Kratos: A solution for data privacy, literacy, and student agency in a data-driven school ecosystem

Dr. Velislava Hillman
vhillman@cyber.harvard.edu

Varunram Ganesh
kratos@varunram.com

June 2019

Abstract Growing digitization has made data ownership an important focus point for institutions and students. Broadly, there are three issues, which require urgent attention for optimization of data privacy, literacy, and utilization. First, schools globally are equivocal about data generated by and about students as a result of the digitization of instruction, learning, and assessment. They lack necessary frameworks for data literacy, data interoperability, and optimization, while maintaining privacy and control. Second, the scale, source, and nature of school data makes its interoperability impractical, resulting in an inability to assess the true impact of educational technologies on instruction and learning. Third, while data helps teachers improve pedagogical practices, an increasingly data-driven decision-making process suggests that student dimensions of learning and equitable participation in curriculum design becomes secondary. Finding a balance between data-driven decision making and student voice is critical for an efficient school ecosystem. In this paper, we introduce Kratos: an immutable decentralised data management system that provides data privacy and applied data literacy while empowering students with a user interface for data governance and active participation in the school ecosystem. Using the advantages of blockchain technologies, Kratos enables easy authentication and access to data. The objective of Kratos is thus to equip students and schools with the ability to access, manage, and control their data and to understand how, why, and by whom data is accessed without compromising student agency and privacy. This paper describes proof of concept for Kratos, its benefits to students and schools, and necessary future work.

1 Introduction

To improve work, school practitioners need data interoperability and educational information from data mining (Bienkowski, Feng, and Means, 2012; Snyder et al., 2016). Broadly, this need emanates from the requirement to measure school effectiveness by combining student achievement, data, and accountability (Militello et al., 2013).

Educational data is important not only for evaluating school quality. It can also contribute to research in learning and advance theory (Baker and Siemens, 2014). It can help guide intervention and lead to higher school attainment (Arnold and Pistilli, 2012), improved pedagogy (Baker and Siemens, 2014), and better parental involvement in school matters (Baker, 2016). A common goal of educational data is to equip educators with key information that they can act upon and use to the benefit of learners (Baker and Siemens, 2014). Educational data can enable an applied data literacy and train students to understand the benefits and limitations from data that is generated by and about them. Furthermore, access to educational data provides an opportunity for student agency by enabling interaction and participation.

Increasingly digitized school environments enable constant data collection, which change core school functions of teaching, assessment, and accreditation (Zeide, 2017). Digital systems for teaching and assessment drive data-based decision-making and enable micromanagement of students that can further pose restrictions on teacher autonomy and student (and parent) participation and willingness to challenge education decision-making. Schools deploy management systems for sorting and storing data and while some data is stored by schools at district level, other data is managed by third-party vendors who may consider this data proprietary and thus inaccessible by school practitioners, less so by students. This puts barriers to effective data sharing and comprehensive understanding and utilization of school data.

In this work we propose the development of a structure for student data management, privacy, accountability, and auditability. We build on top of existing data standards and construct a common data schema for otherwise disparate data across different systems. Our system organises these references onto an integral structure of student data and complements the existing educational data standards and interoperability in three distinctive ways. Through network permissioning and proofs of ownership on a distributed ledger, we enable data auditability and accountability. We design data analytic models to integrate with existing school systems and data standards. Lastly, we build a simple user interface that gives students, parents, and schools access to otherwise scattered and disparate data, enabling control over what portion of the data can be shared. Additionally, we propose an application with social functionality for student feedback.

We propose this structure for K12 schools. However, the aim is that this initial work will pave the way for setting up a unique decentralised data management system that provides students with full control and visibility of data that is generated by or about them throughout their educational life. We acknowledge the legal, structural, technical, and organisational complexities involving school data of minors and therefore do not delve into these particular subjects. We focus on conceptualising how a safe space for student data can be created. We thus propose a tool for K12 students, which enables integrity and auditability of data that is collected about them. At the same time we project our initiative to develop into a platform, which will give students, once independent, full control over their data.

We present Kratos not as an independent solution to lack of data interoperability, accountability, and privacy but rather as a system that complements existing efforts and solutions developed by various stakeholders in the school ecosystem (for example, Data Quality Campaign, 2018; Student Data Privacy Consortium, 2018).

2 Existing problems

To contextualise the complexity related to school data - the opportunities and challenges schools face as a result of the growing digitisation of operation and academic processes - we partnered with Cambridge Public School district (CPS) that administer public elementary and high schools in Cambridge, Massachusetts, the Access for Learning (SIF), and the Student Data Privacy Consortium (SDPC), collaborative of schools, districts, policy makers, and other stakeholders addressing data privacy concerns (SDPC, 2018). With the help of CPS's Information and Communication Technology Services Chief Information Officer and Database Administrator, we explored data interoperability issues along with feedback on potential mitigation schemes:

- **Data access** - CPS is in agreement with over 100 vendors providing education technologies. Many of them provide no direct and comprehensive access to data generated about and by students who use their products and services. Where available, data access is provided in the form of reports - a summary of information, which the district database administrator can request and download. On other occasions, vendors supply data directly to teachers and in some cases to students in the form of digital dashboards. Where teachers obtain data, it requires further work to convert it into meaningful information upon which the teacher can adjust and plan instruction (Data Quality Campaign, 2018).
- **Lack of data standard compliance** - School data frameworks vary across districts and states (CEDS, no date). Additionally, vendors providing education technologies use different data formats, schema, and elements to organise and store student data as no single standard can be enforced upon them to comply with. Thus, disparate data, scattered across different systems with varying degrees of accessibility and usability poses challenges to educators and other stakeholders in the education sector in assessing the impact of education technologies on the learning process and on identifying best practices. The lack of data standard compliance impedes upon data transparency and prevents data interoperability, two conditions critical to ensuring data privacy.
- **Lack of transparency** - The scale, complexity, and number of providers pose challenges for schools to have a comprehensive list of the data that is generated about students. Lack of data interoperability standards which is the process of compiling, organising, and documenting what information is generated about students makes data auditability difficult to achieve, less so to be useful to the instruction and learning processes. While some stakeholders in the education sector make tremendous efforts in ensuring data transparency in order to achieve effective privacy management (SDPC, 2018), issues persist (Kelly et al., 2018).
- **Security** - Due to general lack of transparency with regards to how various education technology vendors organise and structure their data (Ibid.), it becomes difficult to understand the security they ensure for the data their products and services generate. Having inadequate access to available data limits potentials to fully benefit from it.

We thus infer that schools generally experience numerous challenges that preclude them from obtaining student data in a comprehensive and timely manner, which further prevents

students from understanding, accessing, interacting with, or having control (now or in the future) of their data.

3 The need for a solution

Interoperability challenges between vendors and schools at local or district level pose barriers to cohesive data management and sharing while lacking basic technological privacy infrastructure and accountability (Zeide, 2014; Kelly et al., 2018). While digitizing and collecting student data is not new (Fitzgerald, 2014), technological developments like cloud computing and the Internet of Things (IoT) amplify concerns about data transfer, storage, use, and analysis (Sultan, 2010).

Concerns arise about over-prevalence of fine-grained data collected about students (Zeide, 2017) and the risk of creating a 'permanent record' that can impede upon learners' futures (Cody, 2013). The use of online platforms and applications in schools, often provided by for-profit vendors, many of whom have unclear policies about data privacy (Kelly, et al., 2018), generates a continuous stream of data about students' behavior and performance at an unprecedented scale (Zeide, 2017). Big data complicates traditional understanding of what constitutes sensitive information and what information serves an educational purpose. Such data however, continues to drive decision-making of educators and vendors, marginalizing student dimensions of learning and equitable participation in curriculum design.

The present challenges of fragmented data access, the lack of student agency and auditability, and the lack of a concrete framework for data accessibility demand a techno-social solution, which can ensure that educational data can be used to help improve school processes while not diminishing student privacy, agency, and future opportunities.

4 Kratos

Kratos aims to define a set of guidelines and principles that schools should follow and provides a platform for both schools and students to see what kind of data is being collected by vendors with the help of an immutable log for auditing student data changes, access, and use (Figure 1). The goal for students would be to see what data is being collected about them, how their data is being used, and at age of majority, gain full control of this data. We define this as Data Ownership and Visibility - how students can own their data after age of majority and how students can see what their data is being used for. We aim to create a comprehensive reference for schools to otherwise disparate data stored by different vendors, make it compatible with each other and we define this problem as Data Interoperability. For the purpose of our case study we work with two types of data samples - a sample from one vendor supplying applications for instruction and assessment for K12 students and data sample using SIF standards from our partnering school district of Cambridge, Massachusetts.

