

Module 5: Principles of Data Ethics

Ethics

- Ethics is the study of morality. Morality is a subject that pertains to right and wrong action
 - In all human societies on the ethnographic record, people make distinctions between right and wrong (Brown, 1991).
 - I take it that you have your own views about what is right and wrong.
 - In the branch of ethics called normative ethics, we try to arrive at well-founded views about morality.
- Normative ethics relates to using, applying, and developing digital and online tools



Why do we need data and digital ethics?

- There is an international consensus that ethics is vital to the development, application, and use of digital and online technologies (Vallor, 2021).
 - Technology shapes the way people live.
 - While digital and online technologies offer remarkable benefits (e.g., knowledge, communication, efficiency, personalisation), they also pose risks of significant harms to privacy, security, autonomy, fairness, transparency, etc.
 - Lawmakers are often unable to keep up with the speed of technological advancement. Hence, not only expert technologists, but also ordinary users, must learn to develop and use technologies in ways that avoids harms while getting the most from the benefits.

Moral Theories

In normative ethics, moral theories are developed to achieve two aims (Timmons, 2019):

- **Theoretical aim:** To explain what features of actions make them morally right or wrong
- **Practical aim:** To offer practical guidance in making morally correct decisions

These three moral theories are among the most influential in normative ethics (Timmons, 2019):

1) **Utilitarianism (Jeremy Bentham, John Stuart Mill, Peter Singer, etc.):**

An action is morally right when it would likely produce at least as much well-being (welfare) as would any other action one might perform instead. Otherwise, the action is wrong.

- The classical utilitarians, such as Bentham and Mill, took well-being to consist of pleasure and the absence of pain.
- Peter Singer, a contemporary utilitarian, takes wellbeing to consist of the satisfaction of one's preferences/desires.

2) **Virtue ethics (Confucius, Aristotle, etc.):**

An action is morally right when it is what a virtuous person would do in the circumstances. Otherwise, the action is wrong.

- Commonly recognised virtues include honesty, courage, justice, temperance, beneficence, humility, loyalty, and gratitude.
- A truly virtuous person is one who has all the virtues. A virtuous person may only be a hypothetical ideal that we can strive to be.

3) **Immanuel Kant's deontological ethics:**

An action is morally right when it treats persons (including oneself) as ends in themselves and not merely as a means. Otherwise, the action is wrong.

- Kant's theory says that all persons are unconditionally valuable insofar as they are rational and autonomous.
- It also says that we should respect the value of persons, and not use them in a way that disrespects their value.

Principles of Data Ethics

- Moral theories are meant to provide very general explanations and guidance concerning what we morally ought to do.
- While moral theories have the advantage of comprehensiveness, it can be difficult to deduce what they would prescribe in a particular context.
- Several professional associations and private firms have formulated more specific principles to guide actions with respect to data and information technology.
 - Links to these sets of principles are provided in the Notes section below.

- The following principles are sampled from the Singapore Computer Society's professional Code of Conduct:

Integrity

SCS members will act at all times with integrity. They will:

- not lay claim to a level of competence that they do not possess
- act with complete discretion when entrusted with confidential information
- be impartial when giving advice and will disclose any relevant personal interests
- give credit for work done by others where credit is due

Professionalism

SCS members will act with professionalism to enhance the prestige of the profession and the Society. They will:

- uphold and improve the professional standards of the Society through participation in their formulation, establishment, and enforcement
- not seek personal advantage to the detriment of the Society
- not speak on behalf of the Society without proper authority
- not slander the professional reputation of any other person
- use their special knowledge and skill for the advancement of human welfare

Cyberbullying

- Cyberbullying is the use of the internet or digital devices to inflict psychological harm on a person or group (Quinn, 2019; Media Literacy Council 2018).
- Examples:
- Repeatedly texting or emailing hurtful messages to another person.
 - Spreading derogatory lies about another person.
 - Tricking someone into revealing highly personal information. - "Outing" or revealing someone's secrets online.
 - Posting embarrassing photographs or videos of other people without their consent.
 - Impersonating someone else online in order to damage that person's reputation.
 - Threatening or creating significant fear in another person.
- Prevalence:
- According to the 2020 Child Online Safety Index (Cos) report, which includes data on 145,000 children across 30 countries, 45% of 8- to 12-year-olds experienced cyberbullying, either as the bullies or as the victims.
 - Within Singapore, 40% of 8- to 12-year-olds and 52% of 13- to 19-year-olds were exposed to cyberbullying.

➤ **Effects:**

- Depression and anxiety
- Low self-esteem
- Difficulty sleeping
- Headaches, stomach aches
- Suicidal thoughts
- Suicide attempts
- Eating disorders

➤ **What you can do if you are cyberbullied:**

- Don't blame yourself.
- Don't retaliate.
- Save the evidence: Take screenshots of texts.
- Talk to someone you trust.
- Block the bully.
- Report the bully.
- Keep social media passwords private.
- Restrict others' access to your social media pages.
- Change your social media accounts: If you are harassed, delete the account and create a new one.

➤ **How to know if someone you care about is being cyberbullied:**

- Changes in mood or personality.
- Work or school performance declines.
- Lack of desire to do things they normally enjoy.
- Upset after using phone or going online.
- Secretive about what they are doing online.
- Unusual online behaviour: Not using phone/computer at all; using phone/computer all the time; receiving lots of notifications.
- Deleting social media accounts.

Informational Privacy

- Digital and online technologies have a **major impact on one's ability to secure privacy.**
- In particular, these technologies affect what the philosopher Anita L. Allen describes as informational privacy: **"confidentiality, anonymity, data protection, and secrecy of facts about persons"** (Allen, 2005)
- Consider this incident where some researchers released the personal profile details of 70,000 users on OkCupid, a dating website:
Brian Resnick, "Researchers just released profile data on 70,000 OkCupid users without permission," Vox (12 May 2016).
- Critics maintained that the (informational) privacy of the OkCupid users was violated by the researchers, because the **researchers stored and re-deployed the personal information of the users without their consent.**

- A right to privacy is recognised in all international and regional human rights instruments, including Article 12 the Universal Declaration of Human Rights:

- “

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

” -

Whistle-Blowing

- In large organisations, it can be difficult to hold people accountable for unethical or illegal acts.
- Law enforcement and regulators are not able to constantly monitor the internal operations of organisations. Such constant surveillance isn't even desirable.
 - Leadership within the organisation may cover up any corrupt activities.
- There are many examples of misconduct in organisations not being brought to light until much damage has already been done, or only after a private citizen reported it at great personal cost.
- The 1986 Challenger Disaster is a memorable case where something catastrophic happened as a result of internal mismanagement.
 - A more recent case involving Wirecard, an electronic payment company, was reported in Singapore.
 - Data analytics firm Cambridge Analytica crossed many ethical lines.
- Sometimes it is up to ordinary, low-level people to “blow the whistle” on unacceptable conduct in their organisations.
-  “A whistle-blower is someone who breaks ranks with an organization in order to make an unauthorized disclosure of information about a harmful situation after attempts to report the concerns through authorized organizational channels have been ignored or rebuffed.” (Quinn, 2019, emphasis added)
- The question of whether to “blow the whistle” can arise in any organisation—not just in government agencies and private businesses.
 - NTU has its own dedicated whistle-blower channel, which is taken very seriously

- But when should one whistle-blow? In his well-known textbook on business ethics, Richard T. De George proposed that whistle-blowing is **morally permissible** when **three conditions are fulfilled** (De George, 2006; Brenkert, 2009):

1. The firm...will do [or has done] serious and considerable harm to employees or to the public.
2. Once employees identify a serious threat to the user of a product or to the general public, they should report it to their immediate superior and make their moral concern known.
3. If one's immediate supervisor does nothing effective about the concern or complaint, the employee should exhaust the internal procedures and possibilities within the firm.

- De George went on to suggest that if two additional conditions are met, then it would be **morally obligatory** for someone to whistle-blow (De George, 2006; Brenkert, 2009):

-  4. The whistle-blower must have, or have accessible, documented evidence that would convince a reasonable, impartial observer that one's view of the situation is correct; and
-  5. The employee must have good reasons to believe that by going public the necessary changes will be brought about. The chance of being successful must be worth the risk one takes and the danger to which one is exposed.

- **First objection** to De George's criteria (Quinn, 2019): **The criteria are too stringent.** It can be morally permissible to whistle-blow, even when not all of conditions 1 through 3 are met.

- For instance, it may be morally permissible to whistle-blow when you know that serious harm will be done to the public, but there is not enough time to lobby supervisors and exhaust all internal reporting procedures.
- By itself, the effort to prevent serious harm may be enough to make whistle-blowing morally permissible.

➤ Second objection to De George's criteria (Quinn, 2019): The criteria are not demanding enough. It can be morally obligatory to whistle-blow even when conditions 4 and 5 have not been fulfilled.

- For instance, a single employee may have satisfied conditions 1 through 3, but still be unable to acquire enough documented evidence to convince an impartial observer that any wrongdoing has been done.
- However, it may still be morally obligatory to whistle-blow, if one is confident that another organisation, such as law enforcement or the media, would be able to persuade an impartial observer of the organisation's wrongdoing.

Lams Questions

1. 1 Why is ethics important to the use and development of digital and online technologies?

Why is ethics important to the use and development of digital and online technologies?

*

Choose one of the following answers.

- a) These technologies only inflict harm and misery upon humanity. We need ethics to finally end the madness.
- b) It is morally wrong to use digital and online technologies. Ethics is needed to help us find a way to overcome our dependence on these technologies.
- c) These technologies pose risks of harms to privacy, security, fairness, and other values. Ethics shows that these values are ultimately not important.

Although digital and online technologies bring many benefits, they also pose risks of harms to privacy,
✓ d) security, fairness, and other values. Therefore, we need to develop and use these technologies in ways that avoid their associated harms while getting the most from their benefits.

A is incorrect. Digital and online technologies offer remarkable benefits in the form of knowledge, communication, efficiency, and personalization.

B is incorrect. While some uses of digital/online technologies can be wrong, such as cyberbullying and stealing private information, not all uses of these technologies are wrong.

C is incorrect. Privacy, security, and fairness are important values, and they are widely recognized as such.

D is correct. Ethics helps us assess how to develop and use digital/online technologies in ways that avoid their associated harms while getting the most from their benefits.

1. 2 Which of the following is an incorrect application of a moral theory to the evaluation of cyberbullying?

Which of the following is an **incorrect** application of a moral theory to the evaluation of cyberbullying?

*

Choose one of the following answers.

- a) Society as a whole would be better off if people didn't cyberbully each other. Therefore, from a utilitarian point of view, cyberbullying is morally wrong.
- b) Cyberbullying is cruel because it subjects another human being to anguish and humiliation. A virtuous person would not be cruel. Hence, from the perspective of virtue ethics, cyberbullying is morally wrong.
- c) Cyberbullying respects the rationality and autonomy of the victim, since it gives the victim a chance to rationally and autonomously overcome the distress caused by cyberbullying. Therefore, cyberbullying is morally right from the perspective of Kant's ethics.
- d) Cyberbullying does not respect the victim as a rational and autonomous being. It causes depression and anxiety, which is known to weaken a person's sense of control over their own lives. It also causes irrational, self-harming behavior such as eating disorders and suicide attempts. Therefore, from the perspective of Kant's ethics, cyberbullying is morally wrong.

