Internet Economics and Financial Technology - Notes

Dom Hutchinson

November 17, 2020

Contents

1 The Big Picture

Remark 1.1 - *History of Commercial Computing*

1950-60 Mainframes - slow; size of rooms.

1960-70 Minicomputers - slow; couple per rooms.

1970-80 PCs - faster; one per desk.

1980-90 LANs - distributed networks.

1990-10 Internet - world wide distributed network.

2010-20 Cloud Computing

Where does IT go next? Has it peaked as IT is almost fully diffused?

Remark 1.2 - *Economics in Computer Science*
Market Economics is a useful metaphor for new methods in computer science & engineering which deal with allocation of scare resources. This is field is known as *Market Based Control*. Algorithms in this field tend to model sellers & buyers, and are applicable across most problems in the field (from server allocation to automated stock traders).

2 Economic Principles

Definition 2.1 - *Externality*
The production or consumption of a good has an *externality* if it affects a third party who was not involved in the transaction. e.g. Pollution from production is a negative externality; education is a positive externality.

2.1 Micro-Economics

Definition 2.2 - *Microeconomics*
The study of the behaviour of individual economic actors (individuals & business) and how decisions are made based on the allocation of limited resources.

Definition 2.3 - *Production-Consumption Cycle*
Producers produce goods & services which consumers wish to buy. Consumers have a limited about of money so have to choose what to & to-not buy at given prices. Similarly, producers have a limited number of resources (raw, labour & capital) so need to decide what goods & services, at what price, to produce. These lead to the idea of supply & demand curves.

Definition 2.4 - *Supply and Demand Equilibrium*
The *Equilibrium* of a supply-and-demand curve is a *price* where the quantity demanded by all consumers is equal to the quantity supplied by all producers.

When there is *excess demand* prices will rise due to scarcity of supply. The increase in supply will reduce demand as some consumers will not be happy to pay the higher price, meaning a new (higher) *equilibrium price* will be reached.

If there is *excess supply* prices will decrease as producers try to encourage customers to buy their product over others, this will in turn attract new customers and cause some producers out of business. A new lower *equilibrium price* will be reached.

Definition 2.5 - *Consumer Demand Curve*
A consumer's *Demand Curve* plots the quantity of a product a consumer is willing to buy for a given price-per-unit. These are typically downwards sloping as consumers prefer to pay lower prices. It is assumed a consumer will buy the quantity of units equal to the point where the *Demand Curve* intersects the market price.

The area under the curve, but above the *Market Price* is known as *Consumer Surplus*. This quantifies how much more a given consumer was willing to pay than the market price. The number of items a consumer is willing to buy at the *Market Price* multiplied by the *Market Price* gives the *Expenditure* for that consumer. Consumers want to maximise *Consumer Surplus*.

See `Figure 2`

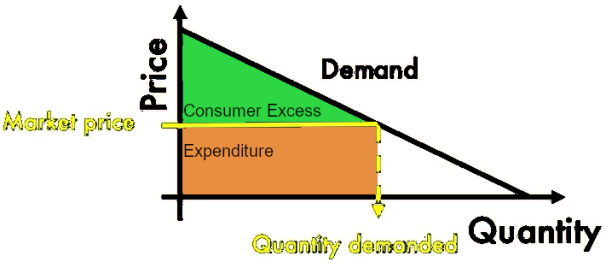


Figure 1: Consumer Surplus & Expenditure

Definition 2.6 - *Production Costs*
A producer will have costs they need to pay in order to stay in business. These costs can be categorised as

Fixed Costs A company must incur in order to operate, even before they start producing. (e.g. rent)

Variable Costs are costs which depend on the number of units produced. (e.g. equipment, raw materials)

Semi-Variable Costs Labour can be considered a variable cost as you can choose to pay overtime or to hire someone new in order to increase production.

The sum of these values will give you the *Total Cost* of production.

Definition 2.7 - *Marginal Cost Curve*
Marginal Cost is the cost of producing the last unit. It is equal to

$$\frac{\text{Change in Cost}}{\text{Change in Quantity Produced}}$$

We can plot a *Marginal Cost Curve* of marginal cost against quantity. Typically these are initially downwards sloping, then upwards sloping.

Definition 2.8 - *Economies of Scale*
When the *Marginal Cost Curve* is downwards sloping *Economies of Scale* are being experienced. *Economies of Scale* are the cost advantages a producer obtains by scaling their business. e.g.

By hiring a new staff member existing staff are able to specialise better on their task and thus production per staff member increases.

When the *Marginal Cost Curve* is upwards sloping *Diminishing Marginal Returns* are being experienced. This is common as it is unlikely that hiring 10 new staff will increase marginal production by 10 times that of a single new staff member.

Economies of scale & diminishing marginal returns affect the *Cost Curve* for a producer.

Remark 2.1 - *Minimum Sale Price*
The *Marginal Cost* of a product is the minimum price a product must be sold at in order to make a profit.

A producer will go out of business if it cannot sell above its *Average Variable Cost* (per unit produced) in the short run; and if cannot cover its *Average Total Cost* (per unit produced) in the long run.

The point where these *AVC* & *ATC* curves intersect the *Marginal Cost Curve* define the minimum amount of units a business needs to sell to stay in business in the short and long term, respectively.

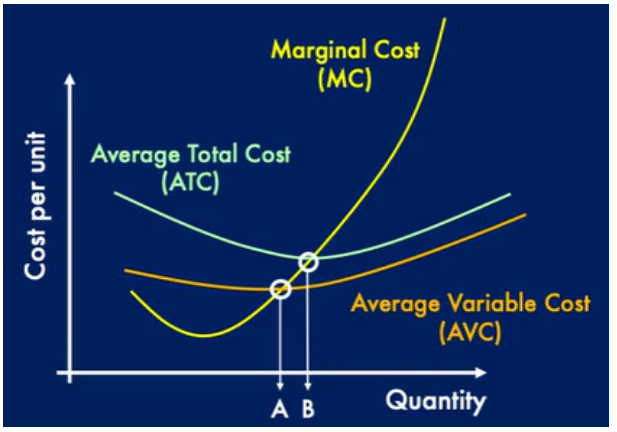


Figure 2: Cost Curve for a Product of a Physcial Retailor

Definition 2.9 - *Business Supply Curve*
A business's *Supply Curve* is the minimum price-per-unit it is willing to sell each quantity of product at. It tends to be upwards sloping as marginal cost increases with quantity. The *Supply Curve* will be truncated and not have a value for small quantities (in practice) as the business would fail if it sold too few products.

