

ELEC2544 Introduction to electronic commerce and financial technology

AI in Fintech

Dr. Wilton Fok

Application of AI in FinTech

Fintech innovation in

- ▶ Artificial intelligence and machine learning
 - ▶ Automating processes
 - ▶ Improving decision-making
 - ▶ Enhancing customer experience

Source: <https://www.forbes.com/sites/alexlazarow/2022/12/10/the-future-of-fintech-according-to-ai/?sh=4a5074833336>



Introduction

Almost 90% of Hong Kong banks are adopting AI

TO WHAT EXTENT are banks in Hong Kong adopting AI technology?

89%



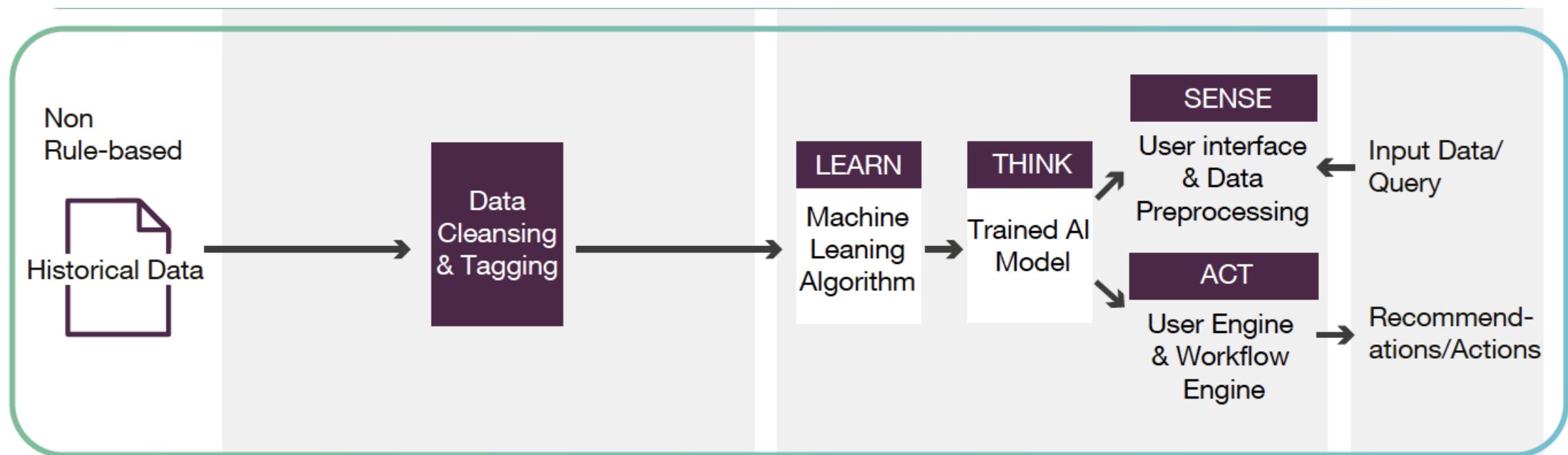
of respondents **have adopted or plan to adopt** AI applications.

Source: [https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Artificial_Intelligence_\(AI\)_in_Retail_Banking.pdf](https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Artificial_Intelligence_(AI)_in_Retail_Banking.pdf)



Introduction to AI

- AI enables computers to learn, sense, think and act.



- Source: https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Whitepaper_on_AI.pdf

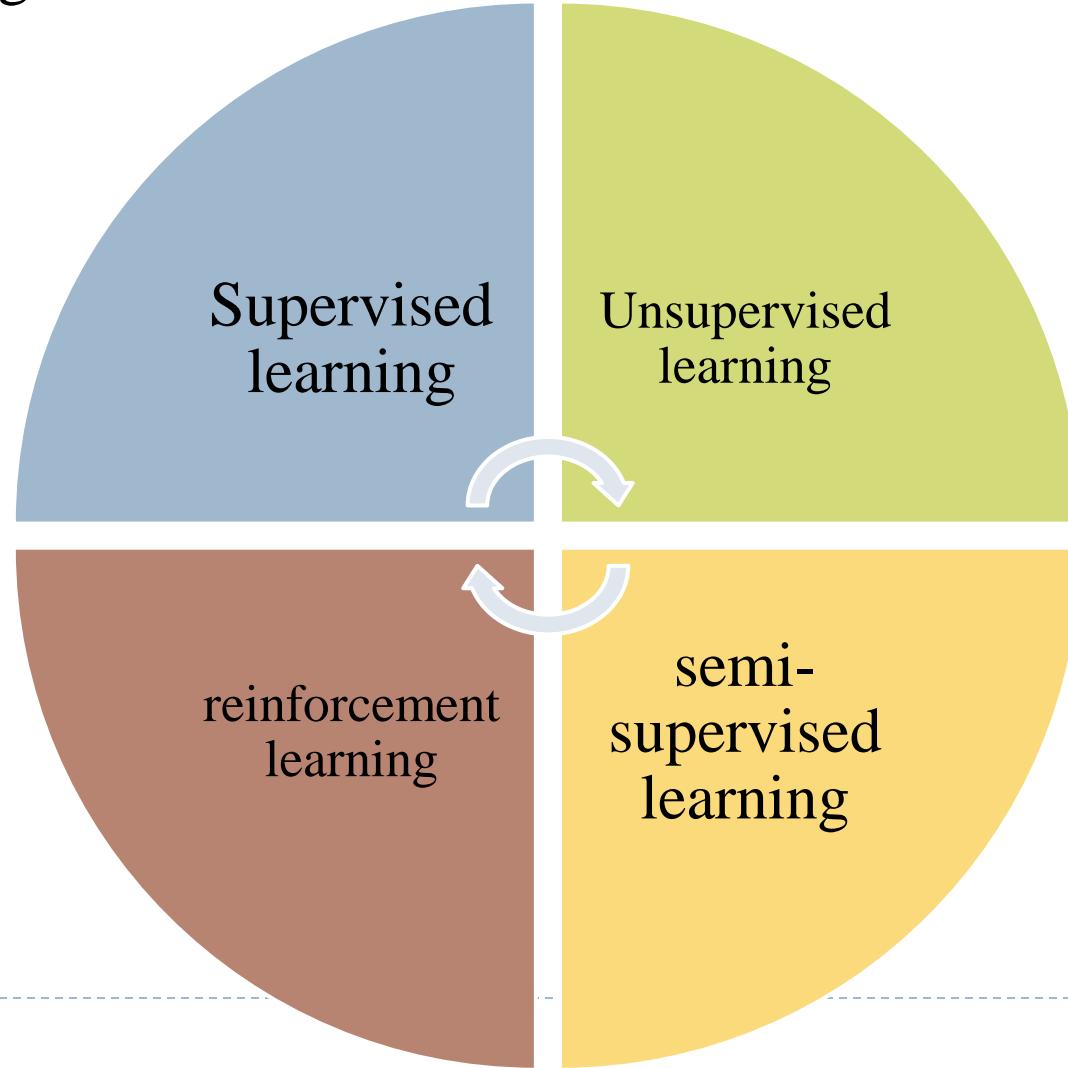
Introduction to ai

- ▶ The core of AI are the 'learn and 'think' components
 - ▶ learn automatically from inputs to make predictions, decisions or recommendations.
- ▶ The machine learning (ML) enables the learn capability of AI.
- ▶ ML models are trained with historical data.
- ▶ Trained ML models can perform predictions or make decisions according to the data patterns observed from the historical data.



Introduction to ai

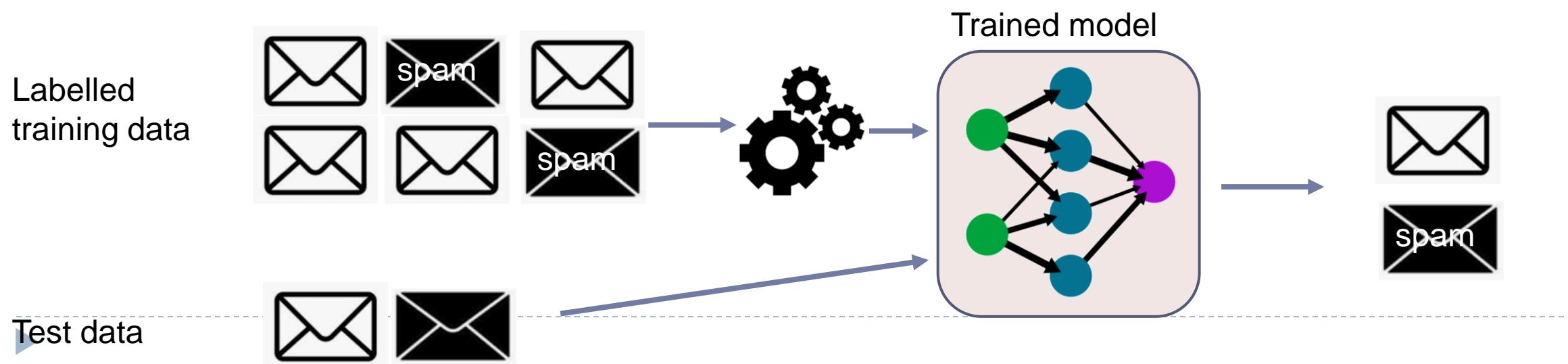
- ▶ Four types of machine learning algorithms:



Introduction to ai

▶ Supervised learning

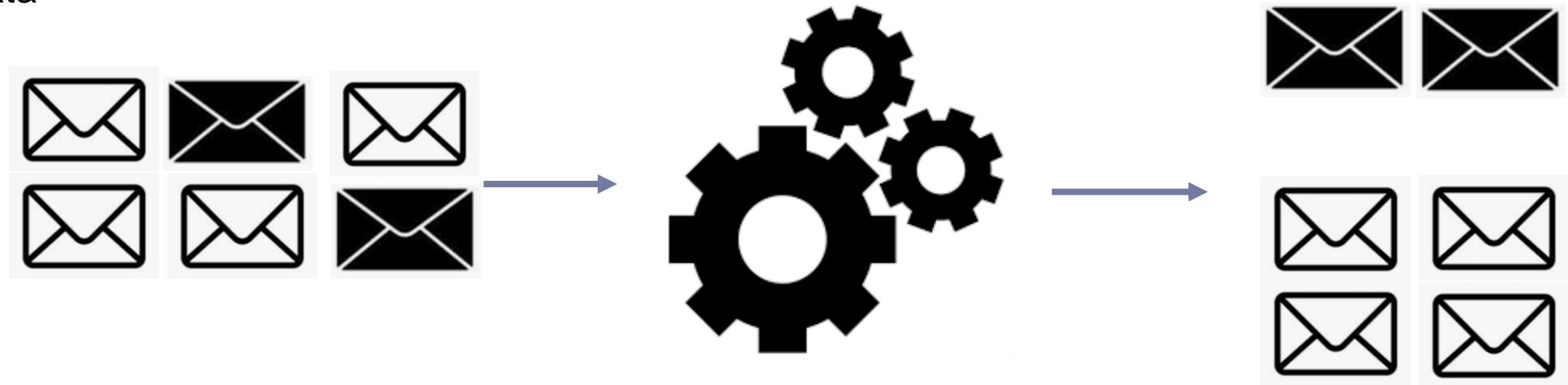
- ▶ humans train a model using labelled data, which means the training data are already tagged with the target output
- ▶ Example: learn which emails are classified as spam by first having a real person label emails to identify those which are spam, then the model predicts the output with test data



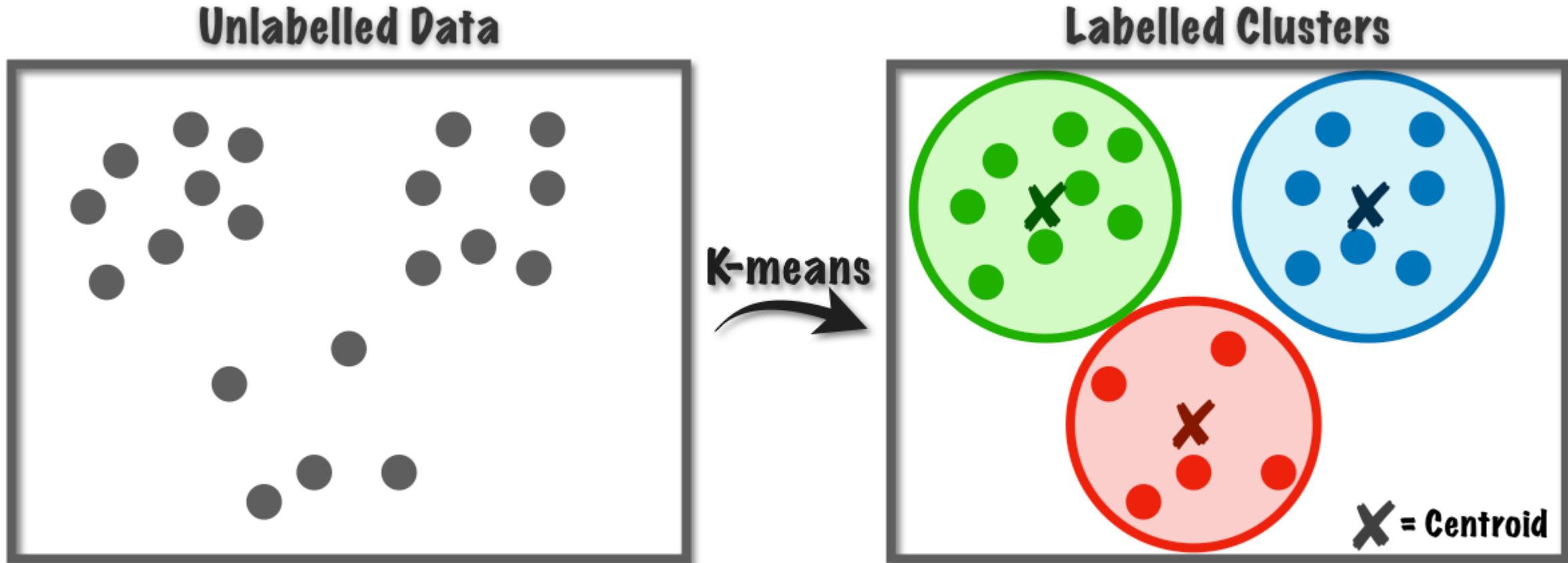
Introduction to AI

- ▶ Unsupervised learning
 - ▶ identifies patterns in a set of unlabelled input data automatically
 - ▶ Example: group common emails into clusters with similar patterns

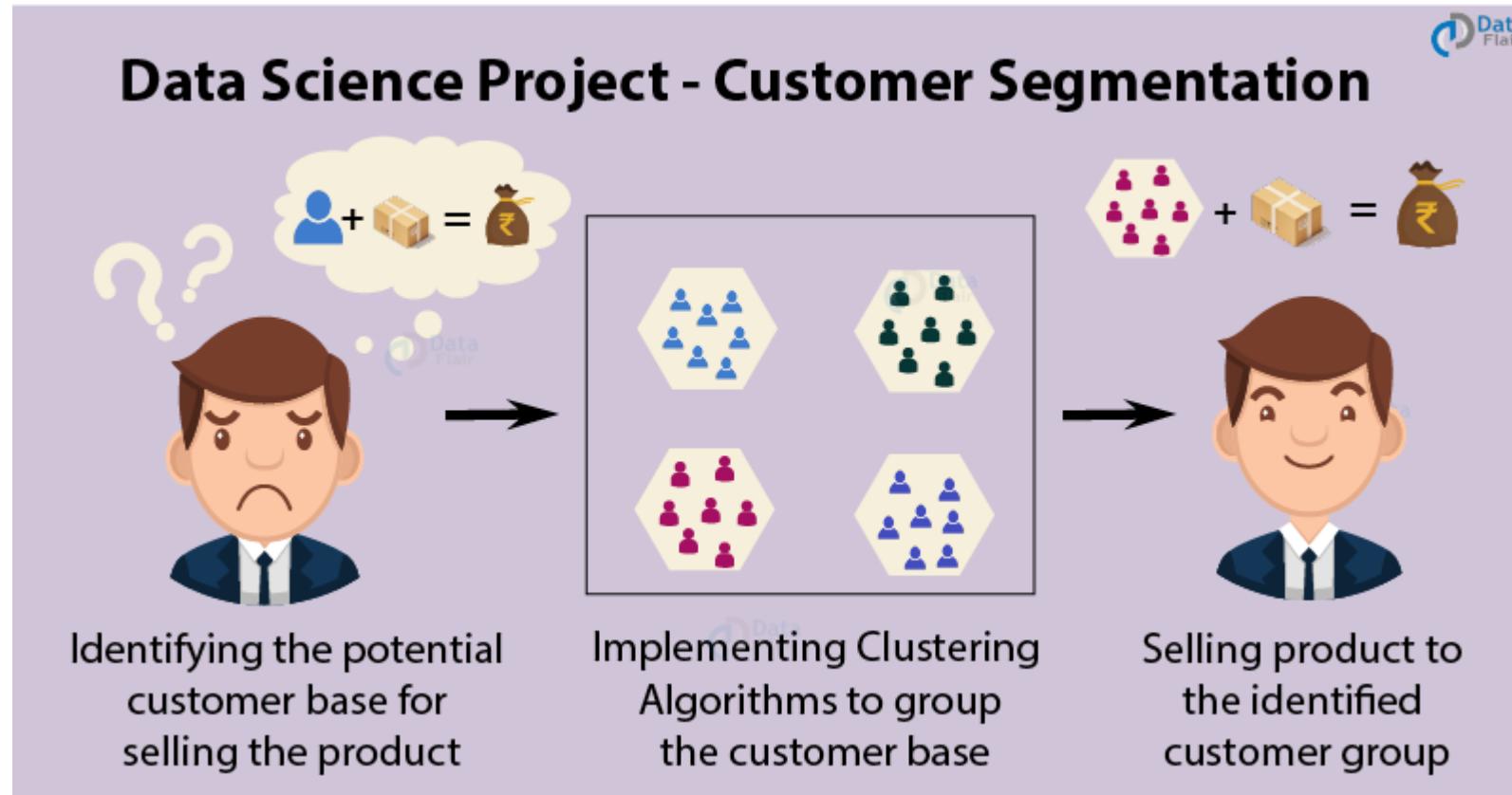
Unlabelled data



Unsupervised learning

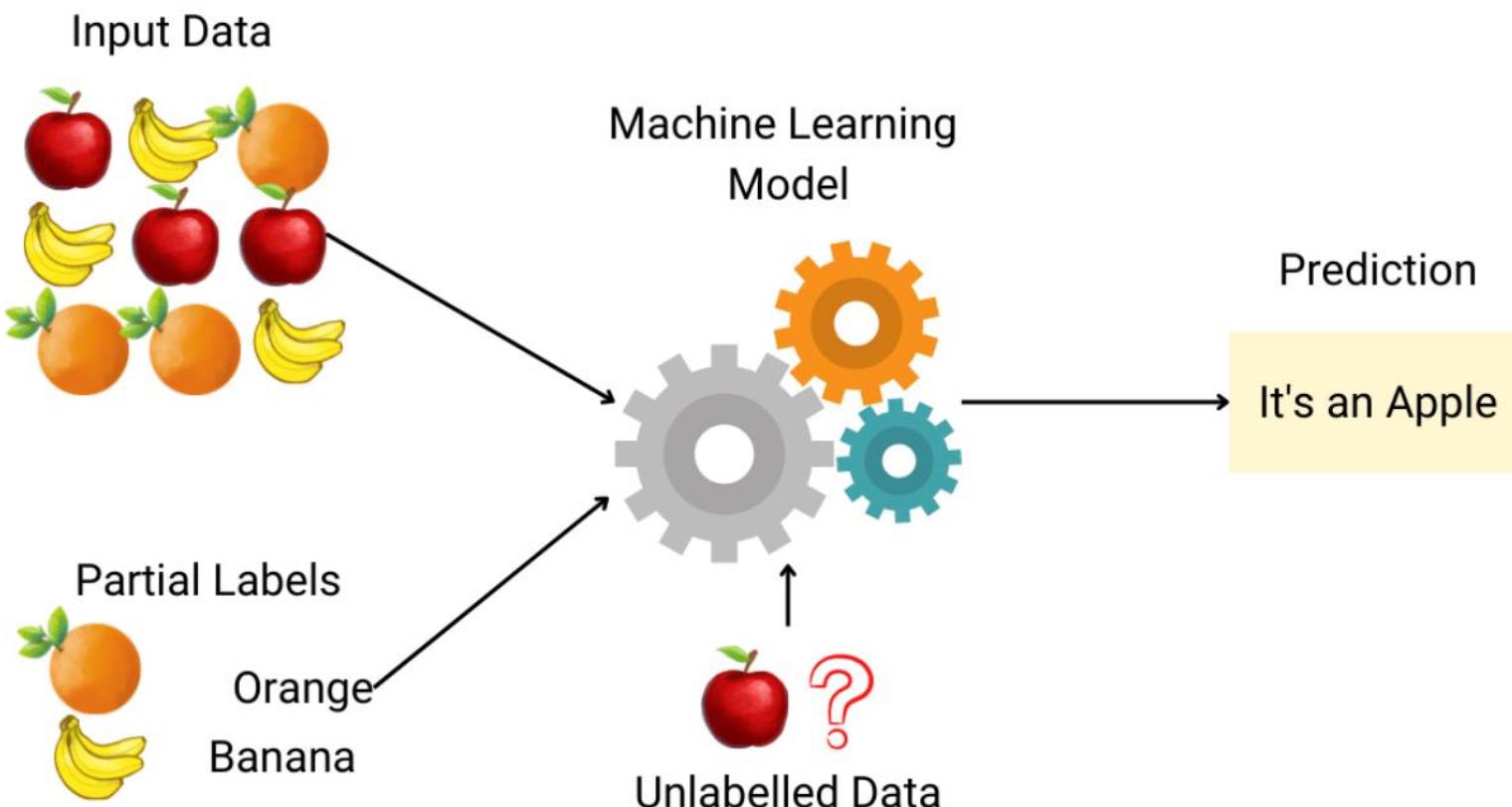


Clustering for customer segmentation



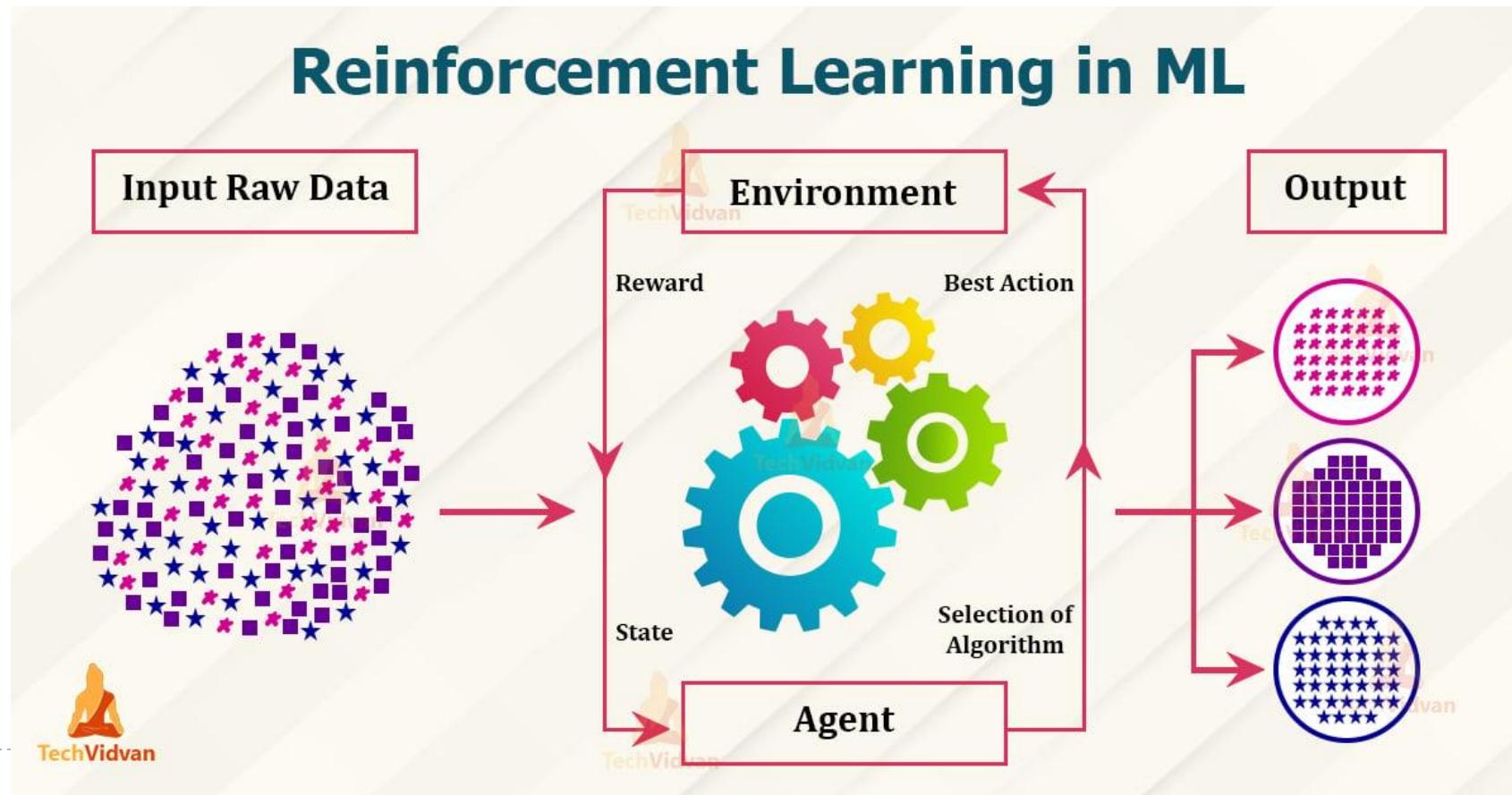
Introduction to AI

- ▶ Semi-supervised learning
 - ▶ data sets are only partially labelled
 - ▶ combines supervised and unsupervised learning algorithms

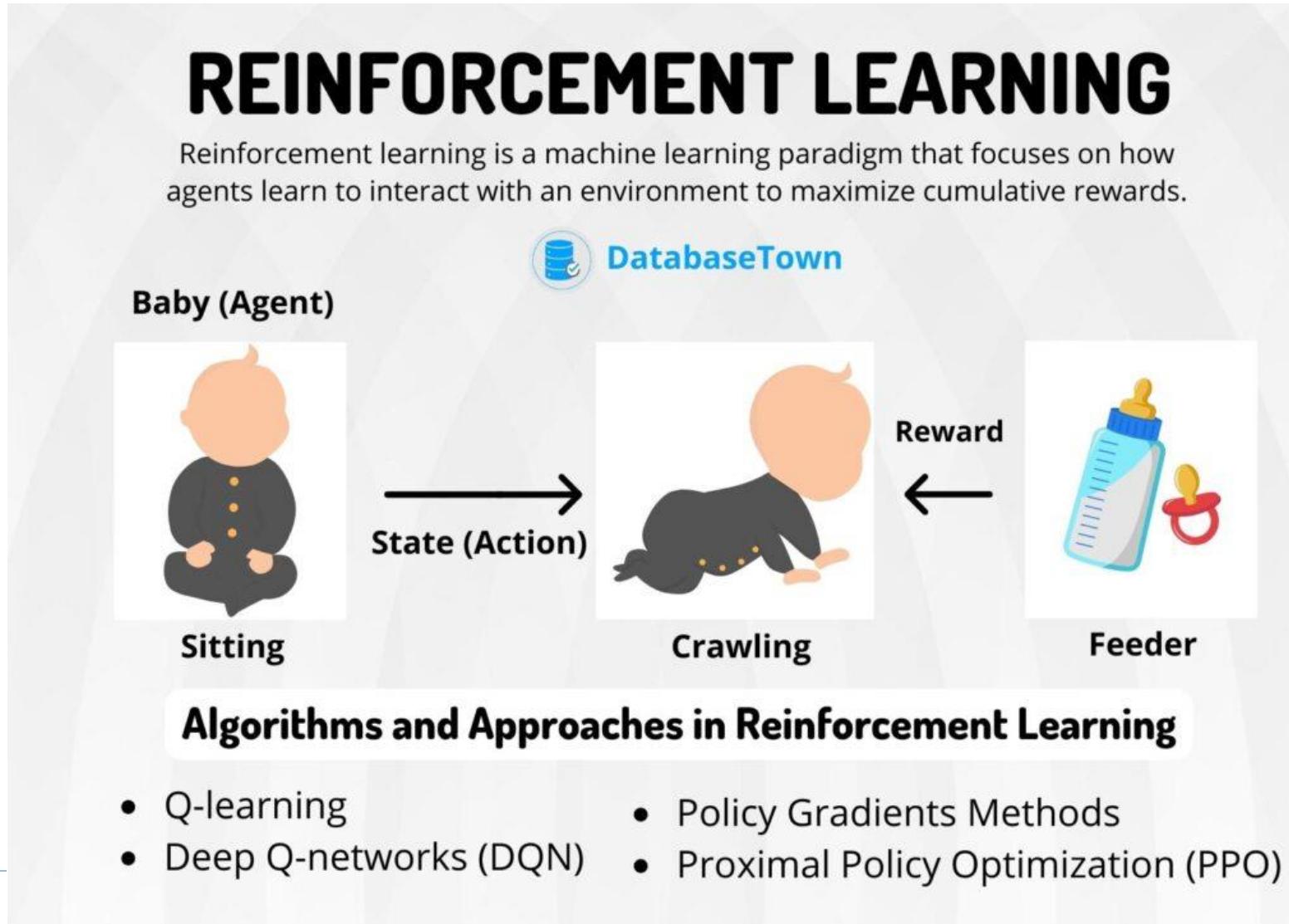


Reinforcement learning

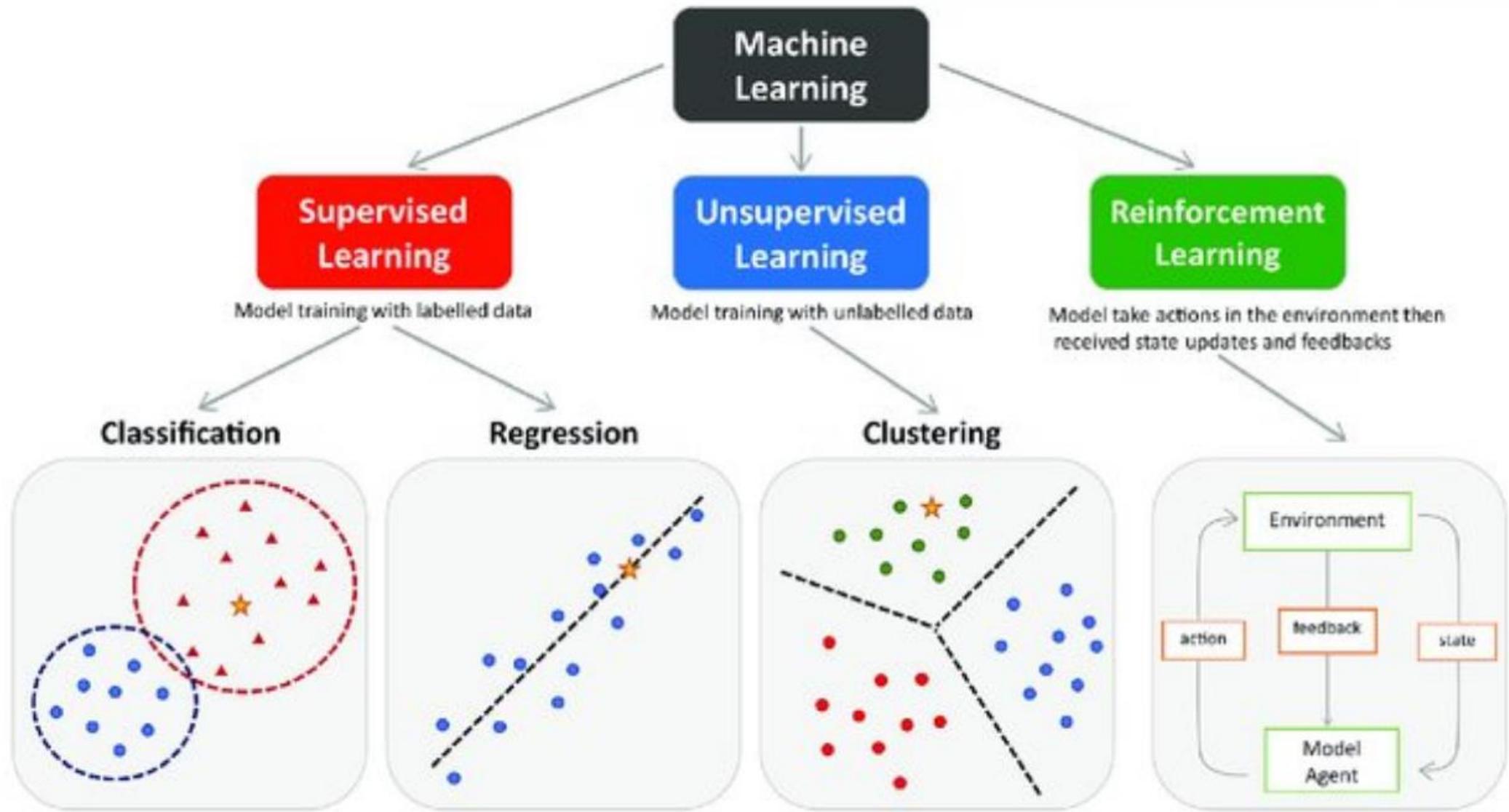
- ▶ teaches machine to learn based on feedback from its environment
- ▶ Learn from mistake



Reinforcement learning

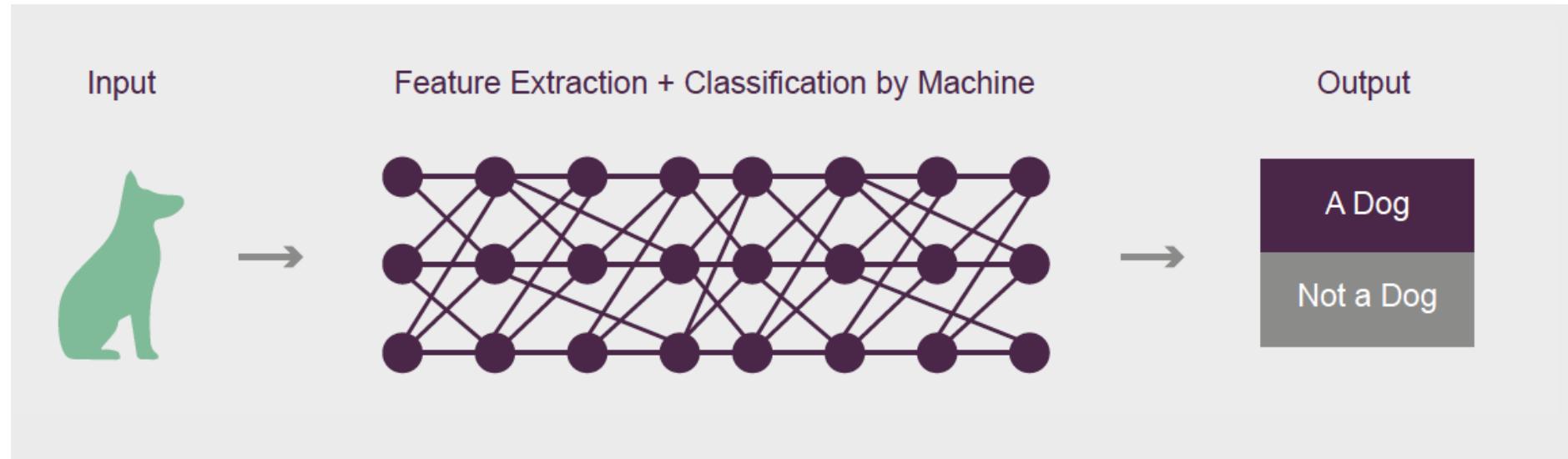


Summary of Machine learning

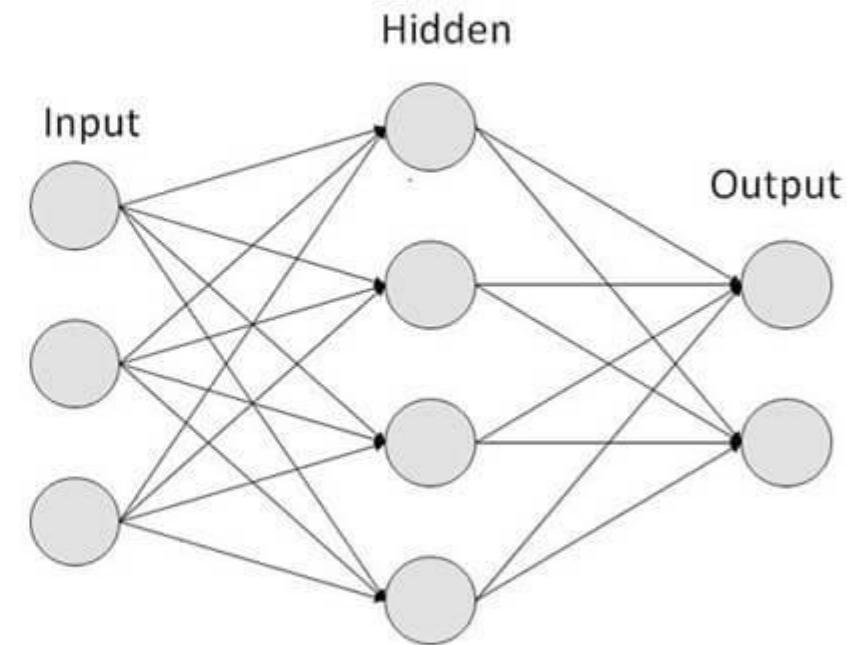
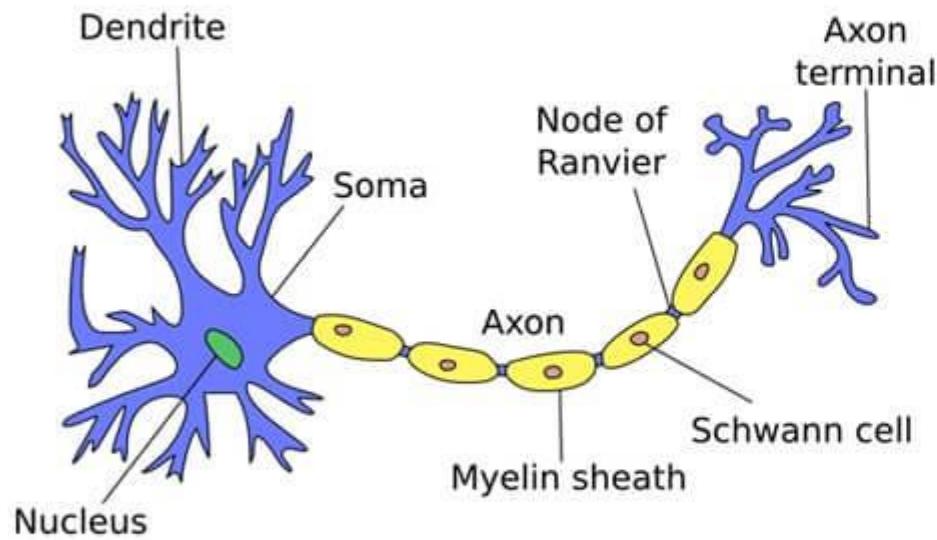


Introduction to AI deep learning – for pattern recognition

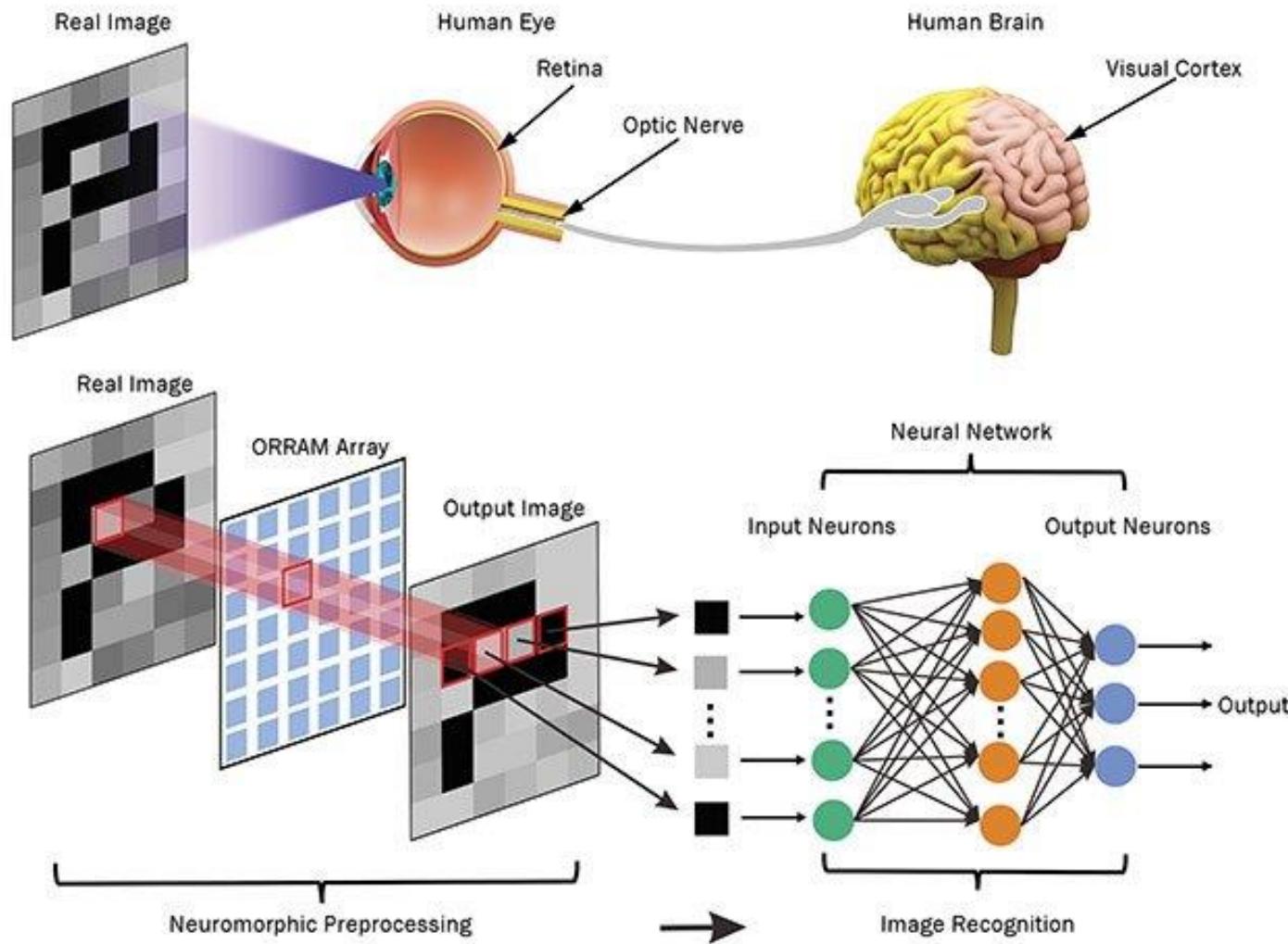
- Deep learning is a subset of machine learning.
- Neural networks (NNs) are the building blocks of deep learning models.
- NNs are inspired by the structure of the brain.



Neutral Network system

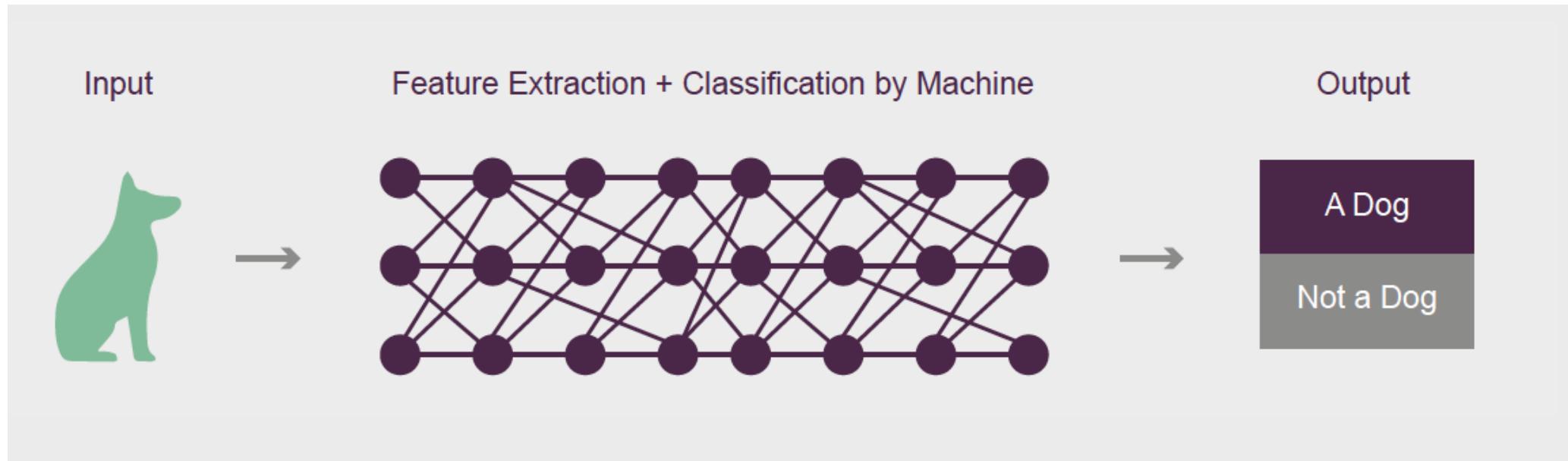


Compare human and AI vision



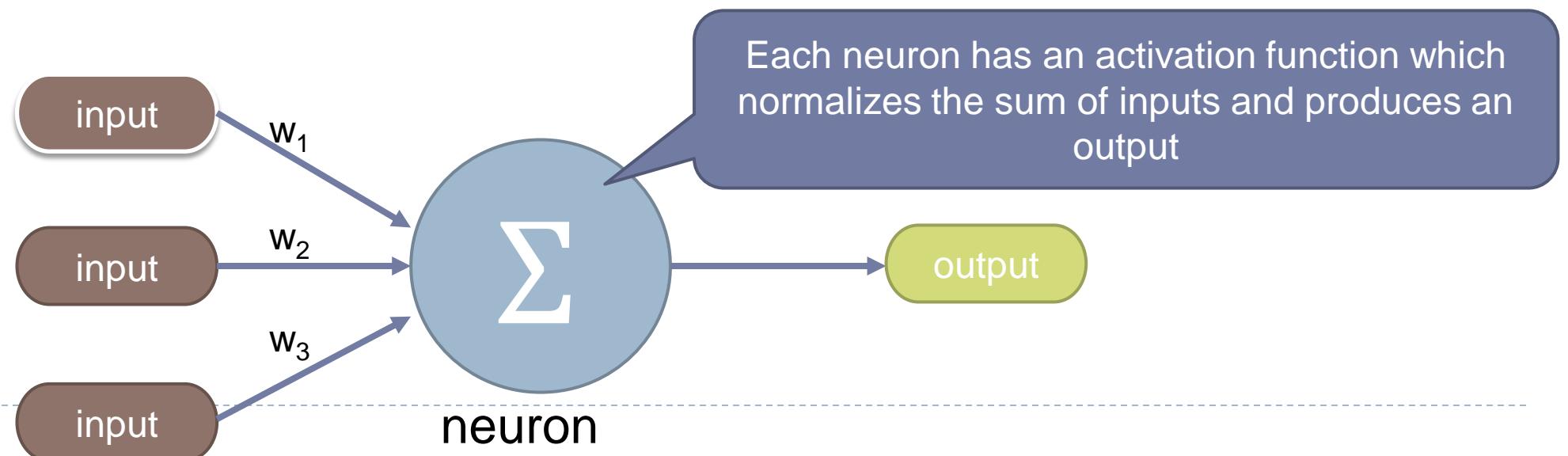
Introduction to ai deep learning

- Through the hidden layer architecture formed by connecting neurons, deep learning extracts high level features and learns classification incrementally with each additional layer of neurons.



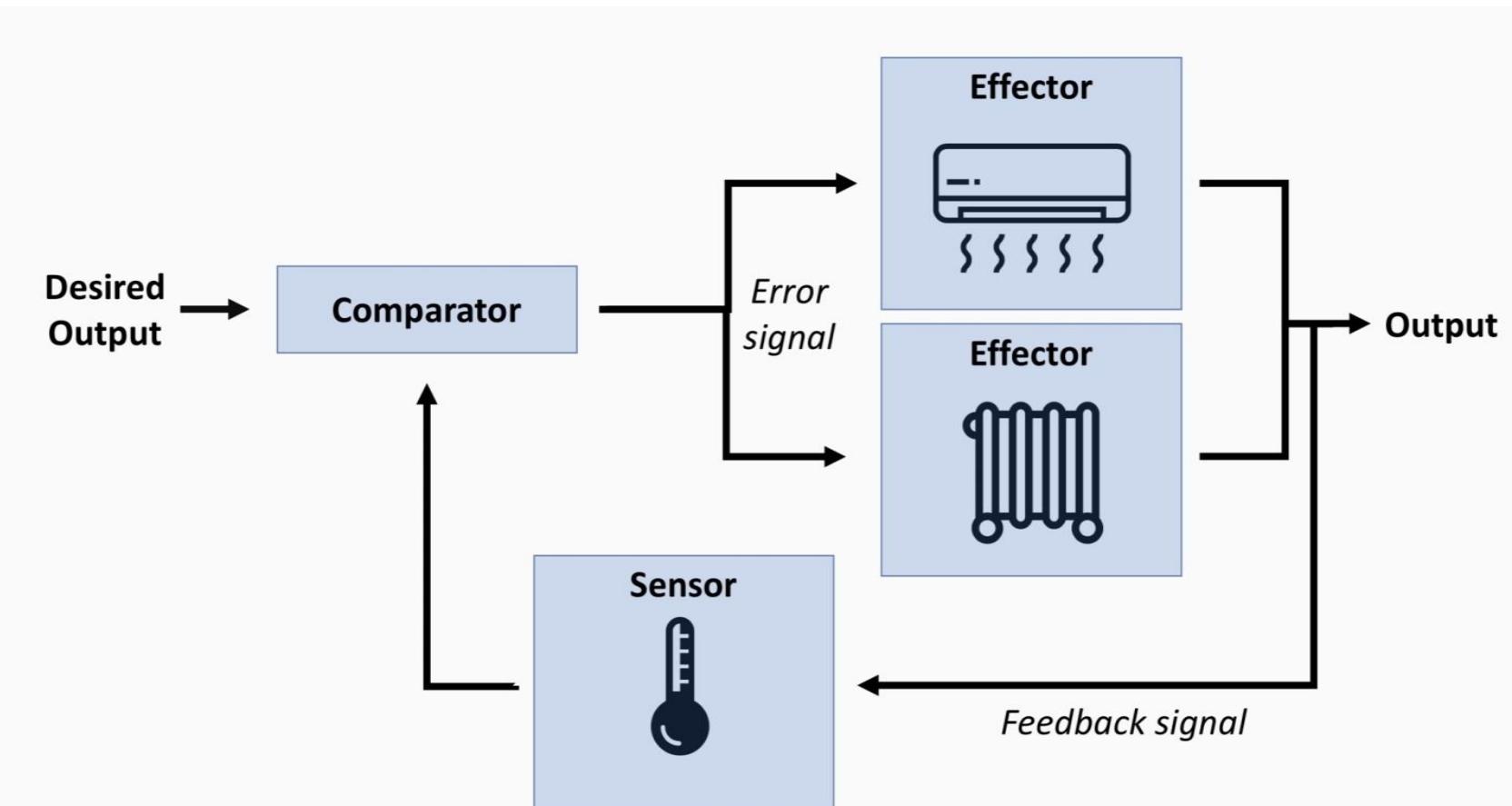
Introduction to AI deep learning

- The basic unit of computation in a neural network is a neuron.
- A neuron calculates an output based on input from other neurons or from an external source.
- The basic idea of ANN is to train the model with a large number of examples to tune the weights so that the model gives an accurate enough output.



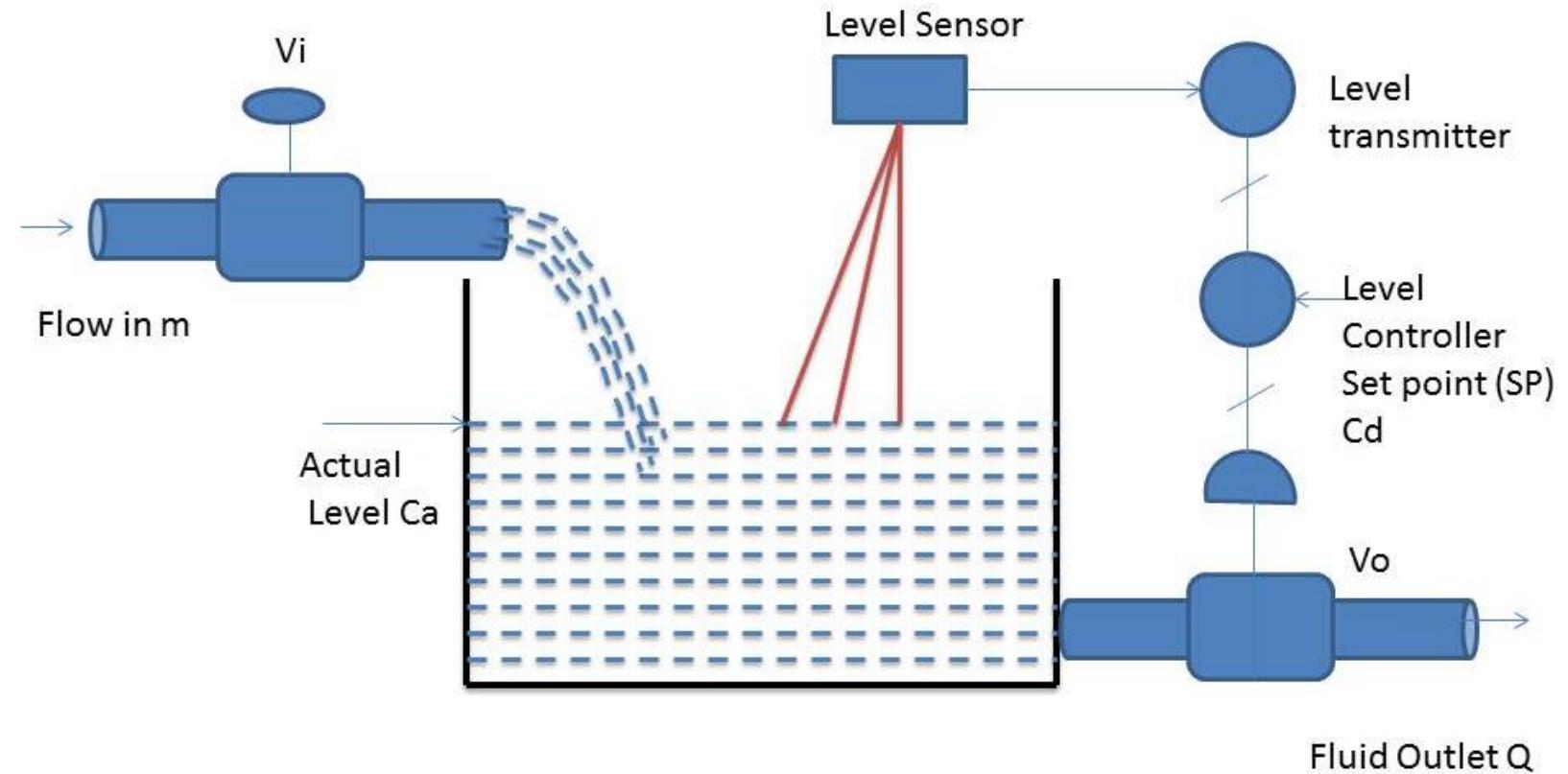
Foundation knowledge of AI

▶ Feedback system



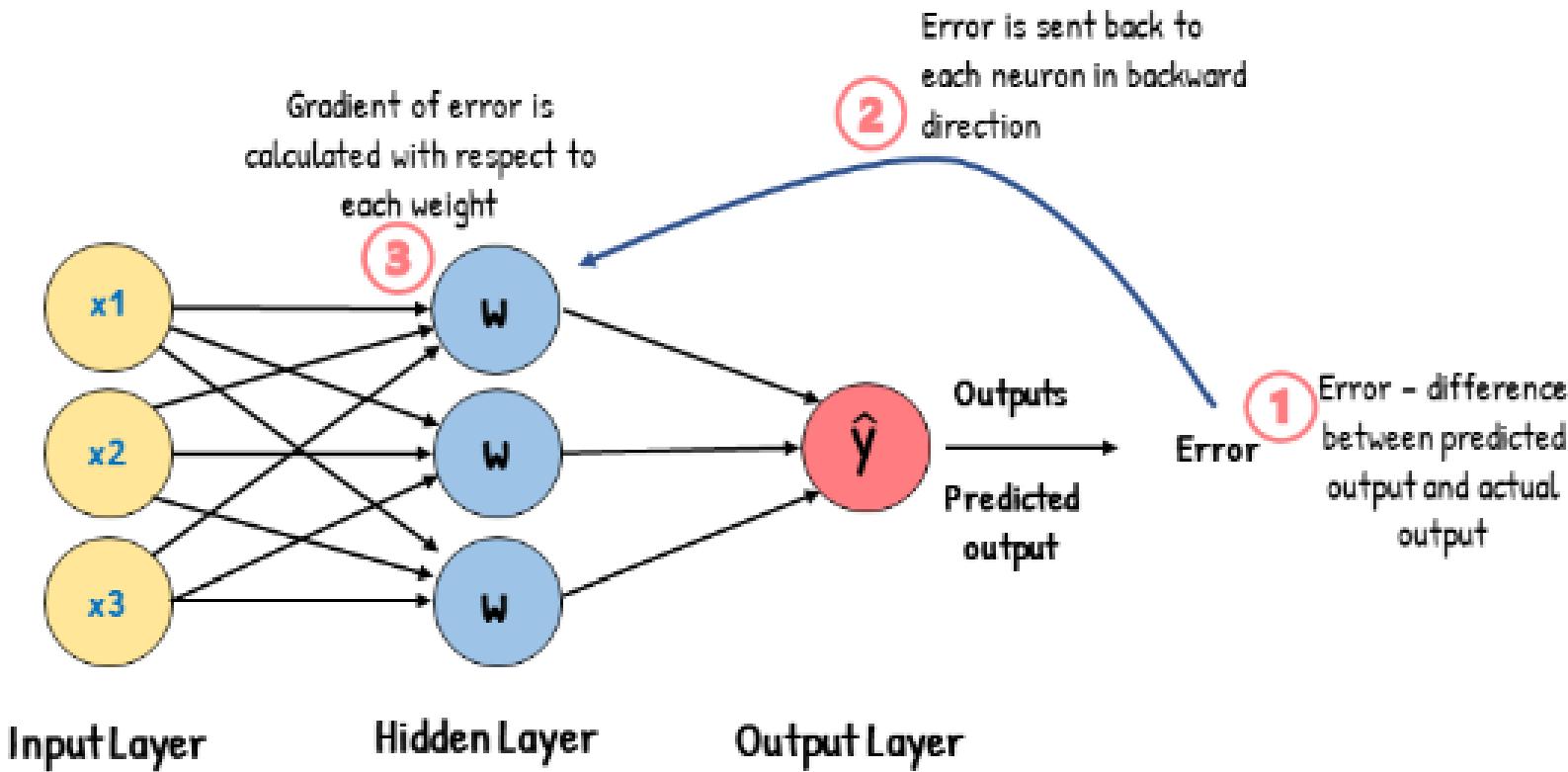
Feedback control for level control

- ▶ Simple IF THEN ELSE logic

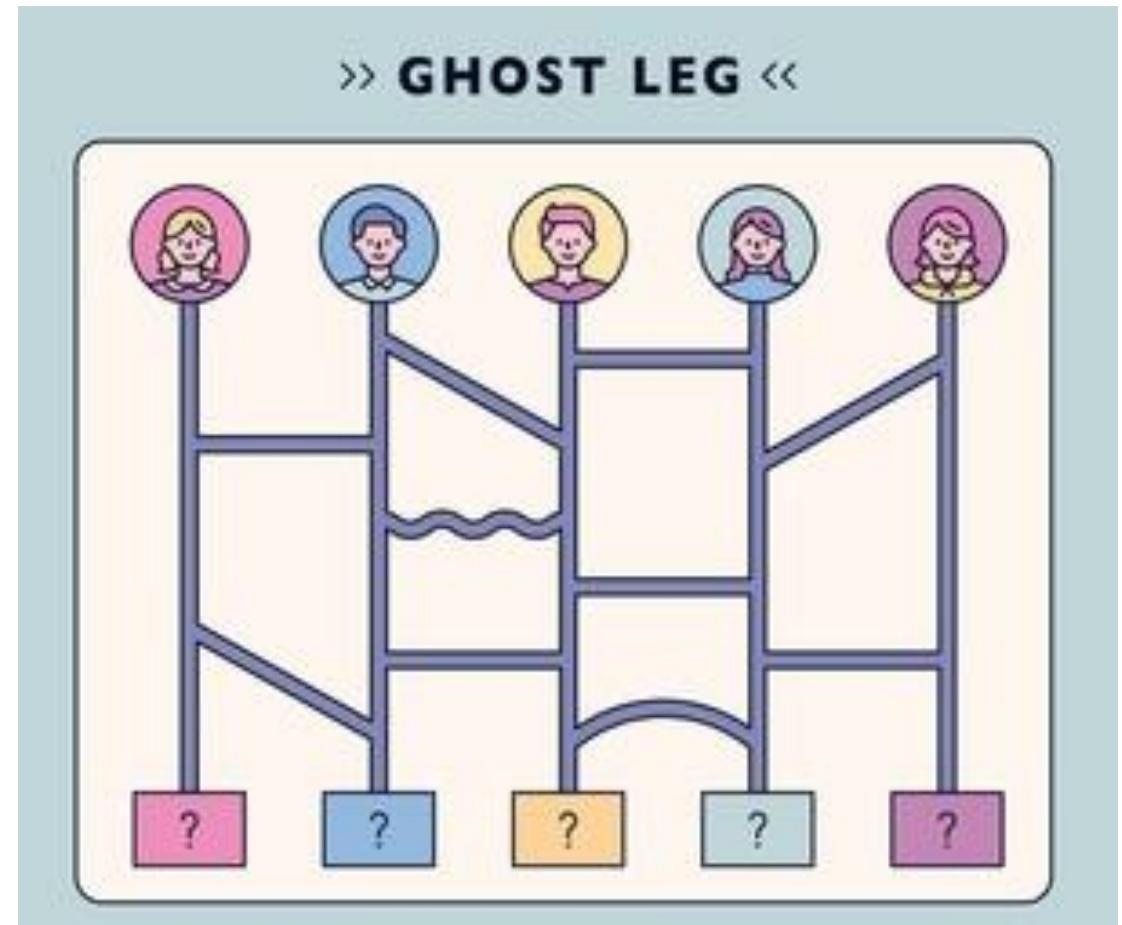
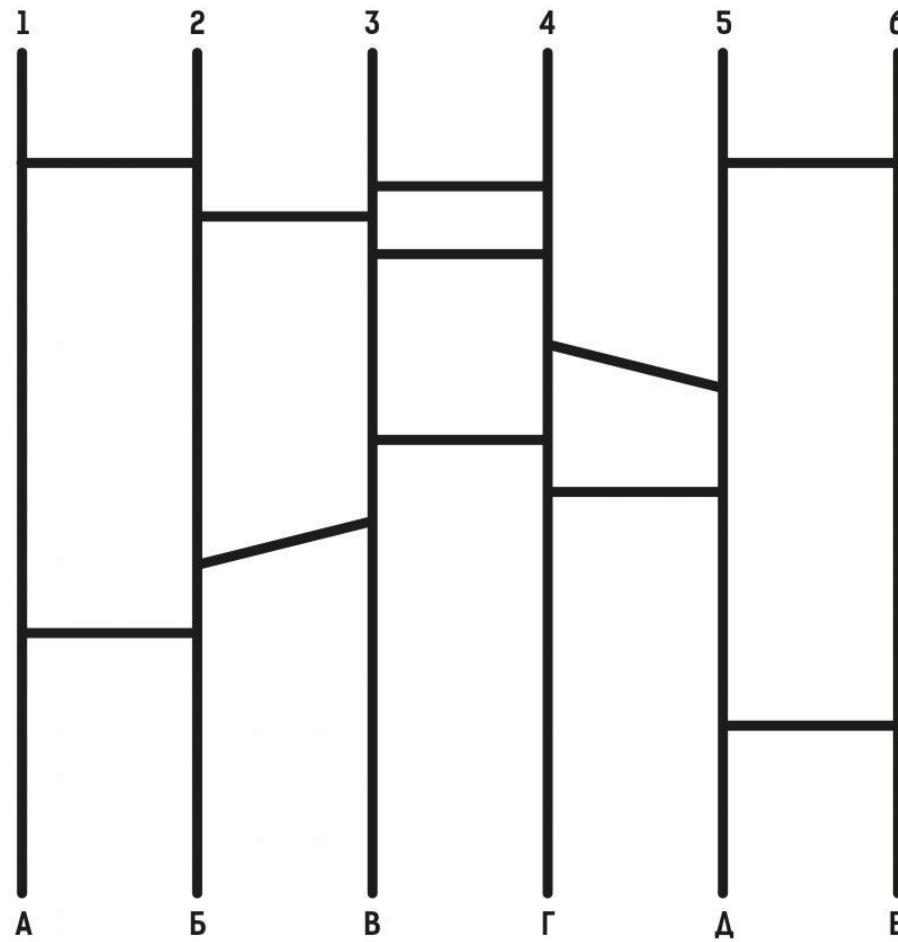


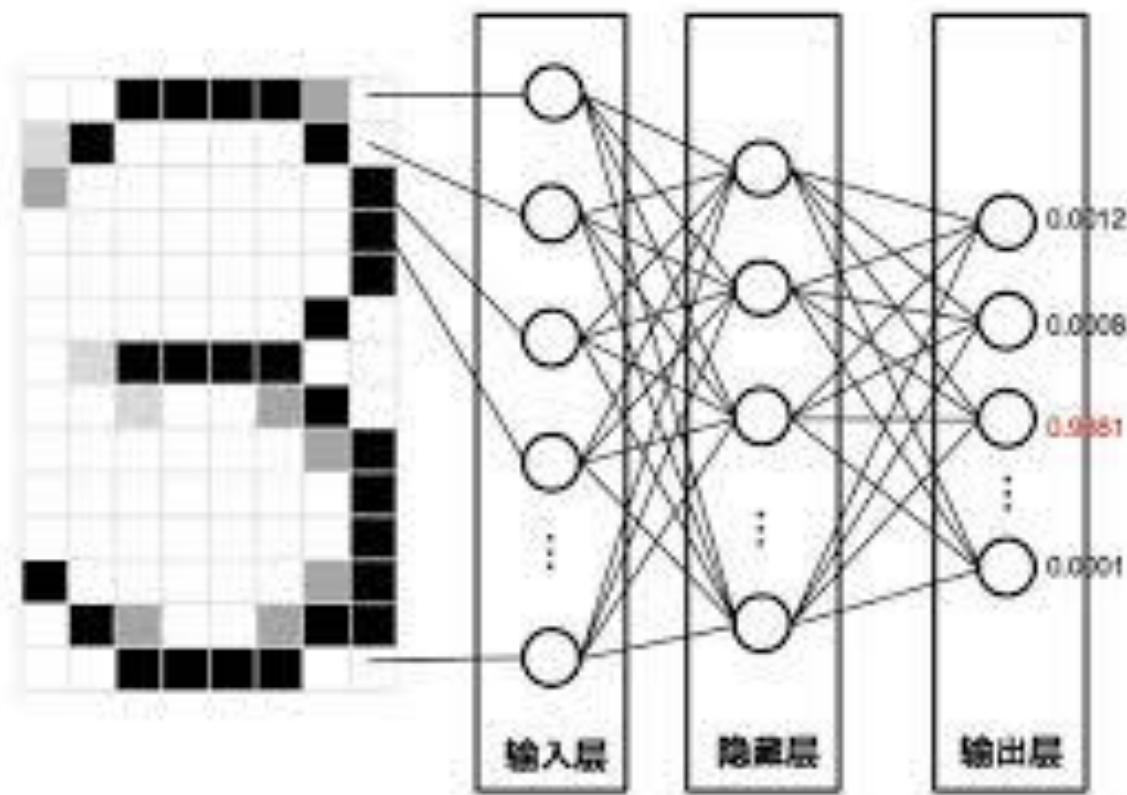
Back propagation in Neural Network = Feedback in Control system

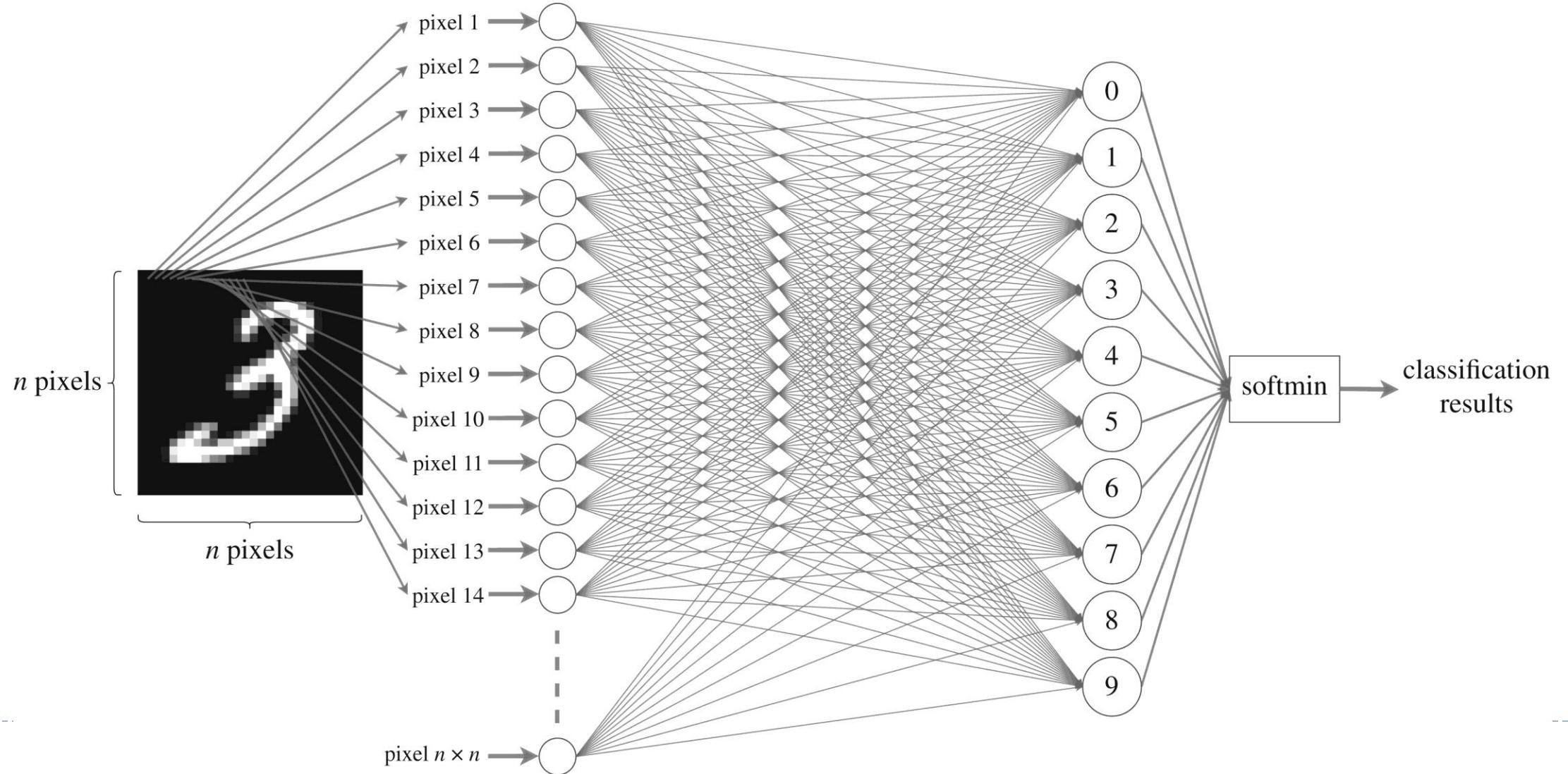
Backpropagation



Like a ghost leg diagram - A mapping model







Animation demo

▶ <https://youtu.be/3JQ3hYko51Y>

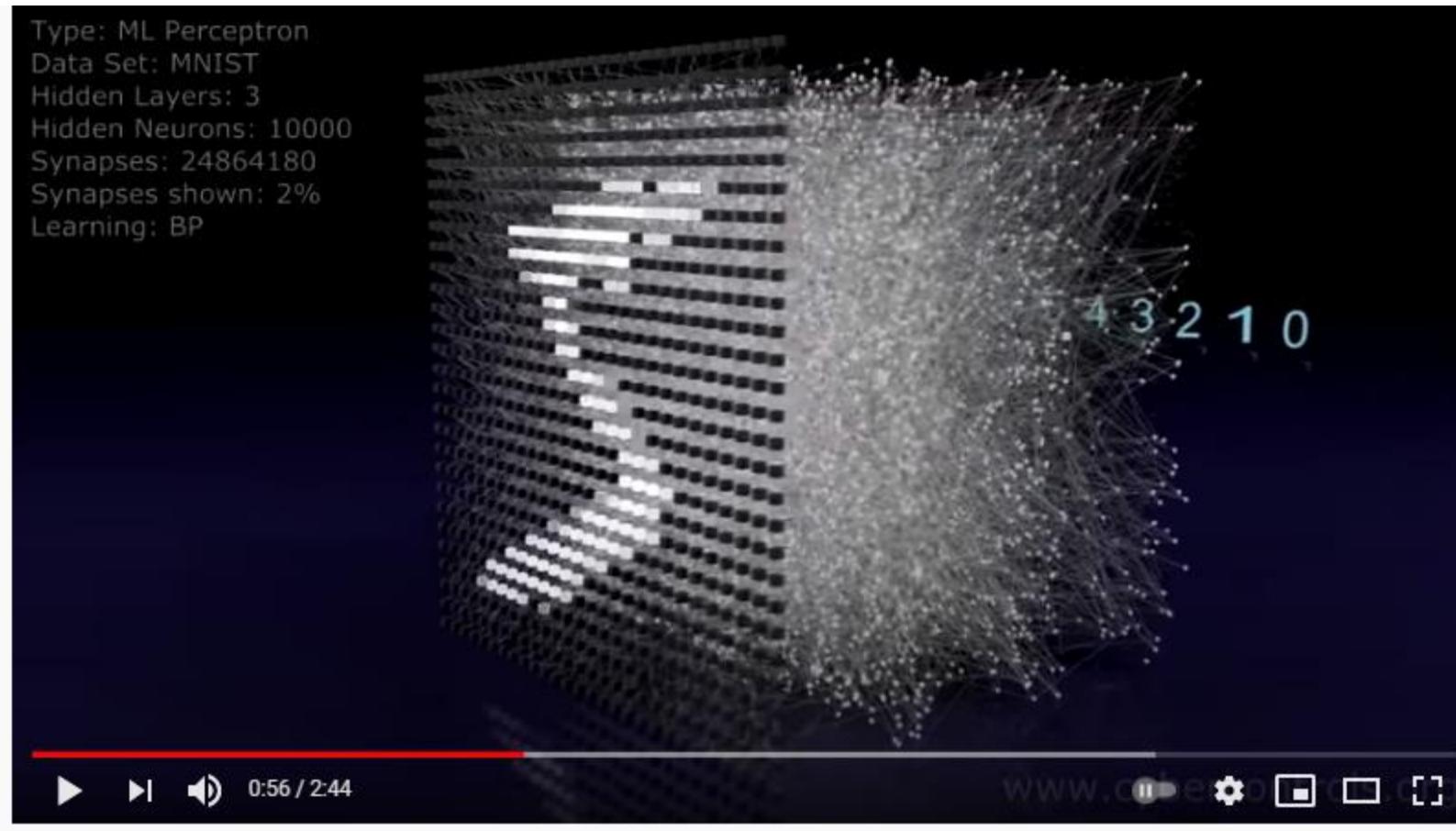


Image classification

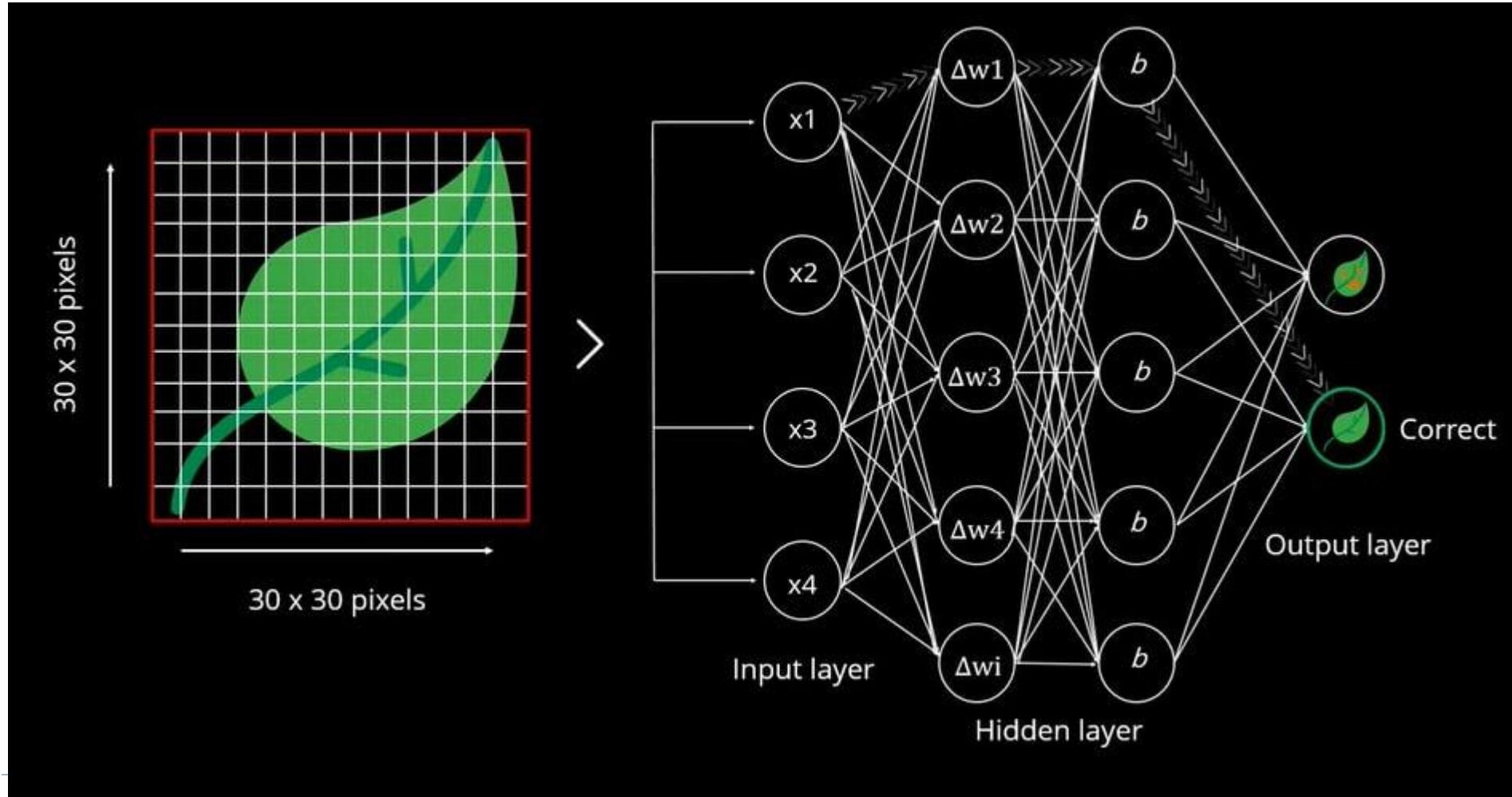
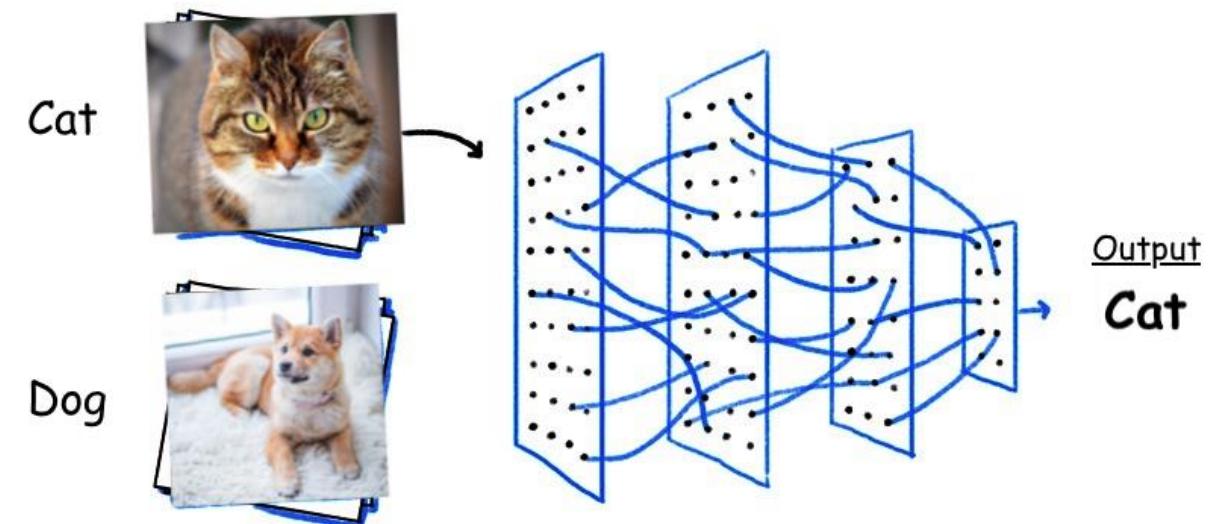
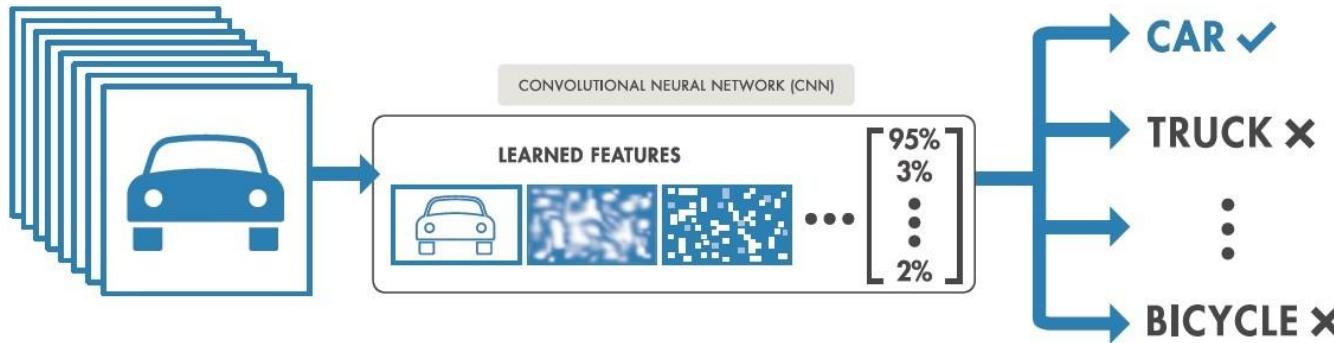


Image Classification



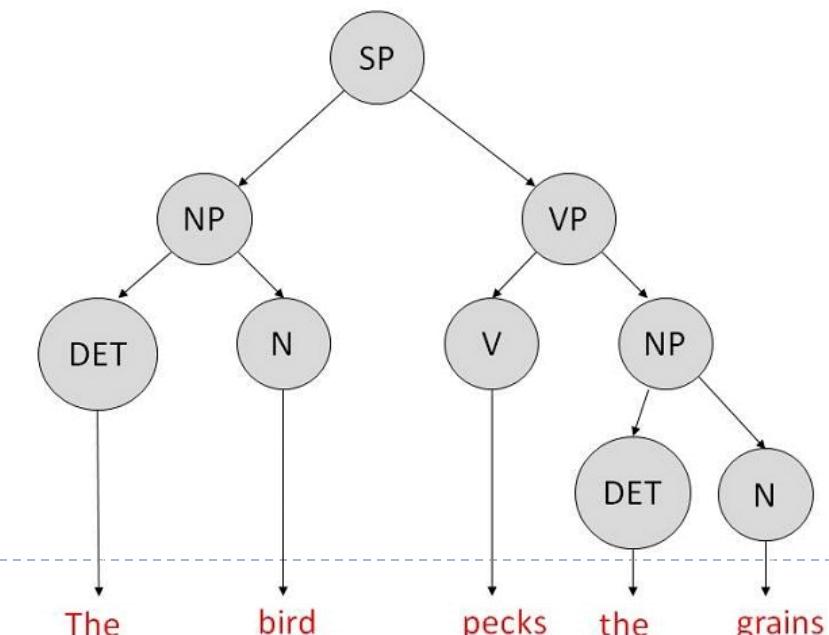
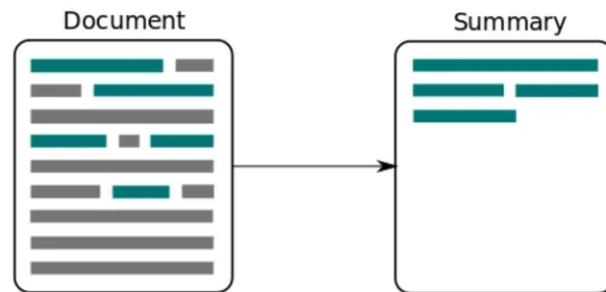
Application of AI pattern recognition in FinTech

- ▶ Image pattern
 - ▶ OCR / text recognition in cheque / contract
 - ▶ Facial recognition for Account holder ID (two factor Authentication)
- ▶ Other non-image pattern
 - ▶ E.g. transaction pattern
 - ▶ Contract renewal/termination pattern
 - ▶ Spending pattern analysis (e.g. Ali Pay)
 - ▶ Text pattern (NLP)



Other AI process: Natural language processing (NLP)

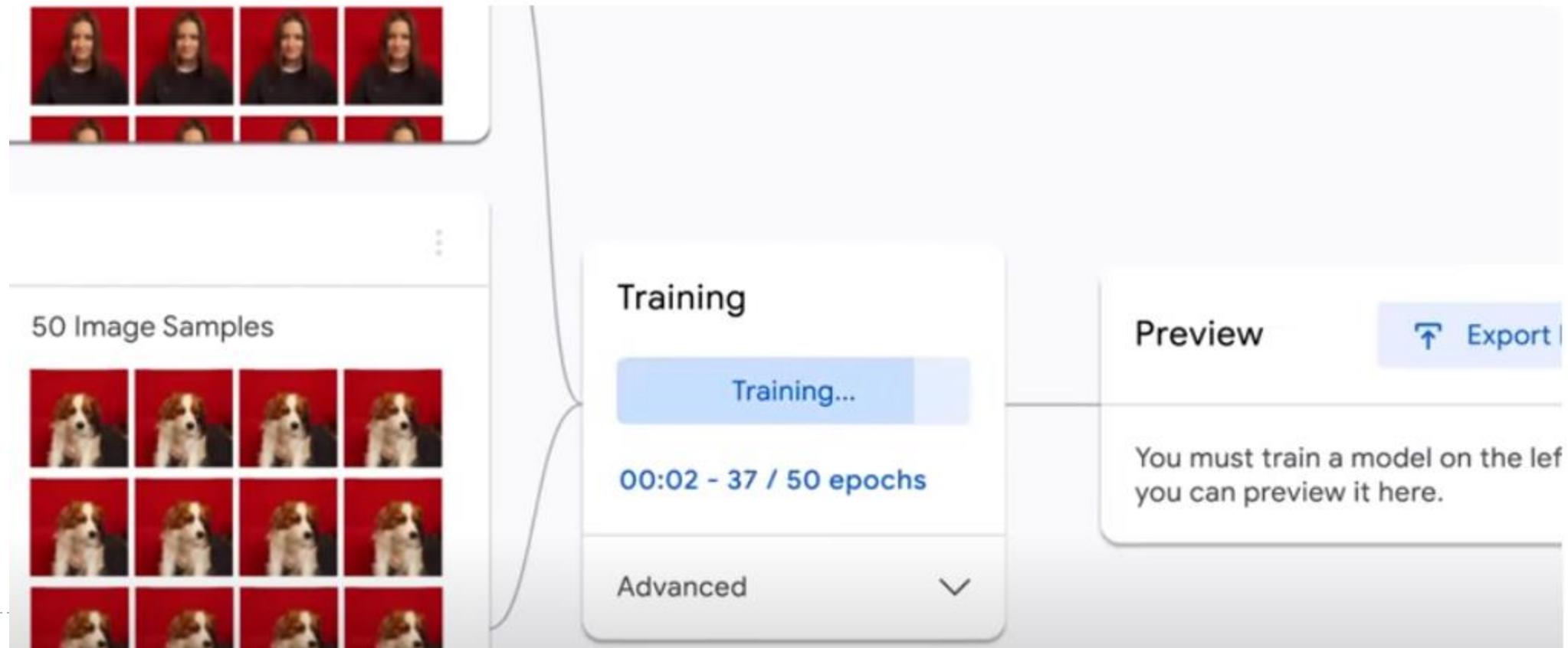
- ▶ Natural Language Processing (NLP) is a branch of AI that aids computers to understand natural human language.
- ▶ NLP has the ability to recognise linguistic patterns and interpret meaning in languages through the use of linguistic analysis tools such as
 - Part-of-speech tagging: labelling each word with its part of speech (for example, noun, verb, adjective, etc.)
 - Automatic text summarization



Training an AI model for pattern recognition in an easy way

▶ Google Teachable machine

▶ <https://www.youtube.com/watch?v=T2qQGqZxkD0>



Application of AI in FinTech

How AI can serve FinTech?

