UNIT 2

Cyber ethics

Significance of cyber ethics

Cyberlaw plays an important role in shaping and overseeing the digital world. It deals with many issues, from protecting people and businesses from online threats to ensuring that digital transactions are private and secure. As technology keeps advancing, cyber law needs to evolve and meet new challenges, encouraging responsible and lawful use of digital tools.

The significance of cyber law lies in its capacity to navigate and regulate the intricate challenges that arise from the pervasive use of technology. Cyberlaw provides a framework for protecting individuals and organizations from cyber threats, ensuring the privacy and security of digital transactions, and establishing guidelines for ethical and legal conduct in cyberspace. As the digital world evolves, the importance of cyber law becomes more pronounced, serving as a cornerstone for the responsible and lawful utilization of digital resources.

Here's a overview of the significance of cyber ethics:

1. Data Privacy and Confidentiality

- **Data Protection**: Individuals and organizations handle sensitive data like personal information, financial records, and health details online. Ethical use of this data ensures that it is protected from unauthorized access, manipulation, or misuse. Cyber ethics emphasizes the responsibility of professionals to secure data and maintain confidentiality.
- **Consent**: Respecting users' consent when collecting, processing, or sharing their data is critical. Ethical practices demand transparency in how data is used and ensure that individuals can control their personal information.

2. Cybersecurity and Protection from Harm

- **Prevention of Cybercrime**: Ethical considerations play a vital role in guiding individuals and institutions to prevent cybercrimes like hacking, phishing, ransomware attacks, identity theft, and malware distribution. Following cyber ethical standards discourages malicious actions and promotes a safer digital environment.
- **Vulnerability Management**: Ethical behavior includes reporting and fixing security flaws, not exploiting them. Ethical hackers or "white hats" actively work to improve security by finding and responsibly disclosing vulnerabilities.
- **Digital Well-being**: Users' mental and emotional well-being should also be protected. Ethical considerations call for efforts to mitigate cyberbullying, online harassment, and manipulation through false or harmful content.

3. Intellectual Property and Fair Use

- **Copyright and Fair Use**: The internet provides easy access to intellectual property, but ethical use means respecting copyrights, trademarks, and other legal protections. Cyber ethics involves recognizing the ownership of digital content (software, media, etc.) and not engaging in piracy, plagiarism, or unauthorized sharing.

- **Open Access vs. Proprietary Content**: Ethical dilemmas often arise in balancing the accessibility of knowledge (open access) with the protection of proprietary work. A robust understanding of ethical frameworks helps in navigating these challenges.

Need for cyber regulations and ethics

Cyber law is of paramount importance in our digital age as it safeguards digital assets, prevents cybercrimes, regulates online activities, protects e-commerce and consumer rights, fosters international cooperation, upholds intellectual property rights, ensures data privacy, and provides legal remedies. It plays a vital role in establishing legal order and security in the digital realm, protecting both individuals and organizations in an interconnected world. The need for cyber regulations and ethics stems from the rapid growth of digital technologies and the increasing prevalence of cyber threats that endanger individuals, businesses, and nations. Cyber regulations are essential for ensuring the safe and responsible use of the internet, protecting users' rights, and securing sensitive information. Ethics in the digital realm guide responsible behavior, ensuring fairness, transparency, and respect for privacy.

Here are some key points highlighting the importance of cyber regulations and ethics:

1. **Protection of Sensitive Data**: With increasing reliance on digital systems, sensitive data (personal, financial, health-related) is vulnerable to

cyberattacks. Cyber regulations establish frameworks to ensure proper handling, storage, and protection of such data.

2. **Preventing Cybercrime**: Cyberattacks such as hacking, phishing, and ransomware are rising. Regulations help criminalize and penalize such behavior, deterring malicious actors.

3. **Safeguarding National Security**: Many cyberattacks target national infrastructure, such as power grids, financial systems, and communications. Effective cyber regulations can safeguard these critical systems and enhance national security.