A is actually a correct application of utilitarianism. Utilitarianism says that an action is wrong when it does not produce at least as much well-being as an alternative action one could perform instead. Since people who cyberbully make others worse off than they'd be if they didn't cyberbully, cyberbullying is wrong from a utilitarian point of view.

B is actually a correct application of virtue ethics. Virtue ethics says that an action is wrong if a virtuous person would not perform it. A virtuous person would not cyberbully, since cyberbullying is cruel, and cruelty is not a virtue. So, from a virtue-ethical perspective, cyberbullying is wrong.

C is the appropriate choice, since it describes an incorrect application of Kant's ethics. Cyberbullying does not respect the victim's rationality and autonomy, because it does not enable rational and autonomous behavior. On the contrary, cyberbullying causes depression and anxiety, which is known to weaken a person's sense of control over their own lives. It also causes irrational, self-harming behavior such as eating disorders and suicide attempts.

D is actually a correct application of Kant's ethics. Kant's ethics says that an action is wrong if it fails to respect persons as rational and autonomous beings. Cyberbullying does not respect persons as rational and autonomous beings. So, from the perspective of Kant's ethics, cyberbullying is wrong.

1. 3 Which of the following actions interferes with a person's informational privacy?

Which of the following actions interferes with a person's informational privacy? *

Choose one of the following answers.

- a) Inviting someone to follow another person's profile on social media (e.g., Twitter or Instagram), because you think they post interesting content.
- b) Revealing confidential secrets about a person's sexuality online.
- c) Spreading defamatory lies about someone in an attempt to destroy their reputation.
- d) All of the above.

A is incorrect. Informational privacy has to do with confidentiality, data protection, and secrecy of facts. It doesn't violate a person's informational privacy to transmit information about them that they have consensually made public. Social media profiles are either publicly accessible, or their owners consent to make their profiles accessible to selected people.

B is correct. Informational privacy has to do with confidentiality, data protection, and secrecy of facts. It would be a violation of someone's information privacy to reveal secrets that they want to keep confidential.

C is incorrect. Although it's wrong to spread lies about someone, it is not necessarily a violation of their informational privacy. For example: if someone tells your teacher that you cheated on a test when you did no such thing, they aren't spreading information you prefer to keep secret. Since you didn't cheat at all, you had no secret to keep.

D is incorrect as options A and C do not describe violations of informational privacy.

1. 4 Frances Haugen

Frances Haugen [see references below] was an employee at Facebook for 2 years until May of 2021. While working at the social media giant, she worked on the civic integrity team. Over time she became persuaded the company was not doing as much as it could to combat misinformation, cyberbullying, hate speech, addictive behavior, criminal activity, and espionage on the platform. She suggested to her superiors that Facebook should hire more people to deal with these issues properly, but the company took no action. *

Haugen then collected thousands of internal memos and studies suggesting that Facebook itself was aware of the harmful and criminal behavior taking place on its platform, but chose not to address it in order to boost user engagement. She released the documents to the United States Securities and Exchange Commission, together with a whistleblower complaint. In October of 2021, she testified before the United States Senate that Facebook was prioritizing profits over the safety of its users. According to Richard De George's criteria, was Haugen's act of whistleblowing morally obligatory, morally permissible, or neither?

*References

- Cat Zakrzewski, Cristiano Lima, Elizabeth Dwoskin and Will Oremus. 2021. "Facebook whistleblower Frances Haugen tells lawmakers that meaningful reform is necessary 'for our common good'" (5 October 2021). The Washington Post. URL: <https://www.washingtonpost.com/technology/2021/10/05/facebook-senate-hearing-frances-haugen/>
- Jeff Horwitz. 2021. "The Facebook Whistleblower, Frances Haugen, Says She Wants to Fix the Company, Not Harm It" (3 October 2021). The Wall Street Journal. URL: <https://www.wsj.com/articles/facebook-whistleblower-frances-haugen-says-she-wants-to-fix-the-company-not-harm-it-11633304122>
- Ryan Mac and Cecilia Kang. 2021. "Whistle-Blower Says Facebook 'Chooses Profits Over Safety'" (3 October 2021). The New York Times. URL: <https://www.nytimes.com/2021/10/03/technology/whistle-blower-facebook-frances-haugen.html>

Choose one of the following answers.

- a) Under De George's criteria, it is morally obligatory to blow the whistle in this case.
- b) Under De George's criteria, it is morally permissible but not obligatory to blow the whistle in this case.
- c) Under De George's criteria, it is neither morally obligatory nor morally permissible to blow the whistle in this case.
- d) None of the above.

A is correct. Haugen fulfilled all 5 of De George's conditions for whistleblowing to be morally obligatory. (Actions that are morally obligatory are morally wrong not to do.) (1) She identified what she judged to be serious harm to the public caused by Facebook's products. (2) She reported her concern to her superiors at the company. When (3) her superiors took no remedial action, she (4) presented documented evidence to support her views and (5) she alerted governmental authorities that were in a position to make positive changes.

B is incorrect. Haugen didn't just fulfill the first 3 of De George's conditions that make whistleblowing morally permissible. She also fulfilled the 4th and 5th conditions, which make whistleblowing morally obligatory. (Morally permissible actions are not morally wrong to do. Morally obligatory actions are morally wrong not to do.)

C is incorrect. Haugen not only satisfied the first 3 of De George's conditions for whistleblowing to be morally permissible, but also the 4th and 5th conditions for whistleblowing to be morally obligatory. (Morally permissible actions are not morally wrong to do. Morally obligatory actions are morally wrong not to do.)

D is incorrect. Haugen satisfied all 5 of De George's conditions for whistleblowing to be morally obligatory. (Morally permissible actions are not morally wrong to do. Morally obligatory actions are morally wrong not to do.)

Module 6: IP and Rights Licensing

Intellectual Property (IP)

- Creations resulting from the exercise of the human brain
 - Examples include inventions, designs, ideas, plant hybrids, music, poems, paintings, photographs, logos, books, films, cartoon characters, trade secrets.
- Bundle of legal rights protecting such creations, i.e., intellectual property rights (IPRs)
- IP law recognises that creators have the right to protect their work.
 - IP law gives legal rights to IP creators, allowing them to control and exploit the use of their IP for a specific period of time.

Different Types of IP

- Copyright
 - Original and related works
 - Written, drawn, composed (books, movies, songs)
 - Reduced to or expressed in material form
- Patents
 - Inventions that present technical solution to a problem (cars, TV, mobile phones)
- Trademarks
 - Signs used in businesses to distinguish business products/services from competitors (logos)
- Confidential information
 - Non-public and valuable information (concepts, trade secrets, personal information/data)
- Others
 - Registered designs
 - Plant varieties
 - Geographical indications
 - Layout design of an integrated circuit

Why protect IP?

- Provides motivation for creators
 - As recognition, protection of intellectual output
- Encourages constant creation and innovation
- Allows creators to exploit their works for commercial gain
- Allows creators to defend their works from infringement (wrongful use of IP)

What is Copyright? ©

- Copyright is the right to prevent the unauthorised copying of the tangible form in which a person has chosen to express his ideas, for example in a:
 - Short story, musical composition, theatre script, painting, computer programme, photograph, movie, or video game
- It can be described as a bundle of exclusive rights belonging to the copyright owner.
 - Allows owners to enforce their rights against infringement
- Singapore's copyright law is governed by the Copyright Act
- Copyright protects the "form" of an idea and NOT the idea itself
- No need for novelty so long as there is independent creation.
- Artistic merit is not a requirement for copyright to attach to a work—too subjective
- Symbol act as a notice to let people know
 - who the owner is
 - when protection came into effect
 - ability to find out if the work is still in protection

written / graphic

Criteria for protection

Copyright protection arises automatically by operation of law, so long as certain basic criteria are satisfied:

- Falls within the categories of protection
- Fixed in tangible form (written/graphic form, capable of being perceived)
- Original
 - Work was created independently by the author
- Author/creator is a Singapore citizen or PR

How does Copyright protect?

- Form of expression, and not the idea or information itself.
- Idea or information is protected by different means.
- Many different media or forms of expression can be protected.
- Expression must, as a general rule, be original.
- No need for registration formalities (official stamps).
- Copyright arises "as soon as the ink dries".

Unprotected Matter

- Ideas and concepts
- Discoveries (a research finding)
- Procedures (steps in applying for a grant)
- Methods (solution to a problem)
- Any subject matter that has not been reduced to a tangible form
- Works in the public domain
 - Conceptual space where intellectual property has exhausted its protection duration reside
 - Use without the need to ask for permission
 - NOT the internet

Exclusive Rights in Copyright

Exclusive rights applicable to different types of subject matter:



Literary, dramatic or musical works

- Reproduce the work in a material form
- Publish the work if the work is unpublished
- Perform the work in public
- Communicate the work to the public
- Make an adaptation of the work
- Do any of the above in relation to an adaptation of the work



Sound Recordings

- Make a copy of the sound recording
- Enter into a commercial rental arrangement in respect of the recording
- Publish the sound recording if it is unpublished
- Make available to the public a sound recording by means of, or as part of, a digital audio transmission



Cinematograph films

- Make a copy of the film
- Cause the film, insofar as it consists of visual images, to be seen in public
- Communicate the film to the public

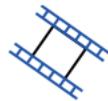


Artistic Works

- Reproduce in material form
- Publish the work if the work is unpublished
- Communicate to the public

Exclusive Rights in Copyright

Exclusive rights applicable to different types of subject matter:



TV and sound broadcasts

- Make a cinematograph film of TV broadcast or a copy of film
- Make a sound recording of TV/sound broadcast or a copy of recording
- Cause it to be seen/heard in public by paying audience
- Communicate the work to the public



Cable programmes

- Make a film of visual images, or a copy of such film
- Make a sound recording of the work or a copy of such sound recording
- Cause work to be seen or heard by paying audience
- Communicate to the public



Published editions

- Make a reproduction of the edition, including by way of a photographic process



Duration of Protection

Literary, dramatic, musical, and artistic works	Life of author plus 70 years from the end of the year in which the author died
Published editions	25 years from the end of the year in which the edition was first published
Sound recordings and films	70 years from the end of the year of release
Broadcasts and cable programmes	50 years from the end of the year of first broadcast
Performances	70 years from the end of the year of the performance

Overlapping Copyright

- One product may contain a variety of copyright works

MUSIC ALBUM
with SONGS

→ Lyrics

→ Musical work

→ Sound recording

- Each protected by a copyright with differing rights

- Purchasing a physical product does not give rights to underlying copyright work(s) (e.g., purchasing an original music CD does not give right to make copies)

Who owns the Copyright?

