Embedding Blockchain Concepts into Common Computer Science Courses

Karol Lejmbach
Computer Science
Marquette University
Milwaukee, USA
karol.lejmbach@marquette.edu

Debbie Perouli
Computer Science
Marquette University
Milwaukee, USA
debbie.perouli@marquette.edu

Marta Magiera
Mathematical and Statistical Sciences
Marquette University
Milwaukee, USA
marta.magiera@marquette.edu

***Abstract*—This work in progress research paper focuses on effectively embedding the blockchain topic into undergraduate Computer Science (CS) programs without introducing a new course. The goal is two-fold: expose students to an important topic without requiring significant new resources, and enhance existing course materials with real world applications. The blockchain theory and technology is based on concepts that span almost the entire undergraduate CS curriculum. As such, it can aid educators in offering assignments that both reinforce lecture topics and relate to modern applications. Our work aims at providing adequate abstractions in each course to shrink the large-scale design and implementation of blockchain to modular pieces, each of which an undergraduate can understand and be expected to complete in an one or two week assignment.**

Current approaches to teaching blockchains focus on one course or a subset of electives. Some provide useful insights into potential assignment topics and courses in the CS program that should be targeted. Related work has also designed an interactive model of a blockchain for students to see how the various components work together. Inspired by prior work, we set out to answer the following questions: "Can we effectively teach students about blockchains by having students explore the concepts through embedded assignments?", and "Are these assignments still within the scope of the course as described in the course syllabus?" To gain insights into these questions, a series of assignments were created targeting four CS courses. Since the student level ranged from freshman to senior the assignments fell into two categories: exploratory and implementation.

Analyzed were 115 student responses collected between 2022 and 2023. The submissions consisted of the student's solution along with surveys that asked for the student's background knowledge and feedback on the assignment. Exploratory assignments were given in Introduction to Computer Science (21), and Introduction to Cybersecurity (36). Implementation based assignments were given in Hardware Systems (44), and Network Design and Security (14). In the first two courses, assignments asked students to research how blockchains work or how they are used in industry. In the last two courses, students were expected to provide a code solution to a problem along with a write up explaining their solution and the tests they ran to check functionality of their code. A background section was provided with the assignment explaining the motivation as well as expected behavior of the component of the blockchain. Instructors were encouraged to add any additional materials they deemed necessary to better prepare the class for the assignment.

The data gathered so far answer positively our two research questions, as all assignments matched well the course topics, the abstractions did not overly complicate the assignment, and students increased their knowledge and skills related to blockchains. We continue to expand the availability and use of embedded blockchain assignments.

***Index Terms*—Competencies Development; Cybersecurity, Computer Networks; Curriculum and Course Development; Project-based**

I. Introduction

Over the past few years many courses have been created that teach students about blockchains and their applications. As an example, Choudhury [3] provides a breakdown of ten programs where one could sign up for such a course. Viewed from a different angle, blockchains can help teach Computer Science (CS) concepts as they incorporate a wide range of topics, such as data structures, computer networks, cryptography, and distributed systems. Sakk and Wang [4] discusses how assignments based around blockchains could be introduced into various courses. The article demonstrates how blockchains offer an alternative way of teaching main computer science concepts through blockchains.

Our goal is to take this approach even further and create a series of standalone assignments. These assignments should provide the instructor with all the necessary material for a specific class. A challenge that needs to be addressed is complexity: industrial applications of blockchains are complex systems with many moving parts requiring substantial background knowledge to explain to a beginner.

To address this challenge, we resorted to abstractions that better align with a course's curriculum. Abstractions also allowed us to shorten the assignment completion time to make it more viable for both instructors and students.

