CC0002 Notes Summary (without additional readings)

Navigating world (Nanyang Technological University)

Module 1: Computational Thinking

Computational Thinking Competencies

Computational: Involving the calculation of answers, amounts, results (e.g., calculations, order)

Thinking: The activity of using your mind to consider something (e.g., reasoning, questioning)

Competencies: Important skills that are needed to do a job (e.g., managerial competencies)

Includes:

1. **Abstraction**
   - Identifying and utilizing the structure of concepts / main ideas
   - Simplifies things
     - Identifies what is important without worrying too much about the detail
   - Allows us to manage the complexity of the context or content
   - Biological Domain
     - Bioinformatics:
       Combines different fields of study, including computer sciences, molecular biology, biotechnology, statistics, and engineering
       Analyse large amount of data: Genomics, Proteomics
   - Computer Science Manifestations
     - Pseudocode:
       An informal description of the steps involved in executing a computer program, often written in something similar to plain [in designed language]
   - Human Genomes
     - Structure of cell: Incredibly crowded and incomprehensible for humans
     - Simplify the representation of cells and make it readable by abstraction (labelling, lettering, shaping, colouring, numbering, etc.)
     - Formulating in pseudo level can enable us to understand concepts more clearly.
     - Abstraction simplifies complex life phenomenon to something readable and understandable.

2. **Algorithms**
   - is about following, identifying, using, and creating an ordered set of instructions
   - ordering things
     - ascending order (e.g., from 1 to 5, or from A B C to X Y Z)
     - descending order (e.g., from 5 to 1, or from Z Y X to C B A)
   - Allows us to order the complexity of the context or content
   - Biological Domain

    - Transcription, Translation
    - Prediction (Gene Function, Protein Function)
- Computer Science Manifestations
    - IF ELSE
    - Algorithm efficiency

3. **Decomposition**
- Breaking down data, processes, or problems into smaller and more manageable components to solve a problem
- Each subproblem can then be examined or solved individually, as they are simpler to work with
- Natural way to solve problems
- Also known as divide-and-conquer to synthesize the final solution
- Solve complex problems
    - If a complex problem is not decomposed, it is much harder to solve at once. Subproblems are usually easy to tackle
- Each subproblem can be solved by different parties of analysis
- Decomposition forces you to analyse your problem from different aspects
- Biological Domain
    - Biological decomposers (Fungi, Bacteria)
- Computer Science Manifestations
    - Functions
    - Factorials

4. **Pattern Recognition**
- is about observing patterns, trends and regularities in data
- A pattern is a discernible regularity
    - The elements of a pattern repeat in a predictable manner
- In computational thinking, a pattern is the spotted similarities and common differences between problems
- It involves finding the similarities or patterns among small, decomposed problems, which can help us solve complex problems more efficiently
- Patterns make problems simpler and easy to solve
- Problems are easier to solve when they share patterns, we can use the same problem-solving solution wherever the pattern exists
- The more patterns we can find, the easier and quicker our problem solving will be
- Biological Domain
    - Gene finding
    - Biomarkers
    - Protein synthesis
- Computer Science Manifestations
    - Machine learning
    - Artificial intelligence
    - Probability and statistics

Module 2: Quantitative Reasoning

Quantitative Reasoning

Steps to obtain the desired insights

- How to **frame** concrete numerical questions?
- How to **identify** tools and data for analysis?
- How to **build** models to analyse the data?
- How to **analyse** the results you obtain?

Mean

- The "average" behaviour of the data points, and is computed as "average" as well
- Single point statistic from entire data distribution

Standard deviation

- The average deviation of a data point from the Mean of the distribution
- Higher SD, wider distribution

Correlation

- $-1 \leq 0 \leq 1$
- Margin of error is narrower/stronger correlation when CORR closer to -1 or 1
- The higher the correlation, the lower the standard error.

Module 3: Cybersecurity

Phishing

- Check who the sender of the email is
- Be cautious before clicking on any hyperlinks (Type the correct address yourself to ensure you are viewing the actual website)
- Look out for the lock icon in the address bar to ensure the website starts with https
- Report suspicious email to ServiceNow@NTU
- Delete the email
- Do not forward the email to anyone
- CIA
  - ○ **C**: Confidentiality
    Protect personal information and share only what is necessary
  - ○ **I**: Integrity
    Practice cyber hygiene and beware of fake sources of information
  - ○ **A**: Availability
    Prevent getting locked out of devices, your actions can affect others

Strong Passwords

- At least 8 characters long
- Contains number
- Contains symbols
- Contains upper case letters
- Contains lower case letters
- Use uncommon and nonstandard words or create a password from a sentence that makes sense to you
- Do not use personal information that people who know you can guess as your password
- Use different passwords for different accounts
- Change passwords regularly
- Use Two Factor Authentication or Multi Factor Authentication (MFA)
  - ○ By enrolling your mobile number or email address to receive a one-time password, or through an authentication app

Data Security

- Data can exist in both physical and digital forms
- Data can belong to an individual or an organization
- Levels of Data Security
  1. **Open:**
     Data distributed to the public or published on the internet
  2. **Restrict:**

Data made accessible to members to the community and not to the public (project reports, presentation files)

3. **Confidential:**
   Contractually defined as confidential or by nature confidential (personal identifiable information, audit reports)
   If data is disclosed, target can face statutory penalties,cause damage to the organization
4. **Classified:**
   Data covered under the Official Secrets Act
   Unauthorised disclosure leads to damage to national security

- Lock workstations when leaving desk
- Adopt clean desk policy and keep desk clear
- Send and store work information through organizational accounts
- Keep data storage devices securely
- Secure sensitive digital information through encryption

Acceptable IT Usage

- Use trusted Wi-Fi networks
- Avoid doing sensitive transactions
- Use BCC instead of CC when sending mass emails to keep the identities confidential, especially when a third party is incolved
- Be mindful when connecting external devices to computer as it may contain viruses and malware
- Install antivirus software and always ensure it is up to date

Cybersecurity in NTU

Objectives:

- Confidentiality: Ensuring Data and Information cannot be read by unauthorised personnel
- Integrity: Data and Information held by NTU remains accurate and unmodified by unauthorised personnel
- Availability: Data and Information remains usable with sufficient capability to deliver educational services

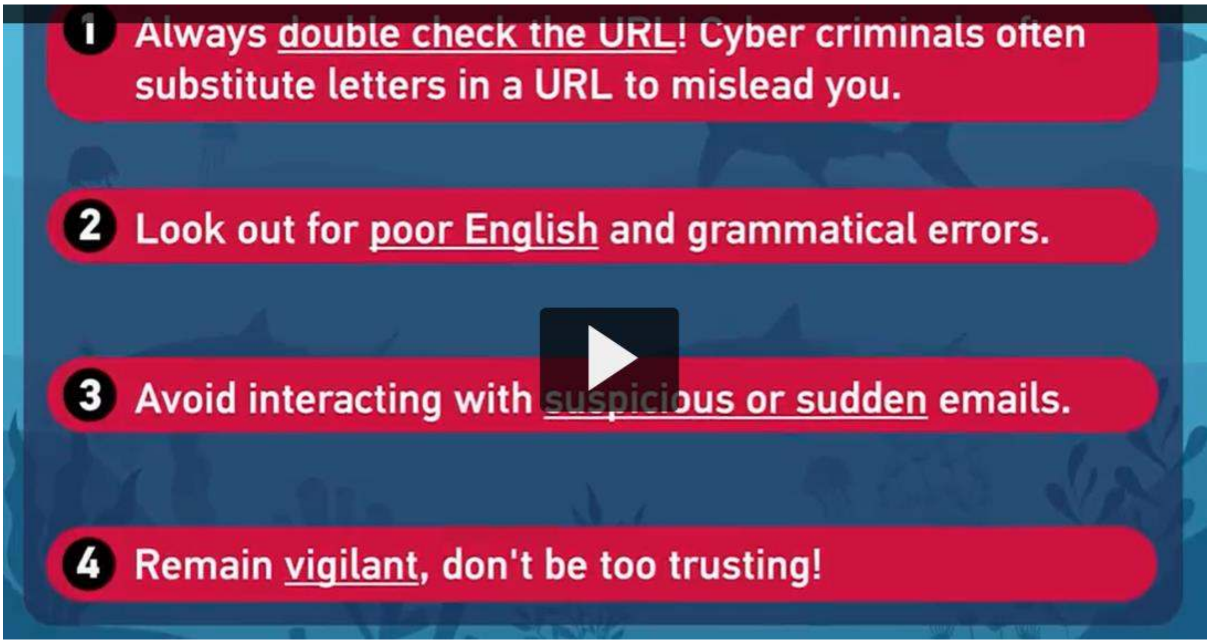
Functions:

- The Cyber Security Governance: Responsible for development and maintenance of NTU Cyber security policies, standards and procedures
- The Cyber Security Engineering: Responsible to explore different technologies to enhance NTU security capabilities
- The Cyber Security Defence Team: Manage university Security Operations Centre (SOC). Operates 24/7 365 Days to detect and responds to any cyber-attacks against NTU

Acceptable IT Usage Policy (AIUP):

- serves to protect information and IT resources
- reduce the risks and damages to the university by governing the usage of all its IT resources (computer, email account, mobile devices, IT services)
- Dos
  - Update your passwords regularly
  - Always ensure that you keep your password safe
  - Use the NTU email for all official communications
  - Use Blind Carbon Copy (BCC) for mass emails
  - Keep your software updated with security patches
- DONTs
  - Don't share your password with anyone
  - Don't forward any University document to your personal email address or online storage that's not approved by the University
  - Don't install software without appropriate licenses
  - Don't turn off your anti-virus software or cancel any software updates
  - Don't over share information in social media
- Good habits
  - Spot the signs of phishing emails
  - Use strong passwords
  - Enable MFA
  - Secure your sensitive digital information through encryption
  - Follow the AIUP and conform to the security bets practices

In General
P: Passwords
A: Anti-Virus
S: Software Application
S: Spot signs of phishing



1 Always double check the URL! Cyber criminals often substitute letters in a URL to mislead you.

2 Look out for poor English and grammatical errors.

3 Avoid interacting with suspicious or sudden emails.

4 Remain vigilant, don't be too trusting!

Module 4 – Fake News

Falsehoods: A statement is false or misleading

Misinformation: The inadvertent dissemination of false information

Disinformation: The intentional dissemination of false information

Fake News:

A type of falsehood intentionally packaged to look like news to deceive others (intention, format, facticity)

Motives:

- Financial
  - Attracting clicks
  - Advertising Revenues
- Ideological
  - Personal Agenda
  - Weapons of Mass Misinformation
- Political satire
- News parody
- Propaganda
- Advertising
- Manipulation
- Fabrication

What makes people vulnerable?