- Person who creates/authors the work automatically owns it from the moment of creation
- Except:
 - Employment: If the work is created by an employee pursuant to the terms of his employment, the employer owns the copyright in the work.
 - By agreement: The author can agree to transfer some or all of his rights.
- Joint authors:
 - Where work is created jointly by more than one author, the authors are all co-owners of the copyright in the work
 - Concept: Where more than one author creates inseparable or interdependent parts of a whole work E.g., two trainers involved in creating the training materials for a course
 - Requirement: contributions must be original material expression, not just ideas or noncopyrightable materials.

What is a Contract?

- Definition of a contract:
“An agreement giving rise to obligations which are enforced or recognised by law”
- It is a voluntary agreement between two or more parties.
- The law exists to govern and regulate the parties' relationship in such agreements.
- It can be verbal or written, simple or complicated.
 - Written contract
 - Done because humans tend to forget especially when it consists of many things to be done
 - To be clear of goals, obligations, deals, duration
 - Hard evidence of an agreement
 - What is expected from party in carrying out/performing obligation in terms of quality/standard of performance
 - By when these are to be performed
 - Can be time-consuming, troublesome, inefficient
- Every time we undertake a transaction, exchange something of real value for something in return – engage in formation of contract

Functions of Contracts

- Set out extent of agreement
- Identify and clarify rights and obligations
- Allocate risk (between parties)
 - Ensure that all foreseeable risk of goals not being met are considered. For instance, breaching of contract (party omits to fulfil a contract obligation), contract would have stated what needs to be done to repair the breach
- Provide certain guarantees
- Set performance standards
- Provide how non-fulfilment of obligations should be dealt with

What the Law of Contract Covers

- Formation of contracts
 - Elements required for a contract to exist
- Contents (terms) of a contract
- Performance of terms of the contract by its parties
- Remedies when there is non-fulfilment of either party's obligations (breach)

Elements of a Contract

- Offer
 - Indication by offeror of willingness to contract
- Acceptance
 - Absolute and unqualified—must be communicated to offeror by offeree
- Consideration
 - Usually indicated by price or the carrying out of an act in return for the benefit
- Intention to create legal relations
 - Reasonable to conclude from conduct of parties of their intention to be legally bound
- Capacity
 - Parties must have the capability to enter a contract
 - Issue of minors (below age of 18) and impaired mental capacity

Once all these elements are in place, a contract is deemed to be FORMED.

Absence of any one of these means that no contract is in existence.

Contractual Terms and Performance

- Set out and determine the rights and obligations of respective parties
- Provide for how obligations are to be performed
- Provide for how risks are to be allocated
- Provide for how the contractual relationship is to be regulated
 - How it begins, carries on, ends, or is renewed

Common Terms in Contracts

- Purpose of contract/description of collaboration
 - What is the aim of the contract?
- Payment/Fees
 - How much and how is payment to be made?
- Rights and obligations of each party
- Duration/Termination
 - How long is the contractual relationship going to last? How will the contract end?
- Warranties (fundamental promises)
 - Basic assurance that the contract can be carried out effectively
- Dispute resolution
 - How will disagreements be resolved?

Breach and Remedies

- Contract is breached when there is non-performance of a term.
- Does not automatically terminate contract!
- Breach entitles the wronged party to demand cure of the breach from the other party, as well as financial compensation (damages) if there is loss. (remedies)
 - May also be entitled to terminate contract

Using Contracts with IP

- You already have an understanding of the law of contract.
- You now have a general understanding of IP, and copyright.
- Contracts combined with IP enables you to transact/deal with IP usage.
- Words you need to be familiar with: Permission, release, licence, assignment, clearance

Dealing with IP

- The law regards intellectual property as a type of personal or movable property
- IP is capable of being owned and dealt with as other types of personal property.
- In other words, you can buy, sell, lease/hire out, or give away IP.
- It has commercial value.
- Two KEY methods that are used in dealing with IP:

Licence (noun)

- License (verb)
- A licence is a type of contract that gives permission to the holder/recipient to carry out a certain act, which would be infringing in nature otherwise.
- A licence gives the owner the ability to use or exploit intellectual property commercially, most commonly requiring a fee in return for the grant of the licence.

Types and Uses:

- Non-exclusive licence
 - Granted to more than one person
- Exclusive licence
 - Granted to one person only
- Where do you see licences being used?
 - All social media platforms
 - All SaaS platforms
 - All media aggregation platforms where works can be accessed for use

Assignment (noun)

- Assign (verb)
- An assignment is another type of contract
 - Legal meaning of "assign": To regard as belonging to
 - Must be in writing and signed by or on behalf of the assignor
- Means by which a person becomes an owner of property/property rights

Legal Effect

- Under the assignment, the assignor (person making the assignment) transfers all entitlement and ownership rights that are the subject of the assignment to the assignee (the person receiving these rights).
- The assignee is now the new owner of the property.

Licensing	Assignment
Grants someone else (other than the IP owner) the right to use the IP	Transfers the entire title and interest in someone's IP to another
Less costly	More costly
IP owner remains in control	IP owner gives up control
Use an IP already created by someone else for a specific reason	Wish to have complete control over something new created for you by someone

Note:

The way a licence is worded can make it almost as strong or effective as an assignment. Thus, it is important to understand the language used in licences and assignment agreements

LAMS questions

1. 1 Match each word in Column A with the correct type of IP protection in Column B.

Match each word in Column A with the correct type of IP protection in Column B.

*

Pick up the corresponding answers

- | | |
|---|--------------------------|
| <input checked="" type="checkbox"/> A made-up word for a brand name e.g. Lazada or Reebok | Trademark |
| <input checked="" type="checkbox"/> Software code | Copyright |
| <input checked="" type="checkbox"/> A new type of paper clip | Patent |
| <input checked="" type="checkbox"/> Formula for a popular soft drink | Confidential information |

Software code is protected by copyright as it is WRITTEN with computer language that has its own syntax.

A new type of paper clip can be protected by a patent as it may present a NEW way to better secure multiple sheets of paper together.

Formula for a popular soft drink can be protected as a trade secret, i.e., confidential information.

A made-up word for a brand name (for example LAZADA or REEBOK) can be protected as a trademark to be used in business.

1. 2 Time passes, and it is now 2050. Jean has a heart attack and dies on 15 March 2050. When does the copyright in her photograph expire?

Time passes, and it is now 2050. Jean has a heart attack and dies on 15 March 2050. When does the copyright in her photograph expire?

*

Choose one of the following answers.

- At the end of 2125
 When Jean dies
 It becomes part of the public domain upon Jean's death
 At the end of 2120

The copyright in Jean's photograph expires at the end of 2120, that is, 70 years after the year of Jean's death. That is when the photograph enters the public domain.

2. 1 What is the purpose of watermarking the image with the copyright notice?

What is the purpose of watermarking the image with the copyright notice?

*

Choose one of the following answers.

- Asserting copyright ownership of the image publicly
 A formality required for copyright to attach to the image
 A requirement for registration at the Intellectual Property Office of Singapore
 A requirement for the copyright to be valid under international copyright law

The purpose is only to assert copyright ownership of the image publicly. All other options do not exist. Remember that copyright automatically attaches to a protectable work as soon as the work is created, as provided by the Copyright Act.

3. 4 Assuming Denise was 25 when she took the photograph in 2021, and that she dies in the year 2060, how many years in total will the copyright in her photograph last?

Assuming Denise was 25 years old when she took the photograph in 2021, and that she dies in the year 2060, how many years in total will the copyright in her photograph last?

Choose one of the following answers.

- 39
 109
 75
 134

This is a matter of doing the math right! $(2060 - 2021) + 70 = 109$!

4. 3 Which of the following is true about Denise's photograph?

Which of the following is true about Denise's photograph? *

Choose one of the following answers.

- It has no originality.
- It is an infringement of Jean's photograph.
- It was made with a digital camera, and is therefore not fixed in a physical copy.
- It enjoys copyright protection as an independently created work.

It is an infringement of Jean's photograph.

This is false. Ideas cannot be protected by copyright.

It has no originality.

This is false. Originality just means that it is not copy of another work.

It was made with a digital camera, and is therefore not fixed in a physical copy.

This is false. Digital forms are protected as tangible expression as they are capable of being perceived.

1. 3 Which of the following statements is true about the law of contracts?

Which of the following statements is true about the law of contracts? *

Choose one of the following answers.

- Contracts can be made verbally as well as in writing.
- Contracts are valid only if a lawyer prepares them.
- All contracts must be approved by a government official to be valid.
- A person can be forced, against his/her will, to agree to a contract

All contracts must be approved by a government official to be valid.

This is false. Contracts are private agreements between parties, which do not require approval from government authorities. However, if you are contracting with a government authority, it may prescribe the FORM in which a contract is drafted.

A person can be forced, against his/her will, to agree to a contract

This is false. The law of contract provides that agreement to a contract is voluntary. If there is no voluntariness, a contract may be set aside/cancelled.

Contracts are valid only if a lawyer prepares them.

This is false. Lawyers are only involved if one or more of the parties wish for a lawyer to review the terms of the contract or its context for legal risk and clarity.

1. 4 What does the following statement from a social media platform Terms of Service mean?

What does the following statement from a social media platform Terms of Service mean? *

"...you grant us a non-exclusive, perpetual, sub-licensable, royalty-free, worldwide license to use any IP content that you post..."

Choose one of the following answers.

- The licensee is able to assign any content posted by the licensor.
- The licensee owns any content that is posted by the licensor on the platform.
- The licensee is the only entity that can extensively use the content.
- The licensor remains the owner but grants the platform a very extensive scope of use for the licensed content.

The licensee owns any content that is posted by the licensor on the platform.

This is incorrect. No language as to transfer of ownership of the content

The licensee is the only entity that can extensively use the content.

This is incorrect. This is a non-exclusive license which means the owner of the content can use the same content for other purposes and the platform cannot object.

The licensee is able to assign any content posted by the licensor.

