The Lifelong Learner: How Blockchain Solutions Can Facilitate Data Transfer and Protect Personal Information for a Lifetime

Traditional ideas about education and the workforce are evolving. In response to the rapid pace of technological change, individuals are continuously training and re-skilling in order to further their careers. As the number of years an individual works in their lifetime grows, regular professional development is increasingly a key component of long-term employment.

To meet this demand for more development opportunities, options to support lifelong learning are rapidly expanding. Online courses, micro-credentials, and work-based learning opportunities are among the many resources available to support a learner in growing their professional skills. Unfortunately, education data regarding such degrees or other credentials still largely exists within a 'siloed' data structure, one that is generated at the institution level for each student.

Over the course of their lifetime, a student may attend various institutions and achieve many different credentials. Because of the increasing likelihood that multiple institutions will hold data about students, siloed data systems represent a challenge for consolidation and review of all a students' education data. This challenge is compounded when these data need to be shared, such as when completing an application for employment and/or continuing education. In these cases, a student would be required to collect their data from each individual institution in order to create a verifiable portfolio of experiences and distribute copies of that portfolio for each data request. This can cause a severe time and financial burden on the student as they seek to compile their information.

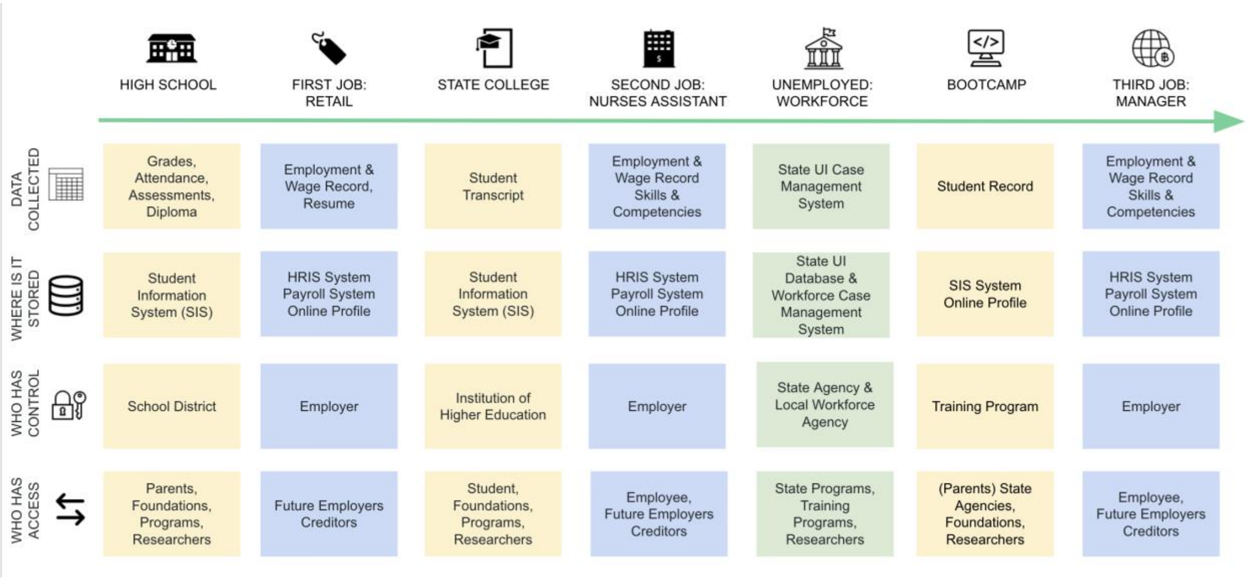
To minimize these barriers, institutions that are transitioning to systems that support open standards for interoperability of data may consider adopting systems that leverage blockchain technology. This approach facilitates the movement of data and makes verification and protections for an interoperable data solution. This has the effect of breaking down existing silos by enabling common data infrastructures to be leveraged across institutions while maintaining the privacy and security of data throughout.

This paper will explore the current challenges of a prototypical lifelong learners' journey, the data silos and data privacy implications, and how education blockchains can alleviate some of the barriers they face.

Data from the journey of a lifelong learner

In order to understand the challenges that siloed data systems present for the lifelong learner, it is necessary to visualize an individual's journey through education and the workforce. By illustrating the various ways data generated at each stage in the learner's journey is used or required, the challenges for the lifelong learner are made clearer.

Our individual for this example will be Sue, and her journey includes many common experiences of today's learners. The following figure summarizes her journey and will be used as reference throughout this paper.