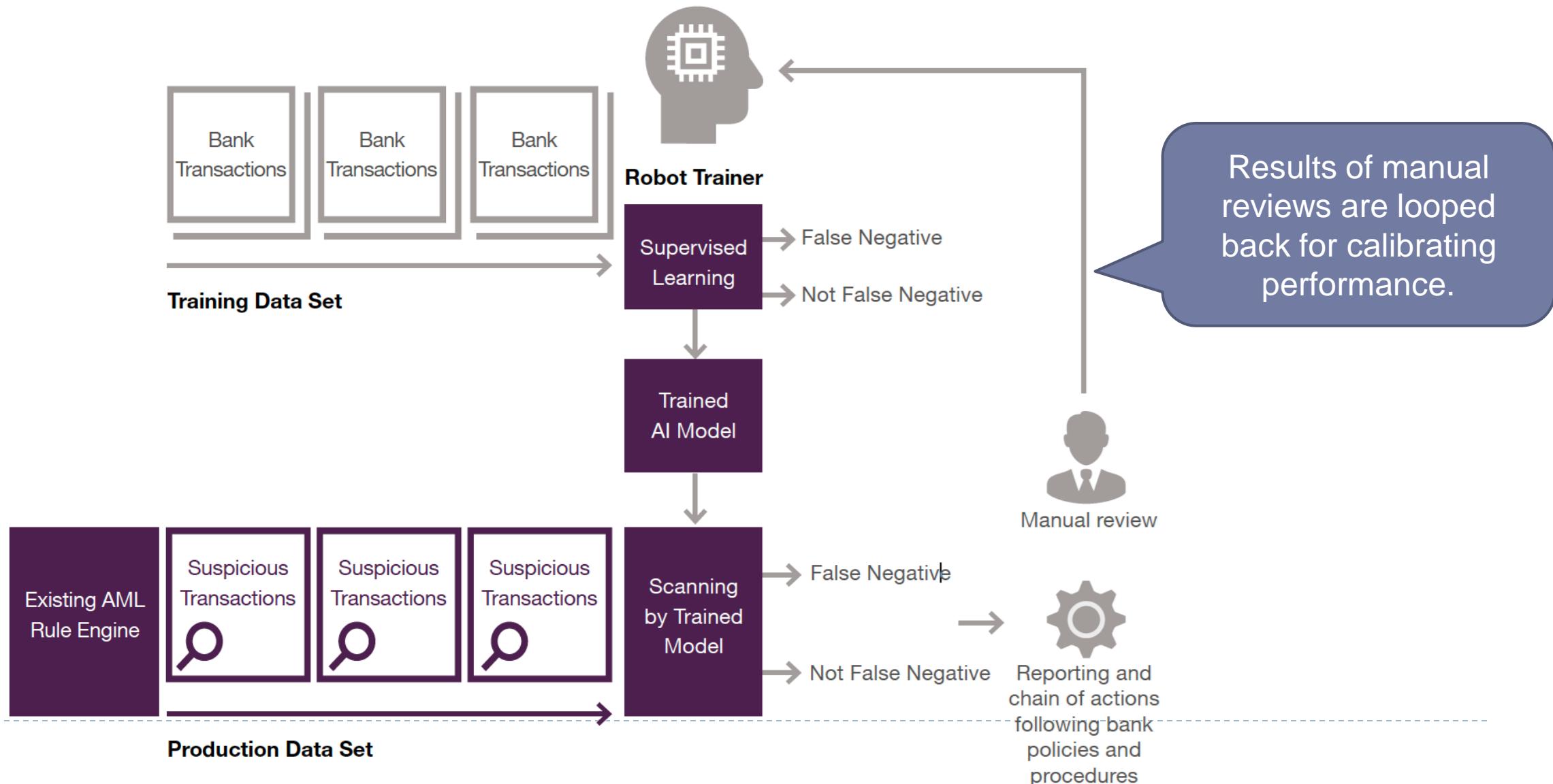


AI Application example 1: Anti-money laundering

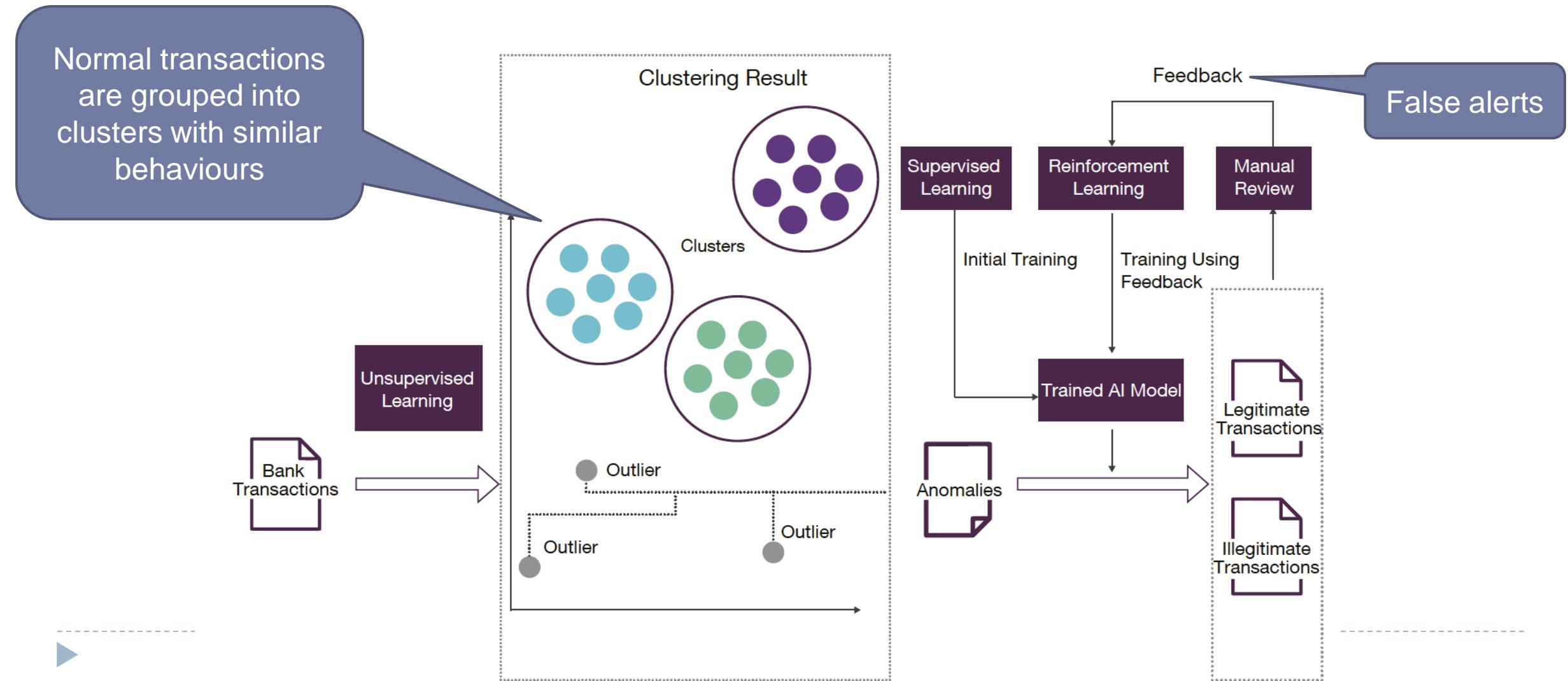
- ▶ Criminals use money laundering to make illicit funds appear to have a legitimate origin.
- ▶ Anti-money laundering aims at uncovering their efforts.
- ▶ Traditionally, significant human effort is required to determine whether any of the transactions identified as suspicious are in fact false negatives (transactions identified as suspicious but which are actually not).
- ▶ Machine learning can be applied to identify false negative money laundering transactions and save human effort.



Application 1: Anti-money laundering



Application 1: Anti-money laundering



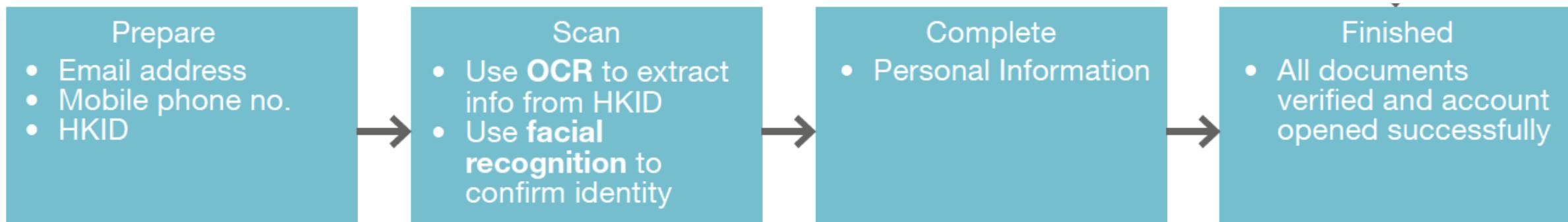
Application 2: Remote client on-boarding – for improvement of customer experience

- ▶ The process of opening a bank account involves paper-intensive manual processes.
- ▶ Remote client on-boarding uses machine learning and AI for fraud detection.
 - ▶ save significant processing time and costs by digitalizing end-to-end processes
 - ▶ customers can spend more time on the actual banking services they require
 - ▶ banks can channel human resources towards performing complex banking transactions and higher value-added activities



Application 2: Remote client on-boarding

- Extracting ID information with machine learning enhanced OCR (optical character recognition)
 - identify the expected position of words based on the type of document recognised
 - extract words from the ID document and validate these against the user's input



Application: Remote client on-boarding

- Verifying customers' identity using facial recognition and biometric liveness detection
 - Facial recognition technology can match the customer's face with that of the photo extracted from their ID document.
 - Face extraction can be used on a selfie video to verify whether the video was shot by user in a live environment.



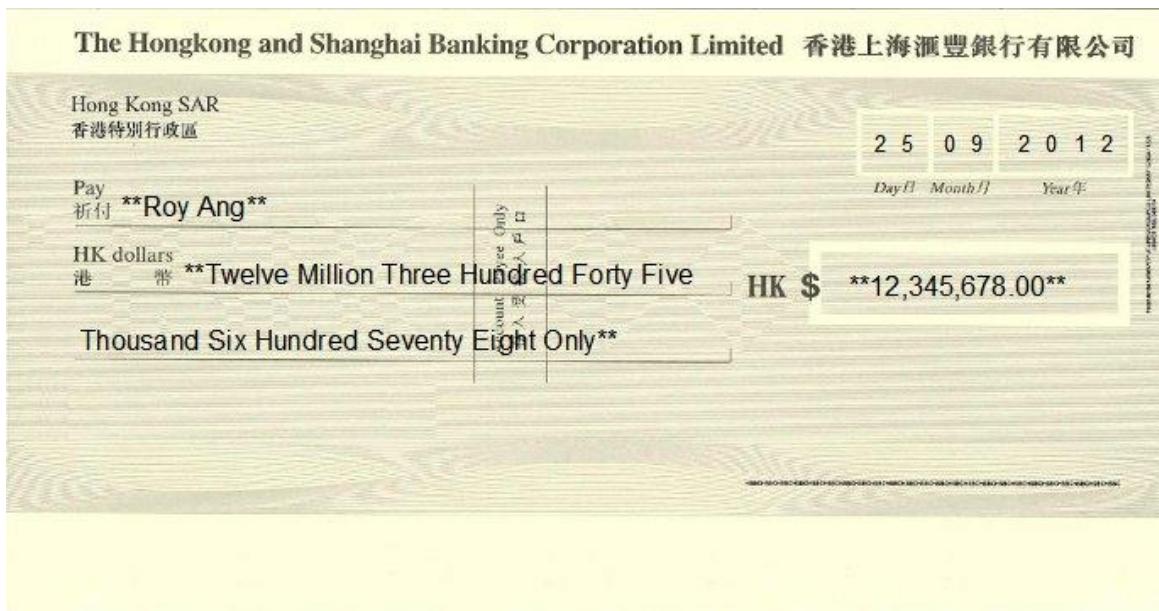
Application 2:Remote client on-boarding

- ▶ Pros:
 - ▶ Reduce cost
 - ▶ Most of the bank functions are still people- and paper- intensive.
 - ▶ Paperwork is one of the main contributors to operating costs.
 - ▶ Manual processing is not only slow, but also increases inconsistencies and human error.
- ▶ AI has become an option for banks to
 - ▶ streamline business processes
 - ▶ alleviate operational costs
 - ▶ reduce the chance of errors



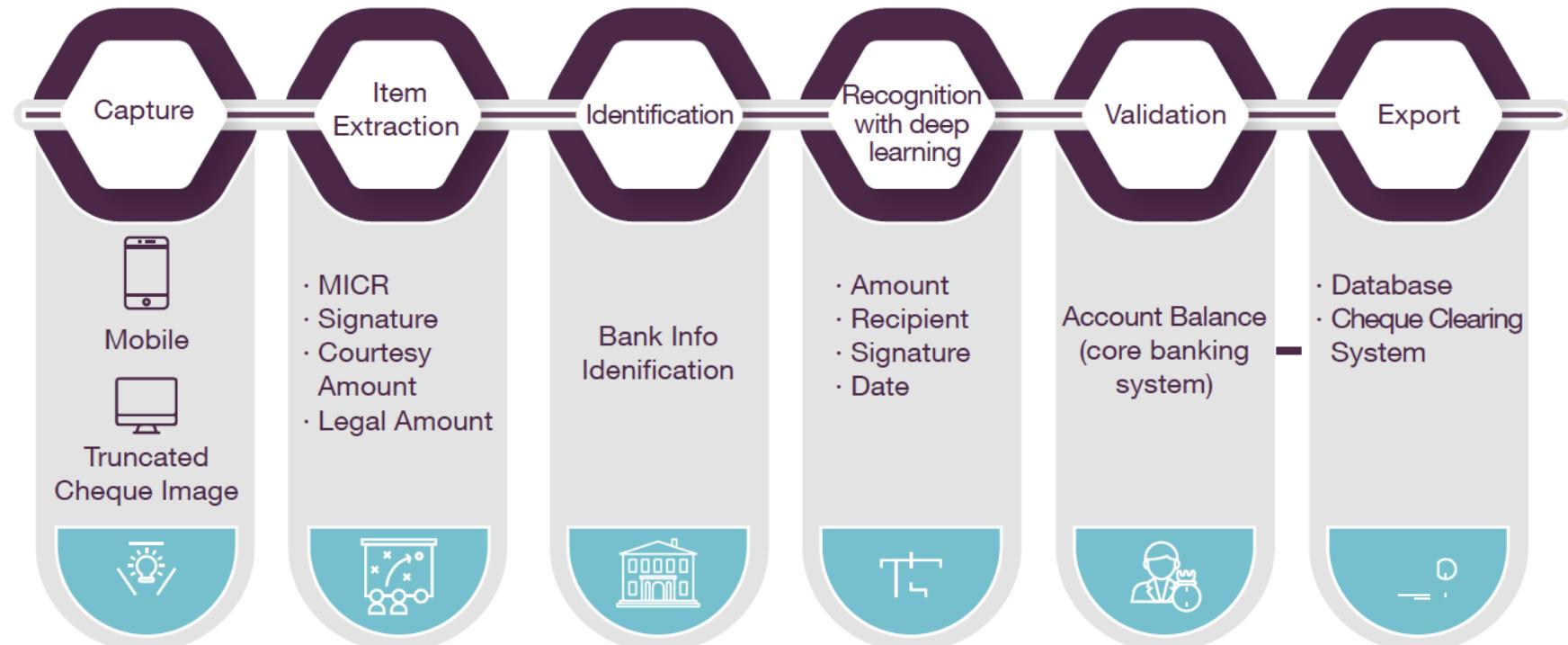
Application 3: Cheque processing

- ▶ Bank cheques have been widely used for financial transactions around the world.
- ▶ Considerable resources are devoted to visually verifying every field in each cheque, such as date, signature, and amounts.



Application 3: Cheque processing

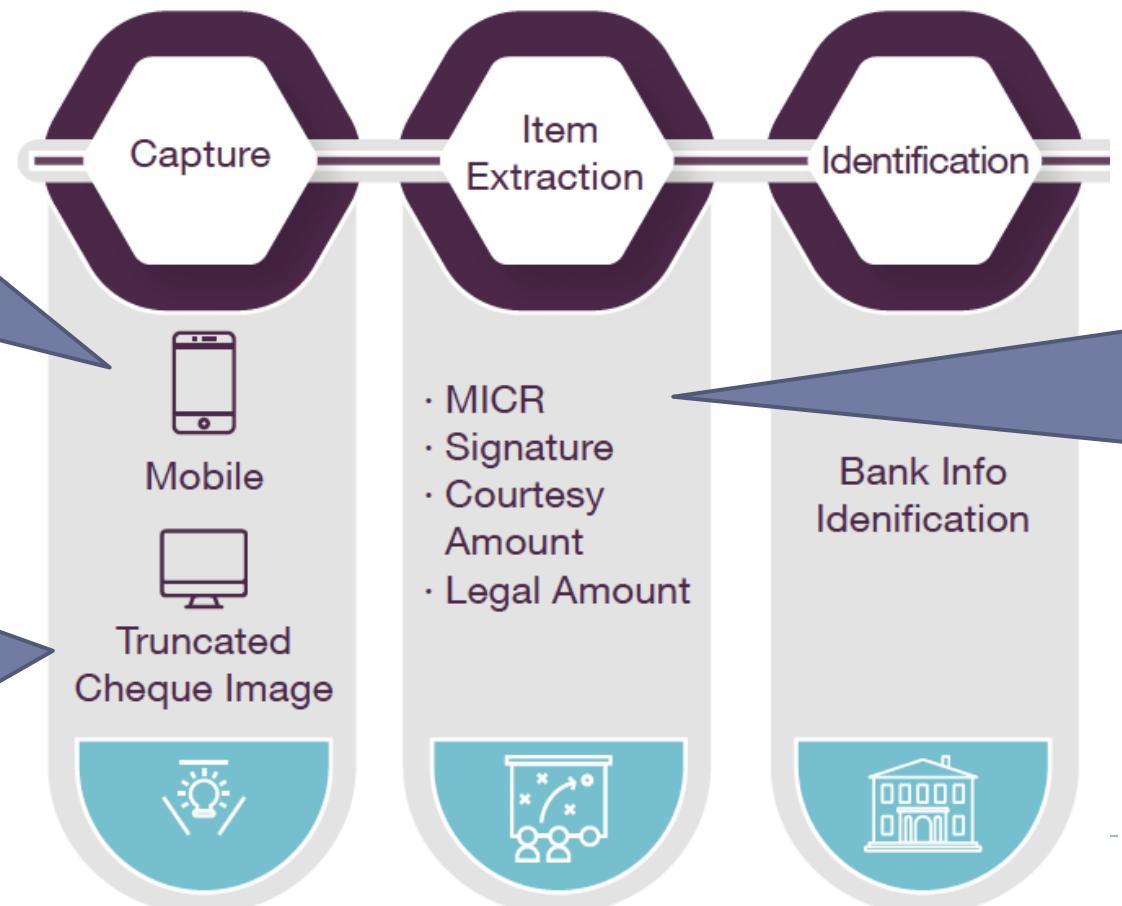
- An automated cheque processing solution based on OCR and supplemented by deep learning can
 - minimize human involvement
 - reduce cost, time and effort.



Application 3: Cheque processing

Mobile is used to digitalize the physical cheques into electronic images

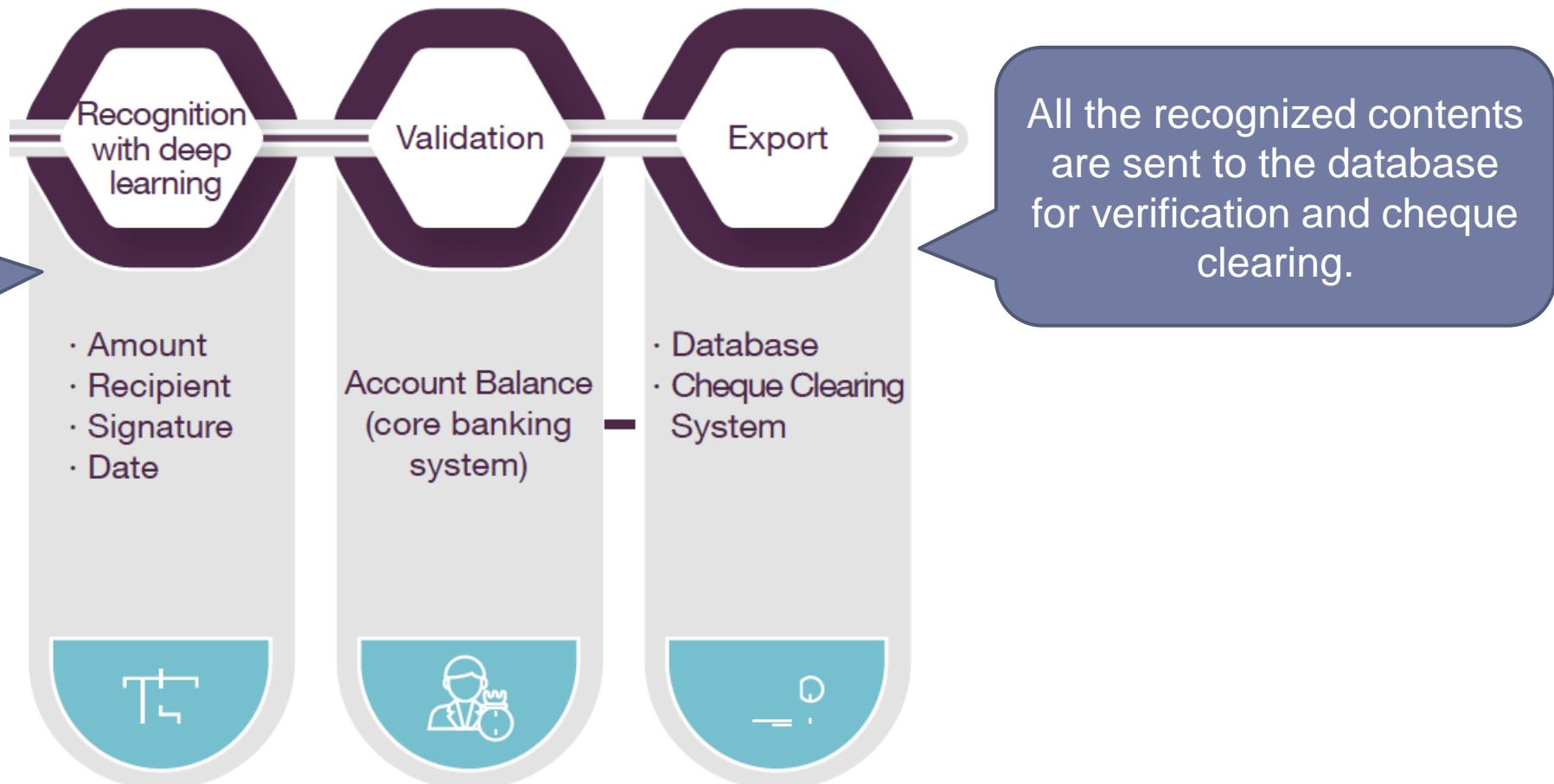
AI is used to analyze the cheque layout to identify relevant fields to be extracted



OCR is used to extract computer-printed MICR data (bank codes, bank account, cheque numbers) from identified fields for identification.

Application 3: Cheque processing

A deep learning neural network model is used for handwritten character recognition.



Application 4: Chatbots

- ▶ Chatbots are online, virtual conversation agents that allow automated responses based on customers' input and simulate human interaction.

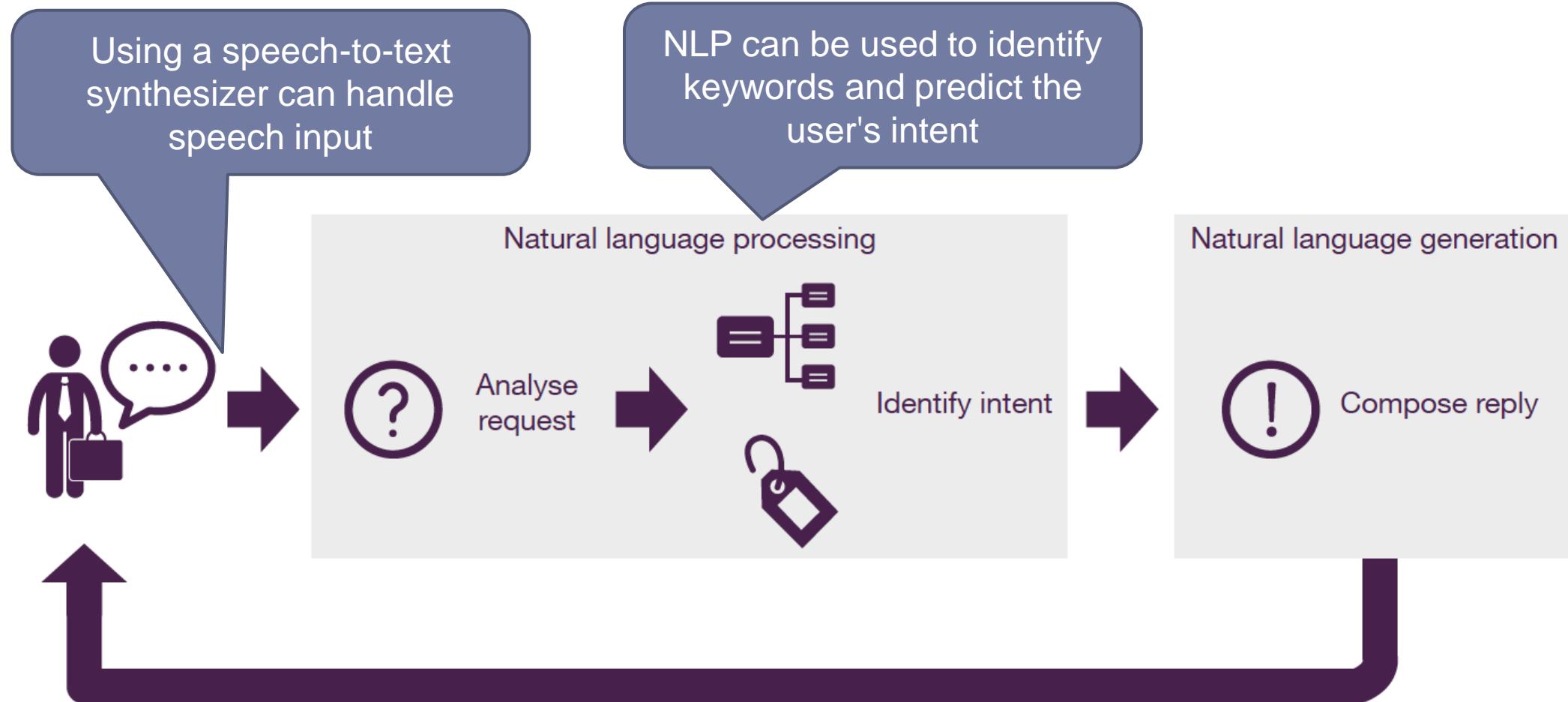
save investment in property and labour for physical customer services centres

provide faster and more consistent responses than a human customer services agent

- ▶ Currently, most chatbots can only offer basic banking services such as balance or account details enquires.
- ▶ Chatbots are still augmenting human actions rather than replacing them.



Application 4: Chatbots



Application 4: Chatbots

► Examples:

- [Erica \(Bank of America\)](#)
- [U.S. Bank Smart Assistant](#)
- [Eno of Capital One assistant](#)
- [HARO of Hang Seng Bank](#)
- [Joy of DBS](#)



 恒生銀行 HANG SENG BANK



H A R O - Your 24/7 Virtual Banking Assistant

Guide you to nearby branches, ATMs and offers timely FX and market updates on WhatsApp

Investment involves risks. Foreign exchange involves exchange rate risk. Terms and Conditions apply.

Personal > Digital Services > **Virtual Assistant H A R O**

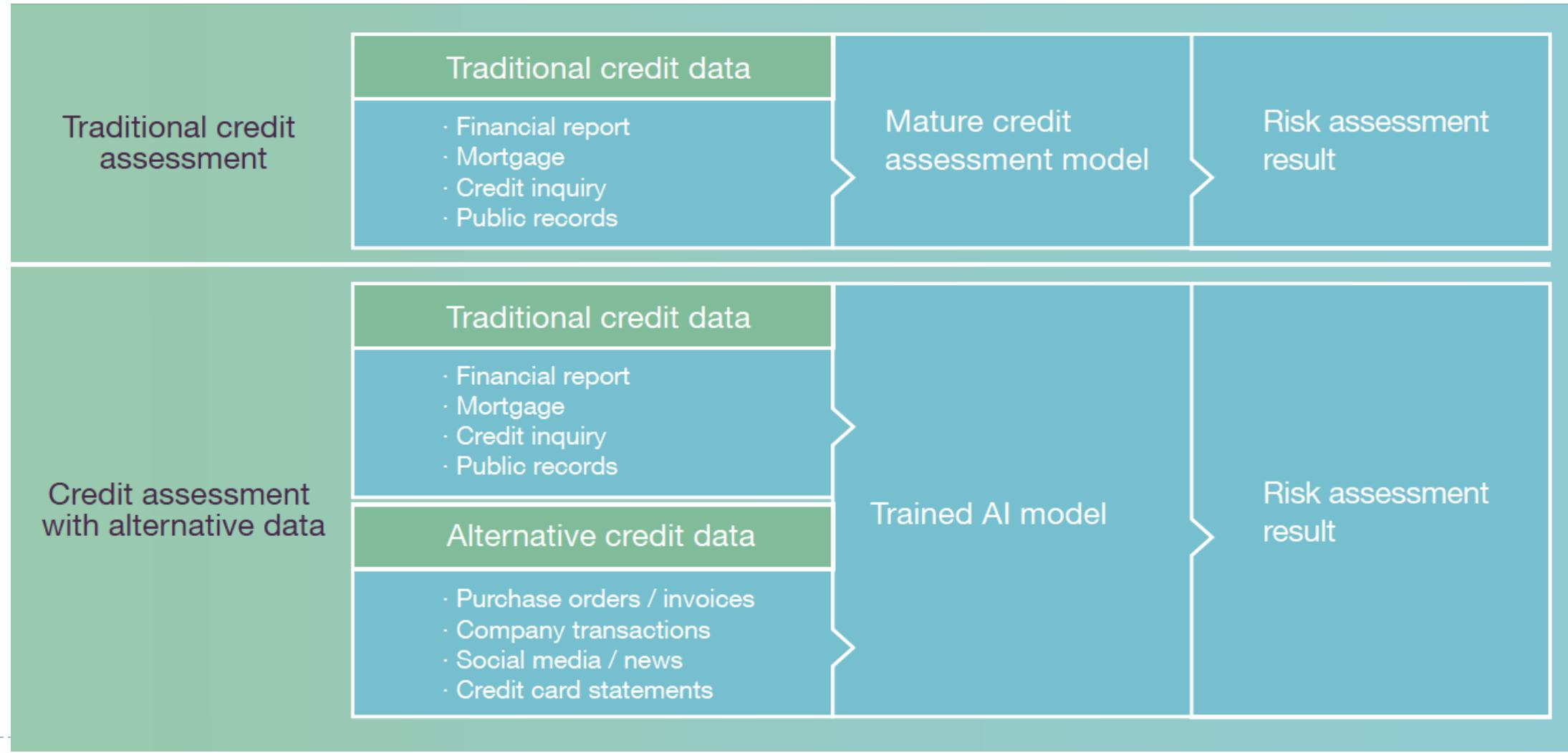
Check account balance
PAY BILLS
TRANSFER MONEY
VIEW INVESTMENTS
LOCK OR UNLOCK CREDIT CARDS
Automated alerts to suspicious activities
Weekly snapshot of spending
Search for past transactions
Monitoring recurring charges
Tracking account balance trends
Check account balance

Application 5: Risk management & Credit risk assessment

- ▶ Risk management
 - ▶ is very complex and tedious
 - ▶ requires high level accuracy and confidentiality.
- ▶ AI + big data
 - ▶ enables banks to carry out a more comprehensive credit risk assessment and a more accurate estimated loss rate on each borrower → more loan approvals
 - ▶ With lower estimated loss rates, borrowers pay a lower interest rate for a loan

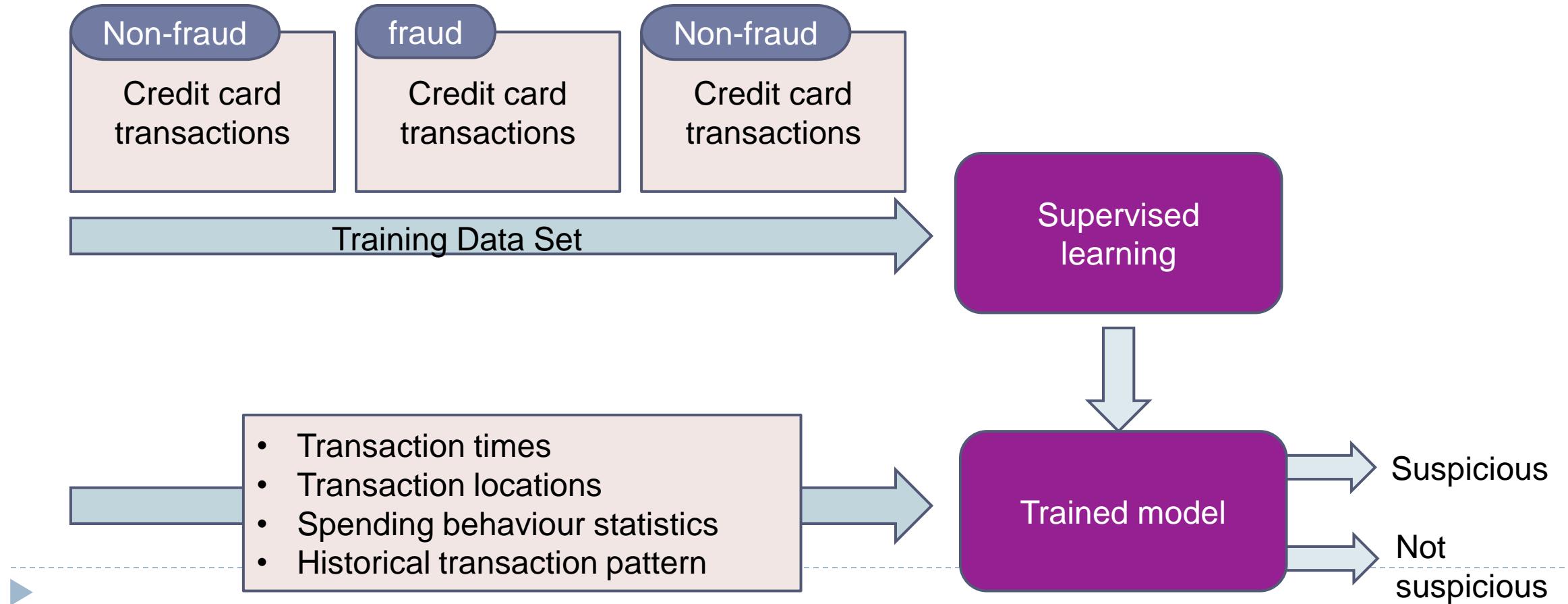


Application 5: Risk management & Credit risk assessment



Application 5: Risk management & Credit risk assessment

Real-time monitoring of Credit card payments



Applications 6: Underwriting

- ▶ Related technology: artificial intelligence decision algorithm (AIDA) – trained on past underwriting methods and payouts
- ▶ Uses:
 - ▶ Provides instantaneous assessment of client's credit risk for loans and investments
 - ▶ Allows advisors to propose a tailor-made offer for clients

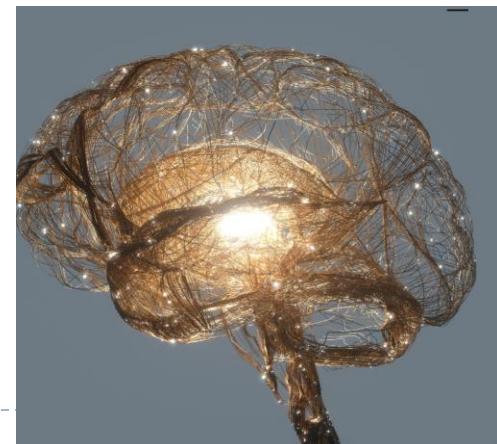
Advantages:

Increases efficiency of proposal preparation

Improves client experience (shortened processing time)

Example: Manulife

<https://myadvisorfocus.ca/winter-2020/aida-underwriting-20>



AIDA underwriting 2.0

Insurance enjoys more artificial intelligence upgrades.

Two years ago, we first told you about an exciting new artificial intelligence (AI) tool called AIDA that was about to have a big impact on Manulife Canada's Individual Insurance business. When AIDA went live in June 2018, the company made history, becoming the first insurance provider in the world to use AI for underwriting. Specifically, AIDA was designed to speed up the application approval process for Family Term cases with face amounts up to \$1 million. Since then, AIDA has processed over 100,000 applications and has been used to underwrite over 100,000 policies. This year, we're excited to announce that AIDA has been updated to version 2.0, which includes several new features and improvements. One of the most significant changes is that AIDA can now handle more complex cases, such as those involving pre-existing conditions or non-standard risks. Another key improvement is that AIDA is now able to provide more personalized offers to clients, based on their individual needs and circumstances. Overall, AIDA 2.0 represents a major step forward for Manulife's commitment to innovation and excellence in insurance underwriting.

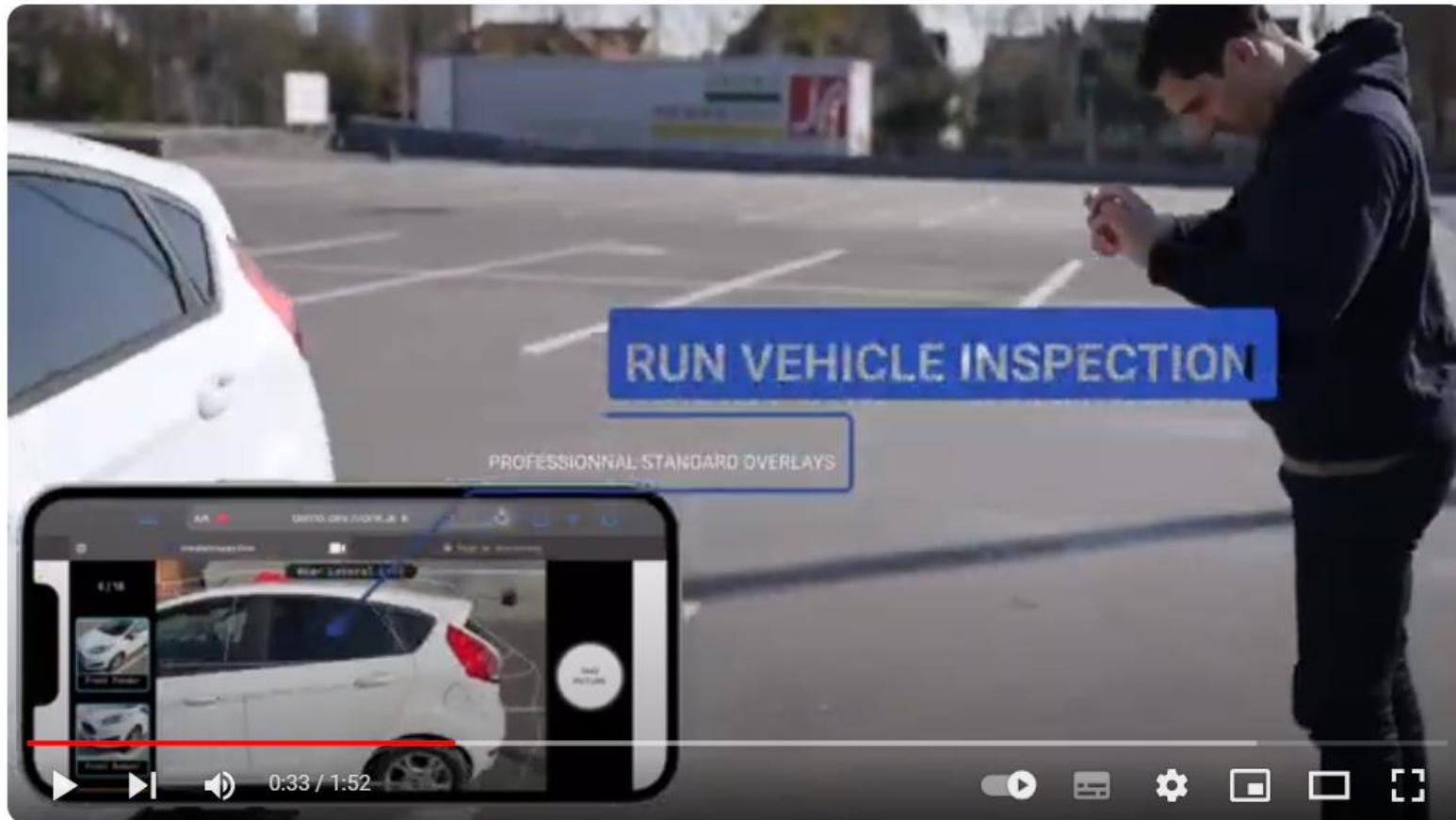
Applications 7: Insurance Claims

- ▶ Related technologies: machine learning models (image recognition + fraud detection + payout prediction)
- ▶ Uses:
 - ▶ Processes videos or photos of the damage (by image recognition)
 - ▶ Detects anomalies and non-compliant data (by fraud detection)
 - ▶ Calculates and proposes payout amount (by payout prediction)



Applications 7: Insurance Claims

- ▶ <https://youtu.be/hnhvsAt5luw?si=rSP90iFFHrgIMy0L>



Monk - AI Powered Vehicle Inspection

Applications 7: Insurance Claims

- ▶ Advantages:
 - ▶ Improves customer experience (less conflict with the insurance company staff)
 - ▶ Reduces operational tasks (calls, background checks)
 - ▶ Minimizes errors
 - ▶ Decreases processing time and cost

- ▶ Example: Lemonade
 - ▶ <https://www.lemonade.com/claims>



Applications 8: Contract Analyzer

▶ Related technologies:

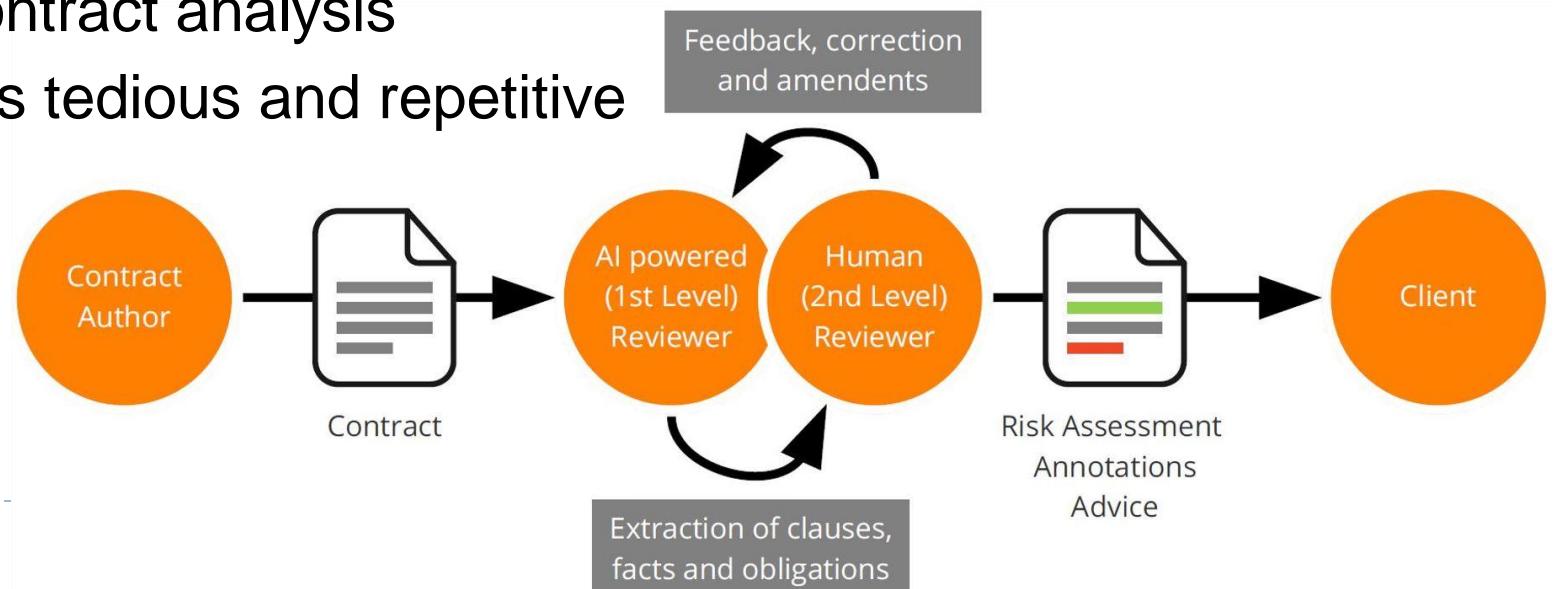
- ▶ machine learning (OCR + NLP), trained on existing contracts

▶ Uses:

- ▶ Digitalizes hard copy documents (by OCR)
- ▶ Interprets, records and corrects contracts (by NLP)

▶ Advantages:

- ▶ Improves accuracy of contract analysis
- ▶ Saves workload, which is tedious and repetitive



Application 9: Churn (Attrition) Prediction

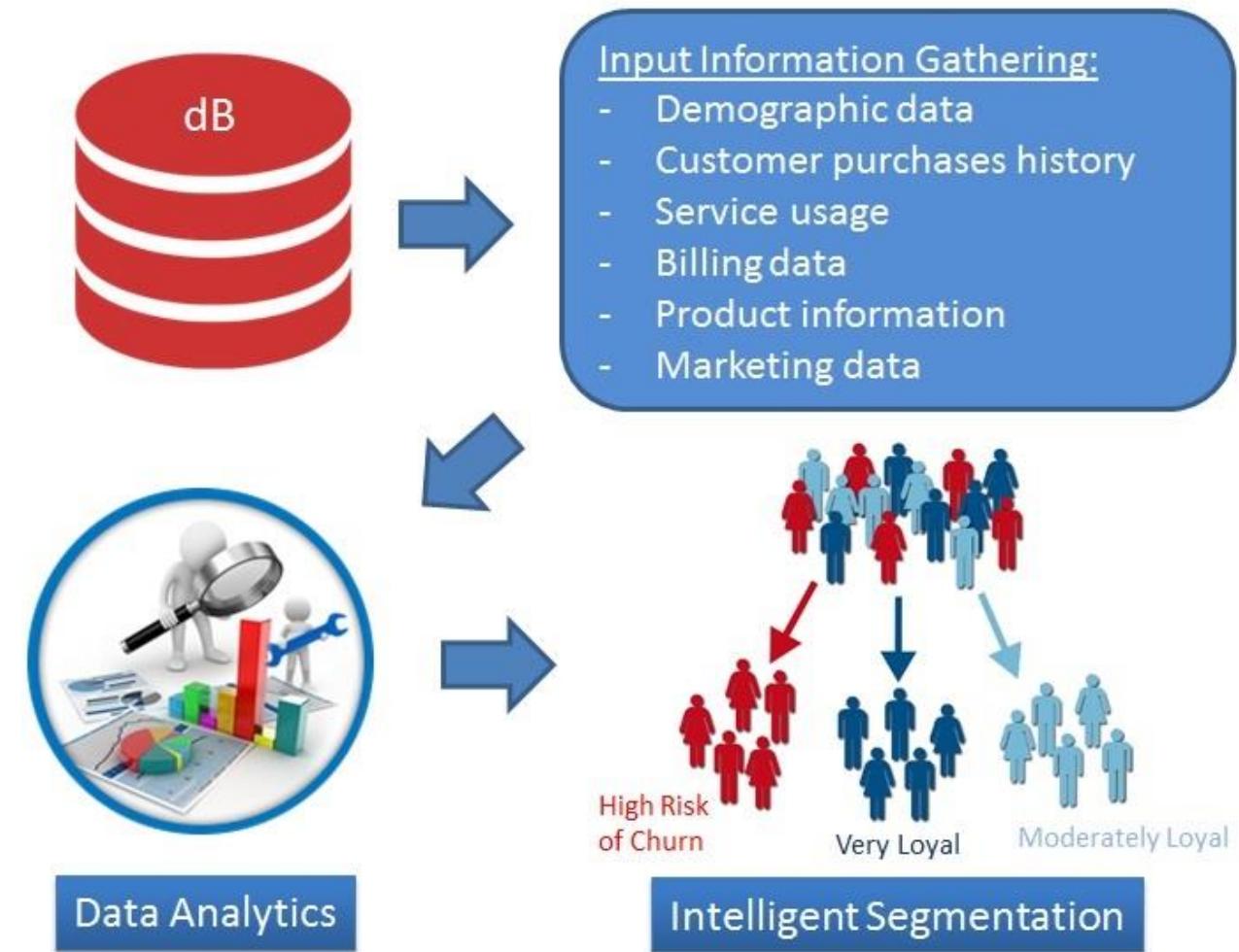
- ▶ Related technology:
 - ▶ classification model – trained on historical behavior data of clients who have canceled their policy and others who have stayed after considering leaving
- ▶ Uses:
 - ▶ Identifies clients who may cancel their policy by detecting customer behavior, e.g.
 - ▶ the number of times statements have been downloaded,
 - ▶ the occurrence of user reading account policies,
 - ▶ unsubscription to newsletters and mailings



Application 9: Churn (Attrition) Prediction

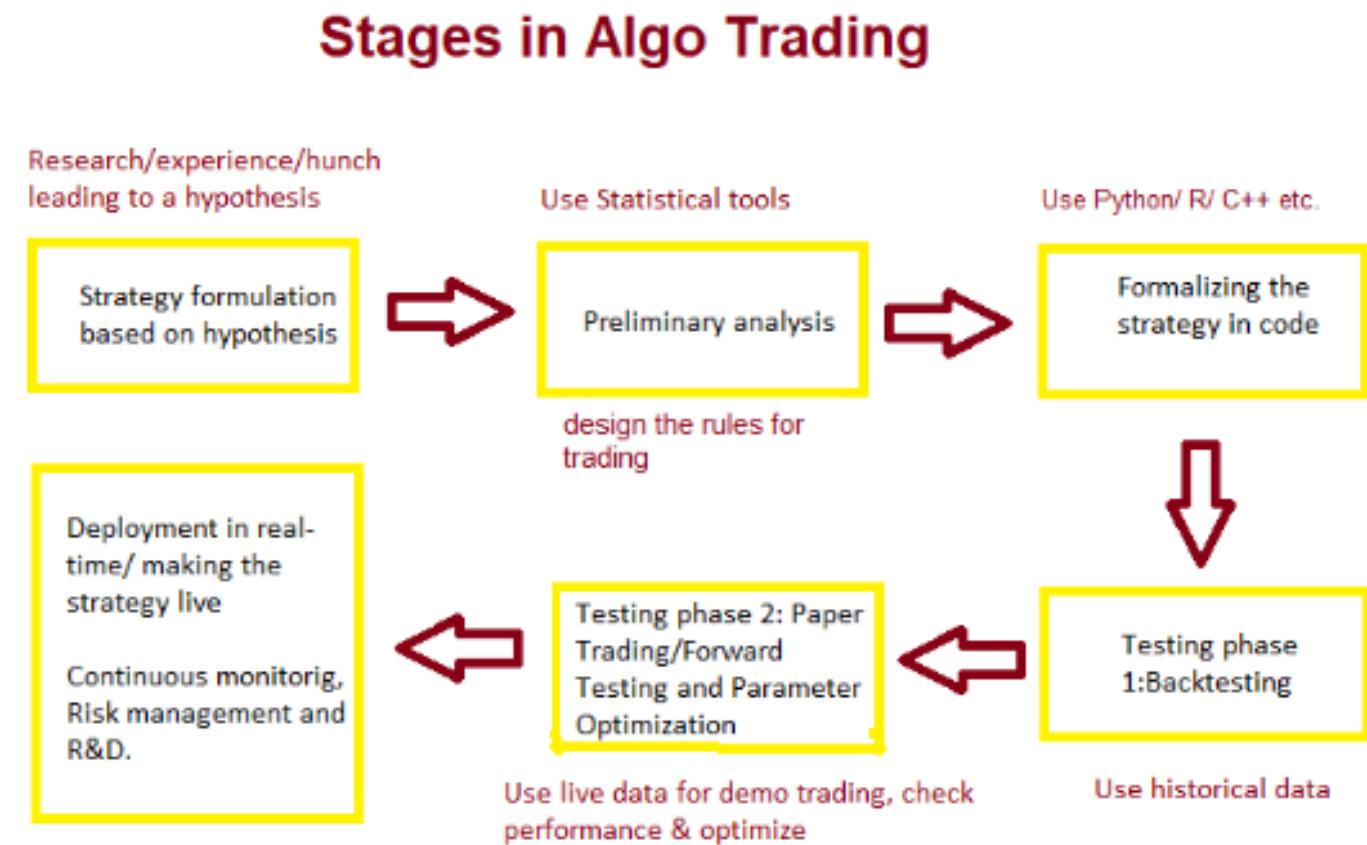
► Advantage:

- Target specific clients
take preventive actions
to retain them



Application 10: Algorithmic Trading

- ▶ Related technology:
 - ▶ big data analysis, machine learning model – trained on market data
- ▶ Use:
 - ▶ Analyzes market data, detects patterns, predicts price movement and executes trades automatically for investment banks and hedge funds
- ▶ Advantage:
 - ▶ Allows human traders to place time-sensitive trades at a speed and frequency that is impossible for them.



Algorithmic Trading (rule-base/ algorithm based)

Recall

- Algorithmic trading (also called automated trading, black-box trading, or algo-trading) uses a computer program that follows a defined set of instructions (an algorithm) to place a trade. The defined sets of instructions are based on timing, price, quantity, or any mathematical model.
- The trade, in theory, can generate profits at a speed and frequency that is impossible for a human trader. Most algo-trading today is high-frequency trading (HFT), which attempts to capitalize on placing a large number of orders at rapid speeds across multiple markets and multiple decision parameters based on preprogrammed instructions.



e.g. Technical Analysis taught in ELEC3845

Moving Average - Trend reversal

Recall

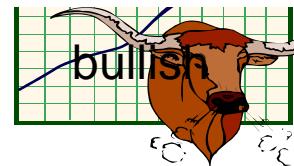
- ▶ E.g. 150-day EMA of 3M Co.
- ▶ It shows how well moving averages work when the trend is strong.
- ▶ 150-day EMA turned down in Nov 07 and again in Jan 08.
 - ▶ → took a 15% decline to reverse the direction of this moving average.
 - ▶ These lagging indicators identify trend reversals
- ▶ The price continued lower into Mar 09 and then surged 40-50%.
 - ▶ EMA did not turn up until after this surge → Another trend reversal (go up now!)
 - ▶ The stock price continued higher the next 12 months!!!



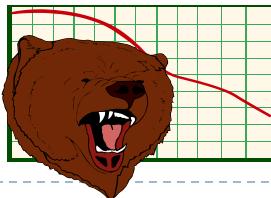
Moving Average - Double Crossovers

Recall

- ▶ A bullish crossover (so-called the golden cross)
 - ▶ Occurs when the shorter moving average crosses above the longer moving average
- ▶ A bearish crossover (so-called the dead cross)
 - ▶ Occurs when the shorter moving average crosses below the longer moving average.



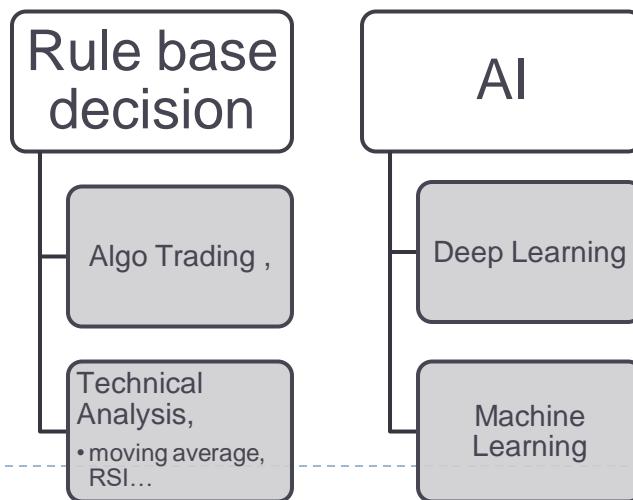
bearish



Recall

Sample Algorithm (rule base)

- ▶ If $\text{SMA}(10,t-1) < \text{SMA}(200,t-1)$
 - ▶ Then IF $\text{SMA}(10,t) > \text{SMA}(200,t)$ ‘short term exceed long term, golden cross’
 - ▶ Then
 - Buy the stock: ‘Gold cross’
 - ▶ Else
 - Keep the stock

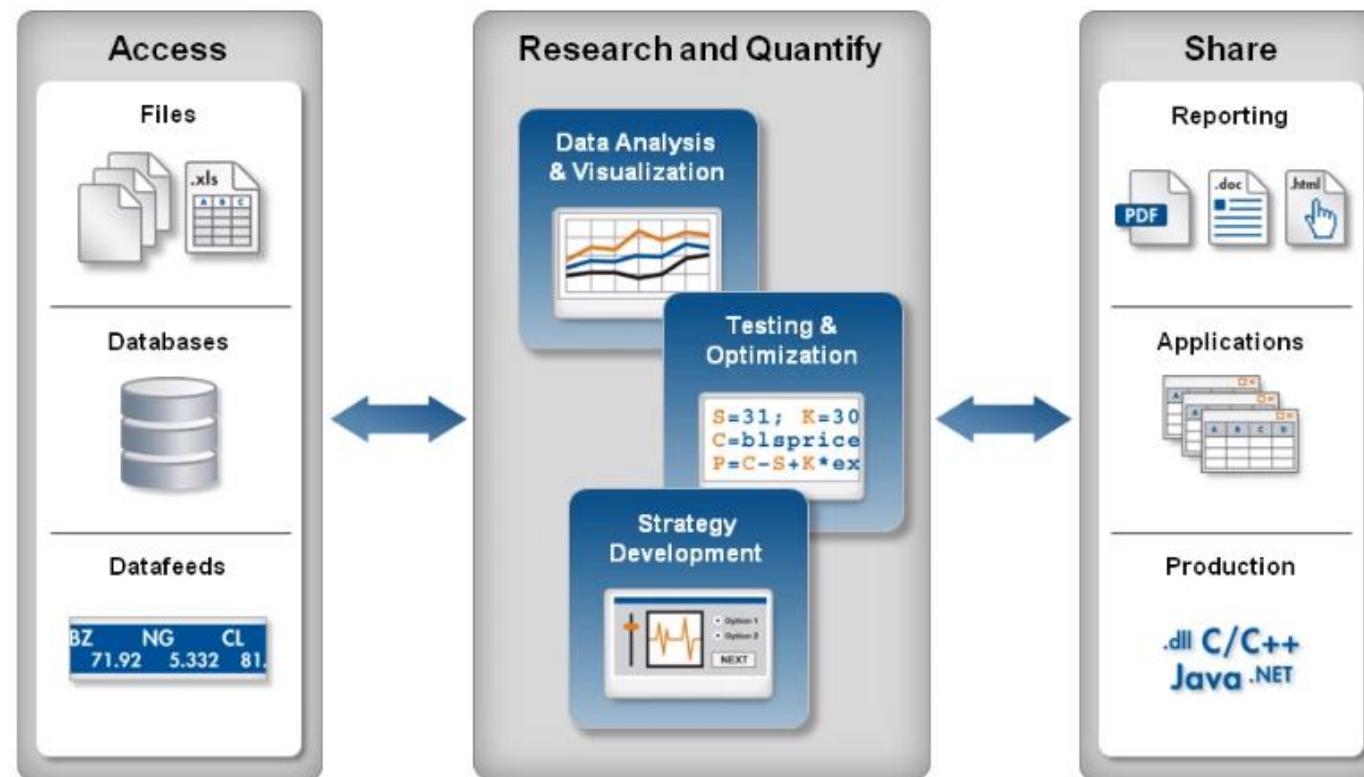


Recall

Algo trading using Matlab

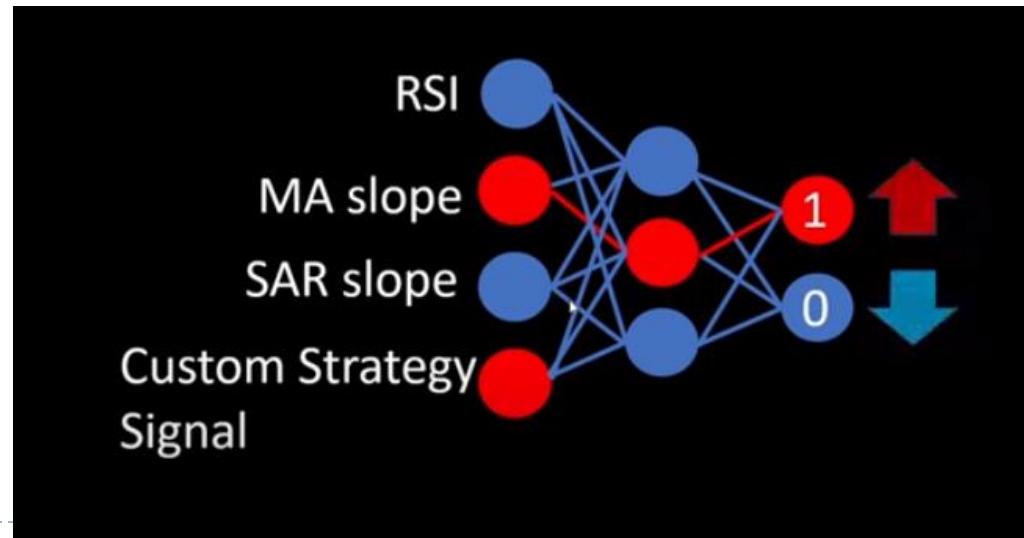
- ▶ <https://ww2.mathworks.cn/en/videos/algorithmic-trading-with-matlab-for-financial-applications-81775.html>

Algorithmic Trading Workflow



Application 10: Algorithmic Trading

- ▶ AI base
 - ▶ Multiple parameter input to the Neutral Network
 - ▶ Output the prediction: Rise or Fall
- ▶ Video demo
- ▶ <https://www.youtube.com/watch?v=m1rY2J8ZIsY>



Advantages of Algorithmic Trading

Recall

- Trade order placement is instant and accurate.
- Trades are timed correctly and instantly to avoid significant price changes.
- Simultaneous automated checks on multiple market conditions.
- Reduced risk of manual errors when placing trades.
- Reduced the possibility of mistakes by human traders based on emotional and psychological factors.
- Algo-trading can be backtested using available historical and real-time data to see if it is a viable trading strategy.



Recall

Disadvantages of Algorithmic Trading

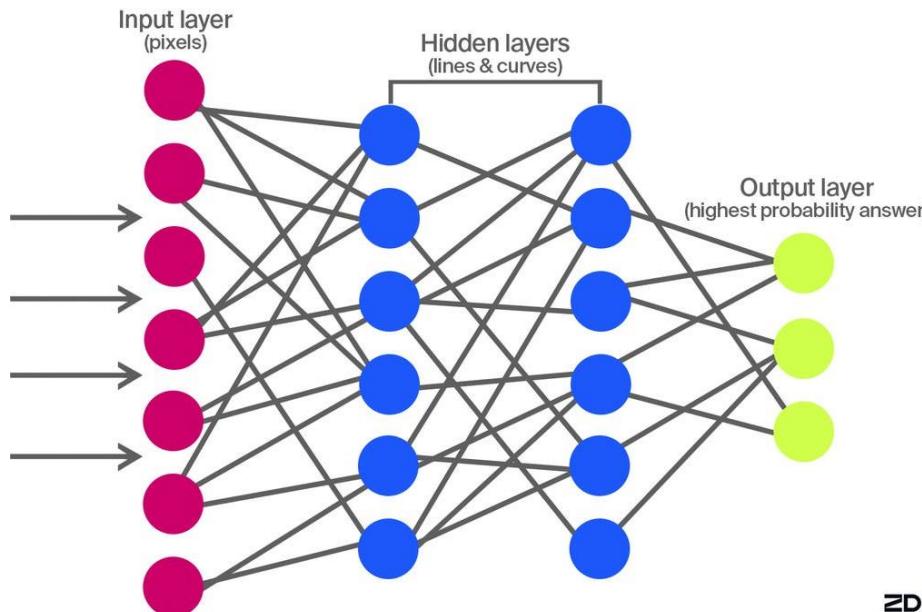
- While algorithmic trading may eliminate the impact of emotion in trading, it also makes investors over reliant on technology and the systems that they deploy. The loss of a viable network connection or a system crash could prevent your order from being executed, causing you to miss out on market opportunities.
- Risk of over-optimization, which can create streamlined algorithms that look great on paper but fail to translate in real market conditions. With over-optimization, you may find that the system is incapable of performing in a live and real-time marketplace.



Applications 11: Valuation Model

- ▶ Related technology: machine learning model – trained on historical data
- ▶ Use:
 - ▶ Calculates the valuation of a company or an asset for investment banking, based on financial analysis data point, market multiples, economic indicators, growth predictions, etc.

financial analysis data point,
market multiples,
economic indicators
Interest rate
Inflation
Unemployment
GDP growth
growth predictions



Summary: application of AI in FinTech

1. Anti-money laundering
2. Remote client on-boarding
3. Cheque processing
4. Chatbot
5. Risk management & Credit risk assessment
6. Underwriting
7. Insurance Claims
8. Contract Analyzer
9. Churn (Attrition) Prediction
10. Algorithmic Trading
11. Valuation Model

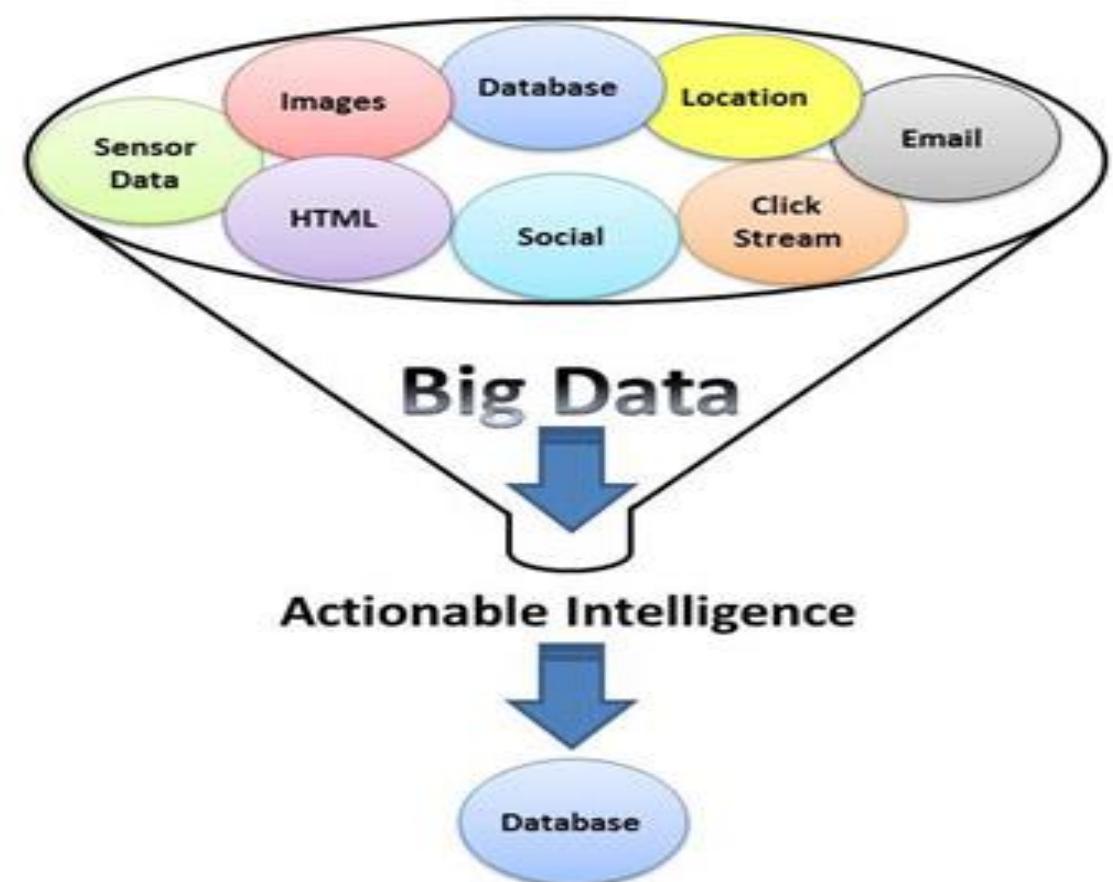


Big Data in FinTech



Big Data

- ▶ Data sets is nowadays so large and complex that traditional data processing applications are inadequate.
- ▶ Big data involves:
 - ▶ Analysis, capture,
 - ▶ Search, sharing, storage, transfer,
 - ▶ Visualization, and information privacy
 - ▶ predictive analytics
 - ▶ other certain advanced methods to extract value from data



Analysis of Big data

- ▶ **Objective:**
 - ▶ To find new correlations between data
 - ▶ To dig out non-trivial information or knowledge from the data set, e.g.
 - ▶ spot business trends
 - ▶ prevent diseases
 - ▶ combat crime...



Why big data?

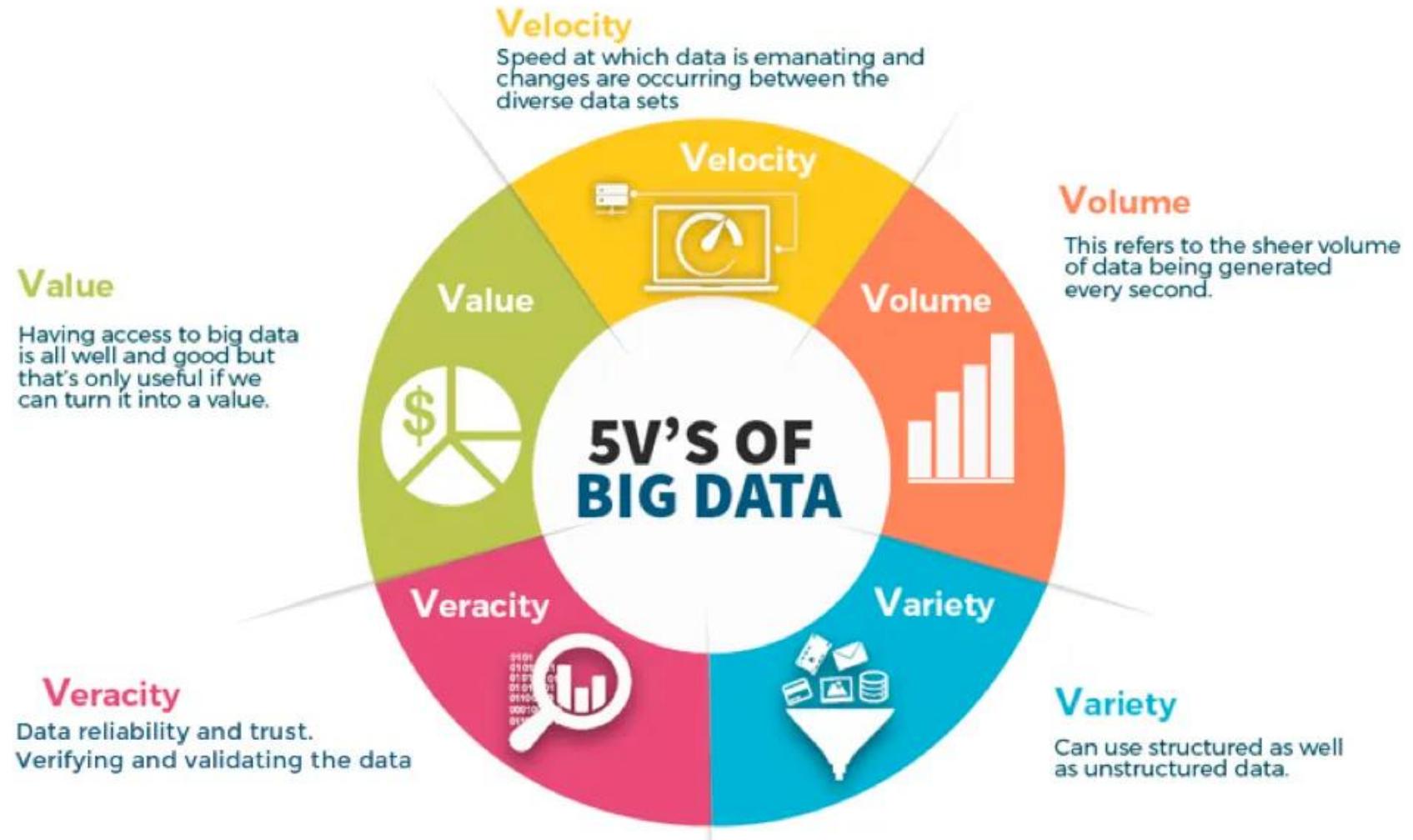
- ▶ Data sets grow in size in part because:
 - ▶ Data increasingly being gathered by cheap and numerous information-sensing mobile devices,
 - ▶ Availability of remote sensing and software logs,
 - ▶ e.g. cameras, microphones, radio-frequency identification (RFID) readers, and wireless sensor networks, bank transactions



Big data

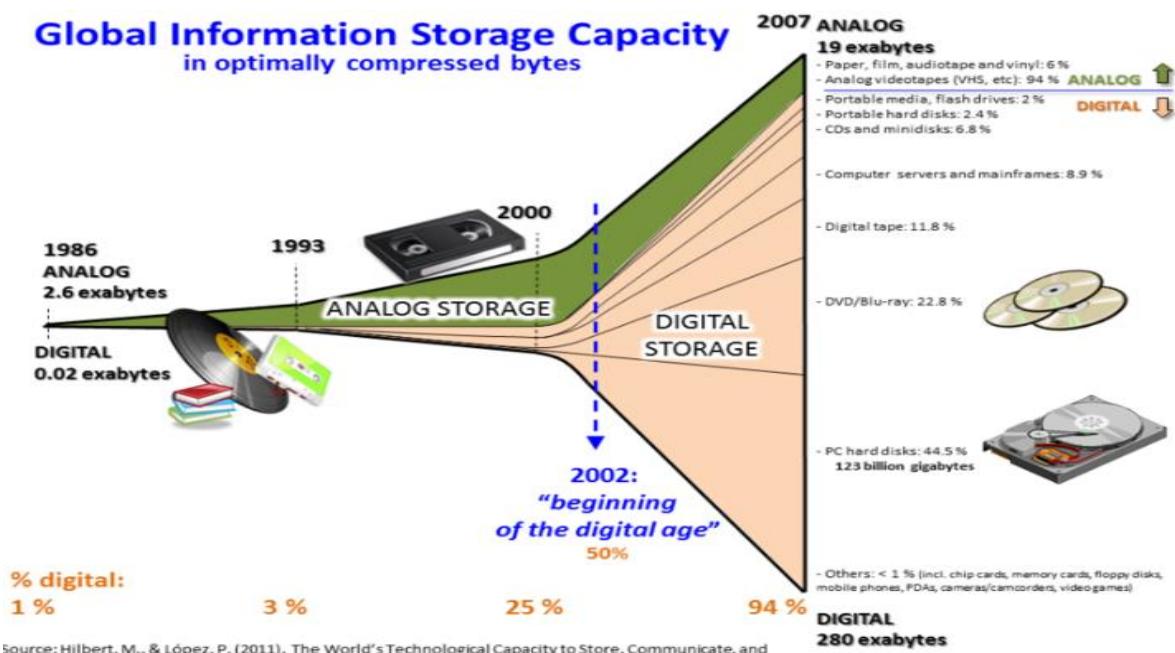
► 5V characteristics:

- Volume
- Variety
- Velocity
- Veracity
- Value



Volume

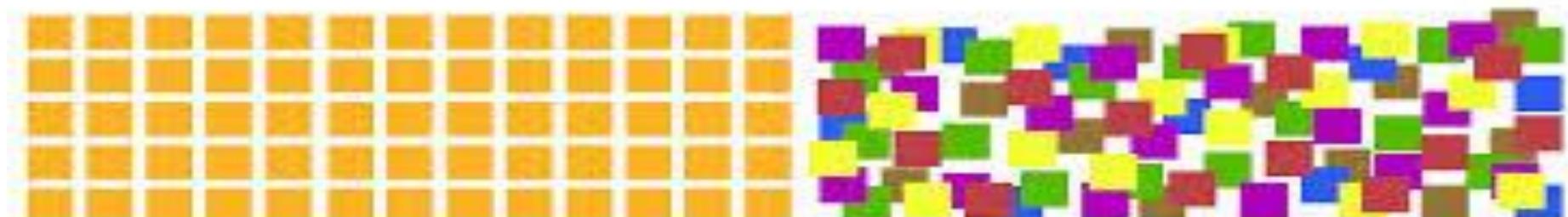
- ▶ The quantity of data that is generated is very important in this context
- ▶ The size of the data which determines the value and potential.
- ▶ ‘Big Data’ contains a term which is related to **size** and hence the characteristic.



Variety

- ▶ The category to which Big Data belongs to is also a very essential fact that needs to be known by the data analysts.
- ▶ This helps to effectively use the data to their advantage and thus upholding the importance of the Big Data.

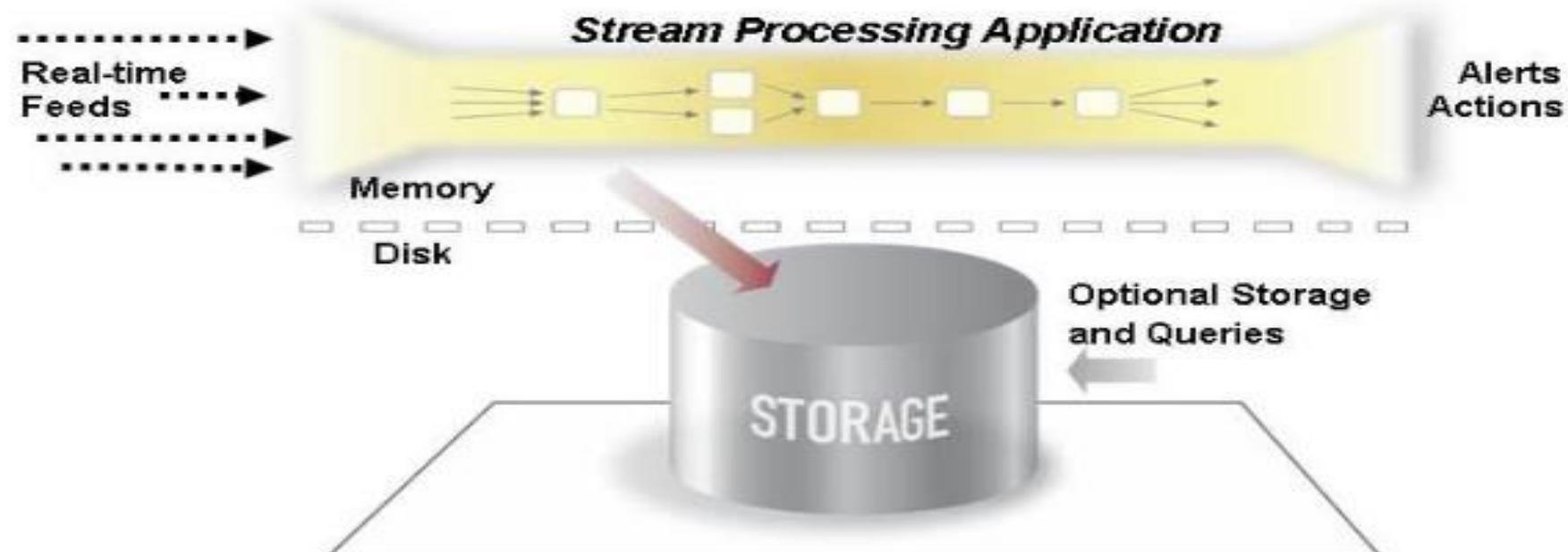
“80% of business-relevant information originates in unstructured form, primarily text.”



Structured Data vs. **Unstructured Data**

Velocity

- ▶ Refers to the speed of generation of data or
- ▶ How fast the data is generated and processed to meet the demands and the challenges



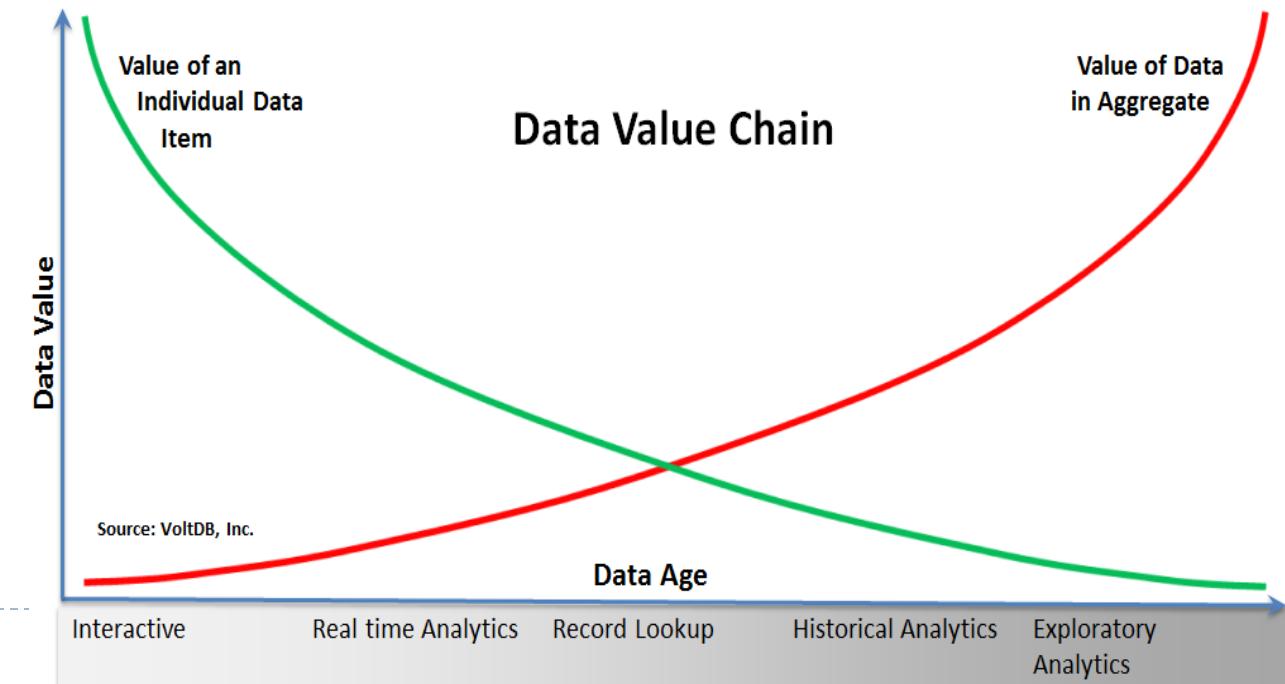
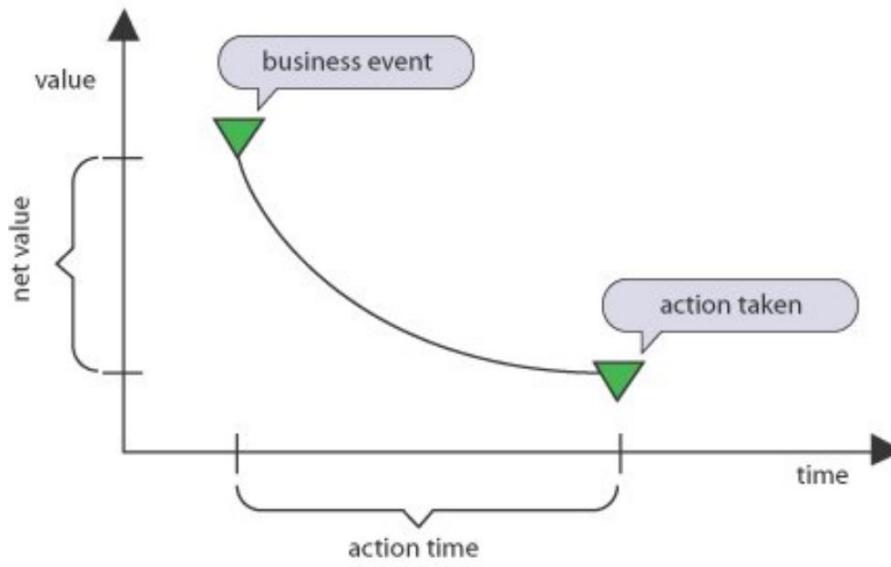
Veracity (Integrity)

- ▶ The quality of the data being captured can vary greatly.
- ▶ Accuracy of analysis depends on the veracity of the source data.
- ▶ It refers to the assurance of **quality/integrity/credibility/accuracy** of the data.
- ▶ Since the data is collected from multiple sources, we need to check the data for accuracy before using it for business insights.