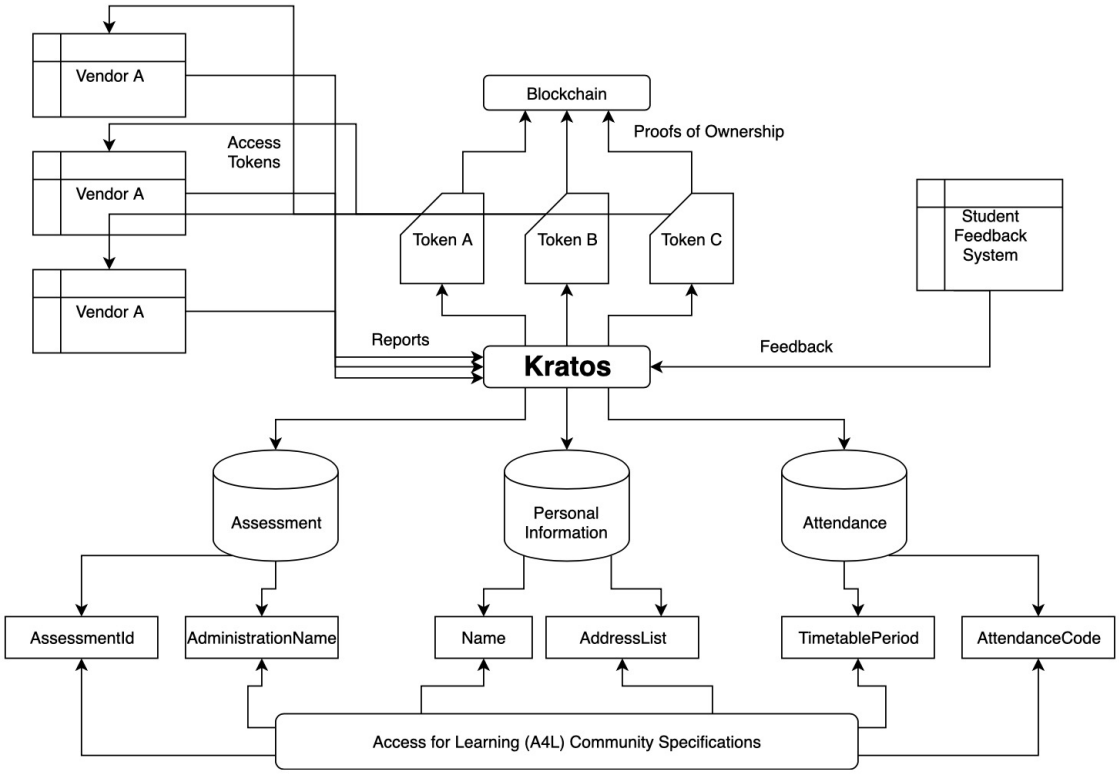

Figure 1: Kratos Architecture

4.1 Data Interoperability

A traditional approach to interoperability would be to force a given set of standards on third party vendors so that they reference them. However, work done by standardization bodies like SIF and CEDS has shown that this is at best partially effective since there is no financial or social incentive for vendors to migrate to the proposed set of standards. Kratos attempts to solve this issue by proposing a solution where different fields described by different vendors can be mapped to a single underlying scheme defined by Kratos so that third party vendors would not have to change their established data organisation and structure. Again, for the purpose of describing conceptual work we refer to only a small sample of disparate data that is stored at the school's and the vendor's end.

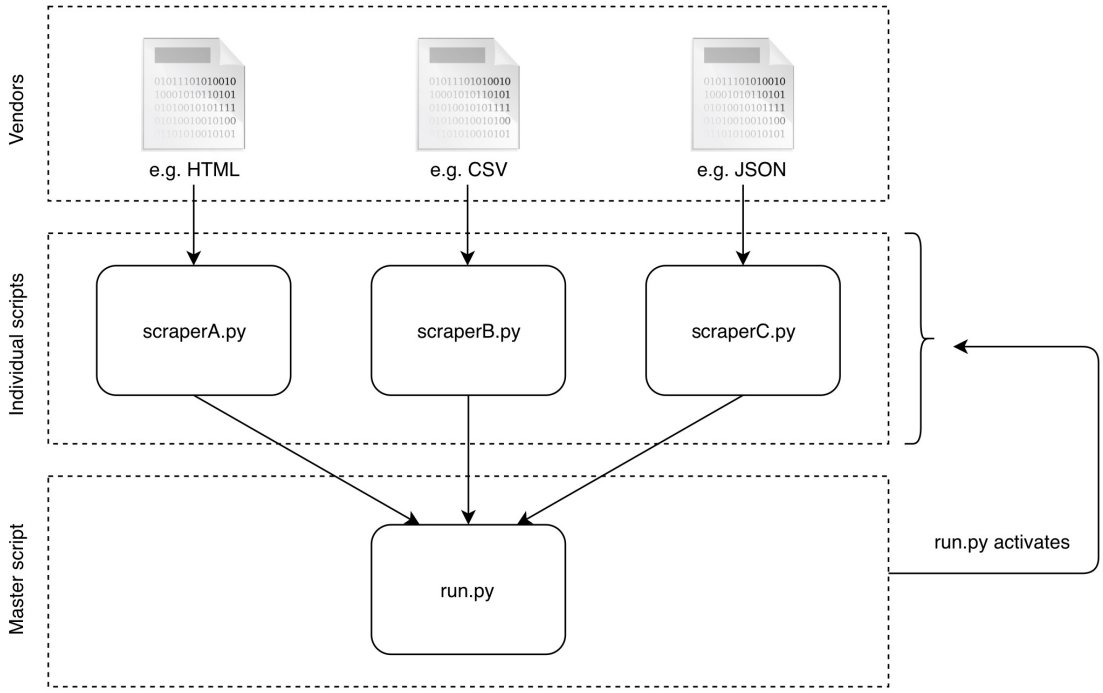

Figure 2: Data Architecture

As an example, let us assume the underlying fields defined by Kratos are Grade_A, Grade_B and Grade_C. If a specific vendor has a different name for the same field (example GradeA, GradeB and GradeC), Kratos would ingest the data from the fields defined by the vendor and convert it to the ones defined by Kratos. This should be done across different formats since the reports database administrators receive right now are formatted as JSON, CSV or are in the form of Excel sheets.