II. Background

Blockchains are a form of decentralized data structure that store information in individual blocks [1]. The order of the blocks is fixed in such a way that does not allow for easy rearrangement of them [1]. Blockchain technology is built upon a wide range of CS concepts that span a large portion of a typical undergraduate CS curriculum. Topics such as networking, linked lists, and cryptography have been taught using blockchains [4]. Blockchain related courses have also been offered as upper division elective courses [4]. Blockchain teaching aids have also been created. These teaching aids vary greatly in scope and sophistication, but their primary use is

demonstrating to students the common interactions a user can have with blockchains [2].

The main drawback we have observed with these teaching aids is that they are tailored towards specific CS programs at a specific institution. We focus our efforts in developing assignments and aids for a larger scope of courses and curricula.

III. Methods

A series of assignments were created that targeted a considerable portion of core CS courses. These assignments were broken down into two major groups, exploratory and implementation. We then approached related instructors and asked if they would be interested in incorporating the assignment in their course. Exploratory assignments were geared towards freshmen and sophomore students as well as non-major students taking the given course as an elective. The primary focus of these assignments was to have students create reports on topics relating to Blockchain such as their applications in industry or security flaws found within them. In the Introduction to Cybersecurity course students researched the various 51% attacks that occurred on the Ethereum blockchain. The assignment in the Introduction to Computer Science course had students looking at how BitCoin works at a high level. Students explored how BitCoin transactions are stored and used for the exchange of BitCoin between users.

Implementation based assignments were given at the Network Design and Security course as well as the Hardware Systems course. Students were asked to implement components of Blockchains, Peer-to-Peer (P2P) connectivity between blockchain nodes, or public/private key programs that would be used for identifying ownership by signature. These assignments assumed more background knowledge from the student regarding the ability of writing source code. Background sections of these assignments included details regarding how the topic related to blockchains, and what functionality they were expected to implement.

Surveys were introduced in Fall 2023 to gather additional feedback from the students regarding the assignment. The pre assignment survey consisted of the following questions:

1) How much do you know about blockchains (1 Never heard of the subject - 5 I have used it in applications)?
2) How much experience do you have with blockchain (1 None - 5 I know how they are used in industry)?
3) How much experience do you have working with the homework topic (1 None - 5 I know how the topic is used in industry)?

The post assignment survey consisted of the following prompts and questions (1 Strongly Disagree – 5 Strongly Agree):

1) I found the assignment more challenging than the other assignments.
2) The assignment was relevant to the lecture topics.
3) The assignment helped me understand the lecture concepts better.
4) The assignment has taught me more about how blockchains work.
5) Using the blockchain example helped me better apply concepts from lecture.
6) Are there additional topics you are interested in surrounding blockchain?
7) Please provide any additional feedback regarding the assignment.

The submissions were graded by the instructor and we received the results after the grades had been posted.

IV. Initial Findings

Our initial results focus on comparing the difficulty of the blockchain assignment to the rest of the course assignments, as well as the opinion of the students regarding its relevancy to course material. We chose to use box plots to visualize class performance on the blockchain assignment compared to other assignments given to the students. We compared all assignment performance together regardless if the other assignment was of a different type, such as presentation or report. The results demonstrated that stand alone assignments do work; however, the correct levels of abstraction were critical for the performance of the assignment.

A. Introduction to Computer Science

The Introduction to Computer Science course is a freshman level course. The instructor of the course combined blockchain related questions with other topics in a larger assignment. Students were asked four high level understanding questions regarding blockchains and BitCoin. Figure 1 shows the performance of how the students did only on the blockchain portion of the larger assignment. The median was still in the low 90s as with other course assignments, while the negative skew was mainly caused by students skipping the blockchain portion or not submitting the assignment. The survey responses showed that the majority of the students did not find the assignment challenging. Also many students marked that they learned more about blockchains through this assignment.