- Sender
  - Credible or familiar?
  - Trustworthy or similar?
  - Proximate or distal?
- Message
  - Format
  - Plausibility
- Channel
  - Trusted or depended on?
  - Closed or open?
  - Feedback
- Receiver
  - Confirmation bias
  - Motivations
  - Corrections
- Context
  - Information overload

    - Instability

Different Sources

- Original Source
- Immediate Source
- Invisible Source
- Trusted Source
- Disregarded Source

Message characteristics

- Plausible?
- Mentions Experts?
- Conversation Tone
- Stirs Emotions
- Asks for call to actions (Forwarding the message)?
- Channels where information flows
    - Popularity cues
    - Reliance
    - Lack of gatekeeping
    - Information overload
- Higher social media news use= Higher likelihood to believe in fake news
- Avoiding news = more likely to believe in misinformation
- Confirmation Bias: Information that aligns with our existing beliefs

Informational apathy (Why people ignore telling people they are wrong about news?)

- Issue Relevance: Does not concern me
- Interpersonal Relationships: Do not want to offend family/friends
- Personal Efficacy: There is no point in reasoning as people already believe

Consequences of fake news

- Short Term
    - Political Decisions
    - Business
    - Peace and Order
    - Reputation
- Long term
    - Devaluations of Information
    - Erosion of trust in institutions
    - Larger social divisions
    - Chilling Effect

What can we do?

1. **Individuals Authentication**

- Internal Acts of Authentication

- The Self: We are old enough to judge and think (experience)
- The Source: Is the source reliable
- The Message: Check the tone and see if its polemical or deliberately misleading to arouse emotions
- The Message Cues: If there are more likes , shares , comments

- External Acts of Authentication
  - Incidental & Interpersonal: By chance discussing with family or friends
  - Incidental & Institutional: Waiting for the follow-up news to confirm it
  - Intentional & Interpersonal: Asking a reliable group to verify
  - Intentional & Institutional: Googling the information to check
- Social process

  Motivations for authenticating
  - Self-image (show that you don't have questionable beliefs)
  - Group cohesion

  Strategies of authentication
  - Group beliefs; "deep stories"
  - Source affiliation ▪ Sharing as authenticating

  Consequences of authentication
  - Institutionalisation of Interdependence
  - Ritualisation of collective authentication

2. **Governments Authentication**
   - POFMA:

     An Act to prevent the electronic communication in Singapore of false statement of fact, to suppress support for and counteract the effects of such communication, to safeguard against the use of online accounts for such communication and for information manipulation, to enable measures to be taken to enhance transparency of online political advertisements, and for related matters.
3. **Tech companies Authentication**
   - Intervention (pressure by the public)
     - Supporting third party fact checkers and journalists
     - Promoting media literacy among users
     - Reducing financial incentives for content producers
     - Implementing new features to flag content
     - Deleting post and removing accounts
4. **Journalists and fact-checkers**
   - Fact checking
     - Verification: The process of evaluating the story before it becomes news
     - Fact Checking: The process that occurs post publications
   - **Types of Fact Checkers**
     - Affiliated with news organisation
     - Government Owned
     - Independent Organization
     - Volunteer Groups

  - Individual
- **Fact Checking Tools**
  - Monitor What's Trending
  - Verify Images
  - Verify Sites
  - Check the Weather
- **Fact Check Message**
  - Videos
  - Rating Scales – demonstrate T or F
  - Mixed Accuracy Statements
  - Truth Sandwich (Correction is presented first followed by debunking the falsehood and then reiterating the correction after) Truth → lie → Truth

What can we do?

1. Reflect on our own information behaviour.

2. Engage, rather than ignore.

3. Strive to understand others.

4. Use and support reliable and legitimate information sources.

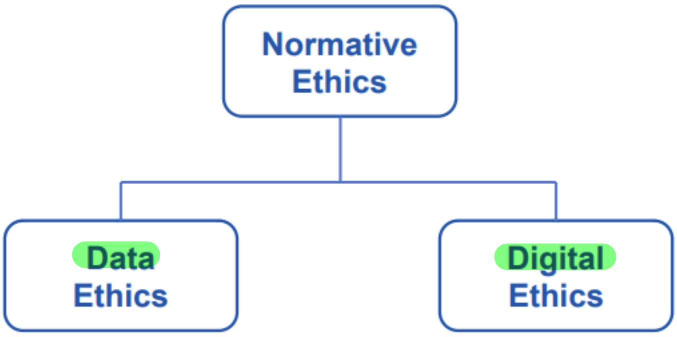
5. Maximise available resources.

6. Equip ourselves.

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

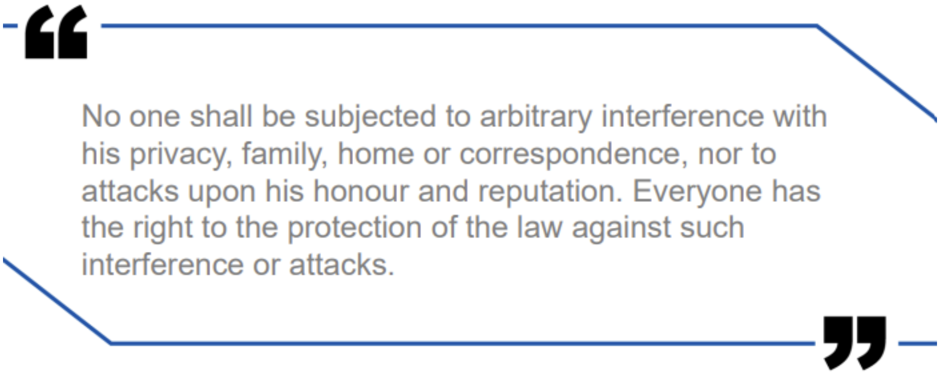
- Cyberbullying is the use of the internet or digital devices to inflict psychological harm on a person or group (Quinn, 2019; Media Literacy Council 2018).
- Examples:
  - Repeatedly texting or emailing hurtful messages to another person.
  - Spreading derogatory lies about another person.
  - Tricking 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 (Cosi) 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 be 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.

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? ©

written / graphic

- 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

Criteria for protection

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

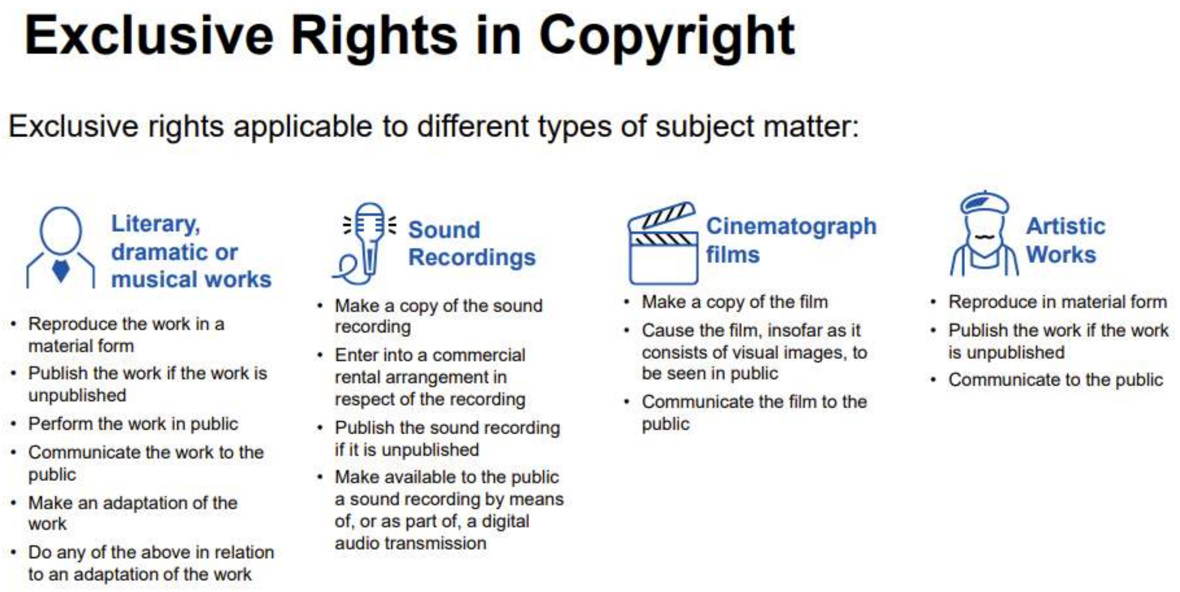
- Falls within the categories of protection
- Fixed in tangible form (written/graphic form, capable of being perceived)
- Original
  - Work was created independently by the author
- Author/creator is a Singapore citizen or PR

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

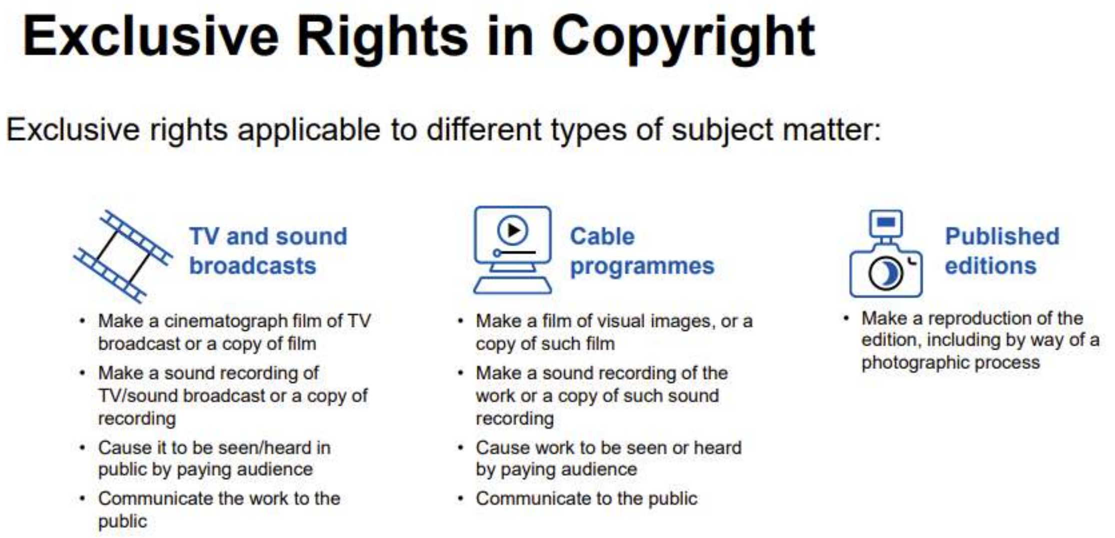
- Make a copy of the sound recording
- Enter into a commercial rental arrangement in respect of the recording
- Publish the sound recording if it is unpublished
- Make available to the public a sound recording by means of, or as part of, a digital audio transmission