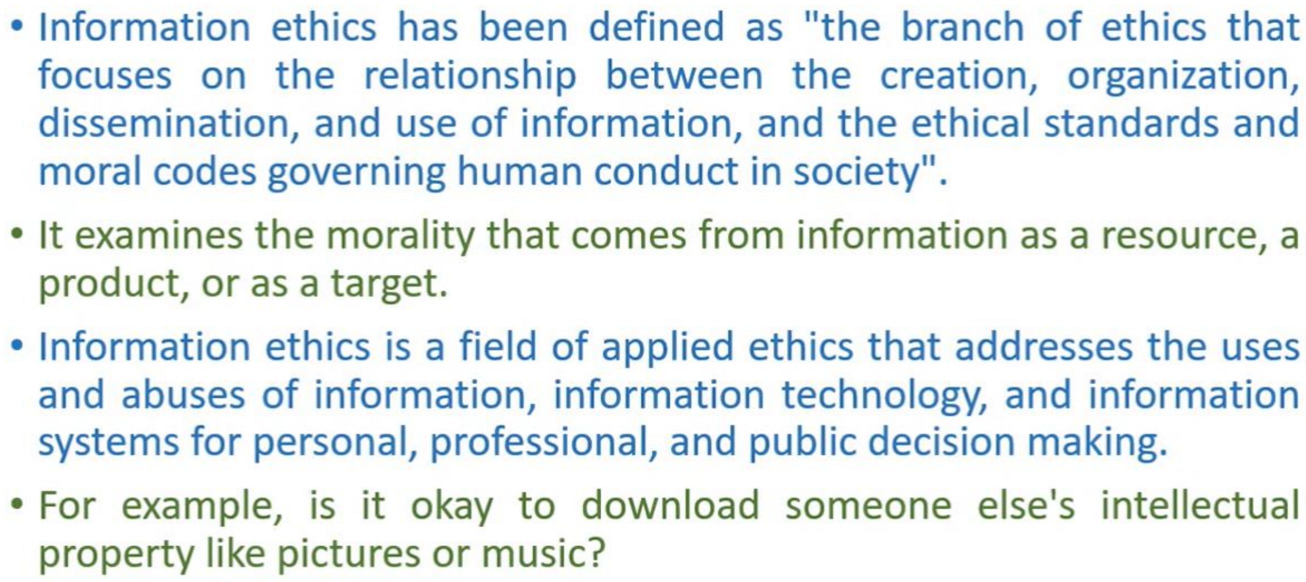
4. **Ethical Use of Technology**: Cyber ethics ensure that technology is used in ways that promote human dignity, privacy, and fairness. For example, issues like mass surveillance and AI ethics are prominent topics in cyber ethics.

5. **Global Cooperation**: Cyber threats often transcend borders, requiring international cooperation in cyber regulations. Global treaties, such as the **Budapest Convention on Cybercrime**, help foster cross-border cooperation.

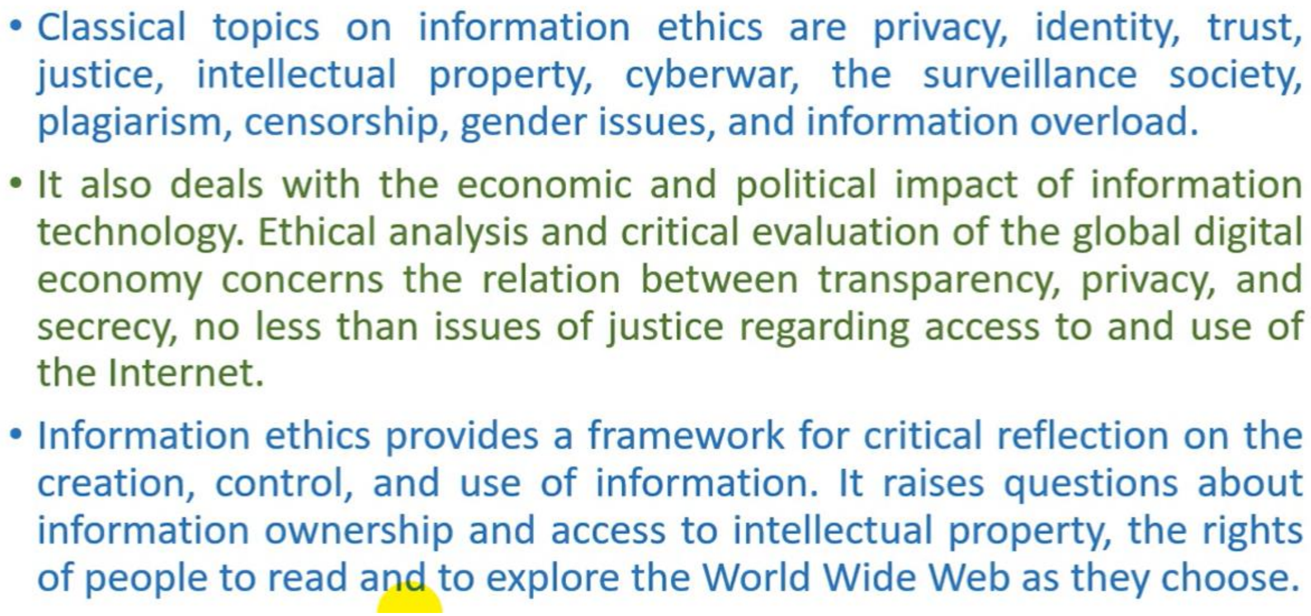
These regulations and ethical frameworks are designed to mitigate risks, encourage responsible behavior, and promote collaboration between governments, businesses, and individuals to ensure a secure and trustworthy cyber ecosystem.