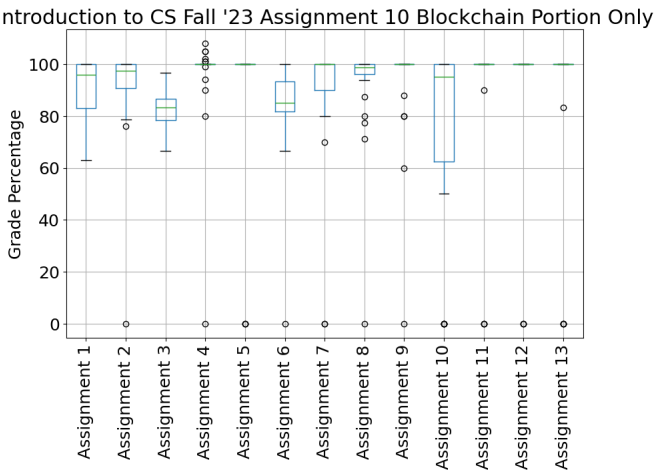

Fig. 1. Box plot showing class performance in the blockchain assignment (Assignment 10) compared to the rest of the assignments.

B. Introduction to Cybersecurity

Introduction to Cybersecurity is a course that can be taken by students of any major and has no computer science prerequisites. The course is also an elective to satisfy university core curriculum requirements. Although students can take it at any point in their education, and class offerings typically have representation from freshman to senior level, the single largest group tends to be sophomores. We ran two assignments in two different semesters.

1) Applications of Blockchains: The focus of this assignment was for students to explore the uses of blockchain. The students were tasked with selecting an industry, explaining how blockchains are used in it, and finally discussing what security implications exist in the industry's use of blockchains. Figure 2 shows the class performance on the blockchain related assignment, which was satisfactory.

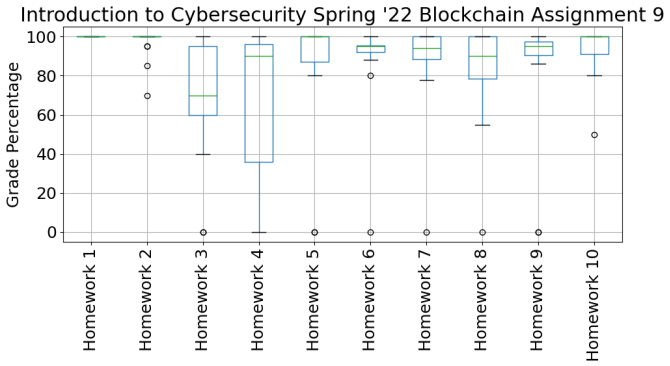

Fig. 2. Box plot showing class performance in the blockchain assignment (Homework 9) compared to the rest of the assignments.

2) 51% Attacks on Ethereum: In this assignment students were asked to write a report detailing various 51% attacks on the Ethereum blockchain. Students were to explain how the attack was carried out, what was the response to the attack, and finally give their opinion on how adequate the response was given the circumstances.

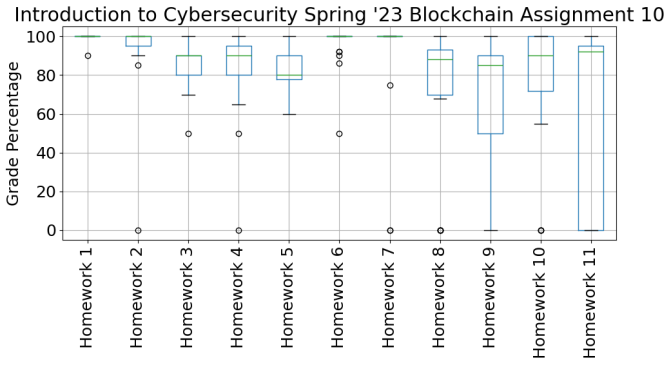

Fig. 3. Box plot showing class performance in the blockchain assignment (Homework 10) compared to the rest of the assignments.

Figure 3 shows the student performance on the assignment. The main item that caused students to lose points was omitting portions of the write up.

