

1. Core concepts

The Internet has long been associated with the possibility of **disintermediation**: people can access content without needing to go through intermediaries, for example, by having access to the news without needing to buy a newsletter. As the Internet evolved, models for peer-to-peer communication appeared in various domains, but intermediaries were still seen as unavoidable in contexts related to money and other scarce goods.

Consider, for example, the problem of sending money online. The usual way to do so goes through an intermediary—a bank—which must be trusted by both parties in the transaction. In addition, reliance on intermediaries leads to a centralised network, as all money exchanges must go through a few trusted actors. For some applications and some users, neither trust nor centralisation is acceptable, prompting the creation of the first blockchain: Bitcoin. Since then, the idea has spread to other domains.

Bitcoin appeared with the goal of creating a decentralised system for exchanging money. It manages to create scarcity through an economic mechanism, as the creation of new coins depends on mining. To mine bitcoin, one must solve a mathematical puzzle associated with a *block*. Whoever finds the solutions to a block is awarded a certain amount of bitcoin, and then a new block is generated and left open for solution. These problems are designed so that people find solutions at a regular pace, ensuring a constant stream of new blocks. If people take too long to solve a problem, the next one is easier, and difficulty increases if blocks take too long to appear.

But what prevents people from simply copying the solution to a problem and replicating coins, just like other forms of digital content can be replicated? The solution to this is to register all the solutions of previous blocks. Whenever a block is emitted, it includes a reference to the previous block, and this reference is used as part of the mathematical problem that leads to awarding bitcoins. If anybody wants to falsely claim they solved a given block, they would need to falsify the entire chain. However, the chain is not stored by a single intermediary. Instead, all users have the entire history of all transactions and can therefore validate on their own each transaction. The longer the chain is, the more blocks there are after a given transaction, making it more secure, as modifying it would require changing all the history of the chain up to that point.

This approach means blockchains have certain properties:

- They are **resilient:** every node of the network has a copy of the blockchain, which means there is no single point of failure in the network;

- They are **resistant to coercion and censorship:** any attempt to force changes to the blockchain would need to reach all users at once, something that becomes difficult in a global network;
- They are **immutable:** it is possible to trace every change to the chain, and other users could detect any adulteration by using their own copies of the blockchain;
- They are **non-repudiable**: every transaction must be signed with a user's private key, which (as long as the key itself is not compromised) means one cannot claim they were not directly involved in the transaction;

Those properties enable blockchains to be a **trustless technology**: you do not need to trust the other party in a transaction, as you can mathematically prove or disprove their claims. The approach described above is a **public** blockchain, in which anyone can enter the network and participate in its activities. In a **private** blockchain, only invited users can join the chain and participate in its transactions. Finally, there are **hybrid** blockchains, in which some participants are more trusted than others and thus conferred an increased role in governance. The choice of the adequate approach depends on the task at hand and the levels of trust between the involved actors.

2. Applications

Blockchain applications include certified registries, cryptocurrencies and tokens, and smart contracts. When dealing with personal data or large files, such as pictures or videos, this data is not usually stored in the blockchain. Instead, what is saved in the blockchain is a hash (digital fingerprint) of the item of content, which can be retrieved from elsewhere. These hashes are one-way functions: you can easily generate the hash if you have the original content item, but you cannot simply generate the content from its hash.

A **certified registry** uses the blockchain as a transparent, tamper-resistant, and time-stamped database to register certain content, which becomes accessible to the entire blockchain. Since hashes of digital content are unique for each item, anybody trying to present an adulterated version of that item will not be able to match the fingerprint stored on the blockchain. For example, one can create a "version of record" of a given database by storing a fingerprint of its contents before an important update. If the fingerprint of the database contents after updating does not match its previous value, somebody might have tampered with the data during the update process. Blockchain registries can provide proof of the existence of certain items, as the only way

to match a hash stored in the blockchain is if you actually have the object that has been hashed. Some applications include notarisation of documents (as Estonia is doing) and registering inventions in the blockchain to later prove the timing of invention without needing to disclose what has been invented. The same approaches can also be used to items in the physical world: some African countries have created proofs of concept of blockchain for land registry, which allow people to independently verify the validity of a property title.

The second major application domain discussed by the Speaker is **tokenisation**: using the blockchain to create tokens that are owned and can be exchanged. Cryptocurrencies represent a fungible type of token: each bitcoin is identical to every other bitcoin. But tokens can also be **non-fungible tokens** (NFTs), which are associated with a unique content item. For example, an NFT of a digital painting contains a hash of that painting, which can only be generated by whoever has the file. This has been used in the art world to ensure digital artworks remain scarce and thus marketable.