We propose that this be done in the form of a templated script that can be written for every vendor. Building a common script for all the vendors poses a challenge since the number of vendors and the different fields and standards they follow are ever changing. This templated script would be triggered automatically by Kratos each time it receives an incoming report and the report itself will be parsed to understand which vendor it originates from.

The fields that Kratos defines will be adapted from the existing SIF standard followed by schools in Cambridge and would also have routine input from various experts on the subject. The number of fields however would change since SIF has over 700 different fields and it is not possible to accurately map all these fields. For Kratos we define the idea of a "bucket" - a collection of data fields collated together as a single entity to make it easier for students and administrators to monitor them. Common examples of buckets would be PII (Personally Identifiable Information), Grade Reports (containing grade reports and tests per subject) and Attendance Records (recording the class wise attendance of the student). Other buckets may include Metadata (recording student use and interaction with an application) and Conduct (including discipline, accidents, and other data relating to student behaviour). To formalise the type of data buckets, it is imperative to develop a data taxonomy - a comprehensive vocabulary of data type, purpose of use, and impact - comprising

data collected by schools and education technology providers.

The models and scripts developed as part of enabling interoperability will be open source and subject to continuous updates. We would also be having a complete code audit before releasing the system in a production environment to ensure the model performs and behaves the way it was designed and intended to.

The buckets defined by Kratos provide reference to corresponding and otherwise disparate data (including data residing with vendors). The data relating to each bucket (each of which further breaks down into concrete elements) can be used in multiple ways: students can have a better understanding of what data is generated about them, what for, and by whom their data is being used; parents can know what kind of data is being collected about their children; and school administrators can benefit from a comprehensive view and access to an ever growing trail of interoperable data.

4.2 Data control

In conventional systems, data control or 'ownership' can be proved with the help of an access token but this provides no guarantee on when the owner came into possession of the data. In order to attest 'ownership' at a specific point in time, we need time-stamping services like those described by Todd (2016), Szalachowski (2018), and Massias et al.(1999). A time-stamping service requires something to be committed along with the time-stamp and Kratos envisions this to be a cryptographic hash which also acts as an access token which vendors can use to access any student-generated data.

The aim of using a cryptographic hash like SHA-3 (Bertoni et al., 2012) is to ensure a uniquely random reference to the data to avoid out-of-channel data leaks. Kratos suggests using an element of randomness like a salt to generate the hash in order to have the ability to revoke tokens by regenerating randomness. Kratos enforces that all schools encrypt their data before creating access tokens to mitigate the risk of loss/theft of data. Past research (Zetter, 2016) shows that firms are willing to circumnavigate laws to collect data and encrypting data by design ensures that no third party can have access without being granted so explicitly.

Kratos suggests that encryption be done at the student level but this can also be at the school level depending on existing frameworks and rules surrounding the school. If the school chooses to encrypt student data on behalf of the student, Kratos enforces that the school use a unique key for each individual to minimize the risk of key theft. In addition to this, Kratos suggests that schools store their encrypted data in a distributed file storage system like IPFS to ensure data redundancy and availability in case of a setback. Storing data on IPFS also makes it easier to create time-stamps since it is sufficient to reference the IPFS pointer instead of potentially hashing the whole data. It is to be noted that schools would not be burdened with the load of encrypting data and choosing between different levels of encryption would be a simple click on Kratos' interface.

In the event that a user wants to revoke access to a particular vendor, he could do so by changing the encryption key or by changing the randomness used to generate the access token. We suggest that users do not regenerate encryption keys but Kratos will provide users an option to choose between the two. As we describe school data of K12 students in principle it is the school or school district administrator who controls such access. The difference is that the system will further establish accountability and auditability to students with the capacity to gain further control over their data when they become legally independent.

Furthermore, since schools have their own sets of policies, Kratos does not strictly enforce a set of practices for users (at school or district level) to follow. This ensures that adoption of Kratos is not constrained by a certain set of rules. At the same time, Kratos defines a set of minimum requirements to be on board to ensure good practices on data protection are followed.

Kratos also does not enforce how commitments need to be generated and stored, leaving it as an option for schools to provide their feedback. The system we propose would include a centralized time-stamping server, a permissioned blockchain with the different schools as the nodes, and simple time-stamping commitments to an existing blockchain. All three have their benefits and constraints and Kratos would enable schools to customize this to their requirements.

4.3 Student agency and participation

The UNESCO framework for educational planning states that "the concern of planners is twofold: to reach a better understanding of the validity of education in its own empirically observed specific dimensions and to help in defining appropriate strategies for change" (Haddad, 1995, pp. 5-6).

While summative and formative assessments provide "empirically observed specific dimensions" about student academic performance, student agency and active participation is equally required in order for policy and education to design "strategies for change". Growing use of education technologies enables data-driven decision-making (Gibson et al., 2015). Technology-mediated instruction and assessment tools with learning analytics functionality track and diagnose student progress (Tempelaar et al., 2013). Most educational technologies can interpret and equip educators with information via digital dashboards and 'skill meters'(Baker, 2016). Fine-grained and continuously accumulated data about student behavior and performance surpasses traditional notions of assessment (Zeide, 2017) posing limitations over student dimensions of learning and equitable participation in the curriculum design.