Definition 2.10 - *Market Supply Curve*
The *Market Supply Curve* is the total number of units available, for a given price, across all producers in a market.

The area above the *Market Supply Curve* and below the *Market Price* is the *Producer Surplus*. This is the total additional income a producer receives after costs (i.e. total profit). Producers want to maximise *Producer Surplus*

Definition 2.11 - *Competitive Equilibrium*
In a *Competitive Market* the *Market Equilibrium Price* will be that where the *Consumer Demand Curve* and *Market Supply Curve* intersect, as this is the price where quantity demanded and supplied are equal. The *Market Equilibrium Price* maximises total surplus for

both consumers and producers.

Definition 2.12 - *Shifts*
Shifts can occur which move the whole of a supply or demand curve. These occur from non-price factors. e.g. a pandemic will cause a shift in the demand curve for face masks. These will cause a shift in *equilibrium price*.

Definition 2.13 - *Monopoly Market*
A market is considered a *Monopoly* if its structure is characterised by a single seller (The *Monopolist*). The *Monopolist* faces no competition and thus can be a price setter, rather than price taker. In the real world a firm with over 40% market share is considered to have a monopoly. Monopoly markets are not competitive.

Definition 2.14 - *Pareto Efficiency*
An allocation is *Pareto Efficient* if no-one can be made better-off without someone else being made worse-off. Pareto efficient allocations can arise from free markets, despite traders acting only to serve themselves (the *invisible hand* guides them).

Free markets are not *guaranteed* to achieve optimal allocations. Some conditions under which this fails are well known (e.g. monopolies).

2.2 Elasticity

Definition 2.15 - *Price Elasticity of Demand*
Price Elasticity is a measure of the how much the price of a product affects the quantity demanded. The more horizontal the demand curve, the greater the quantity demanded increases for a given decrease in price, (i.e. the more elastic the price is).

- A *Horizontal* demand curve has *Perfect Price Elasticity* as a change in quantity has no affect on price.
- A *Vertical* demand curve has *Perfect Price Inelasticity* as a fix quantity is demanded, at any price.
- A *45 degree* demand curve has *Unit Price Elasticity* as an $\Delta\%$ change in supply will produce an $\Delta\%$ change in demand.

Definition 2.16 - *Price Elasticity of Supply*
Supply Elasticity is a measure of how much a change in quantity supplied will affect the cost of production. The more horizontal the *Supply Curve* is the less the price of production increases for a given quantity.

- A *Horizontal* demand curve has *Perfect Price Elasticity* as a change in quantity has no affect on price.
- A *Vertical* demand curve has *Perfect Price Inelasticity* as a fix quantity is demanded, at any price.
- A *45 degree* demand curve has *Unit Price Elasticity* as an $\Delta\%$ change in supply will produce an $\Delta\%$ change in demand.

2.3 Price Discrimination

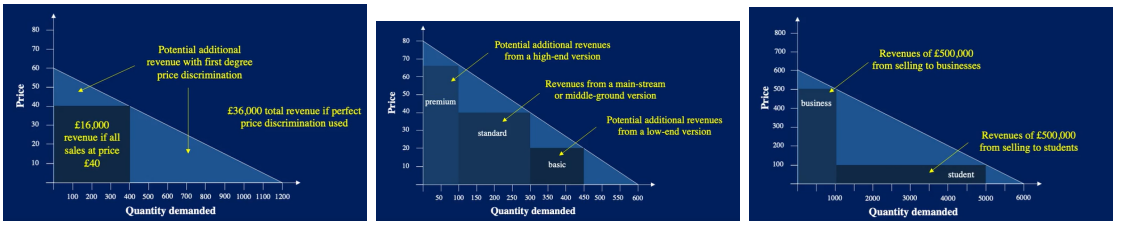
Definition 2.17 - *Price Discrimination*
Price Discrimination is the practice of charging different prices to different customers for the same product. There are three levels of price discrimination

1st Degree *Personalised* pricing. The business charges the maximum possible price for each unit sold (perfect price discrimination).

2nd Degree Product *versioning* or *menu pricing*. A company charges a different price for different quantities/qualities (ie bulk discount). Consumers have a choice over which version they buy, and thus the price. Here the discrimination depends on the product bought, rather than on characteristics of the customer, and encourages customers to self-select/

3rd Degree *Group* pricing. The business charges a different price to different customer groups (e.g. age,location). The consumer does not get to choose their group. The groupings try to separate customers by their *price elasticity* (The more price elastic charged less).

See `Figure 3`



(a) 1st Degree (b) 2nd Degree (c) 3rd Degree

Figure 3: Potential revenue increases for different pricing strategies

Proposition 2.1 - *Requirements for Price Discrimination*
For a seller to be able to effectively price discriminate they must fulfil the following

i). Be able to *distinguish between customers* so as to know what price to charge them.

ii). Have enough *market power* to be able to set prices above marginal costs.

iii). *Resale* must be impractical to prevent arbitrage.

It is generally easier for online business to meet these criteria.

Remark 2.2 - *Loyalty Schemes*
Loyalty schemes can be considered 2nd degree price discrimination. Loyalty schemes can be a useful way of profiling customers and thus contributes to other forms of price discrimination.

Definition 2.18 - *Price Steering*
Price Steering is when search results are personalised to place more/less expensive results at the top of the list. This encourages customers to spend at that price point due to placing an anchor, but the customer is still free to choose any product.

Definition 2.19 - *Net Utility*
The *Net Utility* of a product to a consumer is the difference between the price of the product and the consumer's perceived value of the product. (e.g. If a product is sold at £5 but a

consumer values it at £7, the net utility is £7-£5=£2). It is assumed a customer will never by a product that has a *negative net utility* to them.

Example 2.1 - *Economics of Versioning*
Suppose we have a product priced at £10. Consider two customers: *addict* who values it at £20; and *casual* who values it at £8. The company will sell a single unit (to *addict*) at £10.

Now, suppose the company brought in a *cut-down* version at £5 which *addict* values at £8; and the casual user at £7. The company will now sell one full product (to *addict*) and one *cut-down* product (to *casual*) for a total of £15.

In fact, pricing the *cut-down* version at £7 and the *full* version at £19 would maximise profit (assuming customers go for the superior product when they have the same net utility for both) as this would be a perfect price for *casual* and the net utility is the same (£1) for *addict* for both products.