	HIGH SCHOOL	FIRST JOB: RETAIL	STATE COLLEGE	SECOND JOB: NURSES ASSISTANT	UNEMPLOYED: WORKFORCE	BOOTCAMP	THIRD JOB: MANAGER
DATA COLLECTED	Grades, Attendance, Assessments, Diploma	Employment & Wage Record, Resume	Student Transcript	Employment & Wage Record Skills & Competencies	State UI Case Management System	Student Record	Employment & Wage Record Skills & Competencies
WHERE IS IT STORED	Student Information System (SIS)	HRIS System Payroll System Online Profile	Student Information System (SIS)	HRIS System Payroll System Online Profile	State UI Database & Workforce Case Management System	SIS System Online Profile	HRIS System Payroll System Online Profile
WHO HAS CONTROL	School District	Employer	Institution of Higher Education	Employer	State Agency & Local Workforce Agency	Training Program	Employer
WHO HAS ACCESS	Parents, Foundations, Programs, Researchers	Future Employers Creditors	Student, Foundations, Programs, Researchers	Employee, Future Employers Creditors	State Programs, Training Programs, Researchers	(Parents) State Agencies, Foundations, Researchers	Employee, Future Employers Creditors

Education data flow from education to employment

Sue is an average student. She does well in high school, and when she applies to colleges, she is accepted to her State University system. After graduating from high school, she looks for a summer job to keep busy between the end of the school year and her first semester at the university. Sue finds a promising job opportunity, applies, and is contacted for an interview. The company collects information from her regarding any previous employment and education to be stored in their HR/payroll data system. In the future, employers, and creditors may access this data.

Privacy Considerations

When Sue shares her resume with her summer employer, the data within does not fall under FERPA protections since any education data in it was not provided directly by her school's information system. It should be noted that if the company requires a verifiable diploma or other student information directly from the school, FERPA protections will then apply because the degree verification process would require the disclosure of student records from the school to the employer.

This disclosure will require that the eligible student or parents submit written and signed consent for the data to be released to the company. This consent must contain a description of the data (e.g. diploma information), a description of who will be receiving the data, and a description of the purpose for the release. Current processes for this can be slow, cumbersome, and expensive. Use of digital credentials, anchored to blockchains, can streamline consent processes by enabling users to digitize both consent and verification of records, resulting in faster, less burdensome data management.

Education data flow between high school and postsecondary institutions

In the fall, Sue is also planning to attend a university which requires various pieces of information from her high school, such as transcripts, grades, and proof of graduation. Administrative staff at the high school submit this information to the university on her behalf with her application for admission.

Privacy Considerations

Since her student data is being transmitted from one education institution to another for the purpose of enrollment, FERPA's consent requirements do not apply in this case. However, use of education blockchains could still improve upon this process by reducing burden on school administrative staff.

Education data flow between postsecondary institution and employer

After graduating university, Sue pursues her first full-time job as a sales manager. The data transactions for this look similar to when she applied for her retail job after high school but may now involve her university's data systems and consent processes. Her university is also required to collect consent under FERPA before it can release any of her student data to third parties.

As a postsecondary student/graduate, she is now able to submit consent for herself rather than her parents submitting on her behalf. While she may be able to submit her consent form online now, much of the process still happens on paper. When the university administration receives her consent and her request to disclose, they must print, package, seal, and mail her paper records.

The process may take weeks from start to finish, be costly for Sue due to fees incurred from the university and be labor intensive. Sue may also be left unable to start her employment in a timely way, which could hurt her earnings and even hurt her chances should the employer need to immediately fill the position.

Digitizing the entire verification process would save costs and time in this case. Education blockchains could allow for a secure interoperable data system that would follow Sue through life. She would need to still submit her consent before university data could be released but it might be as simple as checking a box in a mobile app, and that would cut out costly manual processes and allow data to flow more freely and more quickly.

Privacy Considerations

In this scenario, FERPA consent requirements could be built into the interface for a data system. Universities and school districts would each be linked into the system to facilitate the receipt of data requests and consent as needed. The product would be a verifiable education record that the student can then use for employment purposes or other situations in which third parties require education data.

Education data flow between schools and government services

In the situation that Sue is let go by her employer, she may need to grant government-sponsored services, such as state unemployment counseling, access her education records. In this situation, time is more important than ever. Reentering the workforce quickly will result in Sue recovering financially and regaining other benefits such as employer-sponsored health insurance. State unemployment services can respond to needs more rapidly when they have faster and more streamlined access to the data they need.

Privacy Considerations

Due to a provision in the law that allows for states to match employment and education data to gauge performance in terms of unemployment and underemployment for qualified workers[1], the state agency will be able to access Sue's education records without FERPA's usual requirements for consent.

However, the reality is that methods for accessing the data are patchwork and can be efficient for some schools and districts while being inefficient for others. Decentralized data systems cause issues for data sharing between institutions, districts, and states. The establishment of interoperable systems would help greatly but without a universal data framework, interoperability is a distant goal. To start, interoperable systems would need to be implemented at either the state level or at the federal level. A state-level implementation would help school and district data systems coordinate data activities within the state. Federal-level implementation would require opt-in from states and would streamline communication between state systems. This would not immediately solve all of the issues, but it could serve as a starting point for universal data frameworks.