C. Hardware Systems Assignments

Hardware Systems is a sophomore level required course for CS majors, which includes the study of ARM or x86 assembly. As with the previous course, we provided two assignments in two different semesters.

1) Hardware Wallets – Public/Private Key Assignment: In the first assignment students were introduced to the idea of hardware wallets. The assignment background covered how public/private keys are used to verify identity. Students were then asked to implement in ARM assembly a simple program that would use a private key to sign a piece of data. Then the code would verify the signature by using the public key. Students were allowed to work in pairs, although preferred to work individually. Figure 4 shows the student performance on the assignments. The class as a whole did well on the assignment with the median being close to 100%.

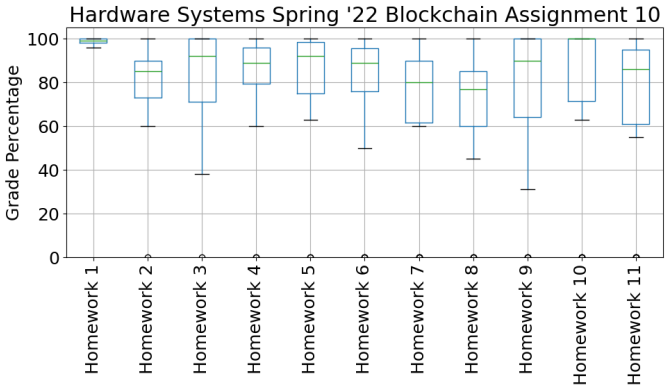

Fig. 4. Box plot showing class performance in the blockchain assignment (Homework 10) compared to the rest of the assignments.

2) Hardware Wallets – Analyzing Code Using Ghidra: The purpose of this assignment was for students to explore a simplified public/private key program written in C using the reverse engineering tool called Ghidra. The students were provided with an executable originally written in C. They were asked to analyze the executable using Ghidra and generate a report of their findings, which should include the purpose of the program. Students were asked to provide screenshots to support their findings.

Figure 5 showed the class performance on the assignments. Student performance on this assignment was worse compared to the blockchain assignment given in this course previously. This was caused by students omitting portions of the write up, or failing to correctly explain how the public/private key is meant to function. One student did criticise the assignment by writing, "I feel like it was more focused on dissecting code and encryption than focusing on how blockchains work". Nevertheless, students were in general still positive about the assignment teaching them about blockchains, many marking option 4 and 5 in their response to the related survey question.

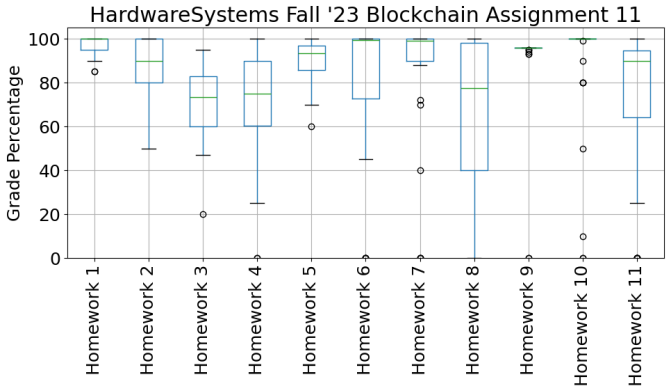

Fig. 5. Box plot showing class performance in the blockchain assignment (Homework 11) compared to the rest of the assignments.

D. Network Design and Security Assignment

One of the most challenging assignments was given in the Network Design and Security course. This course is offered as an elective to upper level undergraduates and cross-listed with the graduate masters program. The purpose of this assignment was for students to explore the differences between a client-server network and a peer-to-peer (P2P) network. The assignment background explained the overall purposes of P2P networks, and why they were useful when dealing with decentralized communication in the context of a blockchain. We provided the students with C header files. Additional C code with a linked list was provided.