Proposition 2.2 - *Competing against Yourself*
A risk of versioning is that consumers who are willing to pay for the higher price, will choose to pay for the lower price one (due to greater net-utility). Thus choosing pricing points & functionalities is therefore critical to business success.

Proposition 2.3 - *Bundling*
Bundling is a form of *versioning* where several goods are sold together for a single price. (e.g. microsoft office). Bundling is used to sell customers products they would not otherwise buy. Bundling can create barries to entry for competitor producers as it requires competitors to produce a wider varity of product (e.g. a spreadsheet software & word processor rather than just one).

3 Economic Agents

Definition 3.1 - *Bull & Bear*
An asset is described as *Bullish* if its value is expected to increase; Or, *Bearish* if its value is expected to decrease.

Remark 3.1 - *CDA Curves in Practice*
The supply and demand curves for continuous-action double auctions are, in reality, stepped. This is due to the relatively few units for sale in the market

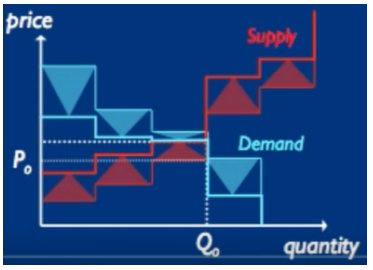


Figure 4: The arrows show the displacement from an agents hidden price and their quoted price

Proposition 3.1 - *No-one Trades their Marginal Price*

In practice sellers do not want to sell at their marginal price, nor do buyers want to buy at their maximum price. To avoid this both are advised to start a little away from these prices. These offered prices are known as *Quote Prices*. Quoted prices have their own *apparent* supply and demand curves which may be very different from the true curves. (See `Figure 4`).

The distance between the apparent and actual curves gives you the margin that agents are trying to achieve in the market. Agents should change their margin to reflect those of other people in the market. You would expect margins to decrease as the time since last transaction increases.

Traders to the left of the equilibrium price can increase their margins to meet the equilibrium, while those on the right have to decrease.

Proposition 3.2 - *Dynamic Variation of Supply & Demand Curves*
In reality markets equilibriums are dynamic, as if the buyer and seller closest to the equilibrium perform a transaction they will drop out the market and a new equilibrium will need to be found. Also, new buyers and sellers may join the market. This is obvious in markets with very few units.

Definition 3.2 - *Experimental Economics*
Experimental Economics perform lab-style studies of human market-trading behaviours.

- A small number of human subjects are split into 'buyers' and 'sellers'.
- All traders are given a private-value/limit price which they cannot exceed.
- Traders interact within some market mechanism.

Experimental Economics has demonstrated rapid equilibration in CDAs with very small number of traders.

3.1 Metrics for Markets

Definition 3.3 - *Smith's α*
Smith's α is a measure of transaction price variation around the theoretical equilibrium price (as a percentage). Lower is better

$$\alpha := \frac{100}{P_0}\sqrt{\sum_{t\in T}\frac{(P_t - P_0)^2}{|T|}}$$

where P_0 is the equilibrium price and $\{P_t\}$ is the set of offered prices.

Definition 3.4 - *Allocative Efficiency*
Allocative Efficiency is a measure of how effecitve the market is at extracting *'gains through trade'*.

$$100 \times \frac{\text{Total utility earned by all traders}}{\text{Theoretical maximum possible total utility}}$$

Definition 3.5 - *Single Agent Efficiency*
Single Agent Efficiency measures how well an individual agent performs.

$$100 \times \frac{\text{Profit Earned}}{\text{Expected profit all all trades done at } P_0}$$

Proposition 3.3 - *Intelligence required for an allocative efficient CDA*
How much of the allocative efficiency of a CDA is due to the intelligence of the traders¿ And how much is due to the organisation of the market?

Experimental Economics demonstrated (in 1993) than a zero-intelligence trading agent (ZIC) which quoted random prices (but constrained not to trade at a loss) is surprisingly human-like. Suggesting most of the intelligence is in the market, not in the traders.

3.2 Trading Algorithms

Proposition 3.4 - *How ZIC Traders achieve an equilibrium*
ZI-C *sellers* generate offer prices at random in a range from the lowest seller limit price $S_{\min}$ and the maximum price allowed in the system $P_{\max}$. This gives us a probability density function for offer prices which follows the supply curve.

ZI-C *buyers* generate offer prices at random in a range from the greatest buyer limit price $D_{\max}$ and the minimum price allowed in the system $P_{\min}$. This gives us a probability density function for bid prices which follows the demand curve.

The intersection of these two distributions gives the distribution of prices at which transactions are done. See `Figure 5`. It is noteworthy that the expected values of these distributions are not equal as it means markets populated by ZIC traders achieve an equilibrium by chance (and will not reach an equilibrium in markets with assymetric supply and demand curves).

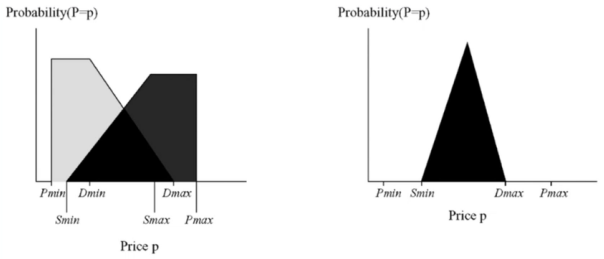


Figure 5: Distributions for offer, bid & transaction prices for ZIC Traders

Proposition 3.5 - *ZIP Traders (1997)*
ZI-Plus (ZIP) Traders are a more advanced form of *Zero-Intelligence Traders*. They still have a limit price which they cannot exceed, but also use machine learning in order to adapt. They have a *profit margin* which is the distance between the price they quote and their limit price, this margin is adjusted by the machine learning over time.

These have been shown to be much more human-like in CDA, than ZIC traders and achieves an equilibrium in cases where ZIC traders could not.

Proposition 3.6 - *ZIP Algorithm - Qualitative*
The algorithm a ZIP trader uses is as follows.

Consider a seller with limit price L. They will ask for a price $P := L(1 + M)$ where M is some profit margin. If this price is *accepted* then increase M; otherwise, decrease M.

Buyers should do the inverse with their value of M.

The amount to change M by is determine by a *learning rule* (e.g. Widrow-Hoff with

Momentum).

