IS4302 Blockchain and Distributed Ledger Technology

Lecture 5
10 Feb, 2023

NUS
National University of Singapore

Mid-term test

- **90 min coding test**
- **Mar 3, 14:00 - 15:30**
- **Open book**
- **E-exam**

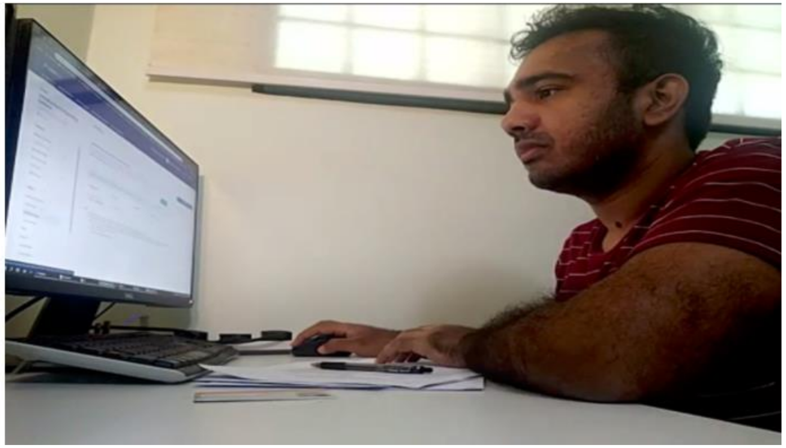
E-exam

- **Canvas to distribute and collect exam paper.**
  - Just like assignments
  - I will post the exam paper at 2 pm and set the deadline of submission at 3:30 pm

- **Zoom chat to communicate. Send me private messages for any questions/requests.**

- **Read https://mysoc.nus.edu.sg/academic/e-exam-sop-for-students/ carefully**
  - We don’t use Examplify and Microsoft teams

E-exam



- **Proctoring protocol: two parts**
- **Zoom camera**
  - The Zoom camera must be positioned to capture one side of your face, both hands with table & the entire PC screen
  - laptop’s built-in webcam does not suffice
- **PC screen recording**
  - Record your screen with a screen recording software
  - Compress the recordings if needed
  - Upload the recordings to Canvas within 3 hours after the completion of the exam
  - Only one screen is allowed

What is blockchain?

- **Blockchain is a ledger writing technology, that can record**
  - Transactions
  - Inventory
  - Personal data
  - …
  - Any information you want to record

- **Distributed ledger with consensus**

What are the features of blockchains?

- **3 main properties of blockchain:**
  - Distributed ledger – everyone has the same info
  - Consensus – everyone(majority) agreed to the same info
  - Immutability – no one can erase a transaction previously agreed upon

Common knowledge

- **Something is common knowledge if**
  - everyone know it
  - everyone know that everyone know it
  - everyone know that everyone know that everyone know it
  - …

- **“Almost common knowledge” can be very different from common knowledge**

- **Blockchain can make a piece of information common knowledge.**

The blue-eyed islanders puzzle

There is an island upon which a tribe resides. The tribe consists of 1000 people, with various eye colors. Yet, their religion forbids them to know their own eye color, or even to discuss the topic; thus, each resident can (and does) see the eye colors of all other residents, but has no way of discovering his or her own (there are no reflective surfaces). If a tribesperson does discover his or her own eye color, then their religion compels them to commit ritual suicide at noon the following day in the village square for all to witness. All the tribespeople are highly logical and devout, and they all know that each other is also highly logical and devout (and they all know that they all know that each other is highly logical and devout, and so forth).

The blue-eyed islanders puzzle

Of the 1000 islanders, it turns out that 100 of them have blue eyes and 900 of them have brown eyes, although the islanders are not initially aware of these statistics (each of them can of course only see 999 of the 1000 tribespeople).

One day, a blue-eyed foreigner visits to the island and wins the complete trust of the tribe.

One evening, he addresses the entire tribe to thank them for their hospitality.

However, not knowing the customs, the foreigner makes the mistake of mentioning eye color in his address, remarking "it is interesting to see blue-eyed person like myself in this region of the world".

The blue-eyed islanders puzzle

- What effect, if anything, does this statement have on the tribe?

- No? Because his comments do not tell the tribe anything that they do not already know (everyone in the tribe can already see that there are several blue-eyed people in their tribe).

- Yes?

The blue-eyed islanders puzzle

- **What if there is only one person in the tribe that has blue eyes?**
  - He or she will realize that the traveler is referring to him or her, and thus commits suicide on the next day, because no one else in the tribe has blue eyes.
- **What if there are two in the tribe that have blue eyes?**
  - Each of them will think, if I am not blue-eyed, then the other guy with blue eyes will know that the traveler is referring to him or her and thus commit suicide on the next day.
  - If no one commit suicide on the next day, then I have blue eyes, so I should commit suicide 2 days later.

The blue-eyed islanders puzzle

- **What if there are n individuals in the tribe that have blue eyes?**
  - After n-1 days and no one suicide, everyone know that there are more than n-1 individuals in the tribe that have blue eyes, but the ones with blue eyes can only see n-1 among others who have blue eyes, so they themselves must have blue eyes. Therefore, all the blue-eyed individuals will commit suicide after n days.
- **So, in the original question, the effect is, everyone in the tribe with blue eyes will commit suicide after 100 days.**

The blue-eyed islanders puzzle

- **The traveler's statement does not communicate any information about the event itself (there is blue-eyed in the tribe).**
- **But, the statement makes this (there is blue-eyed in the tribe) a common knowledge.**
- **Without this statement**
  - If there are two people with blue eyes (denoted A and B), A didn't know that B know that there is blue-eyed in the tribe, B also didn't know that A know that.
  - If there are three people with blue eyes (A, B and C), A didn't know that B know that C know that there is blue eyed in the tribe,…
  - …

Blockchain application - transparency

- **Blockchain can make a piece of information common knowledge.**

- **What information to share?**
  - Health information – health insurance
  - Order book information – markets
  - Inventory, production, sales… information – supply chain
  - …

Blockchain application - immutability

- **Immutability – no one can erase a transaction previously agreed upon**
- **Trust from immutability**
- **Who needs trust?**
  - Fundraisers
  - Currency issuers
  - Sellers
  - …

Group project criteria

- **Don’t need to be extremely innovative in terms of industry.**
- **Be practical, be specific, be comprehensive.**
  - Think about each stakeholder’s incentive, information structure,…
  - Try to design a system such that it makes sense.
  - Don’t be afraid of limitations, but try to make them fall in the least critical aspects
  - Be innovative at overcoming limitations
  - Discuss those limitations

Assumptions

- **Reasonable assumptions beyond current practice can be made.**
  - E.g., Cost for pure computation can be low (introduction of cloud service and layer-2s)
  - The existence of reasonable/incentive compatible oracle systems can be assumed.

What to think about

- **To B? To C?**
- **Why does each stakeholder want to use your system?**
- **Will they behave as intended?**
- **What does each stakeholder know/could know? Is this desirable?**

What to think about

- **Is a token needed?**
- **If so, how to design the tokenomics?**
  - Exclusivity?
  - Limited supply or constant supply or something else?
  - Speculation needed or not?
- **Is data segregation needed? If so, how?**
- ……

Consultation

- **No tutorial or lecture next week.**
- **Consultation on Feb 16, 17.**
- **In person at my office：COM2-04-10**
- **Try to focus on one topic after brainstorming.**

Thank you!