Our prototype provides a graphical interface for student involvement in (Figures 3-8) and accessibility to school data. While students and equally their parents can become acquainted with any changes and meanings of school data, students can also participate with personal feedback in the learning process (Figure 8). Student participation with personal perspectives and reflection are integral to the learning process (Ackermann, 1996). Some reflection is invariably carried out through questionnaire surveys examining school climate (Holahan and Batey, 2019). Both school climate surveys and the proposed student feedback application provide flexible selection of questionnaires and measurements with a common goal to improve school climate. However, the proposed application enables not only feedback from older students (Ibid.) but from all students, provided that the feedback addresses the goal to encourage perspective-taking and reflection that support learning (Kegan, 1982). The application further enables student agency and control over the frequency, depth, and nature of the feedback provided that it directly reflects the learning experience.

Figure 3: Student UI: Student view of data information

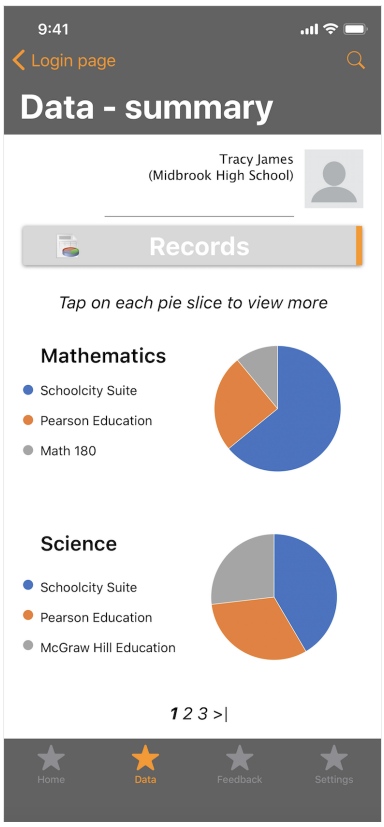

Figure 4: Student UI: Student view of detailed data fields

4.4 Data literacy

Data literacy is still a debatable construct (Bowler et al.,2017). Data means quantified information, which is "situated, taking its meaning from its context and the perspective of its beholder" (Borgman, 2015, p. 18). Making sense of data is relative. What data may mean to someone can mean nothing to others (Bowler et al.,, 2017). In increasingly data-driven systems it becomes imperative not only to understand data but to interact with it and participate in the decision-making processes that it increasingly begins to impact. While data provides insight about how systems operate, the inferences drawn from it can be without context. Fine-grained data collected over long periods of time can lead to negative impact on individual well-being and pose limitations over future opportunities (Altman et al., 2018; Friedman and Nissenbaum, 1996).

The growing digitization of schools create learning environments that enable constant data generation, the access to, and use of which becomes hard to control, audit, account for, and understand its impact. The risk from digitized school environments that constantly generate data into a permanent record (Sirota, 2013) that at any one point in time may limit individual opportunities leads us to prioritise on developing a techno-social solution that enables applied data literacy for students at an ever younger age.

While some studies examine aspects of data literacy in young people's lives (Bowler et al., 2017; Selwyn and Pangrazio, 2018; Kumar et al., 2017), the focus remains on data generated

from the use of the Internet in general and social media specifically. Studies related to young people's perceptions, knowledge, and understanding of school data literacy are meagre.

Existing literature demonstrates that young people have varying interprations and a general understanding of data (Bowler et al., 2017). However, many still find difficulties to connect with data at a concrete level, with the notion of having a data dossier (Ibid., p. 27). This highlights the pressing need to develop strategies for school-related data literacy, introduce data management skills, and encourage student participation in an increasingly data-driven decision-making school environment.

Kratos thus proposes a comprehensive, yet simple access, knowledge, and interaction with school data. At this conceptualisation stage, we choose three core data buckets to work with. These are assessment, including test scores, reports, and credentialing; conduct, including observation reports, behaviour, and attendance; and personally identifiable information, including personal identifiers, demographics, parent information, medical reports, and socio-economic information. We take these three data buckets to be crucial to student privacy and control.

In our conceptual work (Figures 3-5) we recognise that while schools collect data for each of these three data buckets, digital applications used in class also collect similar such data. For example, as schools contain data about conduct, applications such as Class Dojo (Manolev et al., 2018) gather similar data. Teachers may further report behaviour using Swivl, a video application that enables supervision and classroom observation. Currently, students do not have a comprehensive access to or knowledge of all data that exists about their conduct. Moreover, there is no awareness and knowledge of the potential impact of all data that exists about their conduct. We therefore create visibility to the disparate data that exists about student conduct, provide visibility, and learning about such data (Figure 6).