Proposition 3.7 - *ZIP Algorithm - Quantitative*
Let $_i$ denote the limit price of trader i; $p_i(t)$ denote the quote price of trader i at time t; and $\mu_i(t)$ denote the profit margin of trader i at time t. Then

$$p_i(t) = \lambda_1(1 +_i (t))$$

If $p_i(t)$ is accepted then $\mu_i(t + 1) = \mu_i(t) + \textit{something}$; otherwise; $\mu_i(t + 1) = \mu_i(t) - \textit{something}$ where the value of *something* is determined by a stochastically determined *Target price* and a learning rule aimed at achieving that price.

Proposition 3.8 - *ZIP Trader Target Price*
The target price τ_i should be slightly beyond the last quoted price in the market $q(t)$.

$$\tau_i(t) = A_i(t) + q(t)R_i(t)$$

where $R_i(\cdot)$ and $A_i(t)$ are stochastic functions for adjusting the last quoted price with $R_i(\cdot)$ being relative and $A_i(t)$ being absolute. These functions are defined by the learning rule.

Definition 3.6 - *Widrow-Hoff Learning Rule*
The *Widrow-Hoff* learning rule adjusts an observed value A towards a desired value D, at rate β. The rule is defined as

$$A(t + 1) = A(t) + \Delta(t) \quad \text{where} \quad \Delta_i = \beta\big(D(t) - A(t)\big)$$

For ZIP a damping (momentum) factor $\gamma \in [0, 1]$ is introduced

$$A(t + 1) = \gamma A(t) + \Delta_i(t)(1 - \gamma) \quad \text{where} \quad \Delta(t) := \beta\big(D(t) - A(t)\big)$$

In the context of ZIP this is defined as

$$\mu_i(t + 1) = \frac{1}{\lambda_i}(p_i(t) + \Delta_i(t)) - 1 \quad \text{where} \quad \Delta_i(t) := \beta_i\big(\tau_i(t) - p_i(t)\big)$$

Giving

$$\mu_i(t + 1) = \frac{1}{\lambda_i}\big(p_i(t) + \Gamma_i(t)\big) - 1 \quad \text{where} \quad \Gamma_i(0) := 0;\ \Gamma_i(t + 1) := \gamma_i\Gamma_i(t) + \Delta_i(t)\big(1 - \gamma_i\big)$$

Proposition 3.9 - *Todd Kaplan's Sniper (1993)*
Kaplan's *Sniper Algorithm* is a robust and effective trading algorithm.

The trader does nothing until the bid-offer spread drops to a sufficiently small value or the offer is less than the smallest transaction price in the previous period or there is only a short time until the market closes. When one of these conditions is fulfilled the trader jumps in, as long as the deal makes the sniper a profit greater than some threshold, and *"snipes the deal"*.

Note that this algorithm does adapt to the market, nor does it help prices converge to an equilibrium. Moreover, it relies on there being other "more" intelligent traders in the market for it to leech off.

Proposition 3.10 - *GD Traders (1998)*

Gjerstad-Dickhaut (GD) Traders using an algorithm which is based on producing a estimate of the probability of a certain price being accepted. This is defined by the trader's *belief function* which uses data from the n most recent market activity.

$$f(p) = \frac{able(p) + ole(p)}{able(p) + ole(p) + rgbe(p)}$$

where p is the price being queried, $able(p)$ is the number of accepted bids at prices less than p in the last n; $ole(p)$ is the number of offers made below p in the last n; and, $rgbe(p)$ is the number of rejected bids priced above p, in the last n.

Proposition 3.11 - *MGD Traders (2001)*
MGD is a *Modified* version of *GD* with the follow considerations made:

- Use interpolation to smooth the function for prices which have not occurred in the market history.
- Choosing a quote-price which maximises the trader's expected gain (utility gain times probability of acceptance).
- Assign 0 probability for bids lower than previous lowest big, or offers above the previous greatest trade price.

Proposition 3.12 - *GDX Traders (2002)*
GDX is another extension of *GD* which uses real-time *dynamic programming* to formulate agent bidding strategies in a broad class of auctions characterised by sequential bidding and continuous clearing.

Proof 3.1 - *Adaptive-Aggressive Algorithm (2006)*
AA Traders uses past history to adjust it's *aggressiveness* (rather than profit margin) over time. *Aggressiveness* quantifies how quickly it changes its pricing in response to market conditions.

AA Traders use an estimate of the current market equilibrium price P_0 (using past transactions) and *Smith's* α estimate of volatility to determine its level of aggression.

Proposition 3.13 - *Deciding which algorithm to use*
An analytical (game-theoretical) approach to choosing which trading algorithm is optimal is very hard and sometimes impossible. Some proofs require over simplifying assumptions which limit the end conclusion.

Instead *empirical studies* (simulation experiments) are used. This requires good *"Design of Experiments"* and appropriate statistical analysis of results.

Proposition 3.14 - *Design of Experiments*

- *Homogeneous Population Tests* assumes that all traders use the same algorithm. This is true in some cases (such as market-based resource allocation) but not many. This means only limited conclusions can be made.
- *One-in-Many Test* have all but one member of a trading population using the same algorithm. This explores the vulnerability of the dominant algorithm, and the ability of the alternative algorithm to exploit the market. IRL, if the alternative algorithm was better you would expect some other traders to defect.

- *Balanced-Group Test* have groups of equal size, each running a different algorithm but with matched limit prices. This is generally seen as the best test for comparing two different algorithms.

Simplex plots can be used to show the relationship between different ratio of traders.

Remark 3.2 - *The Best Algorithm*

- Balanced-Group Tests showed MGD to be superior to ZIC,ZIP & GD in all cases.
- Balanced-Group Tests AA was shown to out perform GDX & ZIP, in most cases. (Importantly AA is not dominant)

There are likely to be unpublished algorithms which out perform these.

3.3 Empirical Methods

Remark 3.3 - *When to use a t-Test*
A *t-Test* can only be used when it is safe to assume that the underlying distribution is a normal distribution. There are tests of normality to check this.

Proposition 3.15 - *$A - B$ Test*
Here I describe a test to determine whether some method A is better than some method B.

- Calculate the confidence interval on mean of samples from A.
- Calculate the confidence interval on mean of samples from B.
- If the intervals do not overlap then we can determine that one method is better than the other.

Definition 3.7 - *Wilcoxon-Mann-Whitney U Test*
The *Wilcoxon-Mann-Whitney U Test* is a powerful test for two independent samples on a continuous dependent variable. It is a *non-parameteric* version of the t-test. This test makes some assumptions, see `Proposition`

Let A be a sample of size n_A and B be a sample of n_B, with $n_A > n_B$.