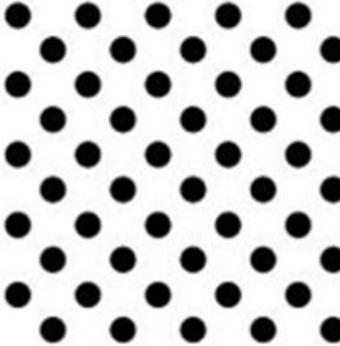
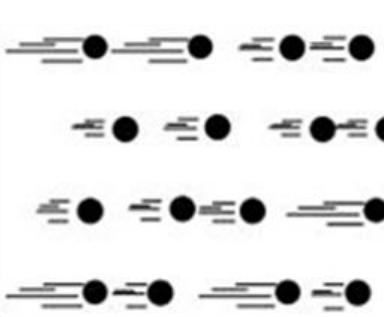
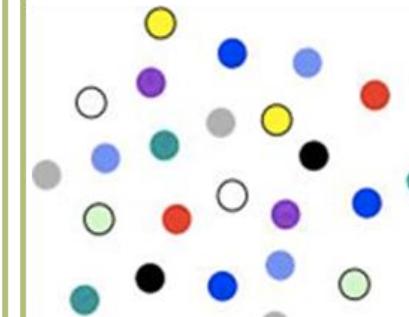
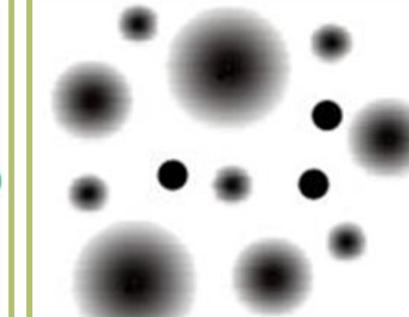


Value

- ▶ Just because we collected lots of Data, it's of no value unless we garner some insights out of it.
- ▶ Value refers to how useful the data is in decision making.
- ▶ We need to extract the value of the Big Data using proper analytics.



Summary of 5V in Big Data

Volume	Velocity	Variety	Veracity	Value
				
Data at Rest Terabytes to Exabytes of existing data to process	Data in Motion Streaming data, requiring milliseconds to seconds to respond	Data in Many Forms Structured, unstructured, text, multimedia,...	Data in Doubt Uncertainty due to data inconsistency & incompleteness, ambiguities, latency, deception, model approximations	Data into Money Business models can be associated to the data

Tools for AI and big data analysis

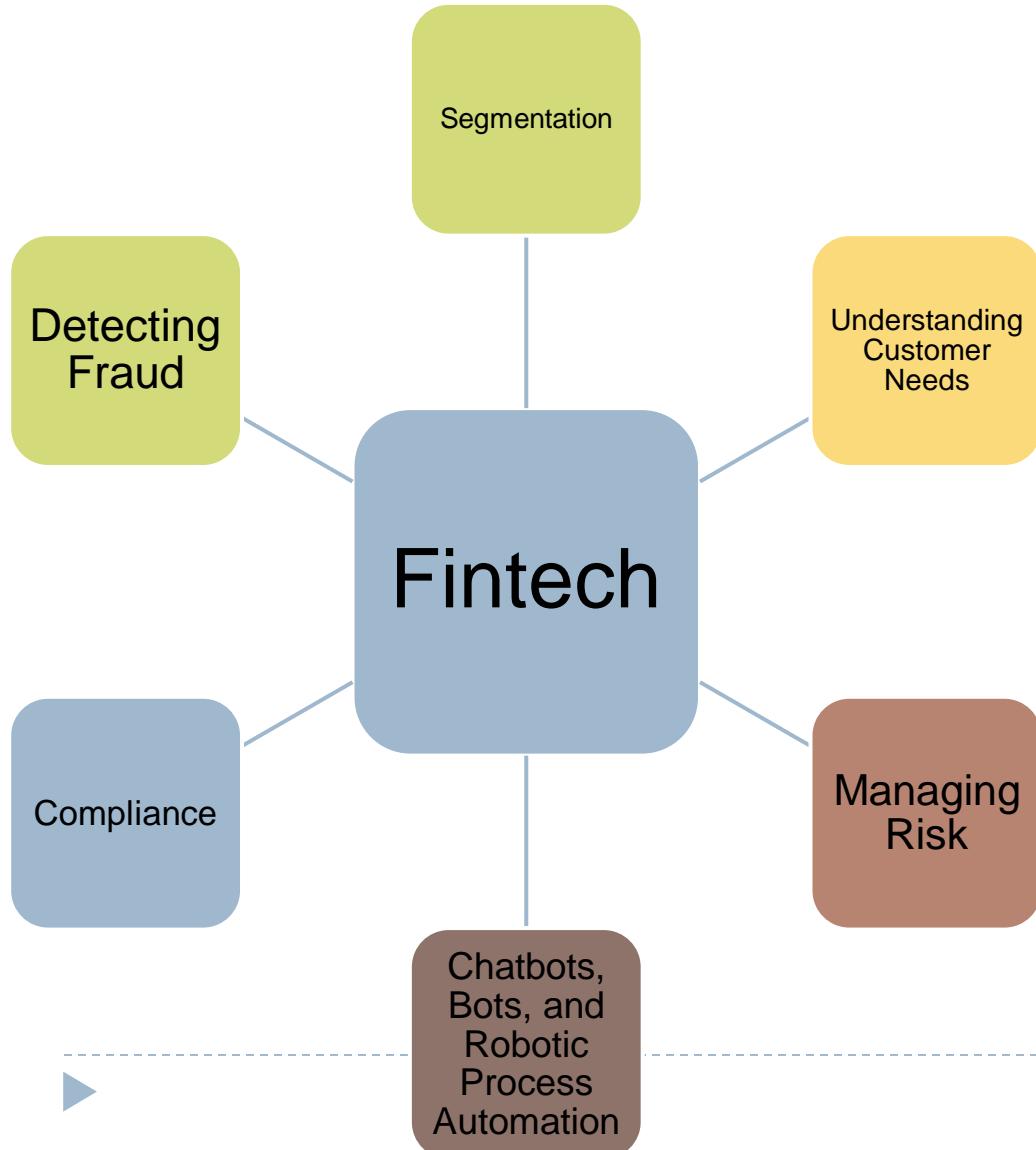
- ▶ **Tensorflow**
 - ▶ <https://www.tensorflow.org>
- ▶ **Caffe**
 - ▶ <http://caffe.berkeleyvision.org/>
- ▶ **Paddle paddle**
 - ▶ <http://www.paddlepaddle.org/>
- ▶ **Microsoft Azure Machine Learning Studio, Co-pilot**
 - ▶ <https://studio.azureml.net/>
- ▶ **Ali Cloud AI API**
 - ▶ <https://m.aliyun.com/act/etapi>



What are the applications of Big Data technology in FinTech?



Big data in Fintech



- ▶ A vast amount of data is generated every day in fintech sector.
- ▶ The data can be used by banks and financial organizations to forecast client behavior and generate sophisticated risk evaluations

Source: <https://www.computer.org/publications/tech-news/trends/6-ways-big-data-in-fintech-is-creating-a-better-customer-experience>

Big data in Fintech

Demographics (Age, Gender, Education, Address)
Family (Size, Dependents)
Employment
Financial (Income, Assets)
Risk perception
Online behavior

Credit card transactions
ATM withdrawals
Credit scores
Other financial tools

Transactions

Spending habits of customers



Application of Big Data 1: Segmentation

- ▶ Sorts customers by various categories and can provide data about what products meet the needs of its customers.
- ▶ Helps identify the high-value customers that are most likely to purchase financial products.
- ▶ Helps to understand customer needs and provide more personalized offers.



Application of Big Data 2: Understanding Customer Needs

- ▶ Proposes correct services/products based on clients' specific spending habits.
- ▶ Let companies continuously optimize their customer's online experience to improve company's credibility and trustworthiness.
- ▶ Establishes a digital trail of a customer's financial behavior, spots possible problems, and gives consistent assistance.



Application of Big Data 3: Managing Risk

- ▶ Identifies potential bad investments
- ▶ Flags customers that are showing warning signs of trouble



Application of Big Data 4: Detecting Fraud

- ▶ Part of managing the risk is quickly identifying fraud when it occurs.
- ▶ By analyzing the spending habits of customers, AI and ML can identify purchases or locations that do not fit the profile (odd transactions) and flag them for review **before** completing transactions.



Application of Big Data 5: Chatbots and Process Automation

- ▶ Enables intelligent Chatbots to handle transactions, provide important information, and help customers in a variety of ways.
- ▶ Improves user experience by enabling bots to handle repetitive (and labor-intensive) tasks without human intervention.
- ▶ Reduces errors.
- ▶ Freed up human resources to handle more complex queries and provides better customer service.



Summary of Big data application for Fin Tech

- ▶ Segmentation
- ▶ Understanding Customer Needs
- ▶ Managing Risk
- ▶ Detecting Fraud
- ▶ Chatbots and Process Automation



References

- ▶ https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Whitepaper_on_AI.pdf
- ▶ <https://www.computer.org/publications/tech-news/trends/6-ways-big-data-in-fintech-is-creating-a-better-customer-experience>



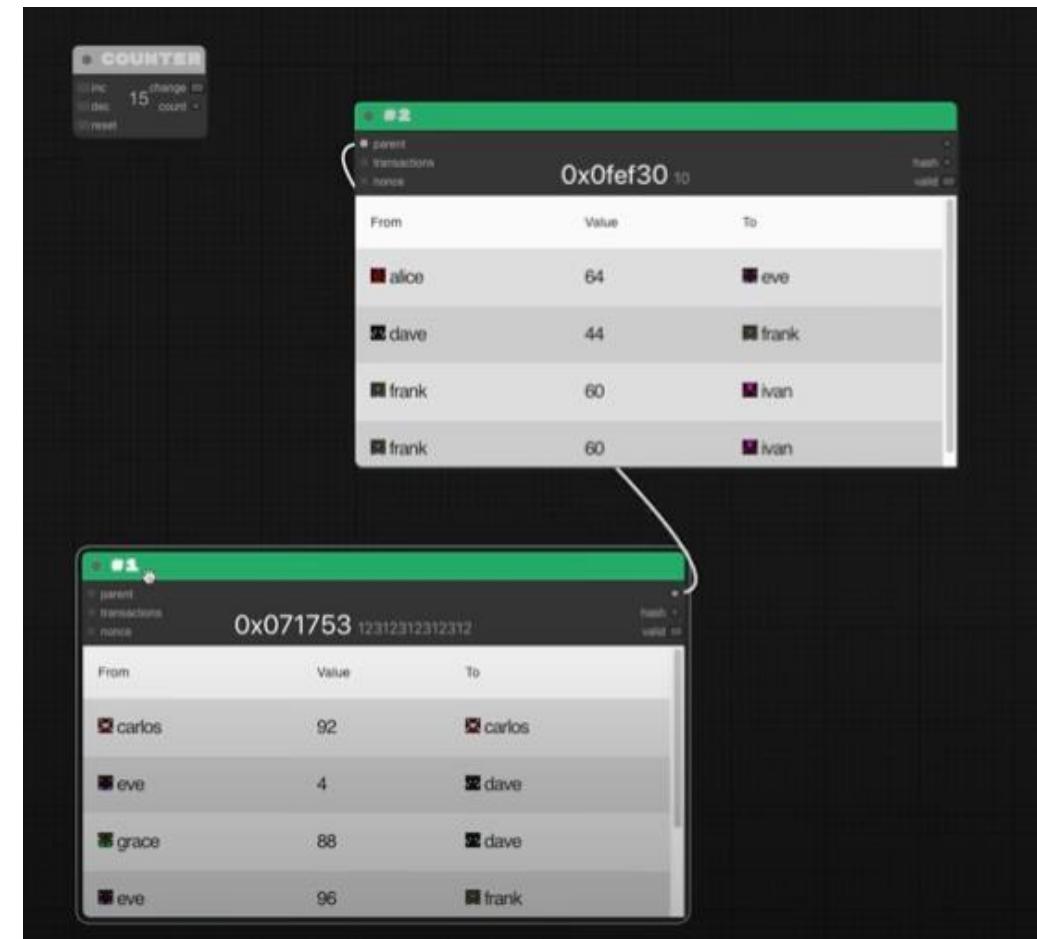
ELEC2544 E-commerce and Fin-Tech

Block Chain and Bitcoin

Dr. Wilton Fok

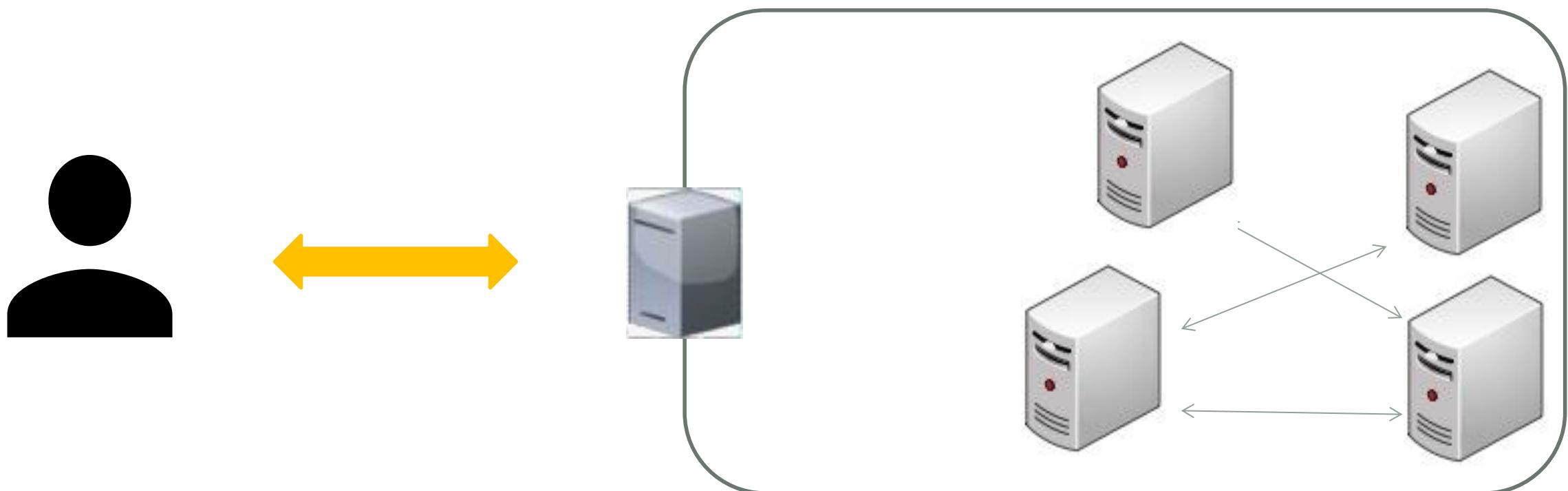
What is Blockchain?

- A **blockchain** is a data structure shared across many computers in a network (a **distributed system**).
- **Block:** Data (transactions) are stored in blocks.
 - Example: if you send money (cryptocurrency) to someone, you need to add this transaction to a block.
- **Chain:** Blocks get chained together such that the data in a block cannot change without changing all subsequent blocks (so, almost impossible).



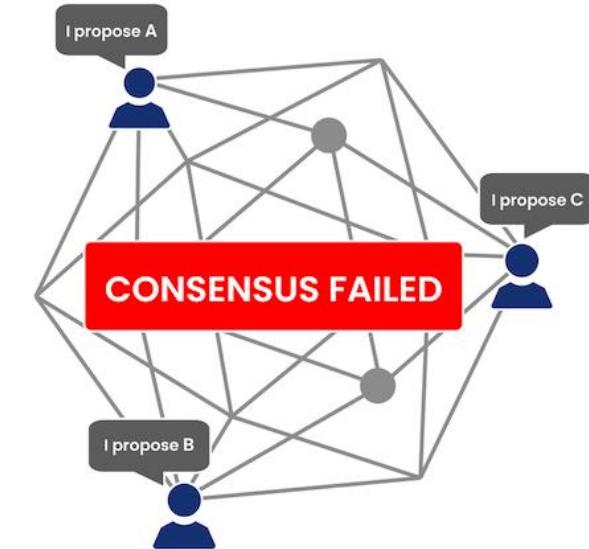
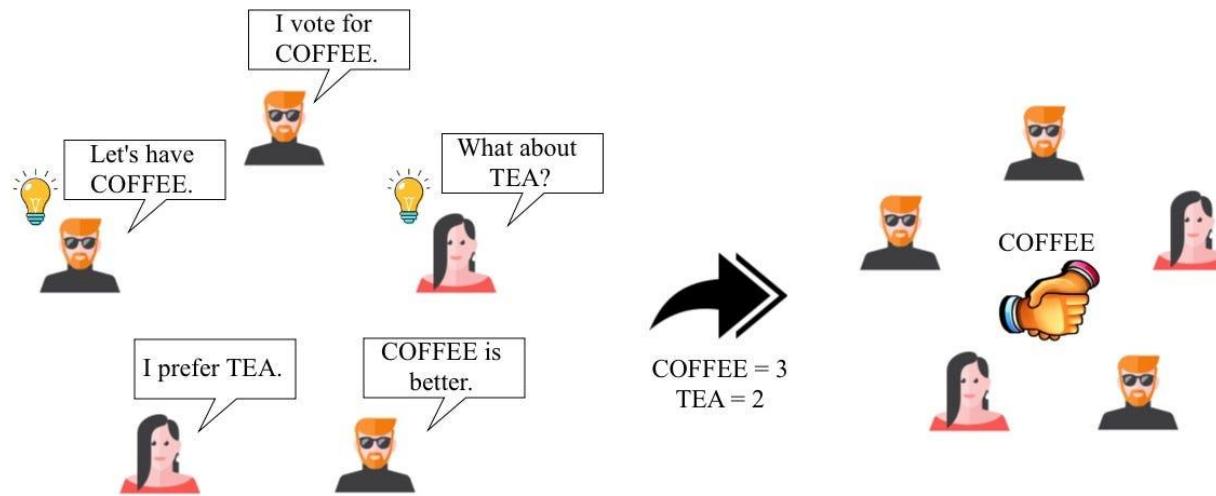
Distributed Computing

- Computing Paradigm:
- Multiple nodes work with each other in a coordinated fashion in order to achieve a common outcome



What is Blockchain?

- To ensure everyone interacting with the blockchain see the same data, every computer (node) in a **distributed system** must agree upon each new block and the chain as a whole via a **consensus** mechanism.



Consensus

- Consistency is achieved using consensus algorithms to ensure that all nodes have the same copy of data.
 - All blockchains are required to agree on their contents, i.e., which transactions to add and in which order.
- A set of steps that are taken by all, or most, nodes in order to agree on a proposed state or value.

Tiers of Blockchain Technology

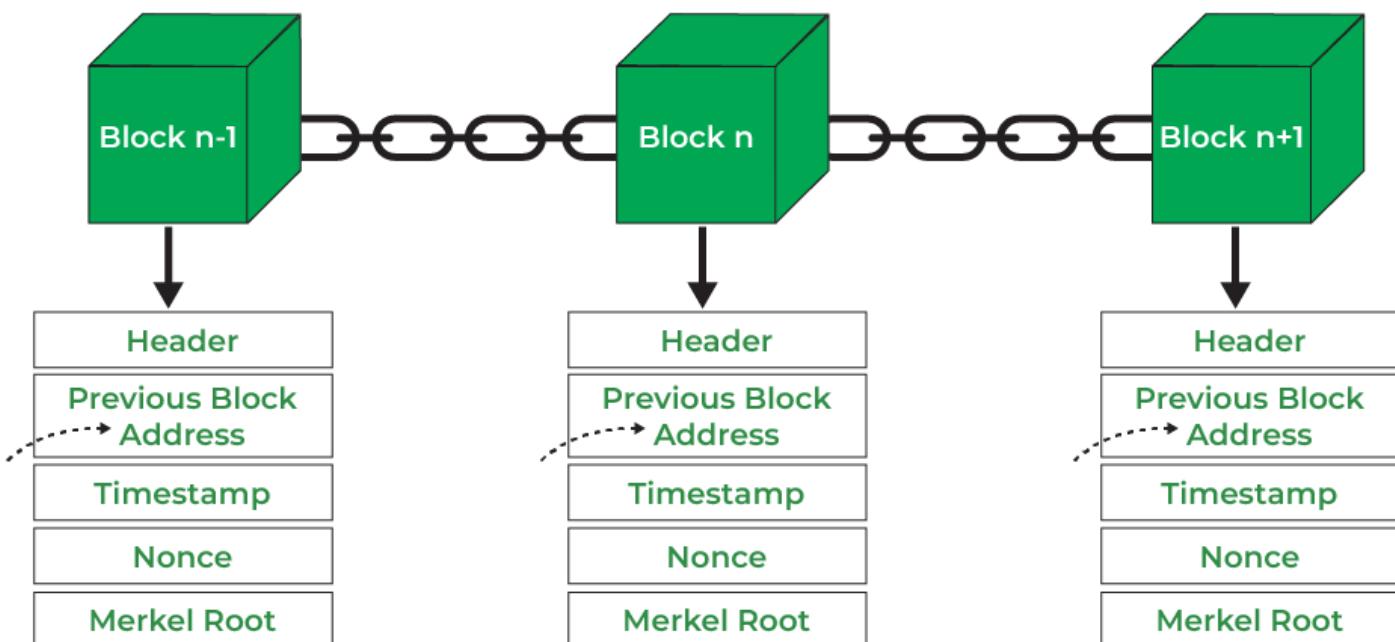
- Blockchain 1.0
 - Cryptocurrencies
- Blockchain 2.0
 - Financial services and contracts
- Blockchain 3.0
 - Other Applications used in general-purpose industries such as government, health, media and the arts

What is Blockchain?

- A blockchain is a chain of blocks storing transactions in a distributed system.
- Recap in technical terms:
 - A blockchain is a **public ledger** of a timestamped, ordered, and immutable list of **transactions** on the network.
 - Each block is identified by a hash and is linked to its previous block by referencing the previous block's hash.

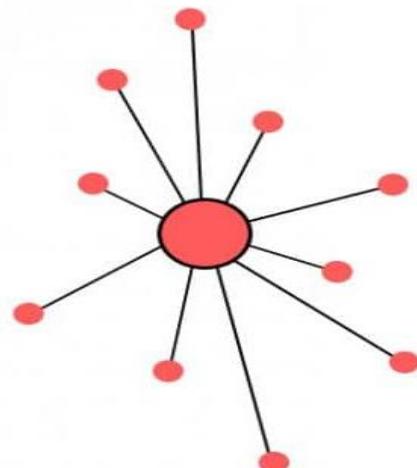
Blockchain

Blockchain is a digital database containing information (such as records of financial transactions) that can be simultaneously used and shared within a large decentralized, publicly accessible network



Decentralization

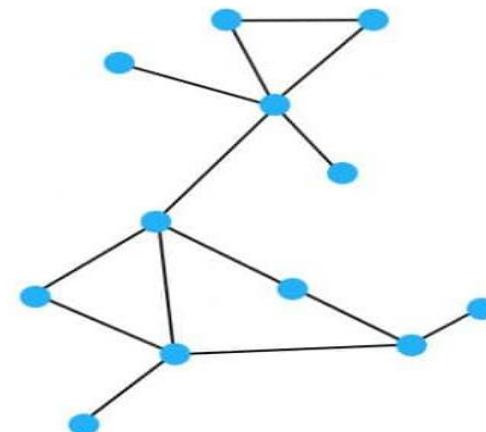
Centralized



Centralized systems have a core authority that **dictates the truth** to the other participants in the network.

Only **privileged users** or institutions can access the history of transactions or confirm new transactions.

Decentralized



Decentralized systems have **no core authority** to dictate the truth to other participants in the network.

Every participant in the network can access the history of transactions or confirm new transactions.

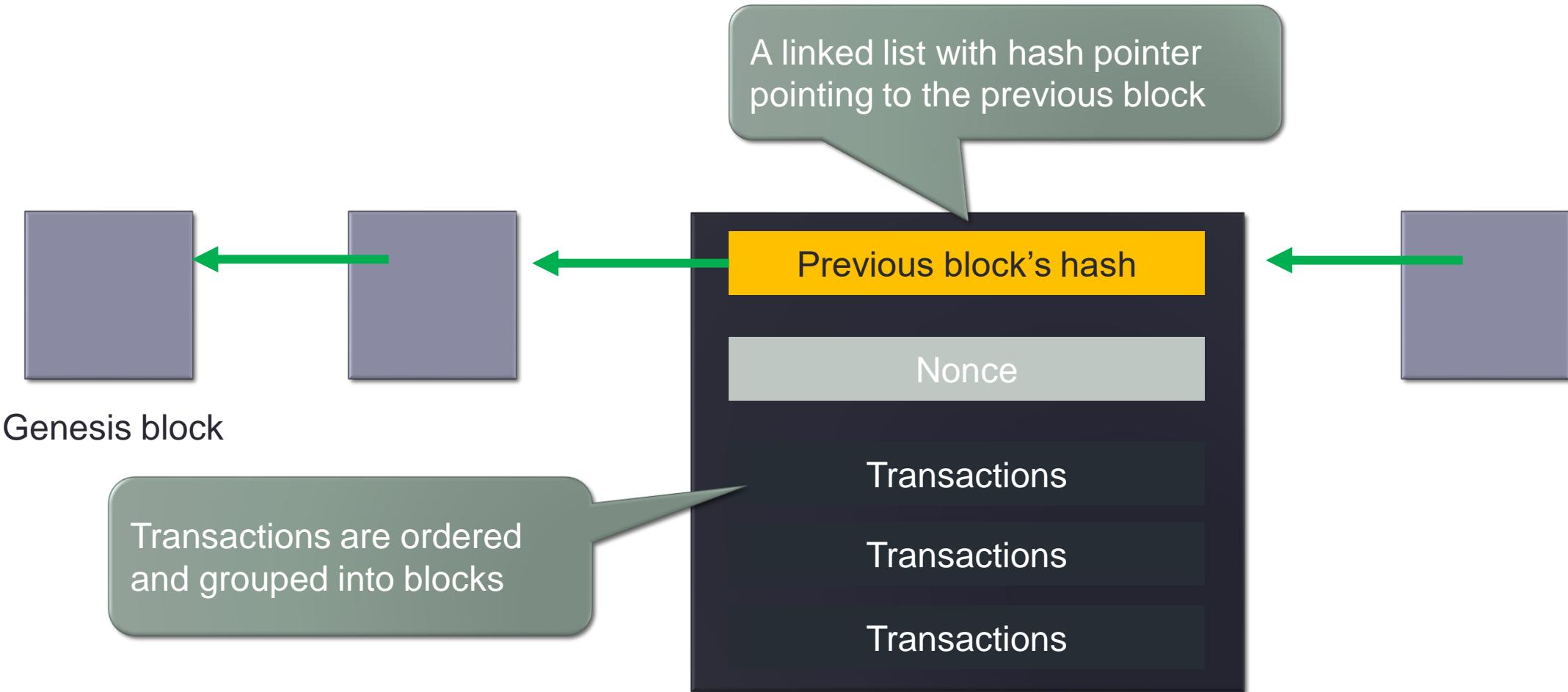
Decentralization

- An example of a **centralized system** is the banks. The banks store all your money, and the only way that you can pay someone is by going through the banks.
- Another example is the client-server systems. The servers store all your information. The only way that you can get the information is by sending query to the servers.

Decentralization

- Vulnerabilities of **centralized systems**:
 - Because they are centralized, all the data is stored in centralized locations. This makes them easy targets for potential hackers.
 - If the centralized system were to go through an upgrade or a shutdown, it would halt the entire system, and nobody will be able to access the information that it possesses.
 - Worst case scenario, if this entity gets corrupted, all the data that is inside the system will be compromised.
 - In **decentralized systems**, you can interact with your peers directly without going through a third party. An example is the Bitcoin. You can send your money to your peers without having to go through a bank.

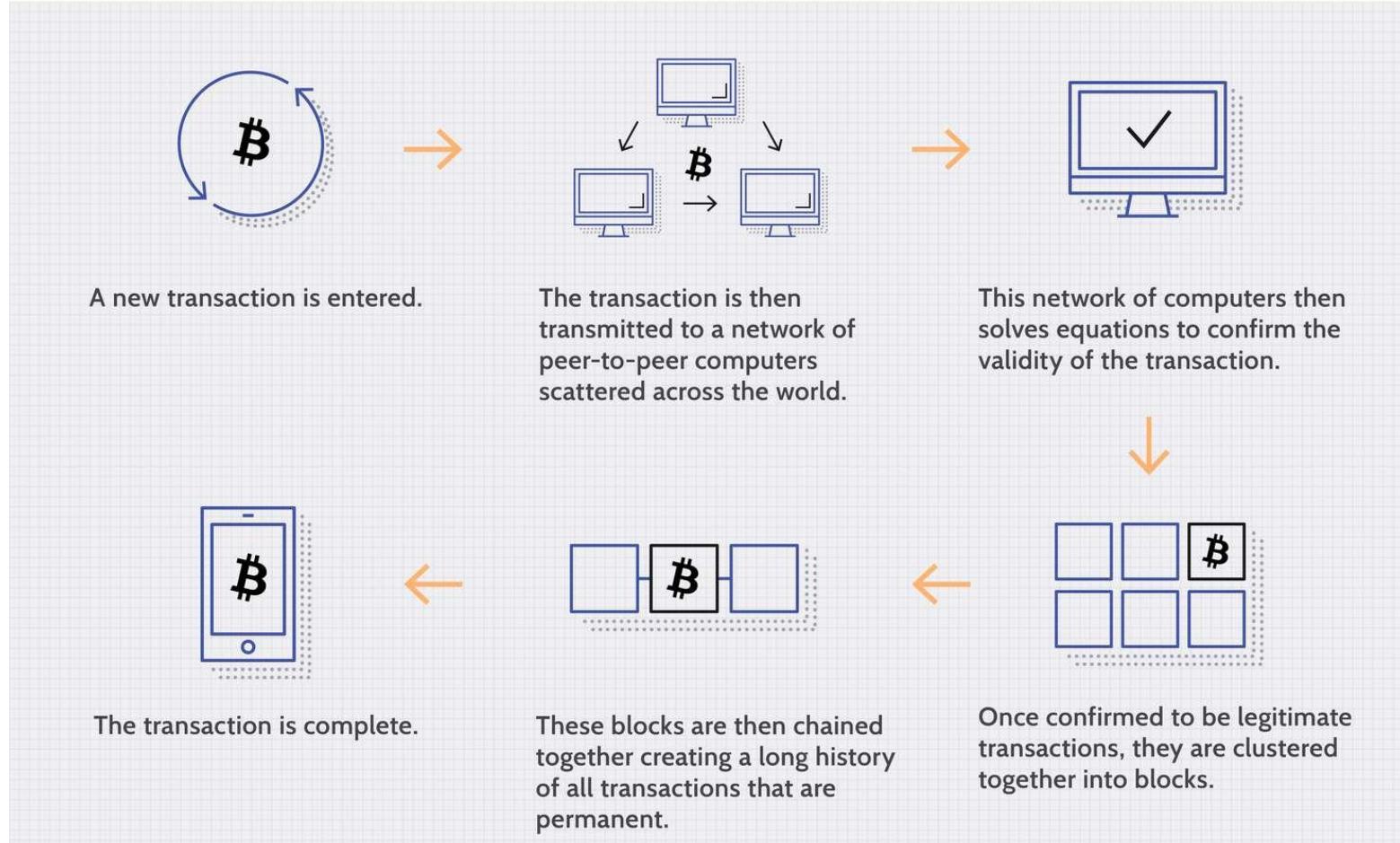
Structure of a Blockchain



How does a Blockchain Grow?

1. A user (node) creates and **signs** a transaction with its **private key**.
2. The transaction is propagated to multiple peers (**miners**) to **validate** the transaction.
3. After validation (by more than one node), the transaction is added to a new block. The block will be propagated onto the network (transaction confirmed).
4. The block becomes part of the ledger and the next new block links itself to the block. Transaction is double-confirmed while the block is confirmed.
5. Transactions are reconfirmed whenever a new block is created.
 - After six confirmations in the bitcoin network, the transaction is considered final.

How does a Blockchain Grow?



Generic Elements of Blockchain

- Addresses
 - Unique identifiers used in a transaction on the blockchain to denote senders and recipients
 - **Public key** or derived from a public key
 - A new address is generated for each transaction (to avoid linking transactions to the owner)



Bitcoin Address

bc1q49rvw2wec4vwaq36r7enszht5h02zrhk59aekf



Binance Pool

Miner



Base58 (P2PKH)



Bitcoin Address

1Q8QR5k32hexiMQnRgkJ6fmmjn5fMWhdv9

Generic Elements of Blockchain

- **Transaction**
 - Fundamental unit of a blockchain
 - A transfer of value from one address to another

TX
USD

Bitcoin Transaction

Broadcasted on 11 Apr 2023 10:20:15 GMT+8

Hash ID
180b4f0b0237686319523db9165d5bc5c1aff8d9c1
8f244684d93a545e0e2216

Amount	0.00490323 BTC • \$147.46
Fee	24,786 SATS • \$7.45
From	2 Inputs
To	3 Outputs

Confirmed

This transaction has 4 Confirmations. It was mined in Block 784,931

From	To
 1 bc1qj8mptgj2ddn8zaj7ma6r8ht46g7ysz8xlx8aal 0.00311093 BTC • \$94.13	 1 bc1q4t5kw73yl6pq9cneqqgx7rgr473ymquym2z9xc4 0.00163534 BTC • \$49.48
 2 bc1q9jnt55xe024nj8r950vpe075j48ht28hst80ht 0.00204016 BTC • \$61.73	 2 bc1qjm7mwdnjhmpl445a0ykjqzwzvknmvj979u6zzl 0.00264072 BTC • \$79.90
	 3 1ChD55vrNF2NspFWwXrNyevP1H5Vb5RVrB 0.00062717 BTC • \$18.98

Generic Elements of a Blockchain

- Block
 - Composed of multiple transactions
 - Also contains other elements like previous block hash, timestamp



Number	Hash	Miner	Mined	Tx Count	Nonce	Fill	Size	Total Sent	Total Fees
784934	0000-4512	ViaBTC	18m 9s	2,600	761,910,339	127.64%	1,338,407 Bytes	6,663 BTC	0.26BTC
784933	0000-ef39	F2Pool	40m 1s	2,294	3,397,150,738	160.66%	1,684,661 Bytes	11,321 BTC	0.15BTC

Blockchain Miner

- Validates transactions broadcasted on the network by **verifying and validating signatures and outputs**.
- Assembles a set of validated transactions into a potential block.
- Performs **Proof-of-Work (PoW)** (to be explained) to create a new block.
- Broadcasts the new block for other miners to verify and accept.
- Claims reward (such as Bitcoin)

How much a miner can be rewarded to create a new block?

6.25 bitcoin

Bitcoin mining

- ❑ Mining is a distributed consensus system that is used to confirm pending transactions by including them in the block chain.
- ❑ enforces a chronological order in the block chain, protects the neutrality of the network, and allows different computers to agree on the state of the system.
- ❑ transactions must be packed in a block that fits very strict cryptographic rules that will be verified by the network.

Mining can:

- ❑ prevent previous blocks from being modified because doing so would invalidate all the subsequent blocks.
- ❑ creates the equivalent of a competitive lottery that prevents any individual from easily adding new blocks consecutively to the block chain.
- ❑ No one can control what is included in the block chain or replace parts of the block chain to roll back their own spends.

What is Bitcoin Mining

- <https://www.youtube.com/watch?v=mrtSAgcpack>



Cost of Mining

- Hardware
 - Not an average computer
 - A mining rig
- Electricity
- Other cost of equipment to support mining rig
 - Ventilation, cabling, etc.
- Fee charged by mining pools
 - Commercial mining pools such as AntPool, F2Pool provide mining service to miners.



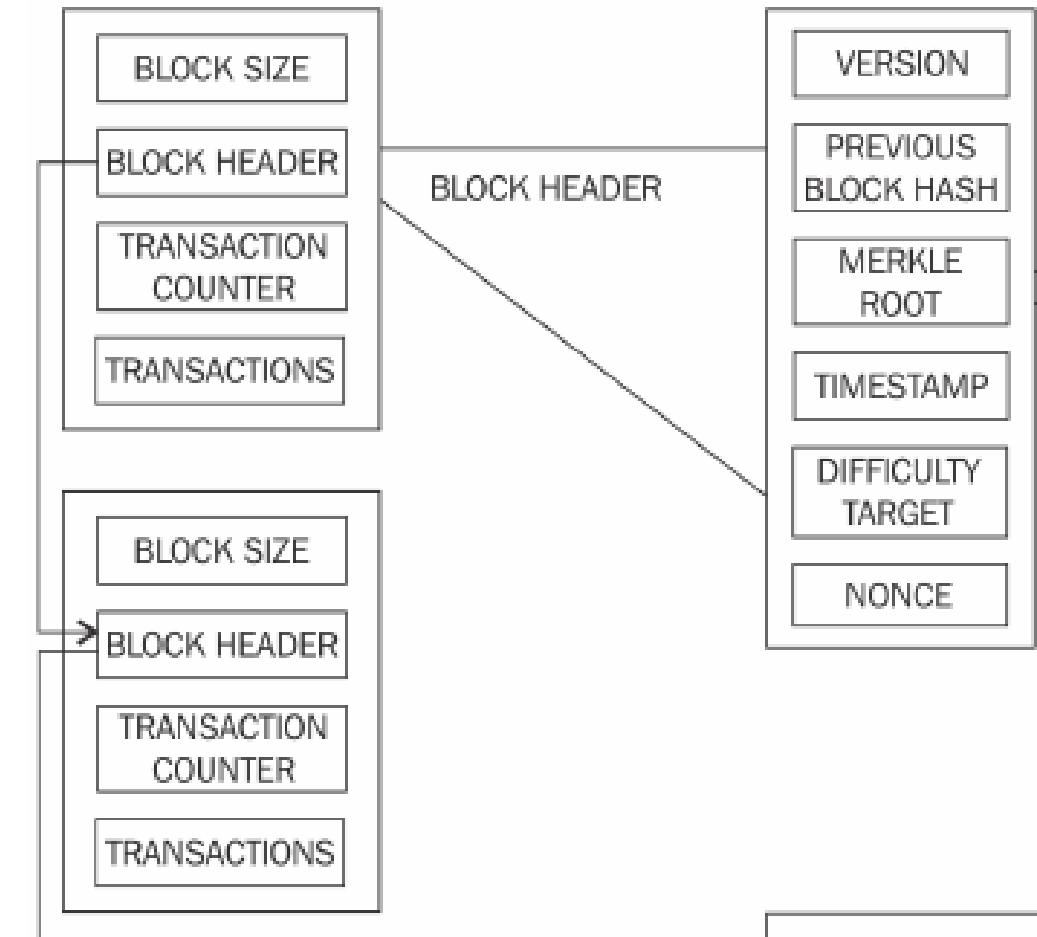
Four types of mining (CPU, GPU, FPGA, and ASIC)

Proof of Work (PoW)

- Blocks are added in the blockchain only after successful **Proof-of-Work (PoW)** solution.
- PoW based on **hashcash** (an e-cash scheme) is currently used in Bitcoin.
- PoW is done by miners, who compete to add new blocks to the chain, by solving a computationally difficult puzzle to meet a pre-determined target that requires a lot of computing power.

Proof of Work (PoW)

- Solving the puzzle is to compute the double **hash** of a block header with a **nonce** and the previous **hash** using the **SHA-256** algorithm.
- Solving the puzzle **proves** that the miner has done the **work** by spending computational resources to build a valid block.



Hash Function

- ▶ Take input of arbitrary length
- ▶ Output a **fixed length** hash value (or simply hash)
- ▶ Always produce the same output for a given input
- ▶ Output cannot be reversed to show the original input

$h(x) = x \% 5$	Hash value
100%5	0
154829%5	4
2156489877%5	2

Hash Function

- Hash can be considered as a digital fingerprint of data.
- A small change in the input string will give a totally different hash (avalanche effect).
- Example: SHA-256 is used by PoW in blockchain and bitcoin.
 - Input: message size < 2^{64} bits
 - Output: 256 bit
 - <https://emn178.github.io/online-tools/sha256.html>

Input string	<u>SHA-256</u>
ELEC2544	76b3b6545e1f65993f49ec7ef496235e8213c87228 ef2ee4fc2115a6633c655c
ELEC2545	8ce7cbdca9f0326545c52561aca95c5c9099a8d525 b8422eddbb0345c759f8bb

Hash Function

- Generating hash is a compute intensive process, but easy and quick to verify.
- Why? Let's try.
- Challenge: Find a number to make the hash start with four zeros.

Input string	<u>SHA-256</u>
ELEC2544	76b3b6545e1f65993f49ec7ef496235e8213c87228 ef2ee4fc2115a6633c655c
ELEC2545	8ce7cbdca9f0326545c52561aca95c5c9099a8d525 b8422eddbb0345c759f8bb

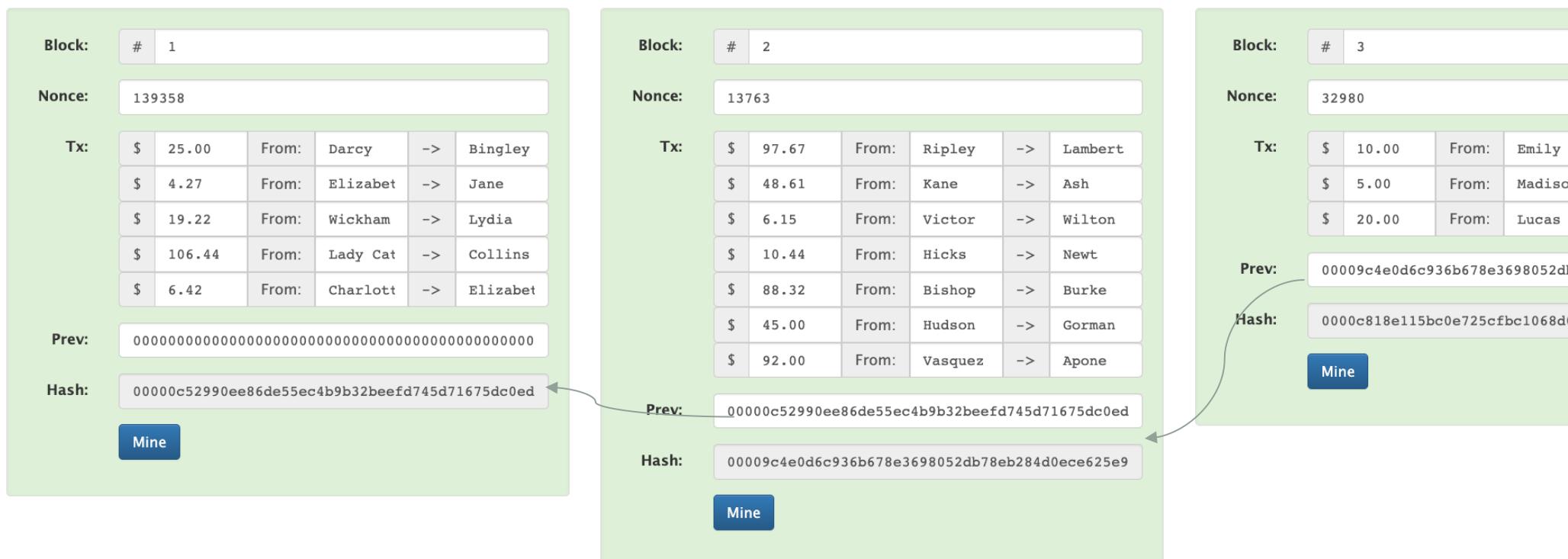
Hash of a Block and Mining

- Hash of a block covers all the information in a block such as block #, nonce and data.
- Suppose a block is valid if the hash starts with four zeros.
- Mining is the process of finding a number for nonce to make the hash start with four zeros again.



Blockchain

- A block contains hash of the previous block, i.e, each block points backwards to the one before it.



Demo of blockchain on Youtube

https://www.youtube.com/watch?v=_160oMzbIY8&t=691s

Blockchain Demo Hash Block Blockchain Distributed Tokens Coinbase

Coinbase Transactions

Peer A

Block	#	4
Nonce	19358	
Coinbase	\$ 100.00	-> Anders
Tx:	\$ 10.00	From: Sylve -> Bugs
	\$ 5.00	From: Twee -> Roadr
	\$ 20.00	From: Daffy -> Marvi
Prev:	000057a728d2dc10eff73f129e319ac636619;	
Hash:	0000ff15c919e4dc59836f8d196ed6d6e9b67;	

Block	#	5
Nonce	168037	
Coinbase	\$ 100.00	-> Sophia
Tx:	\$ 2.00	From: Jacks -> Alexa
	\$ 6.00	From: Ryan -> Carte
	\$ 4.00	From: Ryan -> Riley
	\$ 9.95	From: Grace -> Kathe
Prev:	0000ff15c919e4dc59836f8d196ed6d6e9b67;	
Hash:	0000866779af5c690006fcad95e45aff6117c;	

can just go backwards and find that

Mine

16:11 / 17:49 • Coinbase Trans

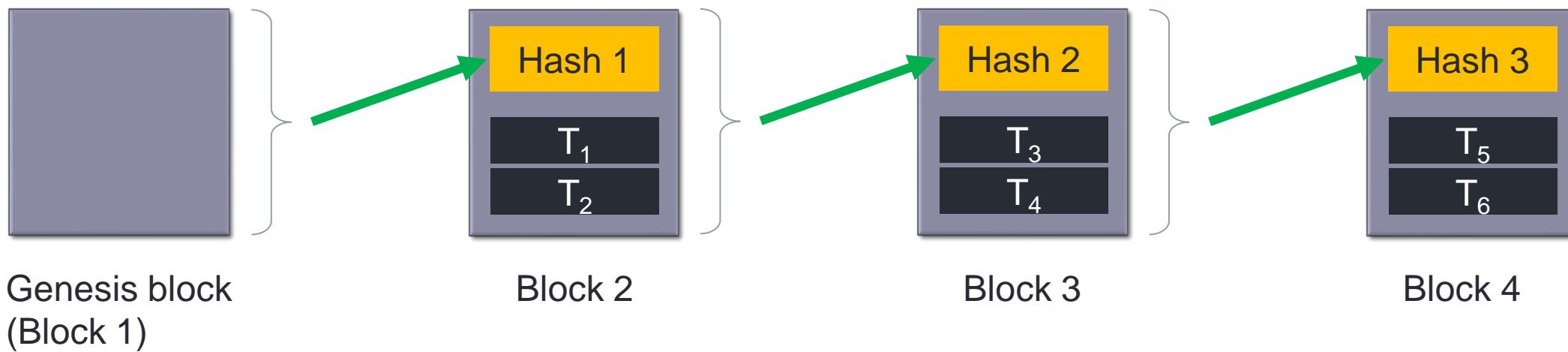
Blockchain

- Making a change of the data in a block is almost impossible (immutability) because the change invalidates the block and all the following blocks in the blockchain, not to mention copies of the blockchain in numerous nodes in a distributed system.

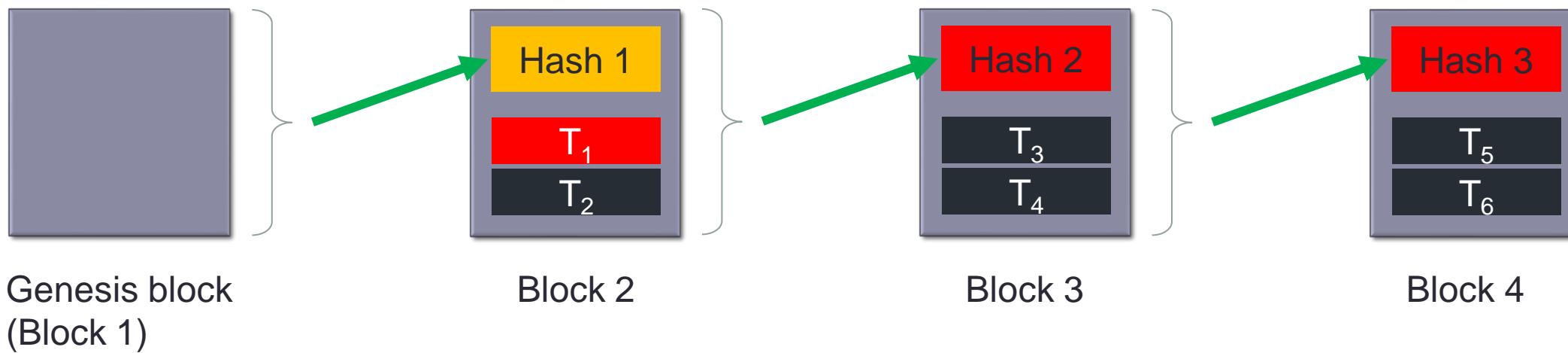
Block:	#	2	
Nonce:	13763		
Tx:	\$ 97.67	From: Ripley	-> Lambert
	\$ 48.61	From: Kane	-> Ash
	\$ 10.15	From: Victor	-> Wilton
	\$ 10.44	From: Hicks	-> Newt
	\$ 88.32	From: Bishop	-> Burke
	\$ 45.00	From: Hudson	-> Gorman
	\$ 92.00	From: Vasquez	-> Apone
Prev:	00000c52990ee86de55ec4b9b32beef745d71675dc0ed		
Hash:	12df67b426b70e5b125341b3eb48d19649496e0a761e10		
	Mine		

Block:	#	3
Nonce:	32980	
Tx:	\$ 10.00	From: Emily
	\$ 5.00	From: Madison
	\$ 20.00	From: Lucas
Prev:	12df67b426b70e5b125341b3eb480	
Hash:	254b88c9f9c3fa1f4550e384bc200	
	Mine	

Blockchain



Blockchain



Benefits of Blockchain

- Decentralization
 - No need for a trusted third party or intermediary to validate transactions.
 - A consensus mechanism is used to agree on the validity of transactions by all parties without the requirement of a central authority.
- Transparency and trust
 - Blockchains are shared.
 - Everyone can see what is on the blockchain.
- Immutability
 - Data / transactions once added onto the blockchain are immutable.
 - To roll back the changes is considered almost impossible as it will require an unaffordable amount of computing resources.

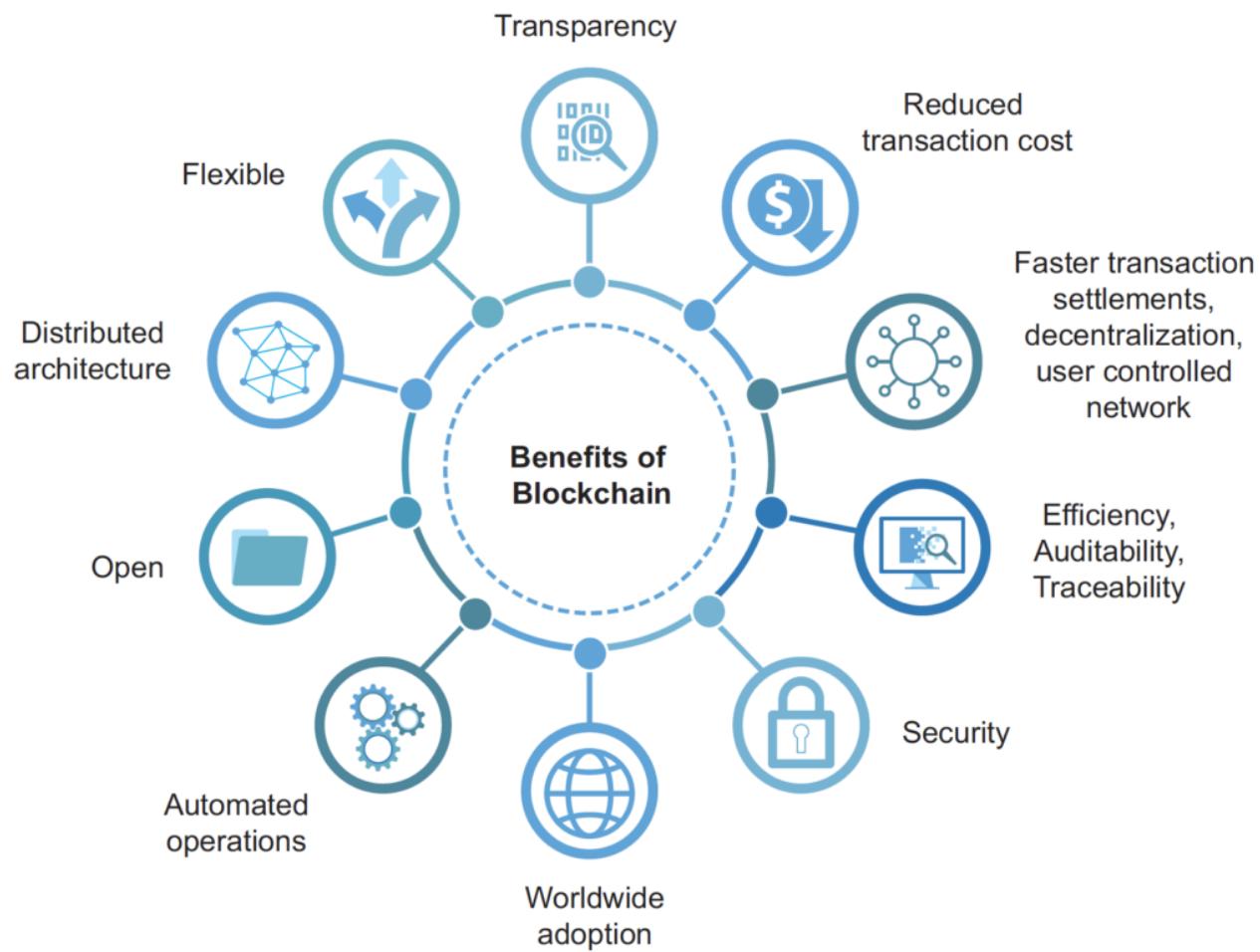
Benefits of Blockchain

- High availability
 - Data are replicated on thousands of nodes in a peer-to-peer network.
- Highly secure
 - Blockchain is based on proven cryptographic technology that ensures the **integrity** of data.
 - All actions in blockchain are secured by using **private keys** and **digital signatures**.
- Simplification of current paradigms
 - Current model: multiple entities maintain their own databases and data sharing is very difficult
 - A blockchain is a single shared ledger among interested parties, reducing the complexity of managing the separate systems maintained by each entity.

Benefits of Blockchain

- Efficient
 - Allows quicker settlement of trades in financial industry because a shared ledger agreed between financial organizations is already available on blockchain.
 - Avoid lengthy processes such as verification, reconciliation, and clearance.
- Cost saving
 - No third party or clearing houses are required in blockchain.

Benefits of Blockchain



Bitcoin

2008: Blockchain was introduced with the invention of bitcoin

2009: First practical implementation

Digital Cash

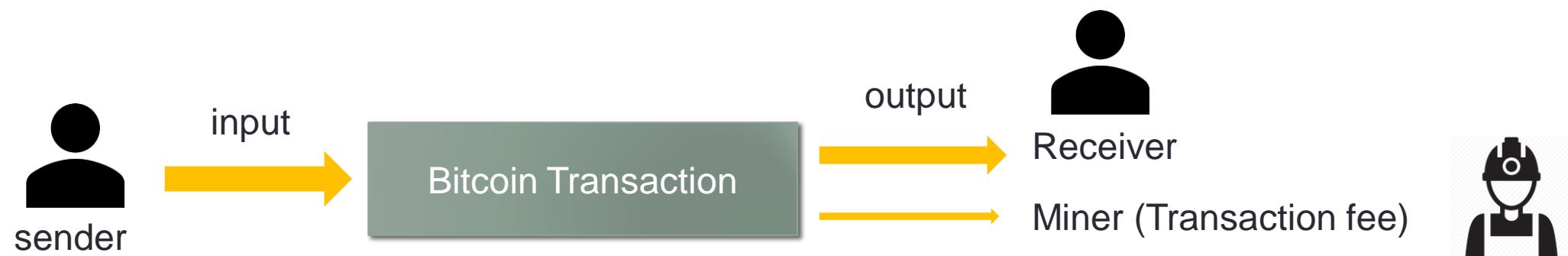


Cryptography

Distributed Computing

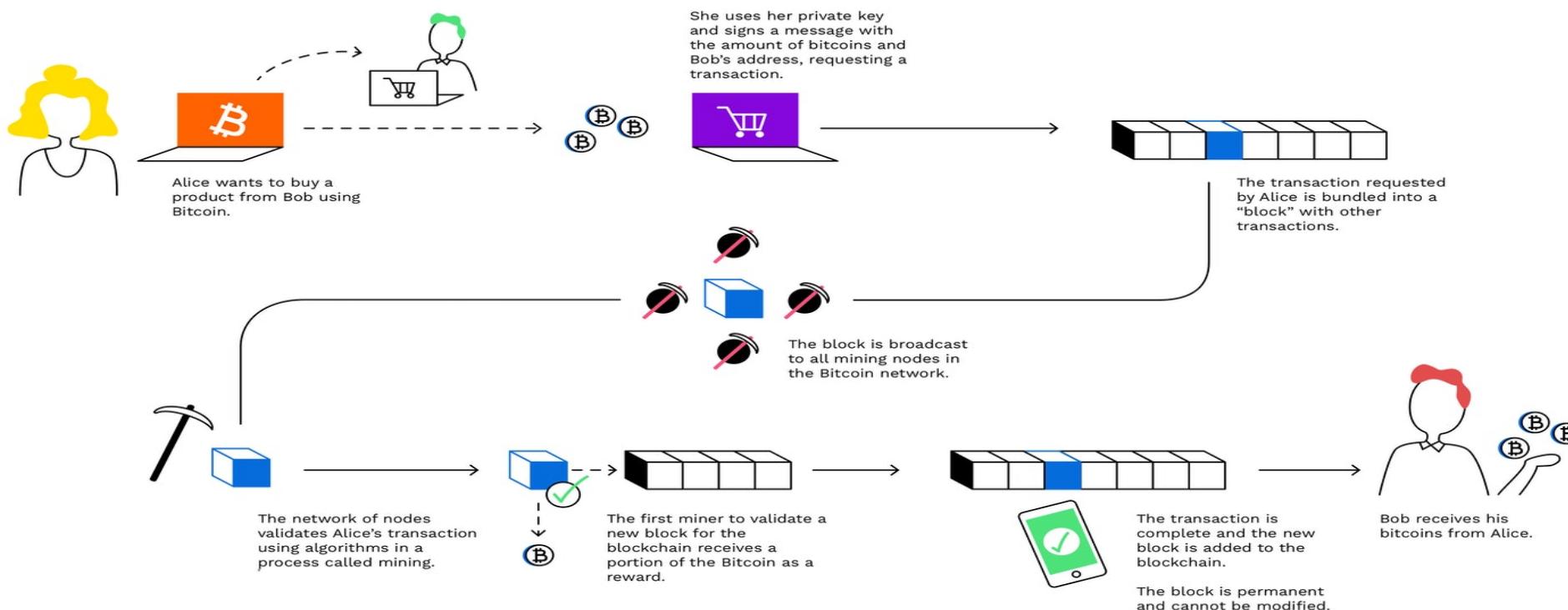
Bitcoin Transaction

- Bitcoin transaction tells the network that the owner of some bitcoin value has authorized the transfer of that value to another owner
- New owner can also send the bitcoin by creating another similar transaction



Transactions

- A transaction is a transfer of value between Bitcoin wallets that gets included in the block chain.
- Bitcoin wallets keep a secret piece of data called a private key, which is used to sign transactions, providing a mathematical proof that they have come from the owner of the wallet. The signature also prevents the transaction from being altered by anybody once it has been issued.
- All transactions are broadcast to the network and usually begin to be confirmed within 10-20 minutes, through a process called mining.

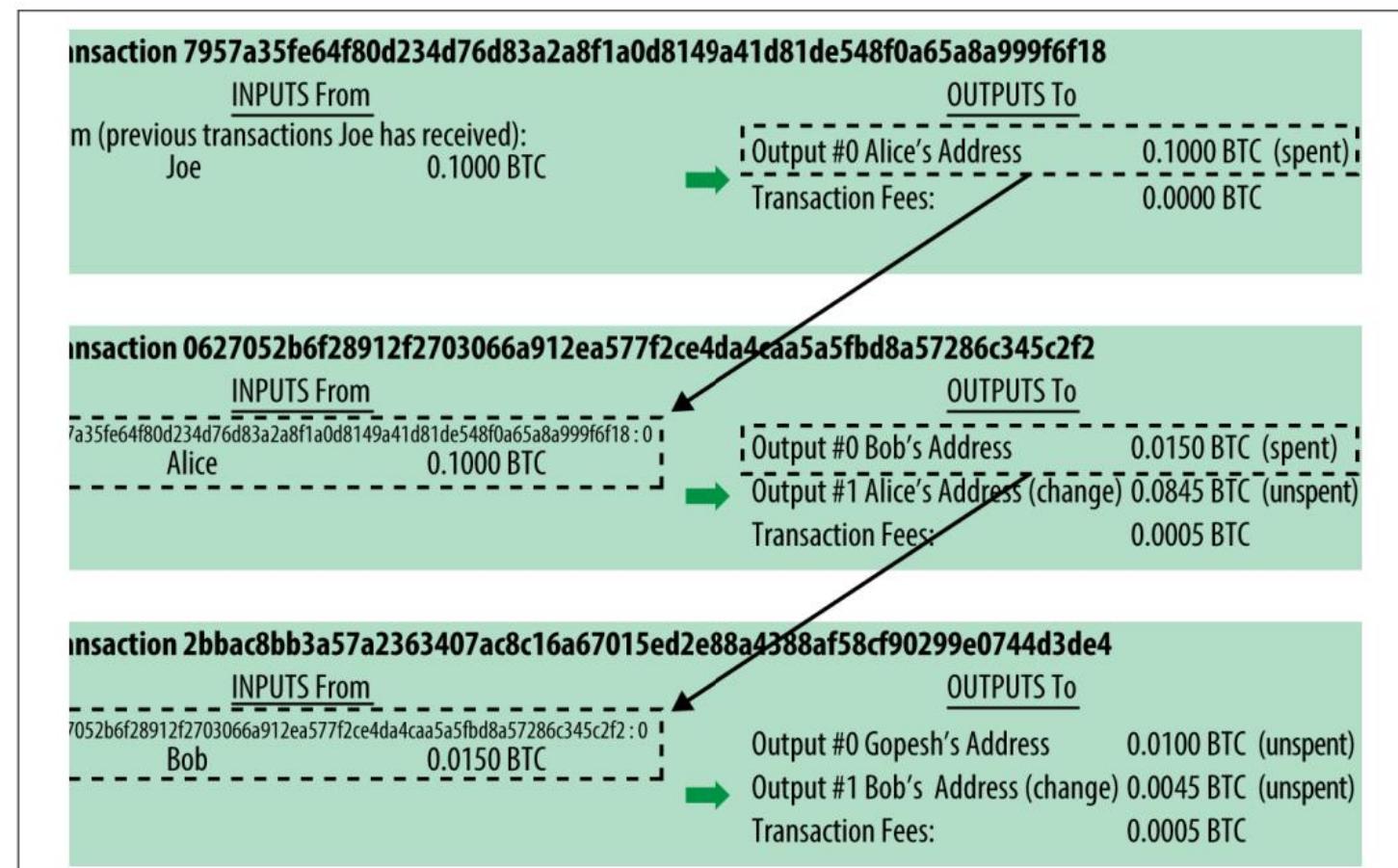


Bitcoin Transaction

Example:

Chain of transactions from Joe to Alice to Bob

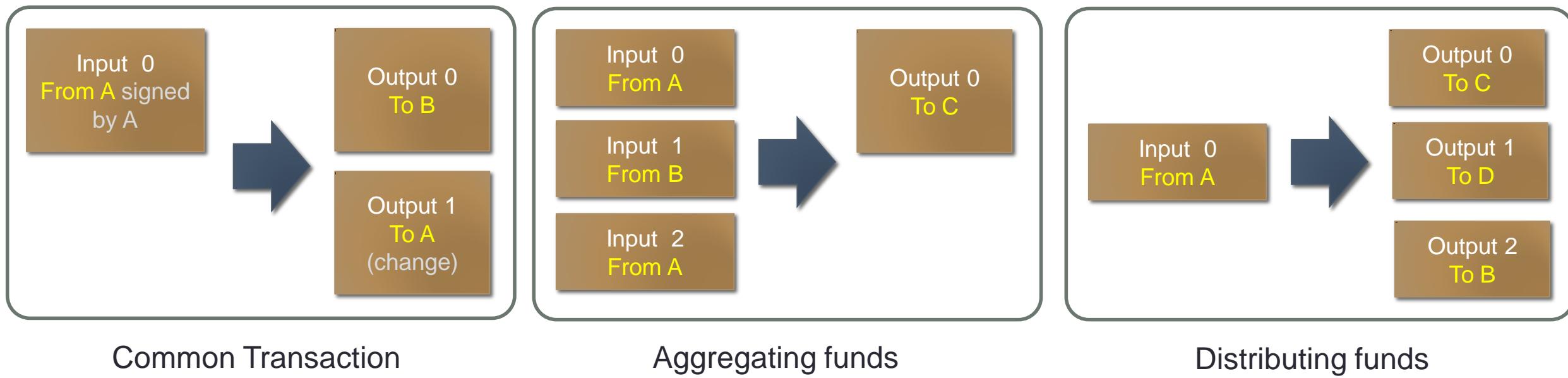
$$\sum \text{inputs} = \sum \text{outputs} + \text{transaction fee}$$



Bitcoin Transaction

- Each transaction contains one or more "inputs" and "outputs"
- Inputs: bitcoin account to be debited
- Outputs: bitcoin account to be credited
- Inputs and outputs are in bitcoin address
- Unspent bitcoin is output to original owner with same / different bitcoin address
- Transactions move value from transaction inputs to transaction outputs

Common Transaction Forms

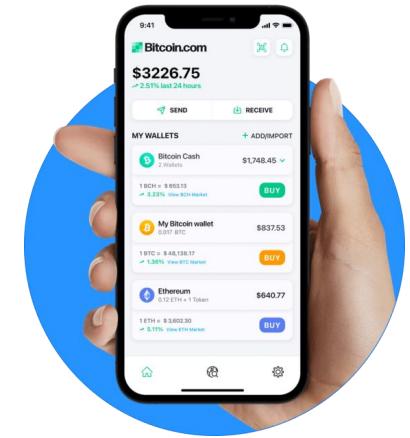


Life Cycle of a Transaction

1. A sender sends a transaction using **wallet** software.
2. The wallet software **signs** the transaction using the sender's **private key**.
3. The transaction is broadcasted to the Bitcoin network using a flooding algorithm.
4. **Miners** include this transaction in the next block to be mined.
5. The miner who solves the **Proof of Work** problem broadcasts the newly mined block to the network.
6. Other miners verify the block and propagate the block further, and confirmation starts to generate.
7. Finally, the confirmations start to appear in the receiver's **wallet** and after approximately six confirmations, the transaction is finalized and confirmed.

Bitcoin Wallet

- **Software/Hot Wallet:** run on internet connected devices like a computer, mobile phone, or tablet. Private keys are secret codes. Because hot wallets generate your private keys on an internet connected device, these private keys can't be considered absolutely secure.
- **Hardware Wallet:** store your private keys in a secure offline environment on the hardware wallet and is separated from the internet-connected devices.
- **Cold Storage Wallet:** store your crypto coins encrypted in a piece of hardware that resembles a wallet. The data can only be accessed with explicit authorization from the holder.



Bitcoin Wallet



Support us

[Contribute](#)

[Subscribe](#)

[LOGIN](#)

[NEWS](#) [CORONAVIRUS ADVICE](#) [LOCKDOWN GUIDE](#) [US POLITICS](#) [VOICES](#) [SPORT](#) [CULTURE](#) [INDY/LIFE](#) [INDYBEST](#) [INDY100](#) [VOUCHERS](#)

BITCOIN: MILLIONS OF DOLLARS OF CRYPTOCURRENCY 'LOST' AFTER MAN DIES WITH ONLY PASSWORD

Conspiracy theories have been raised about the whereabouts of the QuadrigaCX exchange's funds

Anthony Cuthbertson | [@ADCuthbertson](#) |
Tuesday 5 February 2019 11:45 | 20 comments



The unexpected death of the owner of Canada's largest [cryptocurrency](#) exchange has left £145 million of cryptocurrency locked in a digital wallet to which he reportedly had the only password.



Bitcoin Wallet

Operating System

Mobile  **Desktop** 

Hardware 



User type

New 

Experienced 

Criteria

Control 

Validation Not available

Transparency Not available

Below is a list of wallets available for your operating system

iOS Wallets

Control Validation Transparency Environment Privacy Fees

 Bither	●	■	■	■	■	■	▲
---	---	---	---	---	---	---	---

 BitPay	●	▲	■	■	■	■	■
---	---	---	---	---	---	---	---

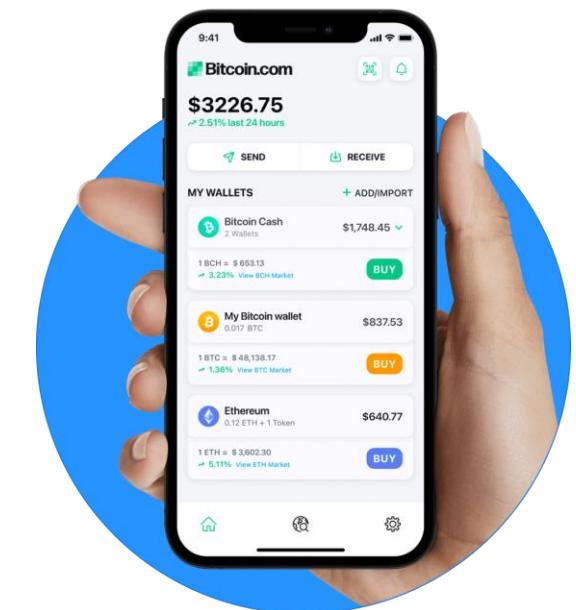
 BRD	●	■	■	■	■	■	●
--	---	---	---	---	---	---	---

 Edge	■	■	■	■	■	■	■
---	---	---	---	---	---	---	---

● Good ■ Acceptable ▲ Caution ■ Not applicable

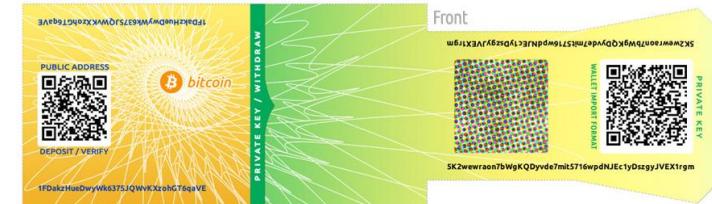
Bitcoin Wallets

- Software which stores **private or public keys** and **bitcoin address** (no coins)
- Receiving bitcoins
- Sending bitcoins
- No concept of balance and number of coins for a user; instead, transaction information stored on the blockchain such as unspent outputs are used to calculate the number of bitcoins.



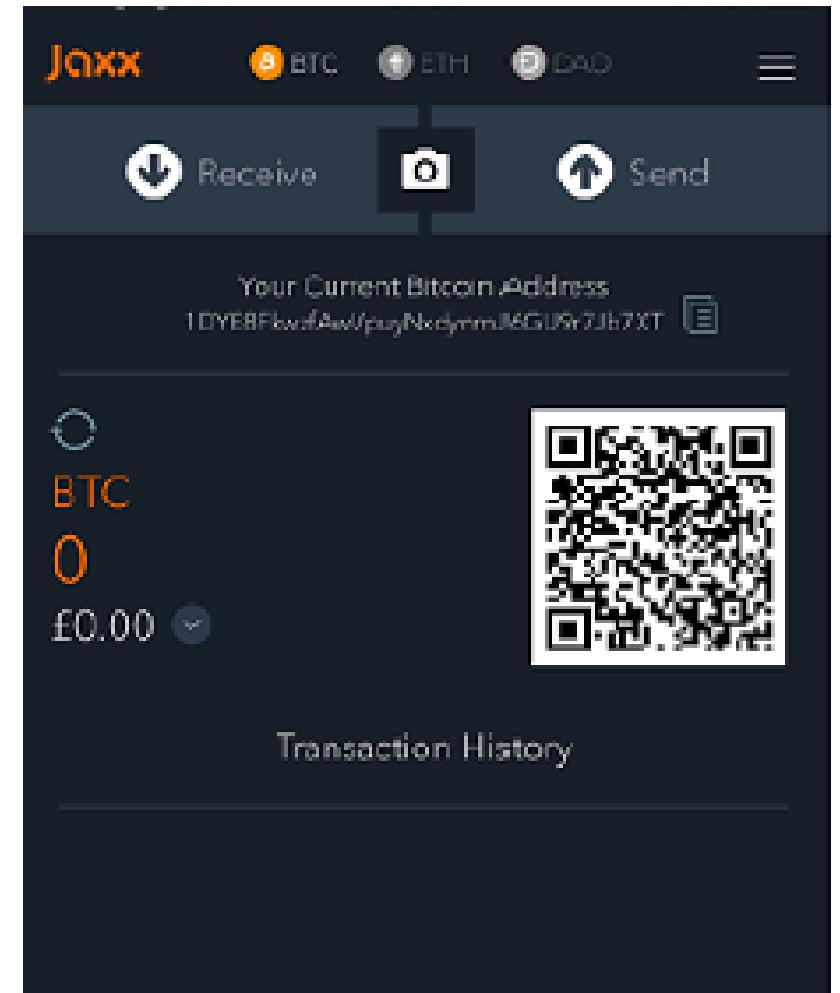
Wallet Types

- Paper wallets
 - Required key material is printed on a paper
 - Requires physical security
- Hardware wallets
 - Use custom-built device or NFC-enabled phone to store keys



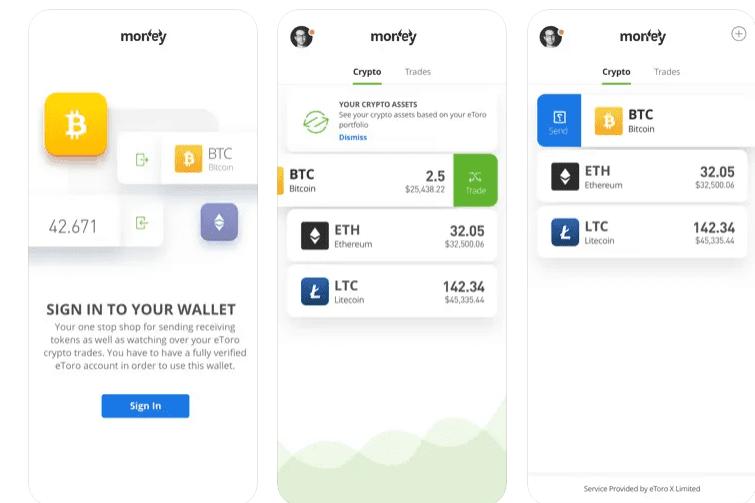
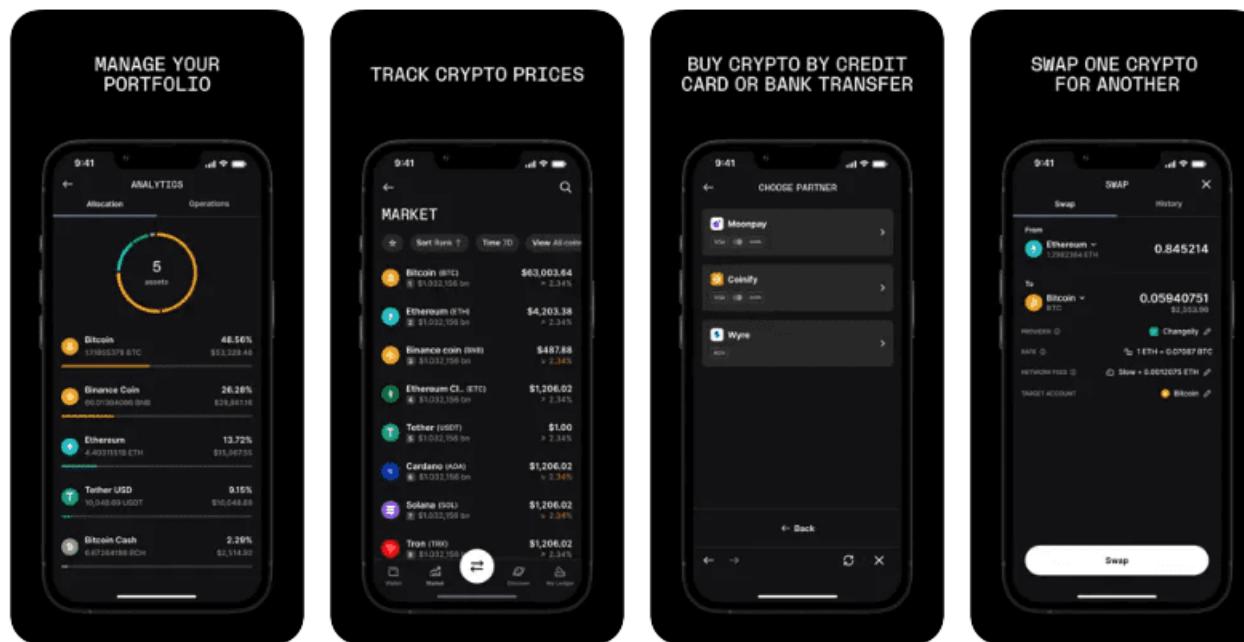
Wallet Types

- Online wallets
 - Stored in cloud
 - Users manage their wallets via web interface
 - Users must trust the online wallet service provider
- Mobile wallets
 - Installed on mobile devices
 - Use camera to scan QR code to make payments



Top 10 Recommended Bitcoin Wallets

- <https://prestmit.com/blog/top-10-recommended-bitcoin-wallets-iphone-users->



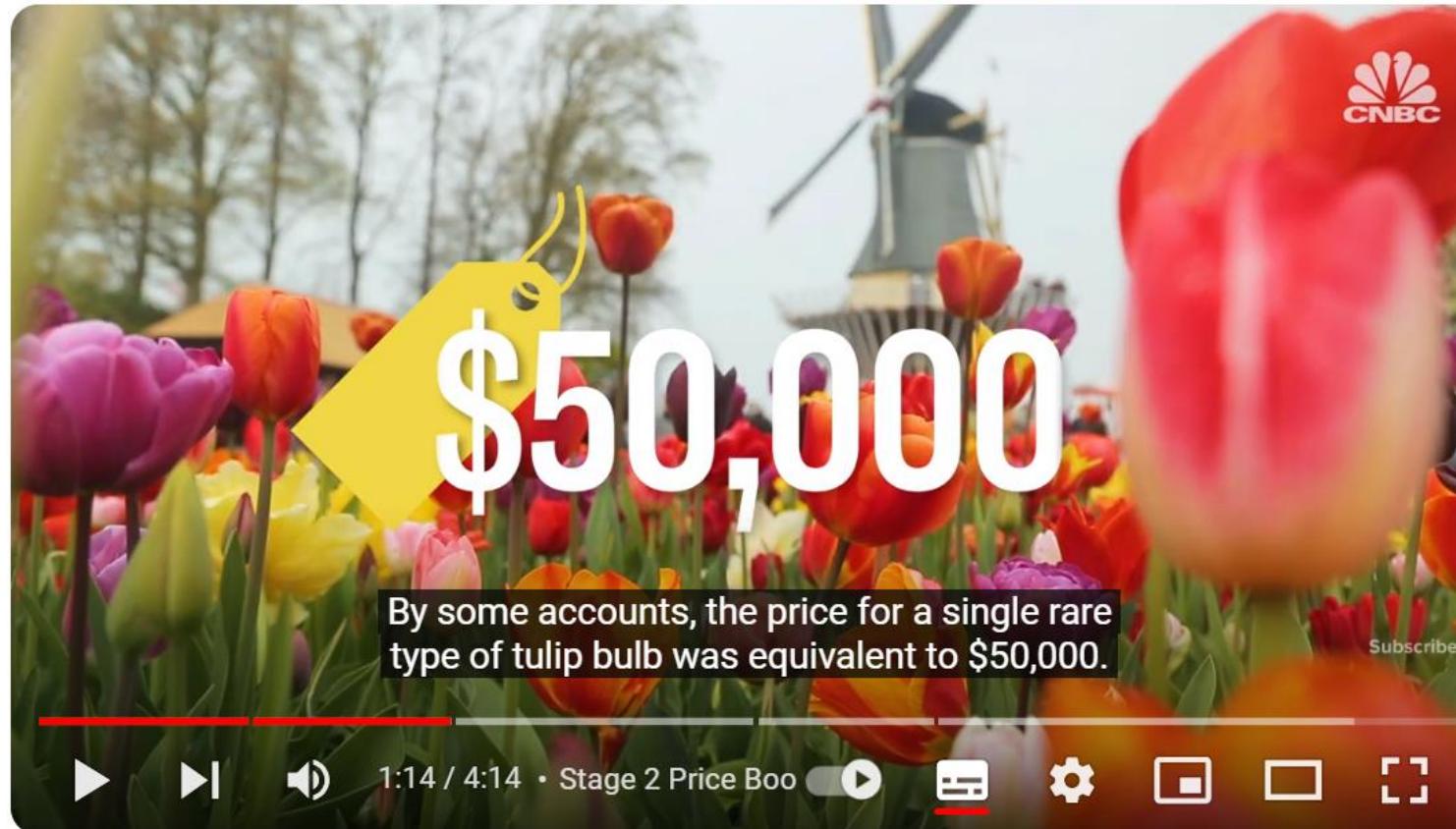
Bitcoin Payments

- Physical shops:
 - Use point of sale terminal and other specialized hardware
 - Customers can pay using their mobile phone by scanning the QR code with the seller's payment URI (Uniform Resource Identifier) which is a string that represents the transaction information
- Online shops:
 - Many online service providers offer bitcoin payment processor for integration with e-commerce websites.



A currency? Or a speculation?

- https://en.wikipedia.org/wiki/Tulip_mania
- <https://www.youtube.com/watch?v=3vDPowCDWc8>



Q&A

ELEC2544 Introduction to electronic commerce and financial technology

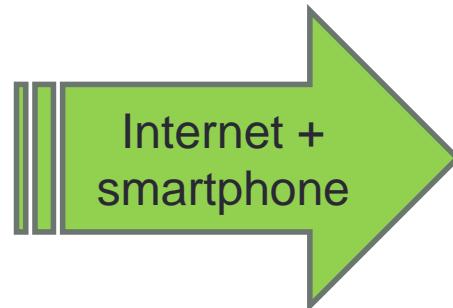
Introduction to FinTech

Dr. Wilton Fok

What is FinTech?

- A combination of '**finance**' and '**technology**'.
- Fintech refers new **technology** that seeks to **improve** and **automate** the delivery and use of **financial services**.

Computer technology used at the back office of banks



Consumer-oriented services such as payments apps, robo-advisors, and crypto apps, etc.

- source: <https://www.investopedia.com/terms/f/fintech.asp>

What is FinTech?

- Fintech describes a variety of financial activities:
 - money transfers, depositing a check **with your smartphone bypassing a bank branch** to apply for credit
 - raising money for a business startup, or managing your investments, **without the assistance of a person.**
- source: <https://www.investopedia.com/terms/f/fintech.asp>

What is FinTech

- integration of technology into offerings by financial services companies in order to improve their use and delivery to consumers.
- by unbundling offerings by such firms and creating new markets for them.
- Startups disrupt incumbents in the finance industry by expanding financial inclusion and using technology to cut down on operational costs.



A screenshot of the HSBC Online Banking interface. The top navigation bar includes links for "Back to previous version of Online Banking", "English", "United Kingdom", "Oliver Antony Maitland", and "Log off". The main menu offers "My banking", "Products & Services", "Investments & financial planning", and "Contact HSBC". The "My accounts" section displays a list of accounts: "BANK A/C" (marked with a green circle containing the number 1), "PREMIER BANK", and "PREMIER SAVE". The "BANK A/C" panel shows a balance of 0 GBP, available balance, and overdraft limit. It also indicates "There are no transactions to display for this account." (marked with a green circle containing the number 2). Other features like "Quick Transfer" and "Welcome" are visible at the bottom.