This is incorrect. There is no language granting the platform the ability to assign posted content, i.e., give away the ownership of the content to someone else.

licensee: receiving IP

licensor: providing IP

Module 7a: Artificial Intelligence

AI Present Day Renaissance



Powerful computers:

Become widely available, such as **Cloud computing and GPU**



Big Data:

Availability of large amount of data due to **internet and smart mobile phones**

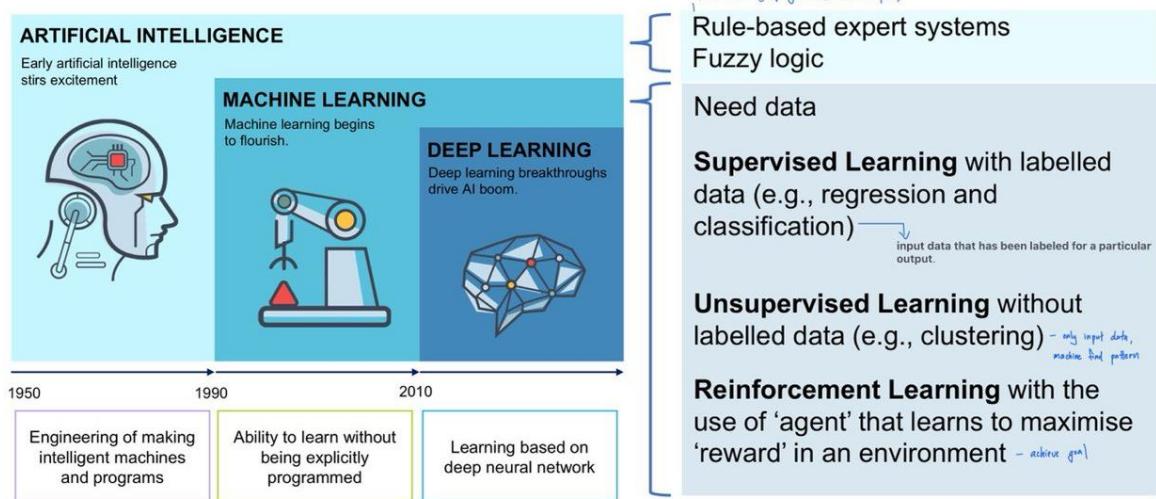


Software Algorithms:



Machine Learning, Deep Learning

AI Implementations



Deep Learning (most popular)

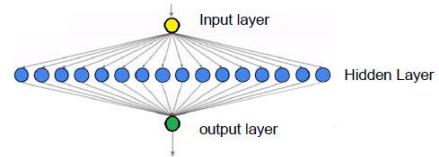
- Implementation of ML based on **Deep Neural Network** that mimics the human brains
- **Artificial Neural Network (ANN)**
 - Classifying numbers-based data
- **Convolution Neural Network (CNN)**
 - Classifying images
- **Recurrent Neural Network (RNN)**
 - Time series data (e.g., audio)
- **Deep Reinforcement Learning**
- **Transfer Learning**

Basis:

AlexNet

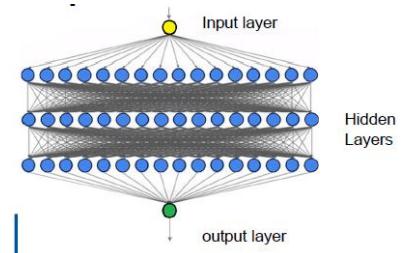
Neurons and Neural Network

- **Hidden layer**
 - Consists of learnable parameters (with large amount of data)
 - The 'algorithm' that can learn and improve by itself
- **Mimics the human brain to recognize pattern**
 - Ability to learn



Deep Neural Network for Deep learning

- **Deep Neural Network**
 - Multiple layers of hidden layers
 - Much more sophisticated algorithms can be learnt

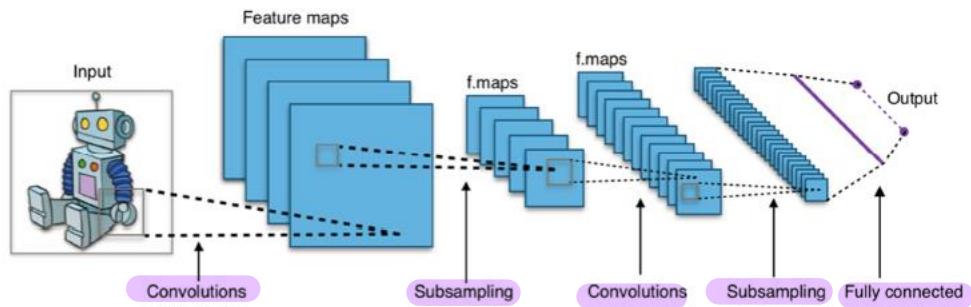


AlexNet

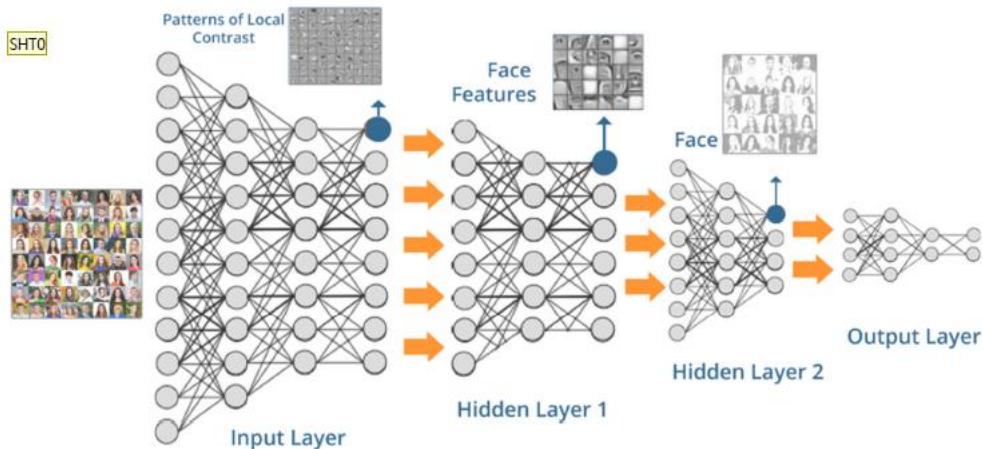
At the 2012 ImageNet computer image recognition competition:

- Alex Krizhevsky used machine to implement machine learning based deep learning algorithm (CNN).
- First time that machine learning based algorithm beat, by a huge margin, handcrafted software written by computer vision domain experts.

CNN for Image Recognition



Face Detection Training and Inference



©2021 Nanyang Technological University, Singapore. All Rights Reserved.

- Does not recognise a particular person but detect that there is a person in front of the camera (e.g., during online quiz)

AI Applications

- Robotics
- Autonomous Automotive and Navigation
 - Via sensors, images
 - Reduce human errors, running cost (predict when to do maintenance, prevent malfunction)
 - Improve convenience, safety
 - Navigation: optimal routes, avoid ERP
- Social Media
 - Recommender, advertisement

➤ Consumer Electronics

- Smartphone with AI-driven apps such as Siri, Google Assistant, Alexa, Cortana
- Smart household devices such as TV, refrigerators, ovens
- Smart Floor vacuum cleaners
- Smart security camera

➤ Business and E-Commerce

- Inventory management (reduce cost)
- Demand forecasting (improve efficiency)
- Personalised merchandising (preference, interest, browsing history)
- Chatbots
- Improve customer experience

➤ Banking and Finance

- Better business analytics (accuracy, high volume of data)
- Algorithm trading (execute trades at optimal prices)
- Credit risks assessment
- Wealth management (automated portfolio manager)
- Fraud

➤ Healthcare

- Analyse medical images
- Early detection (cancer)
- Develop new drugs
- Genomic profiling

➤ Farming and Precision Agriculture

- Nutrient and water management
- Detect pests and diseases in plants
- Detect weeds
- Analyse crop health (by drones)
- Improve harvest quality and accuracy

➤ Education

- Improve teaching and learning strategies
- AI e-tutors
- Automatic grading
- AI based e-proctoring

AI concerns

- Job loss
- Misuse of AI (Deepfake: spread false information, create tension)
- AI explainability
- AI bias (depends on type of data)
- AI ethics in decision making (weapon)

Summary

- AI is rapidly transforming the way we live:
 - Helps to makes things run more efficiently
 - Improves safety and work productivity
 - Frees up time for human to do more creative things
 - Enables better quality of life
- Current generation of AI technologies are still considered as Artificial Narrow Intelligence (ANI)
 - Goal is to eventually achieve Artificial General Intelligence (AGI)
- But there are also many concerns about the potential risk that we need to be aware of
 - Responsible AI

LAMS questions

1. 1 Which of the following is NOT the reason that leads to the renaissance of Artificial Intelligence in recent years

Which of the following is NOT the reason that leads to the renaissance of Artificial Intelligence in recent years? *

Choose one of the following answers.

- Interest in the concept of Artificial Intelligence
- Availability of large amount of data
- Access of high performance computing machines
- Advancement made in more sophisticated algorithms

The concept of AI is not new, there is always interest but not much progress was achieved mainly due to the lack of computing power and the other listed factors.

1. 2 Which of the following statement is NOT correct?

Which of the following statement is NOT correct? *

Choose one of the following answers.

- Deep learning belongs to the family of Machine Learning.
- Unsupervised learning does not need labelled data.
- Machine learning always needs labelled data for its training.
- Supervised learning makes use of labelled data.

Machine Learning can be of unsupervised learning that doesn't need labelled data.

1. 3 Which of the following is true about deep learning?

Which of the following is TRUE about deep learning? *

Choose one of the following answers.

- Deep learning is based on the concept of artificial neurons
- Deep learning consists of multiple hidden layers of neural networks
- Deep learning needs data to develop its algorithm
- All of the above

1. 4 Which one of the following will be most challenging to achieve with AI technology?

Which one of the following will be most challenging to achieve with AI technology? *

Choose one of the following answers.

- Writing a poem
- Predicting stock price
- Managing product inventory
- Monitoring engine condition

Writing a poem involves human emotions and feelings that is still hard to incorporate in AI at the moment.

The other listed options all have ready data that can be used for Machine Learning using training.

2. 4 Which of the following describe how social media platforms make use of AI for product marketing?

Which of the following describes how social media platforms make use of AI for product marketing? *

Choose one of the following answers.

- Monitoring the websites that you visit
- Monitoring the items that you search
- Monitoring your 'Likes'
- All of the above

1. 5 Which could be the reason for using the AI technologies such as Deepfake?

Which could be the reason for using the AI technologies such as Deepfake?

*

Choose one of the following answers.

- To influence stock price
- To influence elections result
- To undermine reputation of a product
- All of the above

Module 7b: Blockchain and its Application in Finance

Barter Economy:

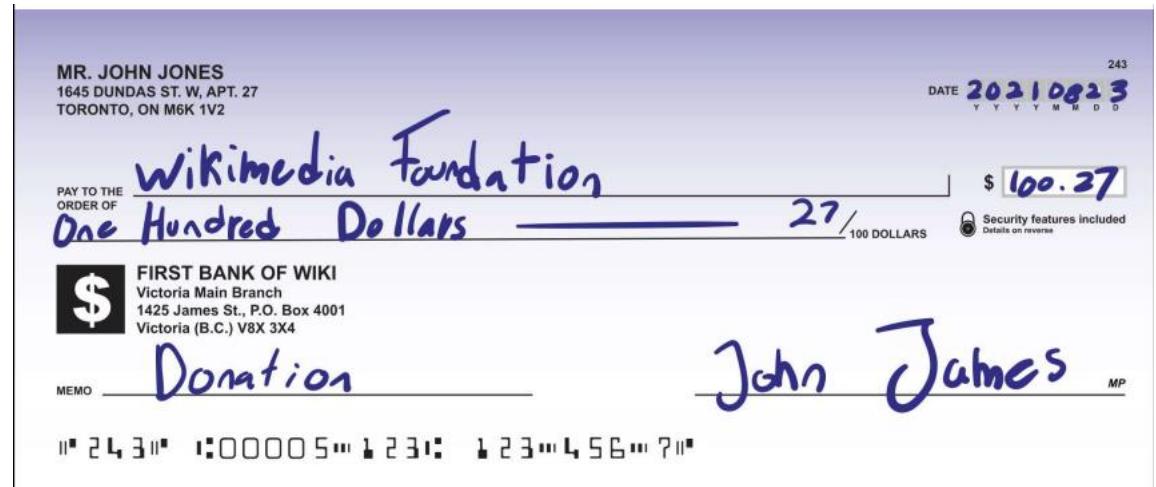
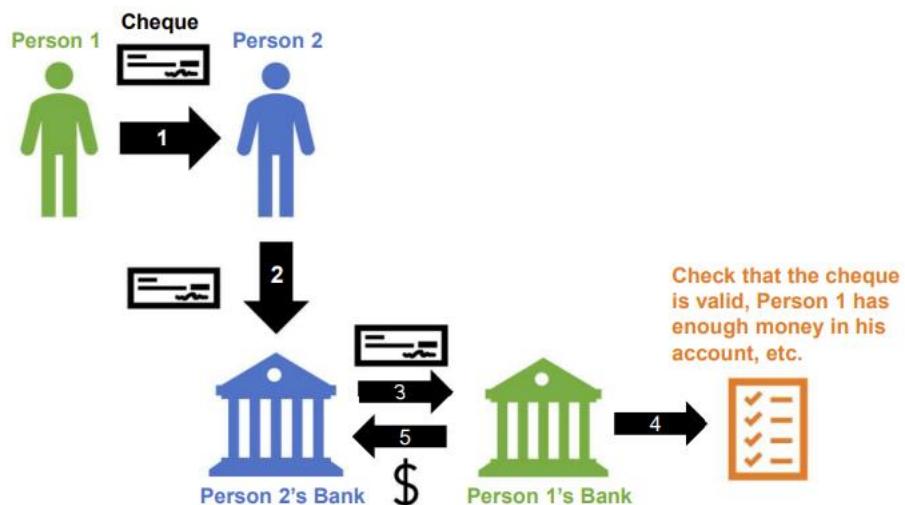
- to trade something you have for something you don't
- use commodities as a mode of payment (cocoa beans)
- disadvantage – depends on size, shelf-life

Money/Currency:

- according to mainstream economics, money (currency) relieves the issues arising from commodity trading as it is a universal store of value that can be readily used by anyone
- allows faster transactions as sellers have an easier time finding a buyer with whom they want to do business with
 - a seller can simply sell his or her goods and in turn pay their trading partners with the money earned
- much easier to bring currency around as compared to bringing bags of cocoa beans
- coins and papers last longer than most commodities used for trading
- can be accumulated and stored
- Egyptians invented minted currency
 - Use metal rings as money
 - Then made coins from precious metals such as gold, silver, or copper
 - Metallic coins are heavy to carry for daily transactions
- Paper money was invented
 - Individuals would deposit their coins with a trustworthy party and receive a note denoting how much coins they had deposited
 - The note could then be redeemed for currency at a later date.
- Central Bank – key concept of modern money
 - paper money is a country's official paper currency that is circulated and accepted for the transactions of goods and services
 - the country's central bank that authorises and regulates the printing of paper money, ensuring that the flow of funds aligns with the monetary policy
 - Paper money used to be backed by a certain amount of gold and later on government-issued currency is purely based on a country's government, so called fiat currency
 - The relationship between supply and demand of the fiat money, and the stability of the issuing government, defines the value of fiat money

- In 20th century, **cheque** becomes a very popular non-cash method for making payments.
 - A cheque is a document that **orders a bank to pay a specific amount of money** from a person's account to the person in whose name the cheque has been issued.
 - Can still issue even if the account has insufficient money!
 - The person **writing the cheque, known as the drawer**, has a **transaction banking account** where the money is held.

Say for example, person 1 issues a cheque to person2. When person2 drop cheque at the deposit box, person 2's bank will send the relevant information to person 1's bank. After person1's bank check that the cheque is valid and person 1 has enough money in his account, person1's bank will transfer the money to person2's bank account.



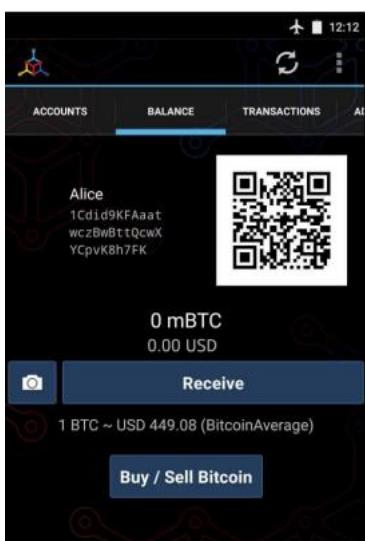
Advantages of cheque	Disadvantages of cheque
It is more convenient than carrying a large amount of cash around.	Cheques are not legal tender; creditors can refuse to accept them.
Cheques are safer than cash when carrying them around since a thief can't do much with your cheque book.	Cheques are valueless if drawer has not enough funds in their account.
They can be post-dated.	There is a lead time from posting to drawing a cheque.
They can be posted.	

- Credit Card

- card issuer creates a bank account for the cardholder, from which the cardholder can borrow money (with a limit) for payment to a merchant or as a cash advance
- contactless payment or mobile payment has become the main tool to transact in our everyday life
- generally do not carry cash, cheques or credit cards around nowadays. We simply use our mobile phone to make a payment

Bitcoin

- type of cryptocurrency
- an example of blockchain application
- Bitcoin price: (exchange rate between bitcoin and money)
 - Set by markets
 - has a floating exchange rate with fiat currency
 - value of bitcoin fluctuates according to supply and demand in the market
- Bitcoin wallet:



Important part:

- Bitcoin address (long string of letters and numbers)
- QR code (contains same info, scanned by camera)



Sending bitcoin, screen is presented with:

1. A destination bitcoin address
2. The amount to send, in bitcoin (BTC) or his local currency (USD).

Essentially, Alice's wallet breaks her funds into two payments: One to Bob and one back to herself. She can then use (spend) the change output in a subsequent transaction.

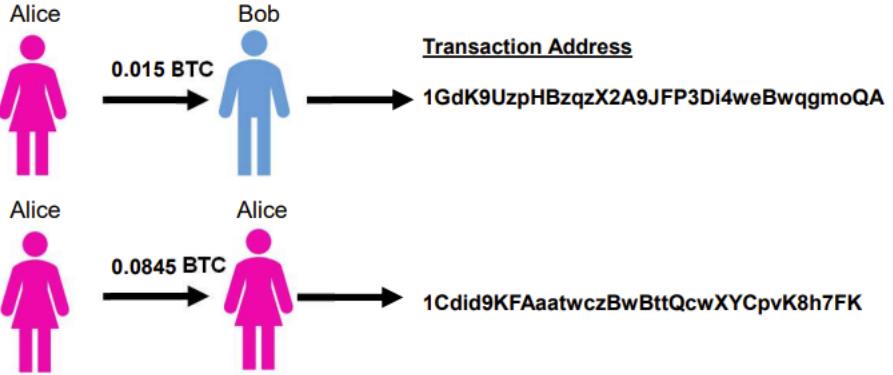
The diagram illustrates a transaction flow from Alice's wallet to Bob. Alice's initial balance is 0.0995 BTC. She sends 0.015 BTC to Bob. This leaves her with a change output of 0.0845 BTC, which is highlighted in green. The screenshot of the Blockchain.com Bitcoin Explorer shows the transaction summary with the same details: an amount of 0.0995 BTC, a fee of 0.00050000 BTC, and a hash of 0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbdb8a57... The transaction is dated 2013-12-28 07:11. The 'From' field shows the previous transaction's outputs: 0.1 BTC to 1CdId9KFAaatwczBwBttQcwXYCpvK8h7FK and 0.015 BTC to 1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA. The 'To' field shows the current transaction's outputs: 0.0845 BTC to 1CdId9KFAaatwczBwBttQcwXYCpvK8h7FK and 0.015 BTC to 1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA.

©2021 Nanyang Technological University, Singapore. All Rights Reserved.

She can then use (spend) the change output in a subsequent transaction. This is called the UTXO unspent transaction output. The transactions will be recorded on the bitcoin blockchain. The transaction ledger can be checked by anybody through various bitcoin explorer. The screenshot on the right is one example.

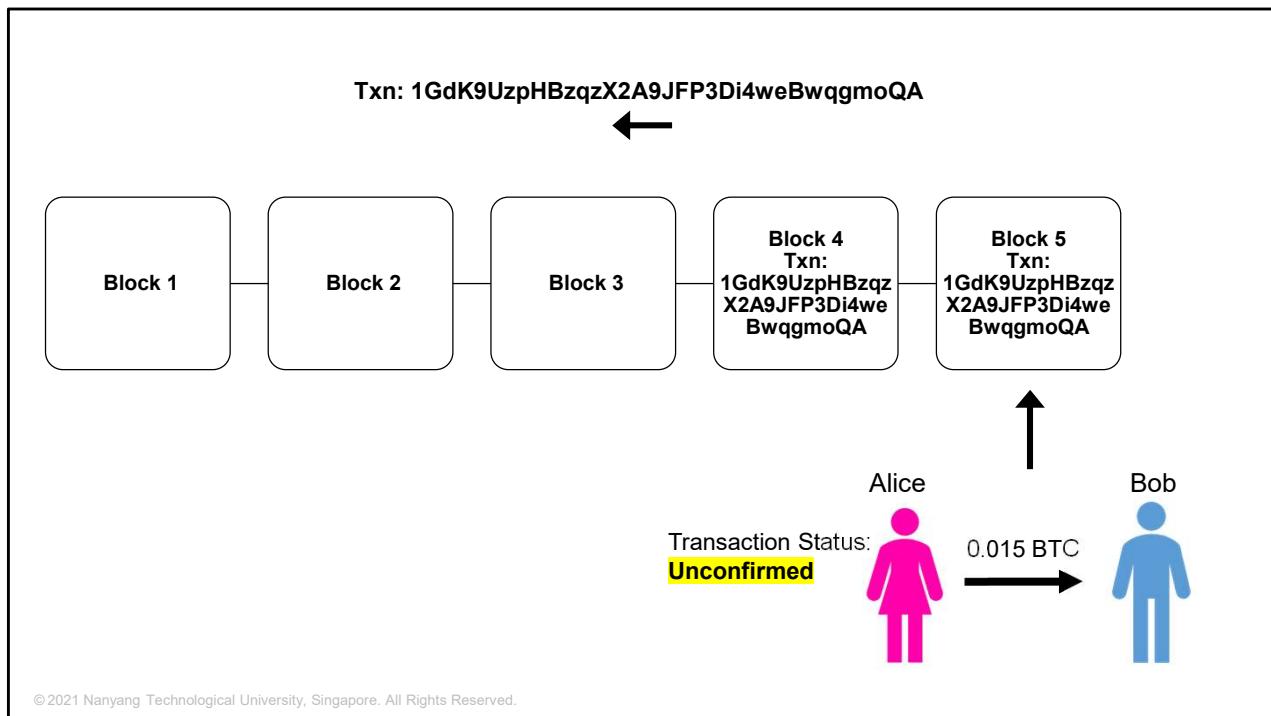
Alice's wallet application contains all the logic for selecting appropriate inputs and outputs to build a transaction to Alice's specification. At Bob's café, Alice only needs to specify destination and amount, and the rest happens in the wallet application without her seeing the details.