H_0: A and B come from the same population.
H_1: A and B come from *different* populations

i). Combine A and B into one list and sort it (keeping track of which data point is from which sample).

ii). Rank the list from lowest to highest. Awarding average rank when ties occur.

iii). Sum the ranks for A and B to get R_A, R_B.

iv). Compute $U_B := n_A n_B + \frac{1}{2} n_A(n_A + 1) - R_A$ and $U_B := n_A n_B + \frac{1}{2} n_B(n_B + 1) - R_B$.

v). Define $U := \min\{U_A, U_B\}$.

vi). Compare U to the critical value from $U_{n_A, n_B, \alpha}$ from a lookup table.

vii). If $U < U_{n_A,n_B,\alpha}$ then reject H_0.

The *U-Test* is a pairwise test, but it is bad to performance a series of these tests as the error grows quickly. (ie If you are testing at a siginifance level of 95%, the probability of being correct after four tests is $.95^4 = .814...$)

Proposition 3.16 - *Assumptions of U Test*

- The Independent variable data is in two groups (Control and Treatment).
- The dependent variable is at least in an ordinal scale.
- Data is randomly selected samples from the two groups
- The population distributions of the dependent variable for the two groups have a similar shape, but have differences in measures of central tendency.

Definition 3.8 - *Kruskal-Wallis Test*
The *Kruskal-Wallis Test* is a generalisation of the *U Test*, extending it to allow multiple group comparisions.

Consider samples A, B, C, D

i). Calculate the mean ranking for each group's entries in the sorted union list. (As in U Test) Compute a statistic H form the mean rank and the sample size n.

ii). Use a χ^2-test to determine whether H is significant.

3.4 Options Markets

Definition 3.9 - *Short Selling*
To *Short* a stock, is when you borrow a stock from someone else and sell the borrowed stock immediately. You will then need to buy a stock at some point in the future to return to the original lender, ideally for less than you sold the borrow stock for.

Shorting can be used as insurance against other market events.

Definition 3.10 - *Derivative*
A *Derivative* contract is based on the *marginal change* in value of an asset. They do not require you to buy/own an actual stock, rather you work on the *margin* of the stock. There are different types of *Derivative*

- A *Futures* contract is one which must be executed by/on a set *delivery* date. A *Forward price* is defined when the contract is issued, and this is the price the final transaction will occur at. Common for selling crop yields.

  Buyers of a forward have the *long position* and sellers have the *short position.*

- An *Options* contract is one which may be executed by/on a set *delivery* date. There is no obligation. *Options* have a *Strike price* which is the price which the transaction will be done at, if a transaction is done at all.

  Options to sell are called *puts* and options to buy are *calls.*

The option is said to be *written* by the seller and *held* by the buyer.

Remark 3.4 - *Futures and Options*
Both futures and options are

- *Standardised*. The size of the contract and the delivery/expiry date are prespecified.
- *Exchange Traded*. The contracts can be bought and sold on a secondary market. This is required so that those who do not have enough money to actually exercise the full value of their option can still realise the option's value, by selling to someone who can afford to exercise the option.

Remark 3.5 - *Price of an Option*
The price of an option depends on the

- *Intrinsic Value*. The money received if the option is exercised now.
- *Volatility Premium*. The volatility in price of the underlying asset.
- *Time Value*. The potential risk-free return on money saved wrt buying the underlying asset. (ie what you could received if the money was placed in a safe investment, rather than the option)

Definition 3.11 - *American-Style & European-Style*
An *American-Style* option can be exercised on any date up to the expiry date.

A *European-Style* option can only be exercised on its expiry date.

Definition 3.12 - *Call Option*
A *Call option* gives the holder the right to buy N units of the underlying asset, at some point in the future, at a specified *Strike Price*. If exercised the option-write (Seller) must sell the N shares at the strike price.

The *Call Option* is *In The Money* (ITM) if the underlying asset price is greater than the strike price; *Out The Money* (OTM) if the underlying price is less than the strike price; Or, *At The Money* if the underlying price equals the strike price.

Definition 3.13 - *Put Option*
A *Put Option* gives the hold the right to sell N units of the underlying asset, at some point in the future, at a specified *Strike Price*. If exercised the option-writer (Seller) must buy the N shares at the strike price.

The *Call Option* is *In The Money* (ITM) if the underlying asset price is less than the strike price; *Out The Money* (OTM) if the underlying price is greater than the strike price; Or, *At The Money* if the underlying price equals the strike price.

Remark 3.6 - *Commissions are paid on setting up option contracts.*

3.4.1 Option Strategies

Proposition 3.17 - *Option Strategies*
Option Strategies are linear combinations of options:

- Long call

- Short call
- Long put
- Short put

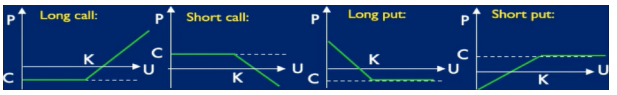


Figure 6: Different Basic Option Pay Off Diagrams

Definition 3.14 - *Bull Spread*
A *Bull Spread* is an option strategy which bounds the pay off to a constant, this limits the risk by placing a cap on potential losses. A *Bull Spred* is made up of a *Long call at* K_1 and a *Short Call at* K_2 (Bullish Call Spread); or the same but with *put* options (Bullish Put Spread). In practice the losses are limited to the K_2 price as if the underlying price was to exceed K_2 then you would exercise the short option.

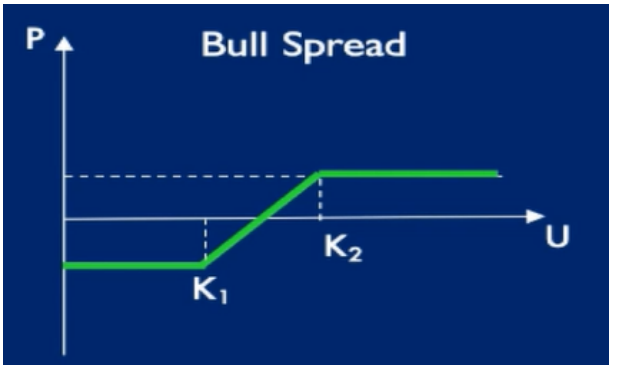


Figure 7: Bull Spread Pay off Diagram

Definition 3.15 - *Bear Spread*
A *Bear Spread* is an option strategy which bounds the pay off to a constant, this limits the risk by placing a cap on potential losses. A *Bear Spred* is made up of a *short put at* K_1 and a *long put at* K_2 (Bearish Put Spread); or the same but with *call* options (Bearish Call Spread). In practice the losses are limited to the K_2 price as if the underlying price was to fall below K_2 then you would exercise the long put option.