4

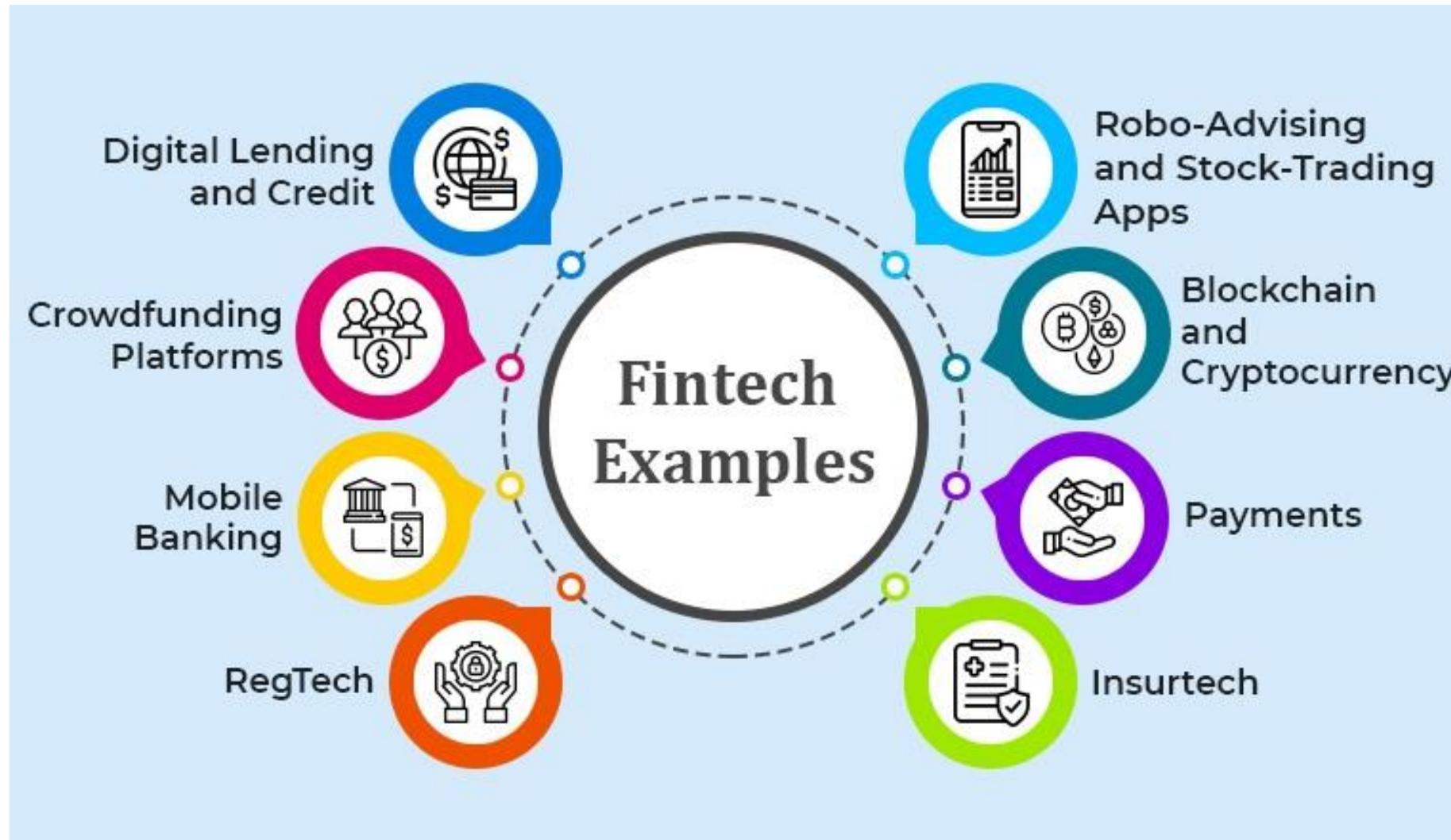
Source: Investopedia

What is FinTech?

- Use your browser to access: : hku.iclass.hk
- Login using your portal ID (Login through HKU Portal)
- **Join the course: (code: LS3151)**
- Give an example of FinTech



More than that

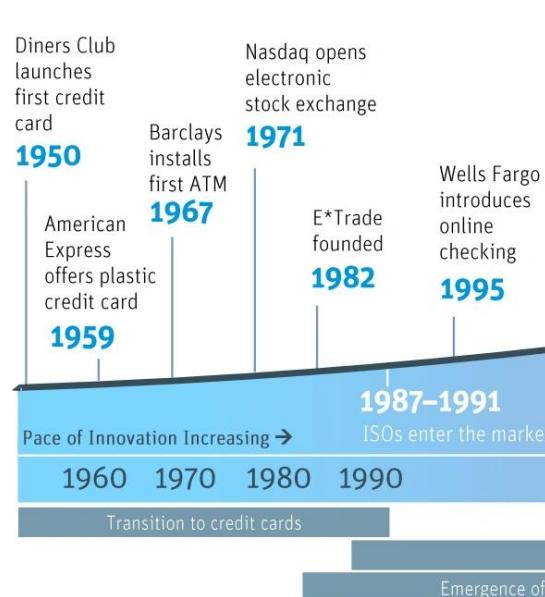


Evolution of FinTech

<https://explodingtopics.com/blog/fintech-guide>

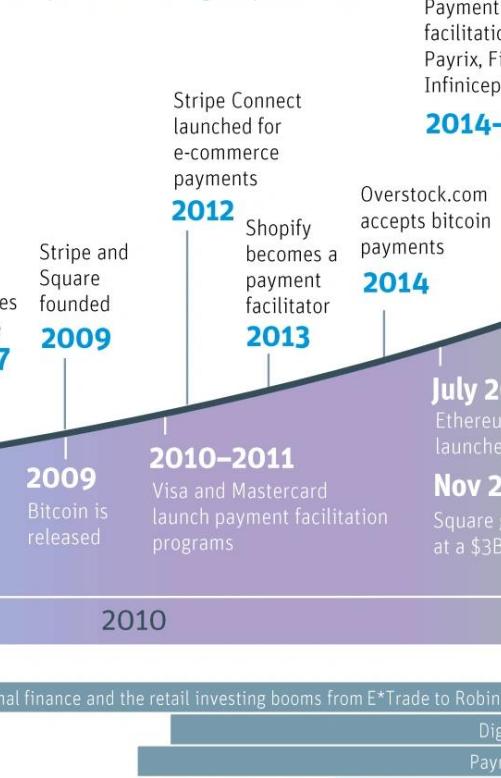
Fintech 1.0: Digitizing Finance

Analog financial services transition to digital, as banking, payments, lending and insurance move online.



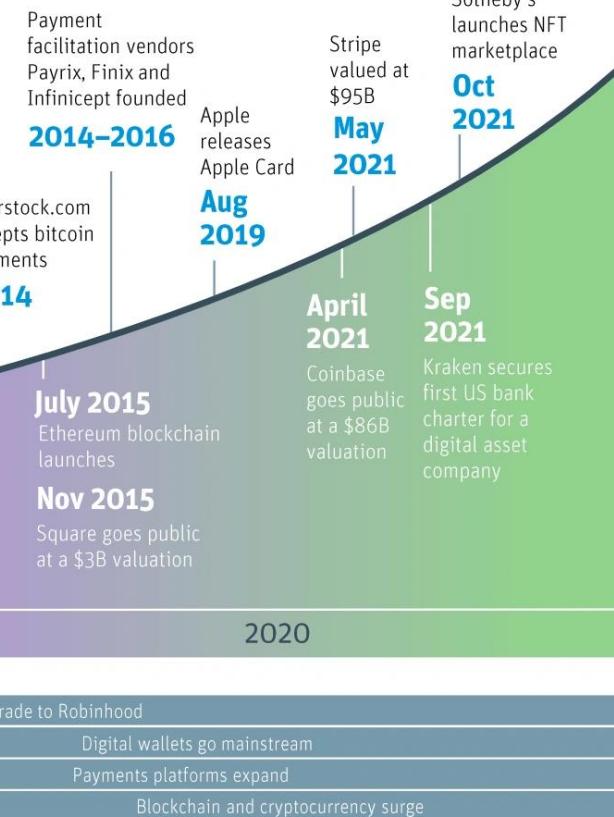
Fintech 2.0: Embedding Finance

Financial services leave the realm of standalone products and are incorporated into digital platforms.



Fintech 3.0: Decentralizing Finance

Financial services migrate away from centralized institutions and rely on self-executing blockchain contracts.



Source: Forbes article by Matthew Harris: The Future Of Money: A Complete Revolution and SVB Analysis.

STATE OF FINTECH: 2021

What does a typical FinTech company look like?

- Large, well-established financial institutions such as Bank of America, Chase
 - Also called incumbents
 - Big tech companies such as Apple, Google
 - Active in financial services space
 - Financial services facilitators such as Visa, MasterCard
 - Provide infrastructure or technology that facilitates financial services
 - Startups such as Stripe (mobile payment), Betterment (automated investing)
 - focused on a particular innovative technology
- source: <https://www.pwc.com/us/en/financial-services/publications/viewpoints/assets/pwc-fsi-what-is-fintech.pdf>



Google Pay



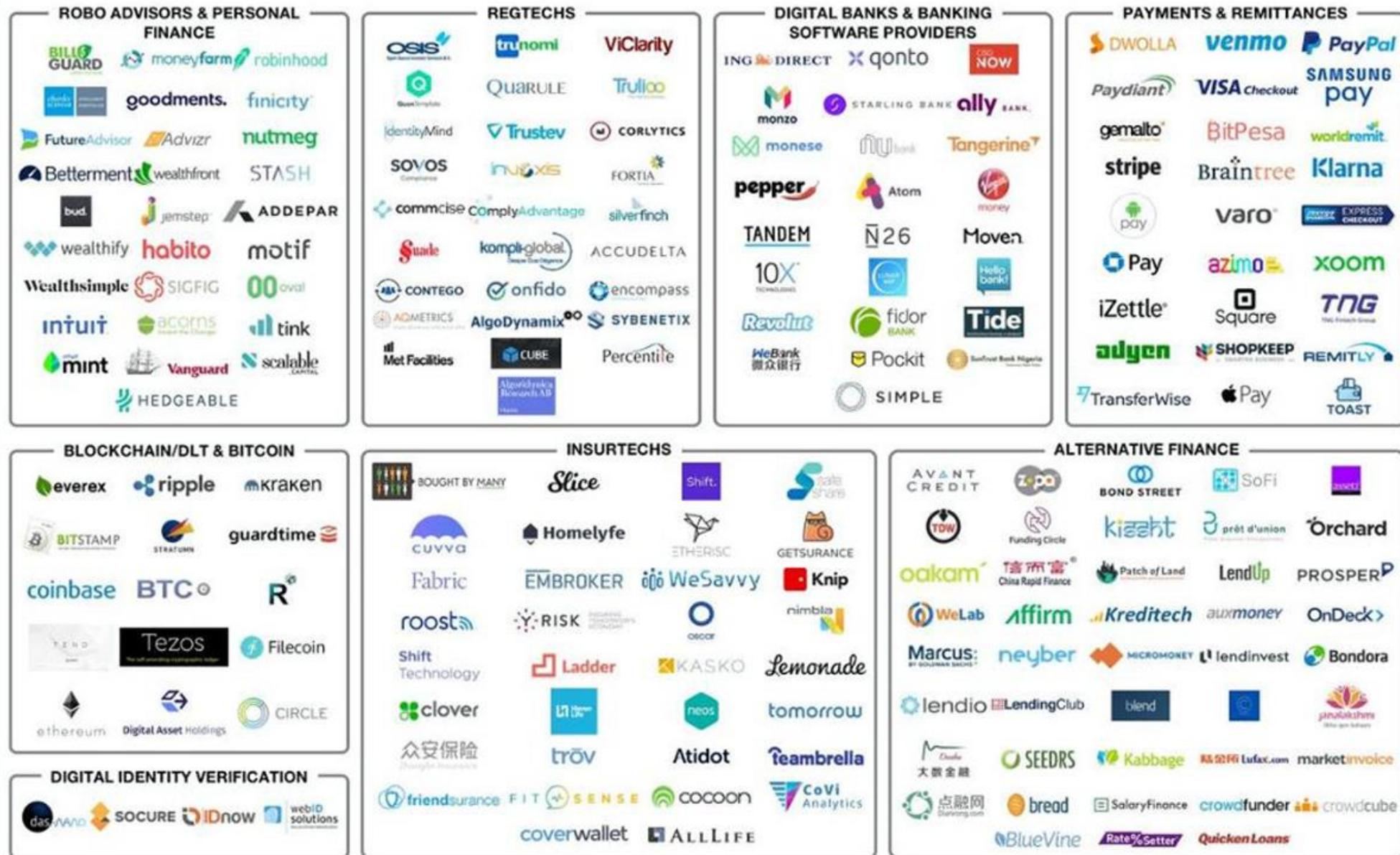
What does a typical FinTech company look like?

Fintech isn't static, it's evolving:

- Incumbents are becoming more technology focused.
 - Big tech companies are offering more financial services such as peer-to-peer payment solutions over social networks and email.
 - Startups are providing financial services such as payments and lending that are conventionally provided by banks.
- source: <https://www.pwc.com/us/en/financial-services/publications/viewpoints/assets/pwc-fsi-what-is-fintech.pdf>

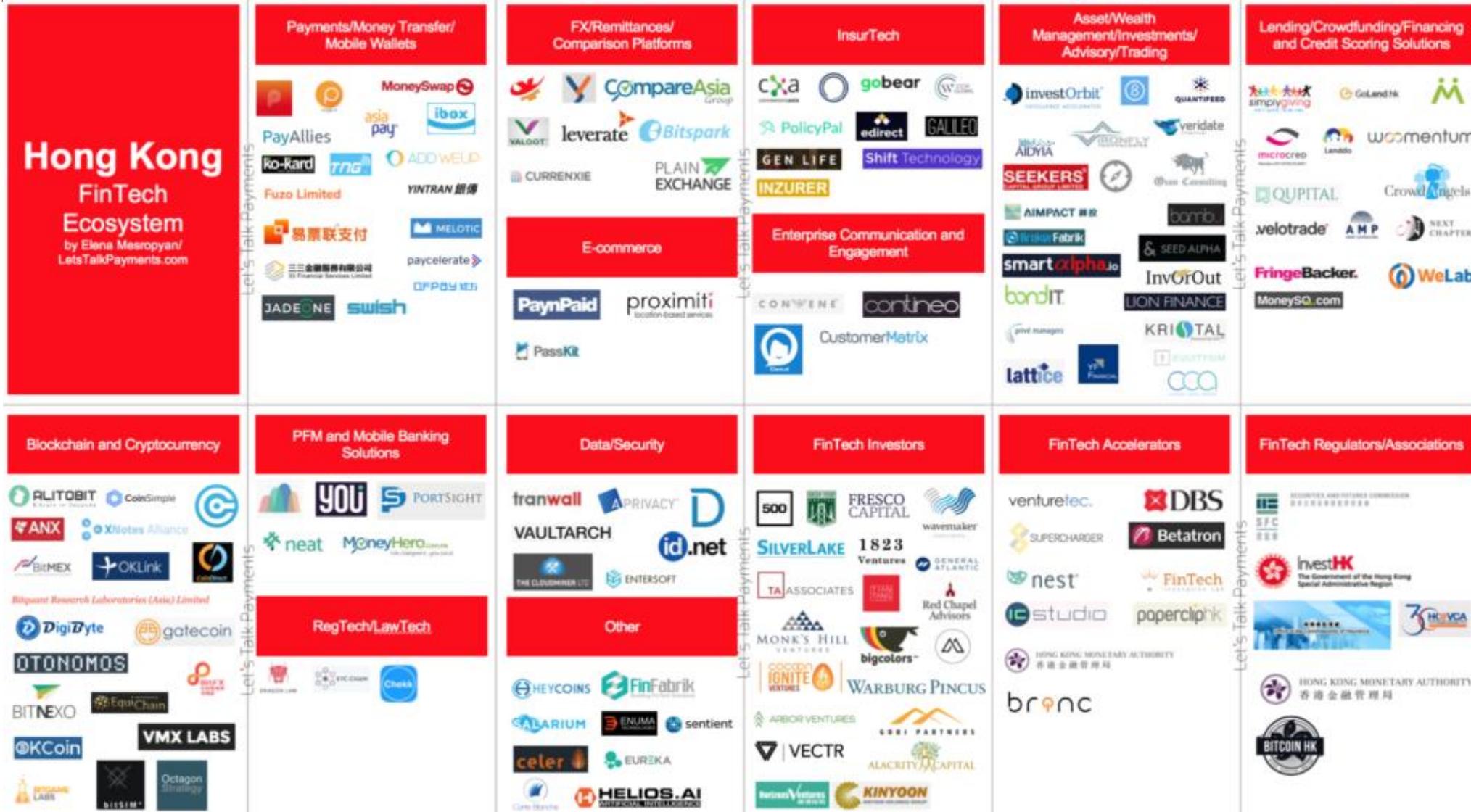


THE FINTECH ECOSYSTEM



Fintech ecosystem in HK

<https://zegal.com/blog/post/5-fintech-solutions-small-businesses-hong-kong/>

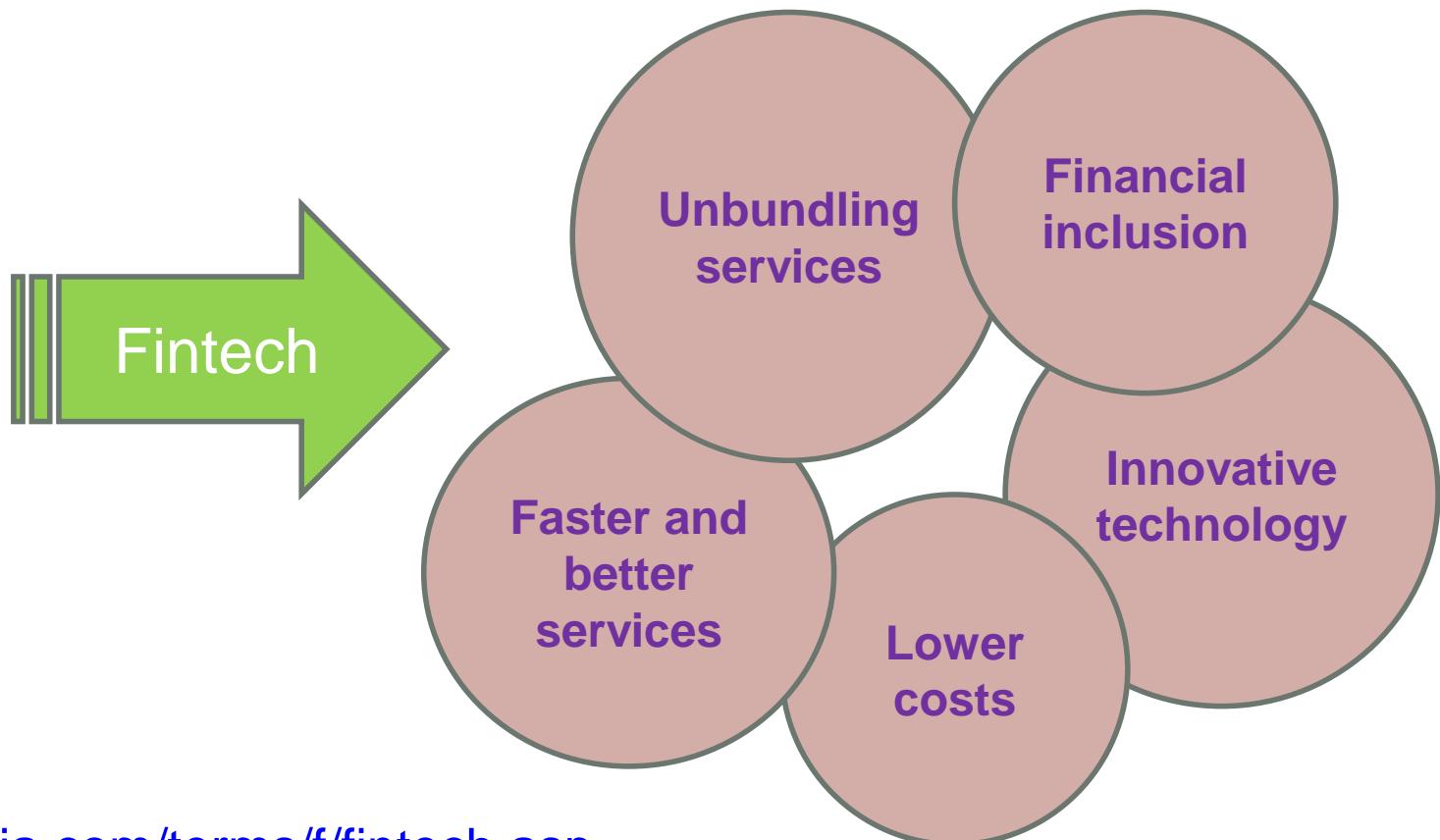


why disruption?

- Fintech startups are also called **disruptors**, as they are breaking into areas that banks and other legacy financial institutions have dominated.
- sources: <https://www.investopedia.com/terms/f/fintech.asp>

why disruption?

A variety of financial services ranging from traditional banking services to mortgage and trading services are offered by banks under a single umbrella.



- sources: <https://www.investopedia.com/terms/f/fintech.asp>

why disruption?

- Examples:
 - Stock trading: no fees for trades (lower cost)
 - Mortgage: pre-approval within 24 hours of submitting a home mortgage application (faster service)
 - Online shopping: immediate, short-term loans for purchases to consumers with poor or no credit (financial inclusion)
- sources: <https://www.investopedia.com/terms/f/fintech.asp>

Top fintech companies

- <https://www.cbinsights.com/research/report/top-fintech-startups-2022/>
- <https://courses.cfte.education/ranking-of-largest-fintech-companies/>
- <https://fintechmagazine.com/top10/top-10-most-influential-fintech-companies>

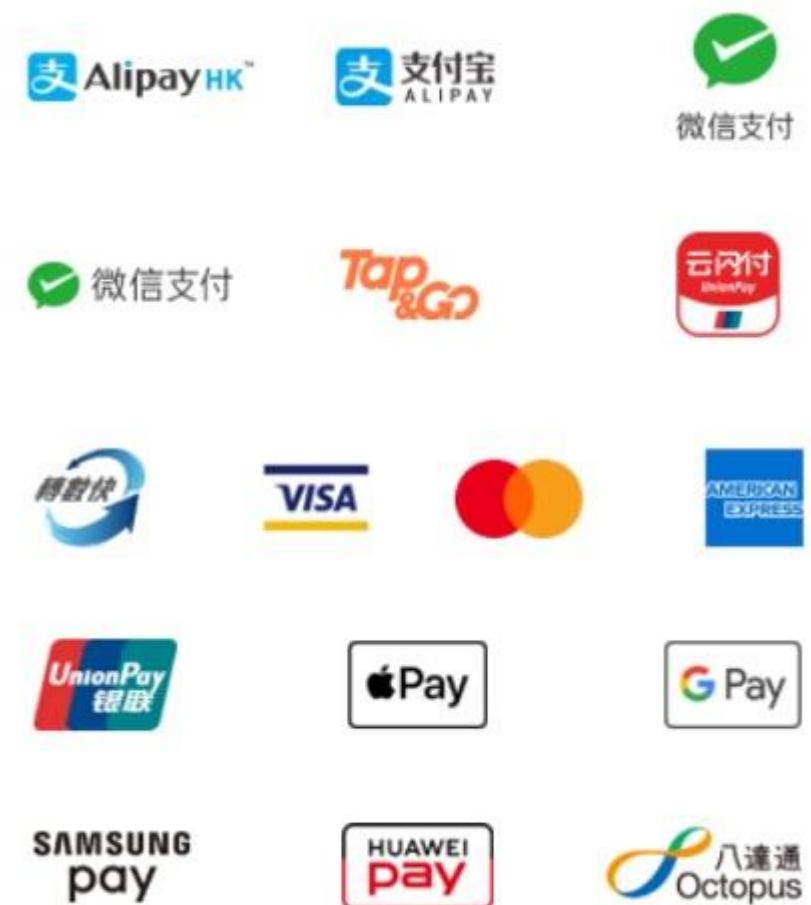
Example fintech companies

- **Robinhood**
 - allows users to trade stocks **commission-free**, and exchange crypto currencies via a **mobile application**
- **Stripe**
 - helps big and small businesses process online payments, take out business loans and **automatically** calculate and collect sales tax
- **Klarna**
 - gives the user the ability to '**buy now, pay later**', without using credit cards
- **Wise**
 - allows users to send money to other countries and receive money in alternative currencies at a **lower fees**

Categories of fintech

- **Electronic payment**

- Technologies that facilitate payments via mobile wireless devices, such as smartphones, tablets, and wearables
- Key technologies: mobile / digital wallets, near-field communication (NFC), barcode or QR code
- Real-world examples: AliPay, Apple Pay, Android Pay, WeChat Pay, Samsung Pay, PayPal, PayMe, Square, Stripe



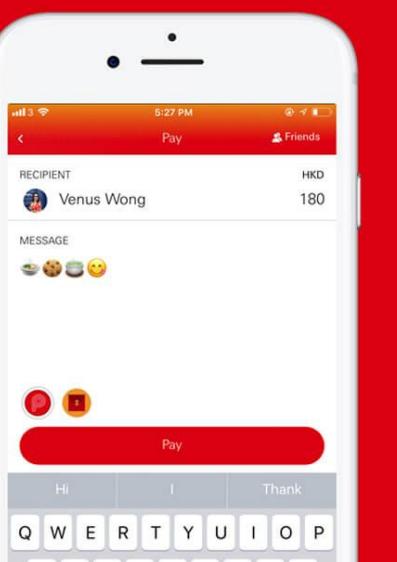
Electronic payment



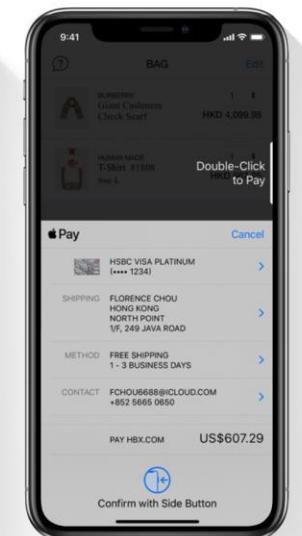
Alipay™



Cashless made effortless.



The PayMe app interface shows a red background with the PayMe logo and "From HSBC". It features a large white button with the text "Send money instantly to anyone for free". Below this is another button labeled "Download now". On the right side, there's a screenshot of the app's messaging screen where a user is sending 180 HKD to "Venus Wong". The screen includes a keyboard at the bottom.



Categories of fintech

- **Blockchain**
 - Distributed ledger technologies (DLT) that maintain records on a network of computers
 - Key technologies: Cryptocurrency, proof-of-work, smart contracts
 - Real-world examples: Bitcoin, Ripple, Blockchain.com, Gemini, Chainalysis

Cryptocurrency & Blockchain

The Gemini website features a dark header with navigation links: Products, Prices, Trust Center, Institutions, Resources, and Sign in. Below the header, a section titled "A variety of fiats and cryptos supported" lists supported currencies: USD, AUD, CAD, HKD, EUR, SGD, and GBP. Another section lists supported cryptocurrencies: 1INCH, AAVE, ALCX, ALI, AMP, ANKR, APE, API3, ASH, ATOM, AUDIO, AVAX, BAL, BAT, BICO, BNT, and BOND. To the right, a smartphone displays the Gemini mobile app's "Account" screen, showing payment methods, default currency set to HKD, transfer funds options, notifications, account settings, and statements.

A variety of fiats and cryptos supported

Gemini currently supports multiple fiats and cryptocurrencies in Hong Kong.

Fiats

- USD
- AUD
- CAD
- HKD
- EUR
- SGD
- GBP

Cryptos

1INCH	AAVE	ALCX
ALI	AMP	ANKR
APE	API3	ASH
ATOM	AUDIO	AVAX
BAL	BAT	BCH
BICO	BNT	BOND

The Blockchain.com website features a dark header with links: Wallet, Exchange, Explorer, Institutional, and three dots. The main content area is titled "The Easiest and Most Powerful Crypto Wallet". It highlights several features: Buy and Sell Crypto in Minutes (instantly buy Bitcoin with credit card, debit card, or by linking your bank), Earn up to 10% on your crypto, Control your funds with Private Key Wallet, At home or on the go, and All your crypto in one place. To the right, a smartphone displays the Blockchain.com mobile app's "Buy Bitcoin" screen, showing a balance of \$150 and a payment method listed as Chase Sapphire Visa.

News about Crypto Wallet in HK

Home > News > Local > Coinllectibles to acquire first instant messaging app "Talk+" in HK that includes...

LOCAL

Coinllectibles to acquire first instant messaging app "Talk+" in HK that includes multiple cryptocurrency wallet functions for over HK\$150m

By Dimsumdaily Hong Kong - 8:45PM Fri July 16, 2021

687

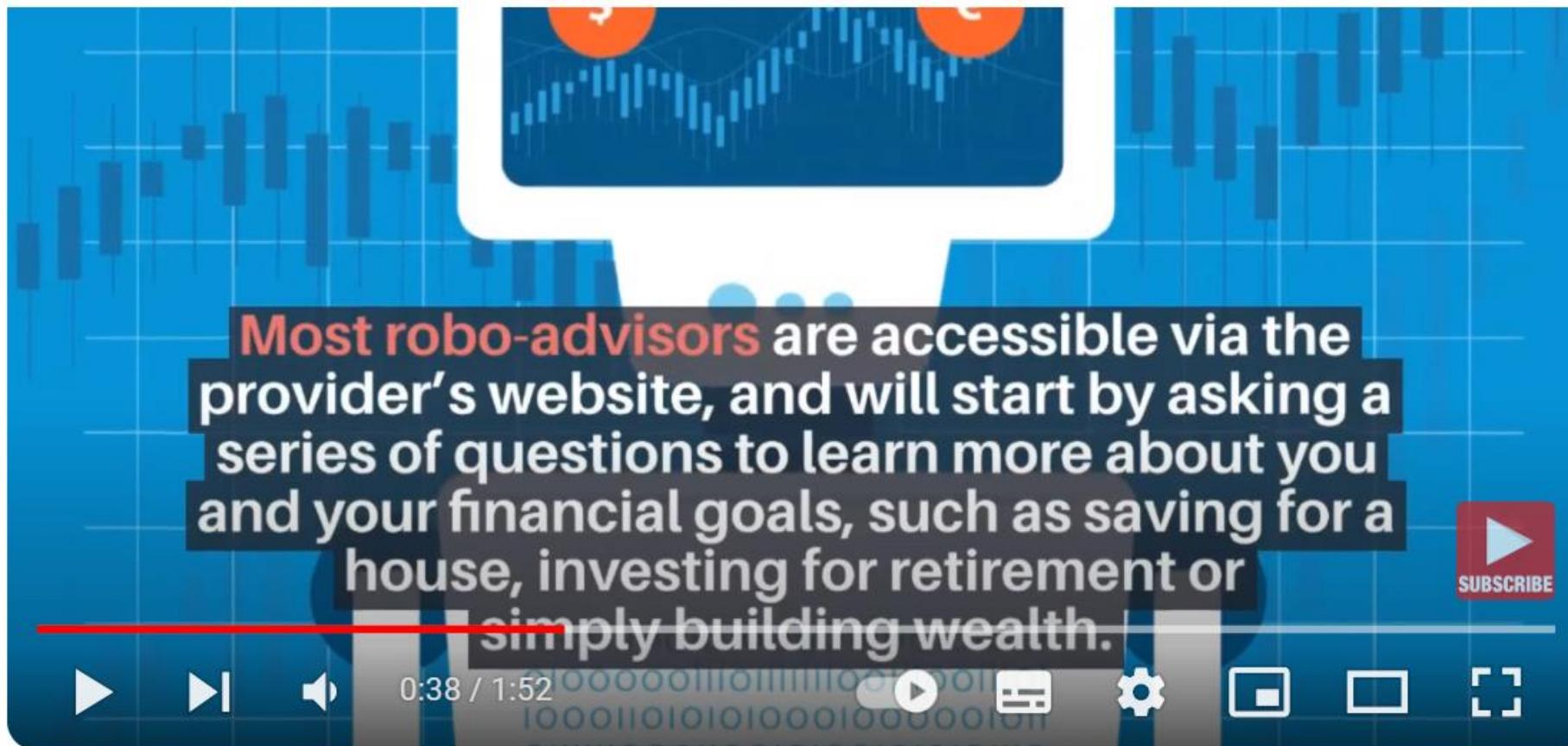


Categories of fintech

- **Robo-advising**
 - Computer systems or programs that utilize algorithms to provide automated investment advice to customers or portfolio managers
 - Key technologies: Artificial intelligence, big data, machine learning
 - Real-world examples: Betterment, Vanguard, WeLab, Sofi

Video: What is a Robo Advisor How Robo-Advisors work

- <https://www.youtube.com/watch?v=IJQdgVKfcK8>



Robo-advising



Home Open account

Interested in learning more about robo advisors?
Check out factsheet and educational video on the Auto Invest page now.

AUTO INVEST

Auto Invest is here

SoFi's robo advisor. It never sleeps. It never stops. All it ever does, is try to make you money.* Using AI technology, Auto Invest automatically invests your money into a diversified portfolio, taking into account how much risk you want to take.

Now, all you have to do, is sit back and see your money grow.

Want to learn more about robo advisors? Check out our [educational video](#) and [factsheet](#).

*Please refer to the risk disclosure under the Robo Advisory Agreement

[Download on the App Store](#) [GET IT ON Google Play](#)

v.sofi.hk/auto-invest



Promotion Features Company Support

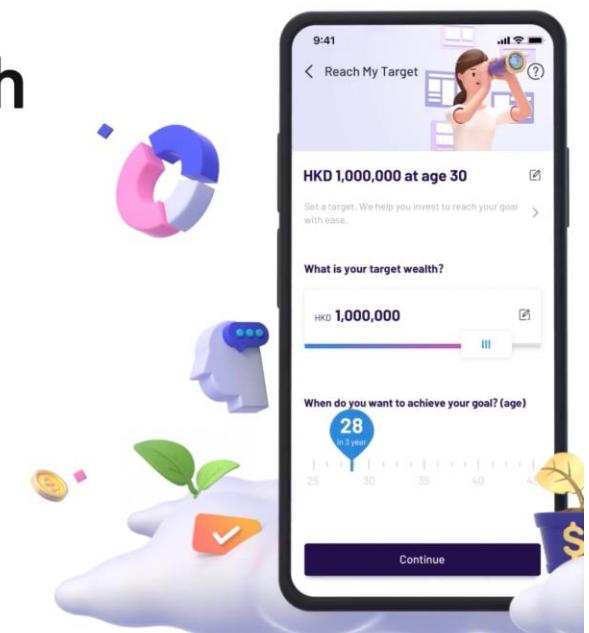


Do

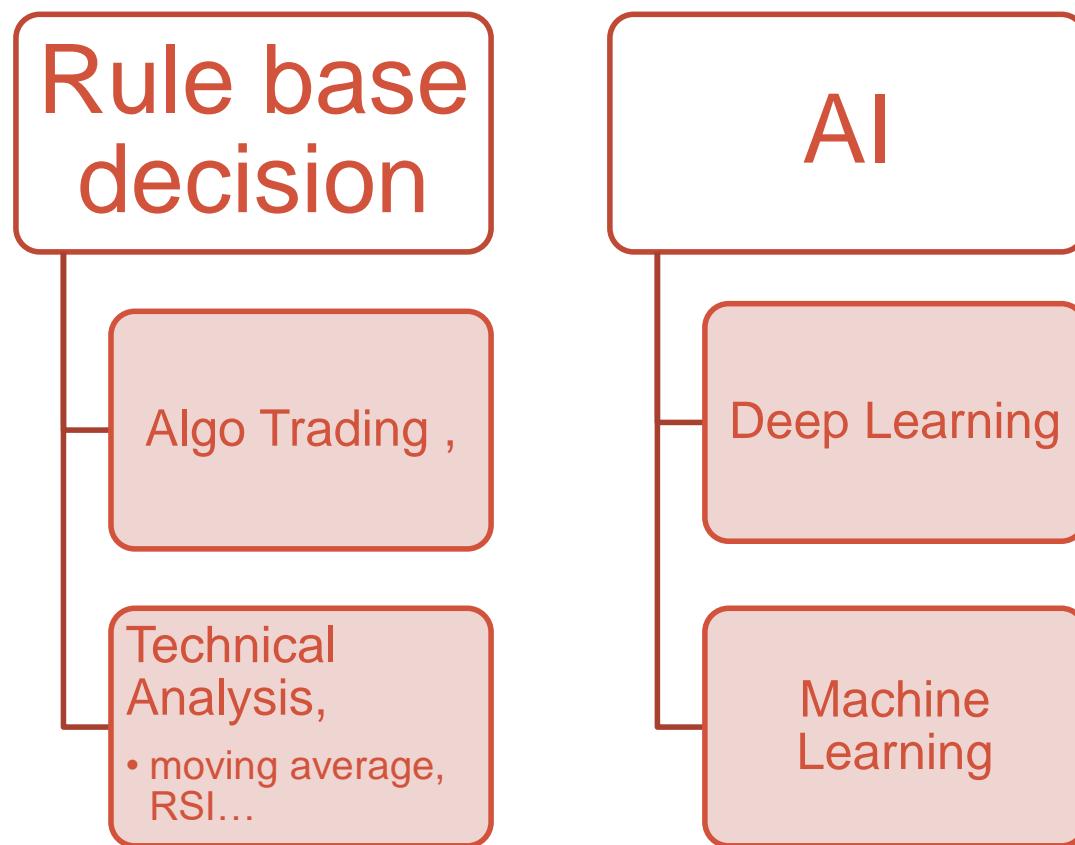
GoWealth Digital Wealth Advisory

Backed by WeLab Bank's fintech experience and AllianzGI's investment management expertise.

Learn More



Methodology of Roboadvisor



Algorithmic Trading (rule-base/ algorithm based)

- Algorithmic trading (also called automated trading, black-box trading, or algo-trading) uses a computer program that follows a defined set of instructions (an algorithm) to place a trade. The defined sets of instructions are based on timing, price, quantity, or any mathematical model.
- The trade, in theory, can generate profits at a speed and frequency that is impossible for a human trader. Most algo-trading today is high-frequency trading (HFT), which attempts to capitalize on placing a large number of orders at rapid speeds across multiple markets and multiple decision parameters based on preprogrammed instructions.



e.g. Technical Analysis taught in ELEC3845

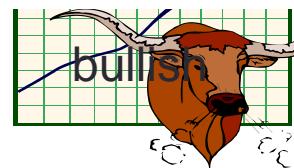
Moving Average - Trend reversal

- E.g. 150-day EMA of 3M Co.
- It shows how well moving averages work when the trend is strong.
- 150-day EMA turned down in Nov 07 and again in Jan 08.
 - → took a 15% decline to reverse the direction of this moving average.
 - These lagging indicators identify trend reversals
- The price continued lower into Mar 09 and then surged 40-50%.
 - EMA did not turn up until after this surge → Another trend reversal (go up now!)
 - The stock price continued higher the next 12 months!!!

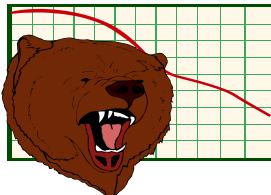


Moving Average - Double Crossovers

- A bullish crossover (so-called the golden cross)
 - Occurs when the shorter moving average crosses above the longer moving average
- A bearish crossover (so-called the dead cross)
 - Occurs when the shorter moving average crosses below the longer moving average.

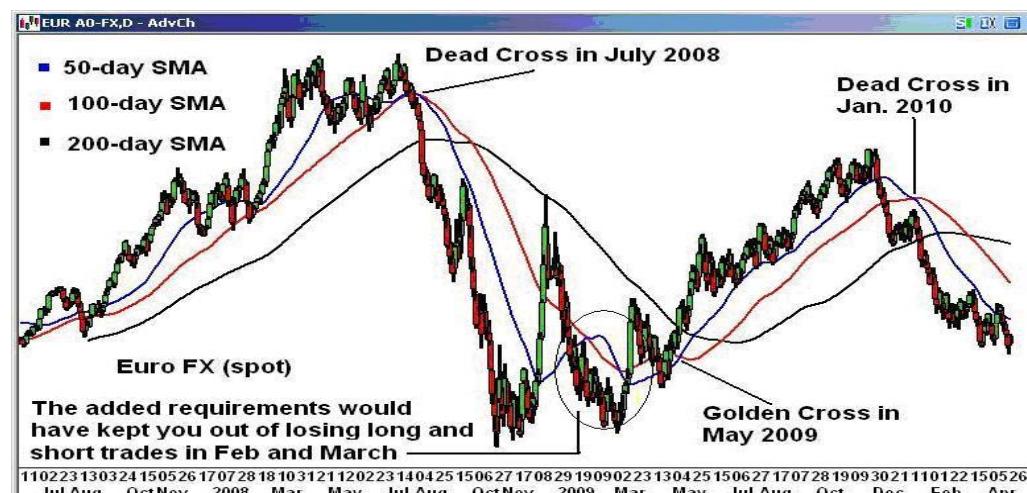


bearish



Sample Algorithm (rule base)

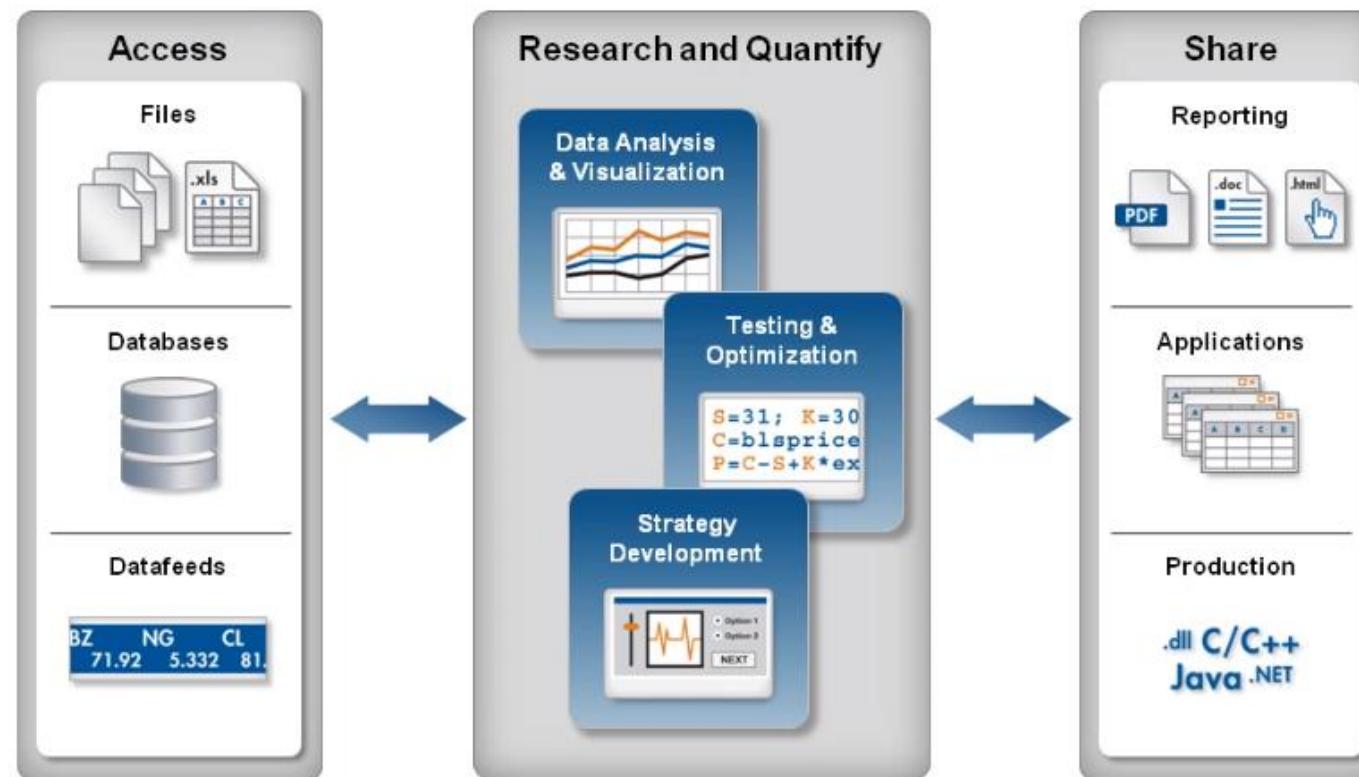
- If $\text{SMA}(10,t-1) < \text{SMA}(200,t-1)$
 - Then IF $\text{SMA}(10,t) > \text{SMA}(200,t)$ ‘short term exceed long term, golden cross
 - Then
 - Buy the stock: ‘Gold cross’
 - Else
 - Keep the stock



Algo trading using Matlab

- <https://ww2.mathworks.cn/en/videos/algorithmic-trading-with-matlab-for-financial-applications-81775.html>

Algorithmic Trading Workflow



Advantages of Algorithmic Trading

- Trade order placement is instant and accurate.
- Trades are timed correctly and instantly to avoid significant price changes.
- Simultaneous automated checks on multiple market conditions.
- Reduced risk of manual errors when placing trades.
- Reduced the possibility of mistakes by human traders based on emotional and psychological factors.
- Algo-trading can be backtested using available historical and real-time data to see if it is a viable trading strategy.

Disadvantages of Algorithmic Trading

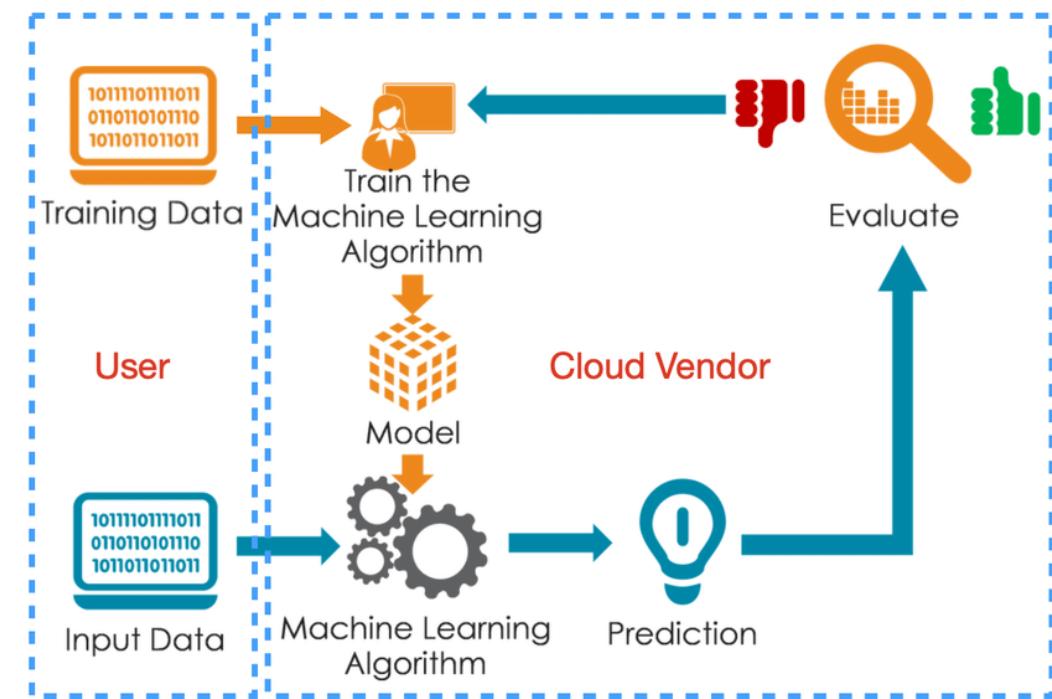
- While algorithmic trading may eliminate the impact of emotion in trading, it also makes investors over reliant on technology and the systems that they deploy. The loss of a viable network connection or a system crash could prevent your order from being executed, causing you to miss out on market opportunities.
- Risk of over-optimization, which can create streamlined algorithms that look great on paper but fail to translate in real market conditions. With over-optimization, you may find that the system is incapable of performing in a live and real-time marketplace.

Robo-Advisor

- Robo-advisors are digital platforms that provide automated, algorithm-driven financial planning services with little to no human supervision.
- A typical robo-advisor collects information from clients about their financial situation and future goals through an online survey and then uses the data to offer advice and automatically invest client assets.

Roboadvisor by AI Machine Learning

- Machine Learning (ML) has been applied in Robo Advisory to improve the advisory quality,
- More banks and clients are turning to Robo Advisory because of its user friendliness, convenience of anytime anywhere and cost competitiveness.
- Matching process of
 - Client investment profile,
 - Portfolio/product profile and
- Today's investment advisories are using simple algorithms. For instance (e.g. rule base), matching clients with low investment risk with low product risk rating portfolio.



Advantages of robo-advisor

- **Available 24/7:**
 - You no longer have to arrange a session to talk to your portfolio manager. You can adjust your portfolio, deposit or withdraw at any point, 24 hours a day.
- **Lower fees:**
 - Since it's completely automated, the annual fees as well as the minimum required investments are lower, making them suitable for investors who don't have a lot to invest.
- **Convenient:**
 - After the portfolio setup, everything is handled by the robo-advisor – you don't have to think about the market trends or have any investment knowledge.

Advantages of robo-advisor

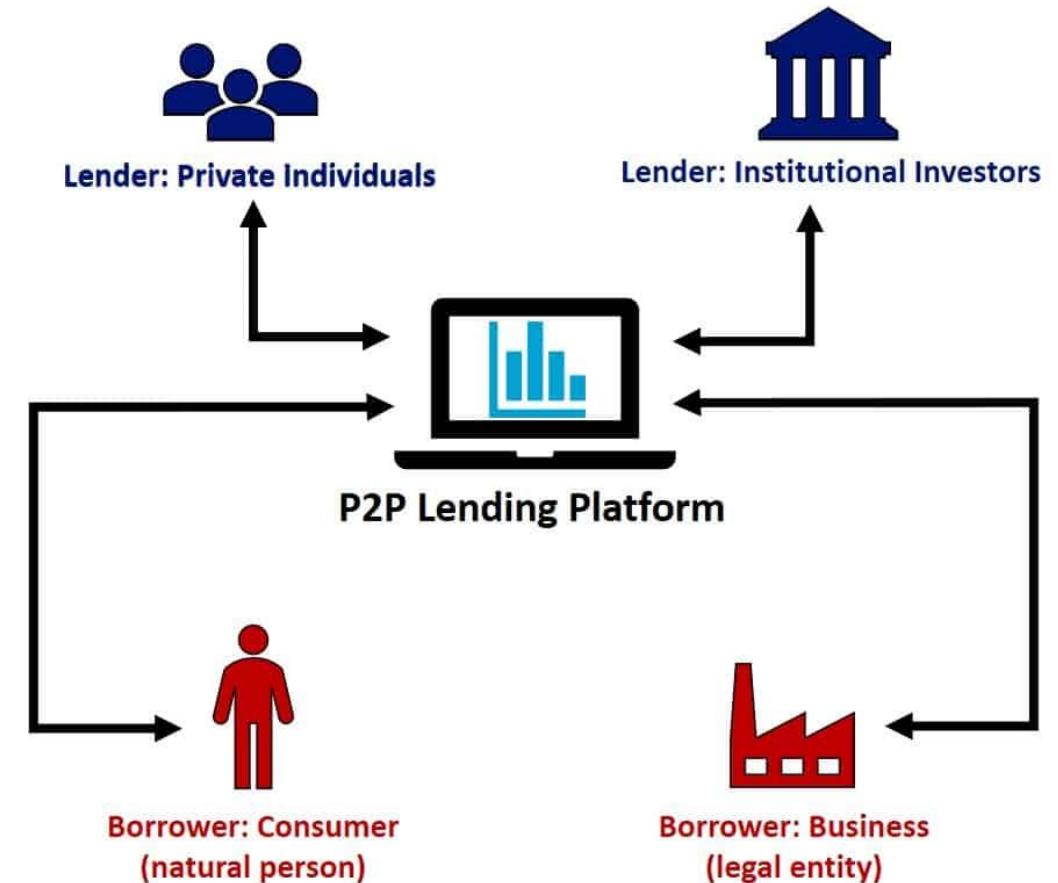
- **Consistent methodology:**
 - Since robo-advisors stick to their investment methodology, they are not affected by the day-to-day swings of the market and can avoid human errors.
- **Portfolios are diversified:**
 - Robo-advisors build a portfolio that consists of multiple types of assets (e.g. stocks, bonds, cash) from different geographies which spreads out your risk and makes your portfolio more stable.

Disadvantages of robo-advisors

- **Lack of empathy:**
 - Good human consultants would want to understand you and your fears before recommending you a portfolio. They also serve as someone to talk to if you have concerns about the market, etc. Robo-advisors just follow the investment plan.
- **Cannot guide you:**
 - Robo-advisors assume that the customer knows what they want – e.g. the goal they are setting for themselves, or how much risk they can bear.
 - In reality, you may not truly understand how much risk you are willing to take or perhaps haven't fully thought out when you would need your money or how much. This could result in a mis-match between the performance of the robo-advisor and expectations of the customer.
- **The process is extremely passive:**
 - robo-advisors follow their investment methodology unfailingly, in the case of adverse events like political factors that affect the economy, the robo-advisor may not adjust its portfolios.
 - Given the lack of empathy, it may be a bit scary to see your portfolio falling in value (even if it's temporary!).

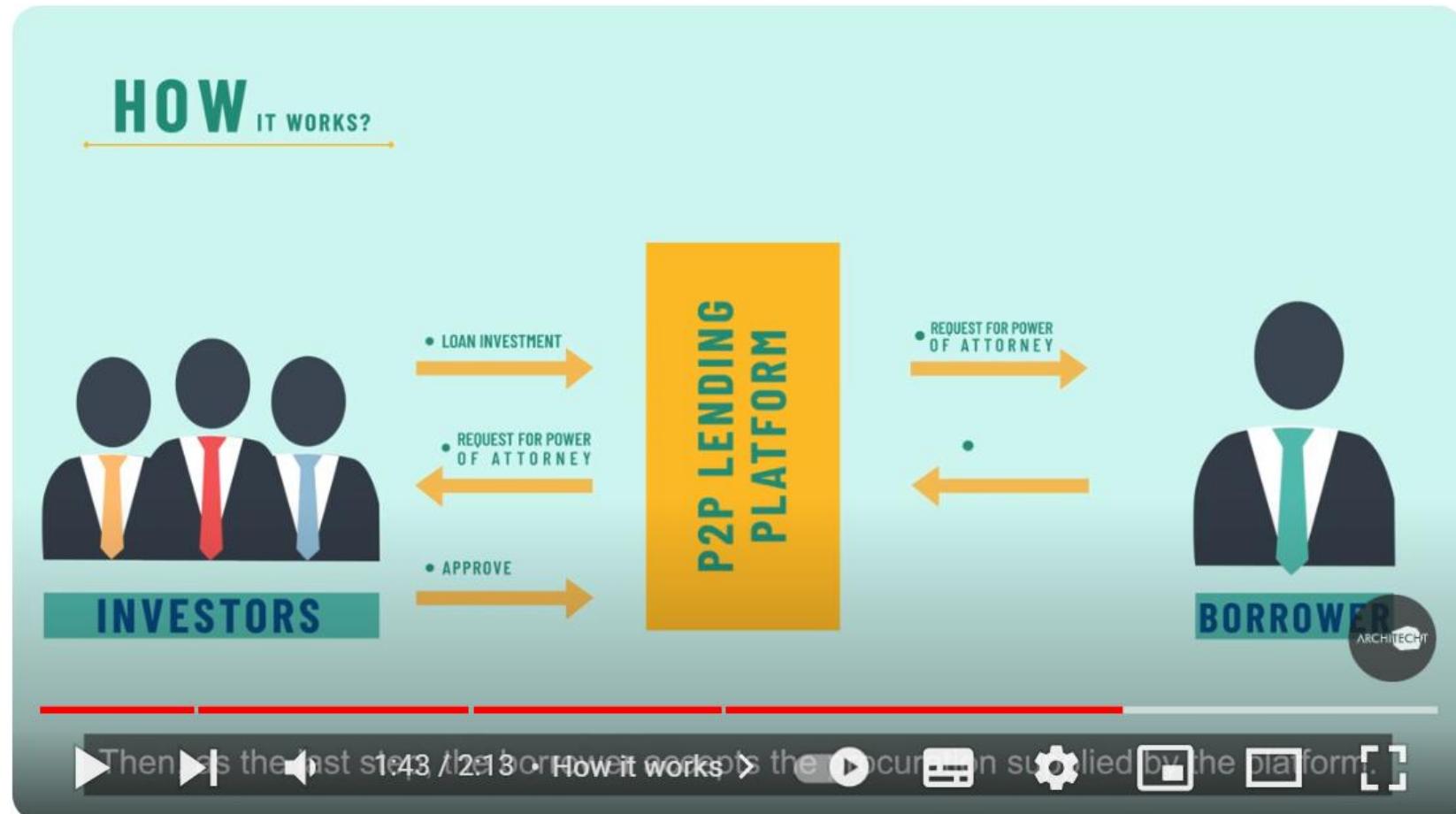
Categories of fintech

- **Peer-to-peer (P2P) lending**
 - Software, systems, or platforms that facilitate loaning of money to individuals and businesses through online services that directly match lenders with borrowers without using an intermediating bank.
- Real-world examples: [GoFundMe](#), Kickstarter, Lending Club, OnDeck, Prosper Marketplace, Zelle, Tala



Video on P2P lending

- <https://www.youtube.com/watch?v=AxbjVbvrOt0>



P2p Lending

We're a global technology company building the world's most accessible financial services.

What We Do How We Do It

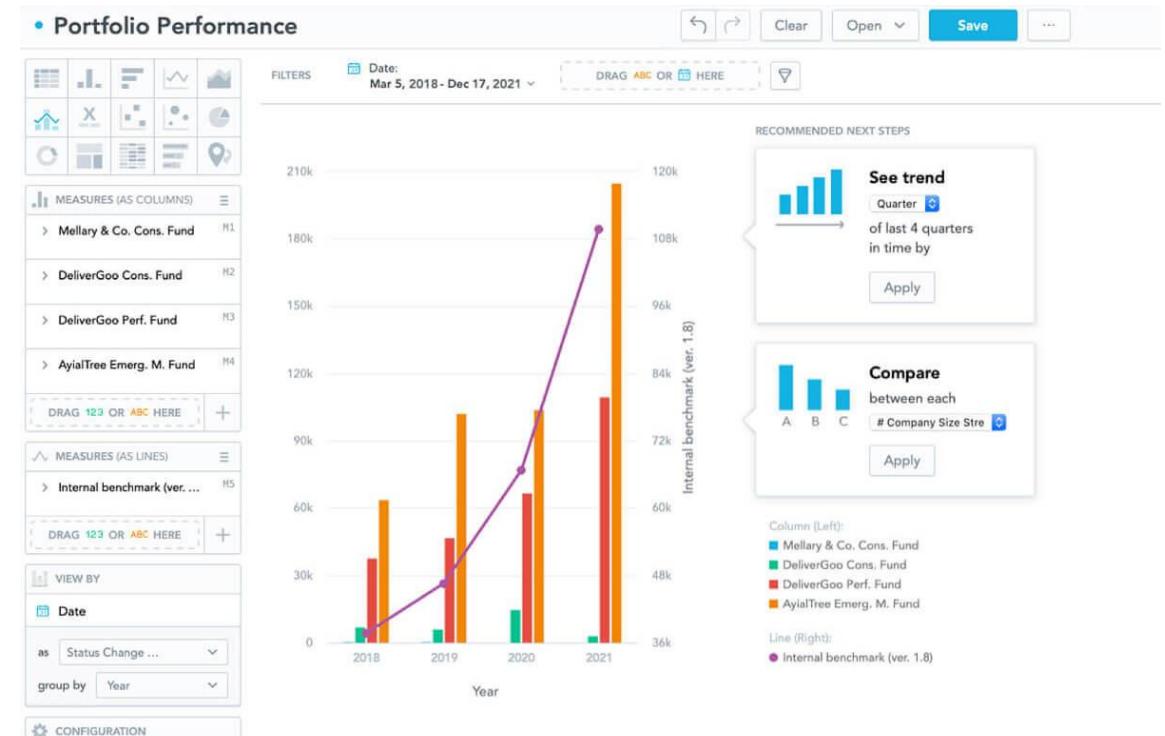
Tala offers digital financial services to help the traditionally underbanked borrow, save and grow their money. Our consumer credit app is the world's most accessible, instantly underwriting and disbursing loans to people who have never had a formal credit history. Loans range from \$10 to \$500 with rates as low as 4%.

Powered by advanced data science and machine learning, we built a modern credit infrastructure from scratch. Anyone with an Android smartphone can apply for a loan, get an instant decision and receive funds directly to their account. We're building new tools to help users manage their money and pursue their goals.

Categories of fintech

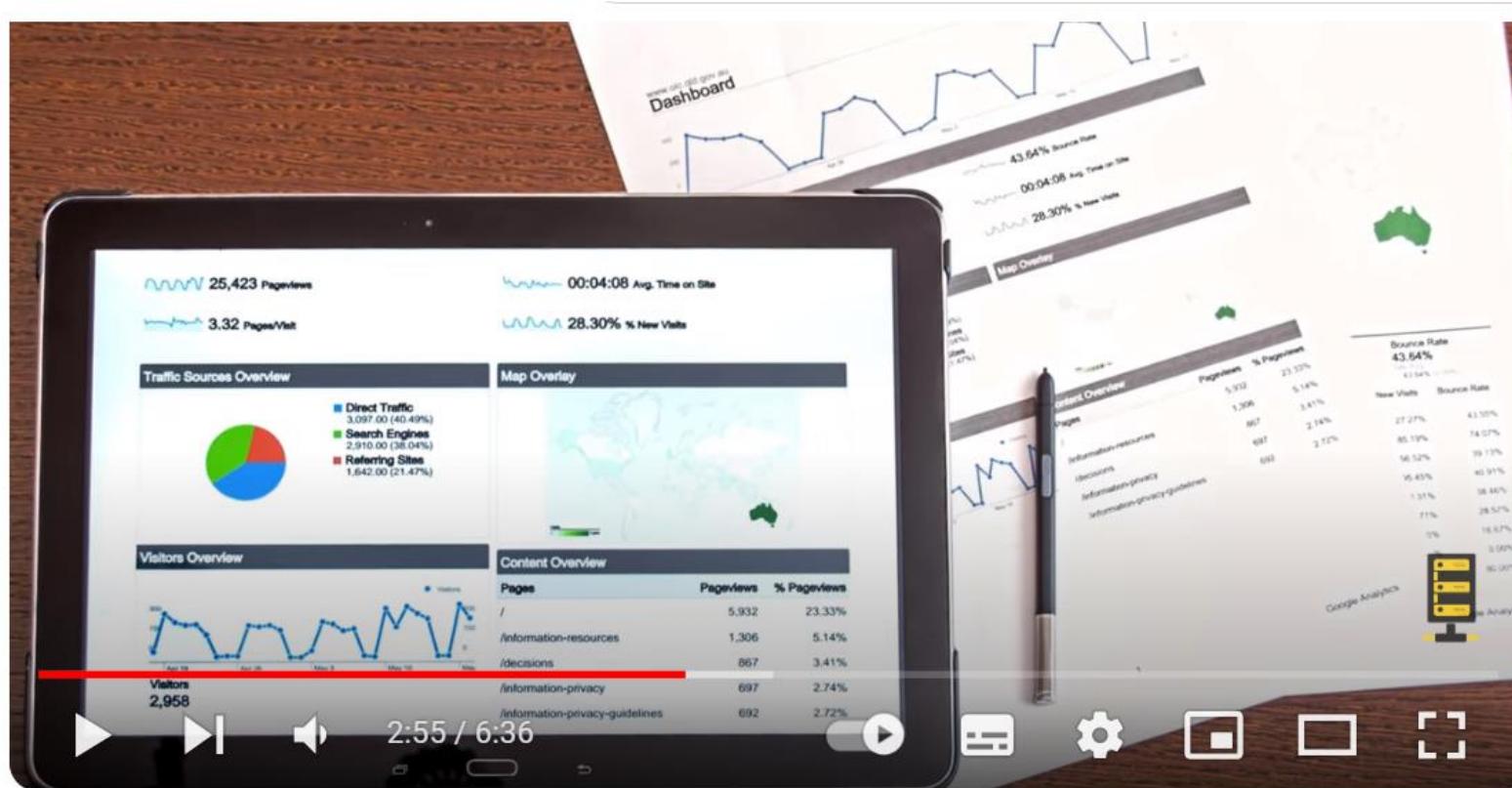
- **Data analytics**

- Technologies and algorithms that facilitate the analysis of transactions data or consumer financial data
- Key technologies: Big data, cloud computing, artificial intelligence, machine learning
- Real-world examples: Equifax NeuroDecision credit scoring, [JPMorgan Contract Intelligence \(COiN\)](#), Bloomberg Social Sentiment Analytics
- Source: Mark A Chen, Qinxi Wu, Baozhong Yang, "How Valuable Is FinTech Innovation?", The Review of Financial Studies, Volume 32, Issue 5, May 2019, Pages 2062–2106.



Top 9 Data Analysis/Science Use Cases in Banking

- <https://www.youtube.com/watch?v=8ijNZE05dQ>



Top 9 Data Analysis/Science Use Cases in Banking

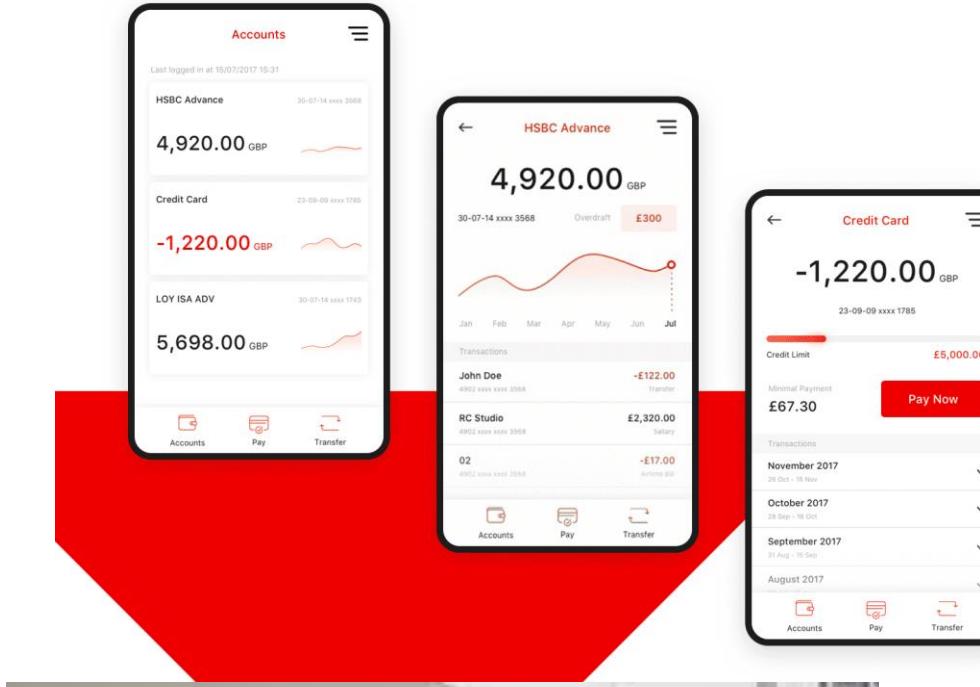
- Fraud detection
- Managing customer data
- Risk modelling for investment banks
- Personalized marketing
- Lifetime value prediction
- Real-time and predictive analytics
- Customer segmentation
- Recommendation engines
- Customer support

Categories of fintech

- **Mobile Banking and virtual banks**
 - Mobile banking: digital access to banking services on a mobile device
 - Neobanks: banks without any physical branch locations, serving customers on completely mobile and digital infrastructure.
 - [What are the differences between a neobanks and a traditional bank](#)
 - [Examples in HK](#): Airstar, Ant, Fusion, Livi, Mox, Ping An, Welab, ZA

Mobile banking

The image shows a screenshot of the HSBC mobile banking app. At the top, there's a navigation bar with a 'Menu' icon, the HSBC logo, and a 'Log on' button. Below the header, the title 'Key features' is displayed. The main content area is divided into two sections. The left section, titled 'Open an account instantly >', features a photo of a man sitting on a couch using a smartphone. Below the photo, text reads: 'New and existing customers² can now use the HSBC HK App to open a bank account in less than 5 minutes.' The right section, titled 'Budgeting made easy >', features a photo of a person with pink hair holding a smartphone. Overlaid on the phone screen are various icons related to budgeting: a lightbulb, a pie chart, a shopping bag, and a red 'X'. Text below the photo says: 'Automatically track expenses from your HSBC accounts and HSBC credit cards with ease. Plan your finances and develop saving habits effortlessly.'



Virtual bank in HK

FIGURE 12: OVERVIEW OF HONG KONG VIRTUAL BANKS

Virtual Bank								
	ZA Bank	Airstar Bank	WeLab Bank	livi Bank	Mox Bank	Ant Bank	PAOb	Fusion Bank
Launch Date	Mar 2020	Jun 2020	Jul 2020	Aug 2020	Sep 2020	Sep 2020	Sep 2020	Dec 2020
Deposits* (HKD '000)	2,757,955	356,578	187,289	183	28,030	1,334	6,591	N/A
Services								
Savings	✓	✓	✓	✓	✓	✓	✓	✓
Time Deposits	✓	✓	✓	✗	✗	✗	✗	✓
Personal Loans	✓	✓	✗	✗	✗	✗	✗	✗
Business Loans	✓	✗	✗	✗	✗	✗	✓	✗
Transfer / Pay	✓	✓	✓	✓	✓	✓	✓	✓
Debit Card	✓	✗	✓	✓	✓	✗	✗	✗
FX	✗	✗	✗	✗	✗	✗	✗	✓
Insurance	✓	✗	✗	✗	✗	✗	✗	✗
Budgeting Tools	✗	✗	✗	✗	✓	✗	✗	✗

*As of June 2020



Offered



Not Offered

Hong Kong Virtual Banks Accumulated Growth



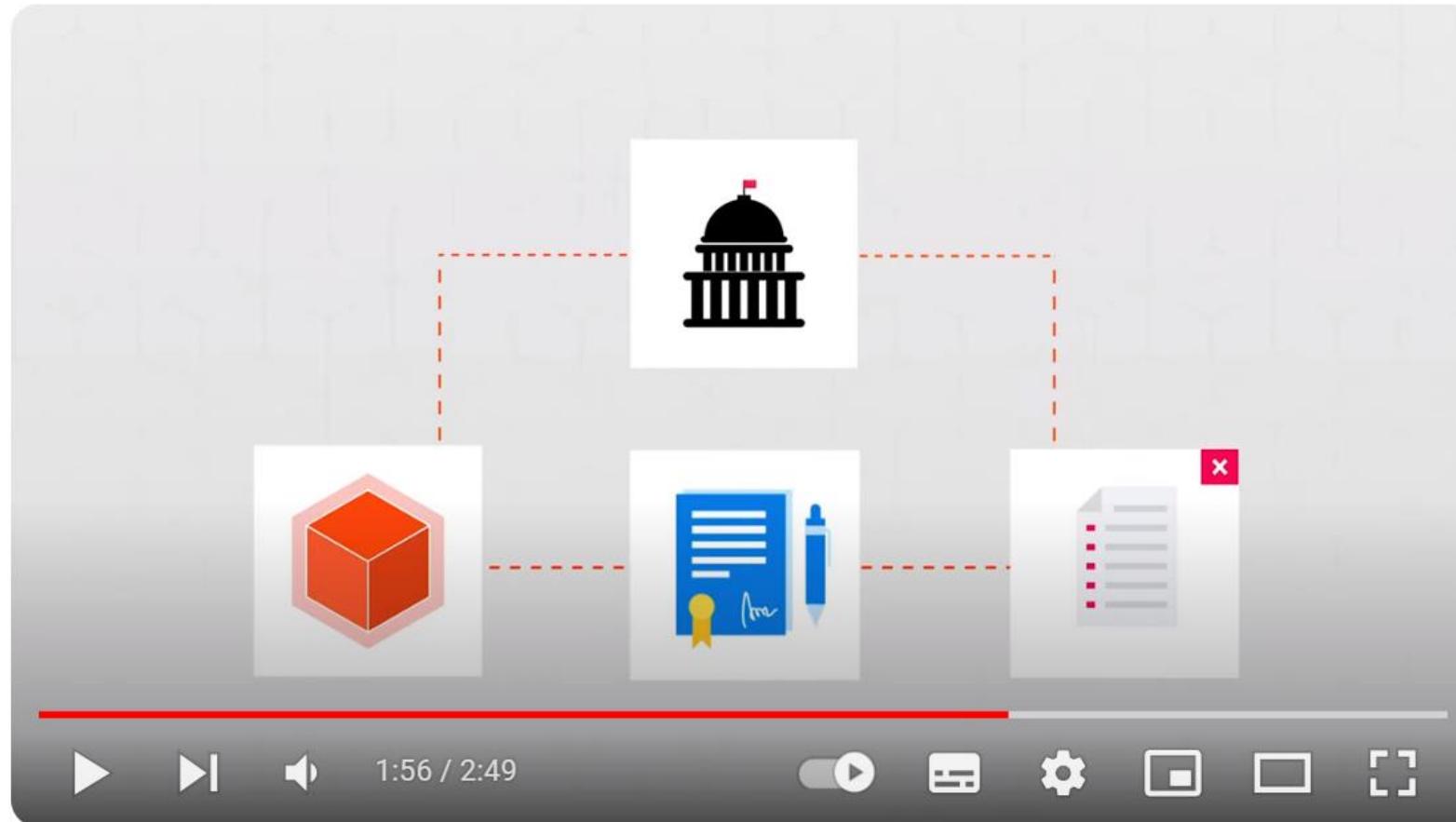
Categories of fintech...

- **Insurance**
 - Insurtech uses technology to simplify and streamline the insurance industry from mobile car insurance to wearables for health insurance.
 - Real-world examples:
 - GoHealth: uses machine learning algorithms to match consumers with plans that meet their unique needs
 - Lemonade: uses an AI claims expert to drive customers through the claim filing process.
 - Insurify: uses AI technology to serve up accurate, real-time quotes.

Source: <https://builtin.com/fintech>

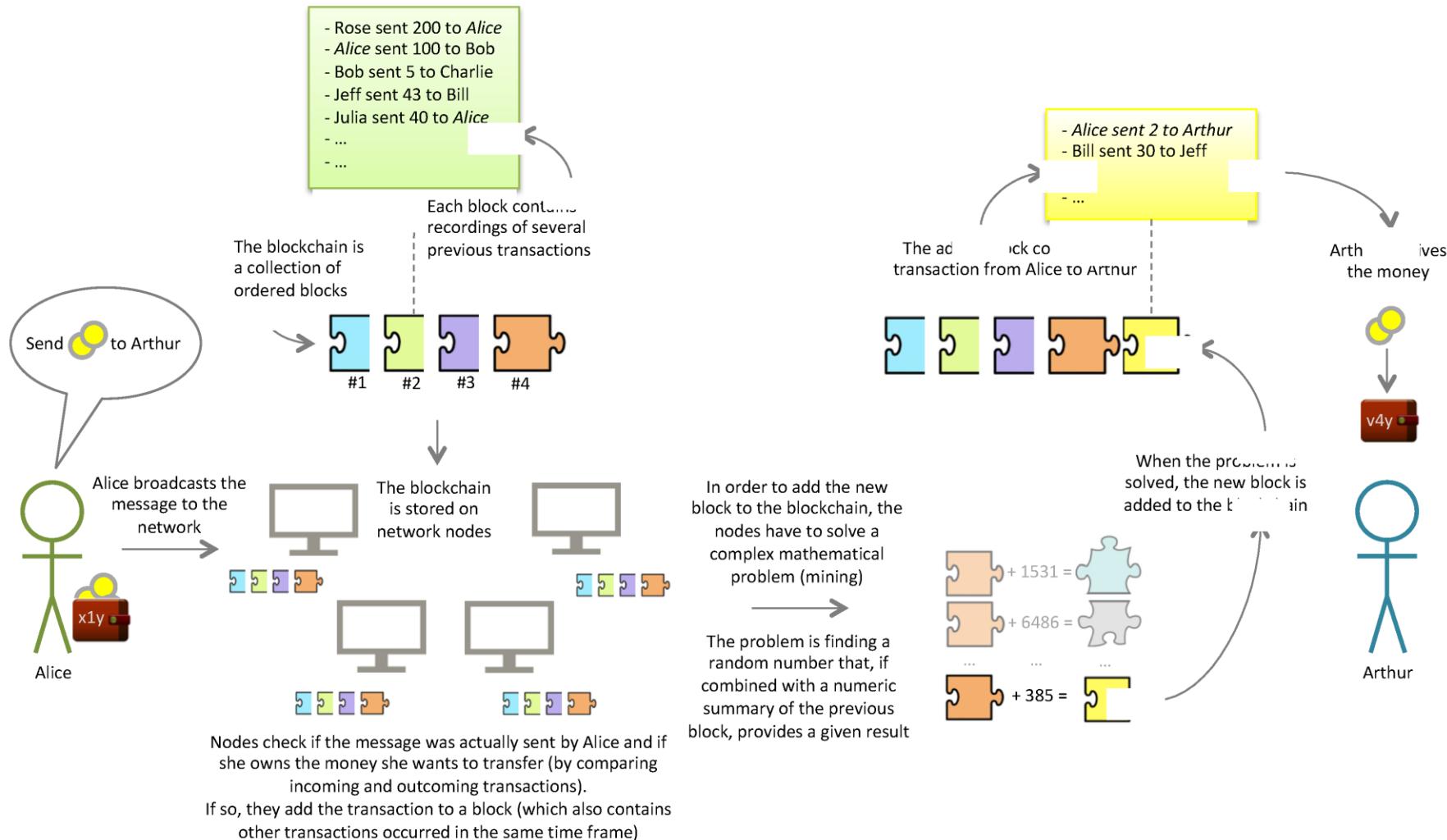
Blockchain in Insurance for Streamlining Claims & Settlements

- <https://www.youtube.com/watch?v=a1U4IOKn0Wc>



Blockchain and Smart Contracts for Insurance

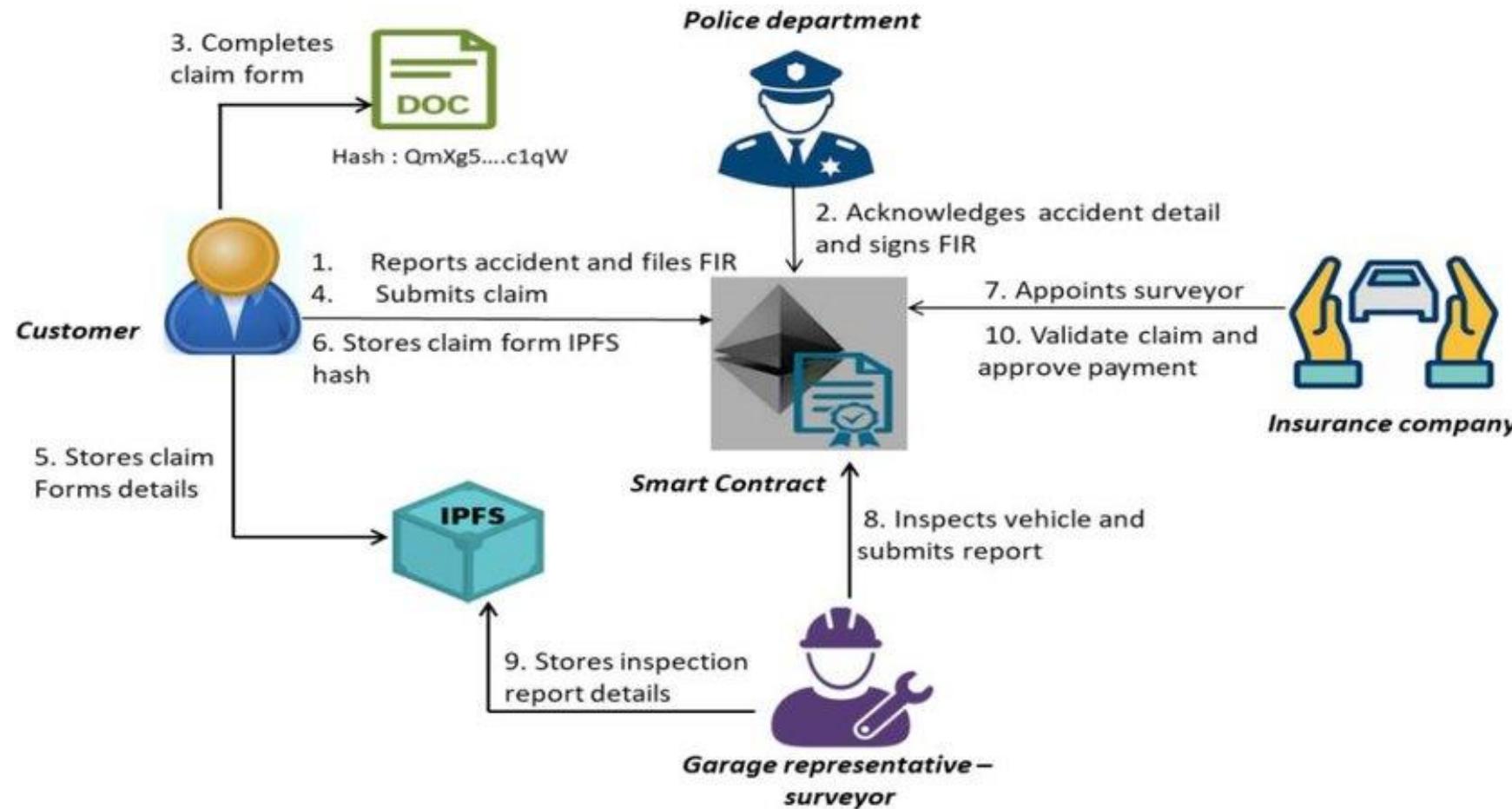
<https://www.mdpi.com/1999-5903/10/2/20>



Blockchain-powered vehicle insurance

Full paper:

https://www.researchgate.net/publication/349915224_Blockchain_for_automotive_An_insight_towards_the_IPFS_blockchain-based_auto_insurance_sector



Q&A

ELEC2544

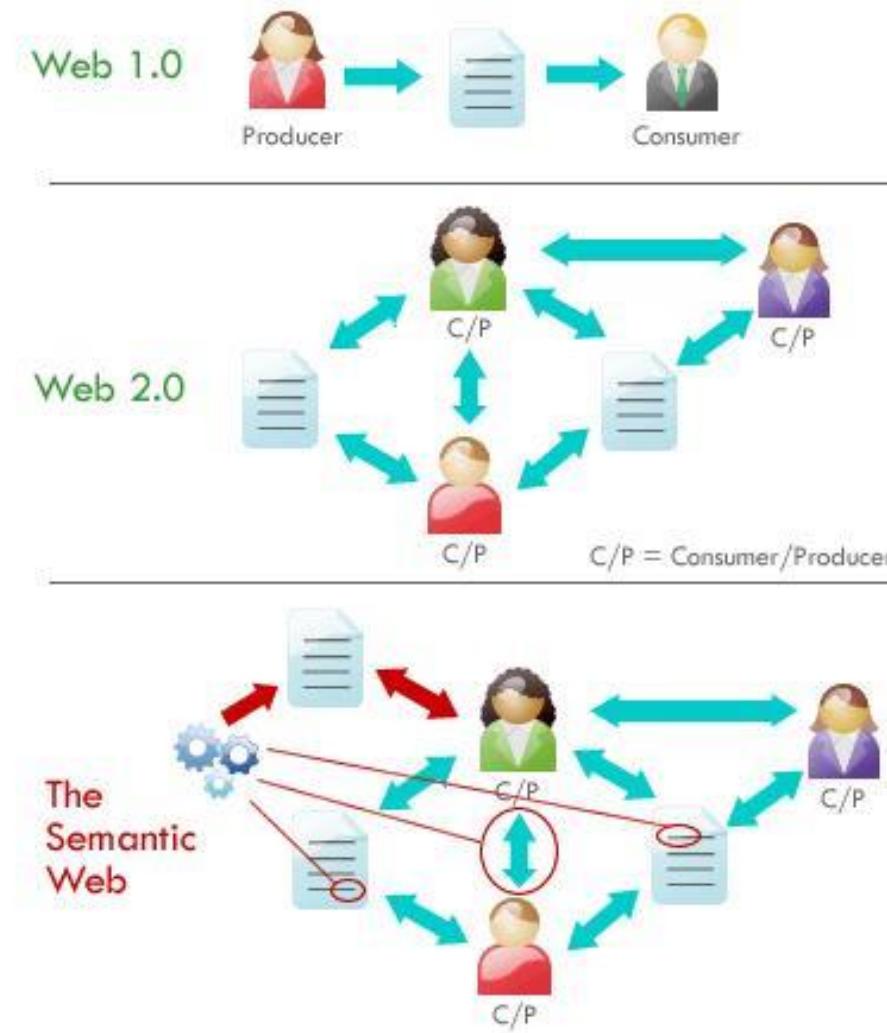
E-Commerce and FinTech

Future of E-Commerce

Web 2.0 and Web 3.0
Big Data
IPv4 and IPv6

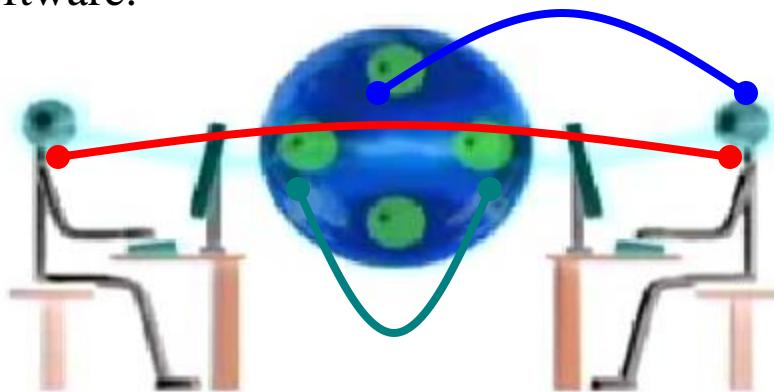
Dr. Wilton Fok

Compare Web 1.0, 2.0, 3.0, 4.0....



Key components of Web2.0

- **Interpersonal computing (Social Web)**
 - involving person-to-person interactions facilitated via websites that enable collaborative content creation, sharing and manipulation.
- **Web services**
 - involving application-to-application (and hence organization-to-organization) data and service exchanges facilitated by automated connections between web servers and other Internet technology.
- **Software as a service (SaaS)/ Service-oriented architecture**
 - involving human interactions with digital content facilitated by applications delivered over the web and that free the user from locally installed software.



Video: <http://www.youtube.com/watch?v=7BAxvFdMBWw>

Web 2.0

- Service-oriented architecture (SOA)—I
 - It is a key piece in Web 2.0 which defines how Web 2.0 applications expose its functionality
 - → so that other applications can leverage and integrate the functionality providing a set of much richer applications
 - E.g.: news feeds, RSS, Web Services, youtube, google map

Web 2.0

- Social Web — It defines how Web 2.0 tends to interact much more with the end user and making the end-user an integral part.



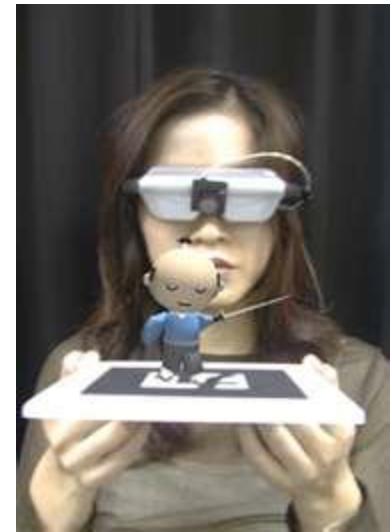
Web 2.0

- Web 2.0 draws together the capabilities of client- and server-side software, content syndication and the use of network protocols.
- Standards-oriented web browsers may use plug-ins and software extensions to handle the content and the user interactions.
- Web 2.0 sites provide users with
 - information storage,
 - creation,
 - dissemination capabilities



Web 3.0

- Convergence of the virtual and physical world
 - e.g. TV-quality open video
 - 3D simulations,
 - augmented reality,
- Pervasive broadband, wireless, and sensors.
 - More devices connected together, E.g. mobile phone, washing machine, car, not only computer
 - These devices communicate to each other
 - Always available, connected at any time and anywhere.