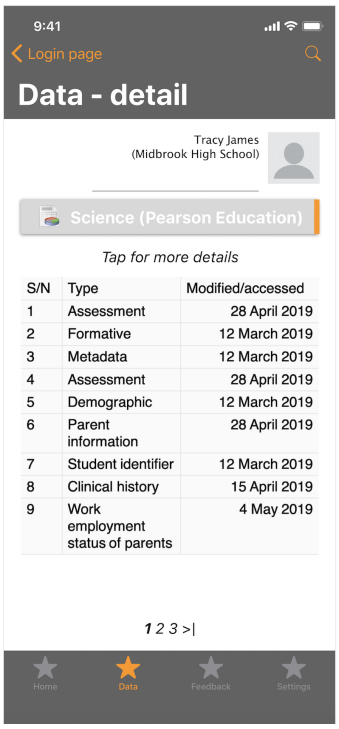

Figure 5: Data view

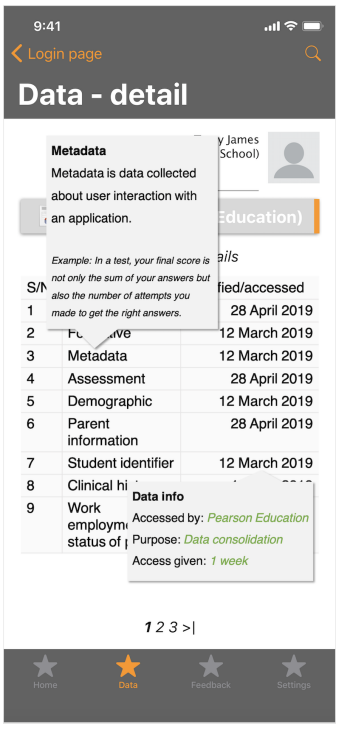

Figure 6: Data view with definition

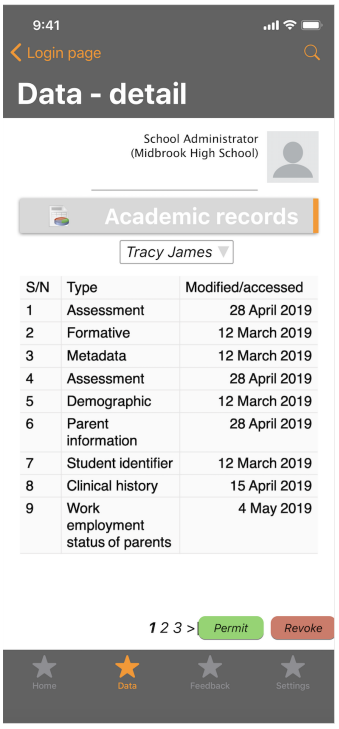

Figure 7: Permit/revoke access

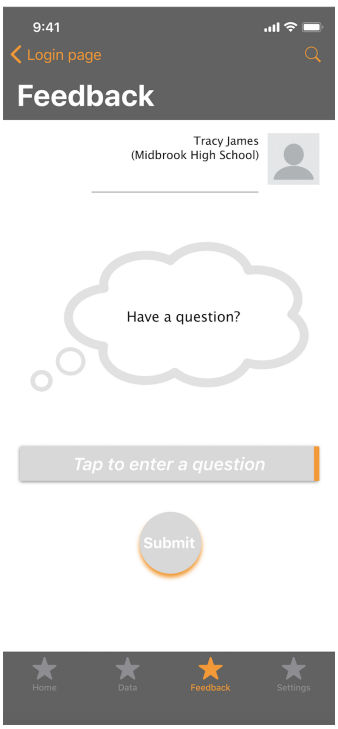

Figure 8: Feedback

5 Discussion and future work

In this paper we propose Kratos, a decentralised data management system, which enables data interoperability, applied data literacy, and student participation. This proposal envisions a techno-social solution that empowers students by providing control over their school data through data transparency and auditability. While legal (Colorado Student Data Transparency and Security Act, 2016; Kelly, 2019) and policy (e.g. SDPC, 2018) efforts are being made to ensure data privacy and security, much more needs to be done (Bulger et al., 2019), which encourages us to continue work on the Kratos project as a technological layer of protection and data privacy.

Unlike other sectors such as retail (Lu and Xu, 2017), finance (Ito et al., 2017), and medicine (Agbo et al., 2019), education is still not fully leveraging the power of global digital transformation. In medicine, for instance, data interoperability is important in order for various stakeholders to access comprehensive patient records. Across Europe (Demertzis et al., 2018) and the United States (Azaria et al., 2016), decentralised architectures have been developed to enable data sharing, interoperability, and access while prioritising patient agency, privacy, and security. Similarly, a more comprehensive data management for interoperability is highly needed in the education sector without compromising student privacy and control over their data.

While our conceptual work focuses on K12 education we understand the complexities surrounding the sheer volume of data that is generated across many different systems, the differing interests of stakeholders in the education sector, and the hurdles involving access to data that many vendors consider proprietary.

We propose Kratos as a decentralised system that enables data integrity and visibility of the huge data trail of students who are still dependent on adults to decide for them. However, such a system can give them an immutable log of their data as an additional layer of security now and at any point in time beyond their secondary and higher education.