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

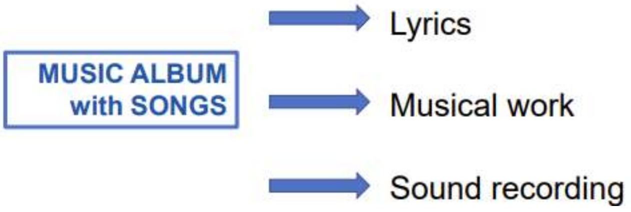
- Make a reproduction of the edition, including by way of a photographic process

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



- 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

Module 7a: Artificial Intelligence

AI Present Day Renaissance

Powerful computers:

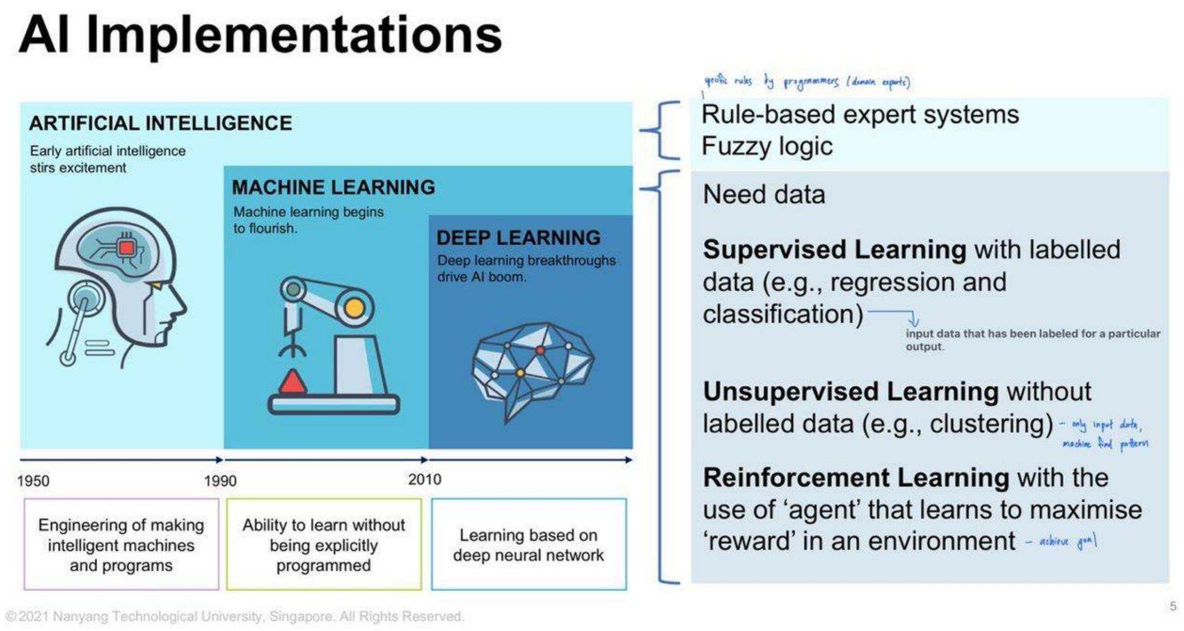
Become widely available, such as Cloud computing and GPU

Big Data:

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

Software Algorithms:

Machine Learning, Deep Learning



AI Implementations

ARTIFICIAL INTELLIGENCE

Early artificial intelligence stirs excitement

MACHINE LEARNING

Machine learning begins to flourish.

DEEP LEARNING

Deep learning breakthroughs drive AI boom.

1950 1990 2010

Engineering of making intelligent machines and programs

Ability to learn without being explicitly programmed

Learning based on deep neural network

specific rules by programmers (domain experts)

Rule-based expert systems

Fuzzy logic

Need data

Supervised Learning with labelled data (e.g., regression and classification)

input data that has been labeled for a particular output.

Unsupervised Learning without labelled data (e.g., clustering) - only input data, machine find pattern

Reinforcement Learning with the use of 'agent' that learns to maximise 'reward' in an environment - achieve goal

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

5

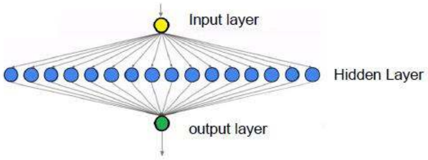
Deep Learning (most popular)

- 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**

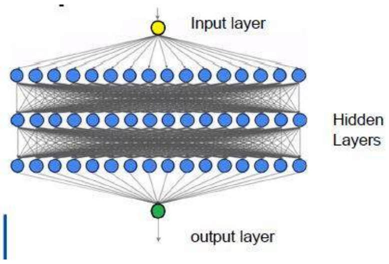
Basis:

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

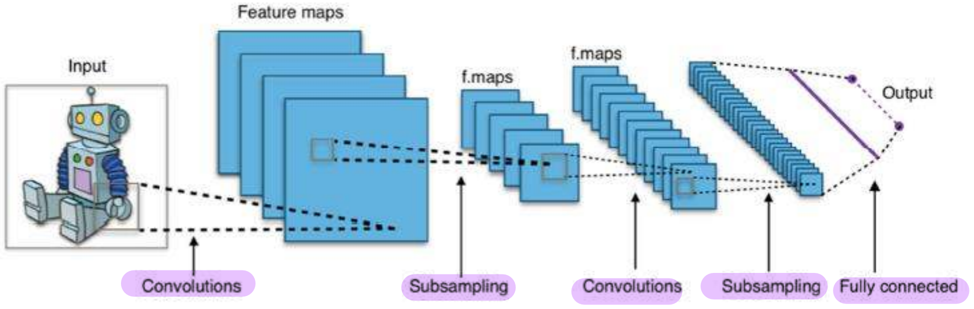
- Deep Neural Network
  - Multiple layers of hidden layers
  - Much more sophisticated algorithms can be learnt

AlexNet

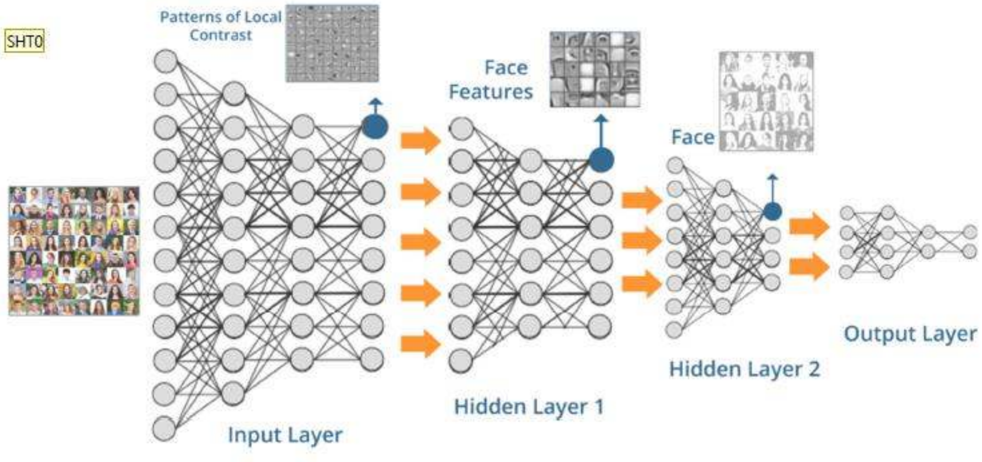
At the 2012 ImageNet computer image recognition competition:

- 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)

<u>AI Applications</u>

- 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
  - AL 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

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

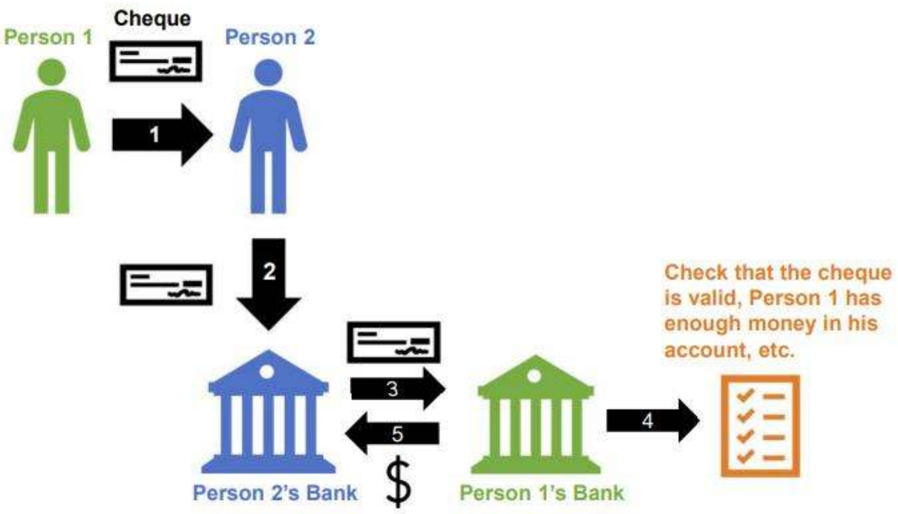
Money/Currency:

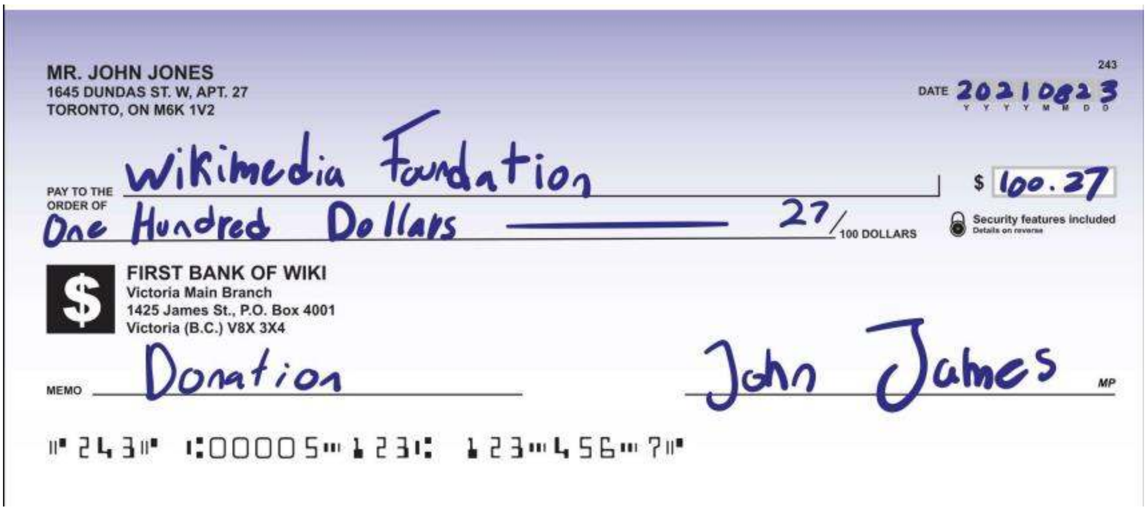
- according to mainstream economics, money (currency)relieves the issues arising from commodity trading as it is a universal store of value that can be readily used by anyone
- allows faster transactions as sellers have an easier time finding a buyer with whom they want to do business with
  - a seller 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.