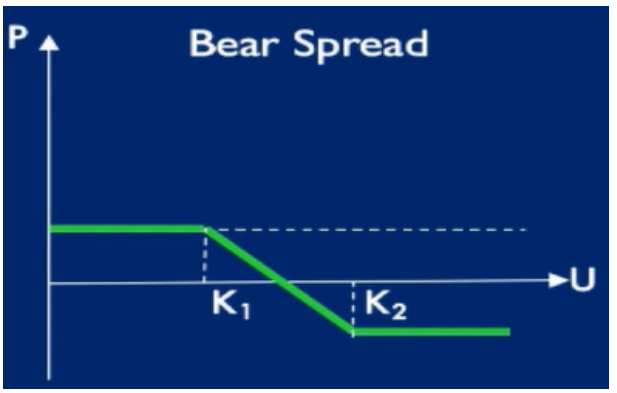


Figure 8: Bear Spread Pay Off Diagram

Definition 3.16 - *Long Butterfly*
A *Long Butterfly* strategy is used when you expect the price not to change much. A *Long Butteryfly* is made up of a *Long Call at* K_1, two *Short calls* each at K_2, and another *Long Call at* K_3

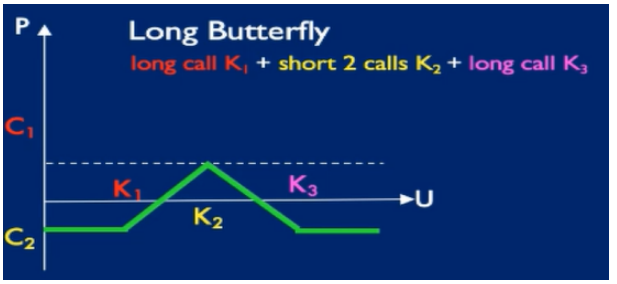


Figure 9: Long Butterfly Pay Off Diagram

Definition 3.17 - *Short Butterfly*
A *Short Buterfly* strategy is used when you expect the price of an asset to change (in either direction) from its current value. A *Short Butterfly* is made up of: a *Short Call at* K_1, two *Long Calls* each at K_2 and another *Short Call* at K_3.

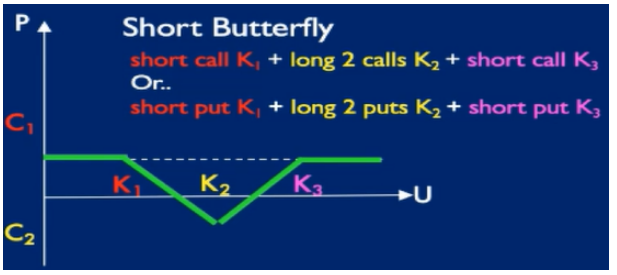


Figure 10: Short Butterfly Pay Off Diagram

Definition 3.18 - *Long Straddle*
A *Long Straddle* strategy has an unbounded payoff, provided the value of the asset moves from its original value (Essentially an unbounded Long Butterfly). A *Long Straddle* is comprised of a *Long Call at* K_1 and a *Long Put at* K_1.

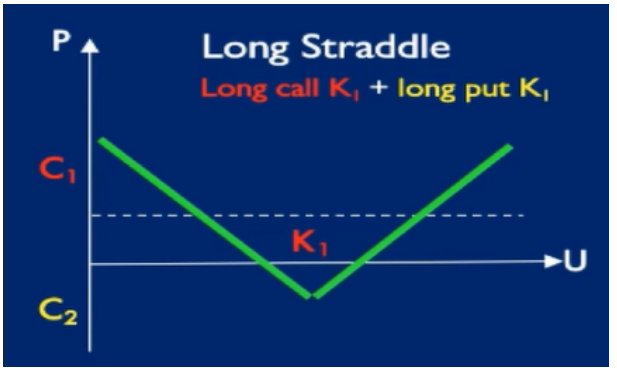


Figure 11: Long Straddle Pay Off Diagram

Definition 3.19 - *Short Straddle*

A *Short Straddle* strategy has an unbounded payoff, provided the value of the asset does not move from its original value (Essentially an unbounded Short Butterfly). A *Short Straddle* is comprised of a *Short Call at* K_1 and a *Short Put at* K_1.

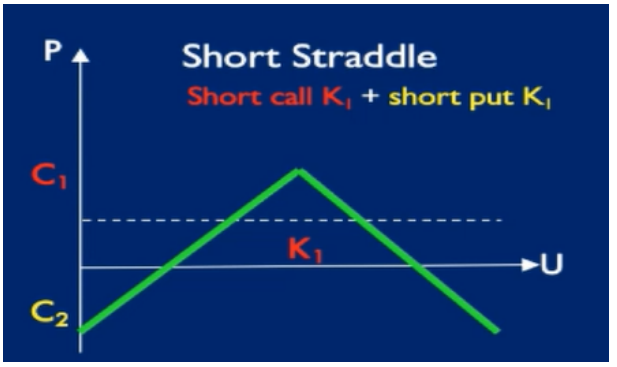


Figure 12: Short Straddle Pay Off Diagram

Definition 3.20 - *Long Strangle*
A *Long Strangle* strategy pays out provided the underlying asset values moves at least some specified amount from its original value (Essentially a long straddle which doesn't just meet at a point). A *Long Strangle* is made up of a *Long Put at* K_1 and a *Long Call at* K_2.

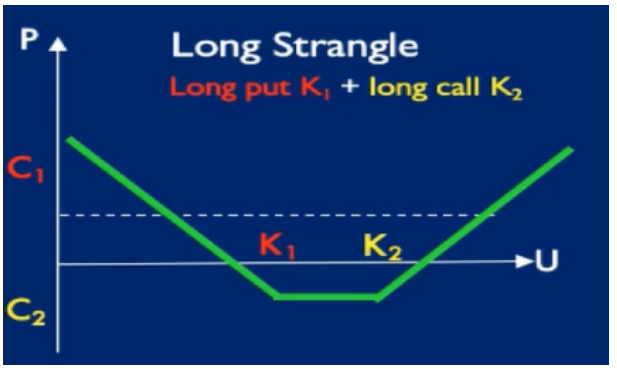


Figure 13: Long Strangle Pay Off Diagram

Definition 3.21 - *Ratio Call Spread*
A *Ratio Call Spread* is similar to a long butterfly, but is unbounded in terms of losses should the underlying value keep increasing. A *Ratio Call Spread* requires three options (One less than a *Long Butterfly* so is cheaper): A *Long Call at* K_1 and two short calls, both at K_2.