ETHICS IN INFORMATION SOCIETY

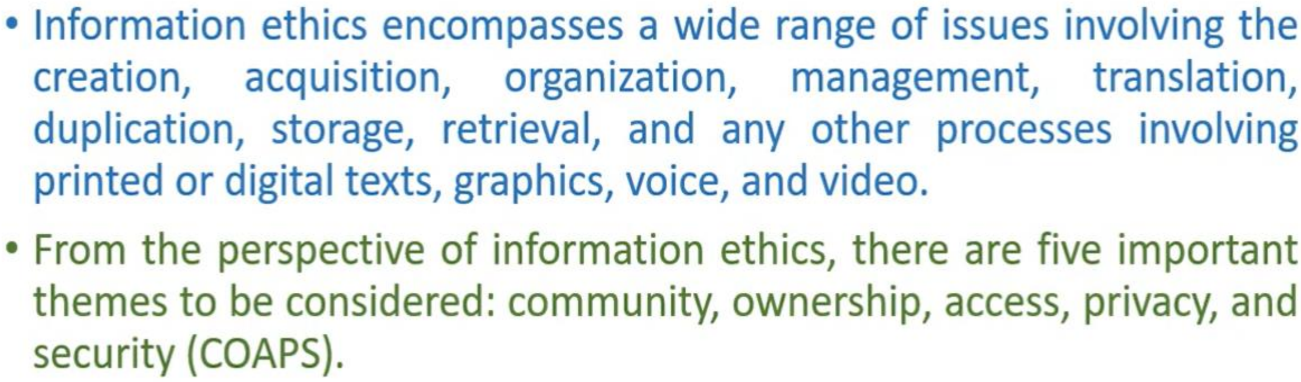
Information ethics broadly examines issues related to ownership, access, privacy, security, and community. It is also concerned with relational issues such as "the relationship between information and the good of society, the relationship between information providers and the consumers of nloainformation".



- Information ethics has been defined as "the branch of ethics that focuses on the relationship between the creation, organization, dissemination, and use of information, and the ethical standards and moral codes governing human conduct in society".
- It examines the morality that comes from information as a resource, a product, or as a target.
- Information ethics is a field of applied ethics that addresses the uses and abuses of information, information technology, and information systems for personal, professional, and public decision making.
- For example, is it okay to download someone else's intellectual property like pictures or music?



- Classical topics on information ethics are privacy, identity, trust, justice, intellectual property, cyberwar, the surveillance society, plagiarism, censorship, gender issues, and information overload.
- It also deals with the economic and political impact of information technology. Ethical analysis and critical evaluation of the global digital economy concerns the relation between transparency, privacy, and secrecy, no less than issues of justice regarding access to and use of the Internet.
- Information ethics provides a framework for critical reflection on the creation, control, and use of information. It raises questions about information ownership and access to intellectual property, the rights of people to read and to explore the World Wide Web as they choose.

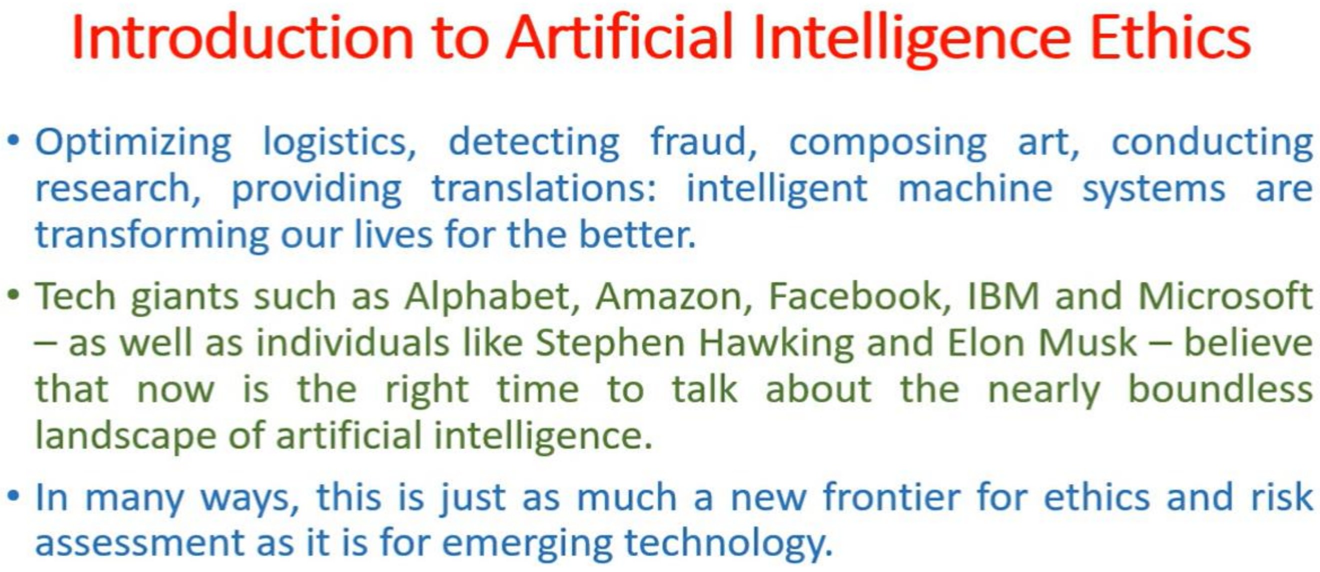


- Information ethics encompasses a wide range of issues involving the creation, acquisition, organization, management, translation, duplication, storage, retrieval, and any other processes involving printed or digital texts, graphics, voice, and video.
- From the perspective of information ethics, there are five important themes to be considered: community, ownership, access, privacy, and security (COAPS).

