Project

INSE 6615: Blockchain Technology

Due: **Last Day of Class**

Upload on EAS by 20:00

Projects must be in PDF format. Please name the file: `sid1_sid2_project.pdf` *(where* `sid1` *is the student id for the first team member, adding additional student numbers as applicable). Upload the file to the EAS system under "Project." If working in a group, only upload one file (it doesn't matter which team member uploads it) and ensure all team members are listed on the first page of the report. Please ensure you are registered for EAS well in advance of the deadline.*

EAS: https://fis.encs.concordia.ca/eas/

In this project, you will pick a topic related to Bitcoin, Ethereum, other cryptocurrencies, or blockchain technologies. Projects might fall into one of two categories (other styles of paper are acceptable as well but please pre-approve with me first): (1) survey of a topic for which a number of results have been proposed, (2) a new deployment of a technology that you design. For (2), I recommend working with Solidity on Ethereum to implement something useful that doesn't exist yet or where you can improve on the existing ideas.

Projects are to be done individually or in groups of 2, 3, or 4. All group members receive the same mark for the project. My expectations will increase as the group size increases.

The project will consist of a written report. If code is developed, you will describe the code in the written report and the code itself will not be graded.

Paper format: No title page, simply a title followed by the group members (names and student numbers) at the top of the first page. The paper should be a maximum of 8 pages in any reasonable format for a paper. References can be in any format.

Your paper should summarize the subject with an introduction, explaining very clearly what the research problem is and how you will address it. You should explain your results with technical detail.

There is no requirements on how many other papers you draw from or if the type of papers they are, however you are responsible for checking to see if there are relevant academic papers on your chosen topic.

If you are describing the work of others, you should do it critically: having looked at a broad set of knowledge on the subject, compare and contrast individual contributions. You can be skeptical of what others have written—authors may miss or leave out important criteria in evaluating their own results.

If you are looking for good quality venues that publish research in this area, here is a partial list:

Conferences with most papers on blockchain technology: *Financial Cryptography, ACM Advances in Financial Technology, DeFi Workshop, Workshop of Trusted Smart Contracts, IEEE Security & Blockchain*

Conferences with occasional papers on blockchain: *IEEE Security & Privacy, ACM CCS, USENIX Security, NDSS, CRYPTO, EUROCRYPT, ASIACRYPT*

Be sure to cite all sources you use. You may do citations in a conversational way (e.g., "Boneh et al list the five essential properties of blah as follows [9].") Under no circumstance can you use someone else's text as your own (even if you modify the grammar)! Review Concordia's plagiarism policy and understand it:

https://www.concordia.ca/students/academic-integrity.html
https://www.concordia.ca/encs/students/sas/expectation-originality.html

I am here to help. You are not required to submit anything to me other than the final report. But I am happy to discuss your topic during office hours. I cannot review drafts of reports as there are too many students and it takes too much time.

Grading:

Grading Scheme	
20	Scope and execution
10	Interpretation
10	Technicality
10	Presentation
50	**Total**

Scope and execution: A good project will have a clearly defined scope: what is on-topic for the project and what is off-topic. I recommend phrasing your project topic as a question and the project itself answers the question. The topic should be important and timely. With a well-defined topic, the paper should be organized with a logical flow through that links its material together. There should be a reason that each portion of the paper exists. The paper should be complete and comprehensive. The material will be appropriate to blockchain technology, cryptocurrencies, decentralized finance, web3, or smart contracts.

Interpretation: It is easy to read other research or technical documents and repeat what they say without truly understanding it. A good project will explain existing research in way that makes it clear that the writer really understands it. It will be selective in how much detail is included to ensure the main point of the paper is made.

Technicality: A good project will include technical details that appropriate for a graduate-level course in security. It will be correct in what it says.

Presentation: The deliverable should be high quality. It should be well written. Sections and subsections should provide a useful organization of the paper. Figures and tables should be used appropriately. Citations should be used appropriately. A good project will demonstrate an adequate level of work went into it (it is a project that is meant to be worked on for the whole course).

Deductions: Outside of these categories, I will deduct marks if the quality and quantity of work does not reflect the number of team members.