Comprehensive access to data opens the possibilities for better analysis of processes and systems (Baker and Siemens, 2014). However, while data analytics gives some insight, not everything that is measured is valuable and not everything that is of value can be measured. Students' perspectives should go on a par with data-driven decision-making. Moreover, the sophistication of data analytics and long-term data collection can potentially decrease individual privacy (Dwork and Rothblum, 2016). The risk of being publicly exposed can lead to embarrassment or discrimination (Altman et al. 2018). Constantly being aware of such risks can diminish one's sense of freedom for self-expression and in the case with children and young people - the freedom to try out new things and make mistakes, things that are integral to learning. Therefore, a decentralised data management system that prioritises student privacy and control over data, becomes crucial to the development of a safe and free learning environment.

Future work includes three distinctive steps. First, we plan to develop a comprehensive taxonomy of school data. This will serve to develop a comprehensive data vocabulary for applied data literacy and identify data elements - data trail, origin, and purpose of use. The second step involves prototyping and formalising platform sections and functionality. And the third involves carrying out user studies to get student feedback and fine-tuning the platform's user interface. All future work is part of the greater effort to provide data privacy protection of students.

6 Acknowledgements

We thank Cambridge Public School district, Student Data Privacy Consortium, and Access for Learning (SIF) for their support, constant, and timely feedback. We would also like to thank Rayner Ng Jing Kai and Geoffrey Martin from Yale-NUS College for their help in sketching mock-up designs and giving feedback on data interoperability. Lastly we greatly appreciate the invaluable feedback on decentralised ledger technologies from Mario Galea at Random Consulting.

7 References

1. Todd, P. OpenTimestamps: Scalable, Trustless, Distributed Timestamping with Bitcoin (2016). URL `https://petertodd.org/2016/opentimestamps-announcemen`

2. Szalachowski, P. (2018). Towards more reliable Bitcoin timestamps. arXiv preprint arXiv:1803.09028.

3. Massias, H., Avila, X. S., & Quisquater, J. J. (1999). Design of a secure timestamping service with minimal trust requirement. In the 20th Symposium on Information Theory in the Benelux.

4. Zetter, K. Google Collected Data on Schoolchildren without permission (2016). URL `https://www.wired.com/2015/12/google-collected-data-on-schoolchildren-without-permission/`

5. Singer, N. (2017). How Google took over the classroom. Available from: https://www.nytimes.com/2017/05/13/education-chromebooks-schools.html

6. Bertoni, G., Daemen, J., Peeters, M., Van Assche, G., & Van Keer, R. (2012). Keccak implementation overview. URL `http://keccak.neokeon.org/Keccak-implementation-3.2.pdf`

7. CPSD. District Agreements Listing (2019). URL `https://sdpc.a4l.org/district_listing.php?districtID=457`

8. Colins, A., and Halverson, R. (2018). *Re-thinking education in the age of technology: The digital revolution and schooling in America.* Teachers College Press: New York. Zeide, E. (2017). 19 Times Data Analysis Empowered Students and Schools: Which Students Succeed and Why?.

9. Cody, A. (2013). Will the data warehouse become every student and teacher's 'permanent record'? *Education Week*, May, 20.

10. Gibson, D. C., Webb, M., and Ifenthaler, D. (2015). Challenges of big data in educational assessment.*Proceedings of the IADIS International Conference of Exploratory Learning in Digital Age*, 92-100.

11. Sultan, N. (2010). Cloud computing for education: a new dawn? 30 International Journal of Information Management 109.

12. Fitzgerald, B. (2014). Data collection isn't new. And it predates common core.Funny Monkey.

13. Keegan, R. (1982). The evolving self: Problem and process in human development. Cambridge: Harvard UP.

14. Ackermann, E. (1996). *Constructionism in practice: designing, thinking, and learning in a digital world.* Routledge.

15. Gibson, D. C., Webb, M. E., and Ifenthaler, D. (2019). Measurement Challenges of Interactive Educational Assessment. In *Learning Technologies for Transforming Large-Scale Teaching, Learning, and Assessment*, 19-33. Springer, Cham.

16. Agbo, C. C., Mahmoud, Q. H., and Eklund, J. M. (2019, June). Blockchain Technology in Healthcare: A Systematic Review. In *Healthcare* (Vol. 7, No. 2, p. 56). Multidisciplinary Digital Publishing Institute.

17. Lu, Q., and Xu, X. (2017). Adaptable blockchain-based systems: a case study for product traceability. *IEEE Software,* 34(6), 21-27.

18. Ito, J., Narula, N., and Ali, R. (2017). The blockchain will do to the financial system what the internet did to media. *Harvard Business Review,* 9(March).

19. Bienkowski, M., Feng, M., and Means, B. (2012). Enhancing teaching and learning through educational data mining and learning analytics: An issue brief. *US Department of Education, Office of Educational Technology,* 1, 1-57.

20. Regulation, G. D. P. R. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46. *Official Journal of the European Union (OJ)*, 59(1-88), 294.

21. Kelly, M. (2019). New privacy bill would give parents an 'Eraser Button' and ban ads targeting children. URL `https://www.theverge.com/2019/3/12/18261181/eraser-button-bill-children-privacy-coppa-hawley-markey`

22. Demertzis, I., Papadopoulos, S., Papapetrou, O., Deligiannakis, A., Garofalakis, M., and Papamanthou, C. (2018). Practical Private Range Search in Depth. *ACM Transactions on Database Systems, 43(1),* 2.