ARTIFICIAL INTELLIGENCE

Artificial intelligence (AI) is the simulation of human intelligence in machines that are programmed to think and act like humans. Learning, reasoning, problem-solving, perception, and language comprehension are all examples of cognitive abilities.

Artificial Intelligence is a method of making a computer, a computer-controlled robot, or a software think intelligently like the human mind. AI is accomplished by studying the patterns of the human brain and by analyzing the cognitive process. The outcome of these studies develops intelligent software and systems.



Introduction to Artificial Intelligence Ethics

- Optimizing logistics, detecting fraud, composing art, conducting research, providing translations: intelligent machine systems are transforming our lives for the better.
- Tech giants such as Alphabet, Amazon, Facebook, IBM and Microsoft – as well as individuals like Stephen Hawking and Elon Musk – believe that now is the right time to talk about the nearly boundless landscape of artificial intelligence.
- In many ways, this is just as much a new frontier for ethics and risk assessment as it is for emerging technology.

Artificial intelligence (AI) is the ability of machines to replicate or enhance human intellect, such as reasoning and learning from experience. Artificial intelligence has been used in computer programs for years, but it is now applied to many other products and services. For example, some digital cameras can determine what objects are present in an image using artificial intelligence software. In addition, experts predict many more innovative uses for artificial intelligence in the future, including smart electric grids.

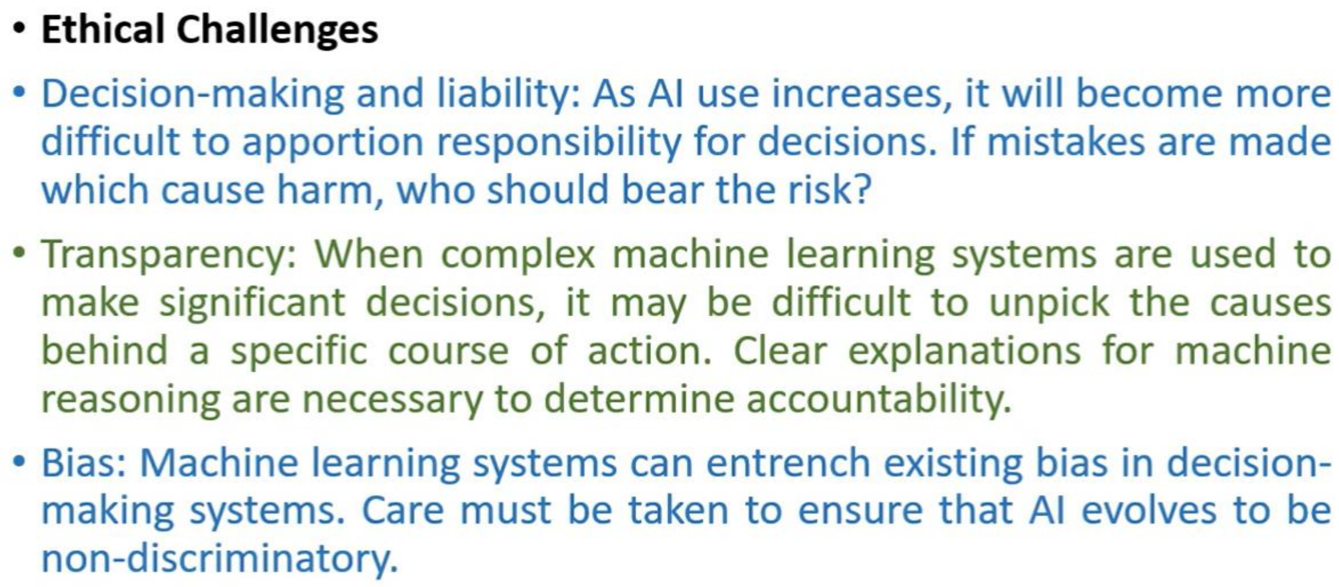
AI uses techniques from probability theory, economics, and algorithm design to solve practical problems. In addition, the AI field draws upon computer science, mathematics, psychology, and linguistics. Computer science provides tools for designing and building algorithms, while mathematics offers tools for modeling and solving the resulting optimization problems.

Although the concept of AI has been around since the 19th century, when Alan Turing first proposed an "imitation game" to assess machine intelligence, it only became feasible to achieve in recent decades due to the increased availability of computing power and data to train AI systems.