Video: Evolution Web 1.0, Web 2.0 and Web 3.0

- <http://www.youtube.com/watch?v=bsNcjya56v8&feature=related>

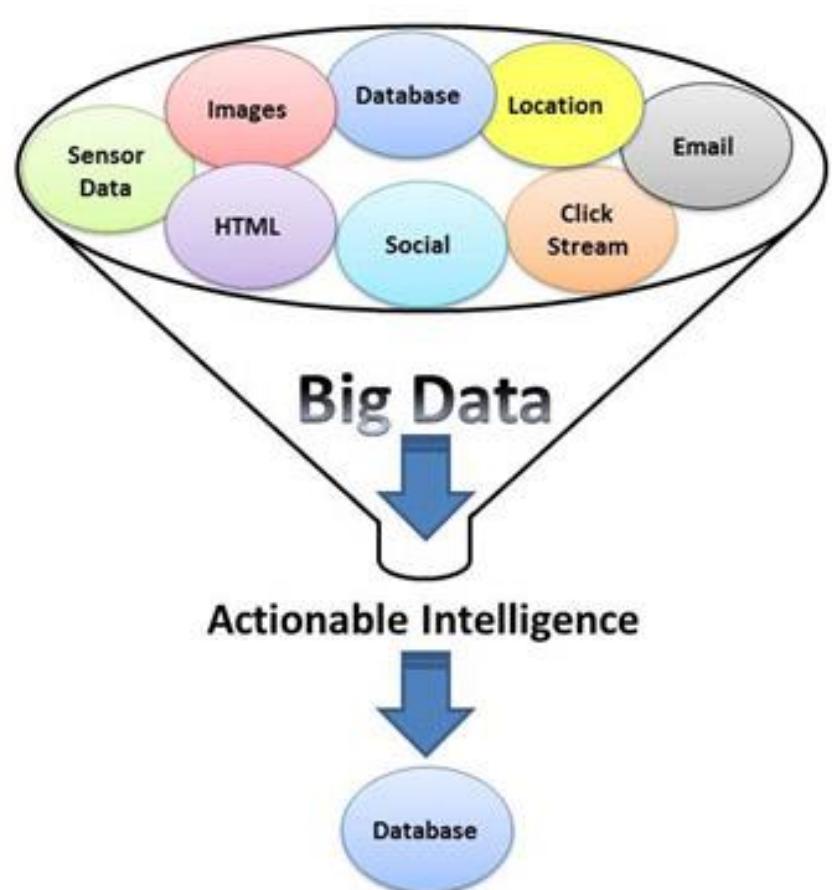


Web 4.0

- Semantic Web
 - I.e. a "web of data" that enables machines to understand the semantics, or meaning, of information on the World Wide Web.
- It extends the network of hyperlinked human-readable web pages by inserting machine-readable metadata about pages and how they are related to each other, enabling automated agents to access the Web more intelligently and perform tasks on behalf of users.
- "a web of data that can be processed directly and indirectly by machines."
- Computer is generating new information, rather than humans.
- Drivers:
 - The rise of statistical, machine-constructed semantic tags and algorithms
 - Driven by broad collective use of conversational interfaces

Big Data

- Data sets in e-commerce is nowadays so large and complex that traditional data processing applications are inadequate.
- Big data involves:
 - Analysis, capture,
 - Search, sharing, storage, transfer,
 - Visualization, and information privacy
 - predictive analytics
 - other certain advanced methods to extract value from data

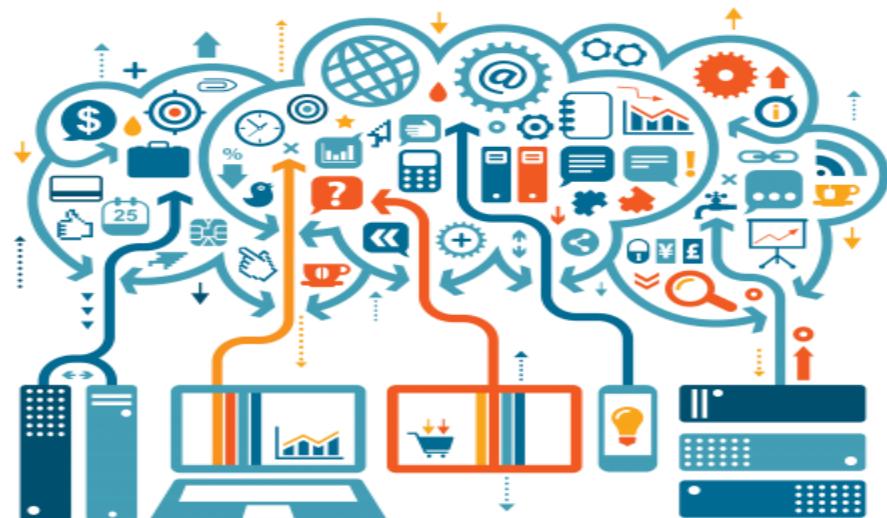


Analysis of Big data

- Objective:
 - To find new correlations between data
 - To dig out non-trivial information or knowledge from the data set, e.g.
 - spot business trends
 - prevent diseases
 - combat crime...

Why big data?

- Data sets grow in size in part because:
 - Data increasingly being gathered by cheap and numerous information-sensing mobile devices,
 - Availability of remote sensing and software logs,
 - e.g. cameras, microphones, radio-frequency identification (RFID) readers, and wireless sensor networks.



Why big data?

- As of 2012, every day 2.5 exabytes (2.5×10^{18}) of data were created.
 - World population: 6 billion (6×10^9)
 - Data per capita per day = 4×10^8 bytes = 400Mbytes
- Large enterprises who own big data wants to know better about their business

Big data

- 5V characteristics:

- Volume
- Variety
- Velocity
- Variability
- Veracity

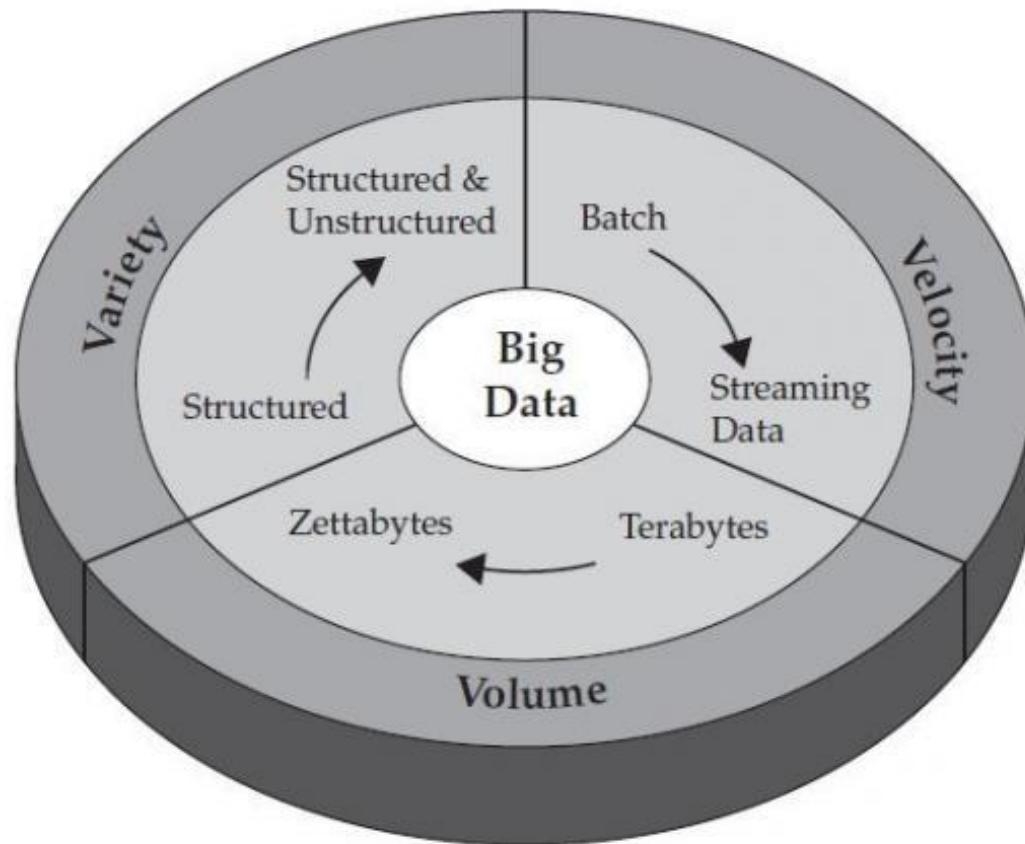
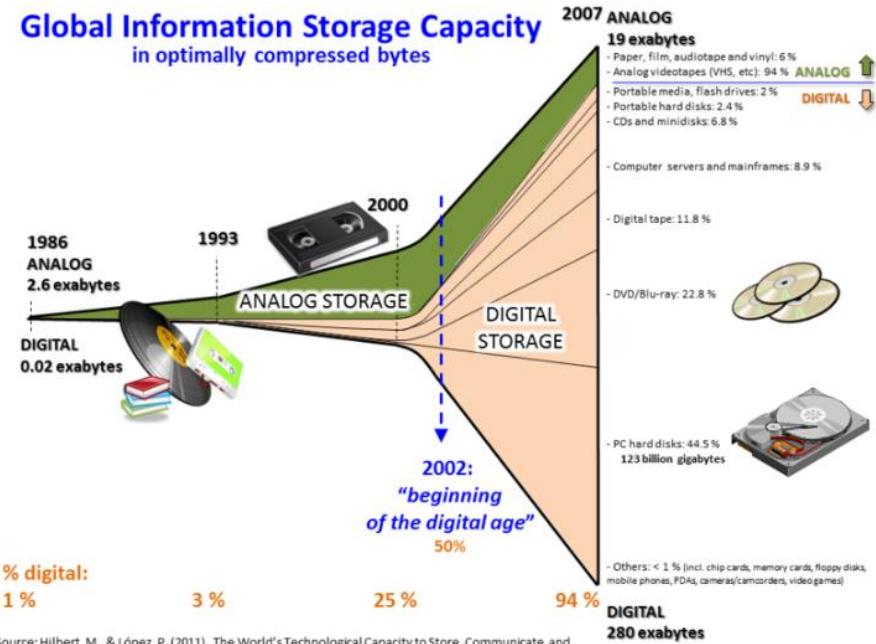


Figure 1-1 IBM characterizes Big Data by its volume, velocity, and variety—or simply, V^3 .

Volume

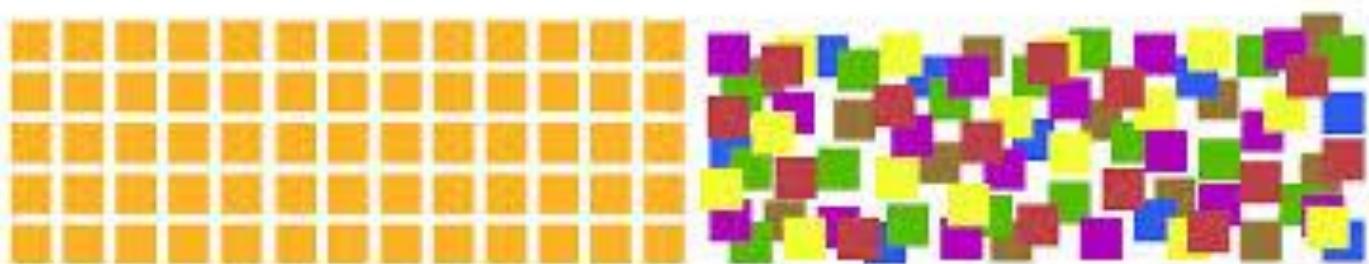
- The quantity of data that is generated is very important in this context
- The size of the data which determines the value and potential.
- ‘**Big Data**’ contains a term which is related to **size** and hence the characteristic.



Variety

- The category to which Big Data belongs to is also a very essential fact that needs to be known by the data analysts.
- This helps to effectively use the data to their advantage and thus upholding the importance of the Big Data.

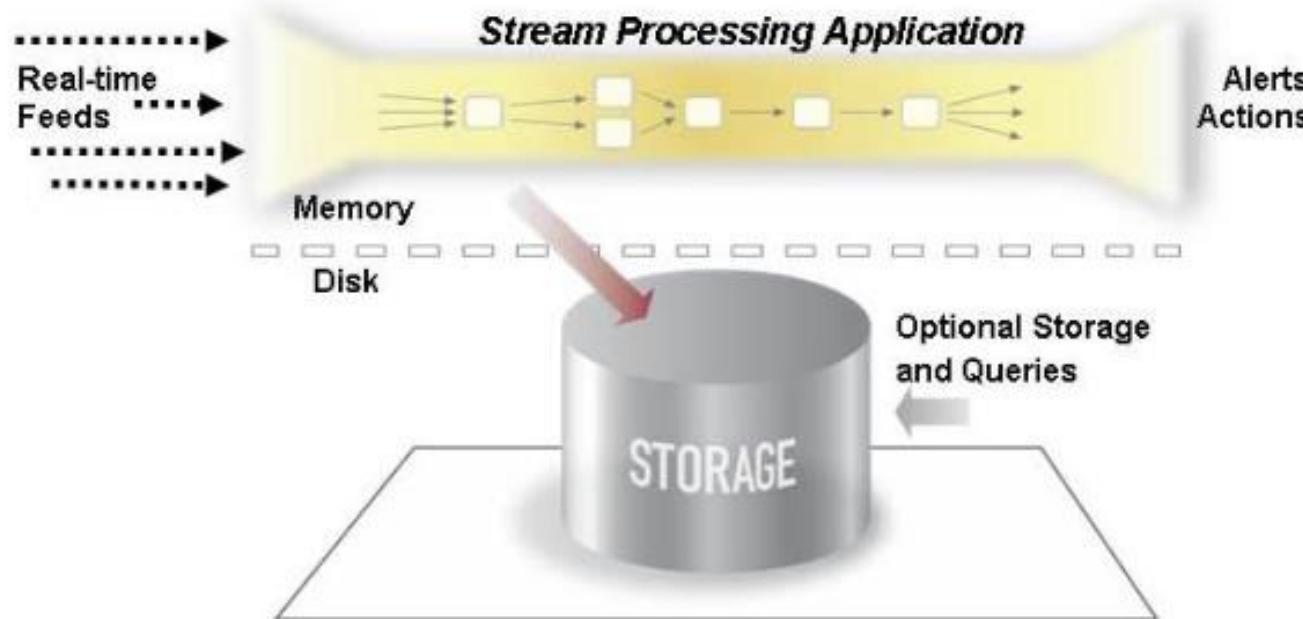
“80% of business-relevant information originates in unstructured form, primarily text.”



Structured Data vs. **Unstructured Data**

Velocity

- Refers to the speed of generation of data or
- How fast the data is generated and processed to meet the demands and the challenges



Variability

- Inconsistency which can be shown by the data at times
- It affects the process of being able to handle and manage the data effectively.

Veracity (Integrity)

- The quality of the data being captured can vary greatly.
- Accuracy of analysis depends on the veracity of the source data.

Other researches on big data

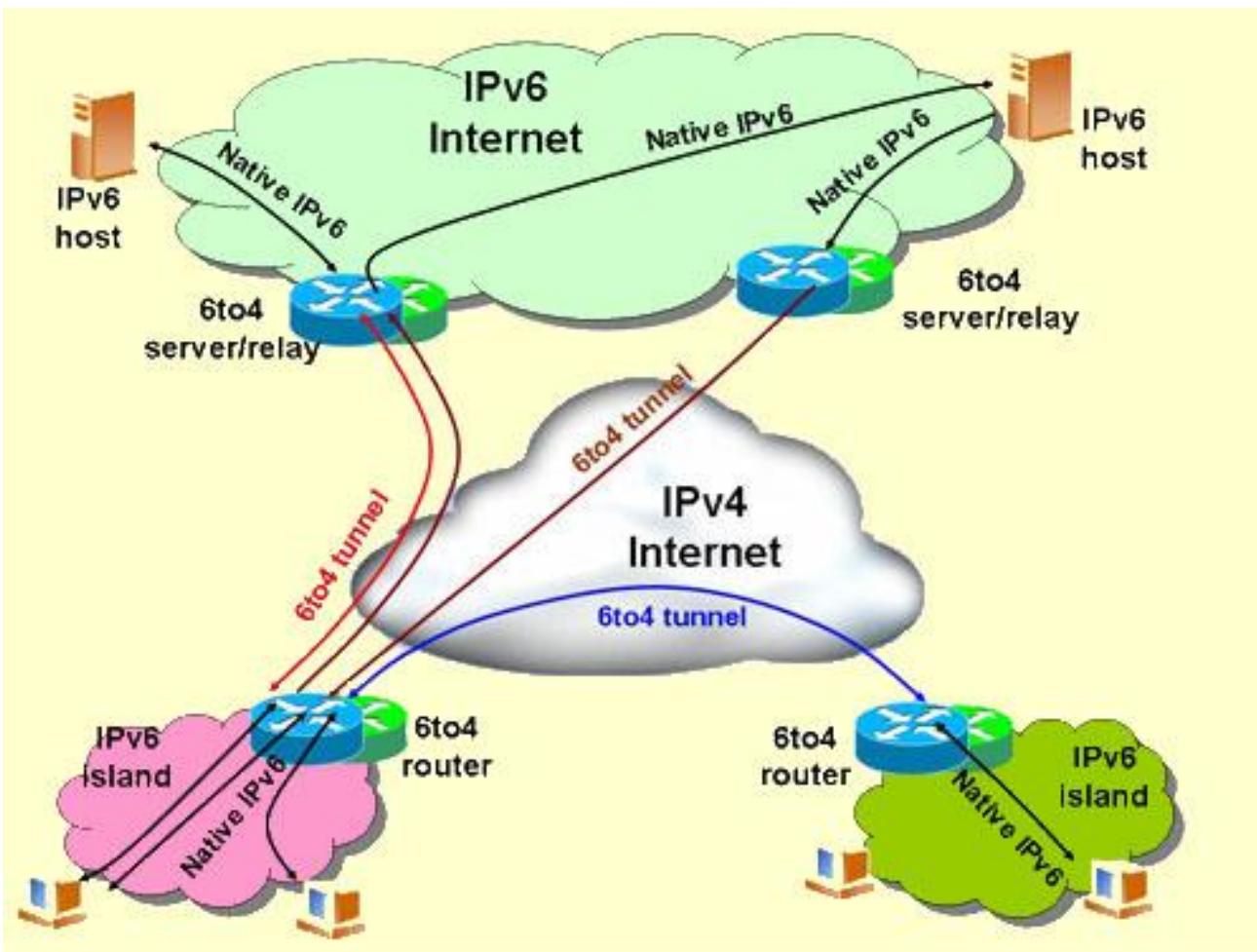
The 6C

- Area of research focus
 - Connection (sensor and networks),
 - Cloud (computing and data on demand),
 - Cyber (model and memory),
 - Content/context (meaning and correlation),
 - Community (sharing and collaboration), and
 - Customization (personalization and value).

Tools for AI and big data analysis

- Tensorflow
 - <https://www.tensorflow.org>
- Caffe
 - <http://caffe.berkeleyvision.org/>
- Paddle paddle
 - <http://www.paddlepaddle.org/>
- Microsoft Azure Machine Learning Studio
 - <https://studio.azureml.net/>
- Ali Cloud AI API
 - <https://m.aliyun.com/act/etapi>

From IPv4 to IPV6

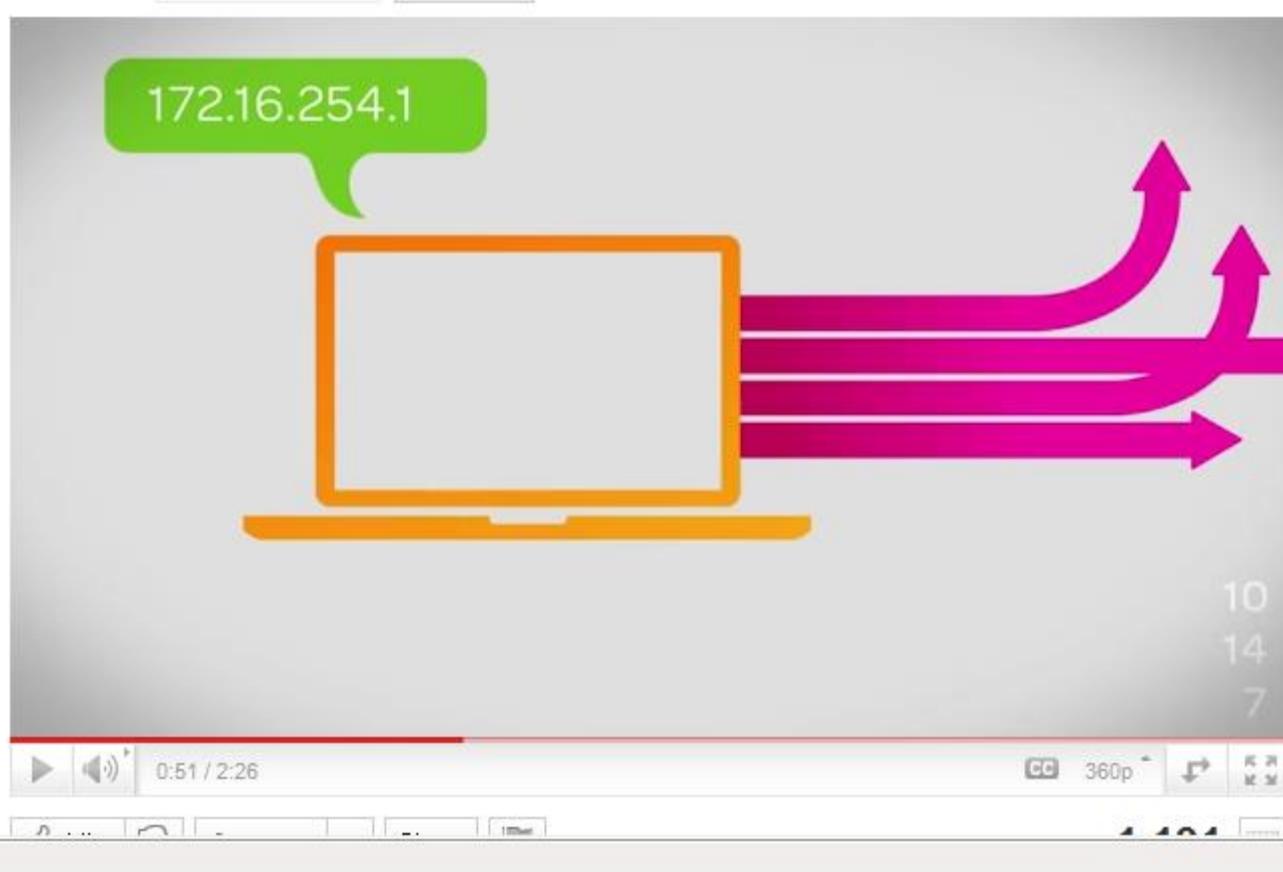


IPv4

- Since 1981, IPv4 was the first publicly used version of the Internet Protocol
- This was deemed sufficient in the early design stages of the Internet when the explosive growth and worldwide proliferation of networks were not anticipated.
- The growth of the Internet has mandated a need for more addresses than are possible with IPv4. IPv6 allows for vastly more addresses.

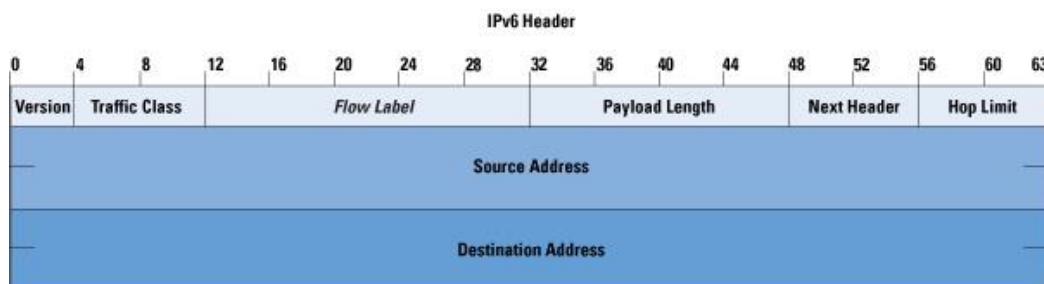
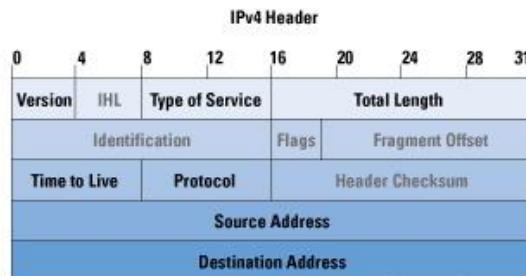
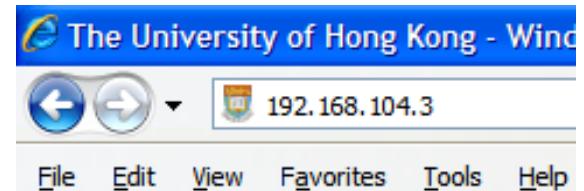
IPv6: Why do we need it?

- <http://www.youtube.com/watch?v=-r3qaVa5bns&feature=related>



IPv4 and IPv6

- IPv4 allows 32 bits for an IP address
 - → support 2^{32} (4,294,967,296) addresses,
- IPv6 uses 128-bit addresses
 - e.g. 192.168.100.1.192.168.100.1.192.168.100.1.192.168.100.1
 - supports 2^{128} (approximately 3.4×10^{38}) addresses.
3400

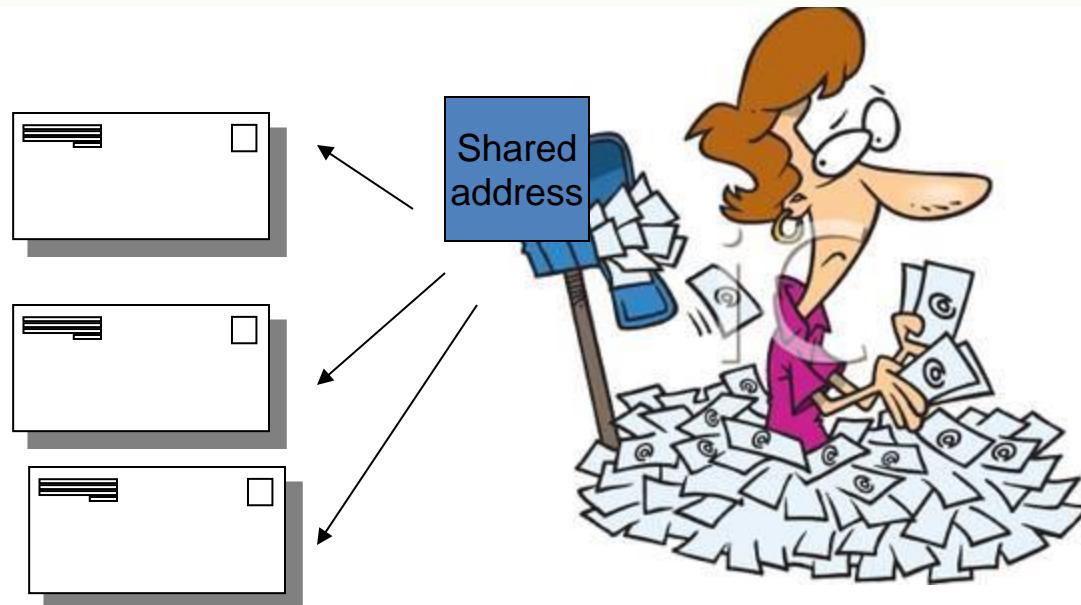
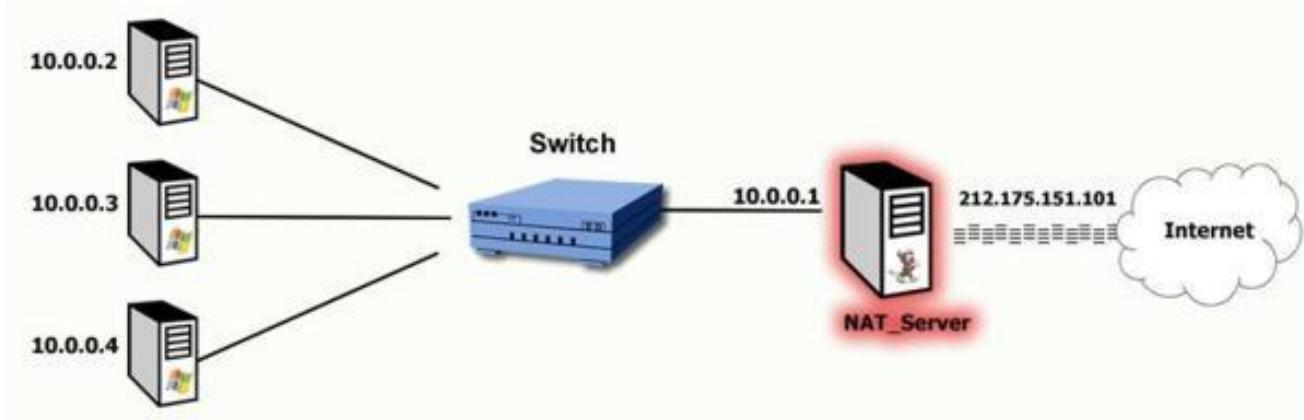


IPv4 and IPv6

- Advantages:
 - allows for many more devices and users on the internet
 - extra flexibility in allocating addresses and efficiency for routing traffic
 - eliminates the primary need for network address translation (NAT)
 - a solution to solve the problem of IPv4 address limitation
 - It simplifies aspects of address assignment and network renumbering
 - Network security is also integrated into the design of the IPv6 architecture

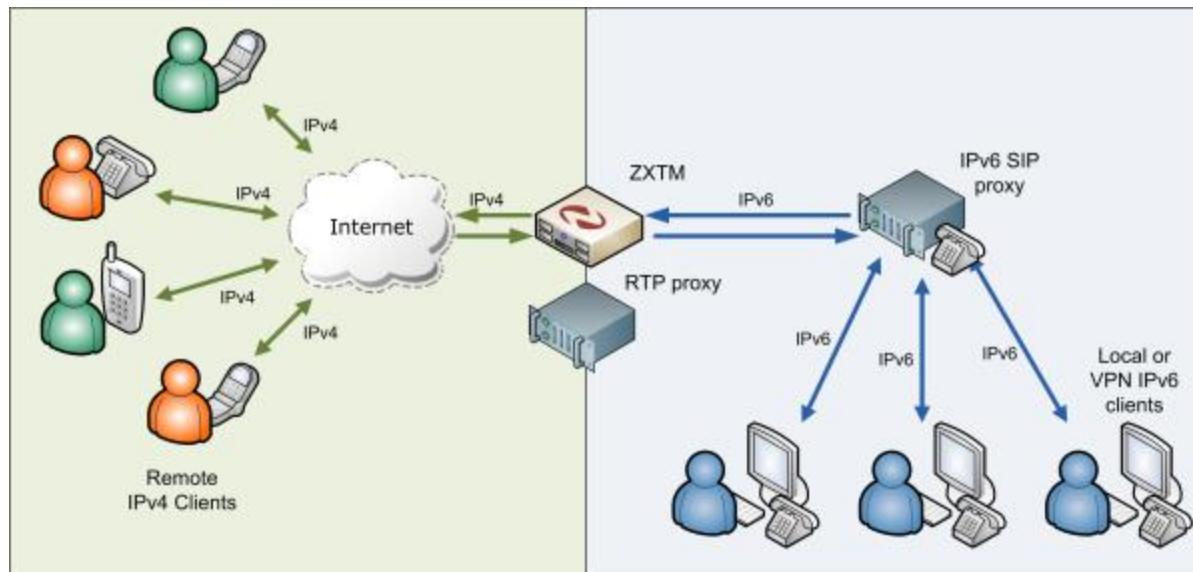
NAT for IPv4

- Network address translation (NAT)



Migration from IPv4 to IPv6

- IPv6 does not implement interoperability features with IPv4
- → Requires a parallel and independent network.
- Exchanging traffic between the two networks requires special translator gateways,
- Modern computer operating systems implement dual-protocol software for transparent access to both networks either natively or using 'tunneling'



Reference:

- http://www.ntt.com/business_e/feature/green_ict.html
- <http://www.ictliteracy.info/greenict.htm>
- http://www.info.gov.hk/digital21/eng/D21SAC/attachments/D21SAC_paper_10-2009.pdf
- http://www.gmn.hkpc.org/images/GMN_bk.pdf

ELEC2544

e-Commerce and FinTech

Wi-Fi Security

Dr. Wilton Fok

Agenda

- **Wi-Fi Basic**
- **Threats against WLANs**
- **Wi-Fi Encryption Mode Overview**

What is Wi-Fi?

- Wi-Fi (Wireless Fidelity) is a generic term that refers to the IEEE 802.11 communications standard for Wireless Local Area Networks (WLANs). It is an industry alliance to promote 802.11 interoperability.



Wi-Fi Generations

Wi-Fi Technology	Frequency Band	Bandwidth or maximum data rate
802.11a	5 GHz	54 Mbps
802.11b	2.4 GHz	11 Mbps
802.11g	2.4 GHz	54 Mbps
802.11n	2.4 GHz, 5 GHz, 2.4 or 5 GHz (selectable), or 2.4 and 5 GHz (concurrent)	450 Mbps

SSID

- An **SSID** is the name of a wireless local area network (WLAN).
- All wireless devices on a WLAN must employ the same SSID in order to communicate with each other.
- The SSID on wireless clients can be set
 - Manually:
 - by entering the SSID into the client network settings,
 - Automatically
 - by leaving the SSID unspecified or blank.

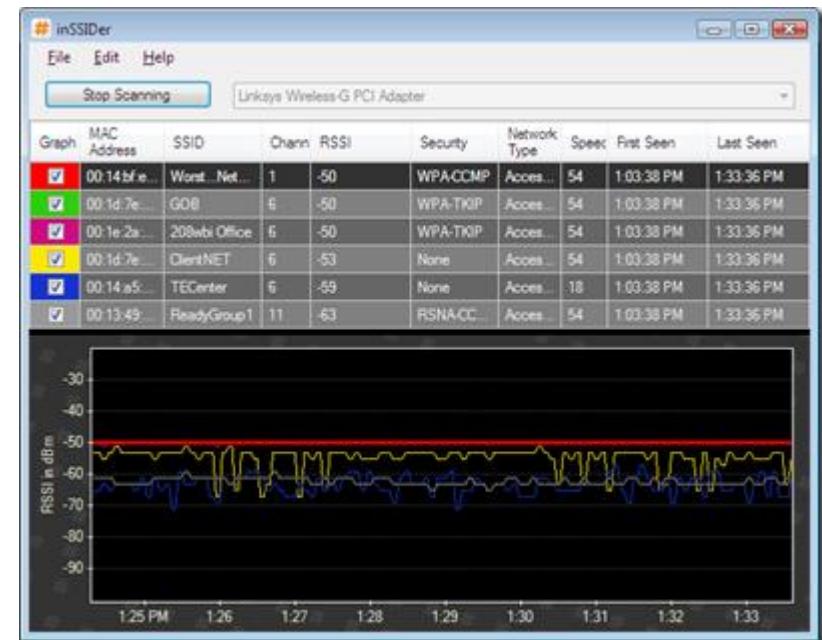


SSID

- A network administrator often uses a public SSID, that is set on the access point and broadcast to all wireless devices in range.
- Some newer wireless access points disable the automatic SSID broadcast feature in an attempt to improve network security.

Tools to detect WiFi

- inSSIDer
 - inSSIDer is Wi-Fi network scanner software for Microsoft Windows from MetaGeek, LLC. It received a 2008 Infoworld Bossie Award for "Best of open source software in networking"



Advantages of WiFi

- Fast and Cheap deployment
 - Wi-Fi allows cheaper deployment LANs (No wiring)
- Cover large areas
 - where cables cannot be run, such as outdoor areas and historical buildings, can host wireless LANs.
- Economy
 - The price of chipsets for Wi-Fi continues to drop, making it an economical networking option included in even more devices (e.g. Printer, camera, Skype phone)

Advantages

- Inter-operable
 - Different competitive brands of access points and client network-interfaces can inter-operate at a basic level of service.
 - Products with "Wi-Fi Certified" can work anywhere in the world (but Mobile is not, e.g. CDMA, TD-SCDMA)
- Secure (reasonably)
 - WiFi Protected Access encryption (WPA2) is considered secure, provided a strong passphrase is used.

Wireless LAN components

- **Access point (AP)** = bridge between wireless (802.11) and wired (802.3) networks
- **Wireless station (STA)** = PC or other device with a wireless network interface card (NIC)



Wireless LAN components

- **Infrastructure mode** = wireless stations communicate only with AP
- **Ad-hoc mode** = no AP; wireless stations communicate directly with each other

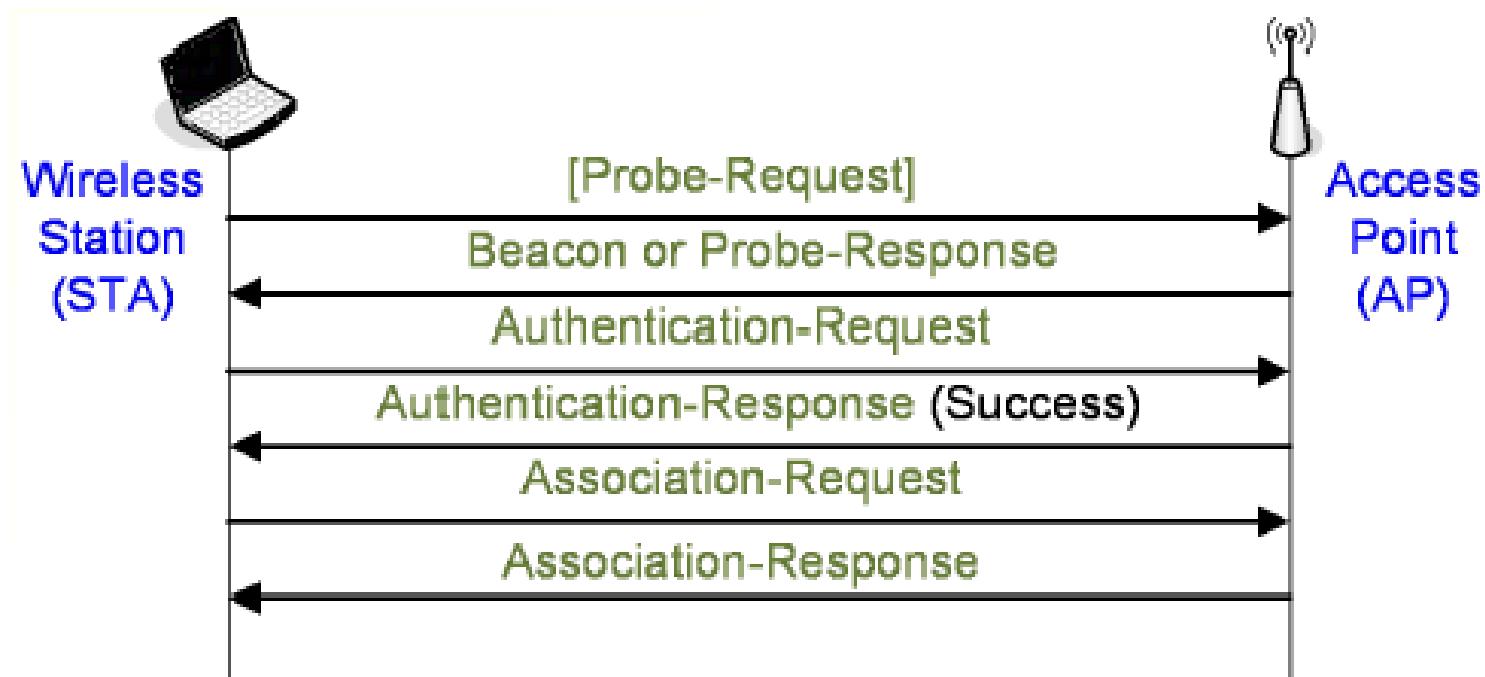


Wi-Fi Network Topologies

- **AP-based topology** (Infrastructure Mode)
 - The client communicate through Access Point
- **Peer-to-peer topology** (Ad-hoc Mode)
 - Client devices within a cell can communicate directly with each other without AP
- **Point-to-multipoint bridge topology**
 - Connect a LAN in one building to a LANs in other buildings

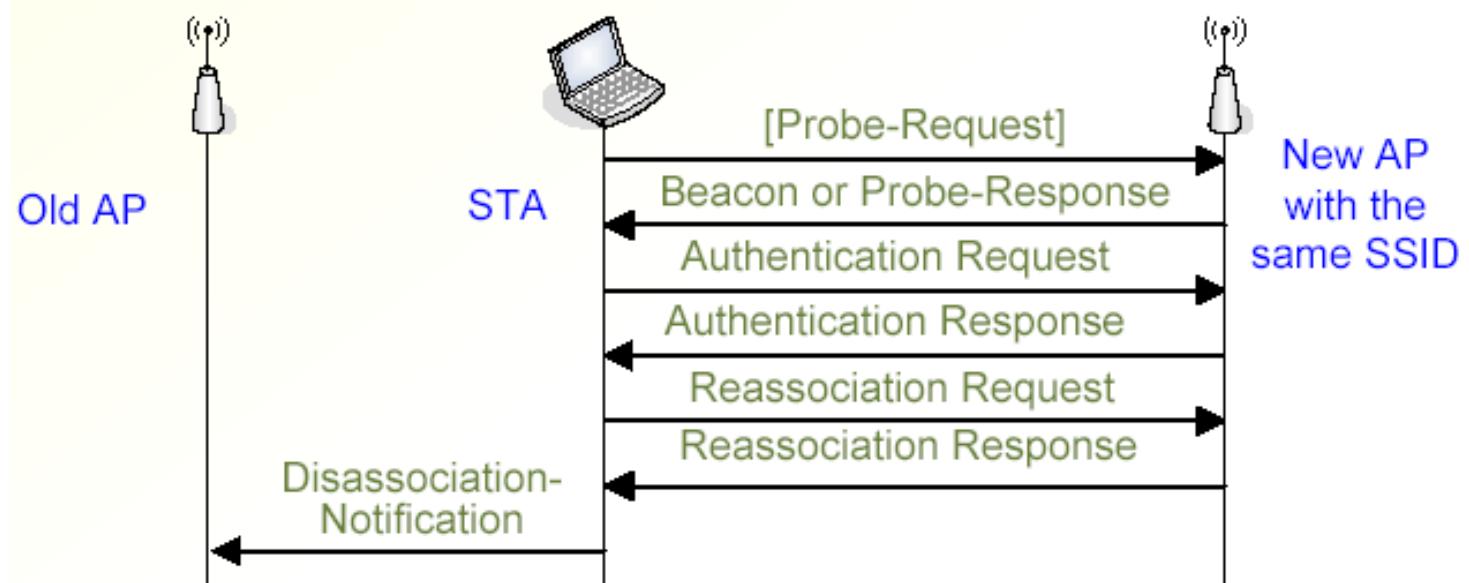
Joining a Wireless LAN

- AP sends beacons, usually every 50-100 ms
- Beacons usually include the SSID but the SSID broadcast can be turned off
- STA must specify SSID to the AP in association request



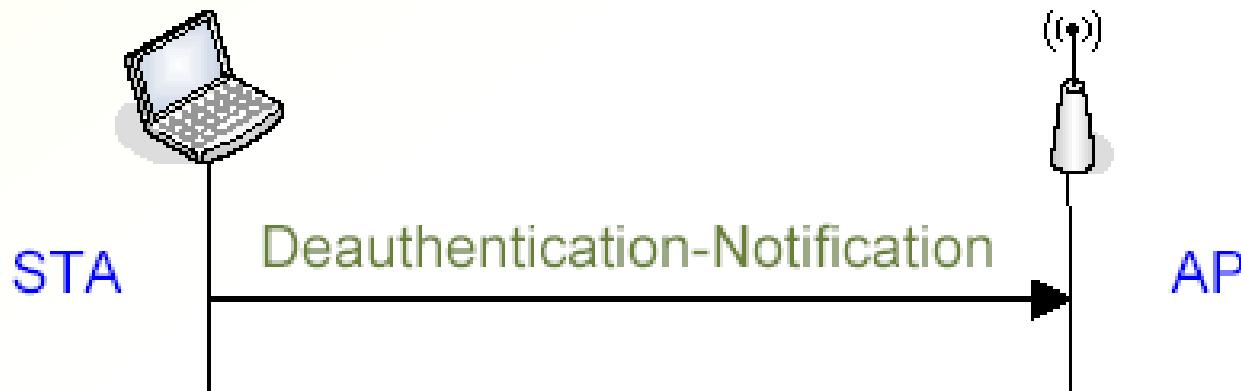
Wireless LAN Roaming

- STA chooses AP by signal strength and quality; STA can re-associate with another AP in the ESS (Extended Service Set: multiple APs with same SSID)
- If APs are connected to same IP network segment, roaming between APs is transparent to the IP layer



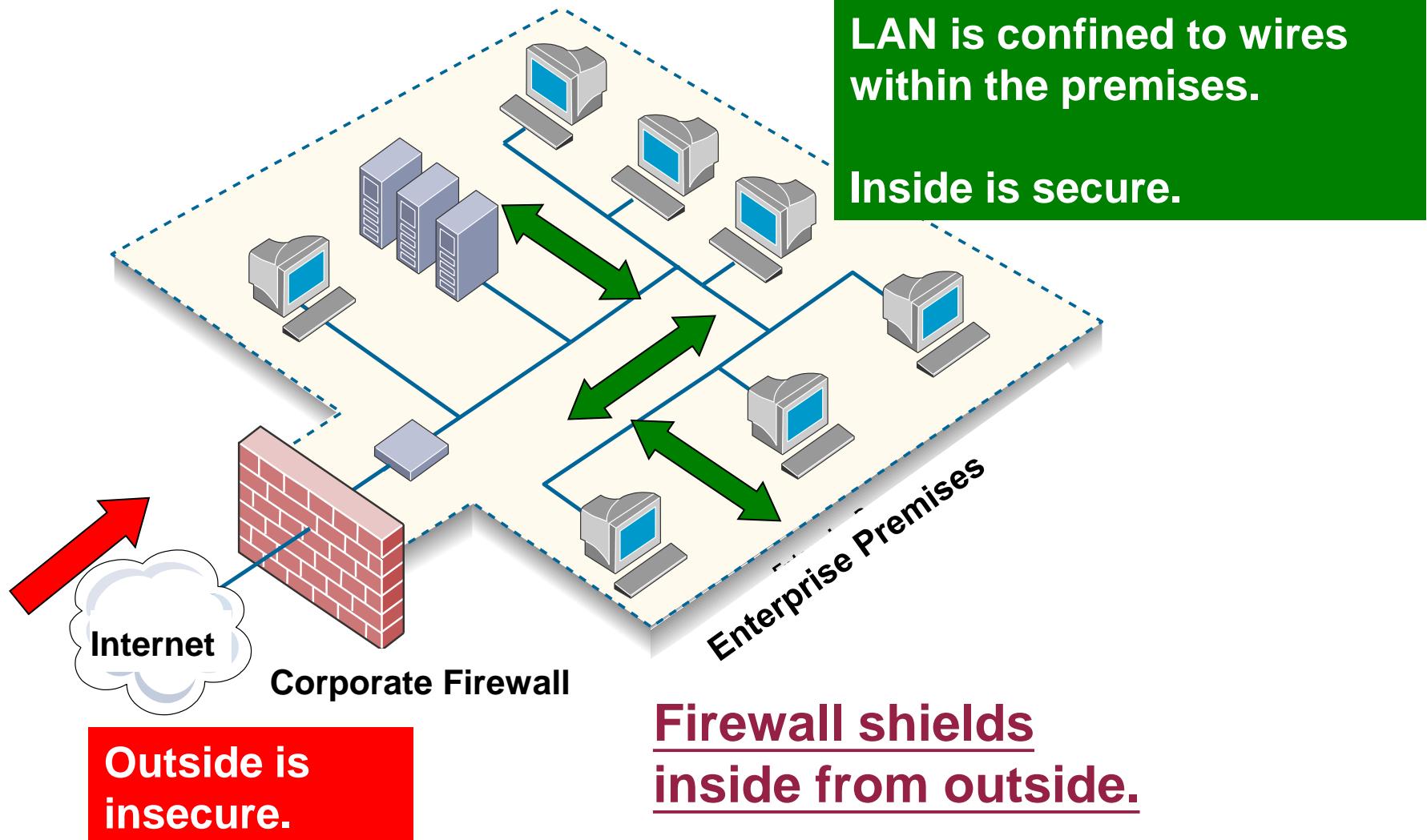
Leaving a Wireless LAN

- ❑ Both STA and AP can send a Disassociation Notification or Deauthentication Notification

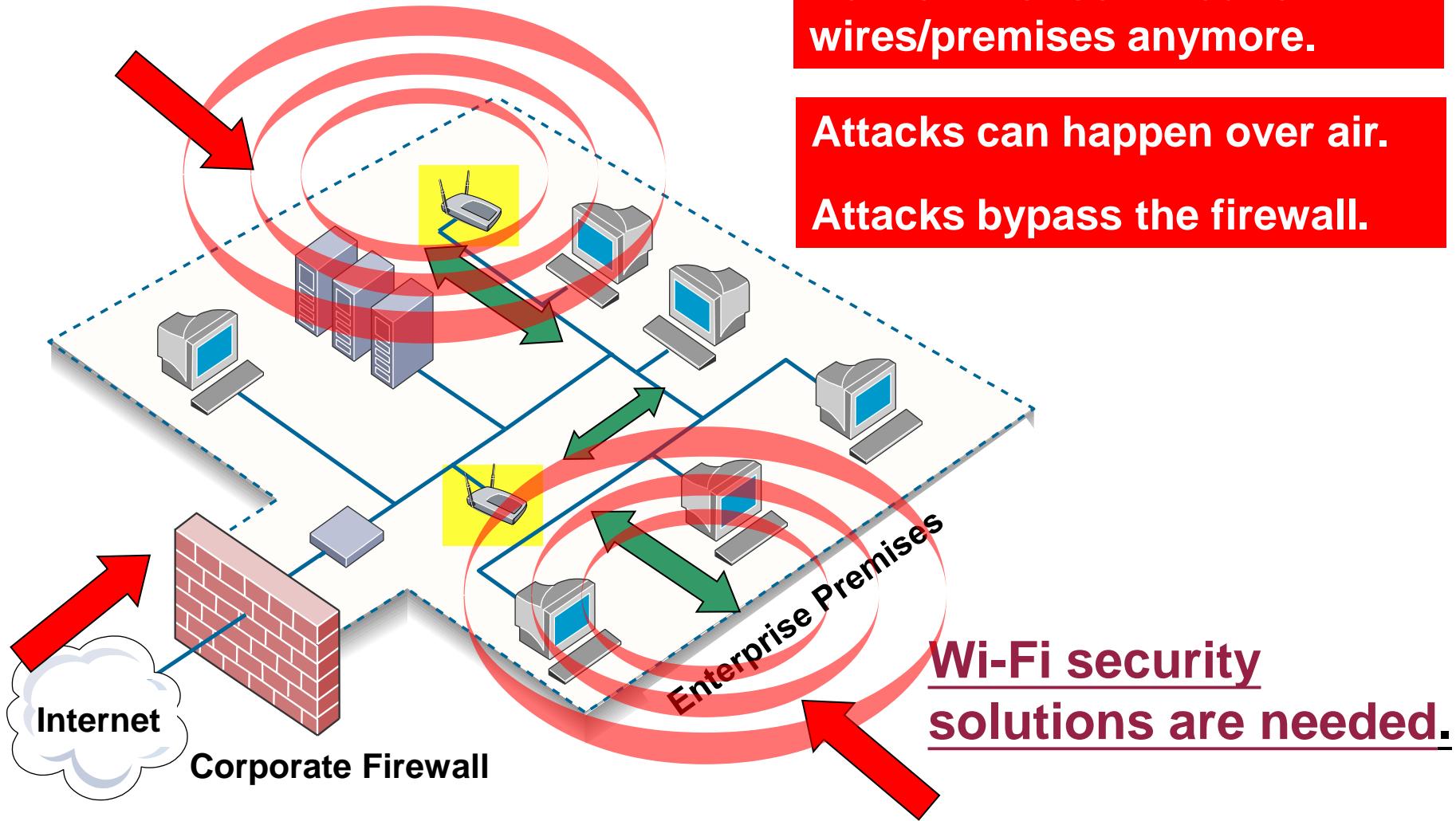


Threats against WLANs

Conventional LAN Security Model



Wi-Fi Breaks the Conventional Model



Class discussions

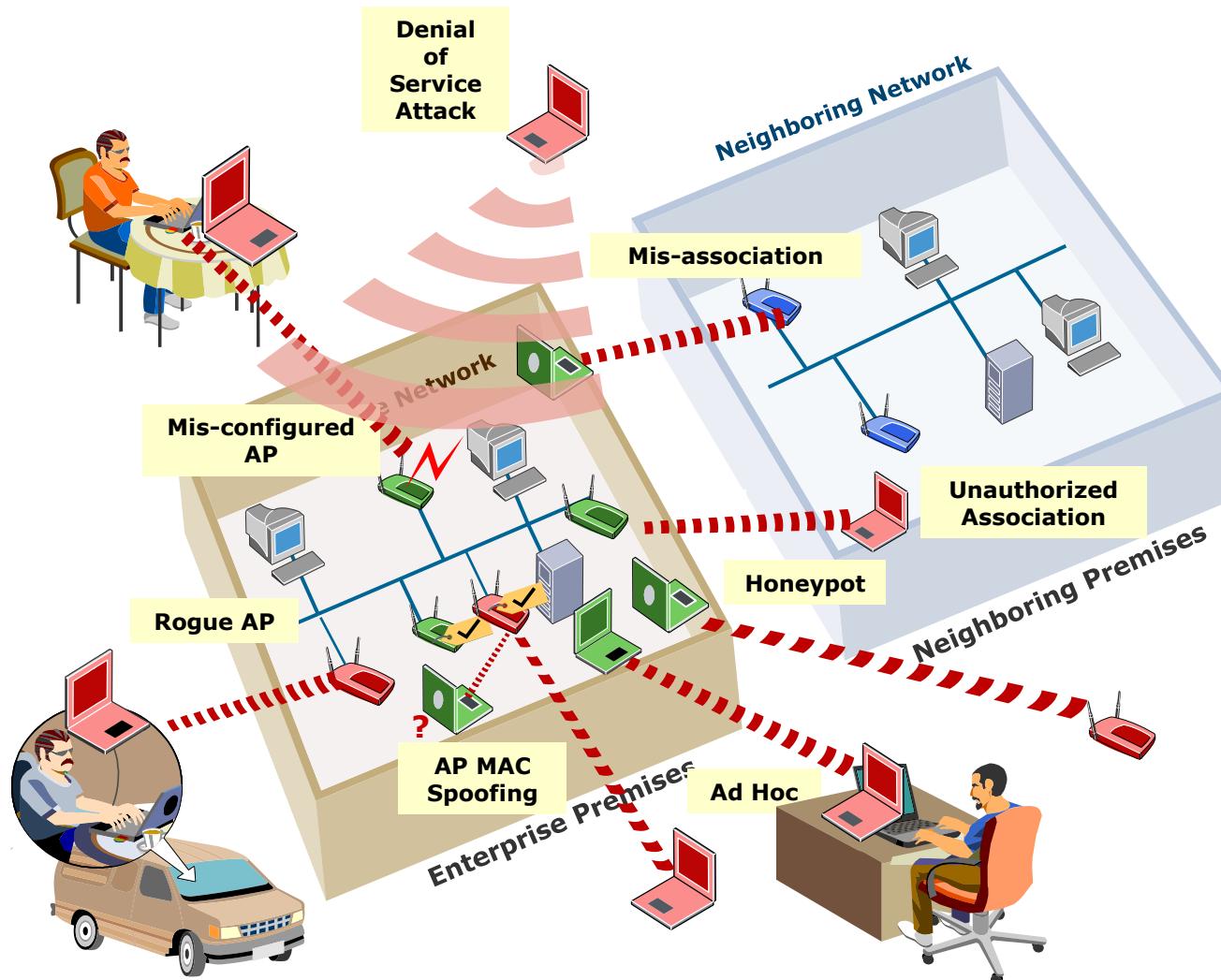
What are the WLAN Security Threat

- List as many threats against wireless LANs as you can think of. What kind of unwanted things can happen?
 - Consider home, small-business, corporate and university networks, Internet cafes and commercial hotspot operators
- Prioritize the threats roughly by how serious they are. Which threats can be ignored and which not?

Threats against wireless LANs

- Virus attack, remote control company server and steal customer information
 - Hook to a company computer, use VNC to remote control
- Intercept the information
- Use default password and reconfigure the network
- Hack WEP security
- Tap information in those WiFi network with security
- Unauthorized access to the WiFi network
- Unstable signal
- War driving

Threats from Unmanaged Devices



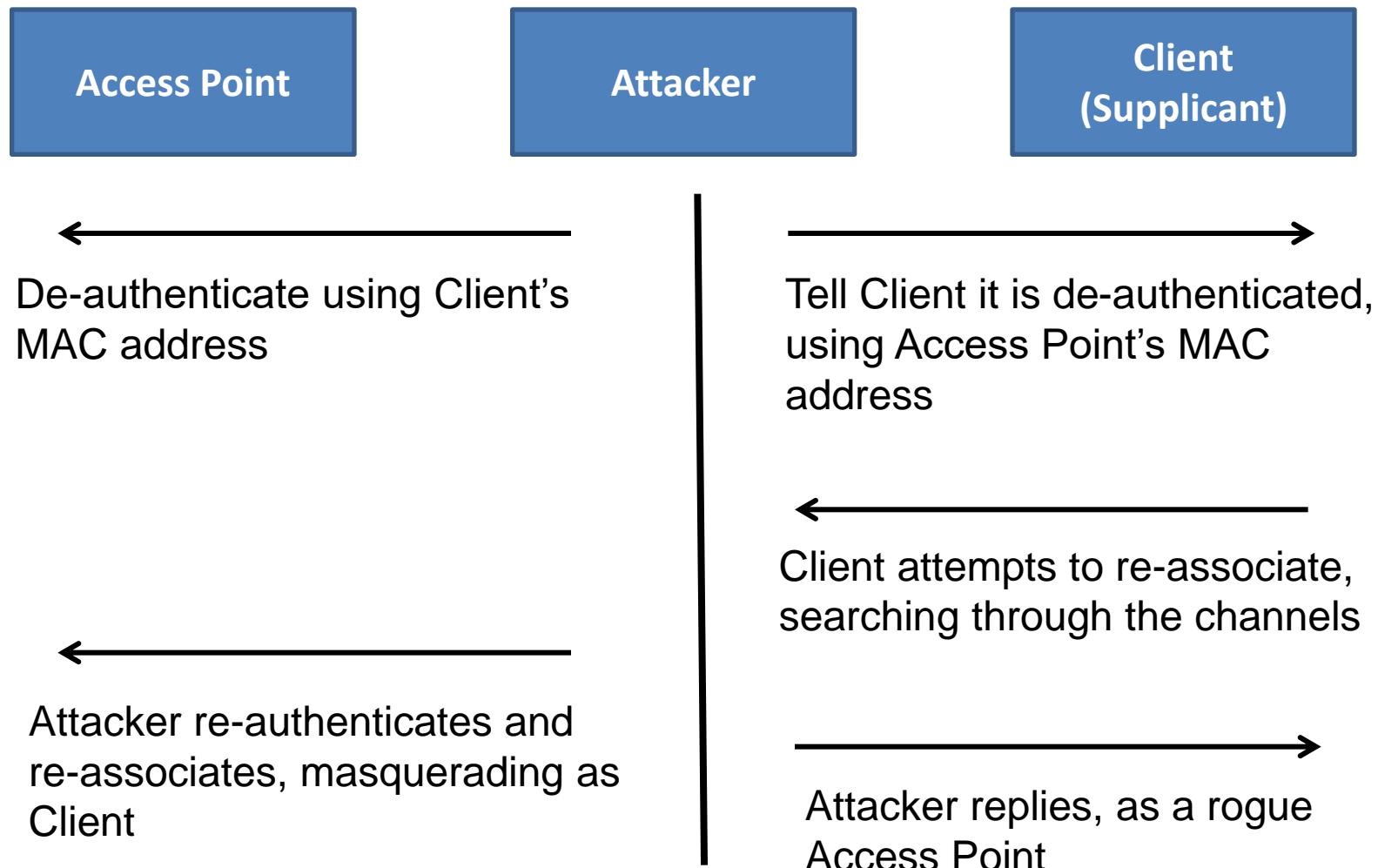
Common

- Rogue Access Points
- Mis-configured Access Points
- Ad hoc connections
- Client mis-associations
- Unauthorized associations

Malicious

- Honeypot APs
- MAC Spoofing APs
- Denial of Service
 - De-authentication flood
 - Packet storm

Example: Man in the Middle Attack -1



Example: Man in the Middle Attack -2

- Rogue APs that pretend to be valid APs
 - STAs tricked into associating with rogue AP
 - Valid AP thinks it's receiving frames from STAs
 - Attacker can change packets in transit
 - Attacker can gather authentication information

WLAN security goals

- Wireless LAN security protocols have following goals:
 - **Data confidentiality and integrity** - prevent sniffing and spoofing of data on the wireless link
 - **Access control** - allow access only for authorized wireless stations
 - **Auditing** - hotspot operators may want to meter network usage
 - **Authentication** - access control and accounting usually depend on knowing the identity of the wireless station or user
 - **Availability** - do not make denial-of-service attacks easy (radio jamming is always possible)

Overview of Wi-Fi Encryption Mode

Overview of Wi-Fi Encryption Mode -1

- **WEP (Wired Equivalent Privacy)**
 - 64 or 128-bit shared key
 - Initialization vector (IV) = 24 bits per-packet
 - RC4 encryption
 - Security weakness
 - short key size
 - may have IV collisions or altered packets, this is a limitation in WEP design, longer key cannot help
 - simple & easy to crack

Overview of Wi-Fi Encryption Mode -2

- **WPA/WPA2 (Wi-Fi Protected Access)**
 - WPA/WPA2 – WPA is based on draft 3 of 802.11i standard ; WPA2 is based on the final draft of 802.11i
 - Mode
 - Personal or PSK (Pre-shared key)
 - Pre-shared key can be a string of 8 to 63 char
 - Recommend using longer and complex key (alphabet, number, symbol) and do not use dictionary word
 - WPA-Enterprise
 - 802.1X authentication / RADIUS
 - Individual user has his/her own password
 - Much safer than Pre-shared key

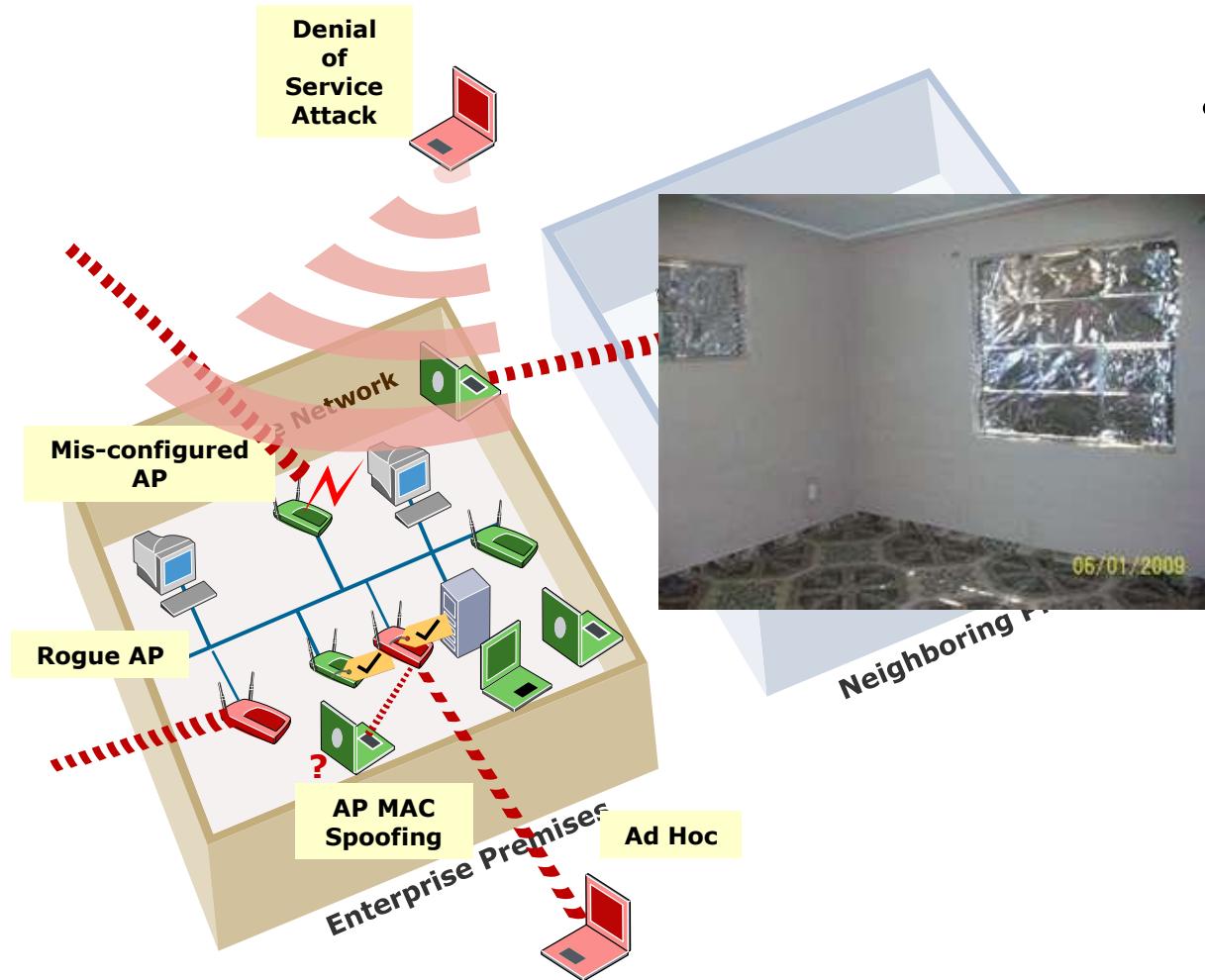
Overview of Wi-Fi Encryption Mode -3

- **WPA/WPA2 (Wi-Fi Protected Access) – cont'd**
 - TKIP (Temporal Key Integrity Protocol) / AES (Advanced Encryption Standard) encryption
 - TKIP was implemented to solve WEP problem. AES is a newer implementation and design.
 - WPA/WPA2 is much more secure than WEP
 - Loopholes were found for WPA/WPA2-TKIP and can be hacked.
 - WPA/WPA2-AES secure?

Recommendations for WLAN security measures

- The following security measures are often recommended to WLAN administrators:
 - Disable the SSID broadcast
 - Maintain a list of authorized MAC addresses and block unauthorized ones from the network
 - Select AP locations in the middle of the building (not close to windows)

Recommendations for WLAN security measures



- Use:
 - directional antennas
 - line walls
 - windows with metal foil
- to minimize the signal leakage to the outside of the building

But hackers are even more advanced...

- Drawbacks of hiding the SSID broadcast
 - Hacker can sniff the SSID when other clients associate
 - While effective against the casual user, it is ineffective as a security method because the SSID is broadcast in the clear in response to a client SSID query.
 - Turning off the broadcast of the SSID may lead to a false sense of security.

Drawbacks of hiding the SSID broadcast

- The method discourages only casual wireless snooping, but does not stop a person trying to attack the network.
- It is not secure against determined hackers, because every time someone connects to the network, the SSID is transmitted in cleartext even if the wireless connection is otherwise encrypted.
- An eavesdropper can passively sniff the wireless traffic on that network undetected (with software like InSSIDer), and wait for someone to connect, revealing the SSID.
- As disabling SSID does not offer protection against determined crackers, proven security methods should be used such as requiring WPA2

Limitations of other security measures

- Access control list of authorized MAC addresses
 - Attacker can sniff and spoof another client's MAC address
 - AP locations, directional antennas and metal foil to keep signal inside a building
 - Attacker can use a directional antenna with high gain
- Weak mechanisms are rarely worth the trouble



Tips and Recommendation

- Enable encryption mode and use WPA/WPA2-AES
- Though MAC address can be spoofed, recommend to enable MAC Address Filtering
- Though hidden SSID can be seen with a suitable tool, recommend to hide SSID
- Change SSID to not easily identifiable
- Do not just use the “off-the-shelf” settings, need to review
- Better not to put the AP near to the Windows to reduce chance of connection outside your home/office
- Consider to use VPN over public hotspots

Reference

- Hong Kong Wireless Technology Industry Association (www.hkwtia.org)
- Hong Kong Wireless Development Centre (www.hkwdc.org)
- Professional Information Security Association (www.pisa.org.hk)
- SafeWifi Hong Kong (www.safewifi.hk)
- Wardrive.net (www.wardrive.net/)
- Wi-Fi Alliance (www.wifi.org)

Appendix

- Below we describe a collection of cost-free tools that can be used both as attack tools and as audit tools.
 - AirJack (<http://802.11ninja.net/airjack/>) is a collection of wireless card drivers and related programs. It includes a program called monkey_jack that automates the MITM attack. Wlan_jack is a DoS tool that accepts a target source and BSSID to send continuous deauthenticate frames to a single client or an entire network (broadcast address). Essid_jack sends a disassociate frame to a target client in order to force the client to reassociate with the network, thereby giving up the network SSID.
 - AirSnort (www.airsnort.shmoo.com) can break WEP by passively monitoring transmissions and computing the encryption key when enough packets have been gathered.
 - Ethereal (www.ethereal.com) is a LAN analyzer, including wireless. One can interactively browse the capture data, viewing summary and detail information for all observed wireless traffic.
 - FakeAP ([ww.blackalchemy.to/project/fakeap](http://www.blackalchemy.to/project/fakeap)) can generate thousands of counterfeit 802.11b access points.
 - HostAP (www.hostap.epitest.fi) converts a station that is based on Intersil's Prism2/2.5/3 chipset to function as an access point.

Appendix

- Kismet (www.kismetwireless.net) is a wireless sniffer and monitor. It passively monitors wireless traffic and dissects frames to identify SSIDs, MAC addresses, channels and connection speeds.
- Netstumbler (www.netstumbler.com) is a wireless access point identifier running on Windows. It listens for SSIDs and sends beacons as probes searching for access points.
- Prismstumbler (prismstumbler.sourceforge.net/) can find wireless networks. It constantly switches channels and monitors frames received.
- The Hacker’s Choice organization (www.thc.org) has LEAP Cracker Tool suite that contains tools to break Cisco LEAP. It also has tools for spoofing authentication challenge-packets from an AP. The WarDrive is a tool for mapping a city for wireless networks with a GPS device.
- StumbVerter (www.sonar-security.com/sv.html) is a tool that reads NetStumbler's collected data files and presents street maps showing the logged WAPs as icons, whose color and shape indicating WEP mode and signal strength.
- Wellenreiter (<http://www.wellenreiter.net/>) is a WLAN discovery tool. It uses brute force to identify low traffic access points while hiding the real MAC address of the card it uses. It is integrated with GPS.
- WEPcrack (www.wepcrack.sourceforge.net) cracks 802.11 WEP encryption keys using weaknesses of RC4 key scheduling.

ELEC2544

E-Commerce and FinTech

Augmented Reality

Dr. Wilton Fok

Augmented Reality (AR)

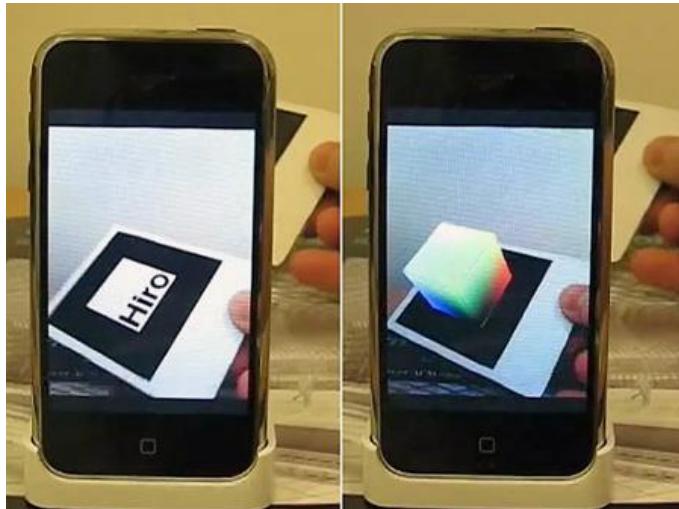
Augmented reality (AR) is a term for the view of a physical real-world environment whose elements are augmented by virtual computer-generated imagery.

Augmented reality (AR)

- AR is a live, direct or indirect, view of a physical, real-world environment whose elements are augmented by computer-generated sensory input such as sound, video, graphics or GPS data.

AR vs VR

- AR enhances user's current perception of reality.
- VR (virtual) reality replaces the real world with a simulated one.



Characteristic of AR

- Real-time
- In semantic context with environmental elements
 - E.g. sports scores on TV during a match
- Information about the surrounding real world of the user becomes interactive and digitally manipulable.



Characteristic of AR

- Artificial information about the environment and its objects can be overlaid on the real world.



Enabling technologies for AR

- Head-mounted displays
- Virtual retinal displays for visualization purposes
- Controlled environments: sensors and actuators
- computer-generated imagery in live-video streams
 - to enhance the perception of the real world.



Enabling technologies for AR

- Image/pattern recognition
 - E.g. identify the food and show the energy content
- Text recognition
 - e.g. Recognize the words in a printed book and provide dictionary service.
- Location base
 - E.g. GPS to identify the position



Advantage of AR

- Applications of Augmented reality (AR)
 - Integrated virtual world with real world
 - Promote real world products in the virtual world
 - E.g. users are required to buy candies in the real world as weapons in the virtual world
 - Brand building in the virtual world
 - E.g. the company logo, brand ad...etc are displayed in the virtual world.
 - Promote selling real product



AR Content Management Systems

- buildAR.com(base on pattern)
 - a web based content platform for building geolocation and natural feature tracking based mobile augmented reality.
 - Demo video:
<http://www.youtube.com/watch?v=NfxDua2RGX8&feature=related>



AR Content Management Systems

- Hoppala Augmentation(Base on location)
 - a web based content platform for creating geolocation based mobile augmented reality.
 - Demo video
<http://www.youtube.com/watch?v=PfdxbL6ue1U>



SDK for AR apps development

- Free closed source
 - metaio Mobile SDK
 - offers free natural features tracking that is available for both Android and iOS.

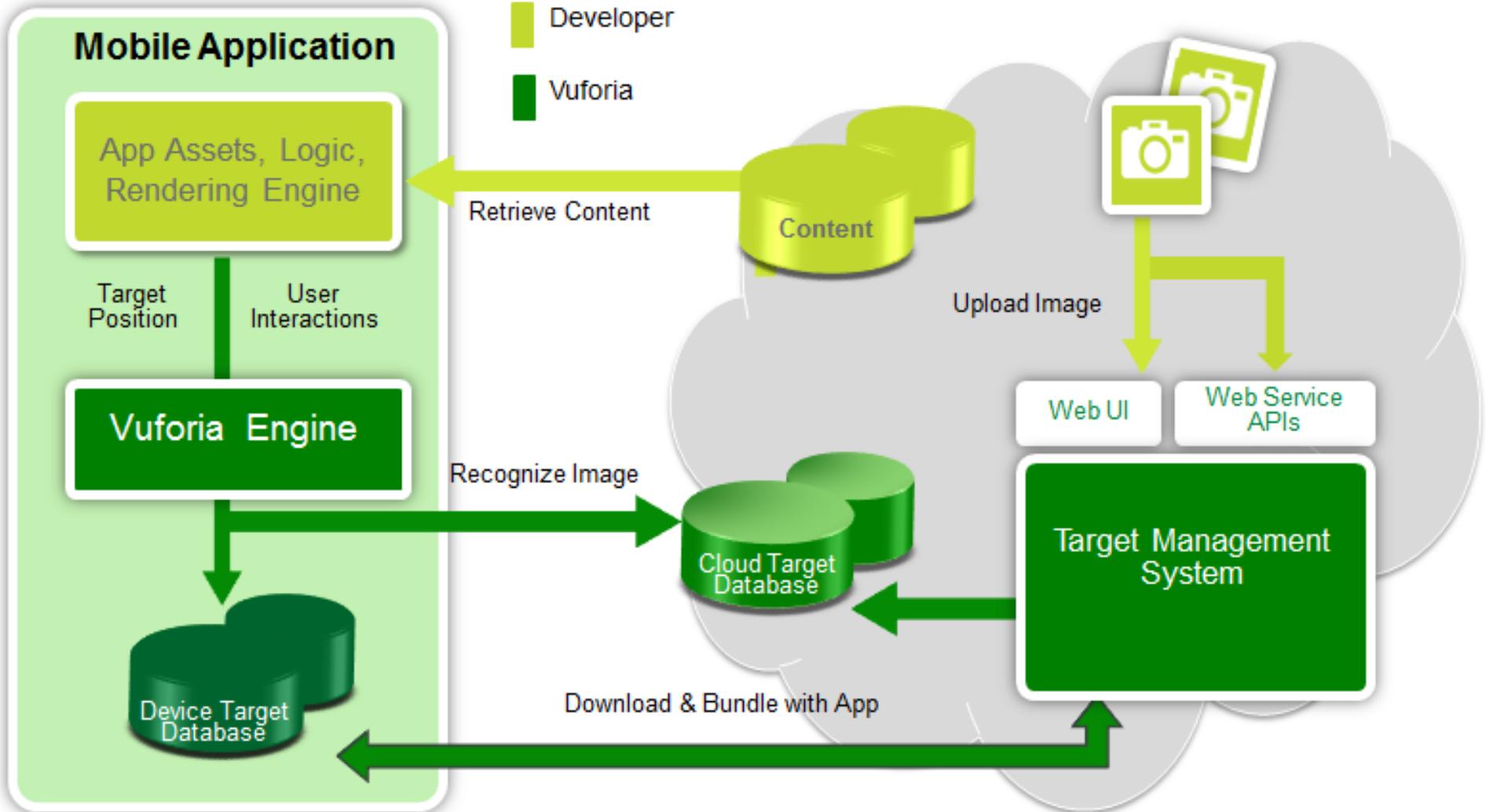


SDK for AR apps development

- Qualcomm AR SDK (QCAR) (Vuforia)
- <https://developer.vuforia.com/resources/sample-apps>
 - A free AR solution for detection and tracking of reference images and markers using natural feature detection that is available for both Android and iOS.



SDK for AR apps development

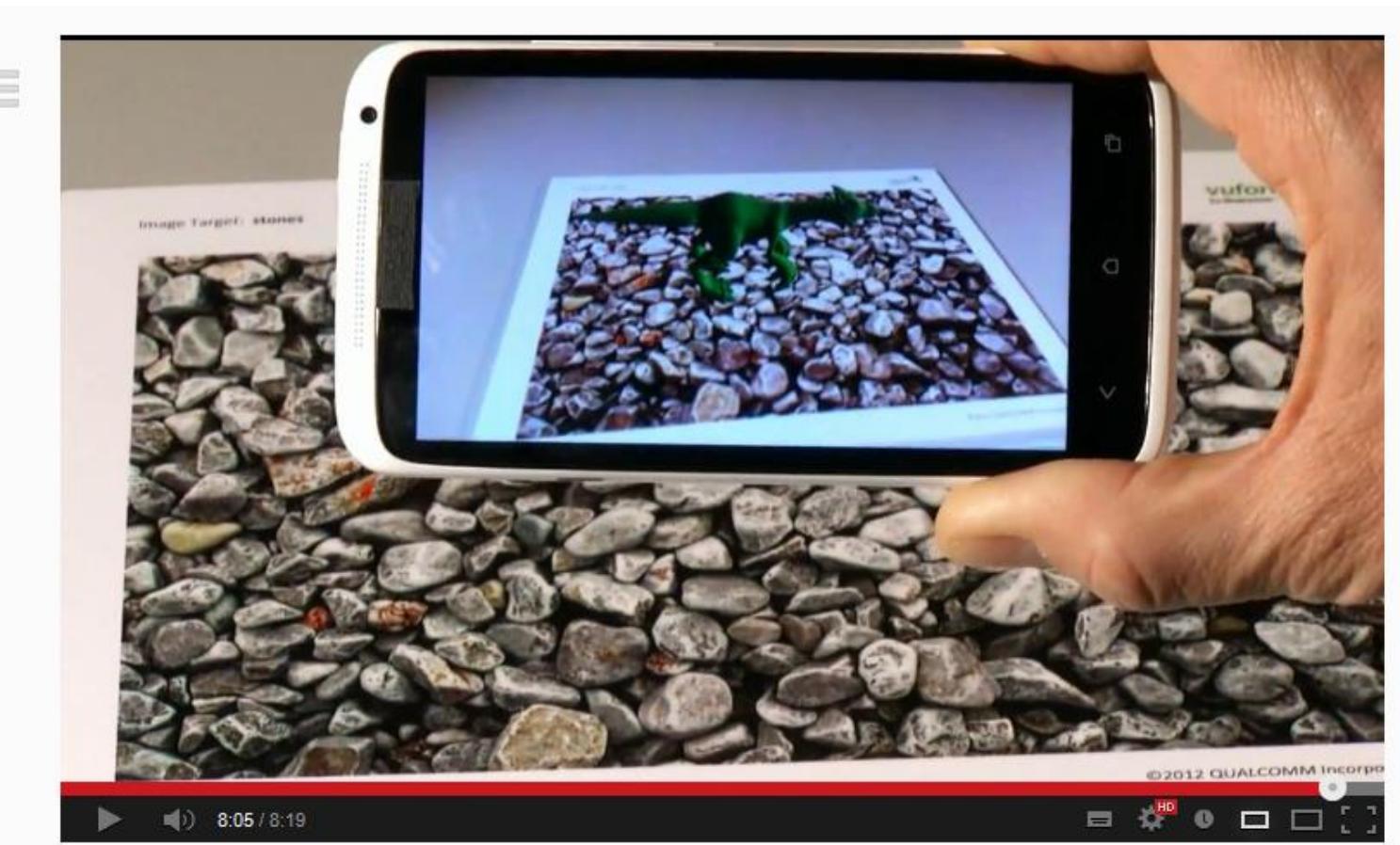


How to build an AR application?

- <https://developer.vuforia.com/resources/dev-guide/step-2-compiling-simple-project>
- <https://developer.vuforia.com/resources/tutorials>

Video demo

- http://www.youtube.com/watch?v=WrEnREOT1F0&feature=player_embedded



Q&A



ELEC2544

e-Commerce and FinTech

Communication Channel Security

Dr. Wilton Fok

Contents

- Introduction of security
- Risk in the Communication Channel
- Securing the Communication Channel
- Symmetric Key Encryption
- Asymmetric Key Encryption
- Digital Signatures
- Hash Functions
- Legal and Ethical Issues
- Summary
- References

Introduction

- E-Commerce loses many potential customers due to the perceived lack of security when making payments.
- Any information being sent from a customer to the web server via the Internet has the potential to be intercepted, altered or deleted.
- There are many reasons why commerce on the Internet is prompted to security problems
- In this session, we will:
 - Look at the various risks a client faces when conducting eCommerce via the Internet.
 - See how security is a combination of technology, policy and procedure, and people.



Security Overview

- There is no point making one area, such as the server secure, if the data transaction is poor secured.
- Security must be considered as a property of the entire system and it should be designed into systems and not as an after-thought if it is to be effective.

End-to-End Security

Application Layer
↓
Network Layer
↓
Data Layer
↓
Physical Layer



Application Layer
↑
Network Layer
↑
Data Layer
↑
Physical Layer

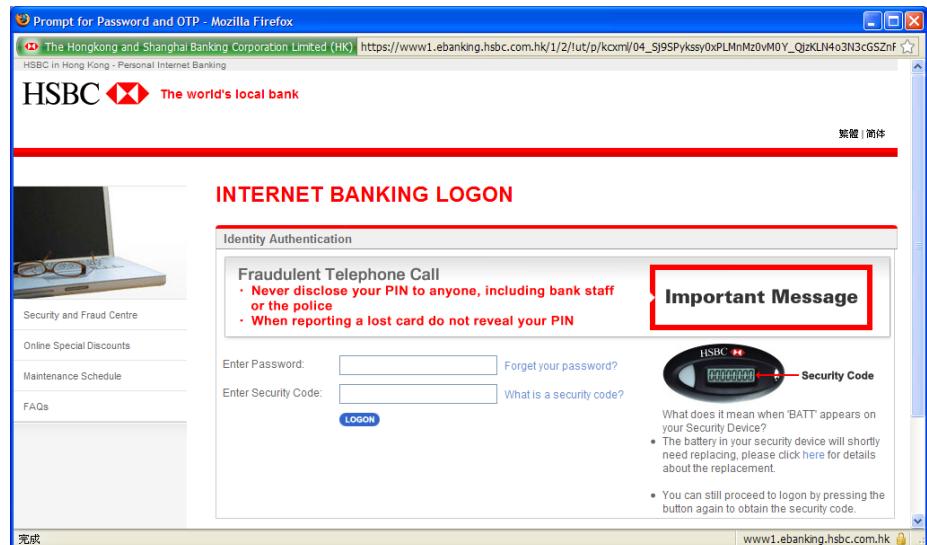
Security Overview

- Elements that needed to secure the system:
 - Technology
 - encryption, firewalls, security tools
 - Policies and Procedures
 - defines what is being protected and why.
 - People
 - educating the people using the system.
- But many companies consider security to be a technology problem only.
- While many security technologies have been proven vulnerability, the majority of security weaknesses have stemmed from inadequate user understanding and a failure to comply with policy or procedures.

(Ref: Schneider, G., Electronic Commerce, Course Technology, 2005, Sixth Edition, pp 345.)

Security Overview

- In e-Commerce, both the Customer and Merchant are vulnerable to risk.
- The amount of risk is dependant on:
 - Financial significance of the data
 - Impact on competitive advantage of the firm
 - Exposure to fraud
 - Need for confidentiality
 - Need for privacy



Q: What are the security risk?