Person 1
Cheque
Person 2
1
2
3
5
$
4
Person 2's Bank
Person 1's Bank
Check that the cheque is valid, Person 1 has enough money in his account, etc.



MR. JOHN JONES
1645 DUNDAS ST. W, APT. 27
TORONTO, ON M6K 1V2

243

DATE 20210823
Y Y Y Y M M D D

PAY TO THE ORDER OF Wikimedia Foundation $ 100.27

One Hundred Dollars 27/100 DOLLARS

Security features included
Details on reverse

FIRST BANK OF WIKI
Victoria Main Branch
1425 James St., P.O. Box 4001
Victoria (B.C.) V8X 3X4

MEMO Donation

John James

MP

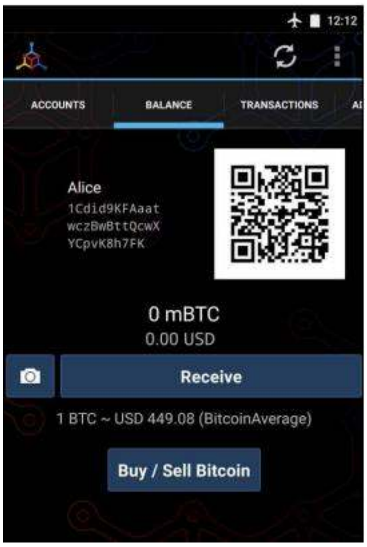
⑈243⑈ ⑆00005⑉123⑆ 123⑉456⑉7⑈

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:



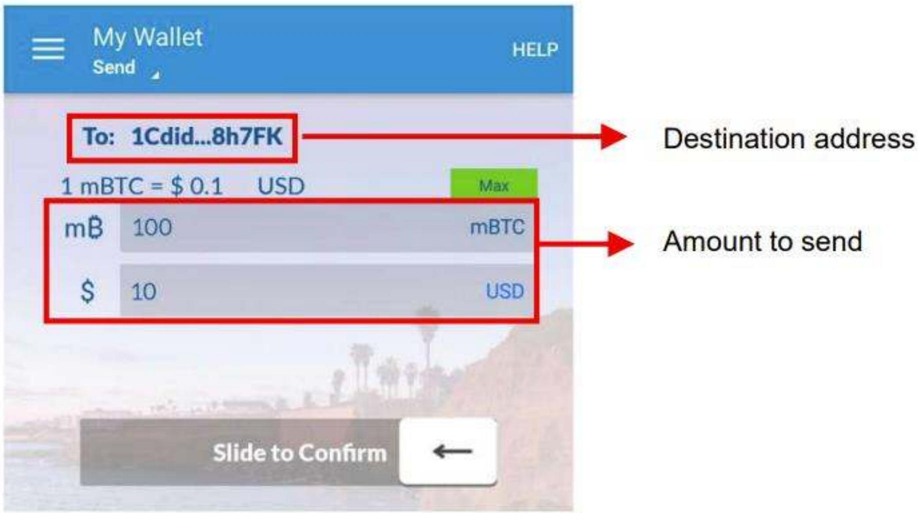
Alice
1Cdid9KFAaat
wczBwBttQcwX
YCpvK8h7FK

0 mBTC
0.00 USD

1 BTC ~ USD 449.08 (BitcoinAverage)

Important part:

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



To: 1Cdid...8h7FK

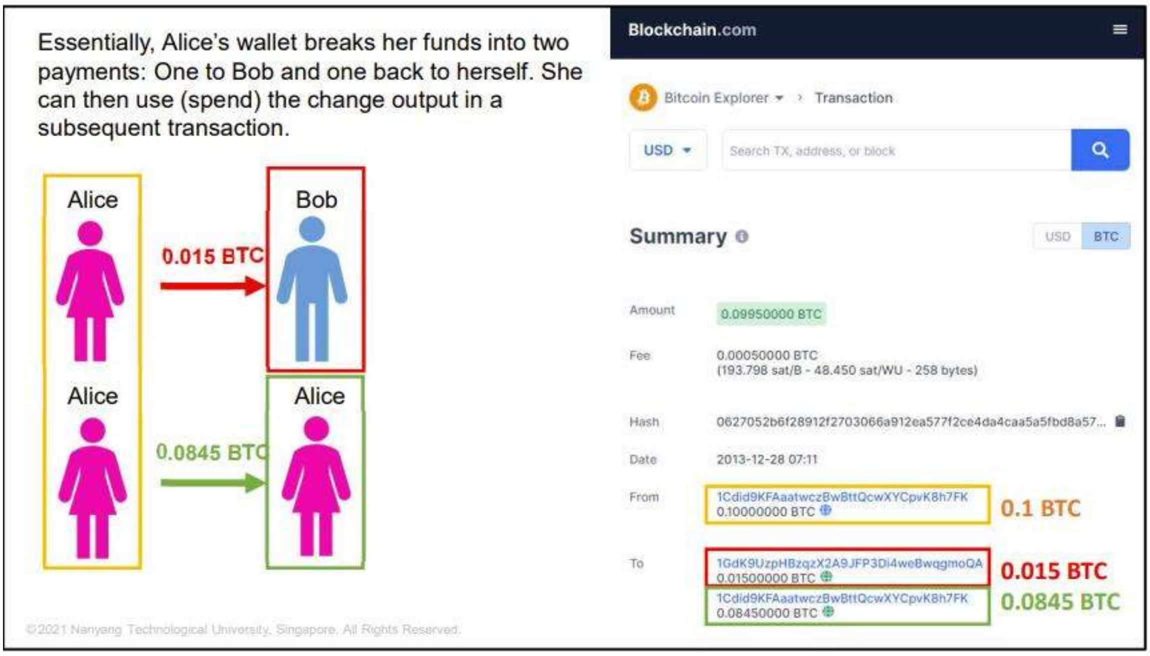
1 mBTC = $ 0.1 USD

mB 100 mBTC

$ 10 USD

Sending bitcoin, screen is presented with:

1. A destination bitcoin address 2.
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.

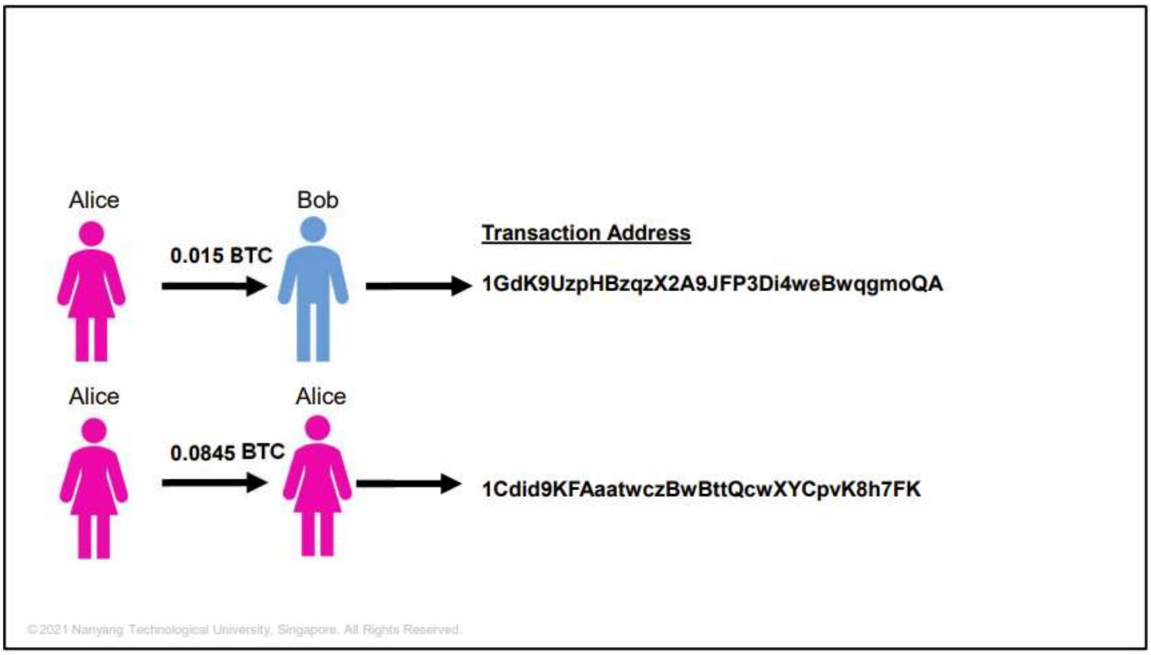
Summary

Amount	0.09950000 BTC
Fee	0.00050000 BTC (193.798 sat/B - 48.450 sat/WU - 258 bytes)
Hash	0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57...
Date	2013-12-28 07:11
From	1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK 0.10000000 BTC
To	1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA 0.01500000 BTC 1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK 0.08450000 BTC

She can then use (spend) the change output in a subsequent transaction. This is called the UXTO 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 keep of the transactions.