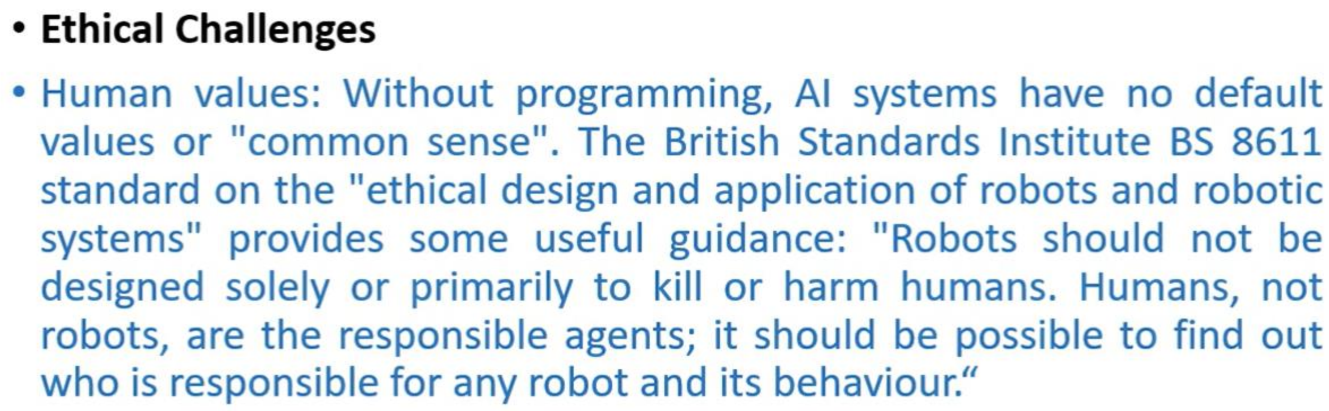
To understand the idea behind AI, you should think about what distinguishes human intelligence from that of other creatures – our ability to learn from experiences and apply these lessons to new situations. We can do this because of our advanced brainpower; we have more neurons than any animal species.

Today's computers don't match the human biological neural network – not even close. But they have one significant advantage over us: their ability to analyze vast amounts of data and experiences much faster than humans could ever hope.

AI lets you focus on the most critical tasks and make better decisions based on acquired data related to a use case. It can be used for complex tasks, such as predicting maintenance requirements, detecting credit card fraud, and finding the best route for a delivery truck. In other words, AI can automate many business processes leaving you to concentrate on your core business.



- **Ethical Challenges**
- Decision-making and liability: As AI use increases, it will become more difficult to apportion responsibility for decisions. If mistakes are made which cause harm, who should bear the risk?
- Transparency: When complex machine learning systems are used to make significant decisions, it may be difficult to unpick the causes behind a specific course of action. Clear explanations for machine reasoning are necessary to determine accountability.
- Bias: Machine learning systems can entrench existing bias in decision-making systems. Care must be taken to ensure that AI evolves to be non-discriminatory.



- **Ethical Challenges**
- Human values: Without programming, AI systems have no default values or "common sense". The British Standards Institute BS 8611 standard on the "ethical design and application of robots and robotic systems" provides some useful guidance: "Robots should not be designed solely or primarily to kill or harm humans. Humans, not robots, are the responsible agents; it should be possible to find out who is responsible for any robot and its behaviour.“

AI ethics

As AI technology becomes more advanced, ethical issues are more likely to arise. Artificial intelligence simulates human intelligence and decision-making. Unfortunately, this comes with many risks, including those to human safety.

AI needs a lot of data to work. If that data is inaccurate or biased, it can lead to poor-quality or even dangerous output.

AI ethics are a set of principles and guidelines for how we develop and use AI. Organizations incorporate these formally into AI ethics policies. This ensures that decisions made by staff and stakeholders are kept within ethical AI guidelines, minimize risks, and focus on improving life for all human beings.

5 key principles of AI ethics

1. Transparency

From hiring processes to driverless cars, AI is integral to human safety and wellbeing. That's why AI systems need to be transparent. Businesses, customers, and the wider public need to understand how the algorithms work and why AI has made certain decisions.

For example, a bank might refuse a customer an online loan. The customer will naturally want to understand why the algorithm refused their application. With this information, they can potentially improve their chances of approval in the future.

2. Impartiality

Another key principle for AI ethics is impartiality. AI should treat all human beings equally. That means eliminating bias and discrimination from AI systems. How can you achieve this? With high-quality data. Many data sets are not specifically created for training AI. When they’re used for this purpose, they can pass on quirks and biases from the data collection process.

Artificial intelligence can’t pick up on biases within its data. If this isn’t addressed, AI systems could repeat these biases and implement them automatically. There have been many cases of AI bias upholding systemic forms of discrimination towards marginalized groups. That’s why researchers must use unbiased, high-quality data and test models to see if they display biased behavior.

3. Accountability

Accountability is another important aspect of AI ethics. Algorithms are run by artificial intelligence. So, who is held accountable when something goes wrong? People and organizations who have worked on an AI system need to be held accountable at each stage of the process, not just after the AI is already operating.

With AI accountability, prevention is as important as the cure. Teams need to ensure they understand how well the system is working, supervise the development of the algorithms, and select high-quality data to feed into the system. Organizations should consult diversity experts, as well as people who will be using the AI system. What's more, if an AI system is used for sensitive purposes, such as public services, it should always be held accountable by external review.