23. Altman, M., Wood, A. B., O'Brien, D., and Gasser, U. (2018). Practical approaches to big data privacy over time.

24. Bowler, L., Acker, A., Jeng, W., and Chi, Y. (2017). It lives all around us: Aspects of data literacy in teen's lives. *Proceedings of the Association for Information Science and Technology, 54(1)*, 27–35. DOI:10.1002/pra2.2017.14505401004

25. Friedman, B., and Nissenbaum, H. (1996). Bias in computer systems. *ACM Transactions on Information Systems (TOIS), 14(3)*, 330-347.

26. Borgman, C. L. (2015). *Big data, little data, no data: Scholarship in the networked world.* MIT Press.

27. Kumar, P., Naik, S., Devkar, U., Chetty, M., Tamara, C., and Vitak, J. (2017). 'No telling passcodes out because they're private': Understanding children's mental models of privacy and security online. *Proceedings of the ACM on Human-Computer Interaction, 1(CSCW)*, 64.

28. Azaria, A., Ekblaw, A., Vieira, T., and Lippman, A. (2016, August). MedRec: Using blockchain for medical data access and permission management. *In 2016 2nd International Conference on Open and Big Data (OBD)*, 25-30. IEEE.

29. Zeide, E. (2014). The proverbial permanent record.

30. Common Education Data Standards - CEDS 101. Available from: https://ceds.ed.gov/pdf/ceds-101.pdf

31. Tempelaar, D. T., Heck, A. J. P., Cuypers, H., van der Kooij, H., and van de Vrie, E. (2013). Formative assessment and learning analytics. in D. Suthers, K. Verbert, E. Duval, and X. Ochoa (Eds.), LAK 2013: Third International Conference on Learning Analytics and Knowledge: 8-12 April, 2013, Leuven, Belgium, 205-209. New York: Association for Computing Machinery.

32. Bulger, M., Collins, S., Sallay, D., Vance, A. (2019). School safety and privacy: An animated introduction. *FERPA, SHERPA: The Education Privacy Resource Centre.* Available from: https://ferpasherpa.org/schoolsafetyvideo/

33. Baker, R. and Siemens, G. (2014). Educational data mining and learning analytics. In Sawyer K. (Ed.), Cambridge handbook of the learning sciences (2nd ed.), 253–274. New York, NY: Cambridge University Press.

34. Snyder, T.D., de Brey, C., and Dillow, S.A. (2016). Digest of Education Statistics 2015 (NCES 2016-014). National Center for Education Statistics, Institute of Education Sciences, U.S. Department of Education: Washington, DC.

35. Militello, M., Bass, L., Jackson, T. K., and Wang, Y. (2013). How data are used and misused in schools: Perceptions from teachers and principals.*Education Sciences, 3*, 98-120.

36. Arnold, K. E. and Pistilli, M. D. (2012, April). Course signals at Purdue: Using learning analytics to increase student success. Proceedings of the 2nd International Conference on Learning Analytics and Knowledge, 267–270.

37. Baker, R. S. (2016). Stupid tutoring systems, intelligent humans. *International Journal of Artificial Intelligence in Education, 26*, 600-614.

38. Kelly, G., Graham, J., and Fitzgerald, B. (2018). *State of edtech privacy report.* Common Sense Privacy Evaluation Initiative. San Francisco, CA: Common Sense.

39. Data Quality Campaign. (2018). What parents and teachers think about education data. Available from: https://dataqualitycampaign.org/resource/what-parents-and-teachers-think-about-education-data/

40. Student Data Privacy Consortium. (2018). Student Data Privacy Consortium: Policy and procedures. SDPC. Available from: https://privacy.a4l.org/wp-content/uploads/2018/06/Student-Data-Privacy-Consortium-P-and-P-2018-Final.pdf

41. California Consumer Privacy Act of 2018 (CCPA), CAL. CIV. CODE § 1798.198(a) (2018).

42. Colorado Student Data Transparency and Security Act (HB 16-1423). (2016). Available from: https://www.cde.state.co.us/dataprivacyandsecurity/crs22-16-101

43. Agbo, C., Mahmoud, Q., and Eklund, J. (2019). Blockchain technology in healthcare: A systematic review. *Healthcare, 7*, 56, 1-30.

44. Dwork, C., and Rothblum, G. (2016). Concentrated differential privacy. Working paper. Available from: https://arxiv.org/pdf/1603.01887.pdf

45. Sirota, D. (2013). Big data means kids' "permanent records" might never be erased. MOTHERBOARD, October 24. Available from: http://motherboard.vice.com/blog/permanent-records-are-hurting-kids.

46. Selwyn, N., and Pangrazio, L. (2018). Doing data differently? Developing personal data tactics and strategies amongst young mobile media users. *Big Data and Society*, January-June, 1-12.

47. Manolev, J. Sullivan A., and Slee, R. (2018). The datafication of discipline: Class Dojo, surveillance and a performative classroom culture. Learning, Media and Technology, 44(1), 36-51.