Education data flow between university and coding bootcamp

Sue starts to reskill by applying to a coding bootcamp. Her application requires her to submit credentials that certify her high school diploma and university degree.

Privacy Considerations

While most coding bootcamps are not accredited under the same standards that colleges are, most are regulated under the same laws. As a result, Sue would have to provide consent under FERPA for institutions to release her data to the bootcamp.

Education data flow between coding bootcamp and employer

After graduating from the coding bootcamp, Sue applies to an IT firm to become a professional developer. To verify her successful completion of the program, the employer requests her records from the bootcamp.

Unless the bootcamp is part of an educational agency or institution, this transaction of data is occurring between two parties and no longer involves education data that falls under FERPA. The bootcamp would not need to acquire Sue's consent before passing her records to her potential employer.

By this point, it is important to note that Sue has already accumulated three verifiable education experiences: high school, college, and skills training through a bootcamp. In addition to this, she has been employed by two companies. Each experience she has had that adds a line to her resume may need to be verified at some point for future employment or other uses. But each of those items can currently only be verified by accessing individual data systems, obtaining Sue's consent to access certain data, and navigating an ever-growing collection of data silos.

Privacy Considerations

Lifelong learners accrue many educational experiences over their lives and may work for many different employers. It is becoming increasingly rare for people to graduate from one high school or university and

[1] Joint Guidance on Data Matching Facilitate WIOA Performance Reporting and Evaluation: https://studentprivacy.ed.gov/resources/joint-guidance-data-matching-facilitate-wioa-performance-reporting-and-evaluation

stay in one job until retirement. Accounting for an ever-growing series of experiences is becoming increasingly burdensome, both for verifiers and for individuals like Sue.

As a result, the need to break down data silos and enable data to work better for people has become clear. In order to stay career competitive, people are accumulating more credentials from an increasing diversity of sources. But if these credentials are too hard to verify, or the data systems used to verify are too burdensome, they become less useful.

Cybersecurity in disparate data systems

As presented in Sue's example above, data about an individual is stored in many different systems—each for different purposes and governed by different rules on privacy and access. These include educational institutions (high school, university, or even a computer coding bootcamp), potential employers (, a retail company or IT company), and federal or state government agencies (such as an unemployment office or Department of Education). Each of these systems manages and stores the person's data in various forms that may include protected 'education records' (as covered under FERPA). Furthermore, each follows its own data governance rules and may be accessed by different types of people. Data security and consideration of privacy for personal data should be understood in this context.

As one method to reduce risk, it is important to limit the amount of personal data stored across these systems. This can be accomplished by limiting disclosure as much as possible to credentials while excluding extraneous ancillary data from transactions with third parties whose data systems are less regulated by federal privacy law.

The fact that a student's university transcript may be shared by the school with their consent to third parties, such as recruiting services, demonstrates the value of exploring an alternative approach. A streamlined mechanism for a student to provide consent, and mechanism for the university to seamlessly transfer those records to the third party create many opportunities for efficiencies. The data is protected under FERPA from disclosure without consent while in the school's data system, but these protections no longer apply once the data resides in the recruiter's system. The recruiter may use this data in other ways without the student's consent.

Limiting the data that can be stored by these systems can help to protect student privacy. To accomplish this, schools and education agencies can implement blockchains that third parties like recruiters can use to locate and verify the education credentials they need to provide their services.

Because blockchain technology is essentially a ledger of data interconnected or "chained" together using cryptographic technology in a way that makes it impossible to tamper with data on the chain, the implementation of blockchain can also help mitigate cybersecurity risks by avoiding storing PII on the chain itself. Instead of placing sensitive data within the blockchain, it could instead be used as a directory of indexes or keys that point to resources like credentials which reside off-chain. Implementing education blockchains that can be used to help secure education data in this way can reduce the need for data to be stored in individual, third party data systems not regulated by federal privacy law and thus also reduce the chances that personal data become vulnerable due to faulty system security practices.

As far as privacy is implicated, the use of blockchain will not only reduce the spread of personal data over third-party systems, but also facilitate how education data systems will more quickly and efficiently share and control access to an individuals' credentials.

FERPA as a permissive statute

The Family Educational Rights and Privacy Act or FERPA was enacted in 1974 to allow parents and eligible students to exercise some control over the use and transmission of records that schools or institutions create and maintain. A key component of this aspect of control under FERPA is requiring that parents and eligible students provide written consent before a school may disclose records to another party. Given this consent requirement (and barring any of the exceptions to the general consent rule), it may seem that FERPA is overly restrictive when it comes to sharing data from schools. However, FERPA is not inherently the challenge to implementing interoperable systems that speed up data transfer and reduce burden if this concept of 'consent' is considered at the beginning of system development.