Alice

0.015 BTC

Bob

Transaction Address

1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA

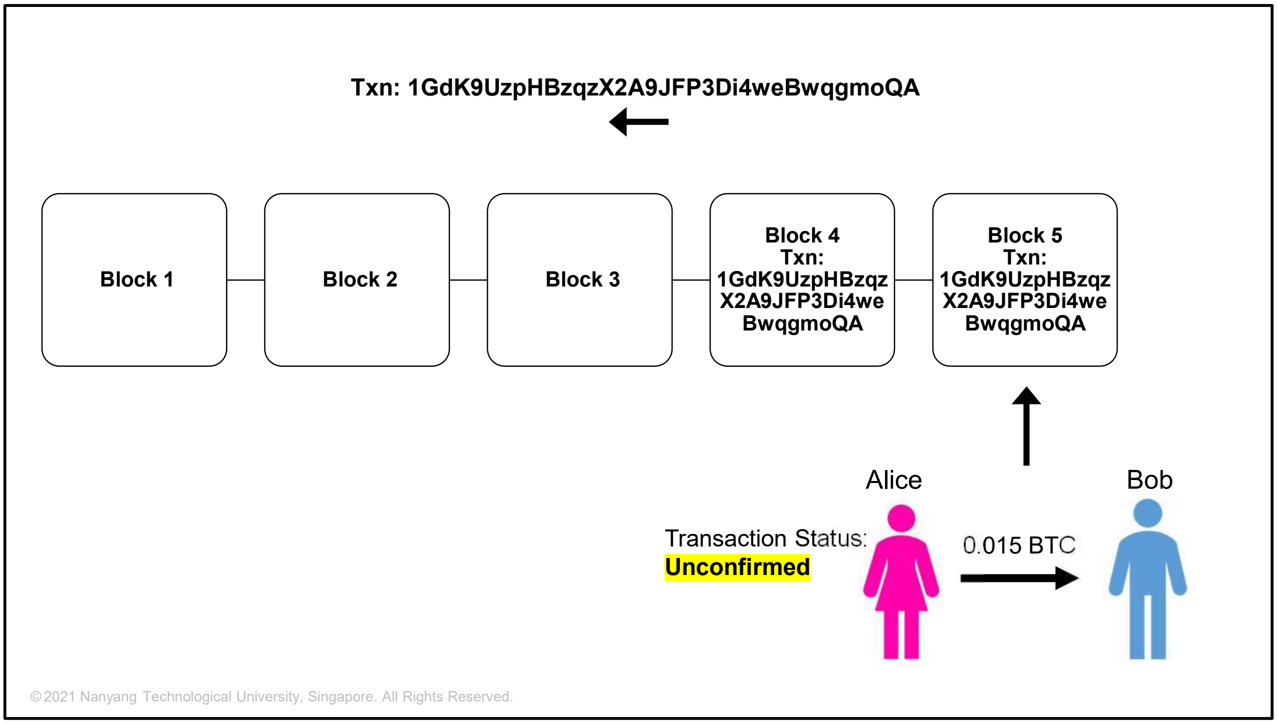
Alice

0.0845 BTC

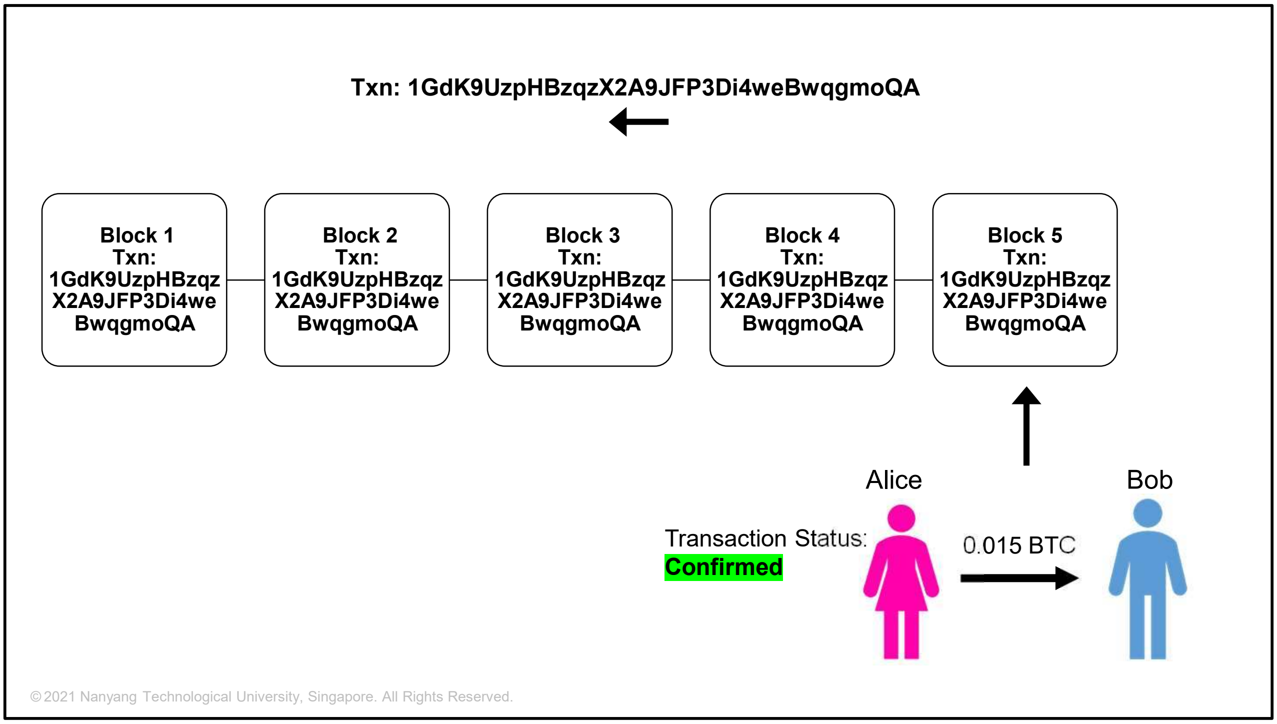
Alice

1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK

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.



Txn: 1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA

Block 1
Txn:
1GdK9UzpHBzqz
X2A9JFP3Di4we
BwqgmoQA

Block 2
Txn:
1GdK9UzpHBzqz
X2A9JFP3Di4we
BwqgmoQA

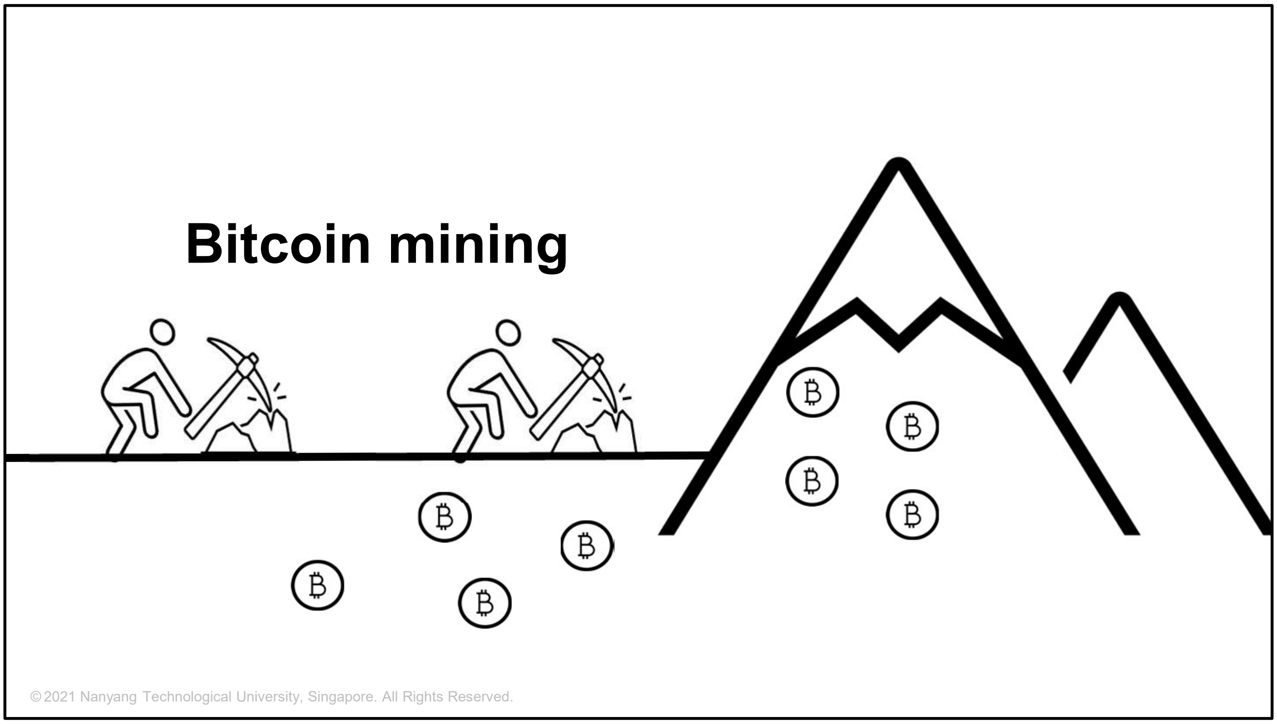
Block 3
Txn:
1GdK9UzpHBzqz
X2A9JFP3Di4we
BwqgmoQA

Block 4
Txn:
1GdK9UzpHBzqz
X2A9JFP3Di4we
BwqgmoQA

Block 5
Txn:
1GdK9UzpHBzqz
X2A9JFP3Di4we
BwqgmoQA

Transaction Status:
Confirmed

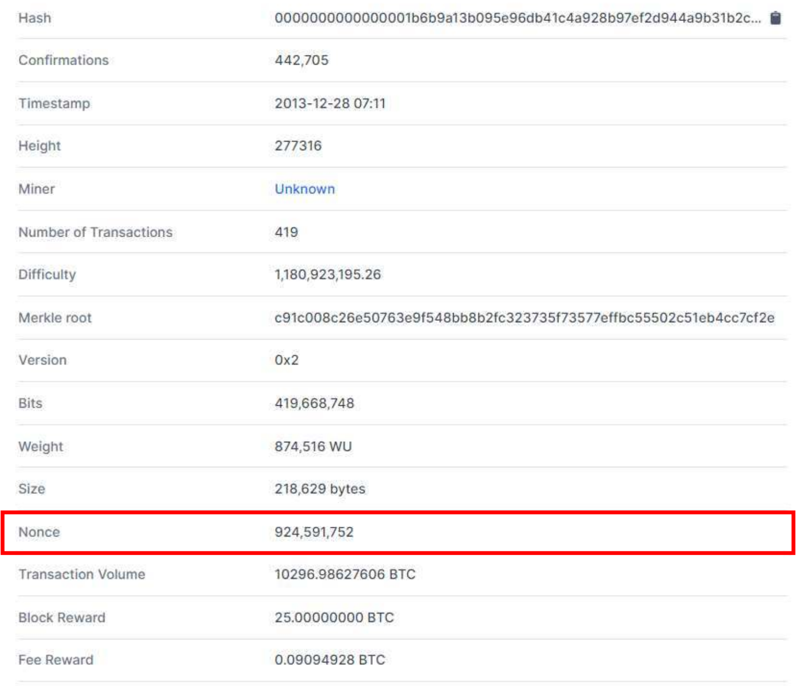
Once the transaction has been propagated to every block and accepted in the network, Alice's transaction is confirmed and Bob can give her the coffee. For small transactions such as this, usually Bob will simply give the coffee even before the transaction is confirmed. Besides, confirmation only takes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