Finally, another major blockchain application is **smart contracts**, which are pieces of code that execute if and only if the conditions are met. Once a smart contract is registered in the blockchain, its execution is guaranteed: if any of the parties to the smart contract attempts to revert execution or stop it in any form, the other party can easily prove this is a breach of contract.

3. Blockchain in the education sector

The first use of blockchain in education in the presentation is **certification**. Universities and a few other institutions are experimenting with issuing diplomas in the blockchain, while some other organisations (notably the MIT Digital Currency Initiative) are creating open badges that certify single courses and other educational experiences that do not amount to a full degree. The idea here is that interested parties—such as potential employers—can ask a person to produce hashes of their certificates and compare them with the value stored in the blockchain rather than relying on an intermediary. So long as the user retains their certification, they can still validate it against the hash stored in the blockchain. This means blockchain certifications cannot be forged, but it also means that certifications retain their value even if their issuing institution ceases to operate.

More generally, blockchain enables a model of **self-sovereign identity**, in which individuals can manage their personal information without needing to share it with a broad range of intermediate validators. Instead, validation depends only on the hash and the certificates, which remain solely with the individual. This allows individuals to pursue **selective disclosure**, as they control what

data they want to reveal in a given context. It also allows for **interoperability**, given that people can move to a new service provider—for example, a new university—while disclosing just the relevant hashes.

Tokenisation also has applications for education. One recent approach is the **proof of attendance protocol**, which uses tokens to verify who has attended a particular class or workshop. Tokens can also be used to validate **endorsements** in a decentralised way: you may give a colleague a token that says they are good at something (say, Excel), and potential employers would be able to verify the truthfulness of this endorsement. Yet, as the Speaker pointed out in response to a question by a EUI Professor, tokens and certificates for educational purposes are not amenable to trade, so they are unlikely to increase the costs of educational certification, unlike the price variation in NFTs.

Another disruptive aspect of blockchain comes from the combination of **interoperability** and **composability**. Storing data such as certificates in the blockchain not only allows people to move providers without hassle but also allows for the use of this information as building blocks for new systems. For example, blockchain certificates could be combined to form personalised degrees. Instead of following rigid course schedules, such degrees would rely on validated information on the blockchain to create personalised learning pathways for each student, integrating formal and informal learning. The Speaker describes a proposal for emitting ECTS credits in the blockchain, which would allow automated diploma emission, avoid “double counting” of credits, and afford the general properties of the blockchain. This would be helpful for exchange students (who would have a single history and not need to wait for verification at home), joint degree students (with a harmonised control of their degree), and institutions. A blockchain system also would allow for creating granularised certifications and ad-hoc diplomas that are more suitable for reflecting a student’s interests and trajectory.

Another EUI Professor asked whether the ability to certify content might lend itself to producing better content. The Speaker points out this might occur through experimentation: students and institutions can validate different forms of education, so they can present unique educational pathways in a validated form. Whether to recognise the demonstrated experience would still be a decision left to institutions and employers, but they would have access to reliable information as they decide.

4. Pitfalls and shortcomings

The Speaker concluded her presentation by pointing out some limitations of current blockchain models. The first one was **scalability**: blockchains can become unwieldy as they store more and more information, making them slower than centralised approaches. Given the complexity of their computational models, blockchains also raise concerns about **energy consumption**. Finally, the evolution of technology might lead to **technological and governance risks**.

These shortcomings were covered in the Q&A. In response to the first question, the Speaker suggested that blockchains in education might converge towards a consortium blockchain, in which educational institutions would be trusted to edit the blockchain itself, for example, to remove certificates obtained through cheating. But, in response to the Moderator, the Speaker pointed out it is unlikely that all education applications rely on the same blockchain. Instead, there would be various blockchains, in part due to the problems of scale and consumption mentioned above.

Given the immutability of blockchains, the Moderator asked in the Q&A whether their use would not be an obstacle to content moderation in social networks, which is seen as a positive thing. The Speaker suggested that moderation could not occur at the level of the blockchain itself, as it is immutable. However, blockchains could provide users with the choice of which filtering algorithm they want to use for the content they see online, rather than relying on a centralised approach to filters.

On the governance front, a participant asked whether the demand for **computational resources** would not lead the blockchain to reflect or amplify existing power asymmetries under the guise of decentralisation. A Professor pointed out that some of the developers of blockchains, notably Bitcoin, were departing from an anarcho-capitalistic ethos that is somewhat antithetical to the institutional uses of blockchain shown in the presentation. The Speaker acknowledges these risks but points out the ideal of disintermediation can be pursued in ways that strengthen, rather than erode, **legitimate institutions**. Governments attempt to rein in some of the uses of the blockchain, for example, through taxation and by applying know-your-customer rules to cryptocurrency exchanges. This might push some users towards avoiding any intermediaries that might create legal risk. Still, regulation can be successful if blockchain users rely on relatively centralised models, such as those based on exchanges.