A *Ratio Call Spread* is used when you are confident U will rise to K_2, but no go beyond that.

Definition 3.22 - *Ratio Put Spread*
A *Ratio Put Spread* is similar to a long butterfly, but is unbounded in terms of losses should the underlying value keep decreasing. A *Ratio Put Spread* requires three options (One less than a *Long Butterfly* so is cheaper): Two *Short Puts at* K_1 and a long put at K_2.

A *Ratio Put Spread* is used when you are confident U will fall to K_1, but no go beyond that.

Definition 3.23 - *Ratio Call Backspread*
A *Ratio Call Backspread* is similar to a short butterfly, but is unbounded in terms of gains should the underlying value keep increasing. A *Ratio Call Backspread* requires three options

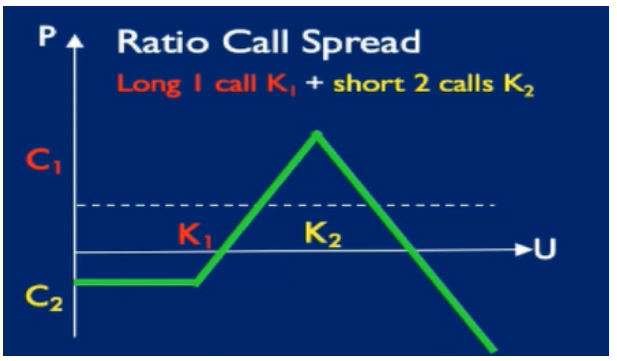


Figure 14: Ratio Call Spread Pay Off Diagram

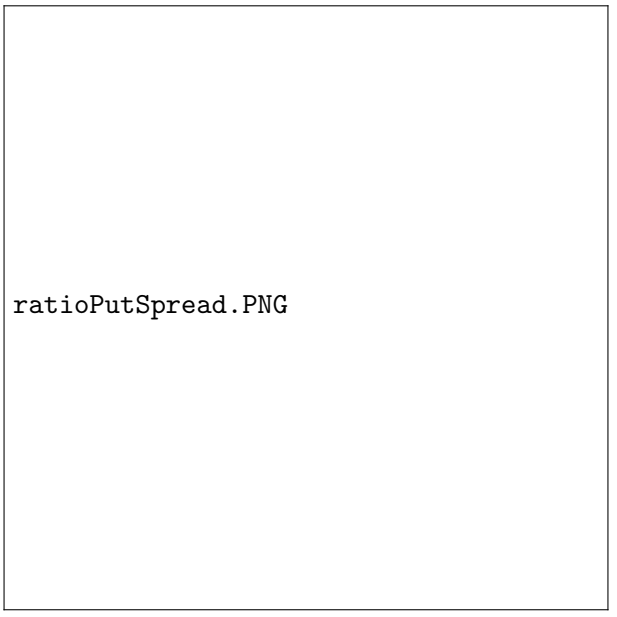


Figure 15: Ratio Put Spread Pay Off Diagram

(One less than a *Long Butterfly* so is cheaper): A *Short Call at* K_1 and two *Long Calls at* K_2.

A *Ratio Put Backspread* is used when you are confident U will shift significantly, with an increase more likely.

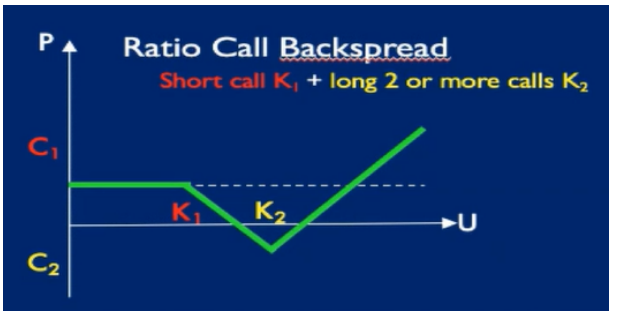


Figure 16: Ratio Call Backspread Pay Off Diagram

Definition 3.24 - *Ratio Put Backspread*

A *Ratio Put Backspread* is similar to a short butterfly, but is unbounded in terms of gains should the underlying value keep decreasing. A *Ratio Put Backspread* requires three options (One less

than a *Long Butterfly* so is cheaper): A *Short Put at* K_1 and two *Long Put at* K_2.

A *Ratio Call Backspread* is used when you are confident U will shift significantly, with an decrease more likely.

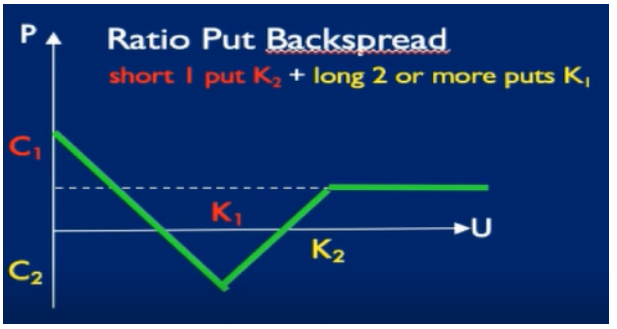


Figure 17: Ratio Put Backspread Pay Off Diagram

Proposition 3.18 - *Betting Exchanges*
Betting Exchanges are similar to *Options Markets* as they allow people who have differing views over some future outcome to wager on it. *Betfair* offer a LOB style way to place bets by allowing users to *"back"* (will happen) an event or *"lay"* (will not happen) an event.

4 The Economics of The Internet

Definition 4.1 - *Network Externalities*
A *Network Externality* is an *Externality* that occurs when the act of buying a product/serivce has an indirect cost or benefit to those who already own the same product/service. Products with positive network externalities are often known as *Network Goods*.

Owning a mobile phone has a positive network externality as you are increasing the number of contactable people. Owning a car has a negative network externality as you increase road traffic.

Positive network externalities can produce a *Positive Feedback Loop* where people by products which are compatible with their friends, rather than necessarily the best product. This is part of *Brand Value*.

Definition 4.2 - *Network Effect Demand Curve*
We can plot a *Network Effect Demand Curve* (`Figure 3`) of the price customers are willing to pay against network size. This is slope upwards initially as the marginal value of each extra user is higher; eventually it will slope downwards as these marginal gains diminish.