Alice's funds are in the form of a 0.10 BTC output, which is too much money for the 0.015 BTC cup of coffee. Alice will need 0.845 BTC in change. The difference of 0.0005 will be treated as transaction fee to reward the miner, who is the ledger keeper of the transactions.

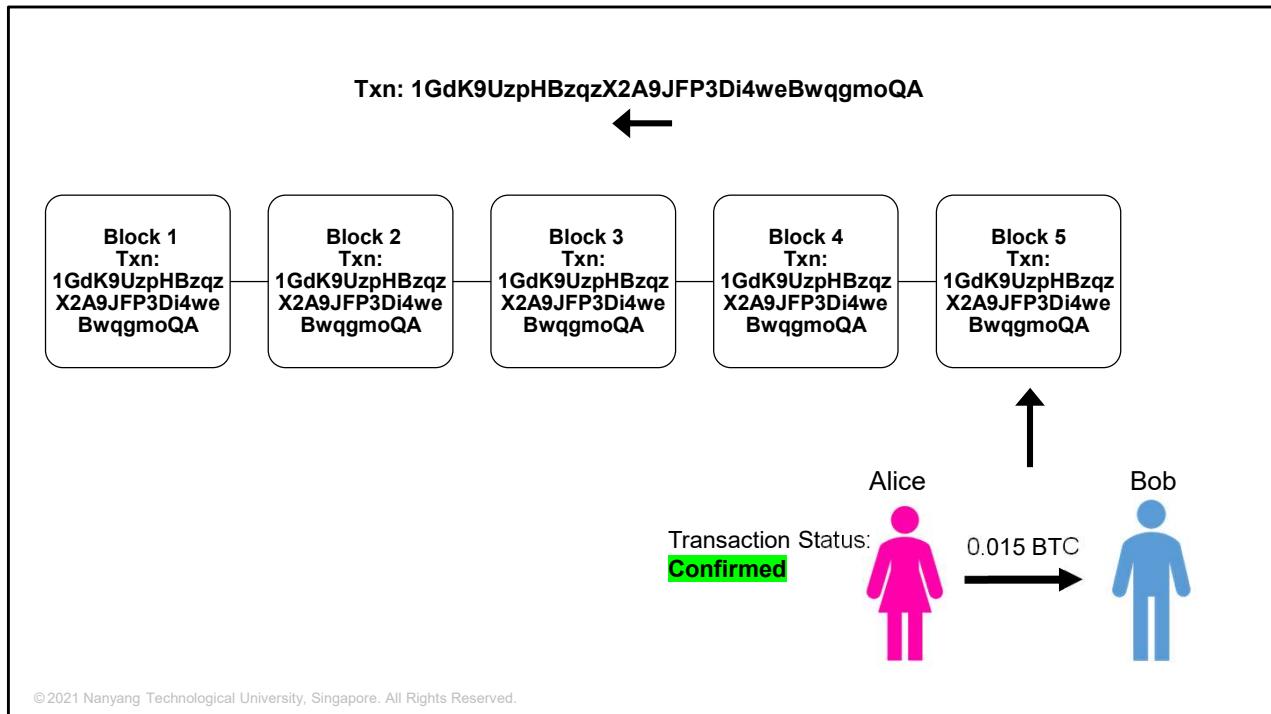


© 2021 Nanyang Technological University, Singapore. All Rights Reserved.

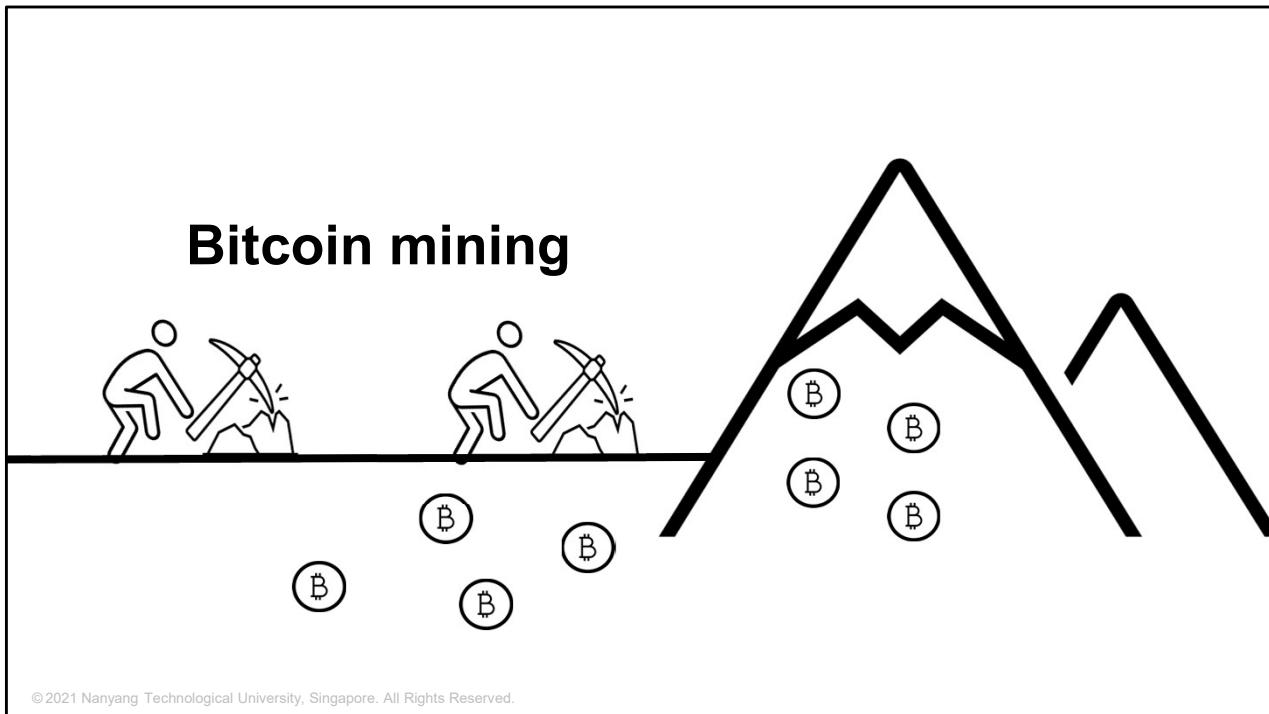
The transaction created by Alice's wallet application is **258 bytes** long and contains everything necessary to confirm ownership of the funds and assign new owners. Now, the **transaction must be transmitted to the bitcoin network where it will become part of the blockchain.**



When the transaction is in the process of propagating to the blockchain network, the transaction status remains unconfirmed. Now, there is a chance that Alice's bitcoin might be fake and be rejected by the network. Hence, Bob should not give her the coffee until the transaction is confirmed. This is similar to how a cheque works.



Once the transaction has been propagated to every block and accepted in the network, Alice's transaction is confirmed and Bob can give her the coffee. For small transactions such as this, usually Bob will simply give the coffee even before the transaction is confirmed. Besides, confirmation only takes a few seconds.



Besides buying bitcoin from someone, you can also **mine it**, like how miners did with gold and other precious metals. This is also known as the **bitcoin mining process**. This is similar to how Central Bank issues money in the modern world.

Block 277316

Hash	0000000000000001b6b9a13b095e96db41c4a928b97ef2d944a9b31b2c... ↗
Confirmations	442,705
Timestamp	2013-12-28 07:11
Height	277316
Miner	Unknown
Number of Transactions	419
Difficulty	1,180,923,195.26
Merkle root	c91c008c26e50763e9f548bb8b2fc323735f73577effbc55502c51eb4cc7cf2e
Version	0x2
Bits	419,668,748
Weight	874,516 WU
Size	218,629 bytes
Nonce	924,591,752
Transaction Volume	10296.98627606 BTC
Block Reward	25.00000000 BTC
Fee Reward	0.09094928 BTC

Here is the Nonce

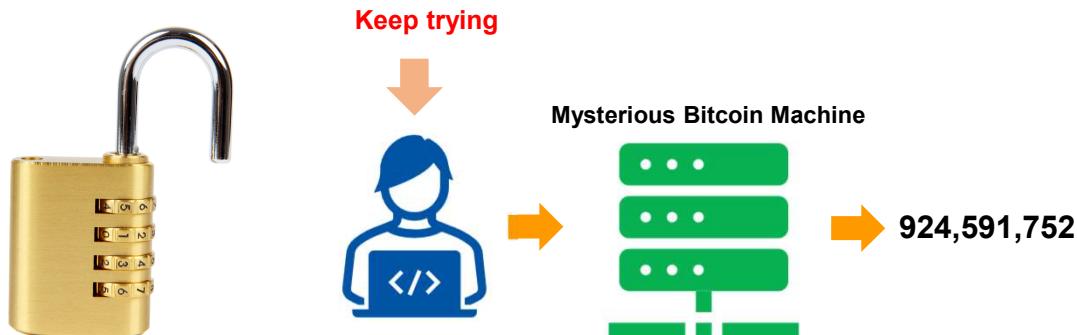


<https://www.blockchain.com/btc/block/277316>

Let's use Block 277316 as an example, which also contains Alice's transaction, for bitcoin mining.

The key to bitcoin mining is the "nonce" value. Nonce is an abbreviation for "number only used once", which is a unique random generated number. The nonce is the number that blockchain miners are solving for, in order to receive bitcoin reward.

Bitcoin Hash Puzzle



© 2021 Nanyang Technological University, Singapore. All Rights Reserved.

Imagine the mining process as a competition where all the miners compete to open the lock without knowing the password. How? It's not the same as solving a complicated math problem. What you can do is keep trying different combinations of these four digits. The search for a nonce is similar, it's done by sheer brute-force use of processing power. Just keep trying, to solve this so-called hash puzzle set by the network of bitcoin blockchain.

Given the above example, you must find the correct nonce **924,591,752** to get the reward for mining the block 277316.

You can consider this as you have a mysterious bitcoin mining machine, like the miner or ledger keeper who records all transactions between Alice and Bob, the machine will search for this nonce that can be combined with all transaction records and generate a hash value that meets the pre-determined requirement.