- http://www.explainingcomputers.com/explaining_security.html



Video: Introduction to Security

- Security Threats
 - User Errors
 - Hardware Failure
 - Theft
 - Power Surges
 - Hackers and viruses
 - Fire and flood
 - Terrorism

Video: Introduction to Security

- Good Security Includes:
 - Making back-ups
 - Protecting hardware and media
 - Encrypting Sensitive data
 - Password Management
 - Firewalls and antivirus software

Video: Introduction to Security

- Good Security Includes:
 - Making back-ups
 - Keeps at least two copies in different media
 - E.g. on USB drive or on-line back up e.g. Google docs
 - Protecting hardware and media
 - Store back-up media in different place
 - Encrypt sensitive data
 - Storing in USB key is risky
 - Use Encryption on storage media

Video: Introduction to Security

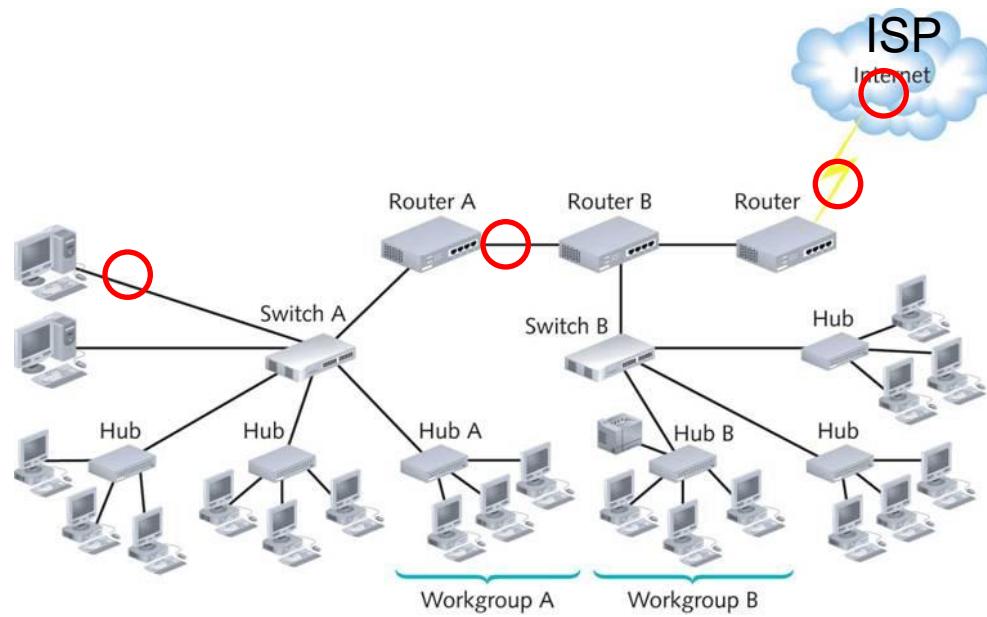
- Good Security Includes:
 - Effective passwords management
 - Password should:
 - Be at least 6 characters
 - Use letters and numbers
 - Be changed regularly
 - Be known only to the user
 - Not be related to the user
 - Be different for each application
 - Firewall and anti-virus software
 - Firewall is a security filter which avoid unauthorized access

Risks in the Communication Channel

- While a customer must protect their data and system at the client end, they must also protect their data as it travels through the network to the service.
- This data could be confidential information such as credit card numbers, usernames, password, etc.
- Data is vulnerable while:
 - It is stored on the client machine
 - It is transferring between computers.
 - Information may be intercepted at multiple points of the network between the client and server.

Risks in the Communication Channel

- These points include:
 - 1. network on the browser's side of the connection
 - 2. network on the server's side of the connection
 - 3. end-user's ISP
 - 4. server's ISP
 - 5. either ISP's region access provider



Risks in the Communication Channel

- To gain unauthorized access to information these attackers will use:
 - Sniffing / Eavesdropping (竊聽)
 - intercepting information and listening to messages.
 - Traffic analysis
 - analyzing which parties are communicating with whom.
 - Crypto-analysis
 - decrypting encoded messages
 - Authentication Attack
 - users pretend as somebody else to gain privileges

Types of man-in-the-middle attacks

- (a) **Normal Communication**
 - In this case, the data is transmitted without incident.

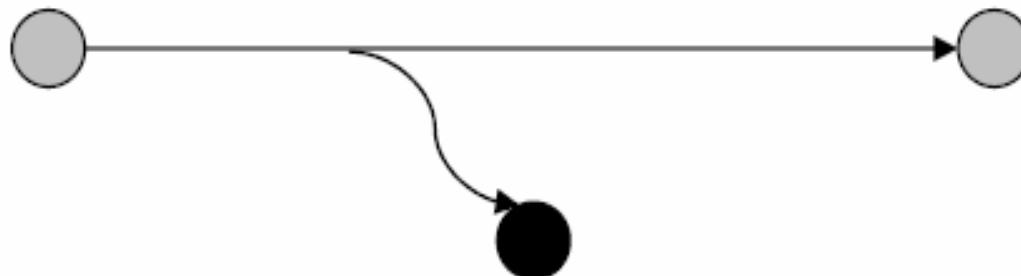


Types of man-in-the-middle attacks

- (b) **Interruption**
 - Data is transmitted; however, the data is stopped by a third party.
 - The data fails to get to its intended destination.

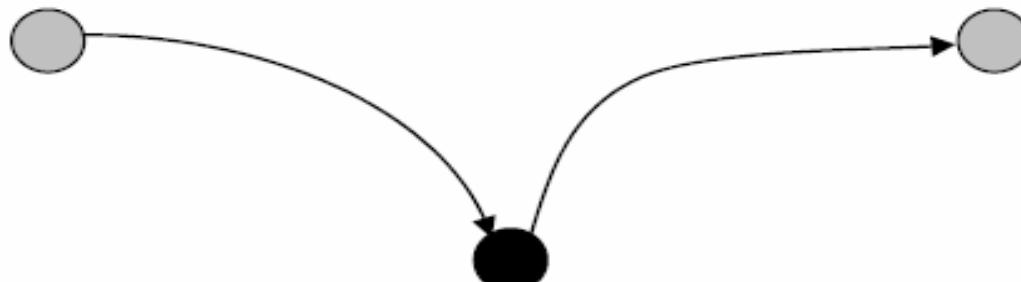


- (c) **Interception**.
 - Data is transmitted and reaches the intended destination. Unfortunately, the data is copied by a third party.
 - Called packet sniffing.

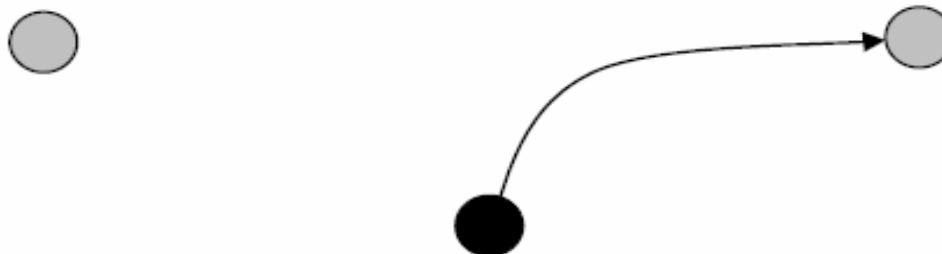


Types of man-in-the-middle attacks

- (d) **Modification**
 - Data is transmitted and intercepted by a third party.
 - Data is modified then sent to the intended destination.

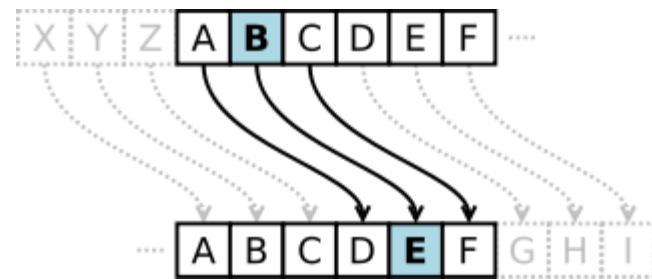
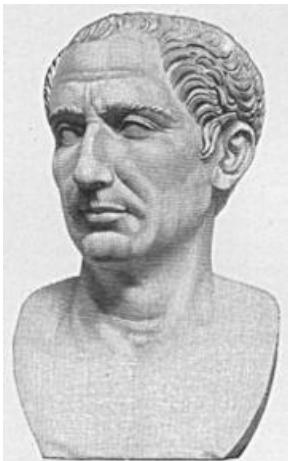


- (e) **Fabrication**
 - Client does not send any data.
 - The data is created and transmitted to a third party.
 - A third party may be required to falsify their identity, such as an IP address.



Securing the Communication Channel

- Cryptography
 - Cryptography Is the science of communicating over insecure communication channels by encoding messages so only authorised persons can decode it.
- Encryption techniques have been used in history, including:
 - the famous 'Caesar Ciphers', and
 - the German's 'enigma' machine of the Second World War.



The Caesar cipher is named for Julius Caesar, who used an alphabet with a left shift of three.

.....



Securing the Communication Channel

- Example: **Substitution Cipher: Caesar Cipher**
 - Caesar cipher involves replacing each letter of the alphabet with the letter standing k places further down the alphabet.
 - The general form of Caesar cipher is given by the following:
$$C = E(p) = (p+k) \text{ mod}(26)$$
e.g., if $k=3$,

Plaintext: **the quick brown fox jumps over the lazy dog**

Ciphertext: **WKH TXLFN EURZQ IRA MXPSV RYHU WKH ODCB GRJ**

- Now encipher the following plaintext using Caesar cipher with a key= $k=3$

Plaintext: **meet me after the party**

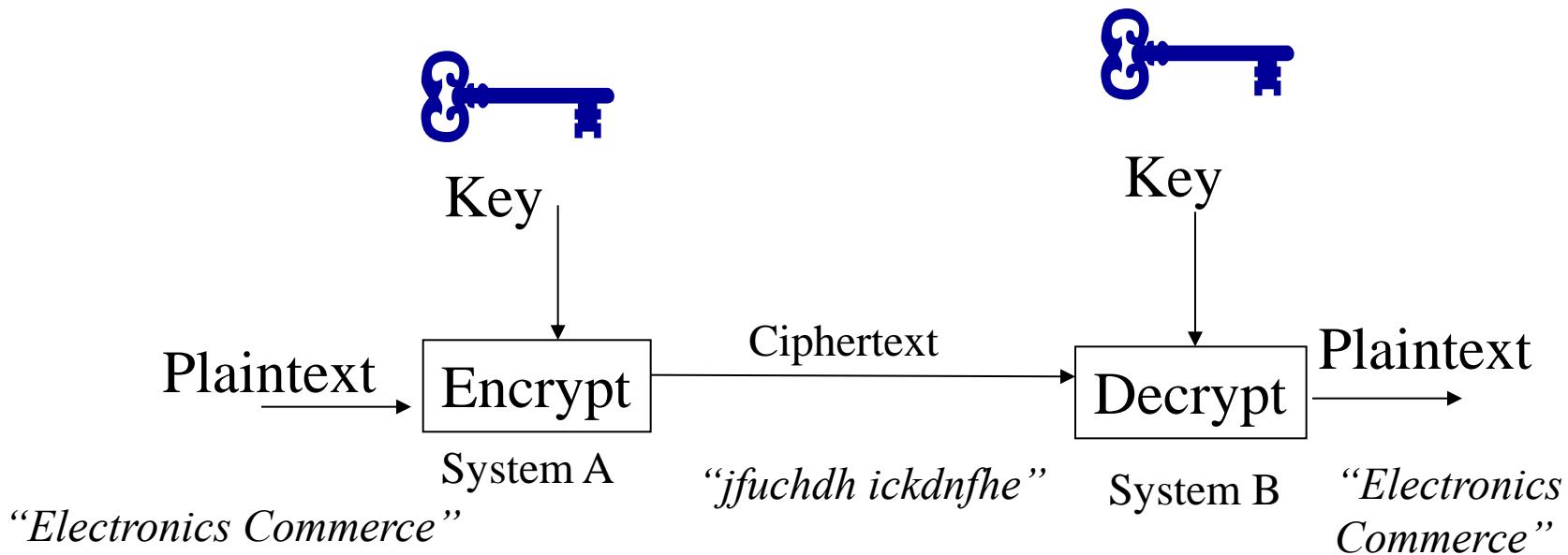
Ciphertext: **PHHW PH DIWHU WKH SDUWB**

Securing the Communication Channel

- Pros:
 - Simple algorithm
 - Fast computation
- Cons:
 - Too simple
 - The key can be easily discovered by counting the statistics of the common characters.

Securing the Communication Channel

- Cryptography involves taking a plain text message that anyone can read and converting it, via an algorithm, into an encoded message called ciphertext.
- To decode the message back into a readable form, another piece of information is needed, this is called a key.



Securing the Communication Channel

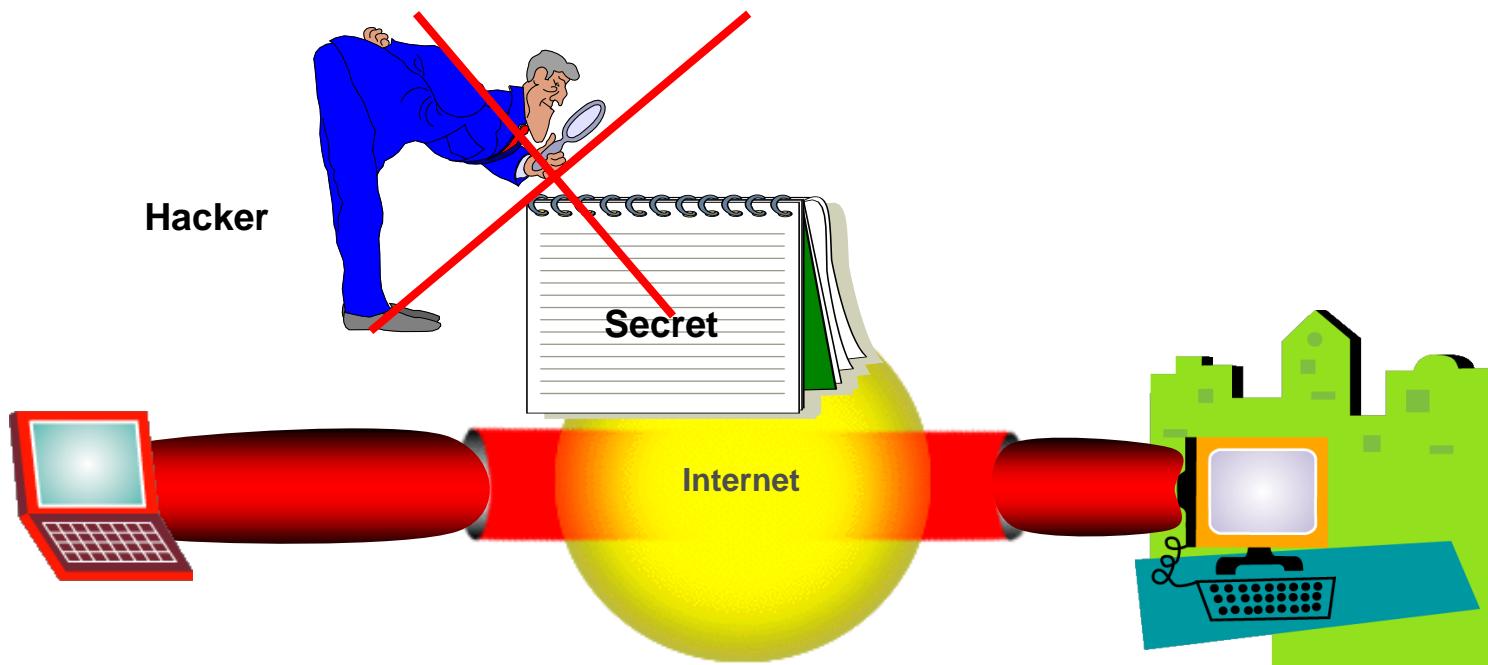
- In this section, we will look at:
 - the two main types of modern encryption techniques,
 - the services provided by encryption, and
 - some of the issues surrounding the use of cryptography.

Services Offered by Encryption

- Encryption is not only used to keep messages secret, but also offers the following services:
 - Privacy
 - Authentication
 - Integrity
 - Non-repudiation
- Remember Security is “**PAIN**”

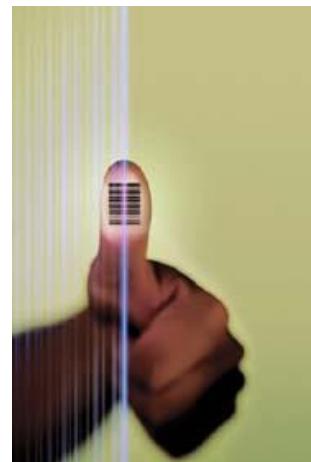
Privacy

- This service ensures only the sender and intended receiver can read the contents of the message.



Authentication

- Authentication allows the recipient of a message to confirm that the message was from a particular sender.
- Authentication allows the sender to confirm the message is going to the intended recipient.



Authentication

- Strong Authentication: Two factors Authentication
 - Something you know + something you hold
 - E.g. password + Token/ RFID Card/ SMS Phone

The screenshot shows the HSBC Internet Banking Logon page. At the top, there's a banner with a red background and white text. Below it, the HSBC logo and slogan "The world's local bank" are displayed. The main form is titled "INTERNET BANKING LOGON". It has sections for "Identity Authentication" and "Fraudulent Telephone Call". The "Fraudulent Telephone Call" section contains the following text:

- Never disclose your PIN to anyone, including bank staff or the police
- When reporting a lost card do not reveal your PIN

A red rectangular box highlights an "Important Message" box. Inside this box, the text "The random password is #5264" is displayed. Below the message box, there are fields for "Enter Password" and "Enter Security Code", along with a "LOGON" button. To the right of the code field, there's a "Security Code" device with a numeric keypad. A small note at the bottom explains what "BATT" means on the device.

The random
password is
#5264



Integrity

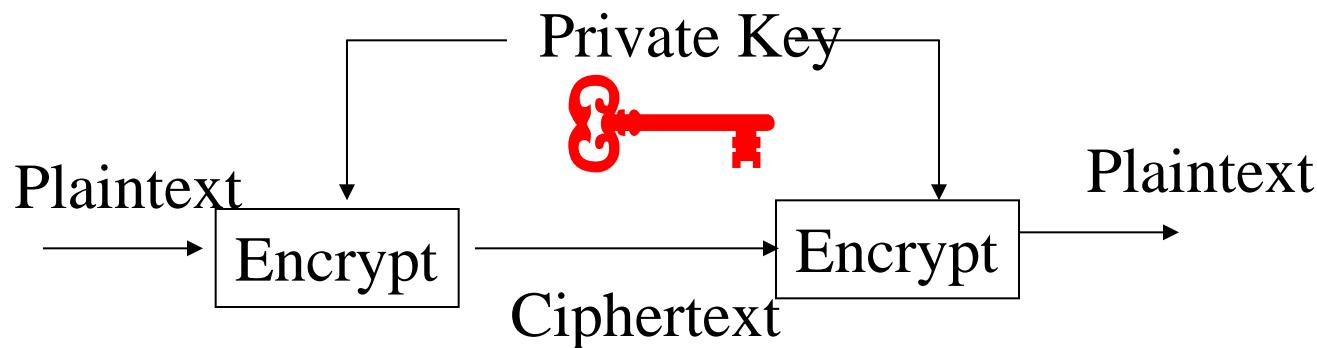
- This service ensures that a message cannot be altered (intentionally or accidentally) while being transferred between the sender and receiver.

Non-repudiation

- Non-repudiation
 - Ensures both parties involvement in a transaction cannot be later denied.
 - Is essential in electronic commerce transactions where legal disputes may occur should one party claim they never received an order or some other data.
 - Protects both sender and receiver.

Symmetric Key Encryption

- Symmetric Key encryption = **Private key encryption** = allows a user to enter a single key (or password) into an encryption algorithm.
- This algorithm will then encode the message.
- Benefits
 - Knowing the algorithm is not enough to decode the message, a key is also required.
 - Faster than asymmetric key encryption based systems.

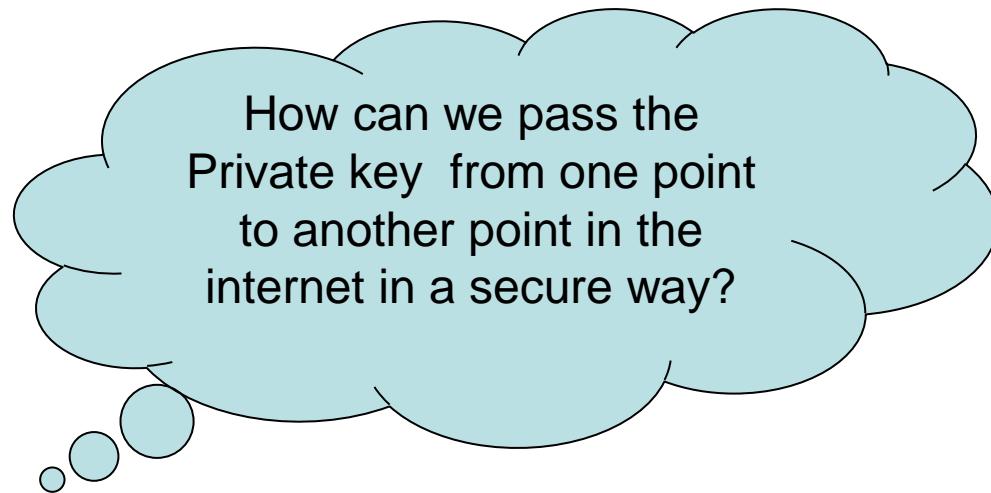


Example of how key encryption works can be referred to:

http://content.hccfl.edu/faculty/wayne_pollock/AUnixSec/PublicKeyDemo.htm

Symmetric Key Encryption

- Limitation:
 - Secret key encryption is the key itself must be securely distributed from the sender to the receiver.
(As the success of this system is based on keeping the key private)



How internet security works

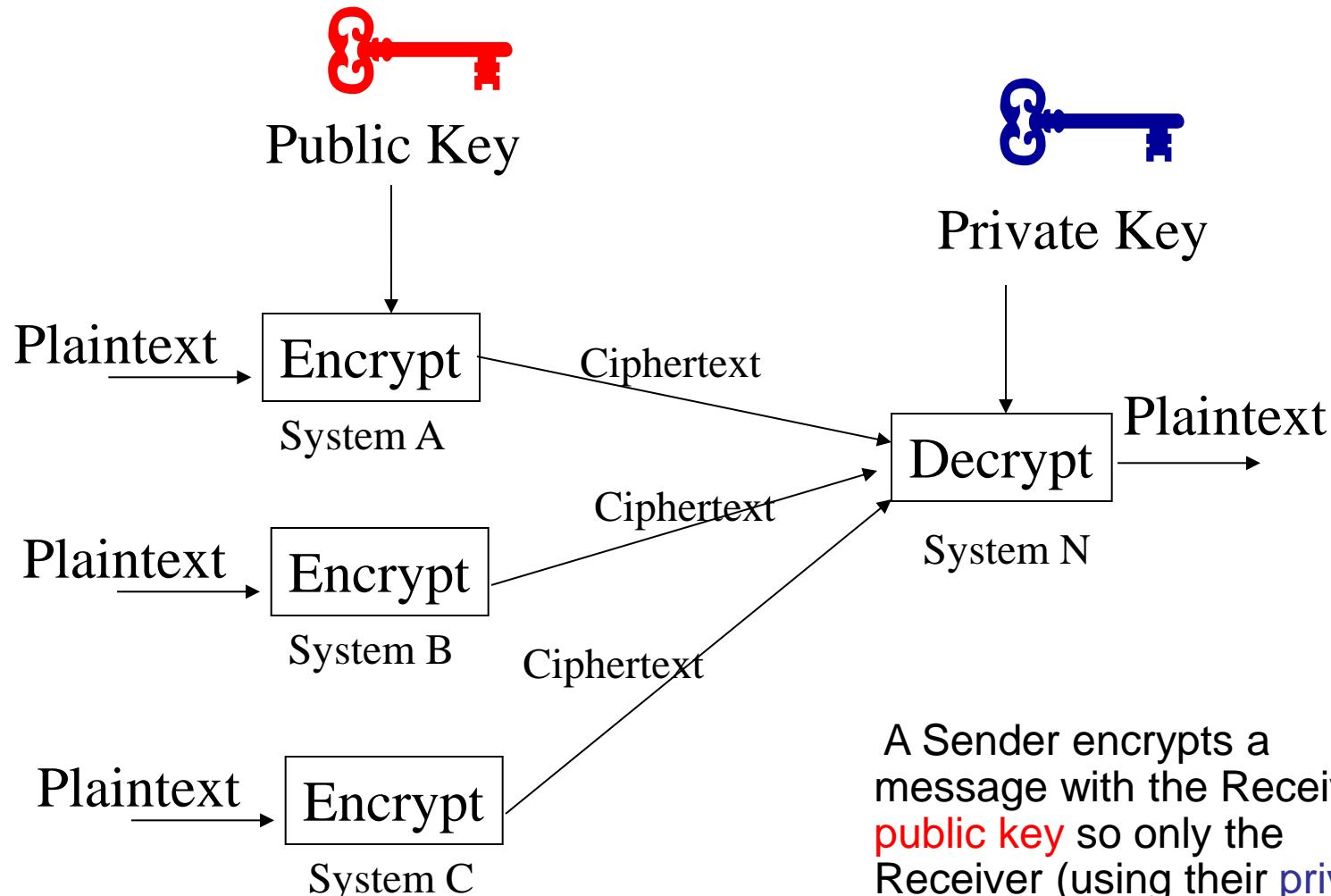
- http://www.youtube.com/watch?v=Ex_0bHVftDg



Asymmetric Key Encryption

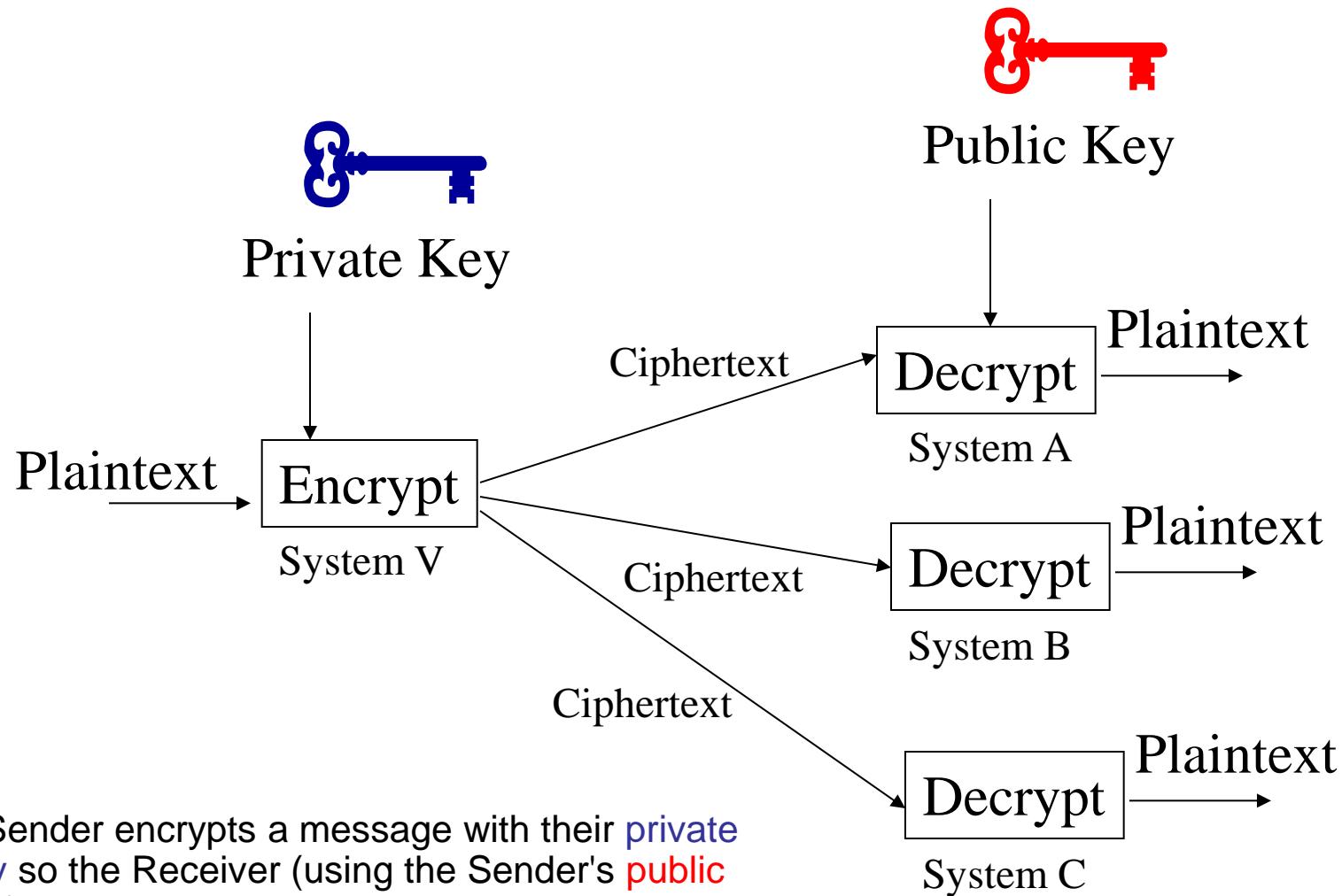
- Asymmetric Key Encryption = Public key encryption
- Asymmetric key encryption uses two keys
 - 1st key, the public key is freely available to anyone
 - 2nd key is private and is kept secret
- This technique is useful in two ways:
 - 1. A Sender encrypts a message with the Receiver's public key so only the Receiver (using their private key) can decrypt the message.
 - 2. A Sender encrypts a message with their private key so the Receiver (using the Sender's public key) can decrypt the message and therefore prove the message did indeed come from the Sender. This is the basis for digital signatures.

Encryption mode



A Sender encrypts a message with the Receiver's **public key** so only the Receiver (using their **private key**) can decrypt the message.

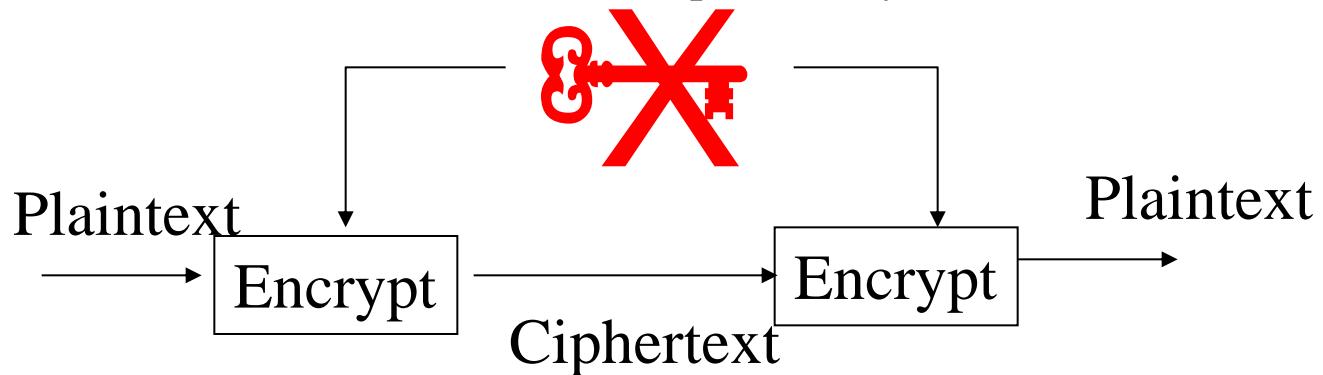
Authentication mode



A Sender encrypts a message with their **private key** so the Receiver (using the Sender's **public key**) can decrypt the message and therefore prove the message did indeed come from the Sender. This is the basis for digital signatures.

Asymmetric Key Encryption

- Advantages of Public Key encryption (over symmetric-key):
 - To send encrypted message to someone, you don't need to send a private key with it, and
 - Non-repudiation can be supported.
 - Symmetric-key encryption cannot provide non-repudiation, as both the sender and receiver know the same private key.

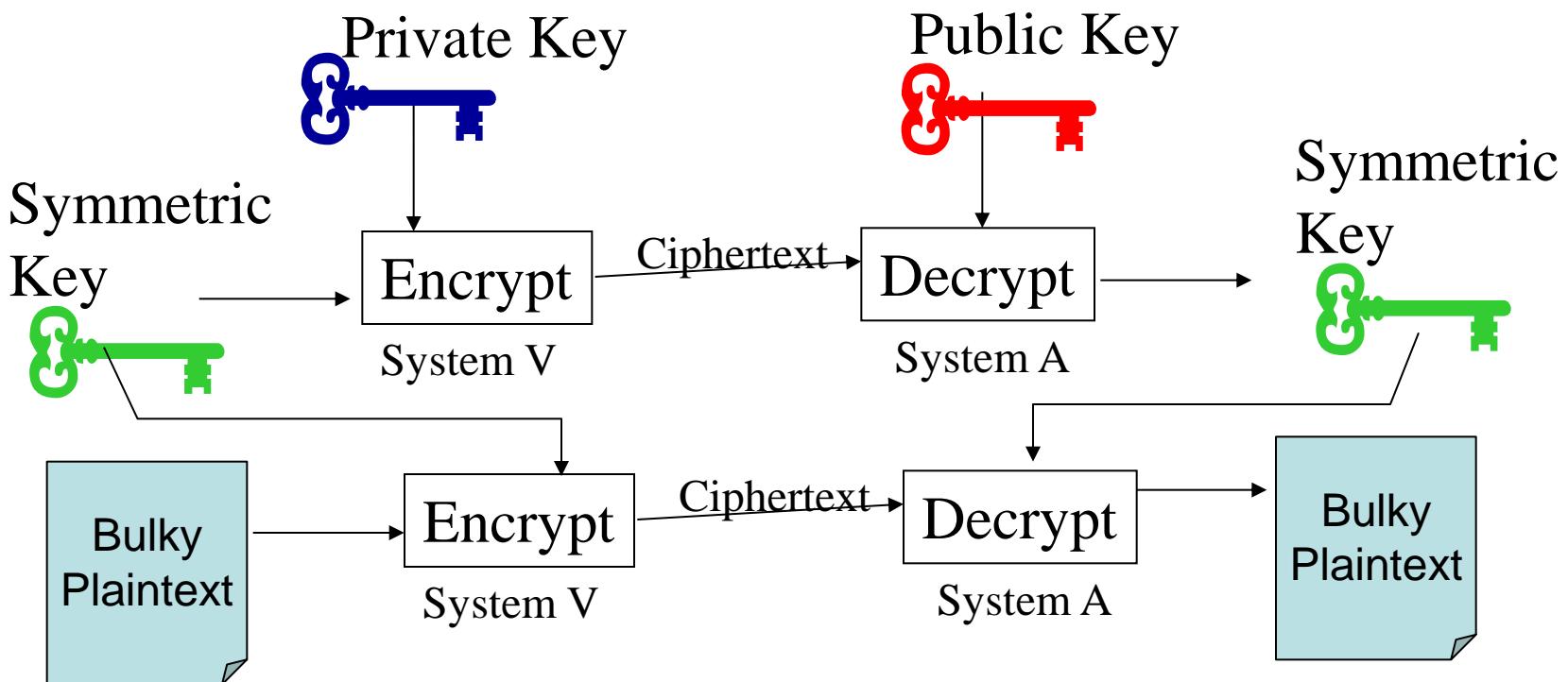


- Limitation in asymmetric key encryption:
 - As mathematics involved, as processing large amounts of information will be slower than a symmetric-key alternative.



Asymmetric Key Encryption

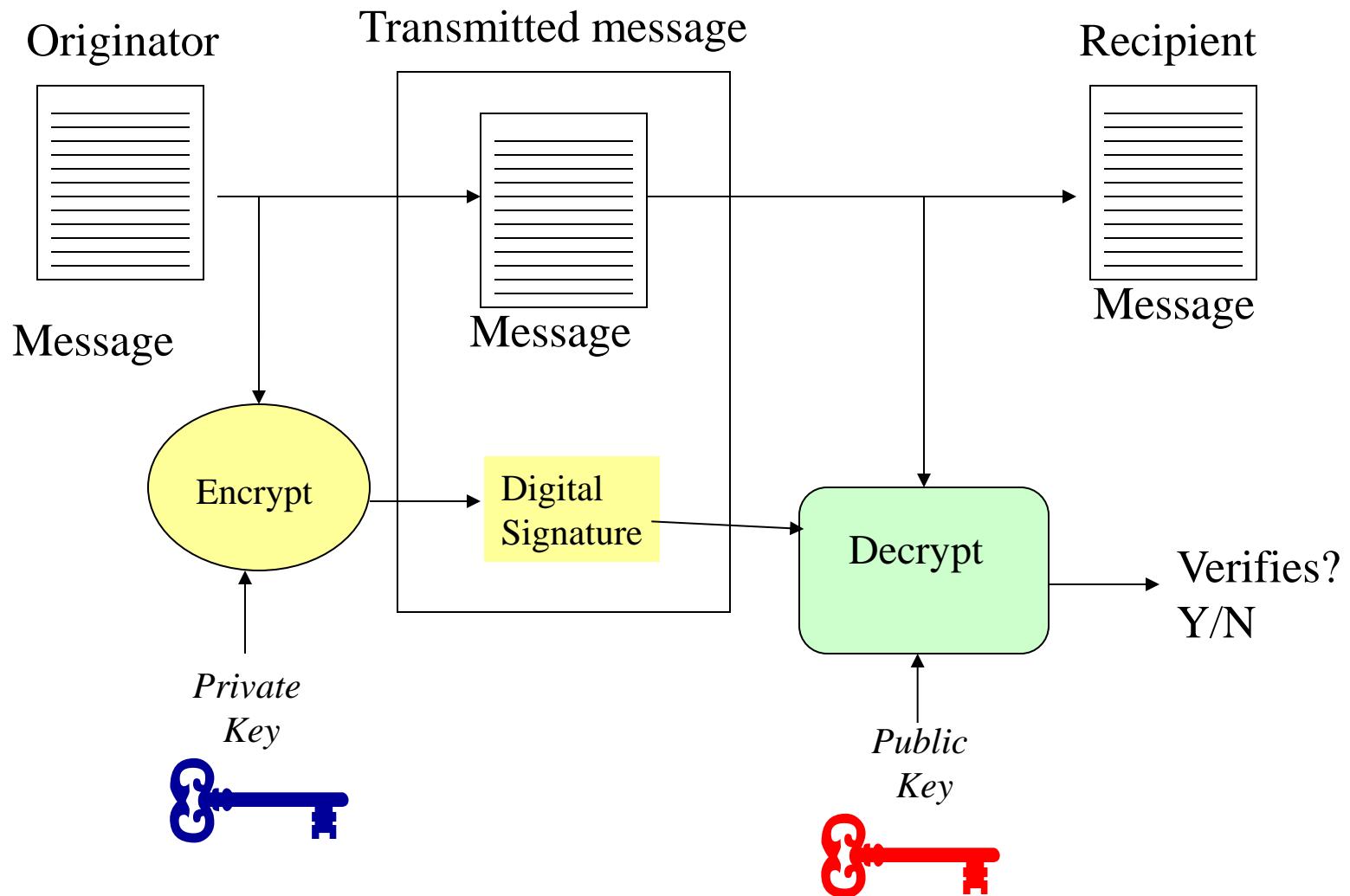
- Solution:
 - Asymmetric-key encryption can be used to distribute symmetric session keys between the sender and receiver.
 - A Combination technique means a performance gain will be made as:
 - Bulk of the information will be encrypted by faster symmetric key techniques and
 - Distribution problems of secret key encryption are resolved using asymmetric key techniques.



Digital Signatures

- Deploy Digital Signature by using asymmetric encryption.
- “Digital signature”
 - A method to provide one’s identity in an electronic manner.
 - Being created encrypting a small document file (known as a hash) with an owner’s private key.
- Private Key
 - Only the signature’s owner knows the private key, nobody else can reproduce the signature.
- Public Key
 - It can be checked by applying the owner’s public key (which is available to everyone) to the signature.

Digital Signatures

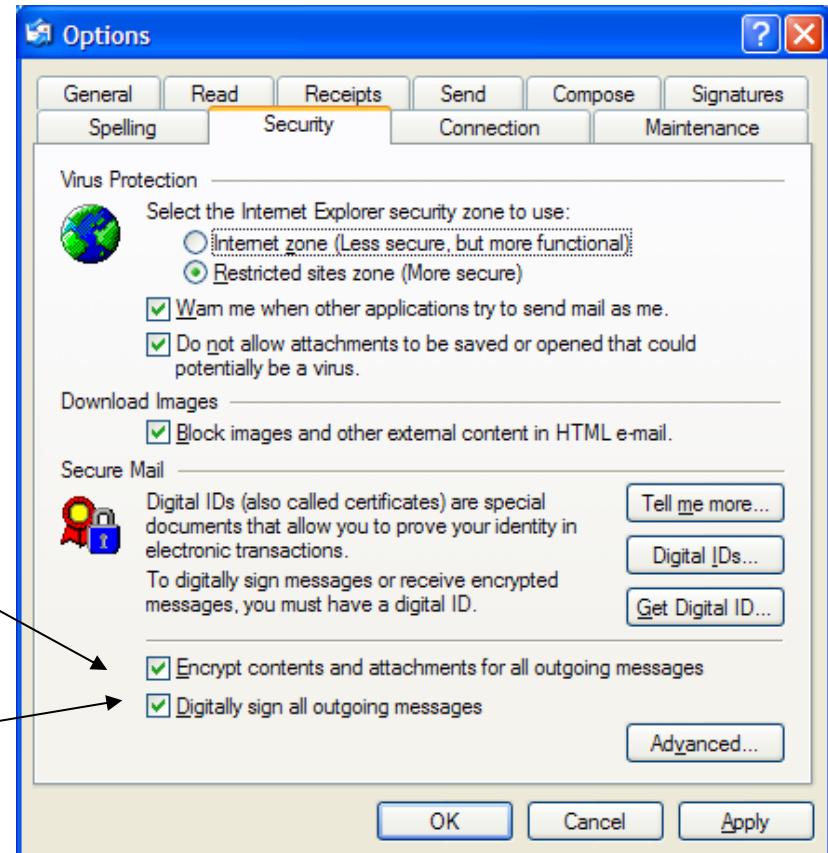


Digital Signatures

- Using digital signature in E-mail: Tool > Option > Security

– You can “Encrypt” and “Sign” your mail using outlook:

- Encrypt contents and attachment for outgoing message
- Digitally sign all outgoing message



Digital Signatures

- Authentication
 - is a service which ensures that a message cannot be altered (intentionally or accidentally) while being transferred between the sender and receiver.
 - can be achieved using secret or public key encryption by encrypting the entire message.
- As the key is only known to the intended recipient
 - If the message decode successfully
 - → then the message can be considered authenticated or free from modification.

Hash functions

- But how about large file? How can we reduce the encryption and decryption time?
- Solution: Using Hash function
 - Hash functions can also be used to prove file integrity. Hash functions are a one-way process, taking a large variable-length file and creating a small fixed length file of 128 to 160 bits.
 - This small file is called a hash or message digest and is used as a surrogate for the large file as two files will have the same message digest.
 - Useful when creating digital signatures.

Hash functions

- Example of Hash Function: E.g.1
 - The Check digit of the HKID Card
 - A123456(9),P131609 (9)



- <http://www.kgv.net/ict-ks4/TheoryTerm2/HKCheckDigit.htm>

Hash functions

- Example of Hash Function: E.g.2
 - Some Finger Print reader decode a fingerprint with a hash function, rather than the true image of the fingerprint



Full high-res image
Can be over 1 M Bytes



Hashed function
Only a few ten K Byte

Hash function calculator

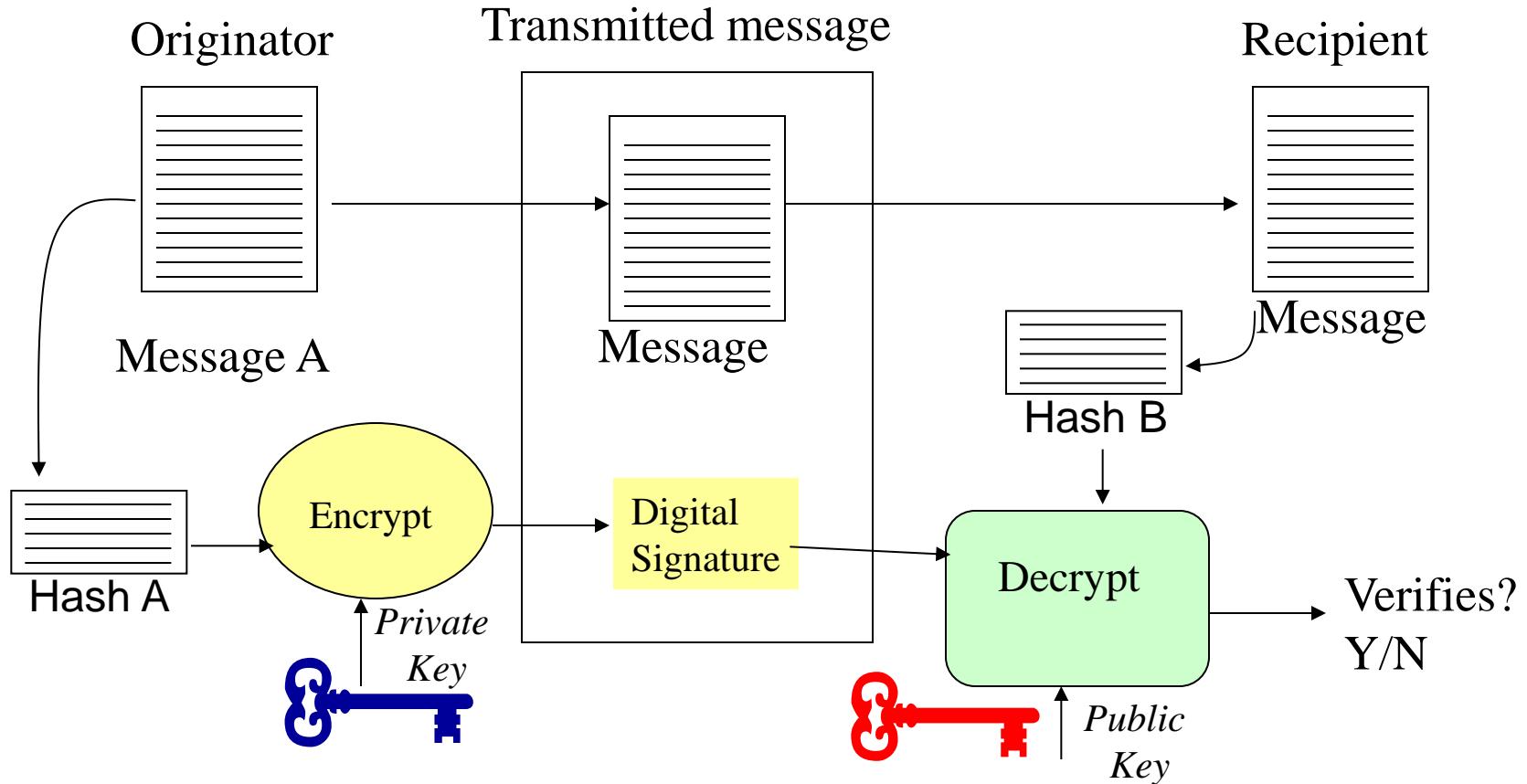
- <http://hash-functions.online-domain-tools.com/>

The screenshot shows a web browser window titled "Hash Functions - Calculate". The address bar displays the URL "hash-functions.online-domain-tools.com". The main content area is titled "Hash Functions Online". It features a "Input type:" dropdown set to "Text", an "Input text:" text area containing a block of text about combining encryption mechanisms, and a "Hash functions:" dropdown menu listing MD4, MD5, NTLM, SHA1 (which is selected), SHA256, and SHA384. Below these controls are two buttons: a green "Hash!" button and a blue "Copy" button with a link icon. At the bottom, there's a "Checkout ?" section with a table showing a basic price of 0.05 and a total of \$0.05.

Item Description	Item Price	Your Price
Basic price	0.05	0.05
Total:	\$0.05	

Hash functions

- The use of Hashing to prove file integrity can be seen in the following scenario:
 1. The Sender creates a hash of Message A called Hash A.
 2. The Sender sends both Hash A and Message A.
 3. The recipient re-calculates the hash using the same hash function called Hash B
 4. The recipient compares Hash B with Hash A



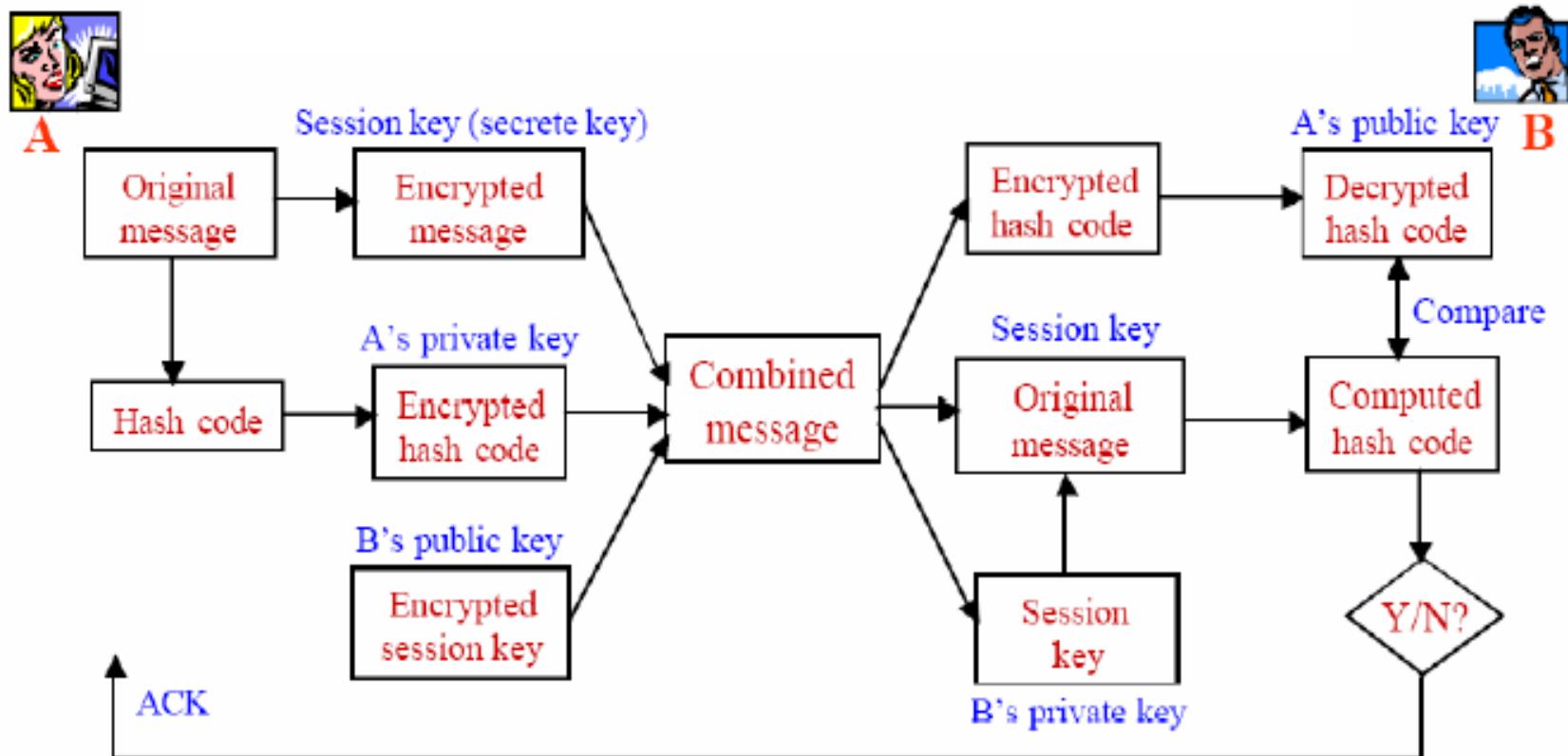
Hash functions

- If the Hashes are the same then the message has not been modified.
- To increase security hashing is used in conjunction with public key encryption.

Applications of digital keys for security

- Combining all – Privacy, Authentication, Integrity and Non-reputation
 - Both public key and private key encryption mechanisms have drawbacks, they do not replace each other, rather they complement each other.
 - In real communication cases, people have invented ways to combine the two encryption mechanisms together to achieve both good security services and efficiency.
 - It uses public key encryption to distribute the secret key and use the secret key to encrypt the lengthy messages.

Applications of digital keys for security



Summary

- In this session, we introduced the risks to data when traveling through the network.
- Encryption offers a method of protecting the data while in transit (and storage).
- We also looked at the other services made available through the use of encryption, such as:
 - Privacy
 - Authentication,
 - Integrity, and
 - Non-repudiation.

ELEC2544 Electronic Commerce and FinTech

Enabling Technologies: Accelerometer

Dr. Wilton Fok

Enabling Technologies: Accelerometer

- An **accelerometer** is a device that measures proper acceleration, the acceleration experienced relative to freefall.
- Single- and multi-axis models are available to detect magnitude and direction of the acceleration as a vector quantity, and can be used to sense
 - orientation,
 - acceleration,
 - vibration shock, and
 - Falling

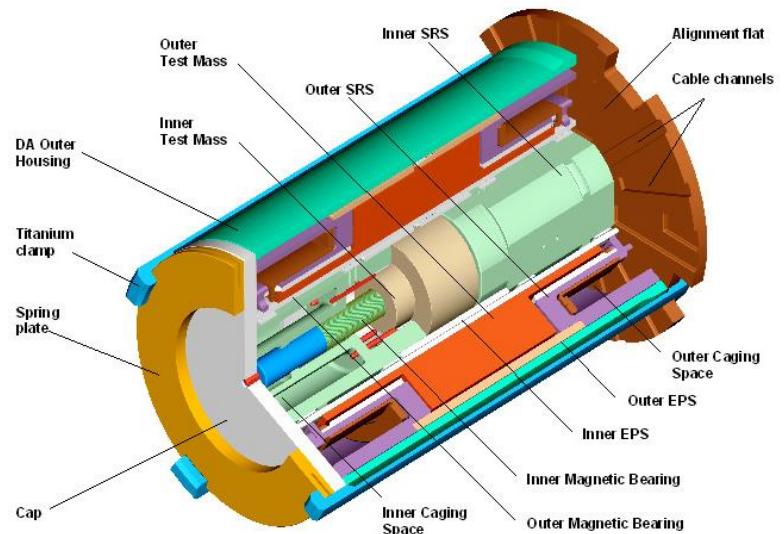
Accelerometer

- Micro machined accelerometers are increasingly present in portable electronic devices and video game controllers, to detect the position of the device or provide for game input.



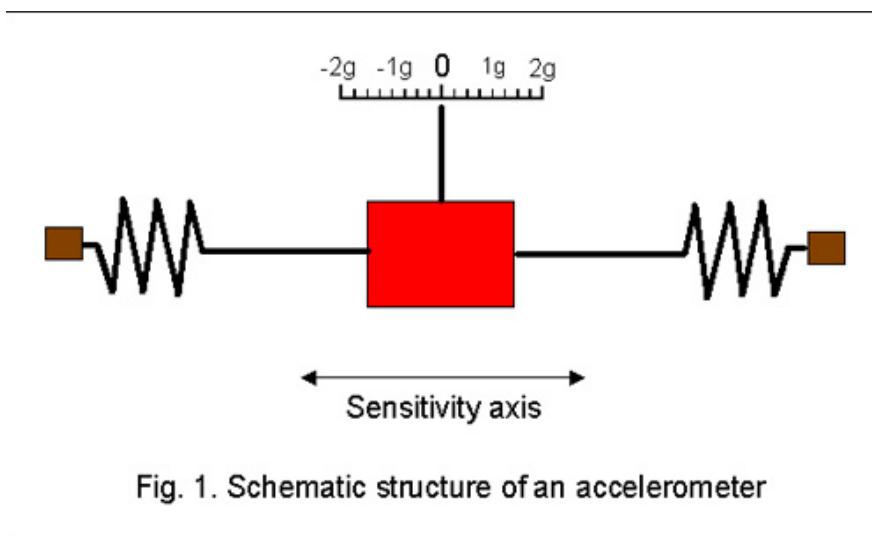
Physical principles

- An accelerometer measures acceleration
 - the acceleration it experiences relative to freefall
 - measured in terms of g-force.
- An accelerometer at rest relative to the Earth's surface will indicate approximately 1 g *upwards*, because any point on the Earth's surface is accelerating upwards relative to the local inertial frame
- To obtain the acceleration due to motion with respect to the Earth, this "gravity offset" must be subtracted.



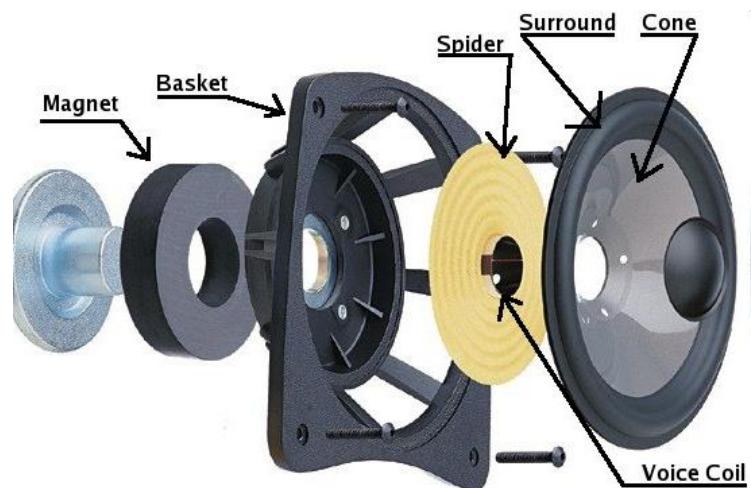
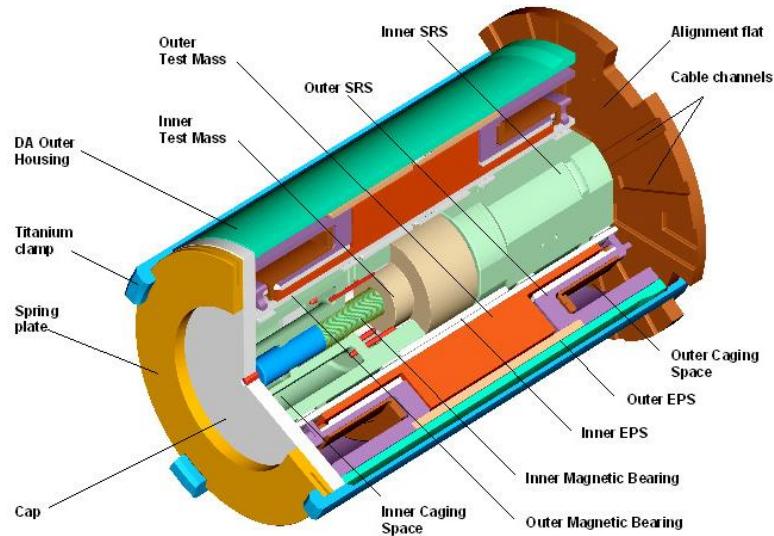
Structure

- Accelerometer behaves as a damped mass on a spring.
- When it experiences an acceleration, the mass is displaced to the point that the spring is able to accelerate the mass at the same rate as the casing.
- The displacement is then measured to give the acceleration.



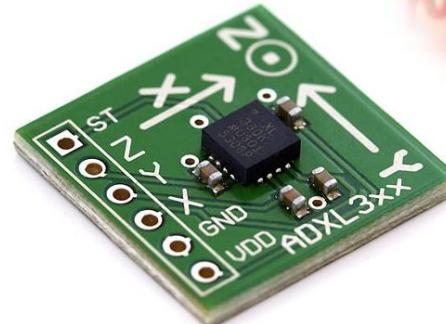
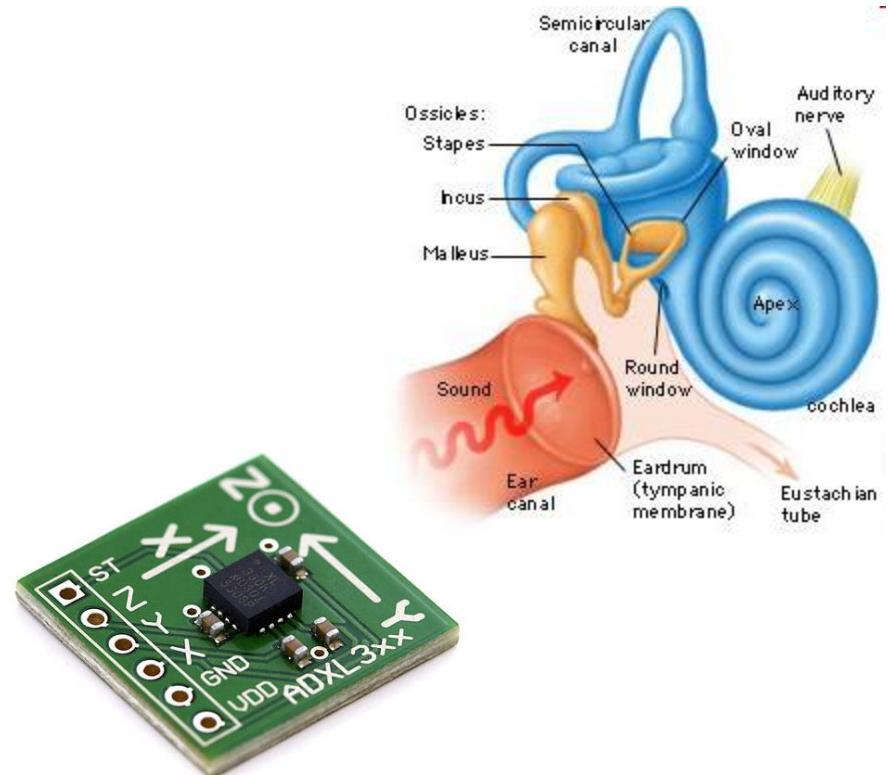
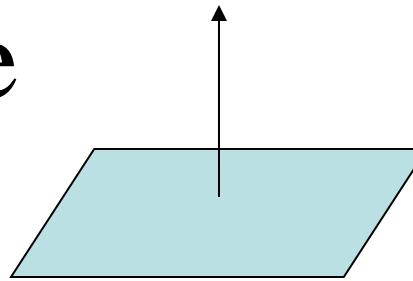
Structure

- Modern accelerometers are often small *micro electro-mechanical systems*
- It consists of a small beam with a proof mass
- Damping results from the residual gas sealed in the device
- Under the influence of external accelerations the proof mass deflects from its neutral position.
- This deflection is measured in an analog or digital manner.
- The capacitance between a set of fixed beams and a set of beams attached to the proof mass is measured.



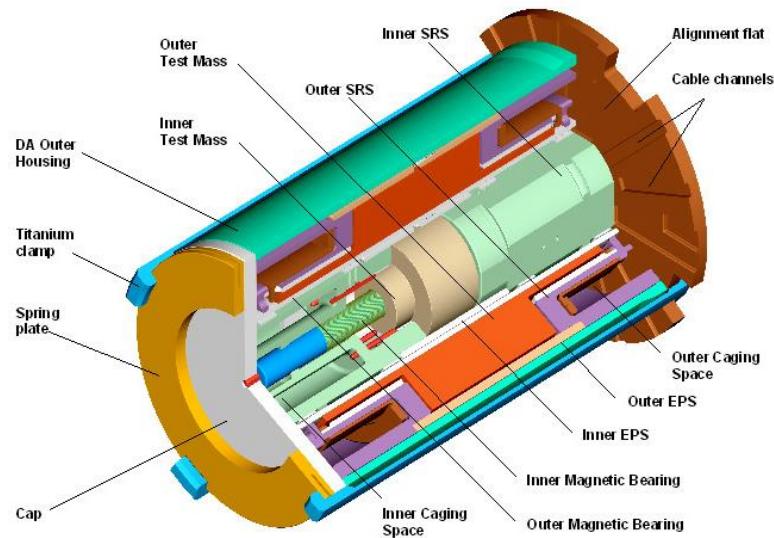
Structure

- Most micromechanical accelerometers operate *in-plane*
 - sensitive only to a direction in the plane of the die.
- By integrating two devices perpendicularly on a single die a two-axis accelerometer can be made.
- By adding an additional *out-of-plane* device three axes can be measured.
- Such a combination always has a much lower misalignment error than 3 discrete models combined after packaging.



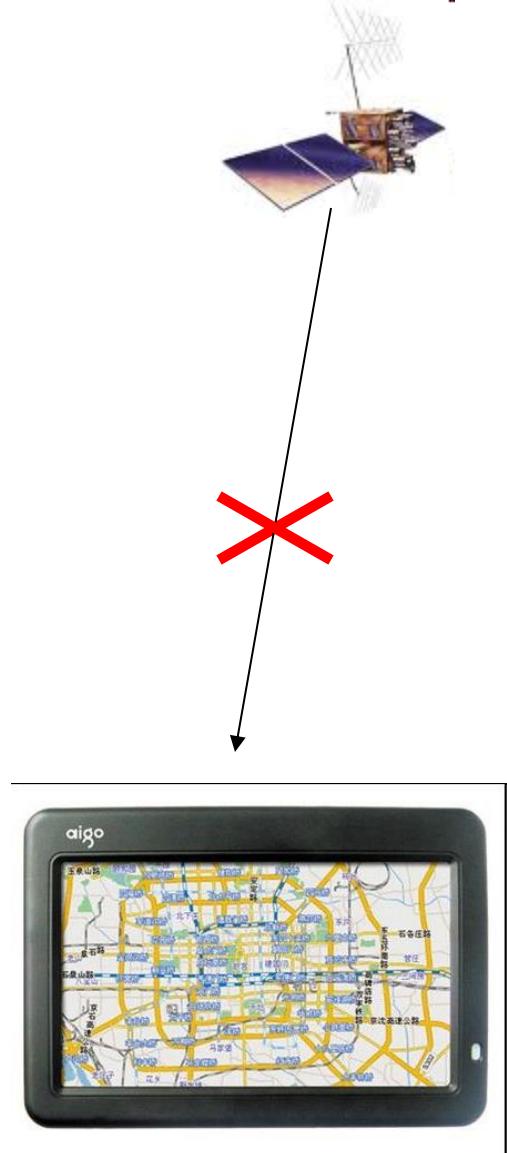
Class Discussions

- What are the possible m-commerce applications enabled by accelerometer



Navigation

- An **Inertial Navigation System** (INS) is a navigation aid that uses a computer and motion sensors (accelerometers) to continuously calculate via
 - dead reckoning the position,
 - orientation, and
 - velocity (direction and speed of movement)
 - of a moving object without the need for external references (e.g. GPS and location base)



Orientation sensing

- A number of modern notebook computers feature accelerometers to automatically align the screen depending on the direction the device is held,
 - i.e. switching between portrait and landscape modes.
- This feature is relevant in Tablet PCs and some smart phones and digital cameras



Car Safety

- Smartphones can download an Automatic Collision Notification (ACN) app such as
 - E.g. [My-911](#),
 - [Onstar AACN service](#),
 - [Ford Link's 911 Assist](#),
 - [Toyota's Safety Connect](#),
 - [Lexus Link](#), or
 - [BMW Assist](#).
- The phone's accelerometer detects crash-strength G-forces and automatically calls for assistance unless manually cancelled.



<http://www.youtube.com/watch?v=KOwAPj3YiPw>

Motion input

- Nintendo's Wii video game console uses a controller called a Wii Remote that contains a three-axis accelerometer and was designed primarily for motion input.



Image stabilization

- Camcorders use accelerometers for image stabilization.
- Still cameras use accelerometers for anti-blur capturing.
- The camera holds off snapping the CCD "shutter" when the camera is moving.
- When the camera is still, even only for a millisecond, the CCD is "snapped".
 - E.g. Nokia N96
- Some digital cameras, contain accelerometers to determine the orientation of the photo being taken and also for rotating the current picture when viewing.



Device integrity

- Some laptops and mobile devices feature an accelerometer for damage protection
 - E.g.
 - Lenovo's (formerly IBM's) Active Protection System,
 - Apple's Sudden Motion Sensor
 - HP's 3D DriveGuard,
 - If a drop is detected, the heads of the hard disk are parked to avoid data loss and possible head or disk damage by the ensuing shock.



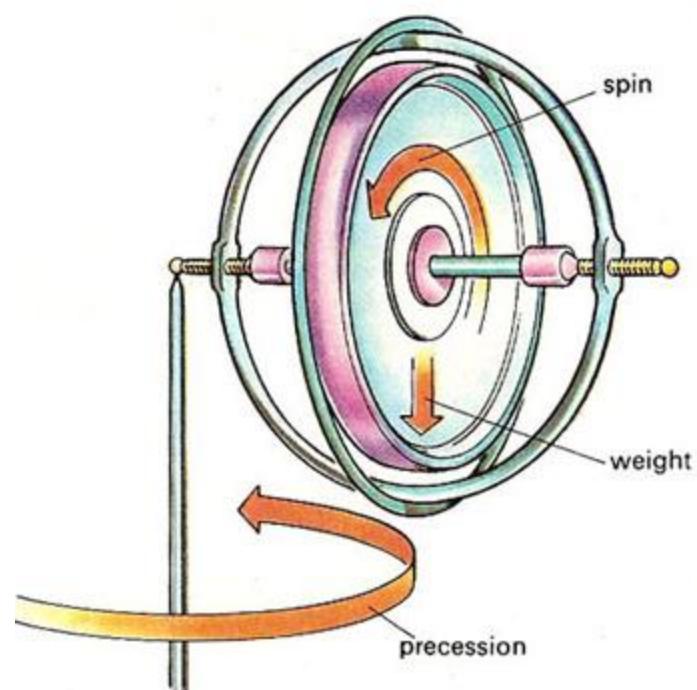
Limitations of Accelerometer

- Limitations
 - Cannot detect the difference between sitting in a rocket on the launch pad, and being in the same rocket in deep space while it uses its engines to accelerate at 1 g
 - Cannot read during free falling

What is this?

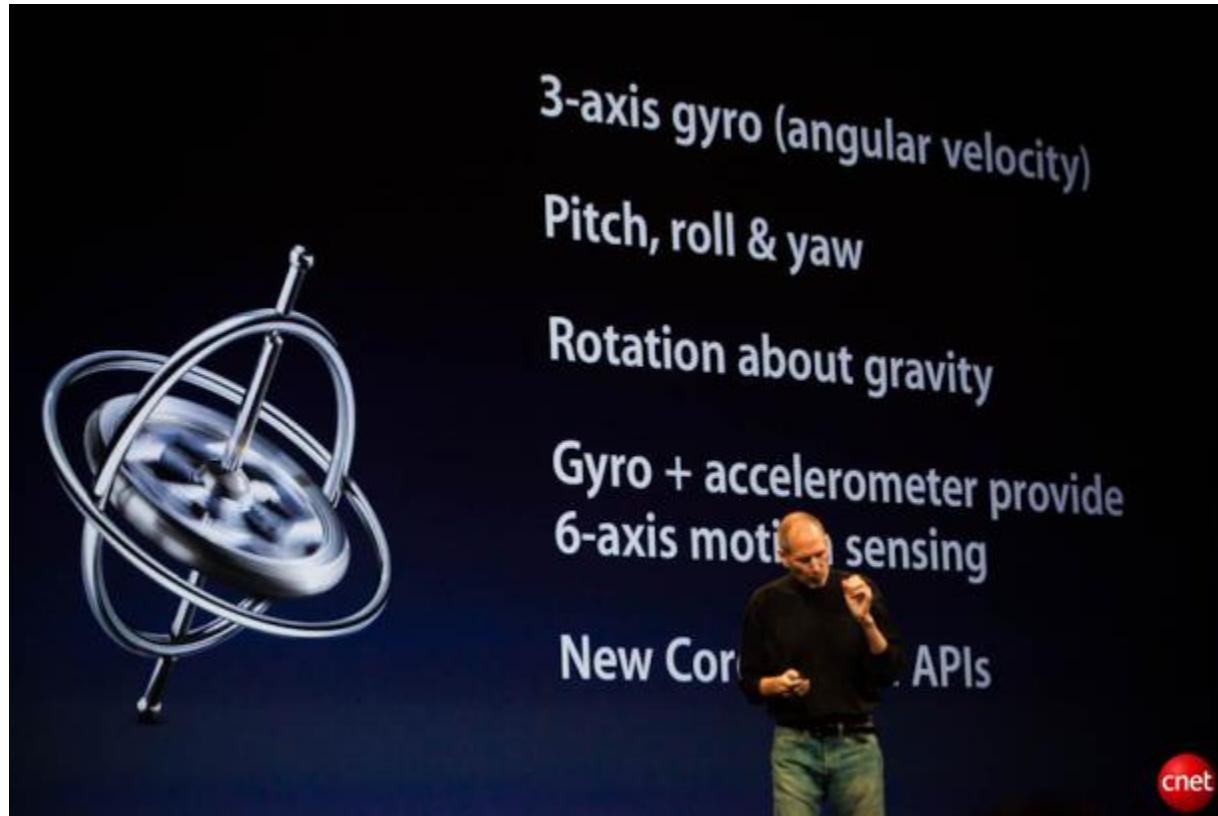


Gyroscope



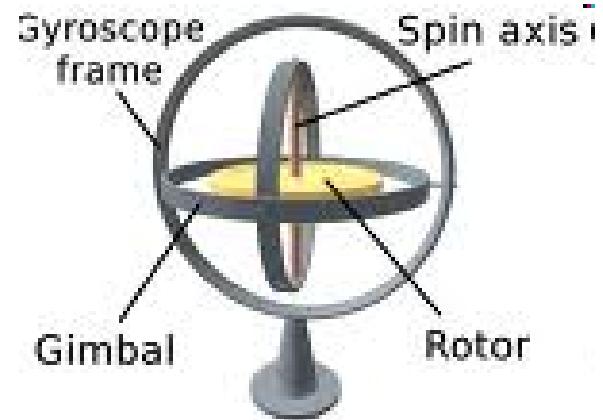
A new enabling technology: Gyroscope

- http://www.youtube.com/watch?v=Nfy_ZIevtvw



Gyroscope

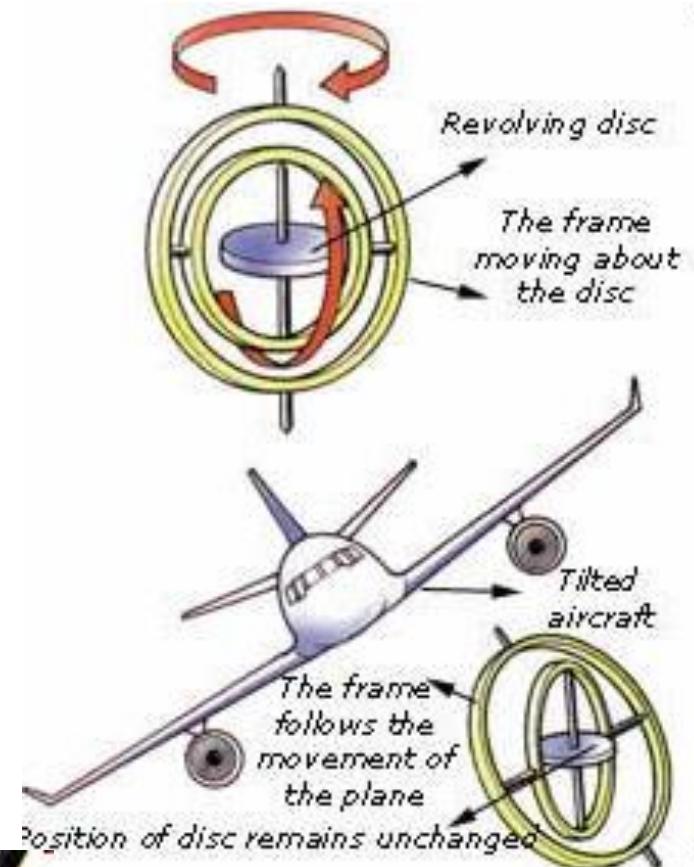
- A gyroscope is a device for measuring or maintaining orientation, based on the principles of conservation of angular momentum.
- There is a spinning wheel or disk whose axle is free to take any orientation.
- This orientation changes much less in response to a given external torque than it would without the large angular momentum associated with the gyroscope's high rate of spin.
- Since external torque is minimized by mounting the device in gimbals, its orientation remains nearly fixed, regardless of any motion of the platform on which it is mounted.



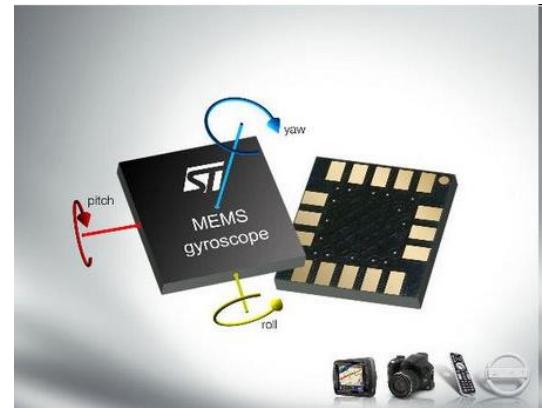
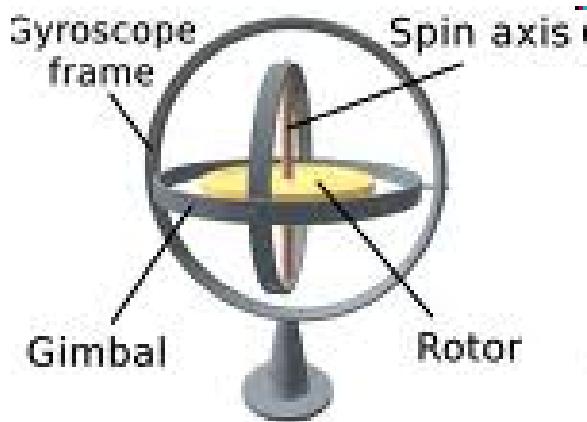
<http://en.wikipedia.org/wiki/Gyroscope>

Gyroscope

- Applications
 - navigation (INS) when magnetic compasses do not work (as in the Hubble telescope)
 - for the stabilization of flying vehicles like radio-controlled helicopters or UAVs.
 - higher precision applications e.g. maintain direction in tunnel mining
 - Golf club stabilizer

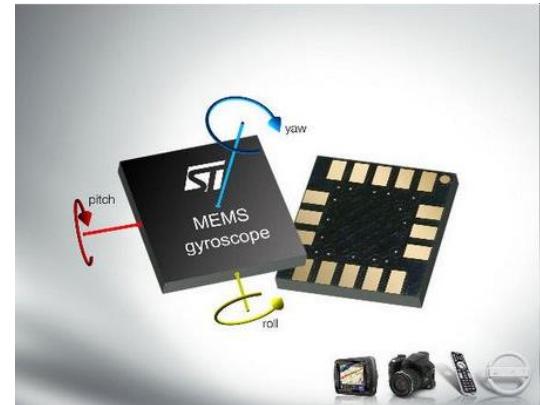


Digital gyroscope



Digital gyroscope market forecast

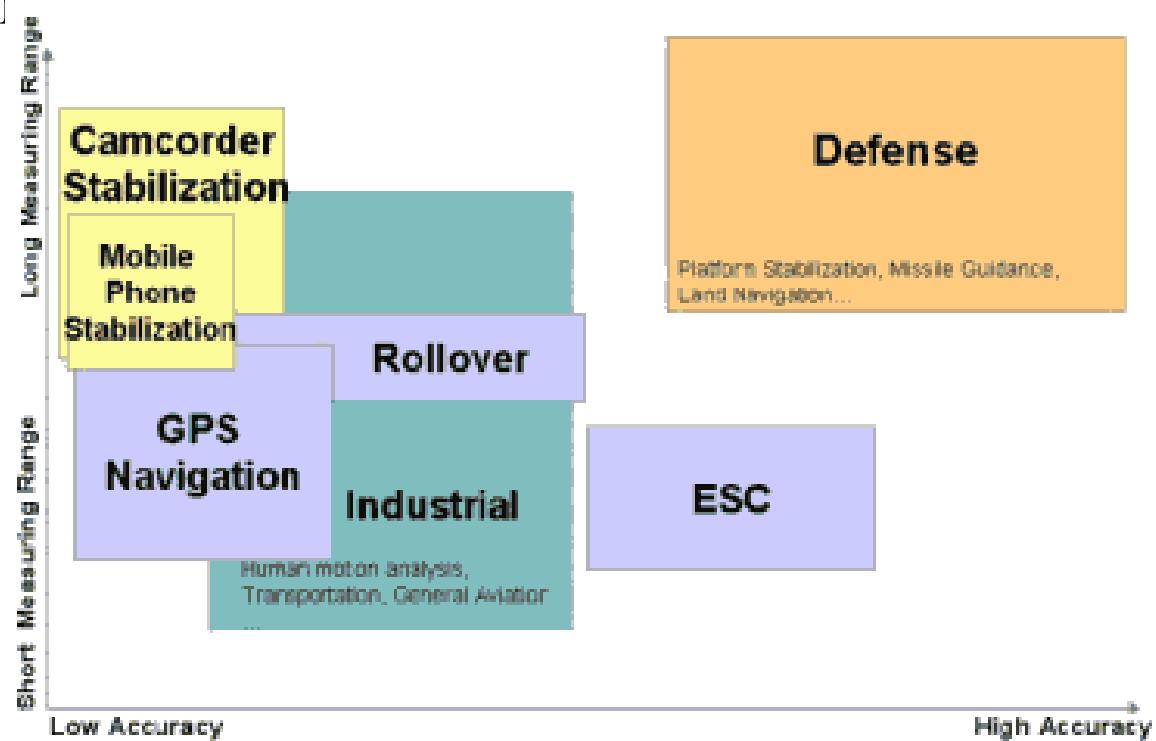
- Digital gyroscope industry plans a high growth potential of the defence and low end automotive applications.
- The Digital gyroscope market is expected to generate in the range of 800M\$ value in 2010.



Digital Gyroscope Market is Expected to Reach 800M\$ in 2010

Digital gyroscope market forecast

- **3 fields with high growth potential**
 - **Automotive** applications -highest new entrant rate
 - **Defence & aeronautics** applications - stable business
 - **Mobile/Consumer** applications- booming markets thanks to sensor introduction

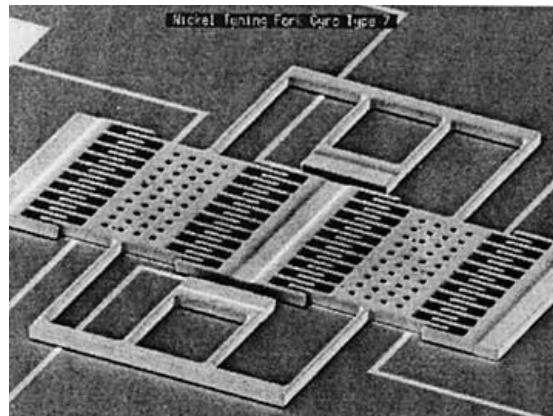
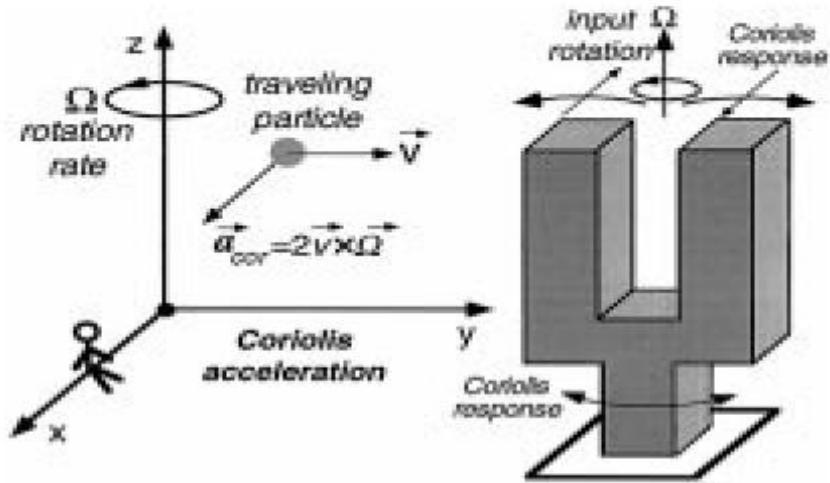


Principles of Digital gyroscope

- Draper Tuning Fork Gyro
- Piezoelectric Gyroscopes

Draper Tuning Fork Gyro

- The rotation of tines causes the Coriolis Force
- Forces detected through either electrostatic, electromagnetic or piezoelectric.
- Displacements are measured in the Comb drive



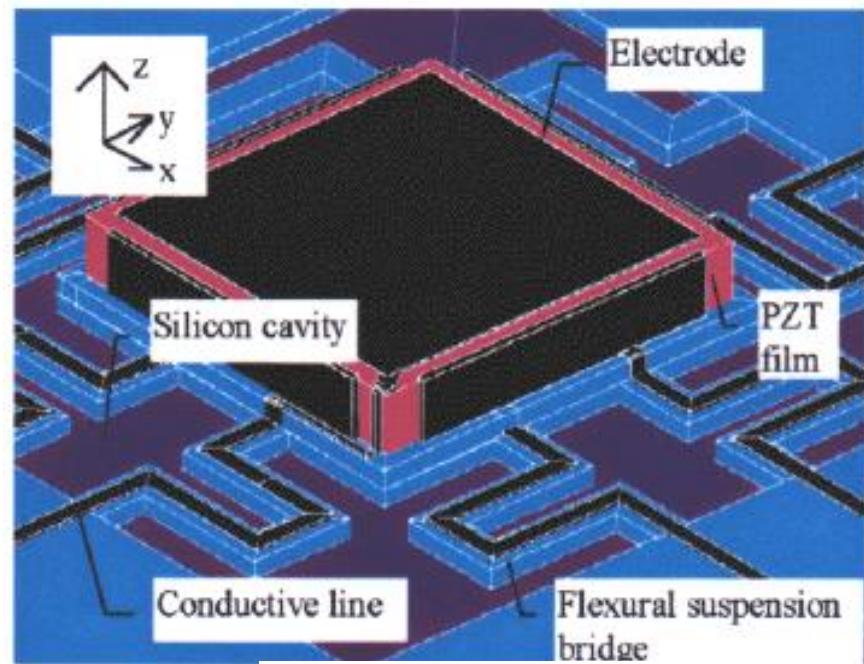
Source: <http://clifton.mech.northwestern.edu>

Performance Advantages

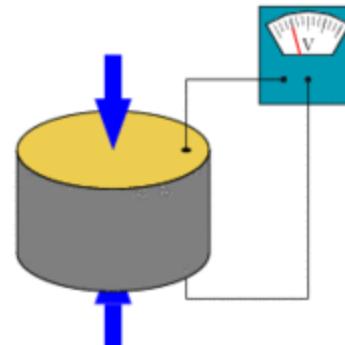
- No change in performance due to temperature
- Lower voltage noise
 - Stronger signal to noise ratio
 - Better communication with external devices
 - Higher sensitivity

Piezoelectric Gyroscopes

- Basic Principles
 - Piezoelectric plate with vibrating thickness
 - Coriolis effect causes a voltage form the material
 - Very simple design and geometry



A piezoelectric disk generates a voltage when deformed (change in shape is greatly exaggerated)



Piezoelectric Gyroscope

- Advantages
 - Lower input voltage than vibrating mass
 - Measures rotation in two directions with a single device
 - Adjusting orientation electronically is possible
- Disadvantages
 - Less sensitive
 - Output is large when $\Omega = 0$

Reference

- http://www.sensorsportal.com/HTML/DIGEST/may_06/MEMS_Gyroscope_market.htm
- <http://clifton.mech.northwestern.edu/~me381/project/done/Gyroscope.ppt>

ELEC2544

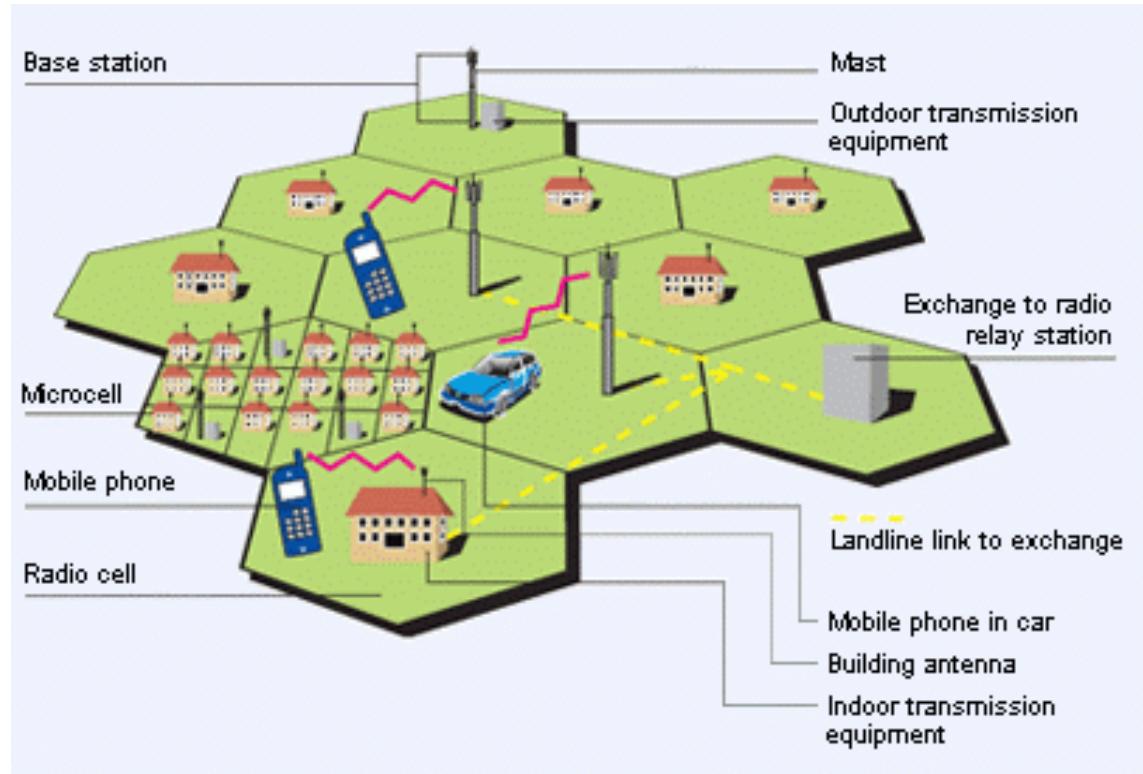
e-Commerce and FinTech

Location Base Service

Dr. Wilton Fok

Enabling Technology: Location Base Service

- Cellular radio network is the foundation for location base services
- GSM is a cellular network
 - → mobile phones connect to it by searching for cells in the immediate vicinity.