It is important to know where consent is required and where it is not so that the proper consent structures can be built into a new system that digitizes consent and release of records. The following table covers the cases experienced by Sue as she used her education data.

SUMMARY **FERPA Implications of Data Transfer**		
Data Transfer Instance	**FERPA consent needed?**	**Explanation**
High school releases official diploma to an employer.	Yes	Employer is a non-educational third-party seeking access to official school records.
Individual providing an employer a resume with her high school graduation listed on it.	No	Students are free to disseminate data they have direct access to from school.
High school releases official transcripts to a university for admission/enrollment.	No	Education institutions can share student data with other institutions for education purposes without consent.
University releases official transcripts to an employer	Yes	Records that are verified and vetted by the school require consent before release to non-educational third parties.
Individual providing unofficial transcripts to an employer.	No	Individuals are free to release unofficial transcripts they personally hold but if the records are being disclosed by the school, consent would be required.
Schools releasing an individual's education data to a state unemployment agency.	No	Education data can be released without consent to state agencies seeking to match it with employment data for evaluation purposes.
University release of official transcripts to a skill building bootcamp for enrollment *(where the bootcamp is not part of an*	Yes	Education institutions must obtain consent to share student data with third parties, even if for educational purposes.

educational agency or institution).		
An individual listing this skill building bootcamp certificate or diploma on her resume *(where the bootcamp is not part of an educational agency or institution).*	No	Individuals do not have to consent to the release of data they personally hold.
The skill building bootcamp releases an individual's official results to her employer *(where the bootcamp is not part of an educational agency or institution).*	No	Consent is not required under FERPA when records pass between two third parties.

As this table demonstrates, with a firm understanding of FERPA and other legal requirements when designing a data system, the system can embrace interoperability goals and provide thorough, transparent, and compliant protections of education data.

Consent-centric models for better data solutions

FERPA and its consent requirements must be thoroughly worked into the overall requirements for any system or application that will facilitate the movement of student data. Designs that come out of a privacy-first approach will also naturally prioritize continued responsible stewardship of education data.

It is important to note that consent via digital signature is acceptable under FERPA (34CFR §99.30 (d)). Thus, consent on demand that can happen in real time reduces complexities associated with such a system and minimizes the chances for mishaps.

There are two opportunities to collect digital consent that should be considered. The first opportunity is when a record is disclosed from an educational institution and given to a student. In a blockchain implementation, this could be in the form of a digital token that corresponds to a public key/location recorded on the chain. The second opportunity to collect consent is when a data recipient seeks to verify a credential. The educational institution will need to confirm details and obtain consent from the student at this juncture. Implemented at either of these points, electronic consent can facilitate and expedite data transfer while adhering to privacy best practices for disclosing records.

In this model consent can be obtained in two ways: initiated by the individual or requested by the institution after receiving a request from a potential recipient.

An example that accommodates for both ways incorporates dynamic consent through application-based controls. In this model, students can pre-consent to data transactions, notifying the issuing institution (i.e.: university releasing an official transcript) and the data recipient (e.g.: future employer) that consent has been submitted. The actual transaction would then be facilitated directly between the institution and the data recipient. As mentioned, this model could also support recipient-initiated data requests. When a data recipient requests to see a credential, the application would request consent from the individual in accordance with FERPA requirements. When the individual consents, the request and consent would both be transmitted to the issuing institution. The common theme for any model is that the system will need to be built around consent to work.

Furthermore, centralizing data storage under common data security measures and limiting third party systems from storing large amounts of education data will further help to protect student information from unwanted use and data breaches. Blockchain can enable a self-sovereign identity model that facilitates the sharing of verifications of credentials, not whole sets of data.

Conclusion

A new way of managing student data can help to promote student privacy and make student data more usable. However, education data teams called upon to engineer these solutions must include privacy experts who can provide a strong stance on how to design consent processes into any implementation. To take advantage of tools such as blockchain and interoperable education data systems, consent processes will occupy many of the moving parts of the end solution.

We must strive to build better pathways for education data to travel alongside individuals throughout their lives, experiences, and achievements. Lifelong learners stand to benefit from a shift in the way education data is shared, going from a highly manual process to one that embraces digital tools such as blockchain to help secure and manage transactions. These changes promise to relieve burden on individuals, schools, and outside organizations looking to verify credentials.

About PTAC

The Privacy Technical Assistance Center (PTAC), a U.S. Department of Education technical assistance resource, helps state and local entities and a variety of education stakeholders understand best practices in data privacy, confidentiality, security, and managing student-level data. PTAC subject matter experts serve as partners with education agencies and help to address potential weak points in their privacy and data security efforts.