Block 277317

Blockchain.com		Wallet	Exchange	Explorer
BTC Testnet	Miner	Unknown		
BCH Testnet	Number of Transactions	643		
Blockchain.com	Difficulty	1,180,923,195.26		
	Merkle root	f83c14f9a014aa8bb790a		
Wallet	Version	0x2		
Exchange	Bits	419,668,748		
	Weight	1,127,412 WU		
	Size	281,853 bytes		
	Nonce	988,108,727		
	Transaction Volume	16513.41634394 BTC		
Block Reward		25.0000000 BTC	Block Reward	
Fee Reward		0.17178924 BTC	Fee Reward	

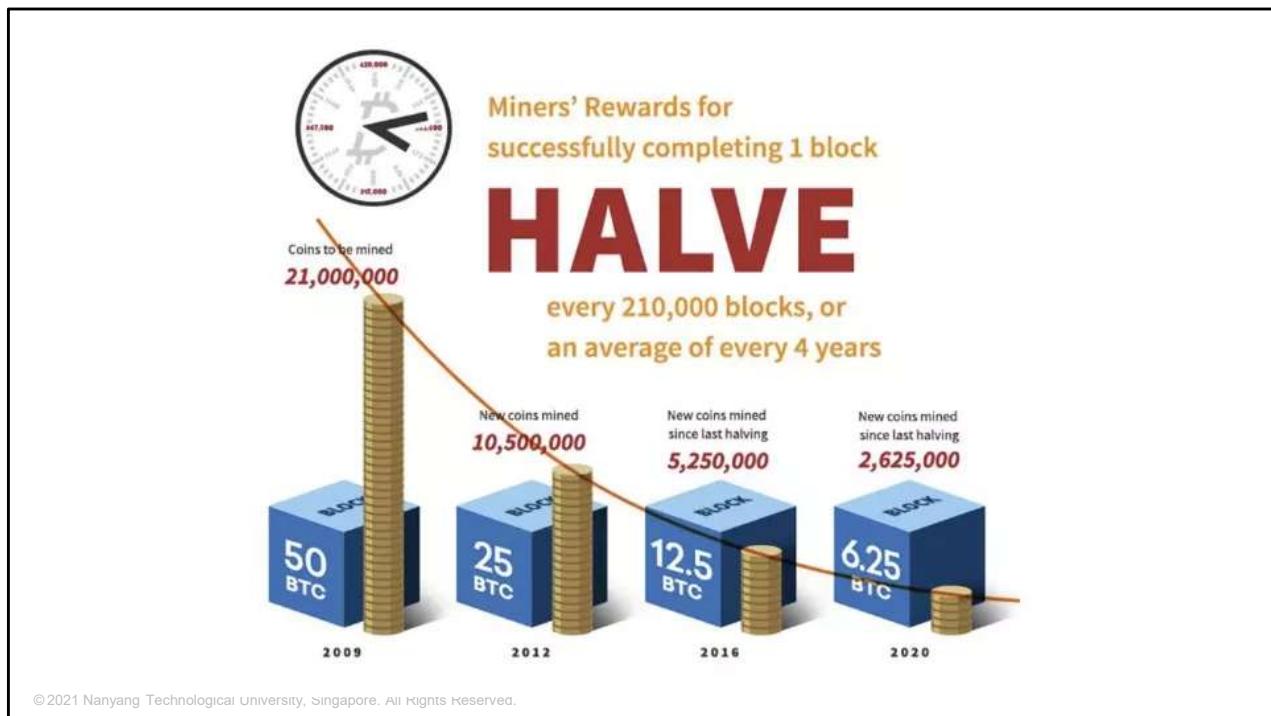
Block 720041

Blockchain.com		Wallet	Exchange	Explorer
BTC Testnet	Miner	Unknown		
BCH Testnet	Number of Transactions	229		
Blockchain.com	Difficulty	26,643,185,256,535.47		
	Merkle root	16e50d10f512ce24e14		
Wallet	Version	0x20400004		
Exchange	Bits	386,568,320		
	Weight	282,418 WU		
	Size	94,348 bytes		
	Nonce	3,531,430,925		
	Transaction Volume	204.48596421 BTC		
Block Reward		6.25000000 BTC	Block Reward	
Fee Reward		0.00445043 BTC	Fee Reward	

© 2021 Nanyang Technological University, Singapore. All Rights Reserved.

How much are the bitcoin rewards? Answer is, it depends.

You would be rewarded with 25 BTC (slightly over \$1,200,000 SGD) if you successfully mined Block 277317, but you would only get 6.25 BTC (slightly over \$300,000 SGD) if you successfully mined Block 720041 (the latest block in the chain as at 23 January 2022, 10:08pm Singapore time).



This is because miners' rewards for successfully completing 1 block halve every 210,000 blocks or an average of every 4 years. The supply of bitcoins is capped at 21 million, which is forecasted to be all mined by the year 2140.

The mining sounds like a good deal? Think of the electricity and telecommunication bills you have to pay for while mining the bitcoins. Also, think of the competition around the world. After all the effort and expenses, there is a chance that you might get nothing.

Original:

Sounds like a good deal? Think of the electricity and telecommunication bills you have to pay for while mining the bitcoins. Also, think of the competition around the world. There is a block generated every 10 minutes, and the supply of bitcoins is capped at 21 million, which is forecasted to be all mined by the year 2140.

After all the effort and expenses, there is a chance that you might get nothing.

Hash Function

- The mathematical algorithm that transforms any kind of message into a bit array of a fixed size (the "hash value"), regardless of the size of the input message. It is a one-way function and infeasible to invert.
- Example:
 - SHA256(Blockchain) = 625da44e4eaf58d61cf048d168aa6f5e492dea166d8bb54ec06c30de07db57e1
 - SHA256(blockchain) = ef7797e13d3a75526946a3bcf00daec9fc9c9c4d51ddc7cc5df888f74dd434d1

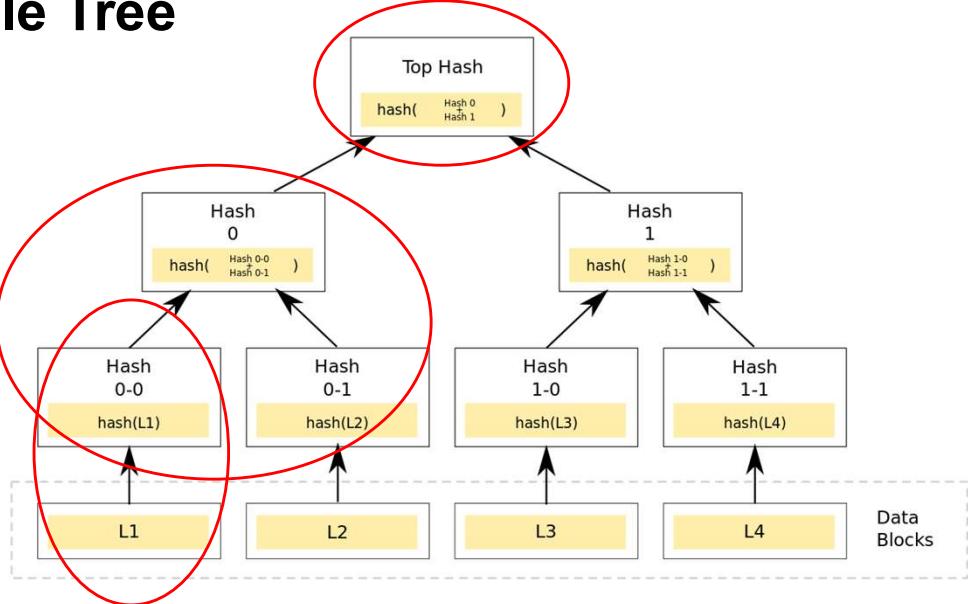
© 2021 Nanyang Technological University, Singapore. All Rights Reserved.

Now let's take a look at how blockchain structures and records data.

The first step is to hash the information. Hash is a mathematical algorithm that transforms any kind of message into a bit array of fixed size (that is, the "hash value"), regardless of the size of the input message. It is a one-way function and is infeasible to invert.

Take the hash function SHA256 for example. It generates a unique, fixed size 256-bit hash. A tiny change of the input information, say changing uppercase B to lowercase b in the word "Blockchain", leads to a completely different output. *different hash values*

Merkle Tree

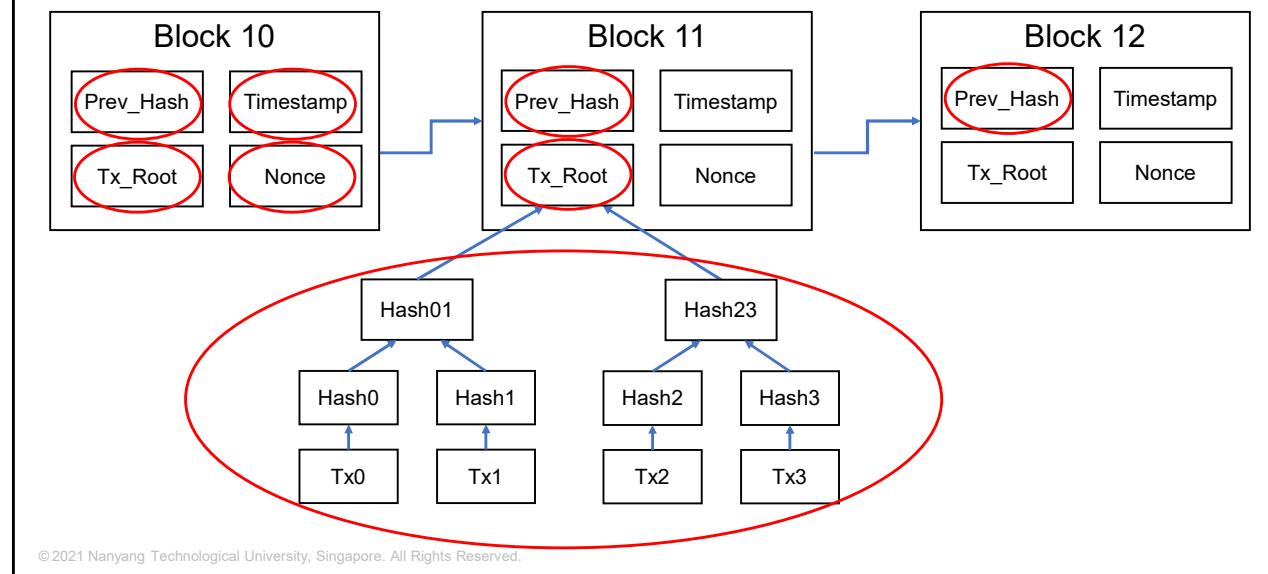


© 2021 Nanyang Technological University, Singapore. All Rights Reserved.

After converting individual transaction message into hash values, a pair of hash values can be hashed again. We keep doing so until we have one single hash value on the top. By doing so, we bundle up transactions in a tree-like manner, deriving a single hash value at the top, which is known as the Merkle tree root. Any small change in original information will lead to a completely different Merkle tree root.

As we can see, the Merkle tree is a data structure used for efficiently summarising and verifying the integrity of large sets of data. It is constructed by recursively hashing pairs of nodes until there is only one hash, the root.

Blockchain: Trust Machine



Now let's zoom in on the blockchain data structure.

A block first collects information together. These transactions are aggregated into the Merkle tree root. Each block stores the Merkle tree root for the transactions, as well as nonce, timestamp, and the hash value of the previous block, that is the hash value of the block information. Blocks are then linked using the hash value of the previous block.

In this way, any change in a single transaction will result in a change in the Merkle tree root. It will then change the hash value of that block and result in a change for all the following blocks. It is not possible to manipulate the earlier record without changing the following. This is how blockchain makes the data tamper proof.