GSM

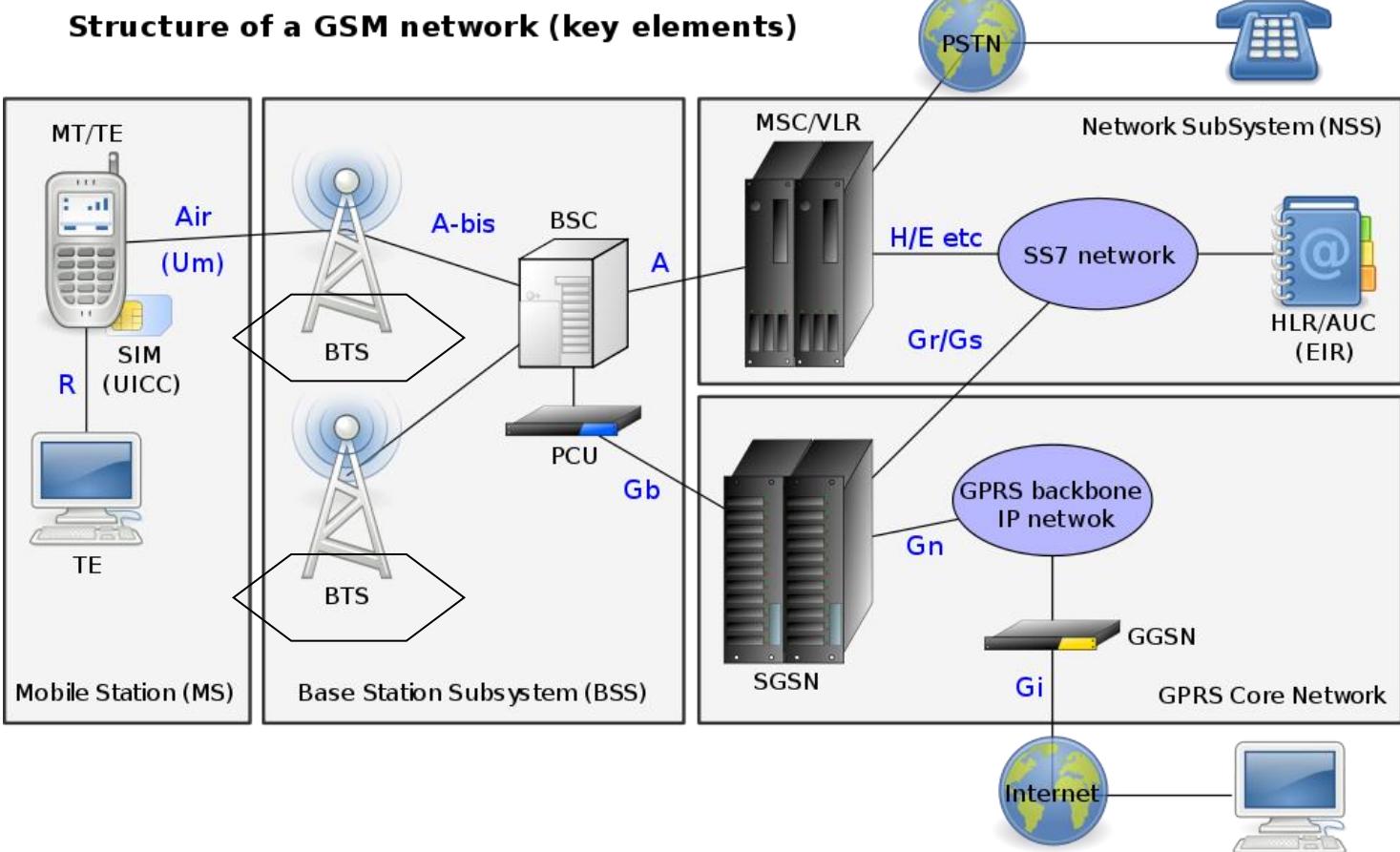
- **GSM (Global System for Mobile Communications)** is/was the most popular standard for mobile telephony systems in the world.
- GSM is considered a 2G mobile phone system.
- It facilitates the wide-spread implementation of data communication applications into the system.
- Advantages
 - Roaming
 - Switch carriers without replacing phones
 - Support SMS
 - Support SIM Card
 - Support a worldwide emergency telephone number feature 112

Network structure

- The structure of a GSM network:
 - Base Station Subsystem
 - base stations and their controllers
 - Network and Switching Subsystem
 - part of the network most similar to a fixed network). This is sometimes also just called the core network.
 - GPRS Core Network
 - the optional part which allows packet based Internet connections
 - Operations support system (OSS)
 - for maintenance of the network.

Network structure

- Base Station Subsystem
- Network and Switching Subsystem
- GPRS Core Network
- Operations support system (OSS)



Cell sizes and coverage

- There are 5 different cell sizes in a GSM network
 - Macro,
 - Micro,
 - Pico,
 - Femto and
 - Umbrella cells.

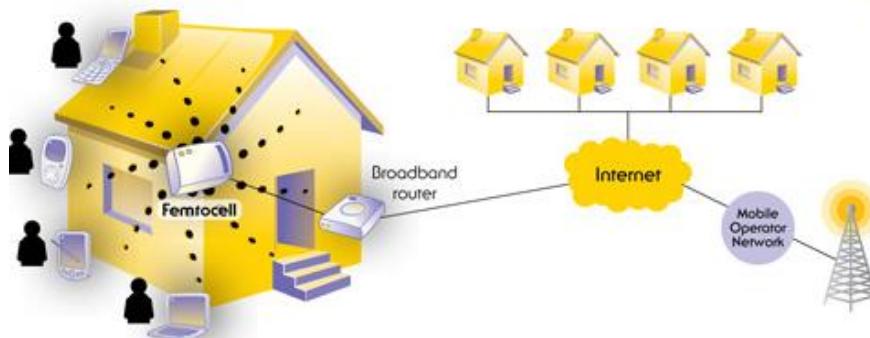
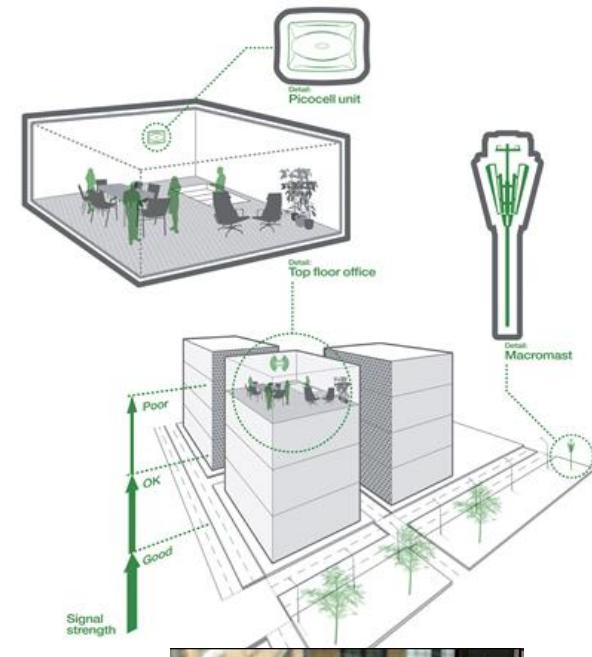
Cell sizes and coverage

- The coverage area of each cell varies according to the implementation environment.
 - Macro cells
 - Cells where the base station antenna is installed on a mast or a building above average roof top level.
 - Micro cells
 - Those antenna height is under average roof top level; they are typically used in urban areas.



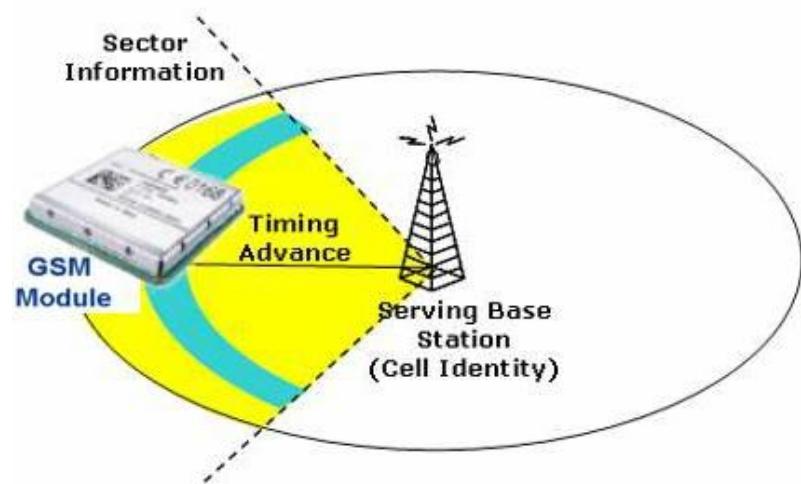
Cell sizes and coverage

- Picocells
 - Small cells whose coverage diameter is a few dozen metres; they are mainly used indoors.
- Femtocells
 - Cells designed for use in residential or small business environments and connect to the service provider's network via a broadband internet connection.
- Umbrella cells
 - Used to cover shadowed regions of smaller cells and fill in gaps in coverage between those cells.



Cell sizes and coverage

- Cell horizontal radius varies depending on:
 - antenna height,
 - antenna gain
- propagation conditions from a 300m -35km



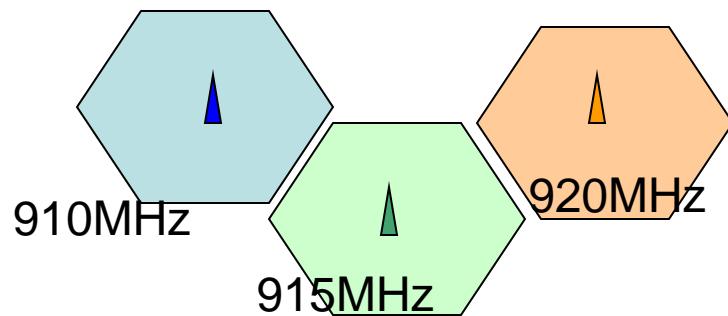
Cell sizes and coverage

- Indoor coverage is also supported by
 - indoor picocell base station, or
 - an indoor repeater with distributed indoor antennas fed through power splitters,
 - to deliver the radio signals from an antenna outdoors to the separate indoor distributed antenna system.
 - E.g. In shopping centers or airports.

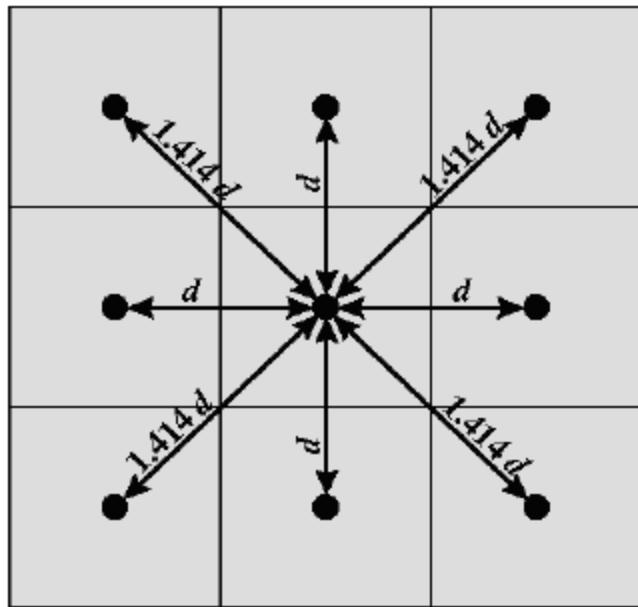


Cellular Network

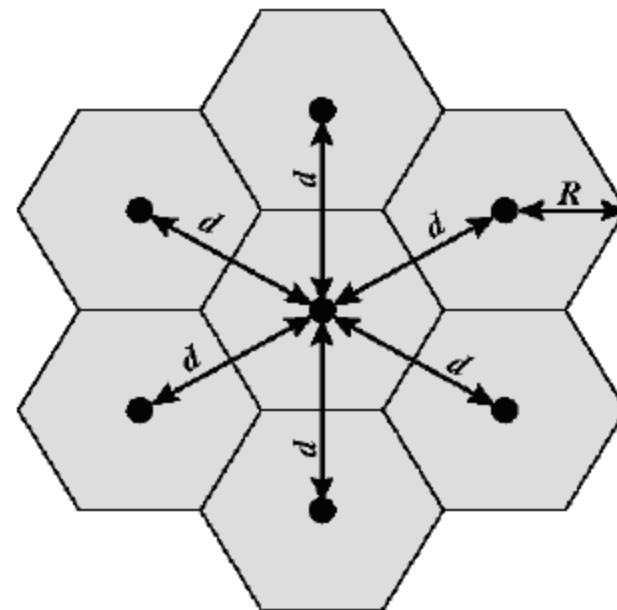
- Use multiple low-power transmitters (100 W or less)
- Areas divided into cells
 - Each served by its own antenna
 - Served by base station consisting of transmitter, receiver, and control unit
 - Band of frequencies allocated
 - Cells set up such that antennas of all neighbors are equidistant (hexagonal pattern)



Cell Format



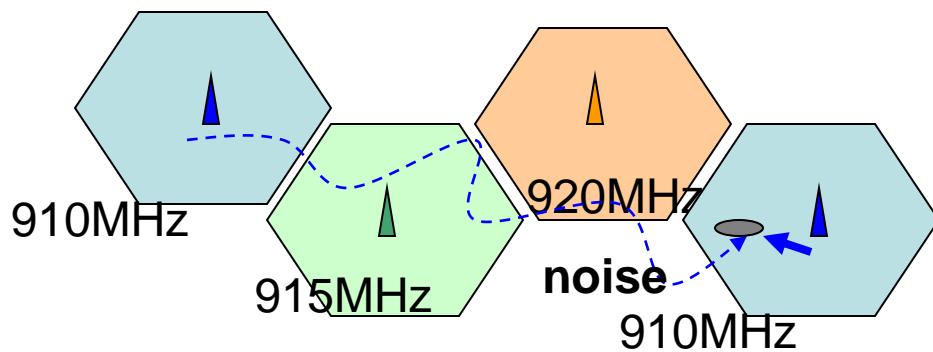
(a) Square pattern



(b) Hexagonal pattern

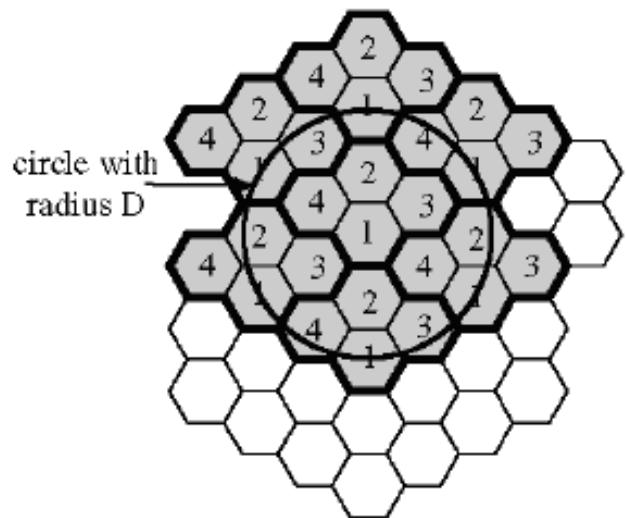
Frequency Reuse

- Adjacent cells assigned different
 - frequencies to avoid interference or crosstalk
- Objective is to reuse frequency in nearby cells
 - 10 to 50 frequencies assigned to each cell
 - Transmission power controlled to limit power at that frequency escaping to adjacent cells
 - The issue is to determine how many cells must intervene between two cells using the frequency

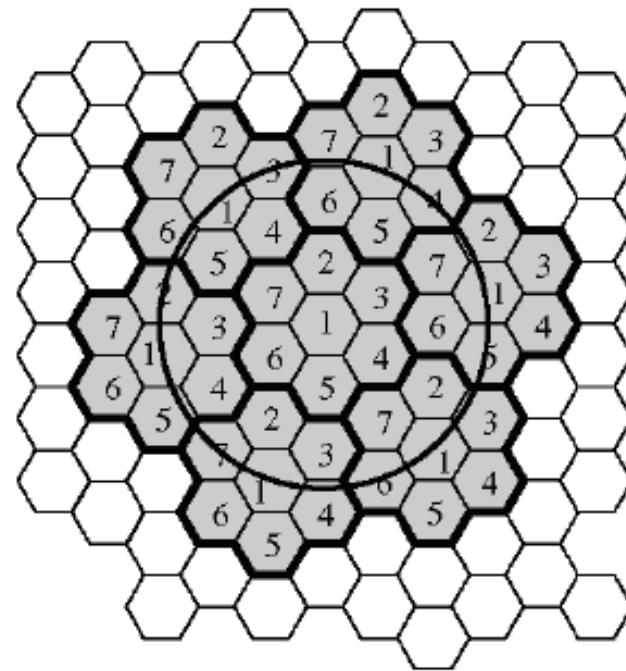


Frequency Reuse

- $N=1,3,4,7,9,12,13,16,19 \dots$



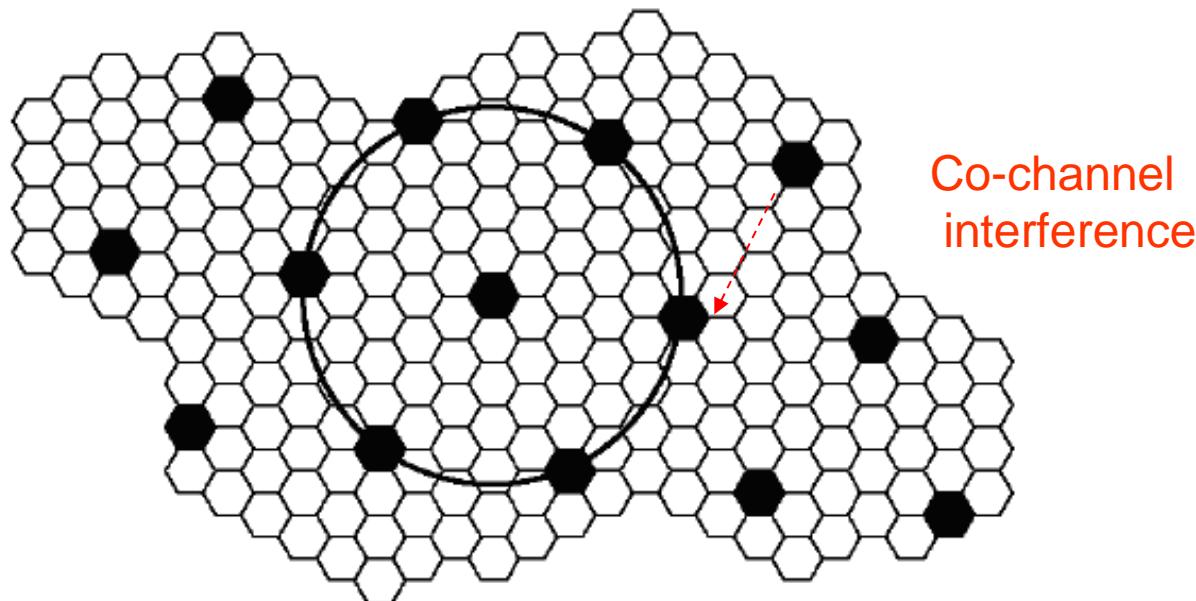
(a) Frequency reuse pattern for $N = 4$



(b) Frequency reuse pattern for $N = 7$

Frequency Reuse

- Larger N
 - Longer distance between cell with the same frequency
 - Less co-channel interference



(c) Black cells indicate a frequency reuse for $N = 19$

Frequency Reuse

Power is inversely proportional to Distance (Inverse square law)

→ Signal to Noise is proportional to N^2

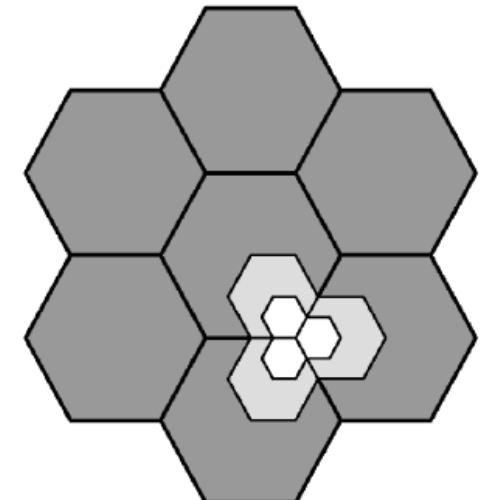


$$D/R = \sqrt{3}N$$

Approaches to Cope with Increasing Capacity

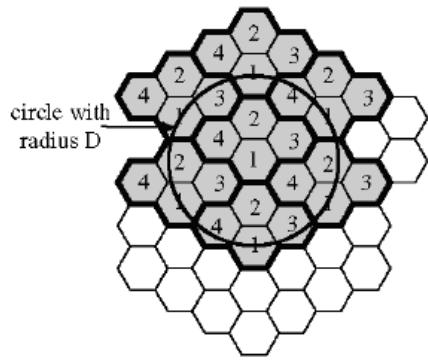
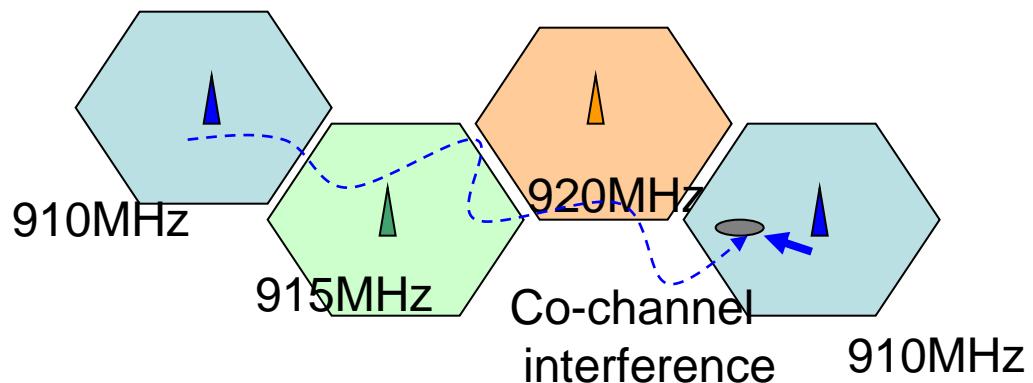
- Adding new channels
- Frequency borrowing
 - frequencies are taken from adjacent cells by congested cells
- Cell splitting
 - cells in areas of high usage can be split into smaller cells
- Cell sectoring
 - cells are divided into a number of wedge-shaped sectors, each with their own set of channels
- Microcells
 - antennas move to buildings, hills, and lamp posts

Cell Splitting

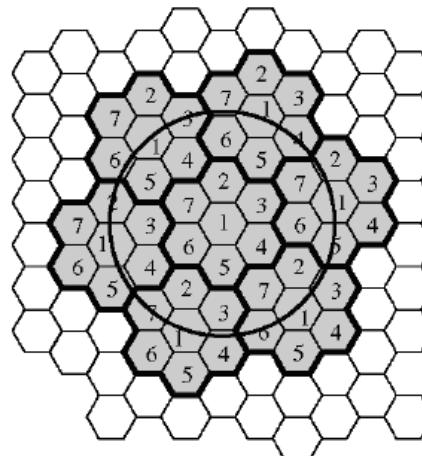


Capacity vs Accuracy

- When N is large
 - Less co-channel interference
 - Stronger signal to noise ratio
 - Smaller cell-site
 - More accurate in location estimation
- But require more frequency resources



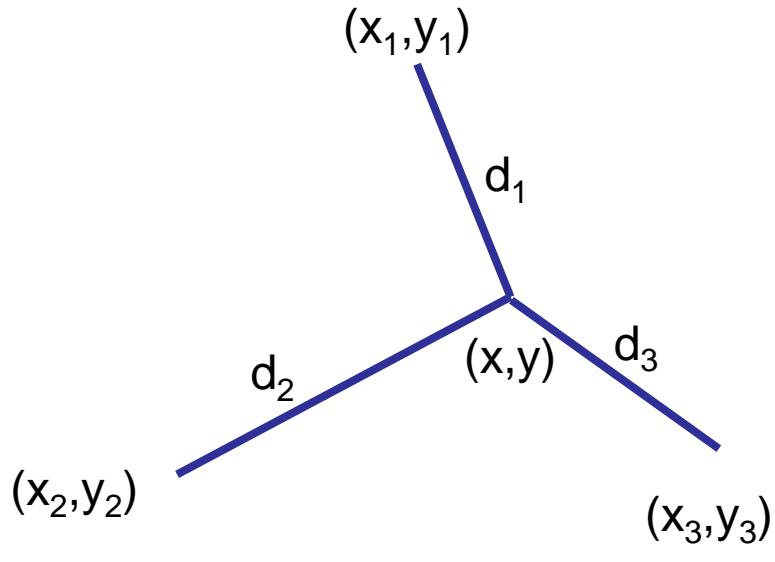
(a) Frequency reuse pattern for $N = 4$



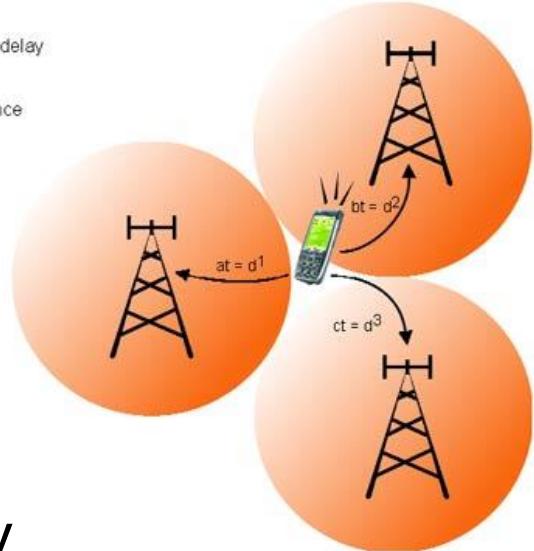
(b) Frequency reuse pattern for $N = 7$

Methodologies for location estimation

- Time of arrival (TOA)
 - Time predict distance
 - 3 distance data locate a point



$a, b, c = \text{delay}$
 $t = \text{time}$
 $d = \text{distance}$



Solve x, y

$$d_1 = t_1 \cdot c$$

$$d_2 = t_2 \cdot c$$

$$d_3 = t_3 \cdot c$$

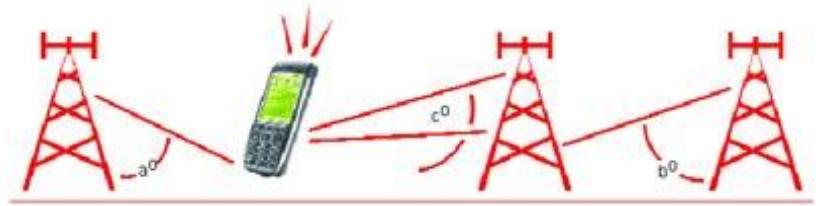
$$d_1^2 = (y_1 - y)^2 + (x_1 - x)^2$$

$$d_2^2 = (y_2 - y)^2 + (x_2 - x)^2$$

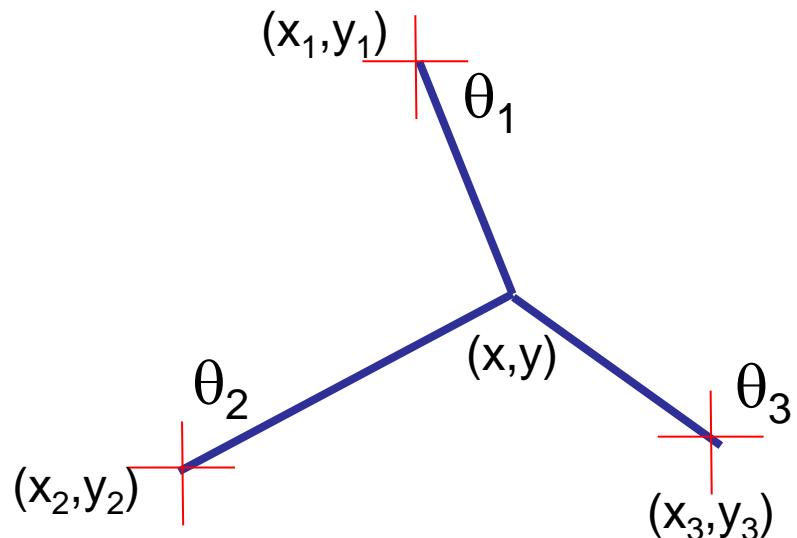
$$d_3^2 = (y_3 - y)^2 + (x_3 - x)^2$$

Methodologies for location estimation

- Angle of arrival (AOA)
 - 3 angles location a point



Solve x,y



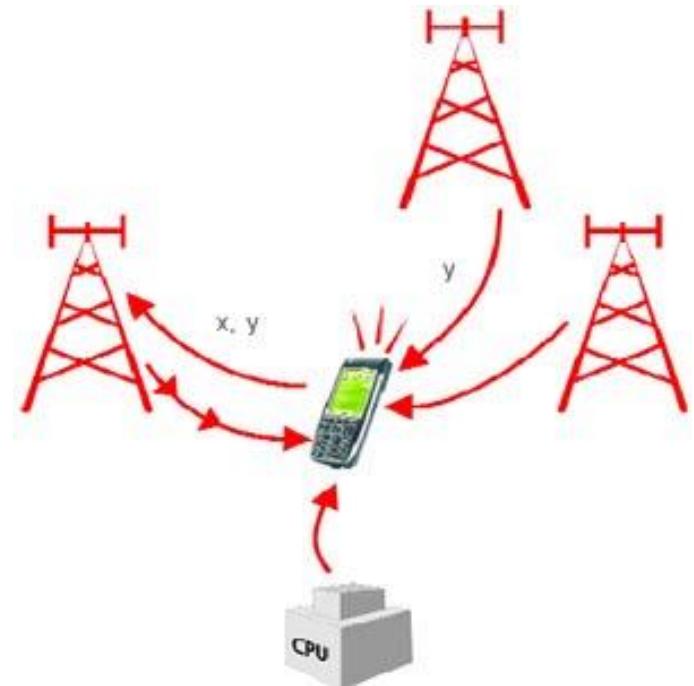
$$\text{Slope}_1 = (y_1 - y) / (x_1 - x)$$

$$\text{Slope}_2 = (y_2 - y) / (x_2 - x)$$

$$\text{Slope}_3 = (y_3 - y) / (x_3 - x)$$

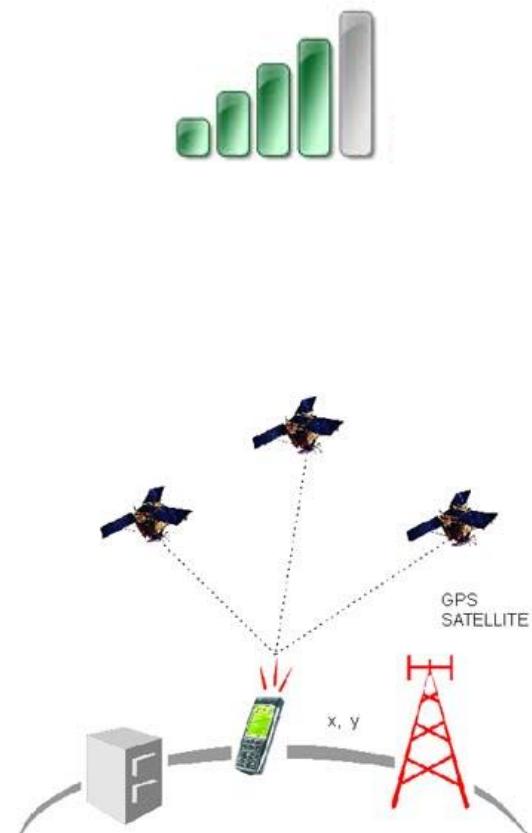
Methodologies for location estimation

- Time difference of arrival (TDOA)
 - If it can only access two Base-station, distance between base-stations provide the 3rd information



Methodologies for location estimation

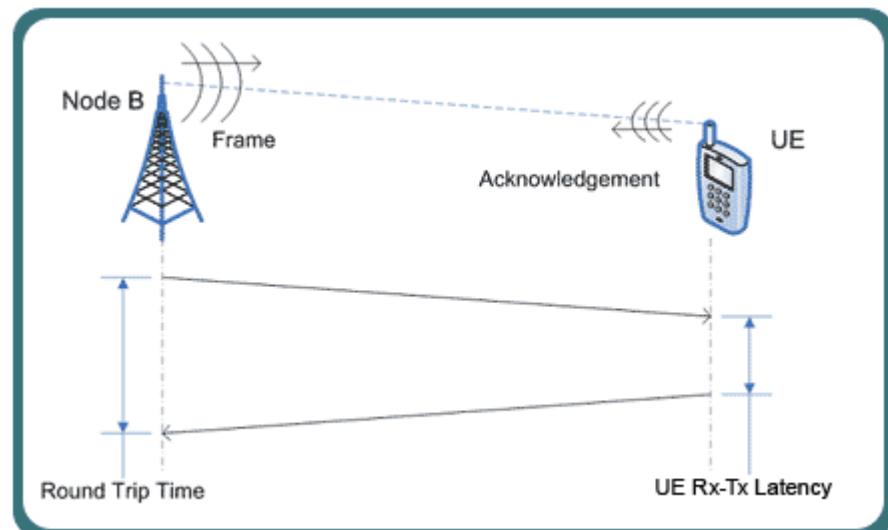
- Enhanced observed time difference (EOTD)
- Cell global identification (CGI) and Timing advance (TA)
- Signal strength (SS)
- Global Positioning System (GPS)
- Control Plane Locating



Methodologies for location estimation

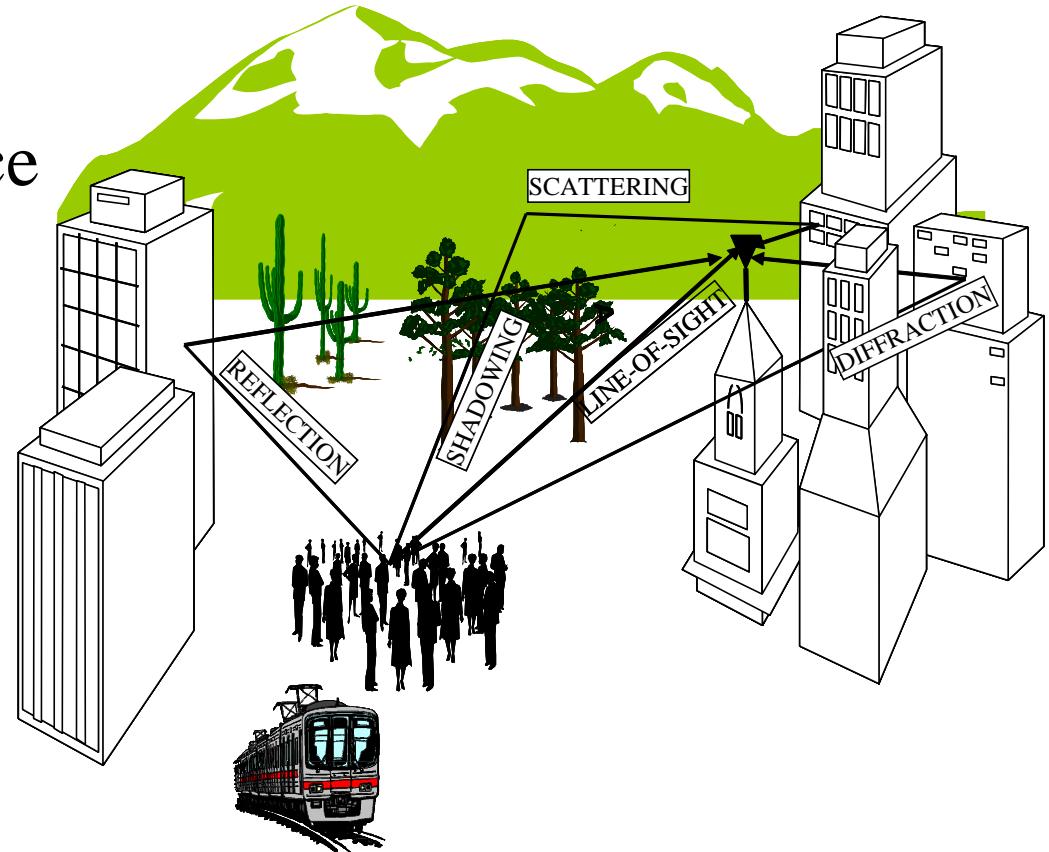
- Control plane locating
 - Service provider gets the location based on the radio signal delay of the closest cell-phone towers (for phones without GPS features) which can be quite slow as it uses the 'voice control' channel.
 - Some primitive LBS services use a single base station, with a 'radius' of inaccuracy, to determine a phone's location. This technique was the basis of the E-911 mandate and is still used to locate cell phones as a safety measure.

- More details
 - <http://www.hkwtia.org/>



Error of location base estimation

- Scattering
- Shadowing
- Reflection
- Diffraction
- Co-channel interference



What's is Location Base Service

- A **location-based service** (LBS) is an information and entertainment service, accessible with mobile devices through the mobile network and utilizing the ability to make use of the geographical position of the mobile device
- E.g. identify a location of a person or object such as discovering the nearest banking cash machine or the whereabouts of a friend or employee.

Basic operation modes of LBS

- Pull
 - The customer initiates mobile positioning measurement at the same time when one requests for a service
- Push
 - The request for service (and hence mobile positioning) is not technically made by the customer but by the service provider
- Tracking
 - Someone (person or service) asks for a location of the mobile terminal (Person, vehicle, fleet etc.)

Class discussions:

What are the applications of LBS?

Applications of Location base Services

- Emergency services
- Mobile advertising
- Location sensitive billing
- Fraud protection
- Asset tracking
- Fleet management
- Intelligent transportation systems
- Mobile yellow pages
- parcel tracking and vehicle tracking services
- Location base coupons or advertising
- personalized weather services and
- location-based games
- Requesting the nearest business or service, such as an ATM or restaurant
- Locating people on a map displayed on the mobile phone
- Receiving alerts, such as notification of a sale on gas or warning of a traffic jam

Applications of Location base Services

- Resource tracking with dynamic distribution.
 - Taxis, service people, rental equipment, doctors, fleet scheduling.
- Resource tracking.
 - Objects without privacy controls, using passive sensors or RF tags, such as packages and train boxcars.
- Finding someone or something.
 - Person by skill (doctor), business directory, navigation, weather, traffic, room schedules, stolen phone, emergency calls. Targeted advertising, buddy list, common profile matching (dating)

Values of LBS

- Use as a filter
 - to restrict results of search that are close enough to the customers' location
- Use as a pointer
 - to show the location of the customers as a dot on a map in tracking services
- Use as a definer/launcher for “area alarm”
 - i.e. to launch a pre-defined activity (e.g. send a MSMS) with customer enters/leaves a certain area



CNN news on location Base service

- <http://www.youtube.com/watch?v=NwuW5BCaj-I>



Class discussions:

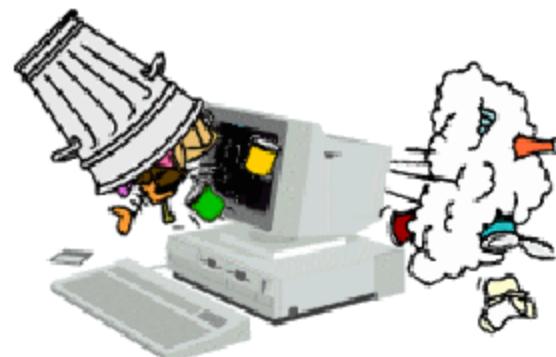
What are the
issues/problems of LBS?

What are the issues/problems of LBS?

- Privacy
- Accuracy
- Coverage
- Useless information (Garbage information)
- Information overload

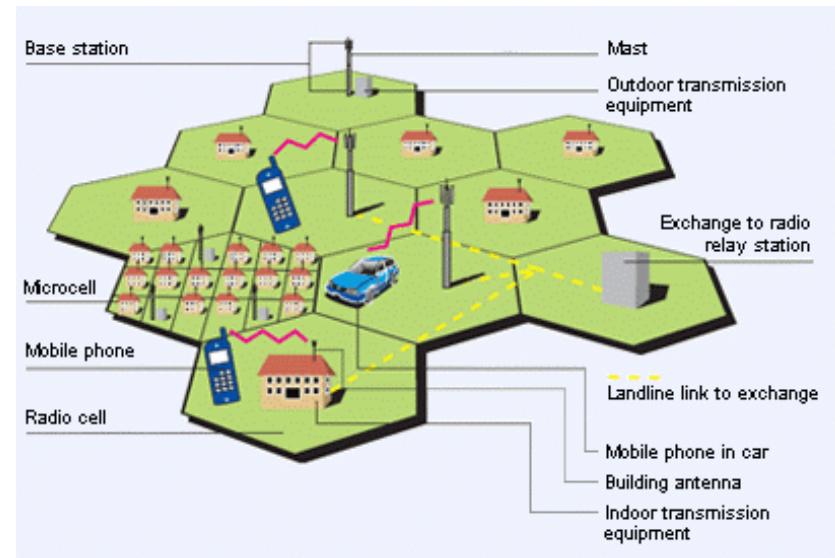
Major issues faced by LBS

- Accuracy of location
 - Mobile network was primarily built for communication, not positioning
 - If location data is not accuracy, the information is not useful (Garbage in, Garbage out)
 - Limiting choice of service



Major issues faced by LBS

- Investment vs penetration
 - Extraction of network measurement for position calculation remains a difficult and expensive task
 - Network base solution offers a full-base penetration → but large investment
 - Terminal based solution is relatively less expansive but largely limits penetration



Major issues faced by LBS

- Business Model (Willingness to pay)
 - Consumer market: position information in most cases are just “nice-to-have”. There is no killer application
 - Enterprise users are more willing to pay a higher fee
- Inter-operability between operators
 - Cross border continuity
 - Difference in positioning accuracy
 - Commercial models in roaming

Major issues faced by LBS

- Privacy
 - Opt-in/ Opt-out policy
 - Applications development/service provider
 - Dilemma of In-house/out-source development
 - Outsourcing the service/development can reduce the cost of operation. But the operator's network data are very sensitive and involve privacy issues.





Q&A

ELEC2544

e-Commerce and FinTech

Business to Business (B2B) Model

Lecturer: Dr. Wilton Fok

Room 703, Chow Yei Ching Building

Tel: +852 2857 8490

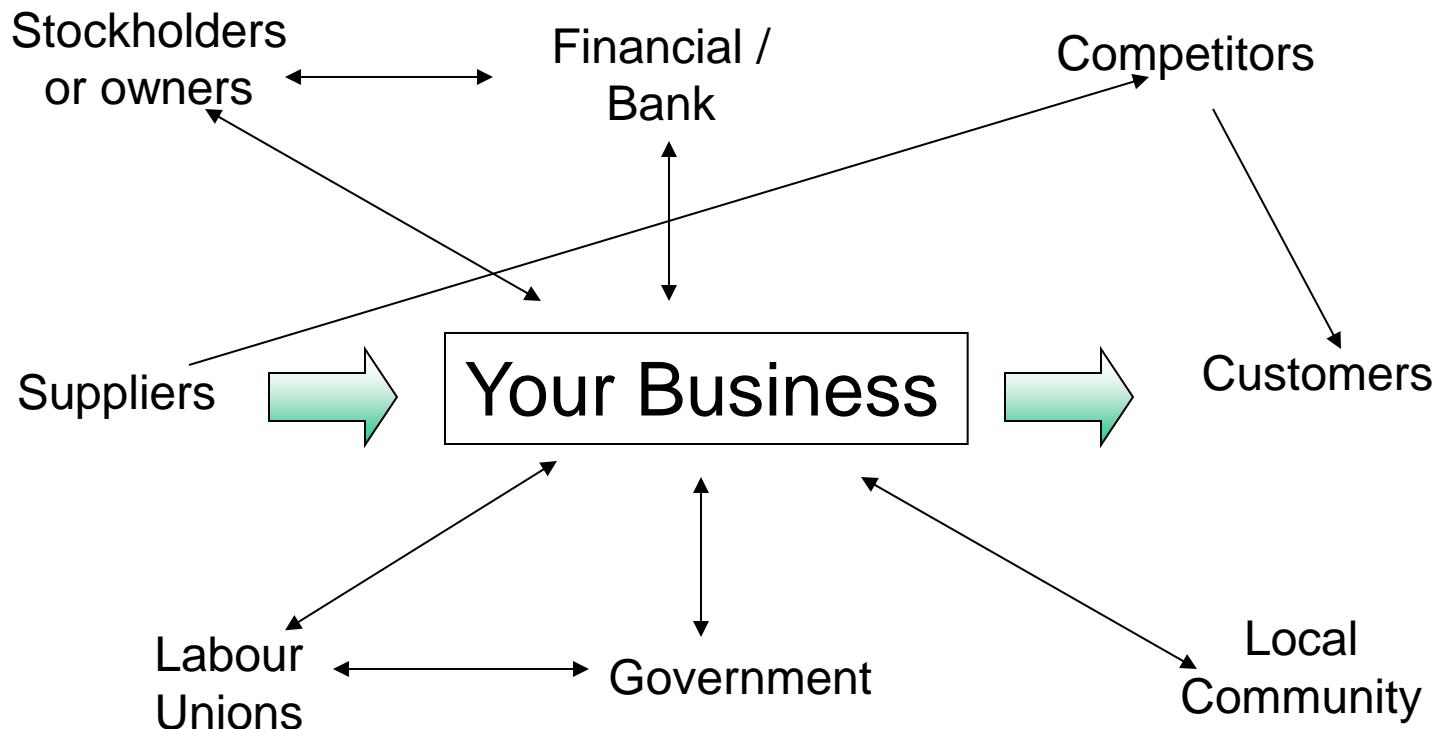
e-mail: wtfok@eee.hku.hk

3.1 Introduction

- In session 2, we looked at how prevailing competitive advantage strategy strengthens information flows with customers. (B2C)
- In this session, we will concentrate on future competitive advantage strategy (B2B)
- To recap, future strategy gains competitive advantage by:
 - Creating information links to outside business elements;
 - Links with other systems in the business;
 - Strengthening information flows with suppliers, financial community, etc

3.2 Purchasing, Logistics and Support

- While B2C models, such as a virtual storefront, can electronically take order and payment information from a customer, they may still need to ship a physical good to the customer.



3.2 Purchasing, Logistics and Support

- Remember, every physical flow has a parallel conceptual flow (i.e. flow of information, data and money)
- If the goods are not in digital form then traditional freight will be required.
- Order fulfillment (or Logistics) is another opportunity for a business to optimize its conceptual flows.
 - Order fulfillment can be: In-house or Outsource
 - e.g DHL offers services directly aimed at web based merchants



Outsourcing logistics for B2B

- Outsourced order fulfillment will generally offer:
 - Storage of goods
 - Goods are picked up from the Merchant and stored in an allocated area.
 - Inventory management
 - The order is sent electronically from merchant to the order fulfillment agent.
 - Information is stored in the order fulfillment agent's order entry system, which can provide detailed reporting and stock-taking.
 - Packing and delivery of order
 - The products are collected, labelled and sent to the customer.
 - Order tracking
 - Allows the customer to monitor their package's progress from the warehouse to the final destination.

(Reference: O'Brien, E-commerce Handbook, Tri-Obi Production s, 2000, pp104 to 123.)

Integrate the outsourced logistics service with the in-house system

The screenshot shows a Mozilla Firefox browser window displaying the DHL Hong Kong Tracking page. The URL in the address bar is <http://www.dhl.com.hk/publish/hk/en/eshipping/track.high.htm>. The page features a yellow header with the DHL logo and navigation links for Products / Services, eShipping, Tools, Information, Press, Careers, and About DHL. A red banner in the center says "Tracking Good Afternoon". Below it, there's a section titled "Track your Shipment" with a "DHL Airwaybill" input field and a "Track" button. To the right, there are images of a smartphone, a laptop, and a package. On the left, a sidebar lists various services: eShipping Quick Access, eMailShip, Web Shipping, DHL Import Express Online, Book a Pick-up, Tracking, Order Supplies, Logistics eServices, Remote Area Service, DHL Airwaybill Printing, Trade Automation Service, and DHL Interactive. At the bottom, it says "Deutsche Post DHL". The main content area includes a "Use DHL Shipping Tools" section, an "On-line Tracking" section with a dropdown menu for selecting tracking types (with "DHL Airwaybill Number" selected), and a message about continuing to track shipments for DHL, Exel, Danzas, or Euro Express customers.

DHL | Hong Kong | Tracking - Mozilla Firefox

檔案 (E) 編輯 (E) 檢視 (V) 歷史 (S) 書籤 (B) 工具 (I) 說明 (H)

http://www.dhl.com.hk/publish/hk/en/eshipping/track.high.htm

Google 搜尋

rfid hk airport - ... YouTube - The... dhl - 雅虎香港 ... HK airport award ... DHL | Ho...

Products / Services eShipping Tools Information Press Careers About DHL

Tracking Good Afternoon

Track your Shipment

DHL Airwaybill ▶ Track

More tracking options

eShipping Quick Access

eMailShip

Web Shipping

DHL Import Express Online

Book a Pick-up

Tracking

Order Supplies

Logistics eServices

Remote Area Service

DHL Airwaybill Printing

Trade Automation Service

DHL Interactive

Deutsche Post DHL

Use DHL Shipping Tools to make your shipment tracking easier.

More information

Whether you are originally a DHL, Exel, Danzas or Euro Express customer, you can continue to track shipments in the same way that you always have done.

On-line Tracking

Track shipments using the box provided. Select number types from the drop down list. For Danzas and DHL Global Forwarding (DGF), track one number at a time. For DHL Air Waybill, Europlus & Europack track up to 10 number - press 'Enter' or hit the 'Spacebar' to separate.

Please select: DHL Airwaybill Number

DHL Airwaybill Number

DHL Europlus & Europack Identcode

DHL Europlus & Europack Reference

Danzas Order Code

DGF/Danzas HAWB (House Air Way Bill)

DGF/Danzas Container Number

DGF/Bill of Lading/Masterbill

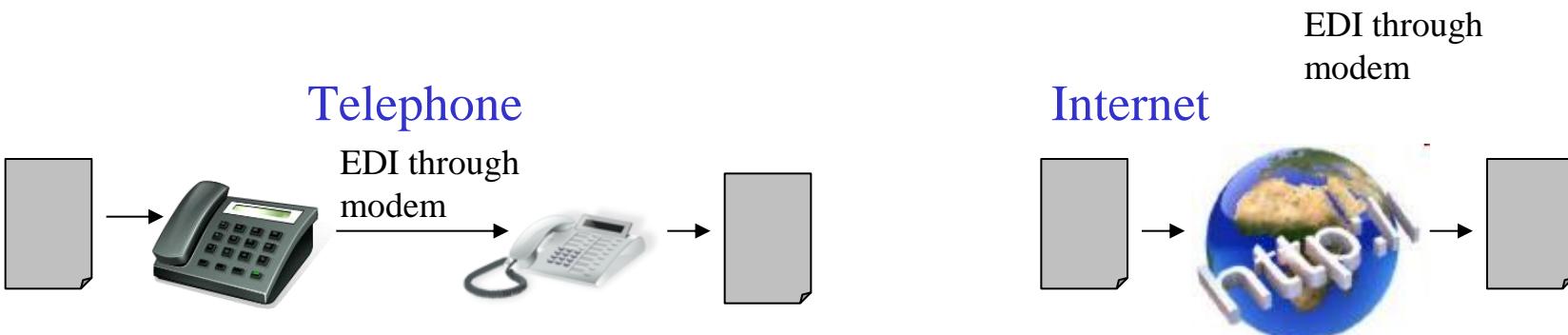
DGF/Danzas Reference Number

Danzas Bill of Lading/Masterbill

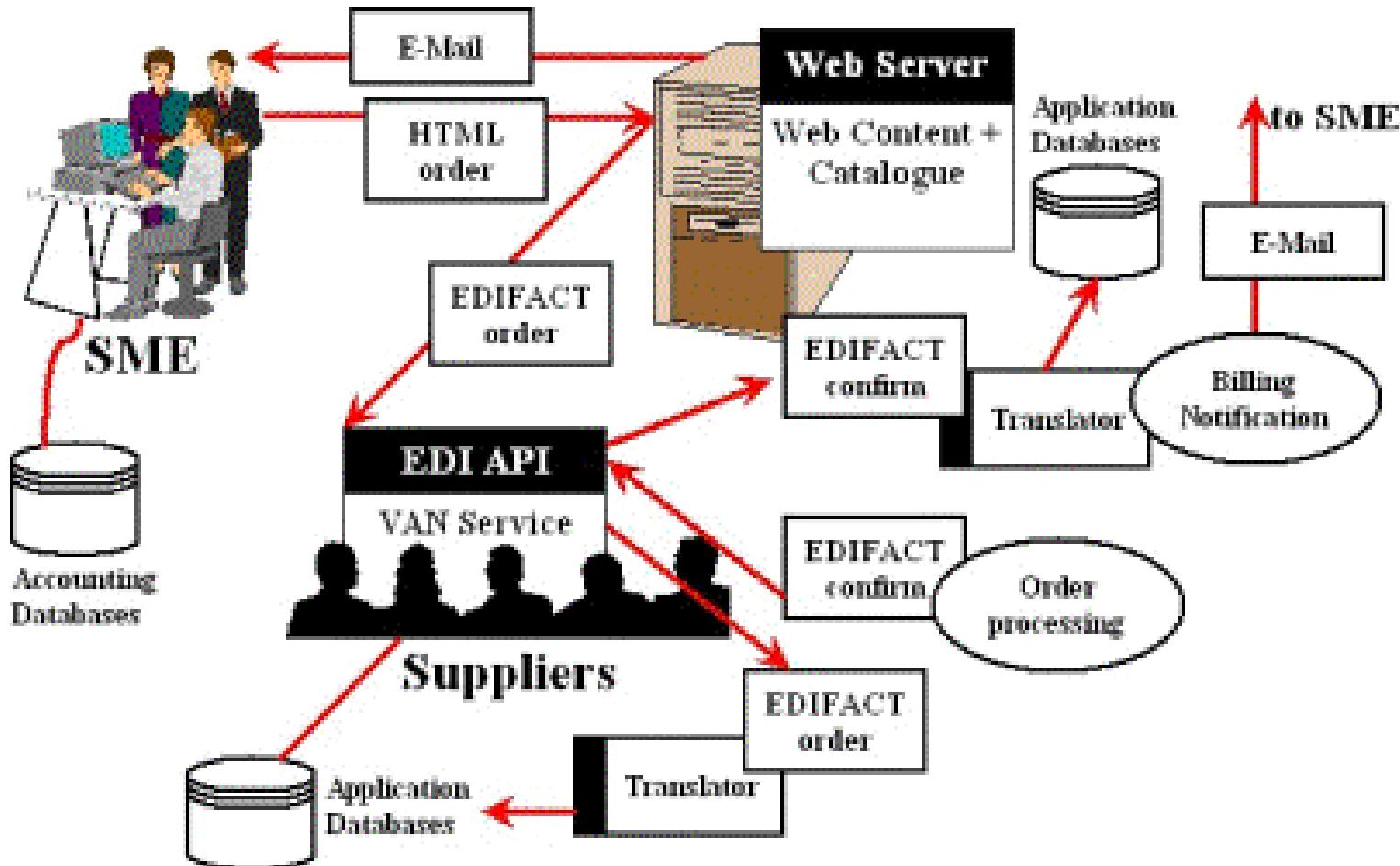
完成

Integration of B2B e-commerce system by EDI

- Electronic Data (Document) Interchange (EDI)
 - A system that allows businesses to send and receive electronic documents.
- There are:
 - EDI purchase orders,
 - EDI quotation
 - EDI delivery note
 - EDI verification of delivery
 - EDI Invoice and so on.
- Initially EDI messages were exchanged between businesses using leased telephone lines
- Today, most businesses will use EDI or XML messages using the Internet.



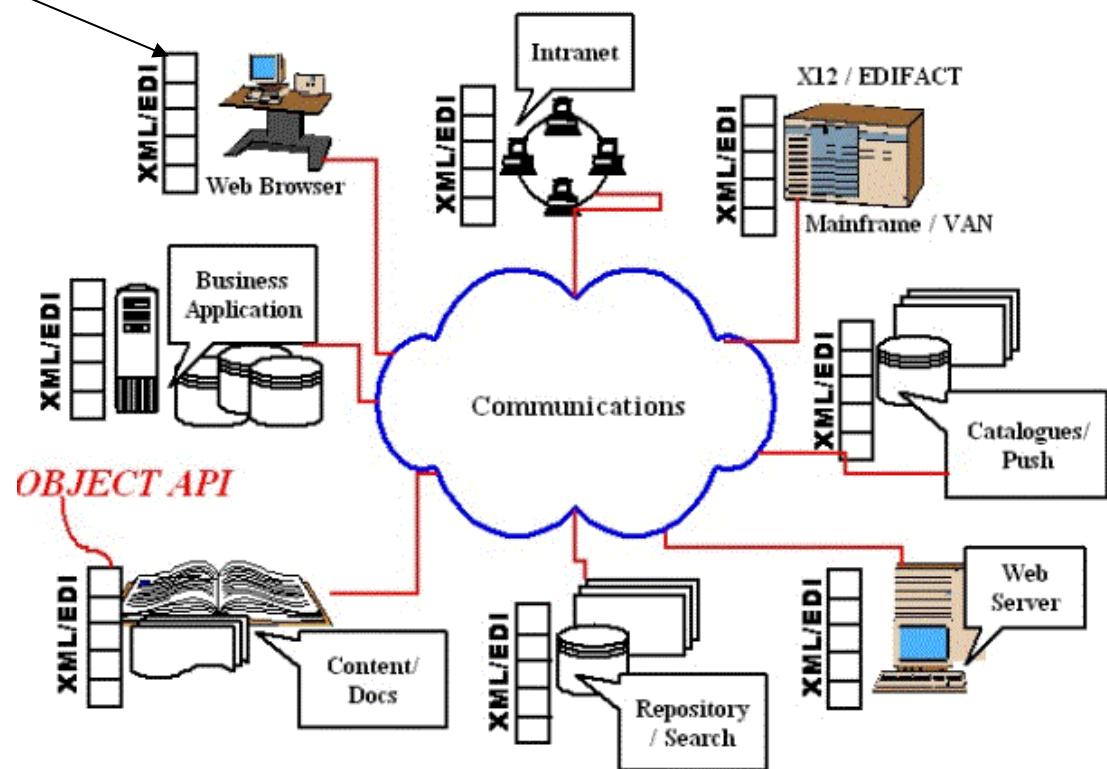
Integration of B2B e-commerce system by EDI



Transferring EDI data through the network

- For example, an EDI XML data could have the form:

```
<!ENTITY % address SYSTEM  
  "http://www.myco.org/messages/XM  
L/address.xml" >  
  
<!ENTITY % items SYSTEM  
  "http://www.edifact.org/messages/X  
ML/items.xml">  
  
<!ENTITY % data "(#PCDATA)">  
  <!ELEMENT order (order-no,  
  deliver-to, invoice-to, item+)>  
  
<!ELEMENT order-no %data; >  
  <!ELEMENT deliver-to (address)>  
  
<!ELEMENT invoice-to (address) > <!--  
 Import standard address class-->  
 %address; <!--Import standard item  
 class--> %items;
```



Advantages of using EDI over paper systems

- EDI and other similar technologies save a company money by replacing information flows that require a great deal of human interaction and materials such as paper documents, meetings, faxes, etc.
- Even when paper documents are maintained in parallel with EDI exchange, EDI reduces the handling costs of sorting, distributing, organizing, and searching paper documents.

Advantages of using EDI over paper systems

- EDI provides benefits of storing and manipulating data electronically **without the cost of manual entry.**
- It **reduces errors**, such as shipping and billing errors, because EDI eliminates the need to rekey documents on the destination side.
- It is **faster in speed** in which the trading partner receives and incorporates the information into their system thus greatly reducing cycle times.
- → EDI can be an important component of **just-in-time (JIT)** production systems.

Advantages of using EDI over paper systems

- According to the Aberdeen report "A Comparison of Supplier Enablement around the World",
 - only 34% of purchase orders are transmitted electronically in North America.
 - In EMEA (Europe, the Middle East and Africa), 36% of orders are transmitted electronically and
 - in APAC, 41% of orders are transmitted electronically.
- They also report that the average paper requisition to order costs a company:
 - US\$37.45 in North America,
 - US\$42.90 in EMEA and
 - US\$23.90 in APAC.
- With an EDI requisition to order costs are reduced to
 - US\$23.83 in North America,
 - US\$34.05 in EMEA and
 - US\$14.78 in APAC.
- Ref: http://en.wikipedia.org/wiki/Electronic_Data_Interchange



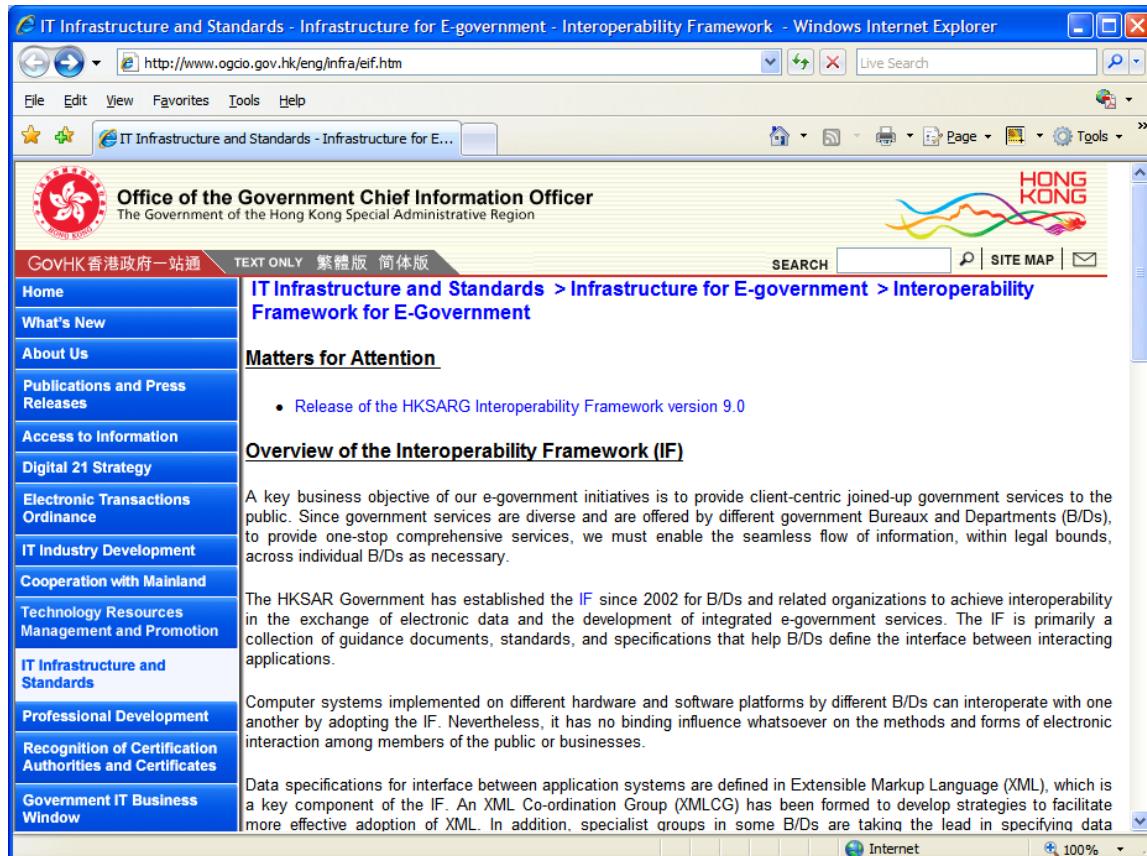
More reference information

Guidelines for using XML for Electronic Data Interchange

<http://www.mmit.stc.sh.cn/Projects/ecforum/otherlinks/XmlEdi/guide.htm>

XML Scheme and standards of the HKSAR Government

- <http://www.ogcio.gov.hk/eng/infra/eif.htm>
 - Part II: XML Schema Design Guide
<http://www.ogcio.gov.hk/eng/infra/download/g55-2.pdf>



The screenshot shows a Windows Internet Explorer window displaying the official website of the Office of the Government Chief Information Officer (OGCIO) for Hong Kong. The URL in the address bar is <http://www.ogcio.gov.hk/eng/infra/eif.htm>. The page content is about the IT Infrastructure and Standards > Infrastructure for E-government > Interoperability Framework for E-Government. It features a sidebar with various government-related links and a main content area with sections on matters for attention, overview of the interoperability framework, and details about the framework's purpose and implementation.

Office of the Government Chief Information Officer
The Government of the Hong Kong Special Administrative Region

GovHK 香港政府一站通 TEXT ONLY 繁體版 簡體版

IT Infrastructure and Standards > Infrastructure for E-government > Interoperability Framework for E-Government

Matters for Attention

- Release of the HKSARG Interoperability Framework version 9.0

Overview of the Interoperability Framework (IF)

A key business objective of our e-government initiatives is to provide client-centric joined-up government services to the public. Since government services are diverse and are offered by different government Bureaux and Departments (B/Ds), to provide one-stop comprehensive services, we must enable the seamless flow of information, within legal bounds, across individual B/Ds as necessary.

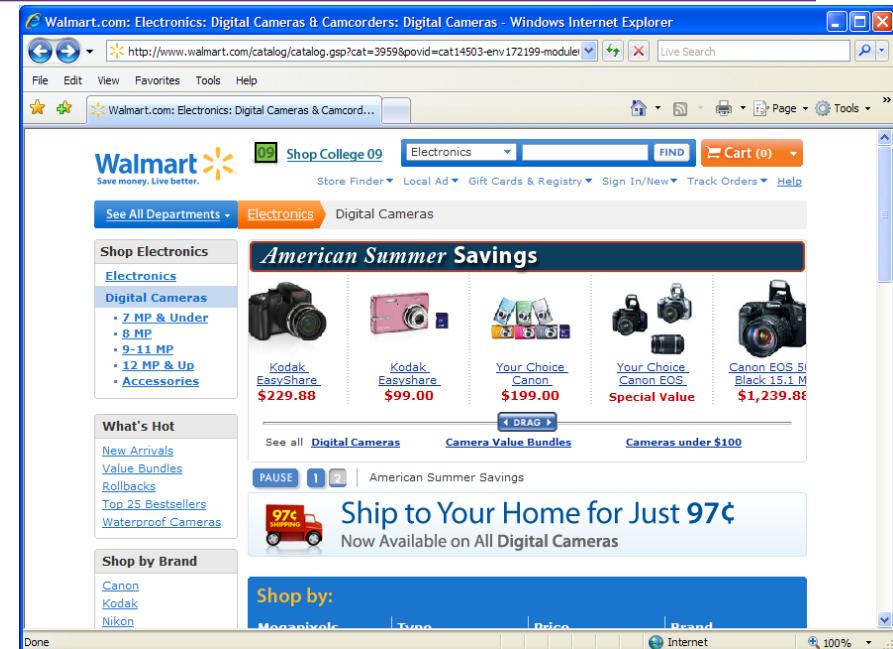
The HKSAR Government has established the IF since 2002 for B/Ds and related organizations to achieve interoperability in the exchange of electronic data and the development of integrated e-government services. The IF is primarily a collection of guidance documents, standards, and specifications that help B/Ds define the interface between interacting applications.

Computer systems implemented on different hardware and software platforms by different B/Ds can interoperate with one another by adopting the IF. Nevertheless, it has no binding influence whatsoever on the methods and forms of electronic interaction among members of the public or businesses.

Data specifications for interface between application systems are defined in Extensible Markup Language (XML), which is a key component of the IF. An XML Co-ordination Group (XMLCG) has been formed to develop strategies to facilitate more effective adoption of XML. In addition, specialist groups in some B/Ds are taking the lead in specifying data

Case Study: Walmart

- E.g. B2C and B2B in Wal-Mart
 - B2C: Wal-Mart offers on-line store service to its customers
 - Ref: Wal-Mart opens doors to new online store
http://news.cnet.com/2100-1017_3-235144.html
 - B2B: Wal-Mart builds RFID with its business partners



RFID for logistics operation

<http://www.youtube.com/watch?v=4Zj7txoDxbE>



How RFID and EDI can reduce operation cost

- Using RFID and centralized inventory information database using EDI/XML
- Supply and demand will be more visible by retailer, logistics and manufacturers
 - Reduce over stocking
 - Reduce warehouse cost
 - Reduce loss due to expiry, especially food
 - Reduce the inventory cost
 - Just-in-time inventory management

E-Commerce Enabling Technology: RFID

Introduction of RFID applications in HK (TVB)

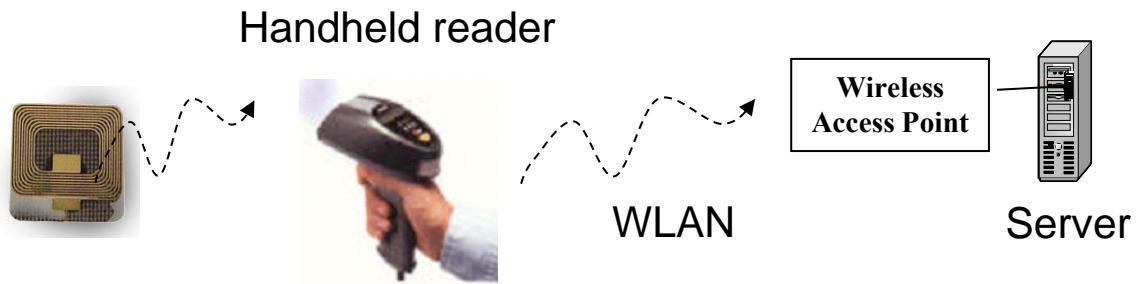
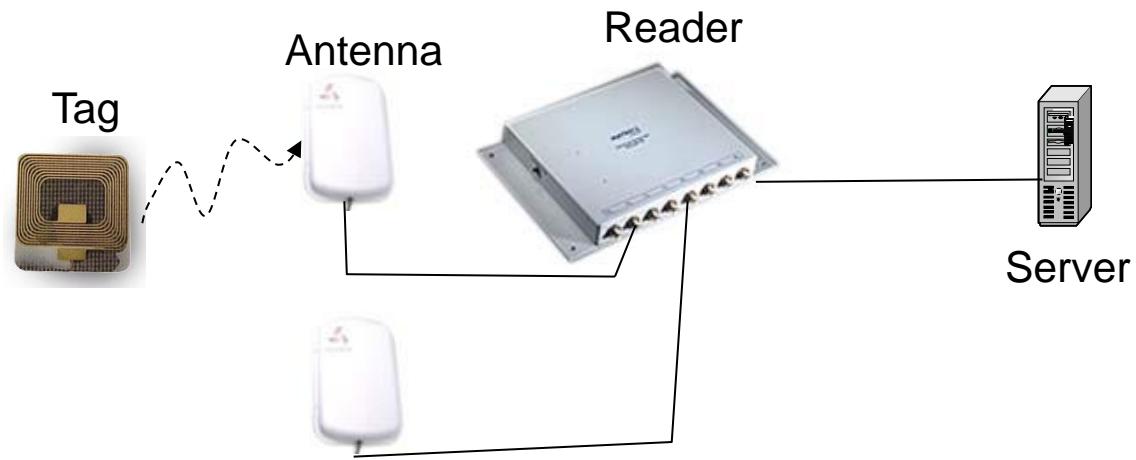
- <http://www.youtube.com/watch?v=O8ac9SmcrLE>



RFID Technology for e-Business

- Introduction of RFID

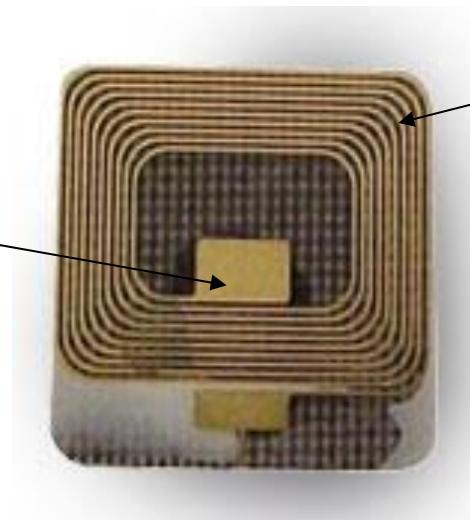
- RFID is an automatic identification method that can store and remotely retrieve data using RFID tags, Reader and Antenna



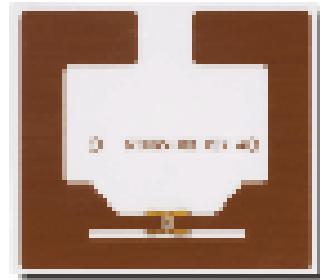
RFID Technology for e-Business

- An RFID tag is an object that attach to a product, equipment, animal, or person for the purpose of identification using radio waves.
- Most RFID tags contain at least two parts

An integrated circuit (IC) for storing and processing information, modulating and demodulating a RF signal and other specialized functions



Loop Antenna



Dipole Antenna

An antenna for receiving and transmitting the signal.

RFID Tags

- Tags can be read-only or read-write
- Tag memory can be factory or field programmed, and optionally permanently locked
- Bytes left unlocked can be rewritten over more than 100,000 times



Types of RFID Tags

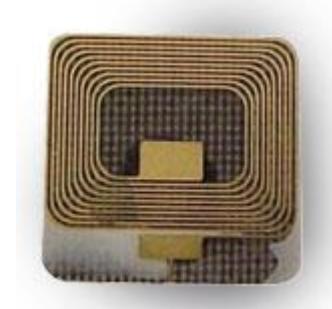
Active

- Tag transmits radio signal
- Battery powered memory, radio & circuitry
- High Read Range (300 feet)



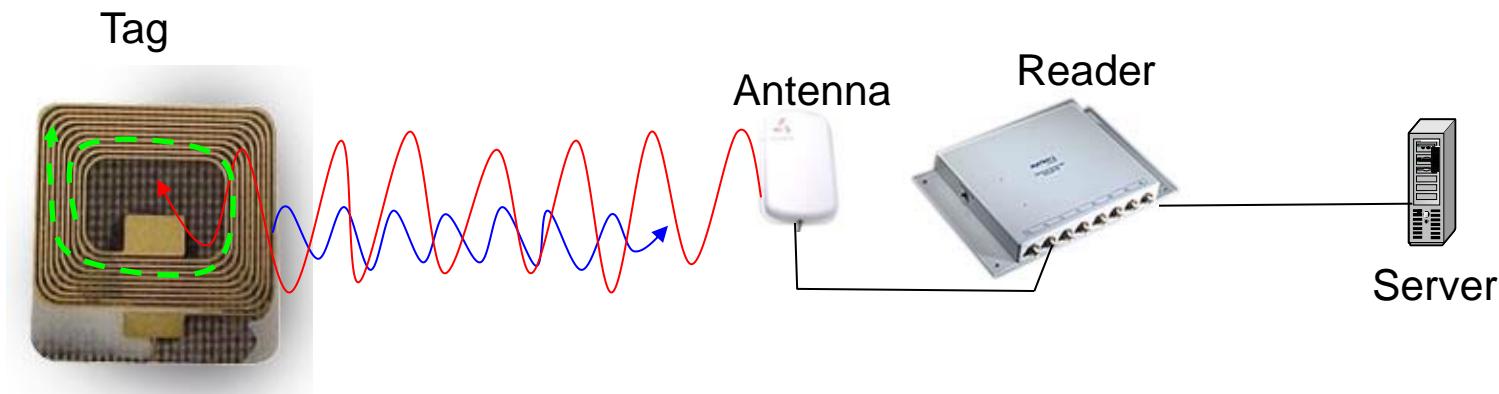
Passive

- Tag reflects radio signal from reader
- Reader powered
- Shorter Read Range (4 inches - 15 feet)



Passive Tags

- Passive RFID tags have no internal power supply.
- The electrical current induced in the antenna by the incoming RF signal provides just enough power for the CMOS integrated circuit in the tag to power up and transmit a response.
- The response could be more than just an ID number; the tag chip can contain non-volatile EEPROM for storing data.



Passive Tags

- Read distances for tag using 13.56MHz (High Freq band) is about 10 cm
- Read range of Electronic Product Code (EPC) (ISO 18000-6) (using 900MHz, UHF band) can be up to a 3 meters, depends on antenna size and design.
- Examples:



EPC compliant tags for logistics.

Frequency: 900MHz (UHF)

These tags are the standard chosen by Wal-Mart, Target, Tesco and Metro AG



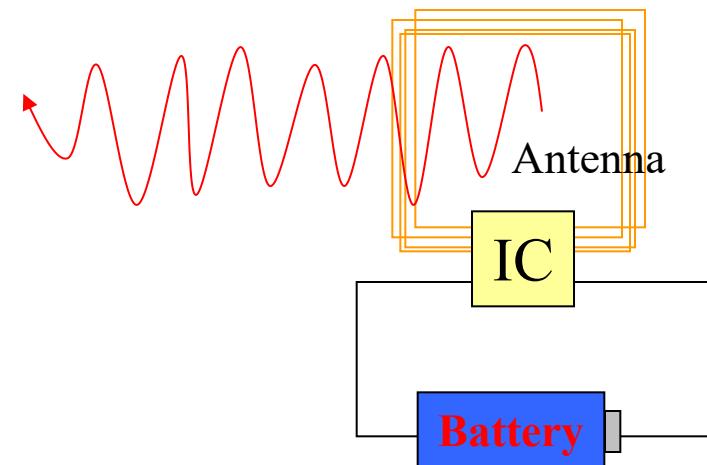
Price of EPC tags are very low:
US\$0.05 each.



Octopus Card
Frequency:
13.56MHz (High Frequency HF)
Reading Range: 10cm

Active Tags

- Active Tags have an internal power source to power the circuits and broadcast the signal to the reader.
- They are more reliable than passive tags as they can conduct a communication session with a reader and can transmit further

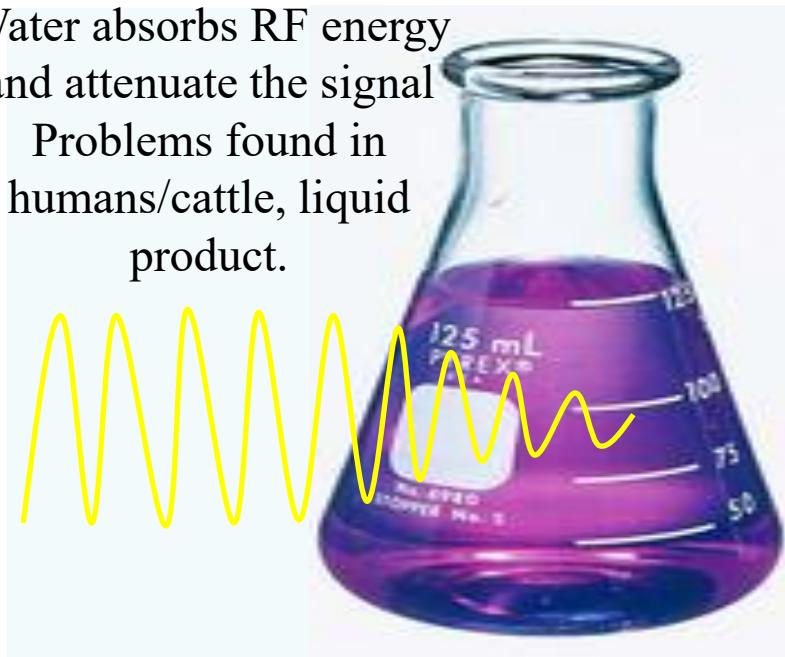


Active Tags

- It can transmit higher power levels than passive tags, allowing them to be more effective in "RF challenged" environments, e.g. Water and metal

Water absorbs RF energy and attenuate the signal

Problems found in humans/cattle, liquid product.