4. Reliability

AI systems need to be reliable. This ensures that the results achieved by the system are reproducible and consistent. That's especially important when AI is being used for an important service, such as healthcare or credit applications.

Monitoring AI systems is key to ensuring their reliability. This way, any issues are immediately reported, and measures can be put in place to mitigate risks.

5. Security and privacy

Security measures need to be established to ensure that sensitive data is stored and used securely. These measures include data encryption, locating system vulnerabilities and defending against malicious attacks. Responsible data collection and robust data governance practices are also essential.

The Future of AI Governance: 5 Key Principles for Ethical and Responsible AI

1 Transparency and Explainability

AI systems used in credit scoring should be able to explain to a rejected applicant which factors influenced the decision, thus allowing for better understanding and trust in the AI's judgment.

2 Fairness and Non-discrimination

A major tech company has implemented an AI-driven hiring tool that not only assesses candidates' qualifications but also runs checks for bias in real-time.

3 Privacy and Data Governance

In the retail sector, a customer recommendation system by a leading online store uses AI to suggest products based on user activity.

4 Accountability

An autonomous vehicle manufacturer has established a detailed accountability framework that tracks decisions made by its AI systems.

5 Safety and Security

AI-driven autonomous drones used in delivery services must have robust safety protocols to handle system failures without causing harm to the public.

Ethical Issues in AI

1. Unemployment. What happens after the end of jobs?

- The hierarchy of labor is concerned primarily with automation. As we've invented ways to automate jobs, we could create room for people to assume more complex roles, moving from the physical work that dominated the pre-industrial globe to the cognitive labour that characterizes strategic and administrative work in our globalized society.

2. Inequality. How do we distribute the wealth created by machines?

- Our economic system is based on compensation for contribution to the economy, often assessed using an hourly wage. The majority of companies are still dependent on hourly work when it comes to products and services. But by using artificial intelligence, a company can drastically cut down on relying on the human workforce, and this means that revenues will go to fewer people. Consequently, individuals who have ownership in AI-driven companies will make all the money.

3. Humanity. How do machines affect our behavior and interaction?

- Artificially intelligent bots are becoming better and better at modelling human conversation and relationships. In 2015, a bot named Eugene Goostman won the Turing Challenge for the first time. In this challenge, human raters used text input to chat with an unknown entity, then guessed whether they had been chatting with a human or a machine. Eugene Goostman fooled more than half of the human raters into thinking they had been talking to a human being.

4. Artificial stupidity. How can we guard against mistakes?

- Intelligence comes from learning, whether you're human or machine. Systems usually have a training phase in which they "learn" to detect the right patterns and act according to their input. Once a system is fully trained, it can then go into test phase, where it is hit with more examples and we see how it performs.

5. Racist robots. How do we eliminate AI bias?

- Though artificial intelligence is capable of a speed and capacity of processing that’s far beyond that of humans, it cannot always be trusted to be fair and neutral. Google and its parent company Alphabet are one of the leaders when it comes to artificial intelligence, as seen in Google’s Photos service, where AI is used to identify people, objects and scenes. But it can go wrong, such as when a camera missed the mark on racial sensitivity, or when a software used to predict future criminals showed bias against black people.

6. Security. How do we keep AI safe from adversaries?

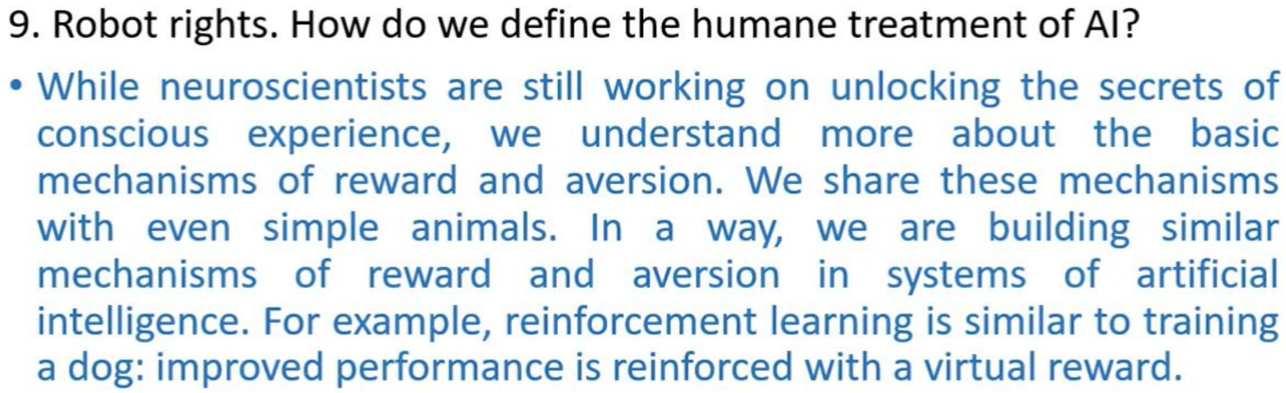
- The more powerful a technology becomes, the more can it be used for nefarious reasons as well as good. This applies not only to robots produced to replace human soldiers, or autonomous weapons, but to AI systems that can cause damage if used maliciously. Because these fights won't be fought on the battleground only, cybersecurity will become even more important. After all, we’re dealing with a system that is faster and more capable than us by orders of magnitude.