Step 1: Hash the Five Highlighted Components

Block 277315

Hash	00000000000000002a7bb
Confirmations	442,733
Timestamp	2013-12-28 06:57
Height	277315
Miner	Unknown
Number of Transactions	40
Difficulty	1,180,923,195.26
Merkle root	5e049f4030e0ab2debb92

Block 277316

Hash	00000000000000001b6b9a13b095e96db41
Confirmations	442,705
Timestamp	2013-12-28 07:11
Height	277316
Miner	Unknown
Number of Transactions	419
Difficulty	1,180,923,195.26
Merkle root	c91c008c26e50763e9f548bb8b2fc323735
Version	0x2

© 2021 Nanyang Technological University, Singapore. All Rights Reserved.

Next, we'll look at the hash value of a block in BTC implementation, which is the identity of the block. Note that other implementations (such as ETC) might use other methods to achieve similar outcomes.

The block header is created with six fields:

1. Version number
2. Hash of the previous block
3. Timestamp
4. Difficulty
5. Merkle root computed in the previous step

Note:

A Merkle root is created by hashing together pairs of Transaction IDs, which gives you a short yet unique fingerprint for all the transactions in a block.

Height is simply the “serial number of the block” where first block is 1 and so on.

Difficulty is a measure of how hard it is to find a valid block to mine. For example, if a previous block is mined in less than 10 minutes, then the next block would be

targeted at more than 10 minutes to be mined by increasing the number of bits as a “password” and so on. BTC targets 1 block to be mined every 10 minutes.

Step 2: Hash the Current Block Header

Block 277315

Hash	00000000000000002a7bbc
Confirmations	442,733
Timestamp	2013-12-28 06:57
Height	277315
Miner	Unknown
Number of Transactions	40
Difficulty	1,180,923,195.26
Merkle root	5e049f4030e0ab2debb92:

Block 277316

Hash	00000000000000001b6b9a13b095e96db41
Confirmations	442,705
Timestamp	2013-12-28 07:11
Height	277316
Miner	Unknown
Number of Transactions	419
Difficulty	1,180,923,195.26
Merkle root	c91c008c26e50763e9f548bb8b2fc323735
Version	0x2

© 2021 Nanyang Technological University, Singapore. All Rights Reserved.

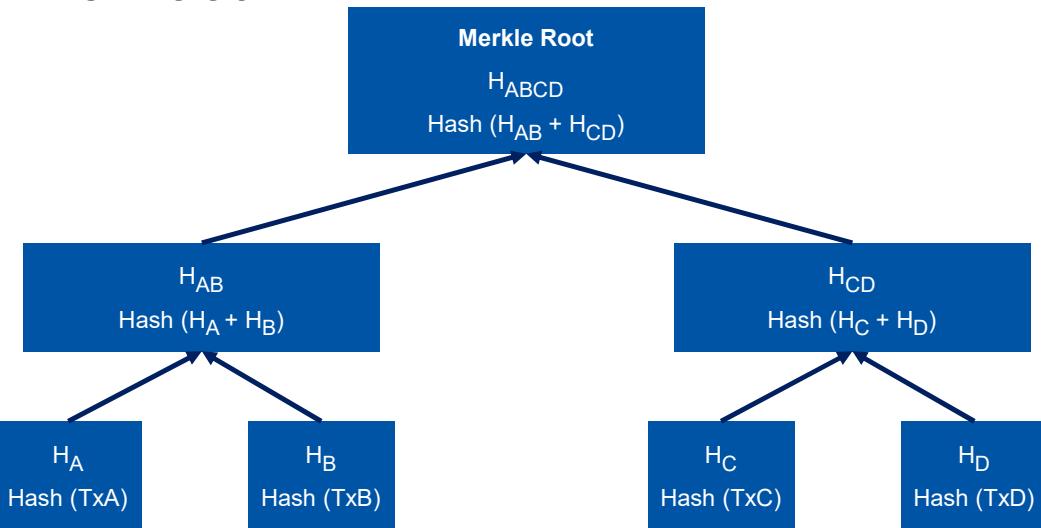
The **block header** (which contains the Merkle root) is **hashed**, resulting in the **block hash**.

Step 3: Hash Values in Steps 1 and 2

Hash a and b =

Hash	0000000000000001b6b9a13b095e96db4
Confirmations	442,705
Timestamp	2013-12-28 07:11
Height	277316
Miner	Unknown
Number of Transactions	419
Difficulty	1,180,923,195.26
Merkle root	c91c008c26e50763e9f548bb8b2fc323735
Version	0x2

Merkle Root



©2021 Nanyang Technological University, Singapore. All Rights Reserved.

Merkle Root

Each block in the bitcoin blockchain contains a summary of all the transactions in the block using a Merkle tree. A Merkle tree, also known as a binary hash tree, is a data structure used for efficiently summarising and verifying the integrity of large sets of data. Merkle trees are binary trees containing cryptographic hashes.

A Merkle tree is constructed by recursively hashing pairs of nodes until there is only one hash, called the root, or Merkle root.

Hash	0000000000000001b6b9a13b095e96db41c4a928b97ef2d944a9b31b2c... ↗
Confirmations	442,705
Timestamp	2013-12-28 07:11
Height	277316
Miner	Unknown
Number of Transactions	419
Difficulty	1,180,923,195.26
Merkle root	c91c008c26e50763e9f548bb8b2fc323735f73577effbc55502c51eb4cc7cf2e
Version	0x2
Bits	419,668,748
Weight	874,516 WU
Size	218,629 bytes
Nonce	924,591,752
Transaction Volume	10296.98627606 BTC
Block Reward	25.00000000 BTC
Fee Reward	0.09094928 BTC

©2021 Nanyang Technological University, Singapore. All Rights Reserved.

What Makes the Bitcoin Blockchain Safe?



After the discussion on the real-life use case, let's discuss several questions.

First, what makes the bitcoin blockchain safe?

Well, the cryptographic system makes transactions irreversible, which means once a block is created on the chain, it cannot be modified. You can, however, can add information to it. This restricts people from reversing any transaction that has already taken place.

What Makes the Bitcoin Blockchain Safe?



Second, the bitcoin blockchain is public which may make it seem unsafe—but in the case of bitcoin, it helps to make it safe. Despite the anonymity of the user, all transactions on the network are accessible to the public, making it difficult to hack or cheat the system.

Finally, the decentralization contribute to the security as well. The bitcoin network is distributed and has thousands of nodes all over the world that keep track of all transactions happening on the system. This ensures that in case something goes wrong on one server, there are others to back up. This makes it meaningless to hack any one server.



So, What's the Big Deal About Bitcoin?

So, what's the big deal about bitcoin? No, I don't mean the price. I mean how does that help the society?

If you want to trade bitcoin, the lowest unit you can trade is called Satoshi, which is the name of its founder, Satoshi Nakamoto. 1 unit of bitcoin is equivalent to 100 million Satoshi. Assume a bitcoin is worth 42,500 SGD now, a unit of Satoshi will be worth 0.000425SGD. 1SGD will give you about 2353 units of Satoshi.



So, What's the Big Deal About Bitcoin?

If you go and buy a coffee that costs 1SGD today, you can use cash, credit card or one of the most popular instant payment systems, PayNow. PayNow is easy to use, and you just need to have your phone and not have to worry about carrying your wallet around. Imagine paying for the cup of coffee with 2353 units of Satoshi using a PayNow equivalent system. As of the current moment, we don't have such a system. For convenience sake, let's imagine a term and call it SatoshiNow. So, you go and buy a cup of coffee using SatoshiNow. You might think, erm, why do I bother since I already have PayNow?

Why Should I Bother?



You are correct. You don't have to bother. But if you are travelling overseas for a holiday, for example, visiting Seoul and checking out its iconic observation tower, or Switzerland for its famous and beautiful Chapel Bridge, and you wanted to buy a cup of coffee. What do you do? You'd either have gone to a money changer to get the local currency with the risk of under or overspending before the trip; or you can solve that issue by paying with a credit card which usually has highly unfavourable exchange rate. Either way puts you at a losing end.

Now, imagine the whole world is accepting bitcoin and its equivalent subunits Satoshi and you have SatoshiNow app on your phone. You want to go for holiday tomorrow? You'll just need to book a ticket and pack your luggage.



Is It Just for the Finance Industry?

Is it just for the finance industry? There are definitely more possibilities. Imagine one day, someone creates a reliable Covid-19 test app that can securely identify you as the one being tested, and at the same time, link the result with it. After which, this information is propagated throughout the world using blockchain technology. You won't have to go to the doctor for a Covid positive or negative certification when you travel.



Is It Just for the Finance Industry?

Once the platform is available, you can simply walk into a mall and travel on a flight with the secure app. And if, what if, the implementation of this technology is you? Stay tuned for the more discussion on blockchain in other courses. We are expecting your big invention.

Here brings to the end of my presentation for this module. Hope you enjoyed and thank you.

LAMS Questions

1. The following statement(s) is/are true about the concept of money. Select all that apply.

Choose at least one answer.

- In minted currency, only coins made from gold and silver are considered as money
- One disadvantage of minted currency is they can be heavy to carry for daily transaction
- One disadvantage of barter trade is the shelf-life of goods
- Paper money was issued and decided by a country's government and never has it been backed by a certain amount of gold

Paper money was once backed by gold. Actual coins can also be made from other precious metal such as copper.

1. The following statement(s) is/are true about the concept of cheques and credit cards Select all that apply.

Choose at least one answer.

- Supposed a cardholder has both a deposit and credit card account with DBS. On a certain day, the deposit account has a balance of \$1,000. The cardholder went to Sim Lim square and fell in love with a Razor laptop that costs \$3,000. He/she cannot buy the laptop with the credit card because the deposit account has less than \$3,000.
- A cheque has the drawer's (owner of the cheque) name on it
 - A credit card is issued by a bank to the cardholder
 - The drawer (owner of the cheque) cannot issue a cheque to another person if the drawer doesn't have sufficient money in the bank that corresponds to the amount specified in the cheque

The owner can issue a cheque despite not having enough money in the bank to back it up.
Also, credit cards allow holder to "borrow" money from issuing bank, potentially exceeding the limit of deposit account balance. Moreover, deposit accounts and credit card accounts are two different accounts even if they issued by the same bank

1. The following statement(s) is/are true about the concept of Bitcoin wallet Select one correct answer.

Choose one of the following answers.

- Alice can receive bitcoins from the hash value of the email address that she uses to create the wallet
- Alice can receive bitcoins from either from the long string of letters and numbers or from the QR code
- Alice can only receive bitcoins from the QR code which represents the wallet address
- Alice can only receive bitcoin from her wallet address, which comprises of long string of letters and numbers

1. The value of mining one successful block is _____. Select one correct answer.

Choose one of the following answers.

- Depends
- 6.25 BTC
- 25 BTC
- 50 BTC

1. The following statement(s) is/are true about hash function. Select all that apply.

Choose at least one answer.

It is one way and cannot be reverted

It is 256 bits in length

It is based on a mathematical formula

It has a fixed value

The value is not fixed and is based on input.

Only SHA256 is 256 in length, there are other hash functions that are different in length.