Bitcoin mining

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



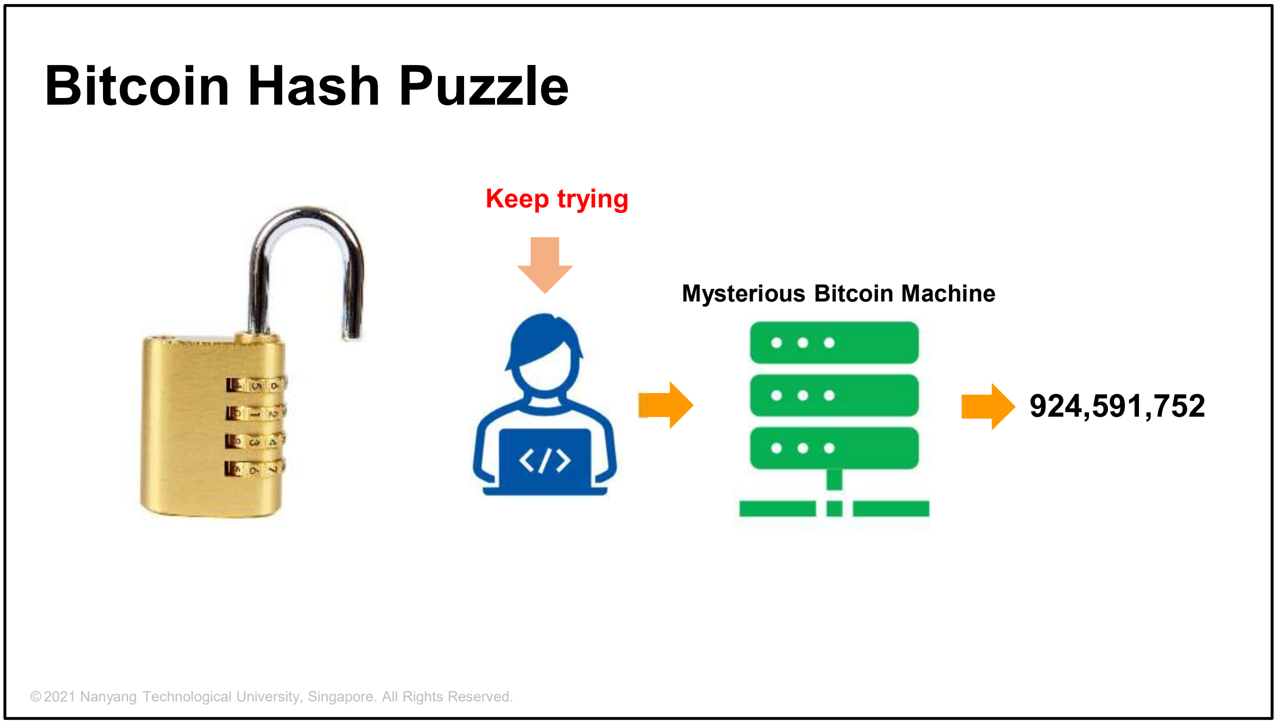
Hash	0000000000000001b6b9a13b095e96db41c4a928b97ef2d944a9b31b2c...
Confirmations	442,705
Timestamp	2013-12-28 07:11
Height	277316
Miner	Unknown
Number of Transactions	419
Difficulty	1,180,923,195.26
Merkle root	c91c008c26e50763e9f548bb8b2fc323735f73577effbc55502c51eb4cc7cf2e
Version	0x2
Bits	419,668,748
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.



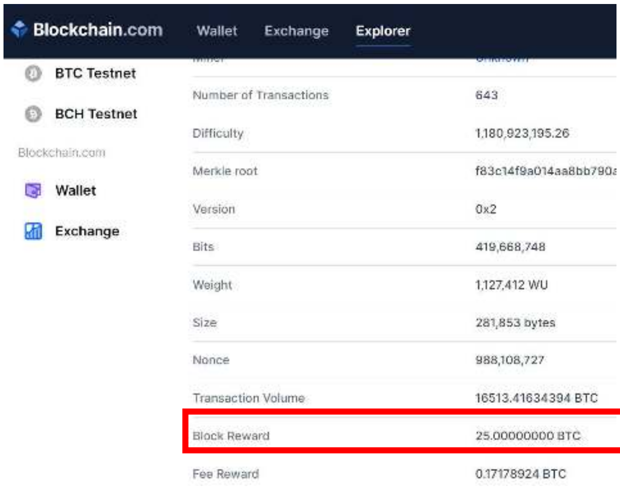
Bitcoin Hash Puzzle

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.

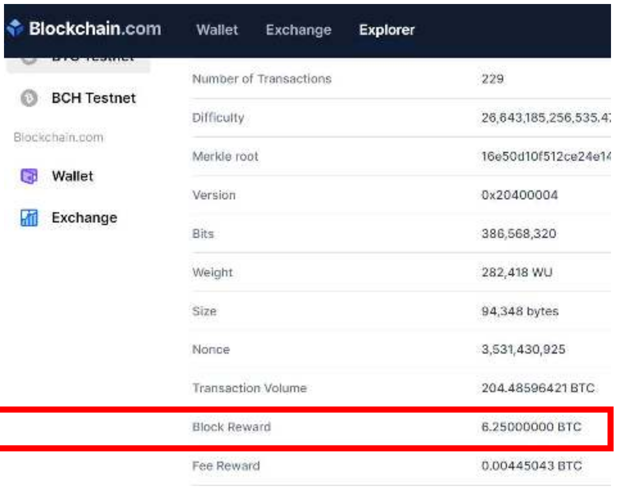
You can consider this as you have a mysterious bitcoin mining machine, like the miner or ledger keeper who records all transactions between Alice and Bob, the machine will search for this nonce that can be combined with all transaction records and generate a hash value that meets the pre-determined requirement.

Block 277317



Number of Transactions	643
Difficulty	1,180,923,195.26
Merkle root	f83c14f9a014aa8bb790a
Version	0x2
Bits	419,668,748
Weight	1,127,412 WU
Size	281,853 bytes
Nonce	988,108,727
Transaction Volume	16513.41634394 BTC
Block Reward	25.00000000 BTC
Fee Reward	0.17178924 BTC

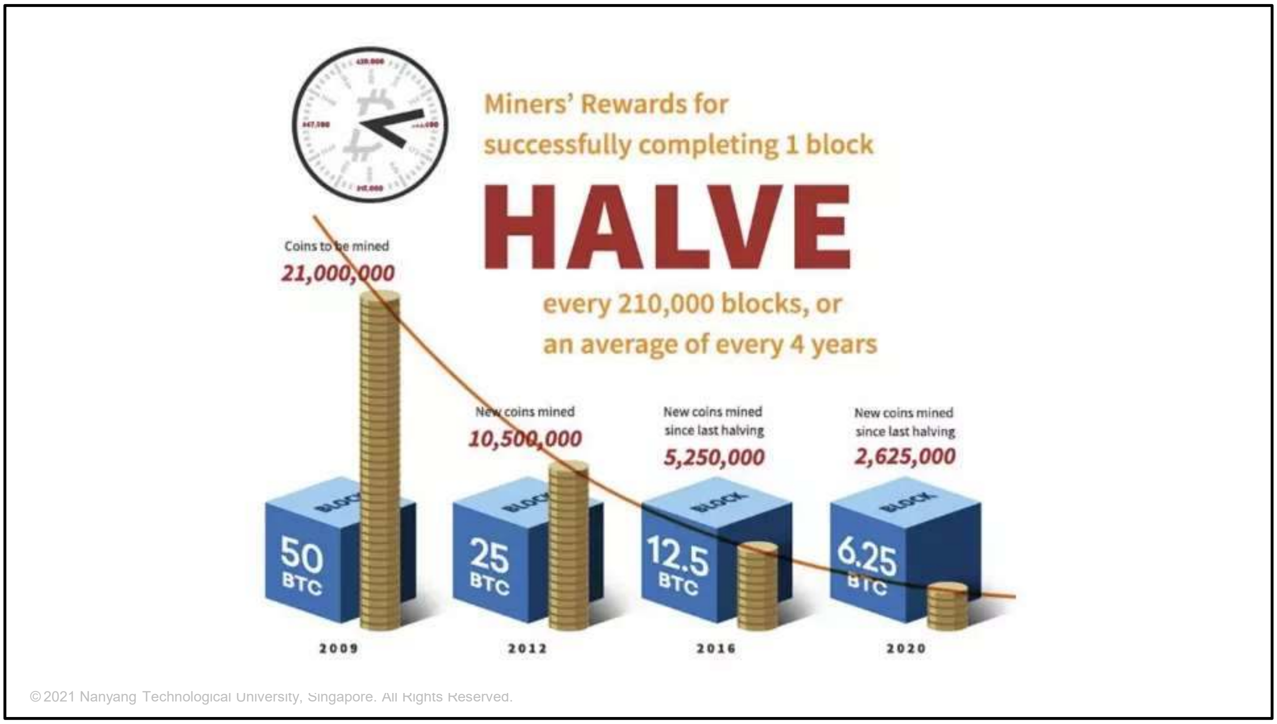
Block 720041



Number of Transactions	229
Difficulty	26,643,185,256,535.47
Merkle root	16e50d10f512ce24e14
Version	0x20400004
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
Fee Reward	0.00445043 BTC

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).