7. Evil genies. How do we protect against unintended consequences?

- It’s not just adversaries we have to worry about. What if artificial intelligence itself turned against us? This doesn't mean by turning "evil" in the way a human might, or the way AI disasters are depicted in Hollywood movies. Rather, we can imagine an advanced AI system as a "genie in a bottle" that can fulfill wishes, but with terrible unforeseen consequences.

8. Singularity. How do we stay in control of a complex intelligent system?

- The reason humans are on top of the food chain is not down to sharp teeth or strong muscles. Human dominance is almost entirely due to our ingenuity and intelligence. We can get the better of bigger, faster, stronger animals because we can create and use tools to control them: both physical tools such as cages and weapons, and cognitive tools like training and conditioning.



9. Robot rights. How do we define the humane treatment of AI?

- While neuroscientists are still working on unlocking the secrets of conscious experience, we understand more about the basic mechanisms of reward and aversion. We share these mechanisms with even simple animals. In a way, we are building similar mechanisms of reward and aversion in systems of artificial intelligence. For example, reinforcement learning is similar to training a dog: improved performance is reinforced with a virtual reward.

BLOCK CHAIN ETHICS –

Blockchain technology is a database management system that stores data in blocks that are linked together in a chain. It's a disruptive technology that can be used to securely record and share information in a variety of ways, including:

- Cryptocurrency

  Blockchain is best known for its role in cryptocurrency systems, where it maintains a decentralized record of transactions.

- Financial transactions

  Blockchain can be used as an alternative to traditional intermediaries for financial transactions.

- Business networks

  Blockchain can be used to transparently share information within a business network.

- Multi-step transactions

  Blockchain can be applied to any multi-step transaction that requires traceability and visibility.

Blockchain technology is based on three key technologies:

- Cryptographic keys

  Each individual or node has both a public and private key, which are used to create a digital signature.