Metal reflects and shield RF signal (e.g. Can drinks, containers, vehicles)

Draw an e-commerce/ mobile commerce application using RFID technology



Draw a RFID e-commerce

- Download and install “iClass - Interactive Class on Cloud” from Appstore
Run the apps> Setting > School [hku]
- For other devices: hku.iclass.hk
- Login using your portal ID (Login through HKU Portal)
- **Join the course: (code: EU9970)**
- Draw an e-com application using RFID Click the submit button after drawing



RFID e-Business Applications

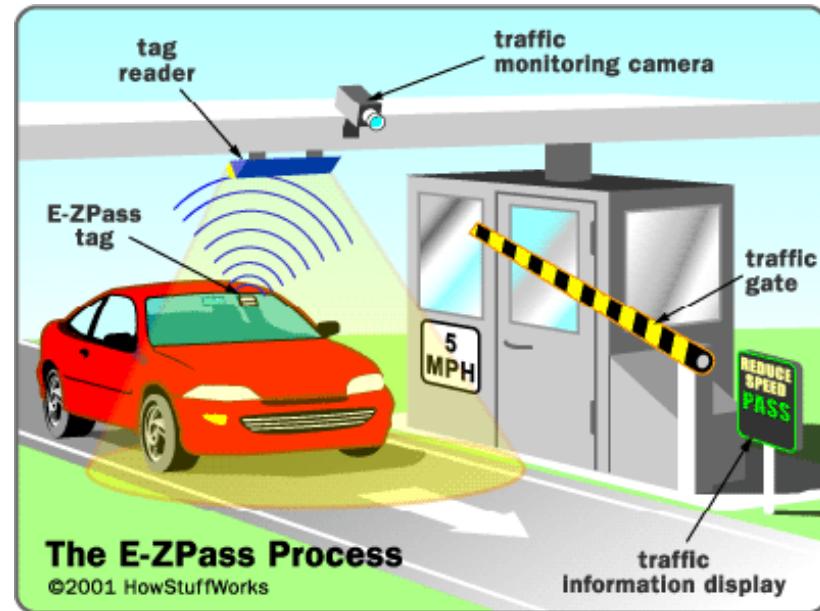
Octopus Card

- *A Passive RFID Tag*
- *Frequency: 13.56MHz (High Frequency HF)*
- *Reading Range: 3 - 8cm*



Automated Toll Collection

- Active RFID Tag (With battery power source)
- Frequency: 900MHz (Ultra-High Frequency, UHF)
- Reading Range: 1m to 8m
- Can read at high speed 50kmh – 80kmh
- Pos:
 - Long reading range
 - Can read at fast speed
- Cons:
 - Expensive
 - Battery will be expired



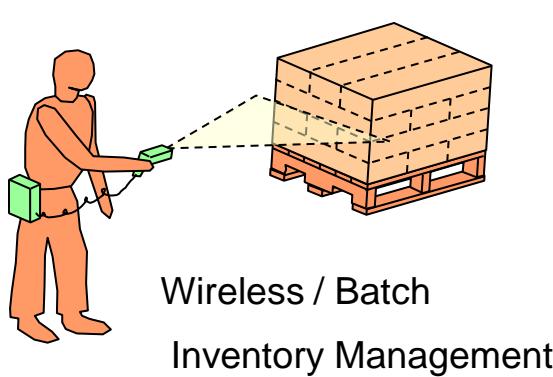
Warehouse Management



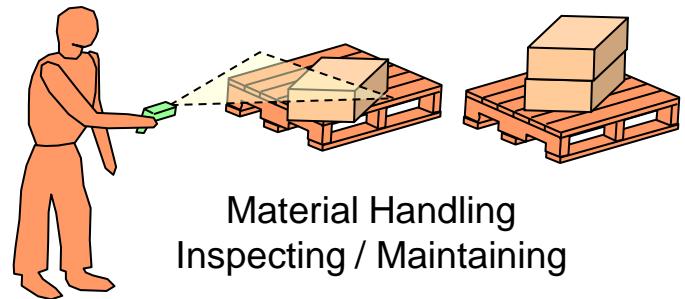
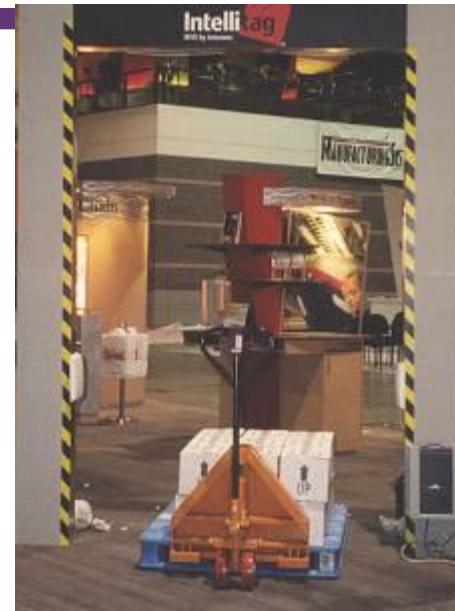
Installed RFID Reader on Fork Truck
(RFID Reader Has 2 Antennas)

- Antenna on Mast - Reads Contents of Saratogas it Picks Up
- Antenna on Undercarriage - Reads RFID Tags in Floor to Determine Location

Application Examples



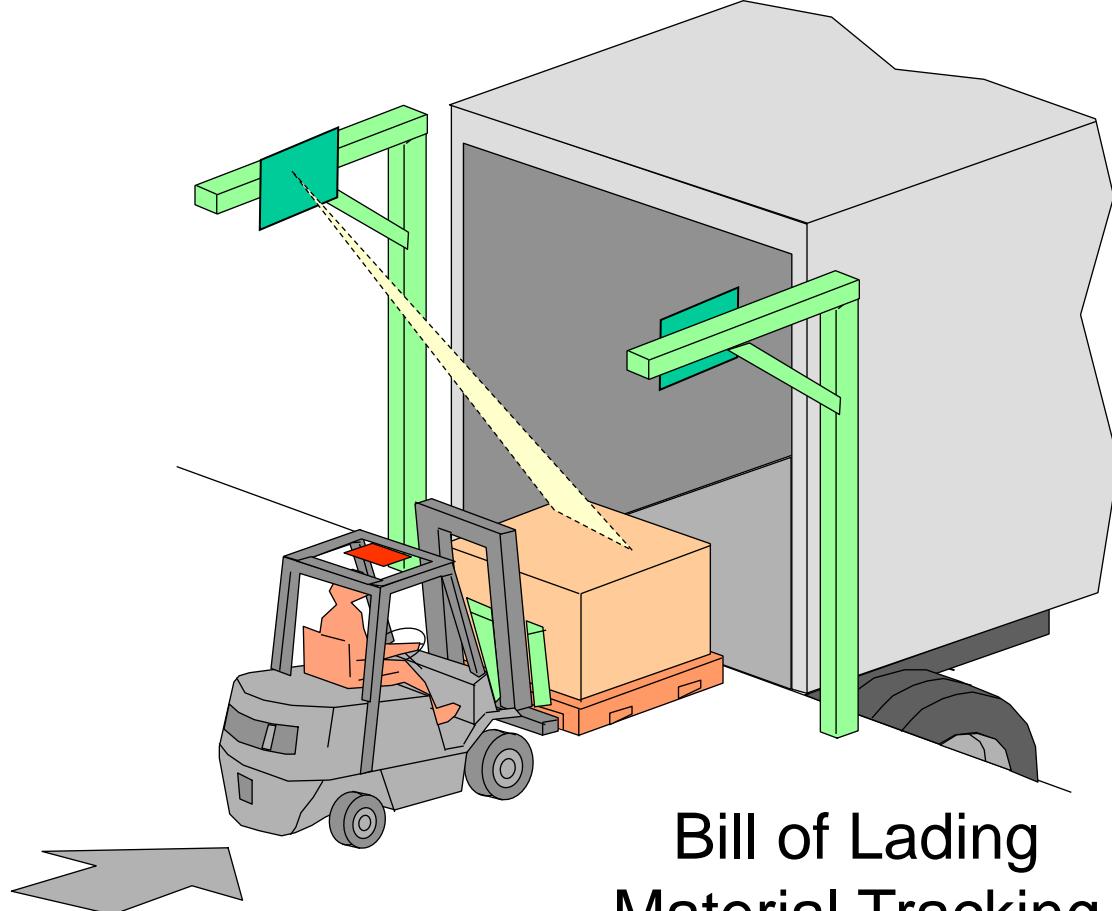
Wireless / Batch
Inventory Management



Material Handling
Inspecting / Maintaining

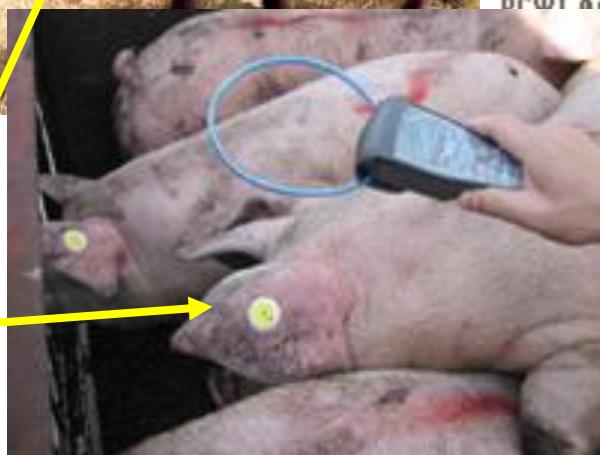
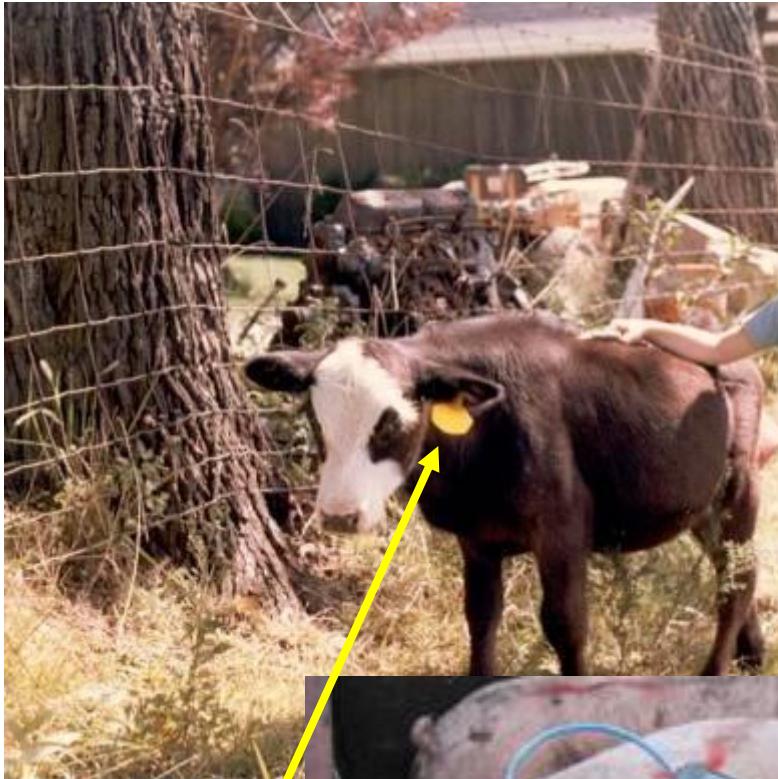
*Has this been repaired?
Is this under warranty?
Has this been inspected?
Is this complete?
What is the asset's status or state?*

Logistics Applications



- ▶ Electronic receipt & dispatch
- ▶ Wrong destination alert
- ▶ Electronic marking
- ▶ Pallet/container item tracking

Livestock Tagging



China Tags Pigs with RFID for the First Time



Bhagaban, New Delhi, INDIA
May 24 2006, 8:57 am GMT

[SendMess](#) [AddFriend](#)

[DROWT Australia](#)

Thickness Gauges to test
on most substrates.

[Eureka RFID](#)

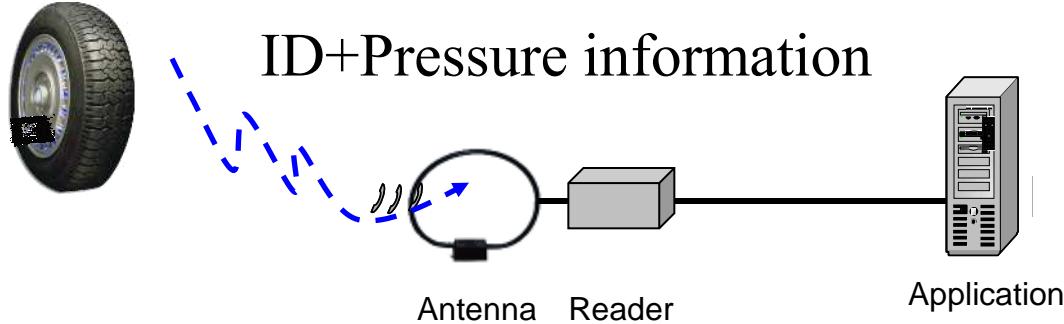
Professional RFID solutions &
manufacturers of RFID systems

Ads by Google

First time, China extensively used the RFID technology on pigs. The growing economy China what the reports say far behind RFID tagging markable step and fixed RFID tags on 1000 tags. The leading pig processing company Sichuan Chunyuan was in charge of the Chinese program. The company attached RFID tags on pig's ear. These are capable of data transformation.

Ear tag for identification.

Other Sensor based RFID System Applications



ID+Pressure
information



ID+ Temperature
information

RFID for Hospital



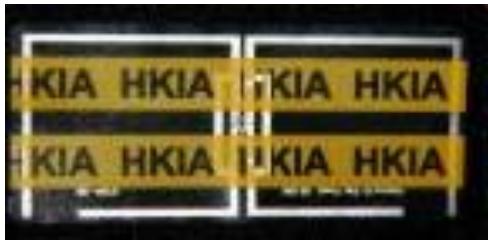
HK airport to deploy RFID

- Motorola has won a three-year contract to supply Hong Kong International Airport with up to **70 million** RFID-enabled IATA standard 21-inch RFID baggage tracking tags
- Specific to this baggage tag award, Motorola has teamed with Avery Dennison RFID for the AD-833 inlay and Print-O-Tape for the baggage tag.
- Unlike bar code-only tags, which require the scanner to be in the line of sight to read the tag, the **EPC Gen2**-enabled RFID bag tags can be read at long distances and without direct contact.



HK Airport RFID Tag Format

Tag Memory Size: 256 bits



Adopt EPC class 0+ label, 256 bits

1. 10 digits license plate number
 2. 10 digits fallback number
 3. Flight number
 4. Carrier ID
 5. Date (6 digits)
 6. 1st destination
 7. 2nd destination
 8. final destination
 9. Class
 10. Security
 11. Passenger name

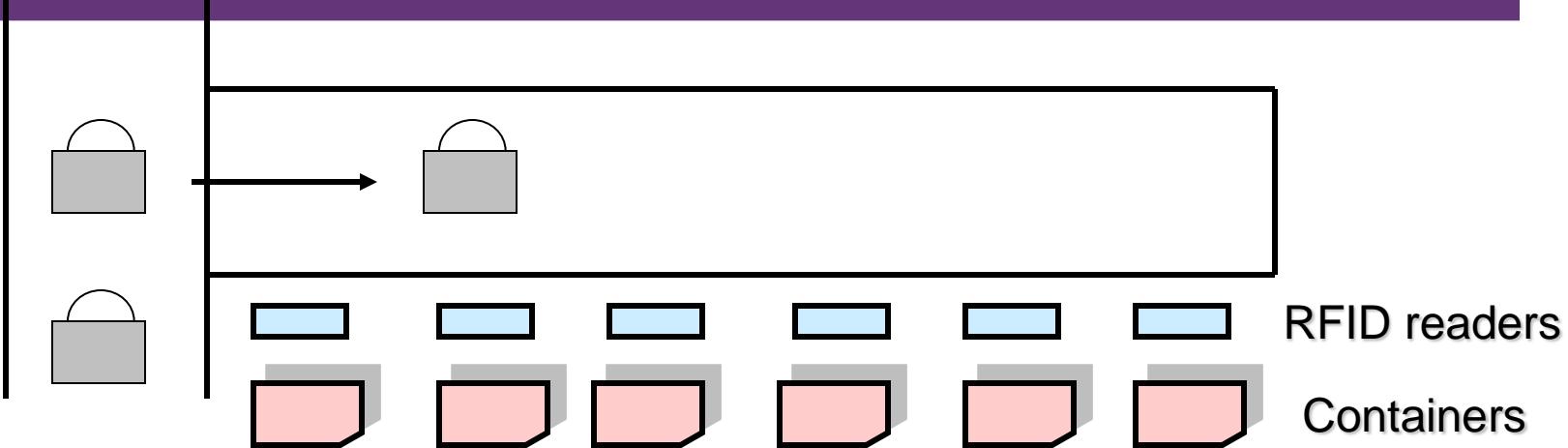
Memory Register ID2:

0	7	9	42	43	51	52	55	56	89	90	103	104	119	120	127
Header 8 bits	0	10 digit UID/FLPN 34 bits	Date 9 bits	Year 4 bits	10 digit LPN 34 bits	Flight # 14 bits	CRC 16 bits	Reserved 8 bits							

Memory Register ID3:

0	7 8	28 29	43 44	58 59	73 74	78 79	108	109	110	112	127
Header 8 bits	Carrier ID 21 bits, 7 bit ASCII	First Destination 15 bits	Second Destination 15 bits	Third Destination 15 bits	Class 5 bits	Passenger Name 30 bits	Security 2 bits	0	CRC 16 bits		

RFID for the Airport

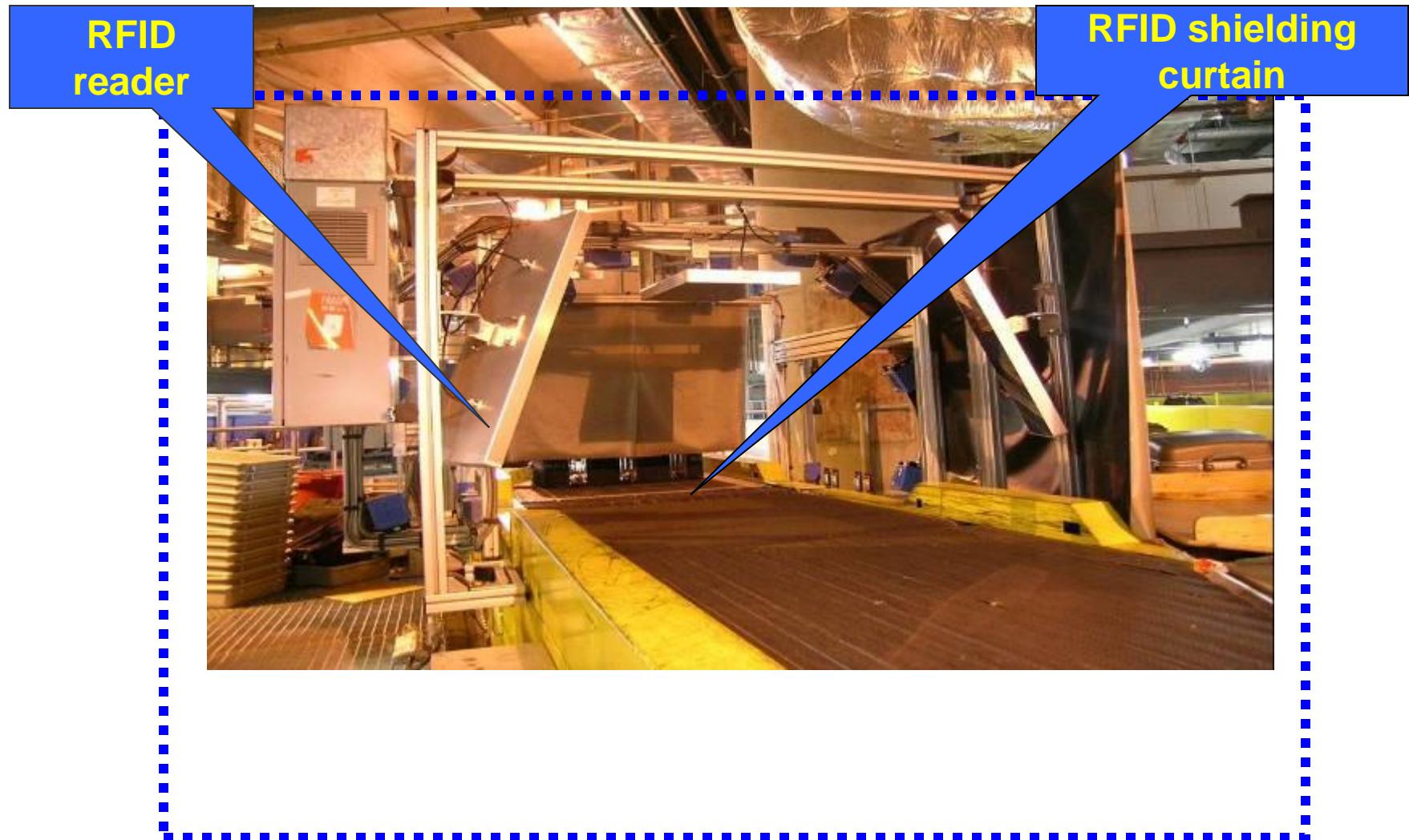


RFID Readers at Lateral



RFID Reader at Lateral

RFID for the Airport



RFID for the Airport – Carousel RF Readers

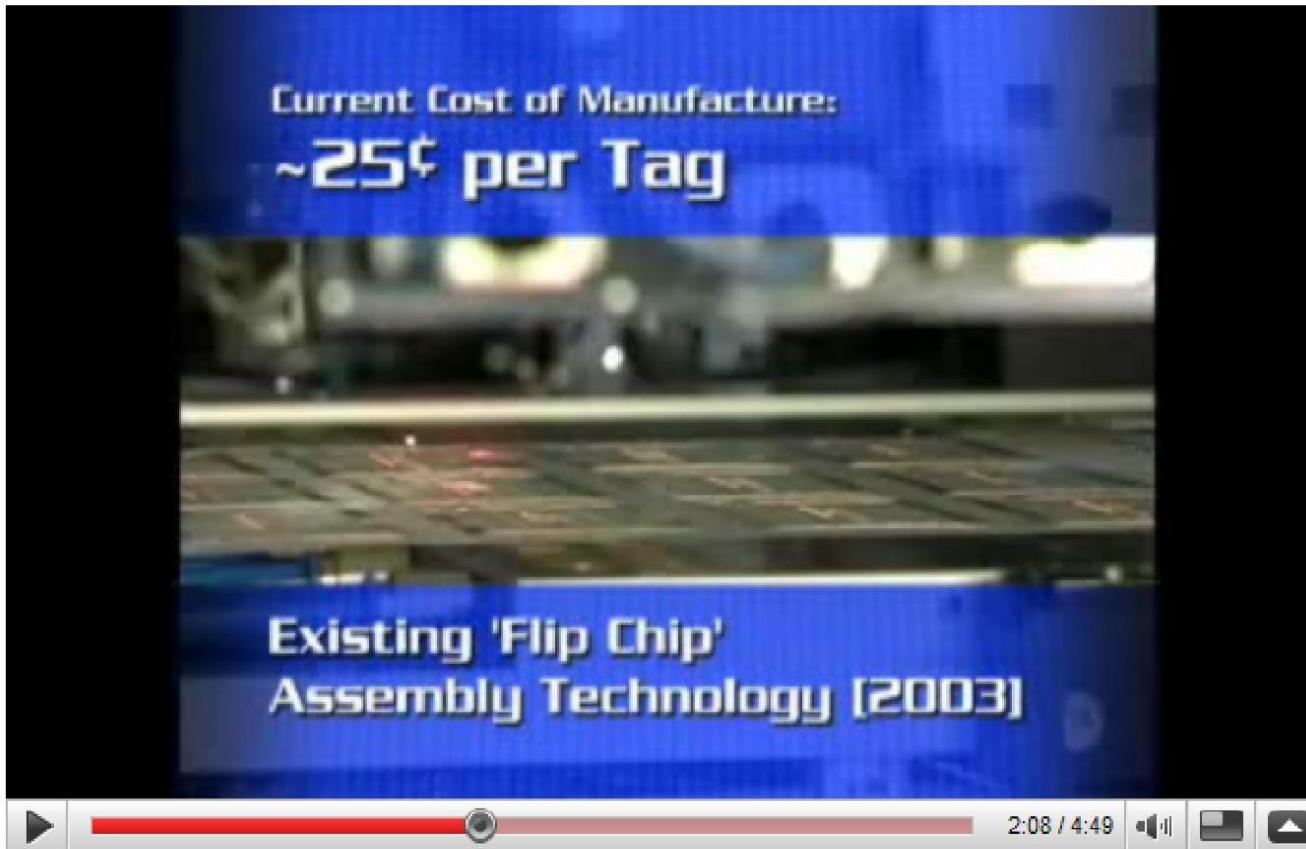


RFID
reader

Light
indicator
on ATL
status

Future Development of RFID

- [http://www.youtube.com/watch?v=Ztfh5TExc_A
&feature=related](http://www.youtube.com/watch?v=Ztfh5TExc_A&feature=related)



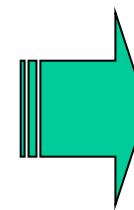
Information from the video

- Tag the World
- RFID can provide $2^{96} = 79$ trillion trillion Unique ID
- Reading speed: 1000 tags/sec or 100 tags at 10mph in 1 sec
- Shrink the size
 - Reduce to 650 microns per tech
 - Antenna: 0.2 inches
- Reduced cost:
 - Existing technology: 25 cents per tag
 - Reduced cost: 5 cents per tag
- → Reduce size → cheaper
- New production technology:
 - Multiple chip direct transfer from wafer to antenna
 - High speed Z-axis conductive adhesive
 - Massively parallel assembly
- → Can produce 1.2 Million to 30 million units per hour
 - (or 150 Billion tags a year)

Smart Dressing Mirror



Smart Dressing Room



Summary

- Businesses can obtain a competitive advantage:
 - By enhancing the information flow between itself and its environment.
 - By digitizing information and automating processes, it is possible to reduce cost and therefore increase productivity and profit.

$\text{Profit} = \text{Revenue} - \text{Cost}$

Technologies for B2C (e.g. Web2.0)

Technologies for B2B (2.g. RFID)

- The old model of managing supply chains is broken
- Business cannot only rely on raising prices nor dramatically increasing sales
- Alternative solution: reducing costs across the supply chain.

Q&A

ELEC2544

e-Commerce and FinTech

Lecturer: Dr. Wilton Fok

Dr. Victor Lee

ELEC2544 e-Commerce and FinTech

- Lecturer: Dr. Wilton Fok
- Room 703, Chow Yei Ching Building
- Tel: 3917 8490
- e-mail: wtfok@eee.hku.hk

- Lecturer: Dr. Victor Lee
- Room 522, Chow Yei Ching Building
- Email: csvlee@eee.hku.hk
- <https://www.eee.hku.hk/~csvlee/>
Tel.: 3917 7098

Objectives:

- introduce basic technical knowledge on electronic commerce and financial technology.
- introduce different e-commerce models: B2C and B2B model and overview different enabling technologies e-Commerce and FinTech such as the location base technology, RFID, GPS, e-payment, server-side and channel security, Near Field Communication, QR Code, augmented reality and other latest technologies deploying in the industry.
- the latest trend and the way forward of e-commerce and Fintech in Hong Kong and overseas will be discussed

Syllabus:

- E-Commerce Introduction, Different business models of e-Commerce: B2C, B2B Model; enabling technologies: QR Code, RFID, Electronic Data Interchange, Location based technology: GPS technology, network based location detection, accelerometer, digital gyroscope, Introduction to security technologies: Client-side Security, Firewall and functions, virus and protection; Server-side Security; Communication Channel Security; concept of symmetric and asymmetric encryption, Public key and private key pairs, hash function, digital signature; WiFi security risks and safety measures, Two factors authentication,
- Financial Technology: Electronic Payment; digital cash, Introduction to block chain, contact and contactless payment card, payment gateway, on-line services, NFC phone payment, Technical Analysis for stock market prediction: Moving Average, Relative Strength Index (RSI), MACD, Data Analysis, Introduction to Artificial Intelligence for Financial application

Assessment Scheme:

- 30% Assignment
 - Group Presentation
- 70% written examination in May
 - In the format of multiple choices, short questions
 - Details will be announced shortly

Part A: 30% Group Presentation

- Form a group of 5 students and present 15 minutes (3 minutes each) on a topic relating to e-Commerce and/or Mobile commerce.
- The group should submit:
 - Powerpoint softcopy on or before 1 May 2019
 - Hardcopies of the presentation slides (6 slides in 1 page to save paper) and the written report and submit to Dr. Fok during the presentation
 - Each member should specify his/her contributions in this group project
- Presentation dates: late Apr 2019
- Submit your group number, full name and UID of the group members and topic of your presentation to Dr. Joe Yuen via e-mail chyen@eee.hku.hk on or before 14 Feb 2019

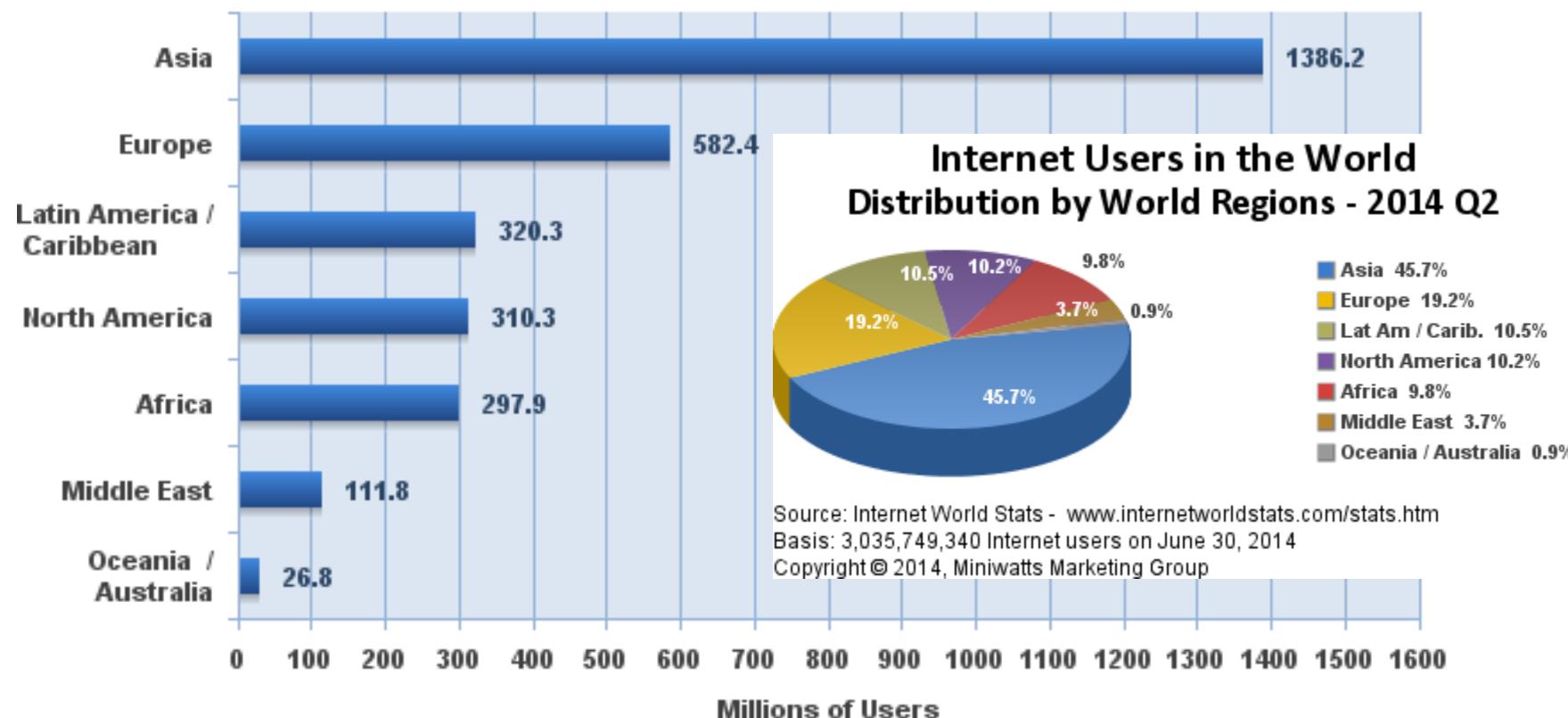
Evolution of e-commerce

- Internet was created in 60's as global network of computer networks.
- Before 90's, it was used by academic and researcher
- There was no central control, authority, or ownership, but according to some, the Internet could change the fundamental way business is done.
- Since mid 90's, Internet has seen an exponential growth in use.
 - No. of Internet hosts grew from one million in 1993 to 350 million in 2005
 - While 12% of US homes had broadband connections in early 2004, this figure increased to 30% by late 2005
 - → lead to the growth of Internet Commerce (= Electronic Commerce)
- Internet offers an immediate channel to a global market



Internet users in the world by Geographical Regions -2014 Q2

Internet Users in the World by Geographic Regions - 2014 Q2

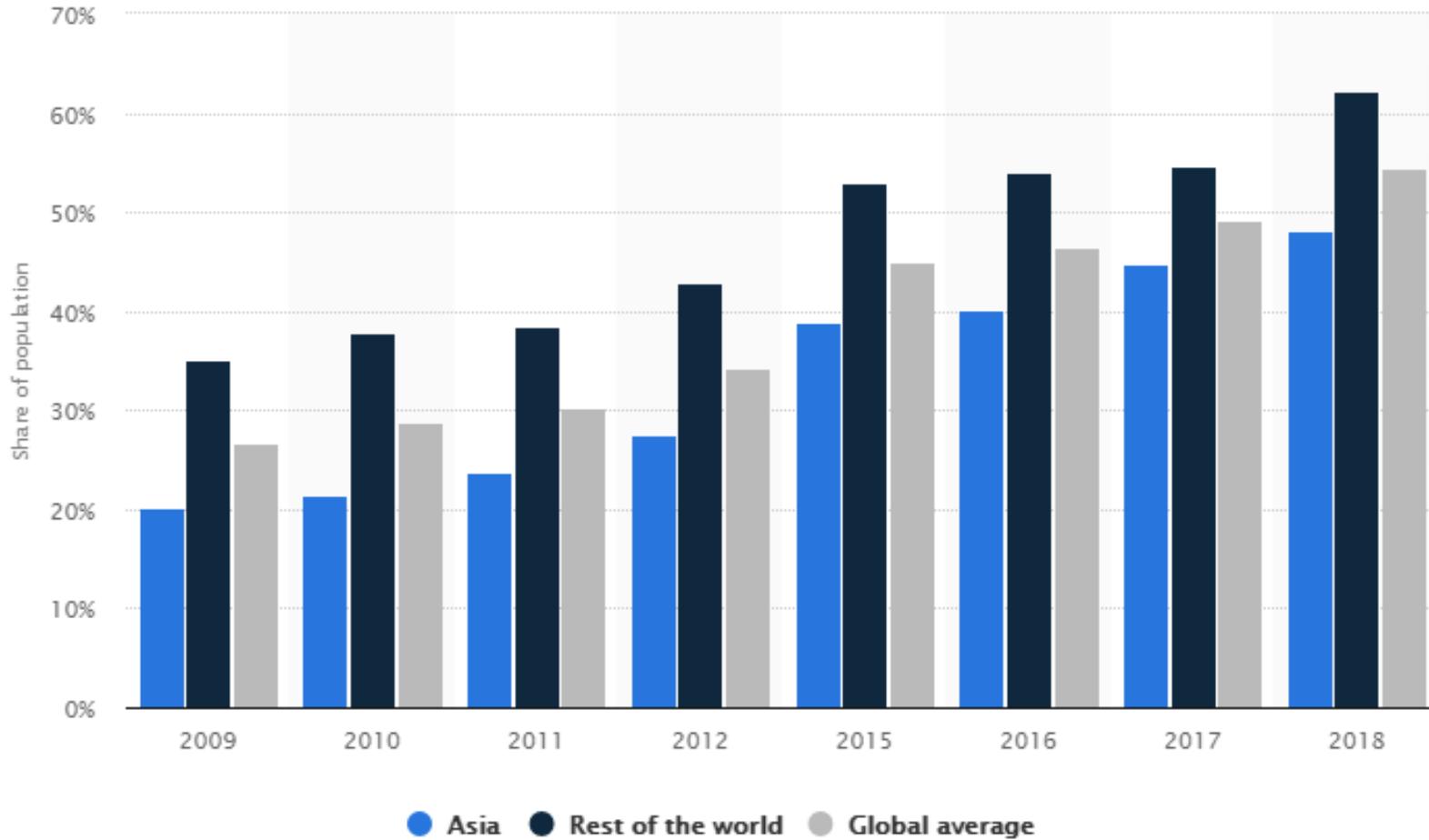


Source: Internet World Stats - www.internetworldstats.com/stats.htm

3,035,749,340 Internet users estimated for June 30, 2014

Copyright © 2014, Miniwatts Marketing Group

Internet penetration rate in Asia compared to the global penetration rate from 2009 to 2018



Growth of commercial use of the Internet

- Two reasons for a business to get involved in e-Commerce:
 - The ability to reach new customers through Internet to the global market place, and create a more intimate relationship with customers by sharing more information.
 - Drastic cost reductions for distribution and customer service.

Revenue ↑

Cost ↓

$$\text{Profit} = \text{Revenue} - \text{Cost}$$

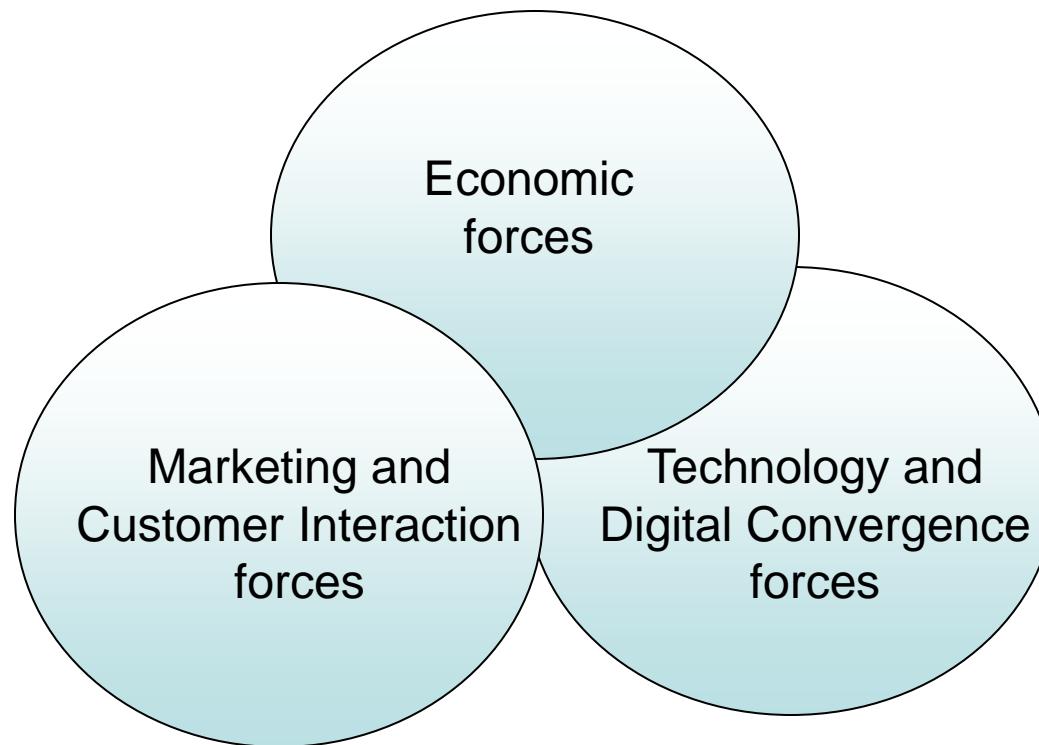
Ref: Treese, G.W, Stewart, L.C, Designing Systems For Internet Commerce, Addison Wesley, 1998, pp 8

Growth of commercial use of the Internet

- While Internet brings new technology and new capabilities to business, the same business problems remain the same
 - you need something to sell,
 - make it known to potential buyers,
 - accept payment,
 - deliver the product or service,
 - and provide appropriate after the sales service.
- So what is driving the interest in Electronic Commerce?

1.2.1 Three main forces fuelling interest in electronic commerce

- There are 3 main forces fuelling interest in electronic commerce



Source: Kalakota, R. Whinston, A., Electronic Commerce – A Manager's Guide, Addison-Wesley, 1997, pp7–11.

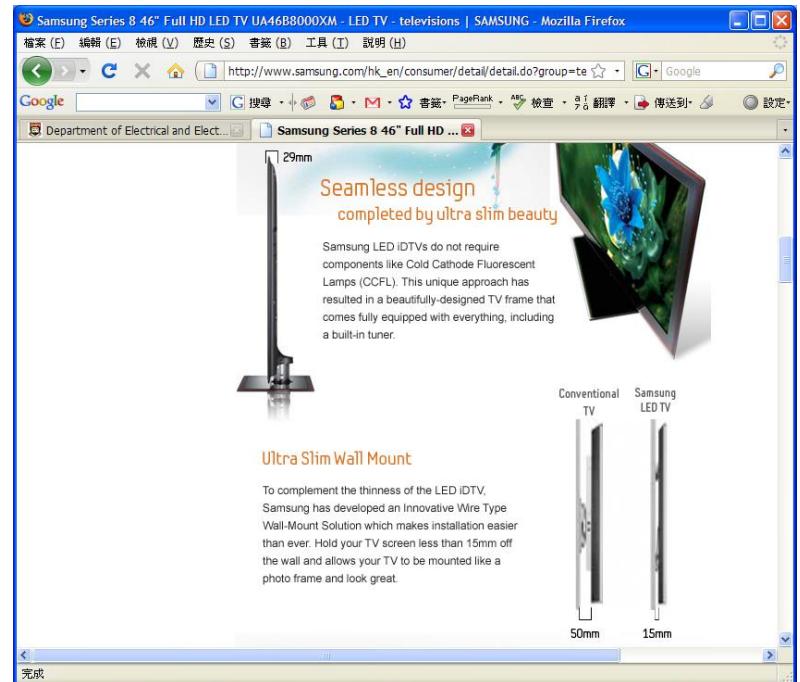
A) Economic forces

- Businesses today are under great pressure to reduce costs and stay competitive.
- Electronic commerce offers low-cost yet accurate electronic transactions with trading partners, low-cost global advertising, and alternatives to expensive customer service call centres.



B) Marketing and Customer Interaction forces

- Business may also implement an Internet presence to market their products to specific markets and improve customer support channels.
- With the use of a website, businesses could offer more product or service information than that provided in television or full-page print-media advertisement.



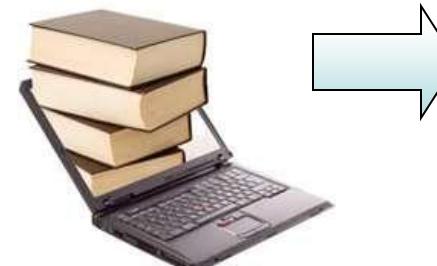
C) Technology and Digital Convergence

- Many businesses are reengineering themselves to take advantage of the Internet as a delivery channel.
- Documents stored in digital form or even video, images and audio can now be broadcast as multimedia streams over the Internet.



C) Technology and Digital Convergence

- Electronic commerce and the popularity of digital media are forcing previously unconnected industries into closer contact, generating new competition and co-operation.
 - e.g. Sony Music Entertainment and Universal Music Group, joined with Microsoft to deliver a co-branded MSN Music subscription service.
 - E.g. e-book
 - > Apple – iBook
 - > Amazon - Kindle



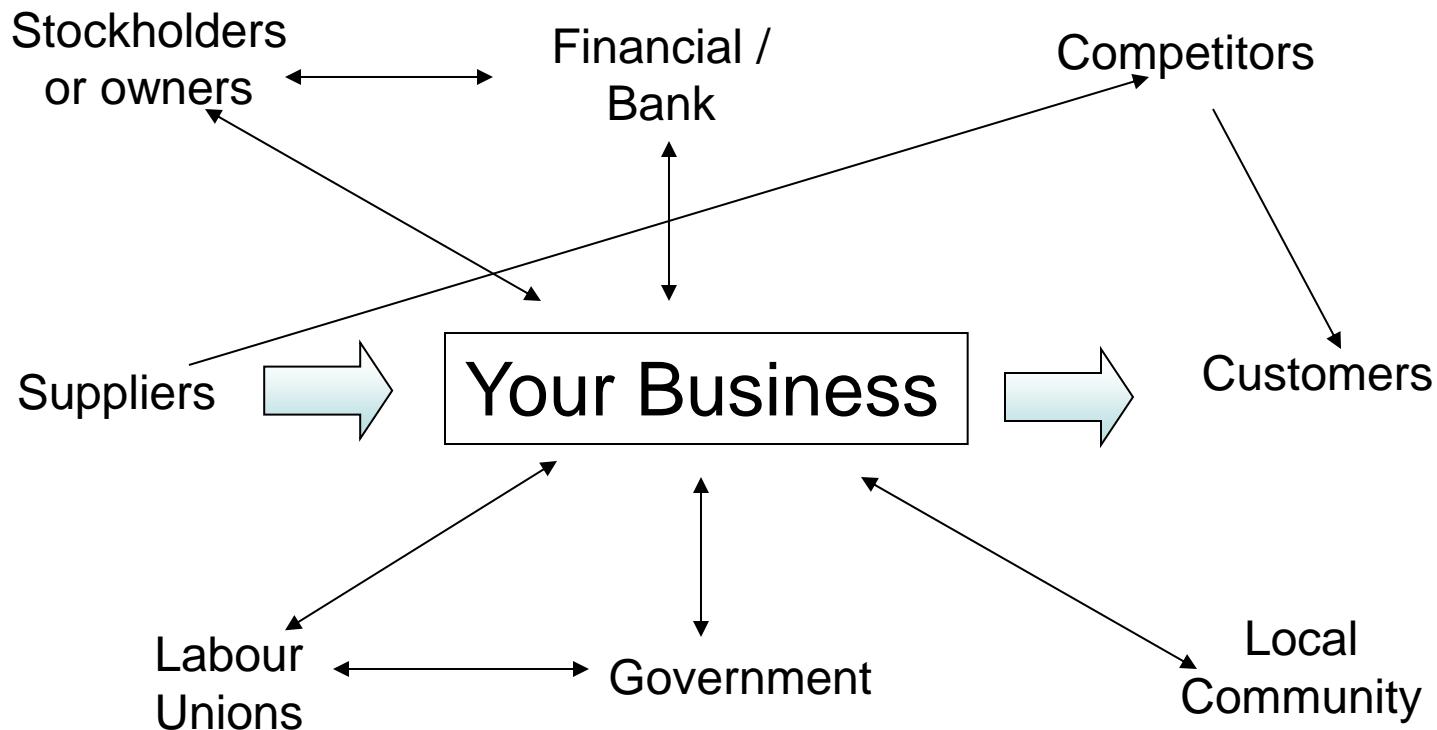
Benefits of e-commerce to business

- Internet offers:
 - **B2C** - Business and customer transactions for home shopping and banking
 - **B2B** - Transactions with trading partners using EDI
 - **Information**
 - > Gathering (Market Research)
 - > Distribution transactions
 - **Workflow** - Developing automated information flow processes
 - **CRM** - New means of providing customer support for new and existing customers
 - **Delivery** – new means of product delivery, e.g. digital products

Benefits of e-commerce to the Value Chains

- Business also use ICT to improve their business systems and enhance their Value Chain, through improved use of information systems.

- 1. Physical Resource Flows - People, Materials, Machines, and Money
- 2. Conceptual Resource Flows - Data and Information



Benefits of e-commerce to the Value Chains

- For every physical flow, there are a few (even many) associated information flow
- Efficient management of information flows can create a competitive advantage in the value chain
- Help to generate more new businesses, and retain existing business, through the Four key components in the e-Commerce Value Chain

If e-commerce is so good, why dot.com bubble burst?

- In 2000 the industry experienced a massive downturn known as the dot com burst.



URL: hku.iCLASS.hk

Join the course: (code: JQ8408)

- Click the question “Why dot.com bubble burst?”
- Click the submit button after entering the keyword



A screenshot of the iCLASS web interface. At the top, it shows the Hong Kong University crest, a user profile picture, the name Fok Wilton Wai Tung, and an 'Edit' button. Below this, a modal window titled 'e-commerce' is open. The modal contains three items: 'Class profile survey' (with a circular icon), 'Give example of e-commerce and mobile commerce (wipe the screen for different category)' (with a clipboard icon), and 'Peer Review' (with a hand icon). There are also 'Add', 'Sort', and 'Edit' buttons at the top of the modal.

Top 10 dot com flops

- MSN list their Top 10 dot com failure:
 - http://msn-cnet.com.com/4520-11136_1-6278387-1.html?part=msn-cnet&subj=re_6278387-1&tag=tg_nl

The screenshot shows a Microsoft Internet Explorer window displaying a CNET.com article titled "Top 10 dot-com flops". The page features a banner for CNET's 10th anniversary and a sidebar with various links like "TRADE IN YOUR GEAR", "SEE YOUR DREAM GADGETS", and "READ OUR TOP 10 LISTS". The main content highlights Webvan as the first flop, describing its rapid growth and subsequent collapse. An advertisement for Dell Inspiron 1521 notebooks is visible on the right.

Top 10 dot-com flops

By Kent German

The most astounding thing about the dot-com boom was the obscene amount of money spent. Zealous venture capitalists fell over themselves to invest millions in start-ups; dot-coms blew millions on spectacular marketing campaigns; new college graduates became instant millionaires and rushed out to spend it; and companies with unproven business models executed massive IPOs with sky-high stock prices. We all know what eventually happened. Most of these start-ups died dramatic deaths. These are the celebrity victims of the new-economy bust. You can avoid giving a flop as a gift this holiday. Take a look at the CNET [Holiday Gift Guide](#).

1

Webvan (1999-2001)

A core lesson from the dot-com boom is that even if you have a good idea, it's best not to grow too fast too soon. But online grocer Webvan was the poster child for doing just that, making the celebrated company our number one dot-com flop. In a mere 18 months, it raised \$375 million in an IPO, expanded from the San Francisco Bay Area to eight U.S. cities, and built a gigantic infrastructure from the ground up (including a \$1 billion order for a group of high-tech warehouses). Webvan came to be worth \$1.2 billion (or \$30 per share at its peak), and it touted a 26-city expansion plan. But considering that the grocery business has razor-thin margins to begin with, it's not surprising that Webvan's growth proved unsustainable.

THE NEW INSPIRON™ 1521 NOTEBOOK. FREE UPGRADE: 2GB Memory* AND 160GB* Hard Drive
\$749
Click Here! [HEY, GET IT HERE ▶](#)

DELL YOURS IS HERE

Some offers end 8/8

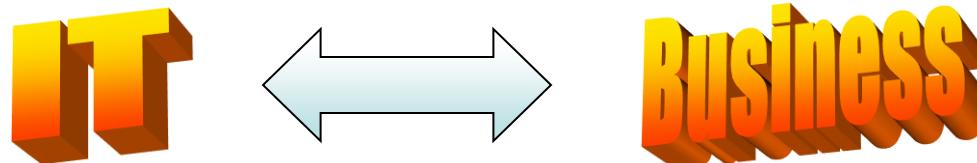
http://adlog.com/adlog/c/r=8693&s=664714&o=33-11136_1&h=ch&p=8&b=1&l=en_US&site=1&pt=4520&nd=11136&pid=&cid=6278387&pp=100&e

Why dot.com failed?

- Most dot com companies failed simply because they didn't create a incoming revenue stream that match the outgoing revenue stream!

Summary: benefits of e-commerce to business

- The Internet provides business with means to **inexpensive** and **fast worldwide** communication.
- Business can obtain a competitive advantage by enhancing the information flow between itself and its environment.
- By digitizing information and automating information processes, it is possible to **reduce cost** and **increase productivity**
- As the use of information technology in business increases, so does the need for understanding the nature of the technology, and the way it can be best employed to **maximize the effectiveness of information flows between business functions**.



Summary: benefits of e-commerce to business

- The real value of e-Commerce is:
 - Optimizing conceptual flows (Information)
 - Cheap communication costs
 - Automating systems
 - Strengthening relationships with trading partners
 - Reducing costs
 - Adding value to existing systems
 - Making systems and messages available to customers

Mobile Commerce



What's Mobile Commerce?

- Wikipedia definition:
 - Mobile Commerce is the ability to conduct commerce, using a mobile device e.g. a mobile phone (cell phone), a PDA, a smartphone and other emerging mobile equipment such as e-book, iPad.
- Source:
 - http://en.wikipedia.org/wiki/Mobile_commerce

What's Mobile Commerce?

- "Mobile Commerce is any transaction, involving the transfer of ownership or rights to use goods and services, which is initiated and/or completed by using mobile access to computer-mediated networks with the help of an electronic device.“
 - Tiwari, R. and Buse, S. (2007): The Mobile Commerce Prospects: A Strategic Analysis of Opportunities in the Banking Sector, Hamburg: Hamburg University Press

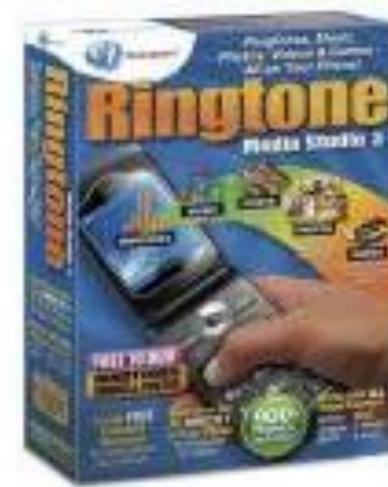
Evolution of m-commerce

- 1997: Mobile phone enabled Coca Cola vending machines in Finland used SMS to send the payment to the vending machines.
- Merita bank of Finland also used SMS for m-banking



Evolution of m-commerce

- In 1998, the first digital content sales:
 - 1st commercial downloadable ringing tones were launched



Evolution of m-commerce

- In 1999, two major national commercial platforms for m-commerce were launched:
 - national m-payments system by Smart as Smart Money in the Philippines
- 1st mobile internet platform by NTT DoCoMo in Japan, called i-Mode.
 - i-Mode was revolutionary also in offering a revenue-sharing deal
 - NTT DoCoMo only kept 9% of the content payment and returned 91% to the content owner.



Evolution of m-commerce

- 2000
 - Norway launching mobile parking
 - Austria offering mobile tickets to trains
 - Japan offering mobile purchases of airline tickets.



Evolution of m-commerce

- Since then...
 - PDAs and cellular phones have become so popular that many businesses are beginning to use m-commerce as a more efficient method of reaching and communicating with their customers.



Application of mobile phones in our daily life

- TVB Pearl Money Magazine: "Internet/BB"
 - <http://www.youtube.com/watch?v=k7CdZcnZSE>



★★★★★ 1 個評分

觀看次數：1,672

34

Information from the video

- Hong Kong has the highest mobile phone and internet penetration
 - 120% penetration rate
 - 8 millions mobile phone for 7 millions of pollution (including elderly and babies)
 - 70% household own internet connected computer
 - Household expenditure on computer and information rose 13.5% (from 2006-2007)
- Applications
 - searching for information, e.g. On-line magazine
 - social communication, e-mail/Chat, On-line networking
- Reasons for its popularity
 - Technical reasons: Availability of free WiFi assess and cheaper connectivity cost
 - Human reasons: Using e-mail / internet us now becoming habitat, like an additive behavior, e.g. alcohol and tobacco

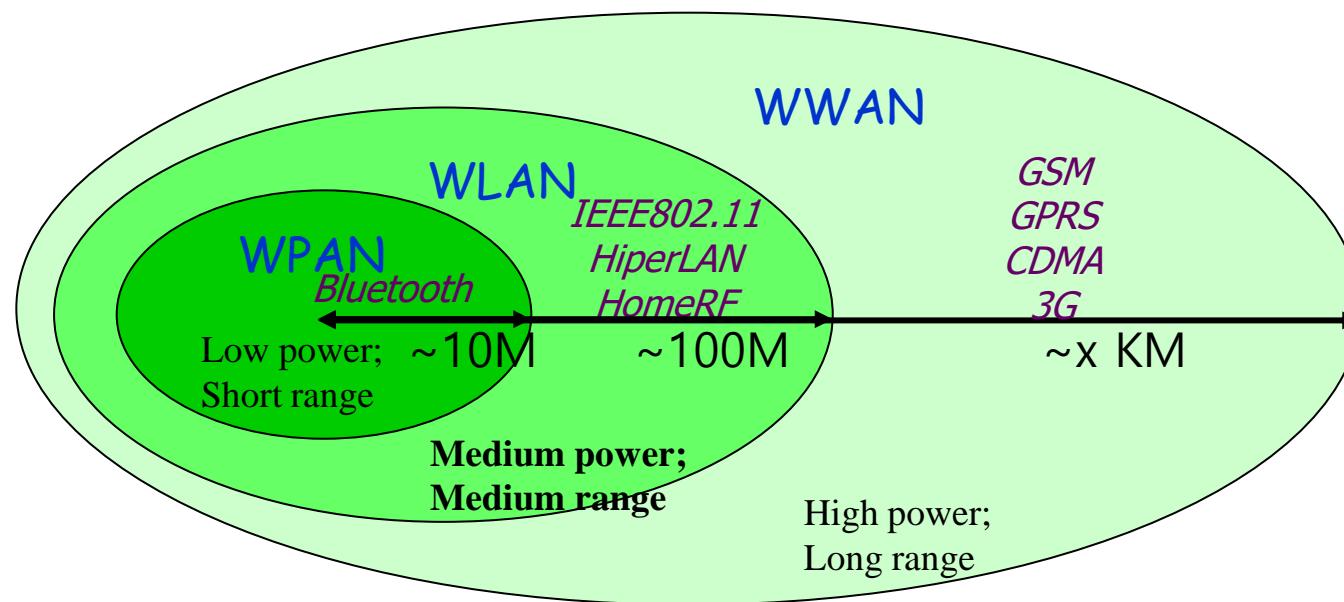
Technology evolves and it evolve our lifestyle!!

What are the m-commerce technology?

- Basic mobile technologies (Connectivity)
 - Bluetooth
 - WiFi
 - GSM
 - GPRS
 - 3G
 - LTE (Long Term Evolution) (4G)
 - WiMax

Basic mobile technologies

- Many mobile devices will support multiple wireless technologies (I.e. GPRS, 3G , WiFi & Bluetooth)
- Classification of mobile technologies according to the coverage:
 - PAN – Personal Area Network
 - LAN – Local Area Network
 - WAN – Wide Area Network



What are the m-commerce technologies?

- Extended/ related technologies
 - QR Code
 - RFID (Radio Frequency Identification)
 - NFC (Near Field Communication)
 - GPS
 - Location base system
 - M-Payment
 - Augmented Reality

- Zigbee
- Geographical Information System (GIS)
- RF SIM
- e-Certificate / m-cert

**Draw a e-commerce/
Mobile commerce
application**



URL: hku.iklass.hk

Join the course: (code: VF1291)

- Draw a mobile commerce application or business model
- Click the submit button after drawing



A screenshot of a mobile application interface. At the top, there's a header bar with the university crest, a user profile picture, the name 'Fok Wilton Wai Tung', and an 'Edit' button. Below the header, a blue navigation bar contains the text 'e-commerce' and icons for 'Add', 'Sort', and a camera. The main content area displays three items: 'Class profile survey' (with a circular icon), 'Give example of e-commerce and mobile commerce (wipe the screen for different category)' (with a clipboard icon), and 'Peer Review' (with a hand icon). The background of the app has a light grey grid pattern.

M-Commerce Models

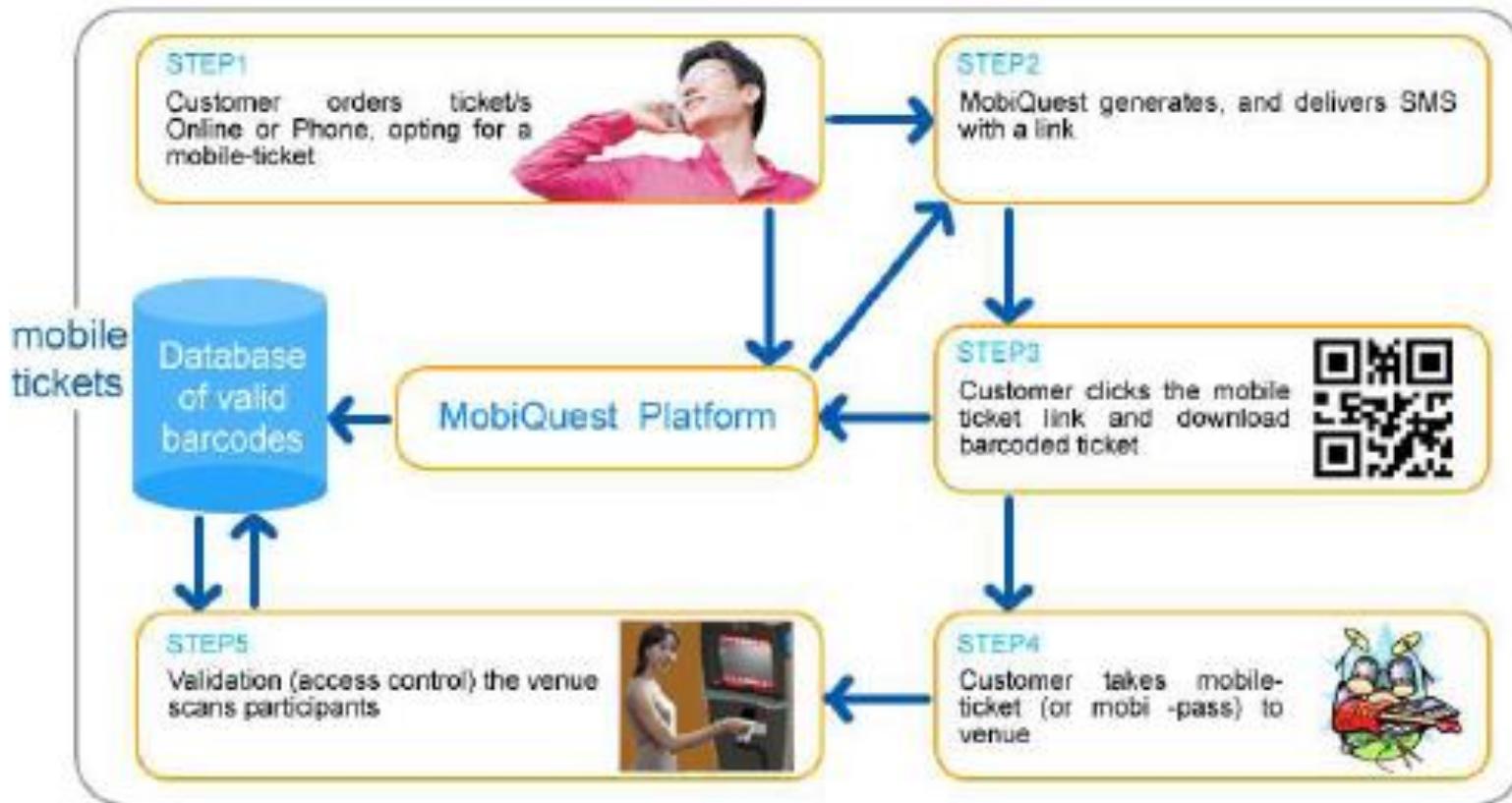
- Revenue Generation
 - Mobile vouchers, coupons and loyalty cards
 - Content purchase and delivery
 - Location-based services
 - Information Service
 - Mobile marketing and advertising
 - Mobile Applications
- Operating cost reduction
 - Mobile ticketing
 - M-banking
- New channels/services
 - Mobile brokerage
 - Auctions
 - Mobile Shopping

Mobile ticketing

- Tickets can be sent to mobile phones using a variety of technologies.
- Users are then able to use their tickets immediately by presenting their phones at the venue.
- Tickets can be booked and cancelled on the mobile with the help of simple application downloads or by accessing WAP portals.
 - E.g. Air ticket, train ticket, parking coupon



Mobile ticketing

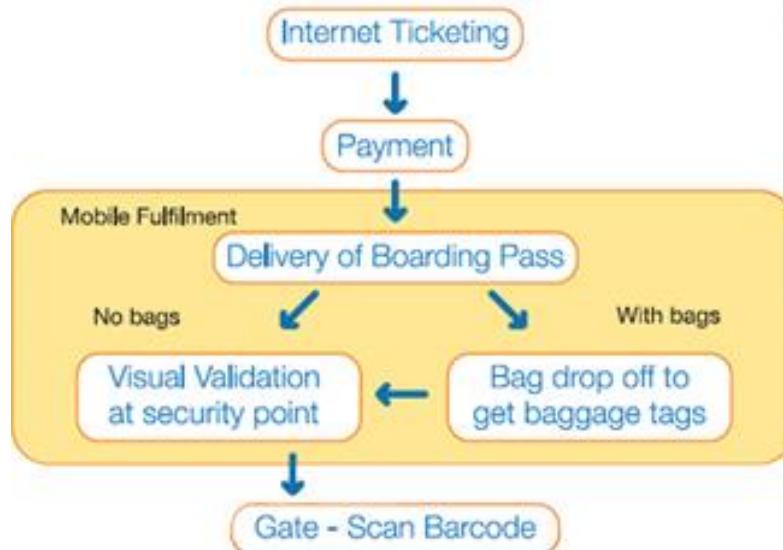


Event: Asia Communica
Event Date: 12/Dec/09
Venue: Singapore



Mobile ticketing

- Mobile boarding pass



Mobile vouchers, coupons and loyalty cards

- 2D barcode can also be used for the distribution of vouchers, coupons and loyalty cards.
- The voucher, coupon, or loyalty card is represented by a virtual token that is sent to the mobile phone.
- Presenting a mobile phone with one of these tokens at the point of sale allows the customer to receive the same benefits as another customer who has a loyalty card or other paper coupon/voucher.
- Coupons may be sent to a customer utilizing location based services when he is in a certain physical proximity
 - (e.g. passing by a store with a current mobile coupon offer).

Content purchase and delivery

- Currently, mobile content purchase and delivery mainly consists of the sale of ring-tones, wallpapers, and games for mobile phones.
- The convergence of mobile phones, mp3 players and video players into a single device will result in an increase in the purchase and delivery of full-length music tracks and video.



Location-based services

- Unlike a home PC, the location of the mobile phone user is an important piece of information used during mobile commerce transactions.
- Knowing the location of the user allows for location based services such as:
 - local offers
 - local weather
 - people tracking and monitoring



Location-based services

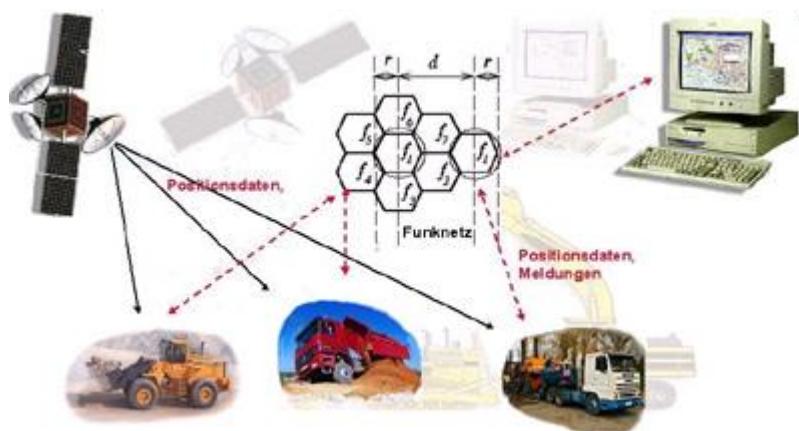
- Mobile phone knows its location
- Access the right customers at the right place
- Applications
 - Target marketing and Royalty program
 - > e.g. E-Coupon, Bonus point program for shopping malls
 - Proactive Direction Sign/ Handheld Information Kiosk to attract customer to walk-in

SMS: Your favourite restaurant is on 3/F
Today Special only
\$38



Location-based services

- Enabling technologies:
 - Geographic Information System
 - GPS
 - Mobile phone cell site positioning
 - WiFi Access Point positioning...etc



Information services

- A wide variety of information services can be delivered to mobile phone users in much the same way as it is delivered to PCs, e.g.
 - news services
 - stock data
 - sports results
 - financial records
 - Traffic information



Mobile banking

- M-Banking : use of mobile commerce to allow bank customers to:
 - access account information,
 - make transactions,
 - > e.g. purchasing stocks, remitting money, via mobile phones and other mobile equipment.



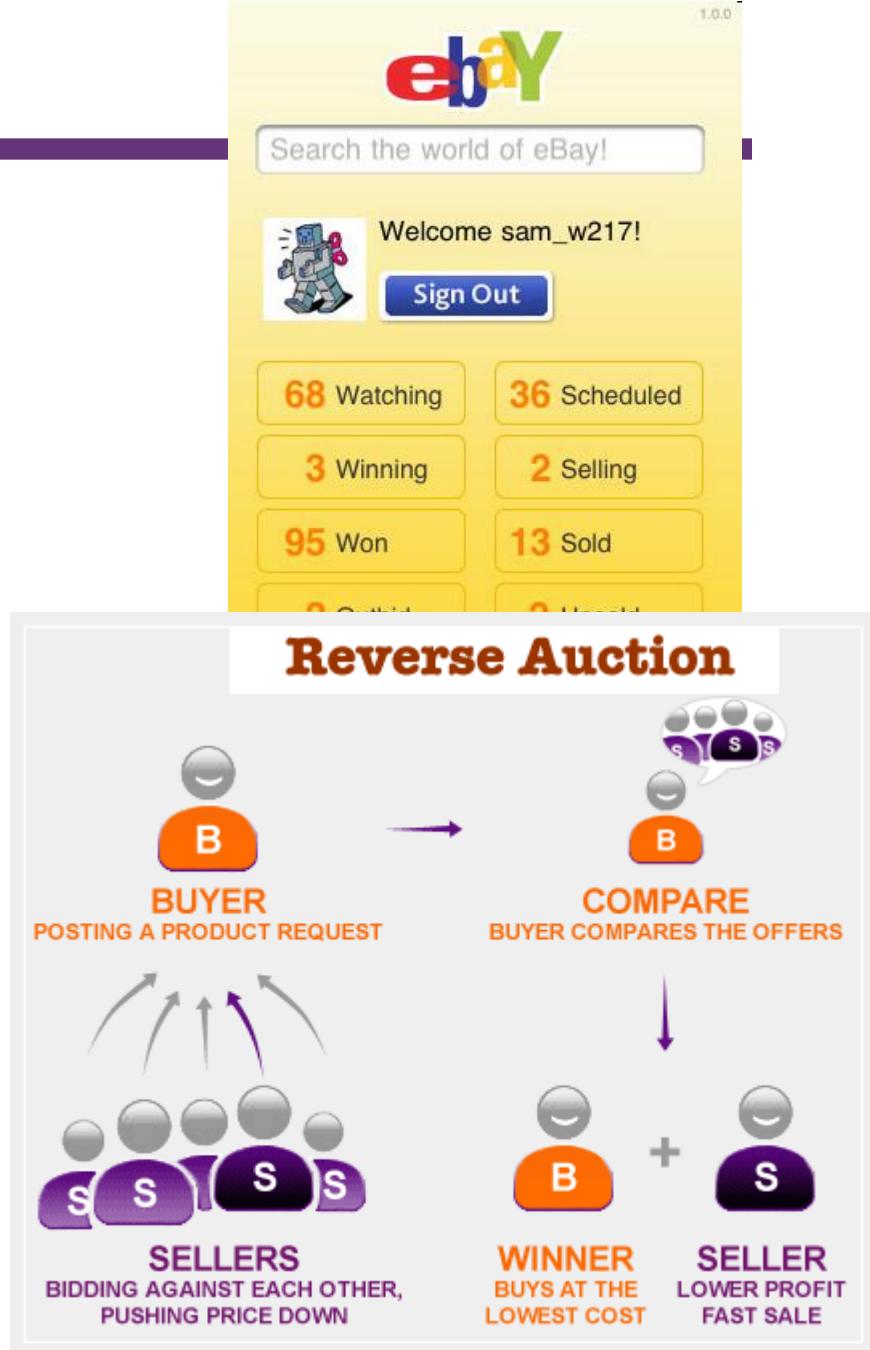
Mobile brokerage

- Stock market services offered via mobile devices have also become more popular and are known as Mobile Brokerage.
 - They allow the subscriber to react to market developments in a timely fashion and irrespective of their physical location.



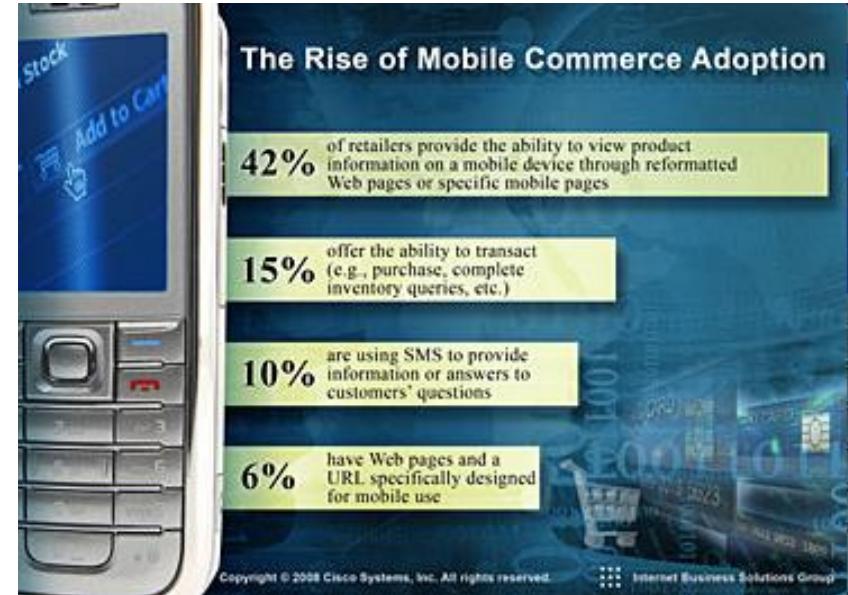
Auctions

- Over the past three years mobile reverse auction solutions have grown in popularity.
- Unlike traditional auctions, the reverse auction (or low-bid auction) bills the consumer's phone each time they place a bid.
- Many mobile commerce solutions rely on a one-time purchase
 - however, reverse auctions are high return applications as they allow the consumer to transact over a long period of time.



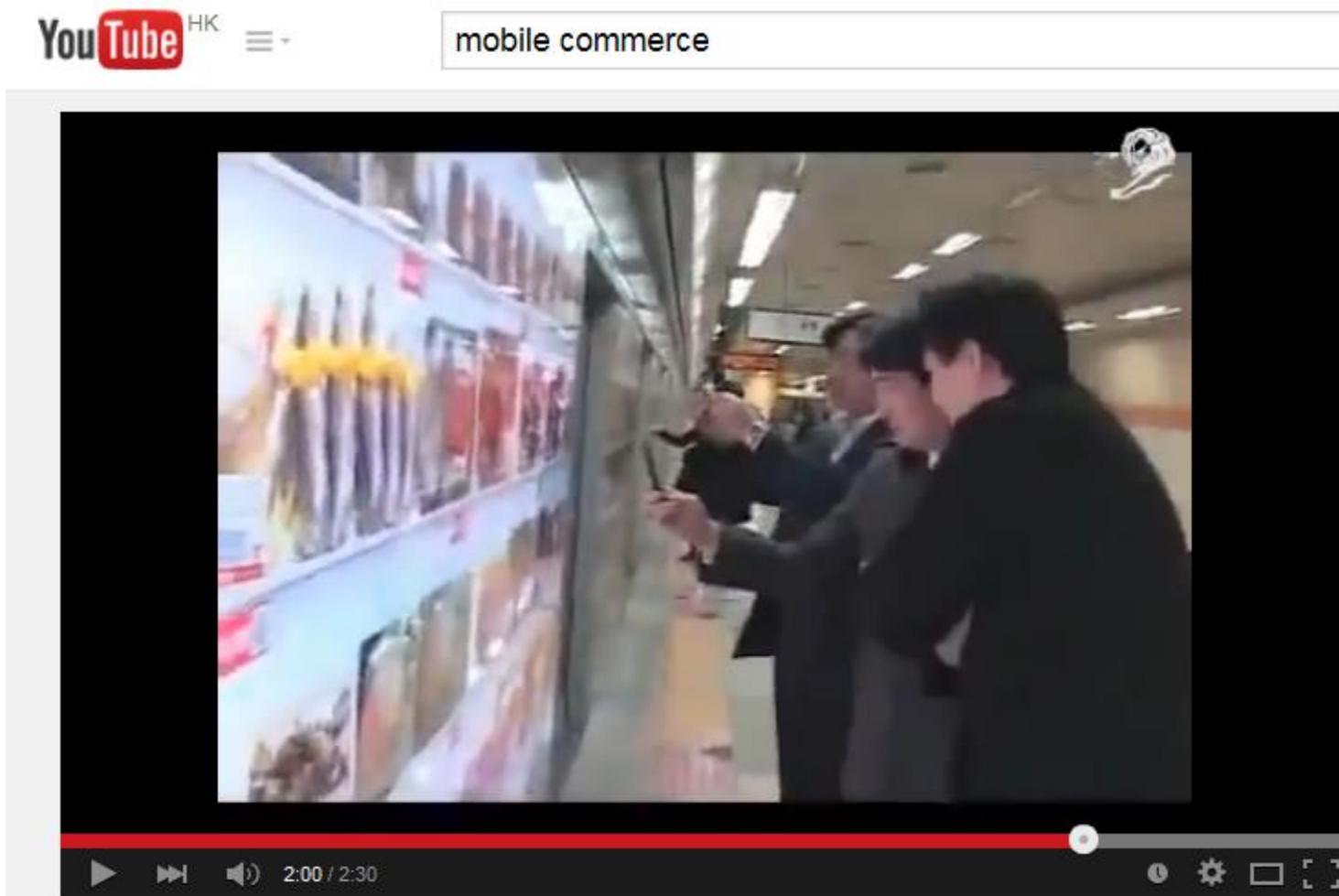
Mobile Shopping

- Instead of using paper catalogues, retailers can send customers a list of products that to their target customers' mobile device or they can visit a mobile version of a retailers ecommerce site.
- Retailers can also track customers at all times and notify them of discounts at local stores that the customer would be interested in.



Shopping with your mobile phone in Korea

- <https://www.youtube.com/watch?v=xxoh4AKGE5M>



Mobile Applications

- M-Commerce also creates a demand of Mobile applications
- Major vendors e.g. Apple, Nokia, Android...etc set up their on-line/mobile market place for developers to sell their apps.



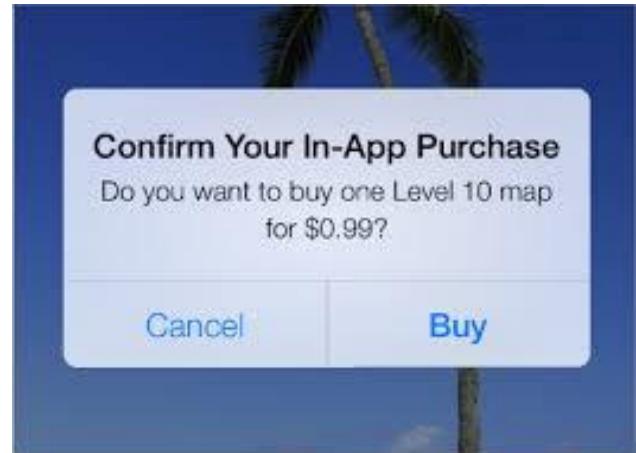
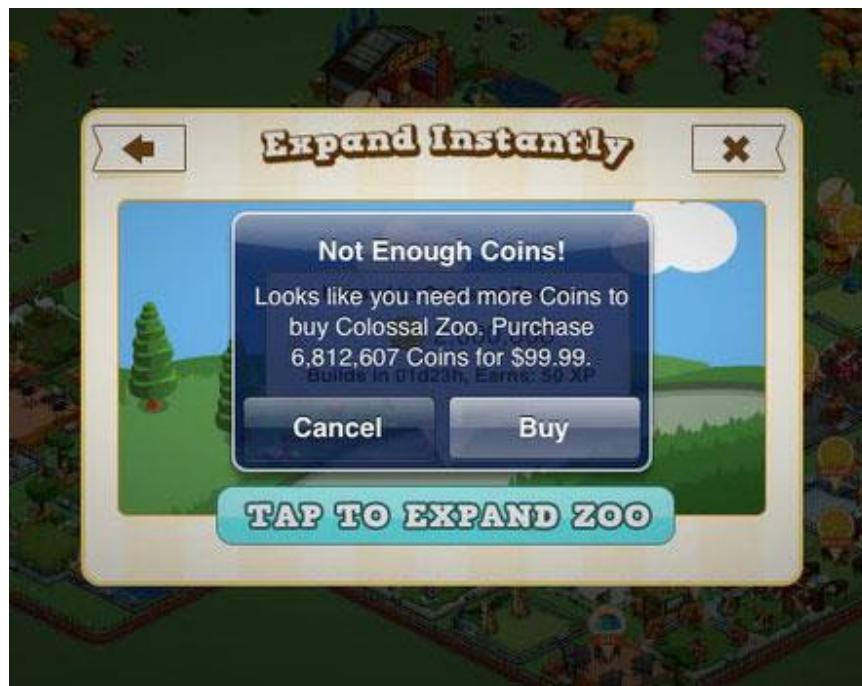
Simple Mobile Apps That Made Millions

- <https://www.youtube.com/watch?v=o-MYvlJ1r-s>



In apps purchase

- Free trial or basic features
- Ask you to pay for upgrade or level rise



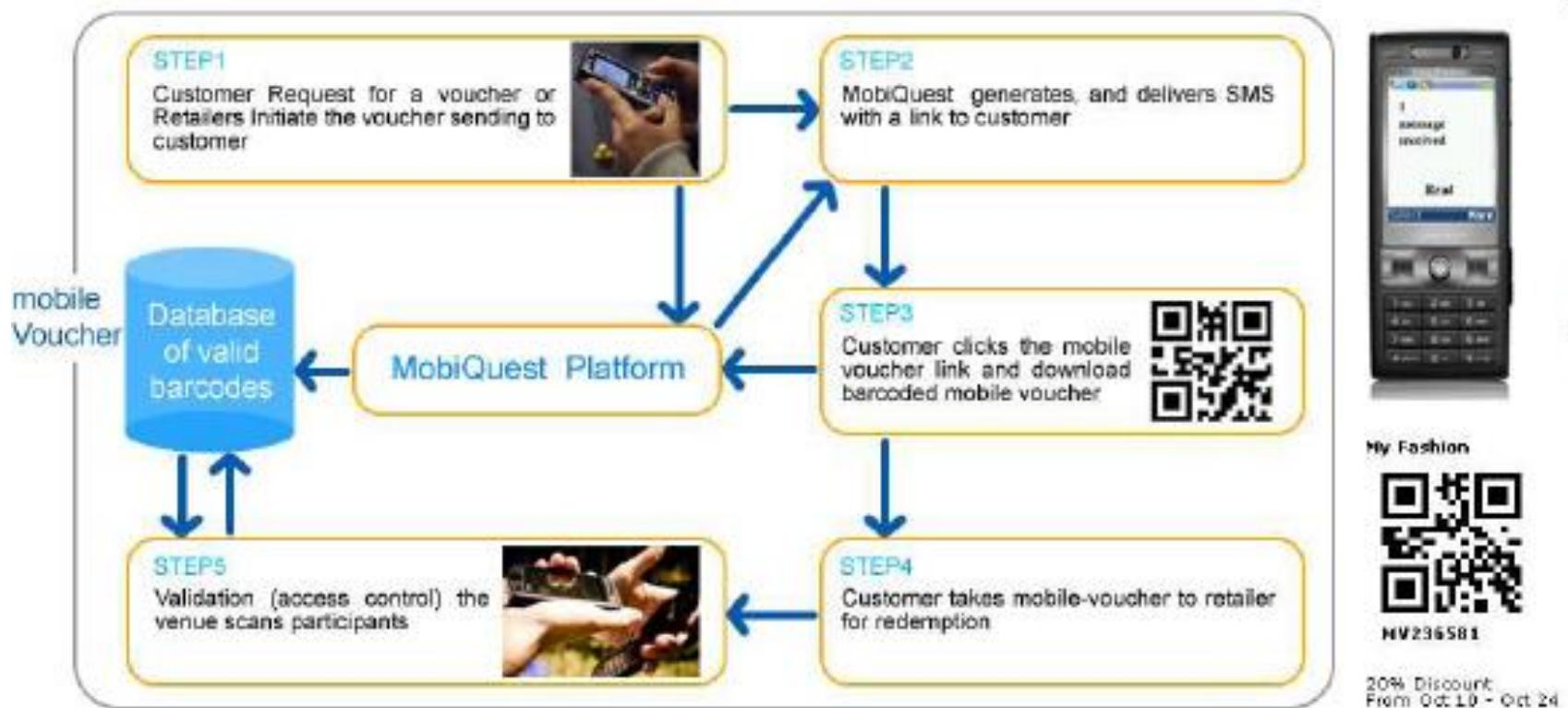
Mobile marketing and advertising

- Mobile marketing is an emerging concept but growing rapidly
- Highly responsive sort of marketing campaign, especially from brands' experience point of view.
- Getting higher campaign response rates
- Corporations are now using m-commerce to expand everything from services to marketing and advertisement.



Mobile marketing and advertising

- Example
 - User request a coupon
 - Service provider send an SMS to the user
 - User click the SMS link to retrieve a 2D barcode coupon
 - User show the 2D barcode at the sales counter to redeem the discount



Mobile marketing and advertising

- In apps ads
 - Developers offer free apps
 - Earn money by iAd banner ads



Mobile Payment Business

- Market Opportunities
 - Monetary transaction is the key for m-commerce
 - Revenue generate from charging % on the transaction, e.g. Credit Card, Octopus
- Market Situations
 - High demand for a security, non-repudiation, confidentiality, integrity, strong authentication & authorization
 - Demand for a “Trusted” organisation to run the business



Mobile Payment Business

- E.g. In early 2000, the market demanded a payment service provider
- Paypal was the early player and they won the market share
- Now the business expands to mobile

The screenshot shows the PayPal Mobile website. On the left, there's a sidebar with links like Overview, Send Money by Phone, Text to Buy, Security and Privacy, FAQ, and Activate Phone. The main content area has a heading "PayPal Goes Mobile" with the subtext "Your money, when you want it—securely". It lists "Send payments by phone" and "Buy stuff with your phone" as features. Below this is a large image of a man and a woman smiling while looking at their phones. A call-to-action button says "Activate Your Phone". To the right, there are sections for "Send money to friends and family" (with instructions for text messaging or calling), "Secure & Private" (mentioning PINs and account security), and "It's free by phone" (noting that nothing is charged by phone). At the bottom, a hand holds a smartphone displaying the PayPal mobile app interface.



Mobile Payment Business

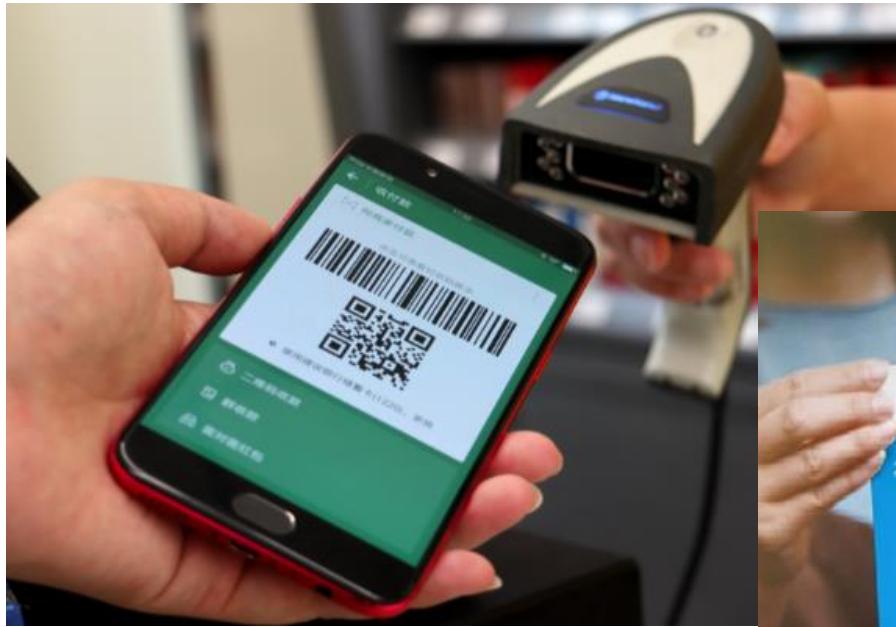
- M-commerce enabled a new business on m-payment:
- E.g:
 - premium-rate calling numbers,
 - charging to the mobile telephone user's bill
 - deducting from their calling credit.
 - registration of a credit card that is linked to a SIM card.
 - Billing a customer's credit card through a secure user interface
 - Mobile paypal
 - Near Field Communication (NFC)
 - RF SIM

To be discussed in lecture 9



Payment apps

- Alipay, Wechat pay



Mobile payment customer testimonial

- <http://www.youtube.com/watch?v=AEfLqzswIIU&feature=related>



Message from the video

- User behavior and expectations are evolving
- m-commerce = internet on hand?
- Users expectations
 - Speed
 - Flexibility
 - Reliability
 - > good back up, damaged information can be restored quickly
 - Robust and reliable infrastructure

Summary of m-commerce (Subscribers applications)

- Subscribers applications
 - In-apps advertising
 - Mobile marketing
 - Selling apps
 - m-Ticketing
 - m-Coupon
 - Mobile banking
 - Mobile shopping,
 - Mobile trading
 - Mobile brokerage

Q&A