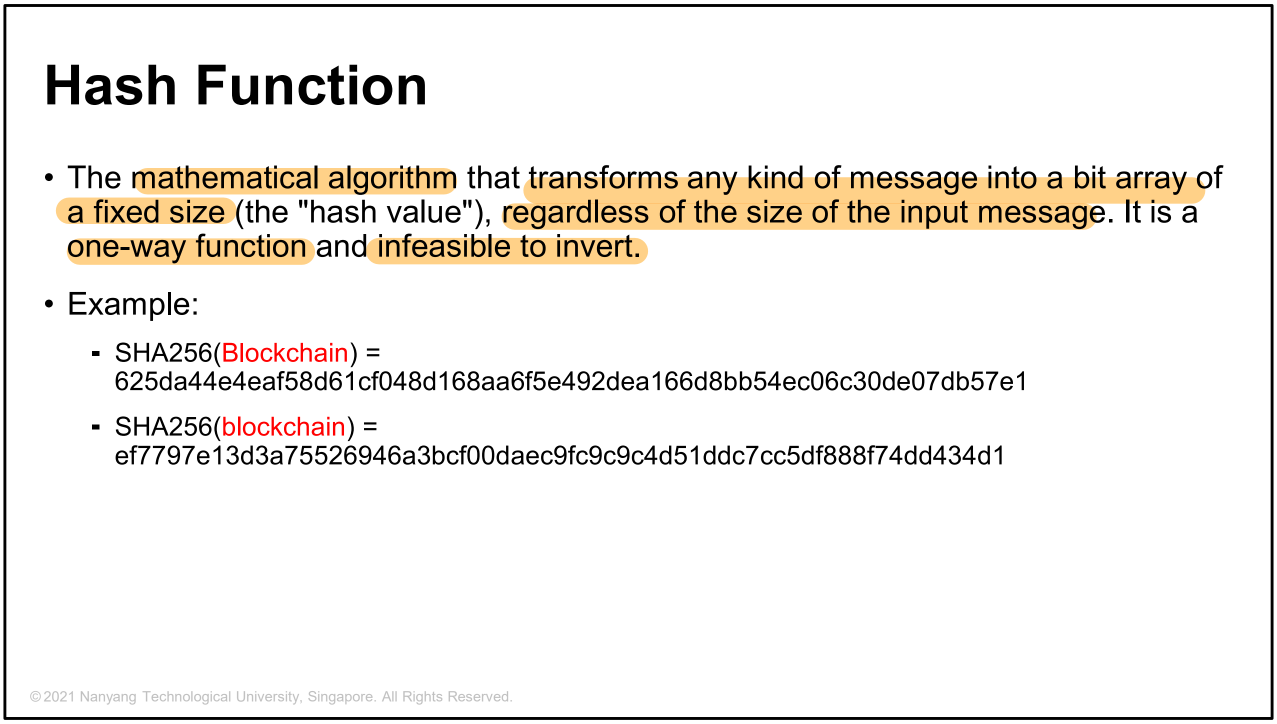


This is because miners' rewards for successfully completing 1 block halve every210,000 blocks or an average of every 4 years. The supply of bitcoins is capped at 21 million, which is forecasted to be all mined by the year 2140.

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.



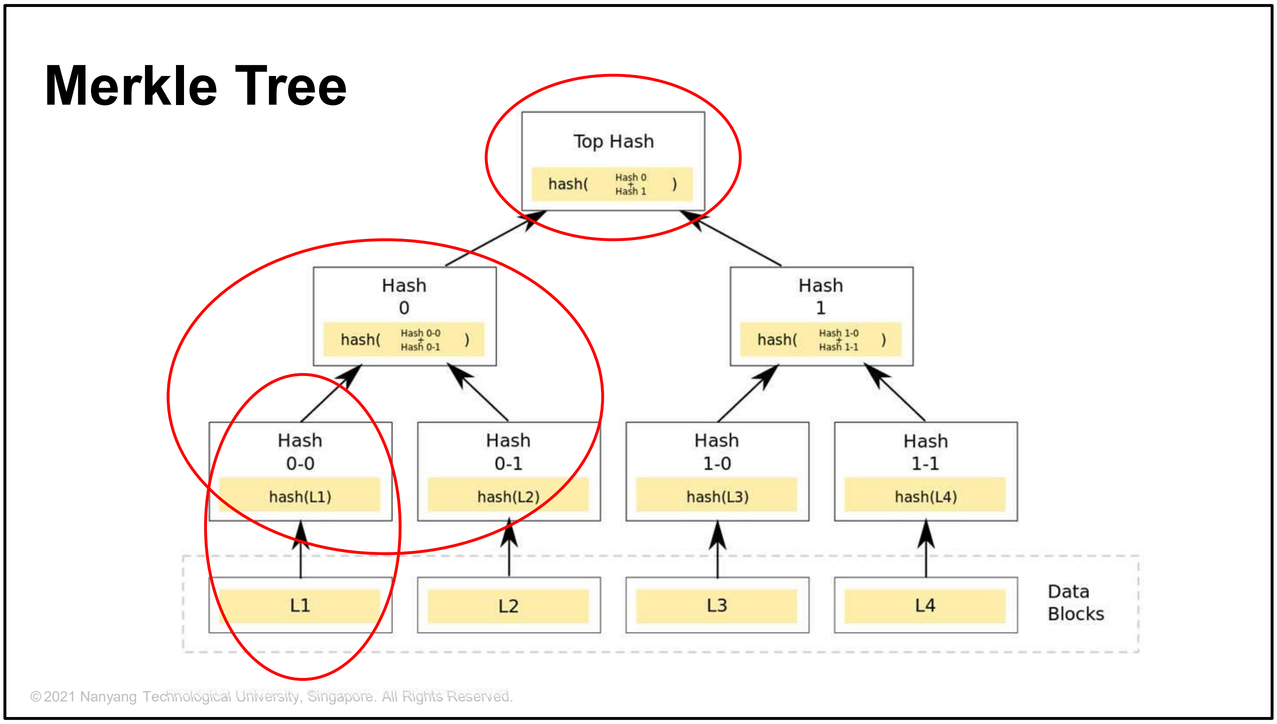
Hash Function

- 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) = ef7797e13d3a75526946a3bcf00daec9fc9c4d51ddc7cc5df888f74dd434d1

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.

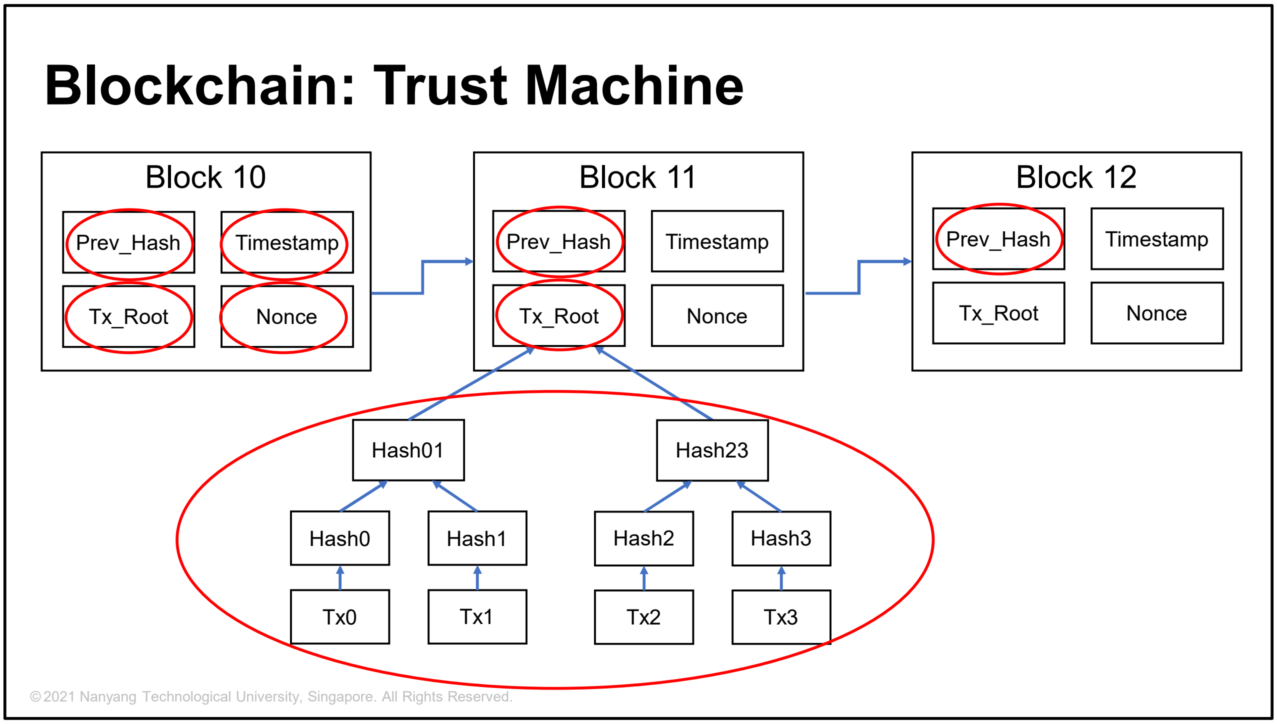
Take the hash function SHA256 for example. It generates a unique, fixed size 256-bit hash. A tiny change of the input information, say changing uppercase B to lowercase b in the word "Blockchain", leads to a completely different output. , different Hash values



Merkle Tree

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.

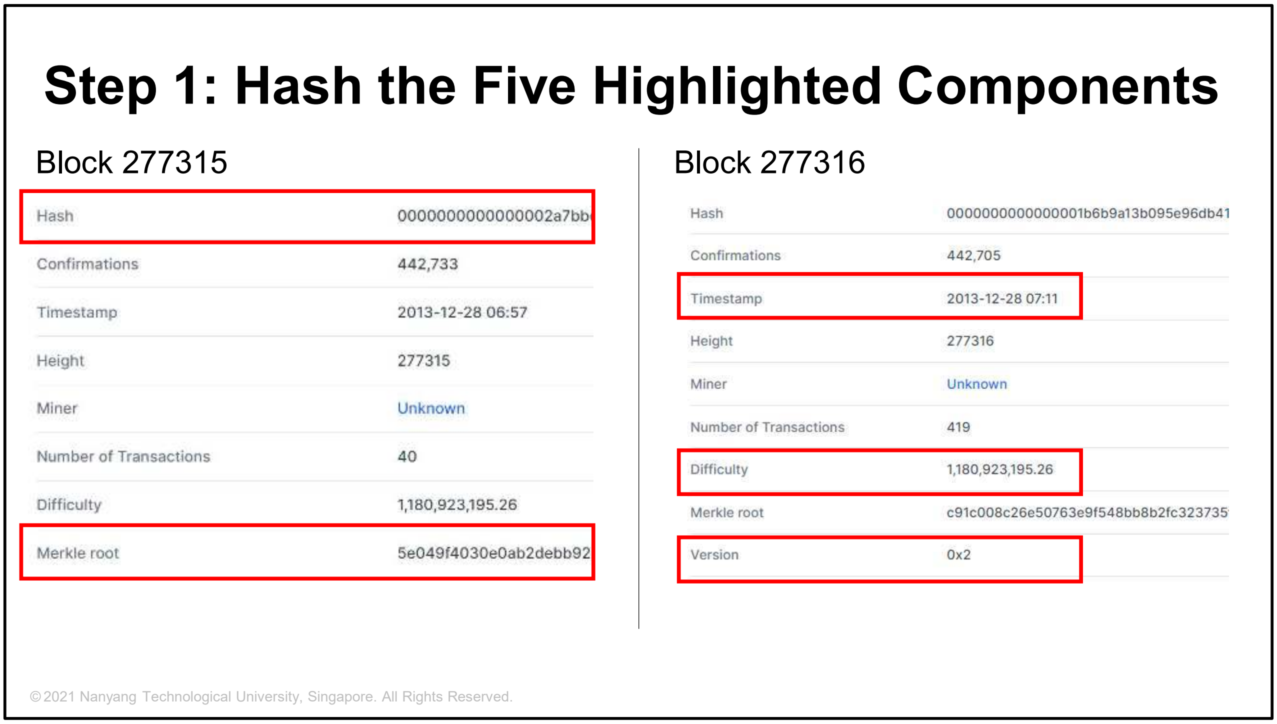


Blockchain: Trust Machine

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	0000000000000002a7bb
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	0000000000000001b6b9a13b095e96db41
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

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.

