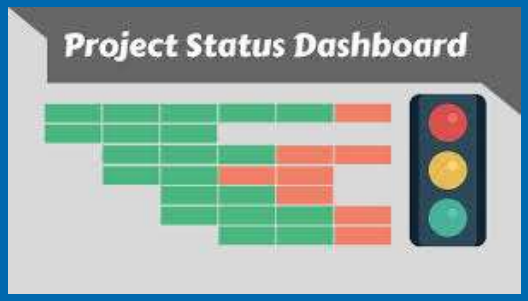
Week 8
Project Info
Mining Competition



Project

- Your project should be well underway by now
- Please let us know if you need help
- Keep an eye on the deadline (end of week 11)

- If you need a refresher on Team Work, here is a good resource:
  - https://www.edx.org/course/working-in-teams-a-practical-guide

- As mentioned in Week 1 and in the ECP, there will be a **Peer Assessment** process which will assess the contributions of individual team members, and adjust individual marks accordingly.
- It's a good idea to keep track of your contributions, e.g. journal, git log, etc., in case there are any issues.

Project Demo

- Answer to question posted on Ed:
- The project demos will be scheduled in weeks 12 and/or 13. I will provide you with a list of possible time slots, and project teams can choose whichever works for them.
- During the demo, you should provide an overview of your project. This should be a team effort, and involve all team members. You should not assume I that I have read your project report, and you need to tell the entire story, including the scope, motivation and background of your project. The key focus will be on your outcomes/implementation, and ideally you should provide a demonstration (if applicable and possible). This is then followed by a Question & Answer part. The demo assessment is relatively informal, and I might also ask questions during your presentation.
- I suggest you prepare a small number of slides for your presentation.
- Your presentation should be around 10-15 minutes, to allow enough time for questions. The entire demo will go for 20-30 minutes.
- I suggest you have a look at the demo marking sheet, provided on Blackboard.
- The best preparation for the demo is to have solid project results and outcomes, then the demo is relatively straightforward.

Project

- Any questions?

Blockchain in the News

POLICY \ TECH \ CYBERSECURITY \

Beanstalk cryptocurrency project robbed after hacker votes to send themself $182 million

The attacker used a flash loan to obtain a controlling stake in the project

By Corin Faife | @corintxt | Apr 18, 2022, 4:26pm EDT

- https://www.theverge.com/2022/4/18/23030754/beanstalk-cryptocurrency-hack-182-million-dao-voting

COMS4507
Crypto Mining Competition

Mining Problem

- Find nonce *n*, so that **h(*studentID* || *n*) < *target***
- h() is sha256
- *studentID* is your student ID, encoded in ascii
  - no terminating '\0' character
  - e.g. **'43330013'**
- '||' means concatenation
- target = 2^{212}
  - This means the first 44 bits of the hash result need to be 0,
  - In hexadecimal representation:
    - The first 11 hexadecimal characters need to be 0
- *n* is an ascii string, maximum 40 characters long
  - only printable characters

How long will it take?

- Expected number of trials?
  - 2^44 ≈ 1.8 * 10^13
- How long would it take (**on average**) with an Antminer S19 Pro Miner, which can do 110TH /s?
  - 110 TH/s = 110 * 10^12 H/s
  - It would take
    - 1.8 * 10^13 / 110 * 10^12 H/s ≈ 0.16 seconds
- Problem?
  - You probably don't have an S19 Pro Miner (maybe you do).
  - And even if you did, it would be of no use, since our hash puzzle is slightly different from than the one used in Bitcoin, and the hash puzzle algorithm 'baked' into the ASIC.
- You can estimate for yourself what the expected solve time is for a standard CPU.

Submitting Solution

- You need to submit *n* and your student ID via email to me
  - I will acknowledge receipt via reply email
- Time of email receipt of valid solutions will determine winner(s)
- You also need to submit your source code, plus stats
  - Details of your ‘mining rig’, in particular the hash rate
  - Number of hash attempts until you found solution

Solution Validation

- I will copy-paste ascii string into this tool:
  - http://www.xorbin.com/tools/sha256-hash-calculator
- Example:
  - Student ID: “43745091”
  - n = “06GH9BYYZ5”
  - target = 2^{228}
    - For this example, only first 28 bits need to be 0, (228 + 28 = 256), or first 7 hex characters
  - Hash (hexadecimal) =
    - 0000000505562365dc9268454f4644a925e1e1bd435be40ce9a63dfd889f8258
  - This took around 20 minutes to find, based on very non-optimised Python code (~10 lines), on a standard PC
    - You can do a number of things to speed this up

What if no one finds a solution?

- I'm trying to set the difficulty so that this is unlikely.
- I also don't want it to be too easy, so that the solution is not found too soon.
  - However, since this is probabilistic, anything can happen.
  - Last time, the winner found the solution with only 3% of the expected work (hash trials).

- Keep your best partial solution, i.e. the one with the lowest value (most leading zeroes), just in case no one finds the full solution, by the end of Week 12.
  - Friday, 27 May, 4:00pm
- In that case, the student(s) with best (lowest value of n) partial solution(s) will win.

Price for the Winner(s)

1 BTC = 100,000,000 Satoshi

- In addition to eternal Fame and Glory

- 1st Price
  - 50,000 Satoshi
- 2nd Price
  - 25,000 Satoshi
- 3rd Price
  - 10,000 Satoshi

- Everybody has a chance to win, even with a slow computer.
- Your price (Bitcoin transaction) will be recorded on the Bitcoin blockchain for ‘eternity’

Mining Pool

- You can solve puzzle individually, or you can form a “mining pool”
- Consider these questions
  - Benefit of forming a pool
  - How do you share prize
    - Winner-takes-it-all
    - Equally
    - According to level of contribution
      - How do you measure/proof that?

Important

- Do not use ‘unreasonable’ amounts of UQ computing resources for this!!!!

Good Luck! ☺

Any Questions?