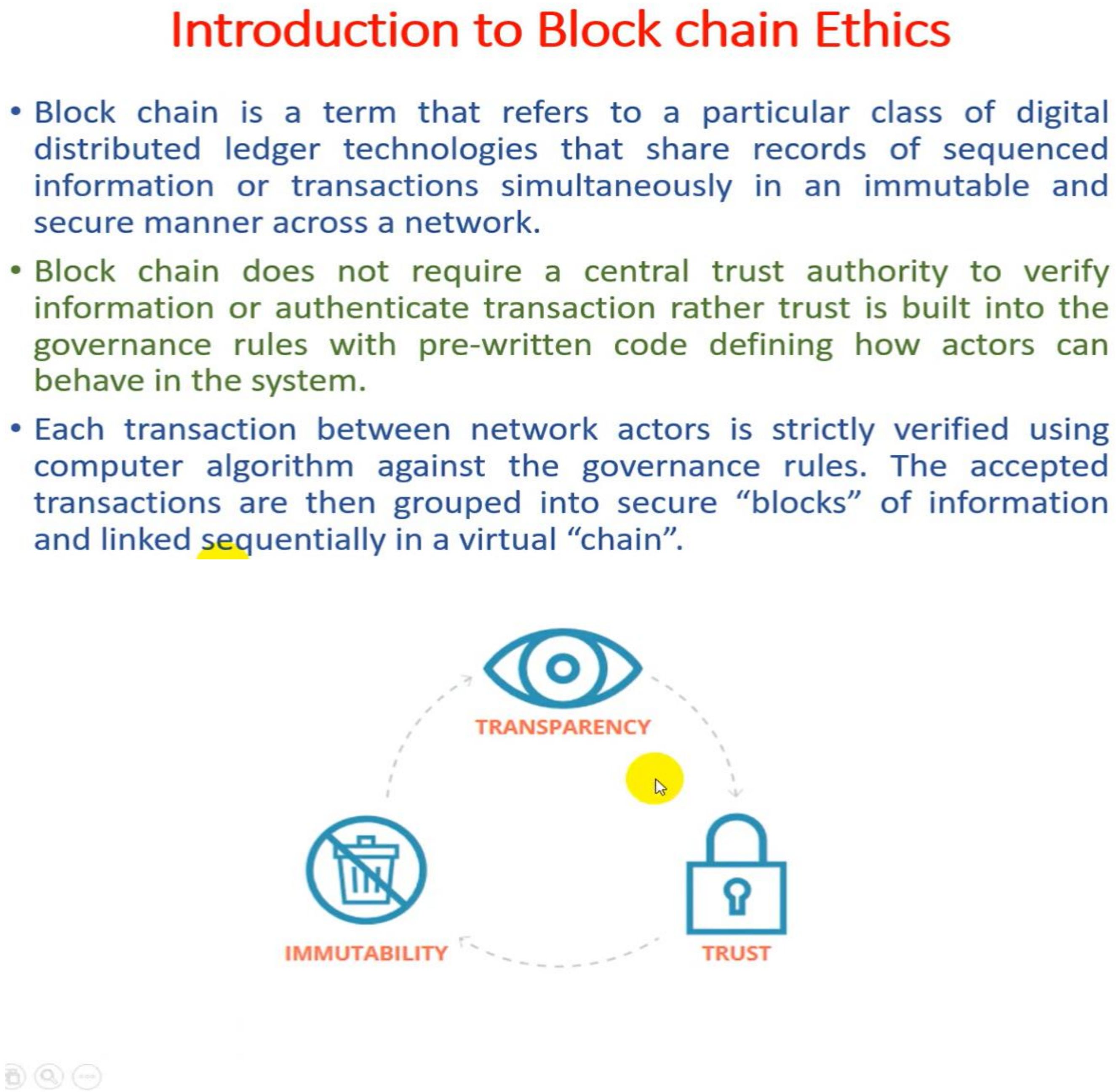
- Peer-to-peer network

  A blockchain database is managed autonomously using a peer-to-peer network.

- Digital ledger

  A blockchain is a distributed database or ledger shared among a computer network's nodes.

"Blockchain ethics is a set of ethical guidelines and considerations for how blockchain systems are governed."

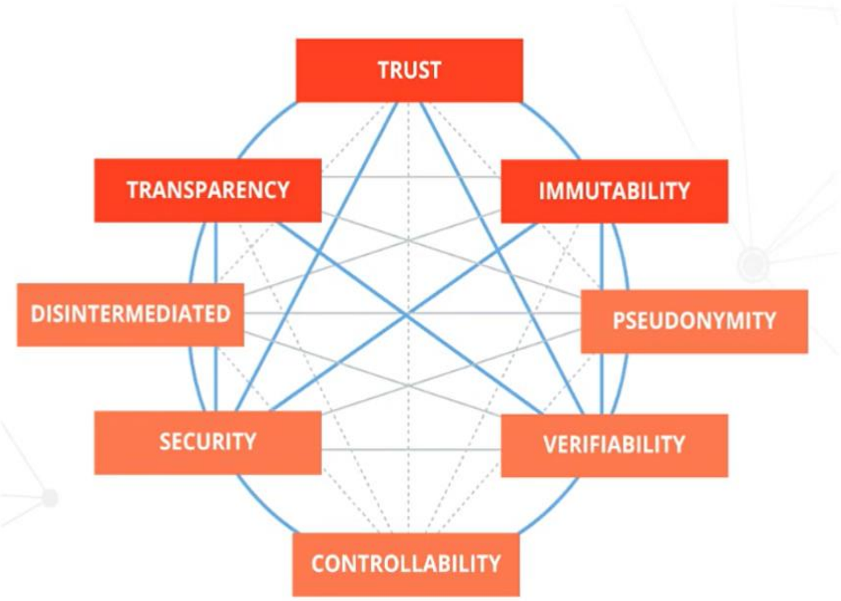


Introduction to Block chain Ethics

- Block chain is a term that refers to a particular class of digital distributed ledger technologies that share records of sequenced information or transactions simultaneously in an immutable and secure manner across a network.
- Block chain does not require a central trust authority to verify information or authenticate transaction rather trust is built into the governance rules with pre-written code defining how actors can behave in the system.
- Each transaction between network actors is strictly verified using computer algorithm against the governance rules. The accepted transactions are then grouped into secure "blocks" of information and linked sequentially in a virtual "chain".

The Key Attributes of Blockchain

- Block chain has a spectrum of key attributes that are highly interdependent and which vary in their relative dominance based on design and implementation.
- All of these key features should be considered as potential attributes since their exact realization depends on the detailed design of a particular block chain system.



- Transparency: Identical copies of the entire record of transactions are available to all particulars at all times. This is often reference to as a distributed ledger. The ledger provide transparency of transactions to anyone with access.
- Trust: Strict governance rules, cryptography and immutability of transactions work together to provide strong security for individuals interacting directly on distributed network without a central trusted authority.
- Immutability: Immutable transactions recorded on a block chain cannot be changed or removed. To change a transaction on the block chain, a new transaction needs to be added to reverse the effects of the original.

- Pseudonymity: Using public and private key systems, participants have a public facing digital “address” that is not publicly associated to them, but over which they exercise unique control.
- Verifiability: Transactions on a block chain are immediately auditable in real time. As an immutable and sequenced digital ledger, a block chain allows the complete record of transaction to be directly verified.
- Controllability: The tracking of individual assets uniquely on a block chain allows an individual to exercise effective and exclusive control over data or digital assets.
- Security: The use of encryption algorithm combined with the disaggregation of data across a distributed network of nodes provides security against attempts to destroy or change the record of transactions.
- Disintermediation: Using direct transactions, block chain technology can streamline processes by cutting out unnecessary intermediaries and process steps, as well as reduce the risk of errors that usually come with extra transactions in a system.