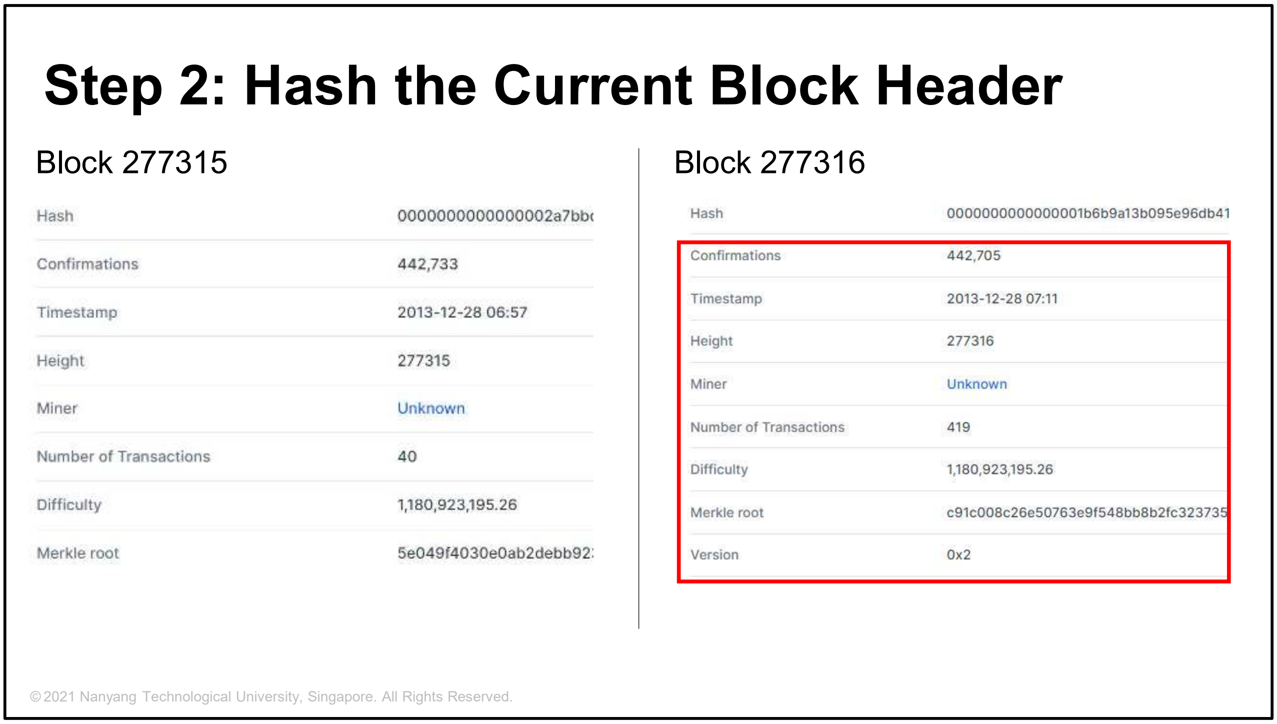
The block header is created with six fields:

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	0000000000000002a7bb
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

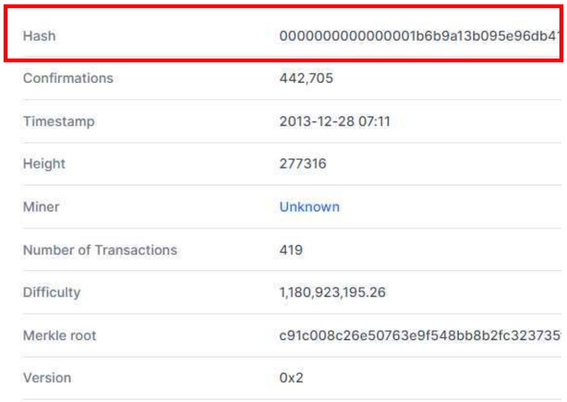
Block 277316

Hash	0000000000000001b6b9a13b095e96db41
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

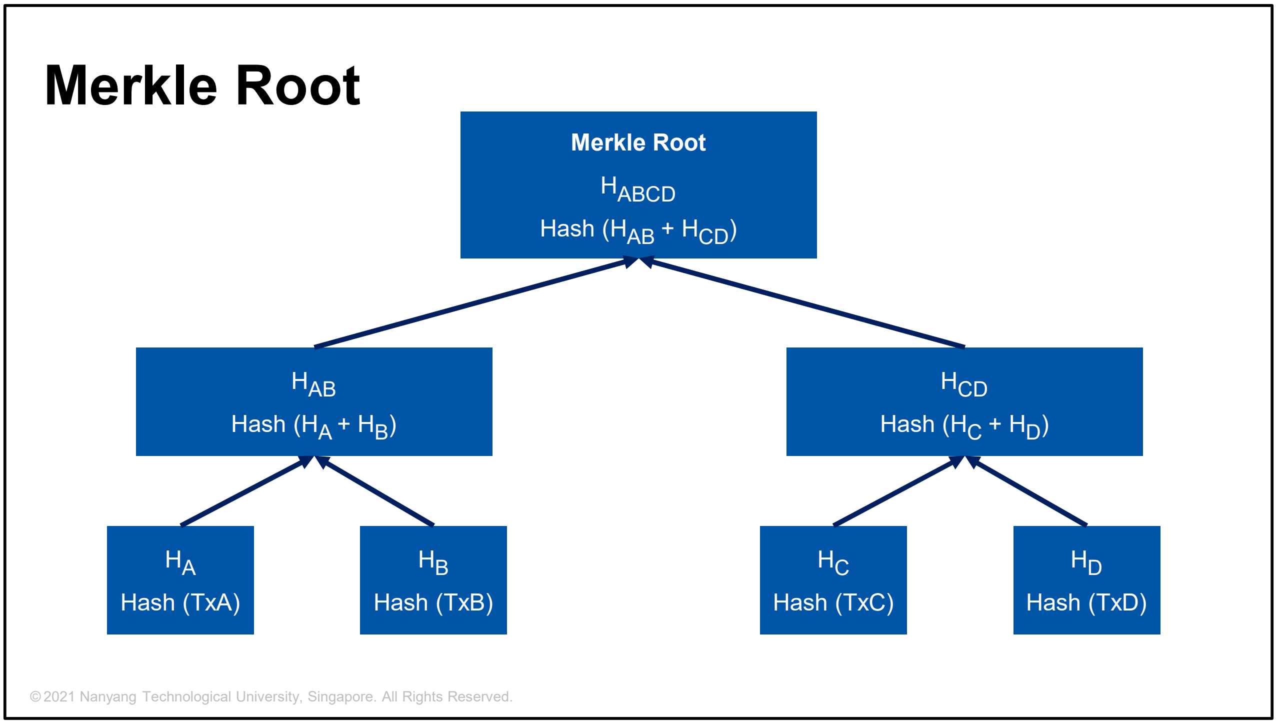
The block header (which contains the Merkle root) is hashed, resulting in the block hash.

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

Merkle Root

H_{ABCD}

Hash (H_{AB} + H_{CD})

H_{AB}

Hash (H_A + H_B)

H_{CD}

Hash (H_C + H_D)

H_A

Hash (TxA)

H_B

Hash (TxB)

H_C

Hash (TxC)

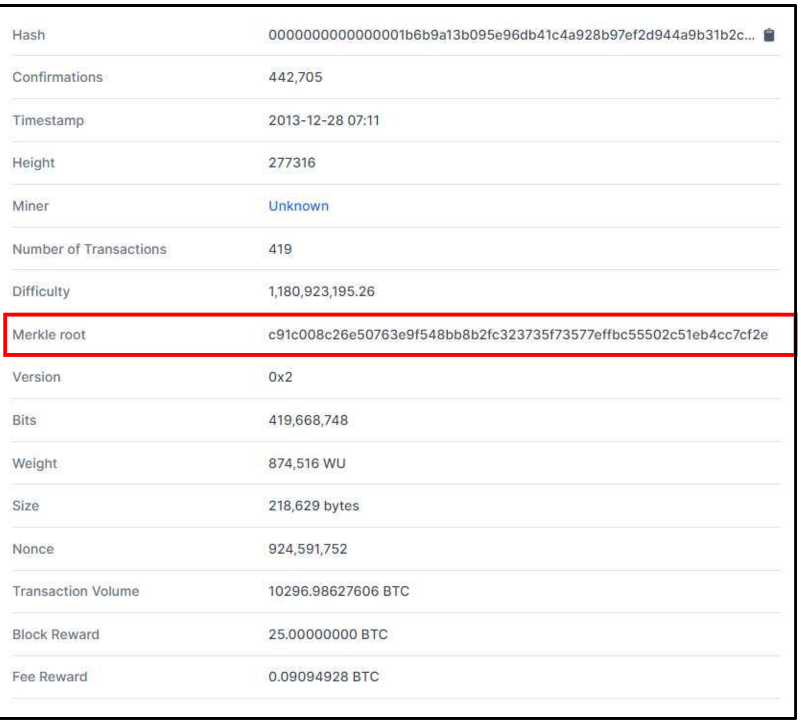
H_D

Hash (TxD)

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

Here is the Merkle root. →

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.