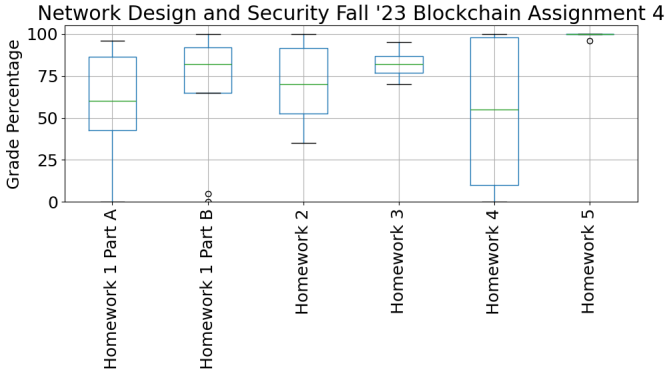

Fig. 6. Student performance on the Blockchain Assignment 4 compared to the other assignments given.

Figure 6 shows the large spread of grades with the median just below 60%. The feedback given by the students confirmed our observation of the difficulty had by the students. Many students marked 4 or 5 on the end of assignment survey. There were a few student who criticised the assignment for being irrelevant to the course; one of the responses to the additional feedback prompt was: "I don't think the assignment was relevant to the course content, nor do I think we were given enough guidance regarding how to execute the assignment". Another student wrote, "I think that reviewing the header files in class would have been helpful".

The main reason for students struggling in this assignment was underestimating the complexity. This assignment had many moving parts and the source code provided to the students was substantial. We have recreated this assignment addressing some of the criticism raised by the students as well as our own observations. The new assignment's background section also goes into much greater detail into the algorithm that the peers will follow when establishing connections, transmitting data, and dealing with disconnects.

V. Discussion

Blockchain technology is not simple. One of the biggest challenges we had to overcome was applying correct levels of abstraction to meet the student's background knowledge. This was especially important in the implementation based assignments. The P2P assignment given in the Network Design and Security course suffered from this. The other assignments given in the Hardware Systems courses performed better but were much less complex. We believe that with some more revisions these assignments will perform a lot better. In the assignment given to the Introduction to Computer Science class only part of the assignment was about blockchains. This assignment fell into the exploratory category and had students learn about various aspects of blockchains by seeing how BitCoin uses blockchain. It came as little surprise that the exploratory assignments performed well. The data gathered does support the first research question and students can be taught about blockchains and their components using these assignments. The research question regarding the assignment scope was also answered. Assignments that were inadequately abstracted demonstrated how easily an assignment can go beyond the scope of the class, especially when dealing with a topic as complex as Blockchain.

VI. Future Work

The first major piece for future work is adjusting the assignments based on student feedback. This should be achieved by adjusting the abstraction in the assignments along with revisions to the background sections. The next major step is the implementation of a tool that will let students implement a specific functionality of a blockchain. The goal here will be to allow students to see a given component of a blockchain as used in daily operations. The final piece is distributing these assignments to other institutions and gathering feedback from instructors that used the assignments.

References

[1] Andreas M. Antonopoulos. *Mastering Bitcoin, 2nd Edition*. O'Reilly Media, Inc, June 2017. ISBN: 9781491954379. URL: https://learning.oreilly.com/library/view/~/9781491954379/?ar.

[2] Xingyu Chen et al. "Blockchain Simulation: A Web Application for IT Education". In: IEEE, Jan 27, 2021, p. 486. DOI: 10.1109/CCWC51732.2021.9375934. URL: https://ieeexplore.ieee.org/document/9375934.

[3] Ambika Choudhury. *Top 10 Free Resources To Learn Blockchain*. Apr. 2020. URL: https://analyticsindiamag.com/top-10-free-resources-to-learn-blockchain/.

[4] Eric Sakk and Shaungbao Paul Wang. "Integration of Blockchain Concepts into Computer Science Curriculum". In: *Journal of The Colloquium for Information Systems Security Education* 8.1 (Fall 2020).