For any given price there are three equilibrium points q_0, q_1, q_2 for network size. q_1 is deemed unstable, the *'tipping point'*, as once the network is larger than q_1 it will naturally grow to q_2 (as there is a consumer excess) but whilst it is smaller it will shrink to q_0 (as there is a consumer deficit). This means q_1 is the *Critical Mass* for the network to be sustainable.

Proposition 4.1 - *The Long Tail*
Sales business typically sell either: high volume, low margin goods (e.g. burgers); Or, low volume, high margin goods (e.g. cars). Physcial sales businesses are constrained by the physical shelf space they have and thus avoid low volume, low margin goods. This means that

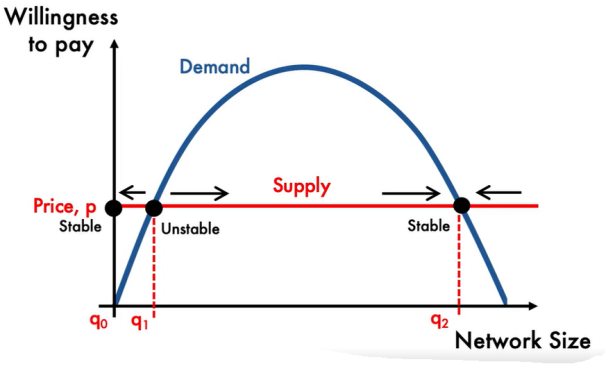


Figure 18: Network Effect Demand Curve

the sales distribution for products in a physical store will be a truncated *Pareto Distribution*.

Internet businesses have unlimited shelf space to advertise products, and since warehouse space is much cheaper (per sq ft) they can store a lot more products for the same cost, effectively increasing the margin of each product. Meaning their are more products which are profitable to stock and the sales distribution for products of an internet business will have a much longer tail. (See `Figure 1`).

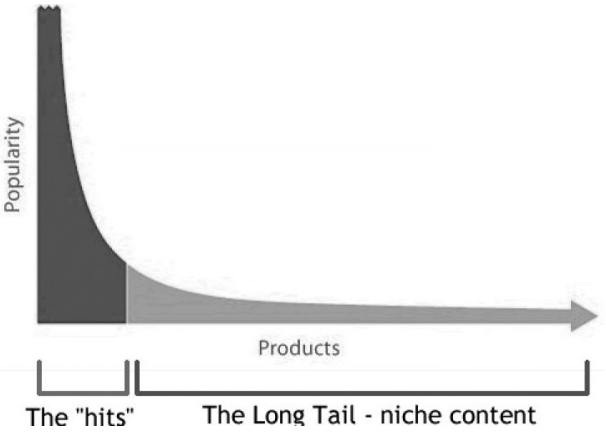


Figure 19: The Long Tail

Remark 4.1 - *How to take advantage of 'The Long Tail'*

i). Make everything available.

ii). Reduce prices (due to economies of scale & reduced costs).

iii). Help customers find new products.

Remark 4.2 - *Sustaining v. Disruptive Innovations*
Sustaining Innovations are those that incrementally improve existing products on traditional performance metrics. Eventually these will superceed customer requirements.

Disruptive Innovations perform less well on traditional performance metrics but sufficiently better along other metrics in order to generate new markets.

Proposition 4.2 - *Disruptive Technology*

Established companies are often late to invest in new *disruptive* technologies. Typically this is due to the *disruptive* tech not reaching the requirements of their customers. However, the *disruptive* tech maybe better in other ways (lighter, more durable etc.) and so can establish a sufficient market for startups to invest in it. Once the *disruptive* tech does reach the requirements of mainstream customers, they are likely to jump to the new tech for these bonus features (lighter, more durable etc.) and the established company may fail.

The new tech may still be less powerful than the established tech, but it is sufficient for customers so it doesn't matter. The traditional performance metric for performance will vary by industry (e.g. mb/£ for hard drives).

Proposition 4.3 - *Timeline of Disruptive Technology*

i). *Disruptive Technology* is invent. Often by an established company.

ii). The *disruptive technology* does not meet established the established company's requirements and so not focused on.

iii). New companies form to pursue the *disruptive technology.* Often by ex employees of the established company.

iv). *Disruptive Technology* improves & meets traditional performance metric requirements. The established company will likely try to enter the new market at this point but will be too late.

v). *Disruptive Technology* becomes the main stream.

Proposition 4.4 - *How to spot Disruptive Technology*

i). *Determine whether the technology is disruptive or sustaining*

4.1 Properties of Online Businesses

Remark 4.3 - *Economic Laws*
The *Economic Laws* are not fundamentally different between online & irl businesses, but the characteristics of online business activities can result in different markets.

Definition 4.3 - *Combinatorial Innovation*
Combinatorial Innovation describes a technology who's components can be combined & recombined to create new products and services. The Internet is a *Combinatorial Innovation* due to its standardised and open-source nature.

Proposition 4.5 - *Economic Differences between Digital & Physical Goods*

- Digital goods tend to be costly to produce; but *cheap to reproduce.* (i.e. Fixed costs are high but variable costs are low).
- Production costs for digital goods are sunk costs. (e.g. You can sell a building you don't need, but cannot get money back from a software developer).
- There are *no capacity constraints* limiting the number of times something can be reproduced.
- Digital goods are often *Experience Goods.* (i.e. a customer will no know whether they will like it before they try it, and thus cannot assign a value to it).

- *Serach Costs* for a consumer are very low. It is easy for consumer to compare products are go with the best. IRL this is harder as it requires going to different stores.
- Digital goods have *strong positive network externalities*

Remark 4.4 - *Switching Costs*
A customer may incur a cost (inc. non-monetary) to switch services. This is more common (and costly) in the digital space than the physical. When switching costs are too high, consumers are *locked in*. Possible switching costs include:

- Training cost.
- Network effects.
- Setup costs.
- Reduced service quality due to new provider not having all your information (consider switching from Netflix).

Proposition 4.6 - *Cost Curve for Digital Goods*
Since digital goods have high fixed cost but low variable costs their *cost curves* are very different. The *Marginal Cost Curve* is effectively zero for all quantities; Average Variable Costs are effectively zero for all quantities; and, average total costs tend asymptotically towards zero.

This means it is easy for an online business to survive in the short term and the minimum price they are willing to sell a product at is zero (due to v. low variable costs). Eventually the company will need to pay off its fixed costs.

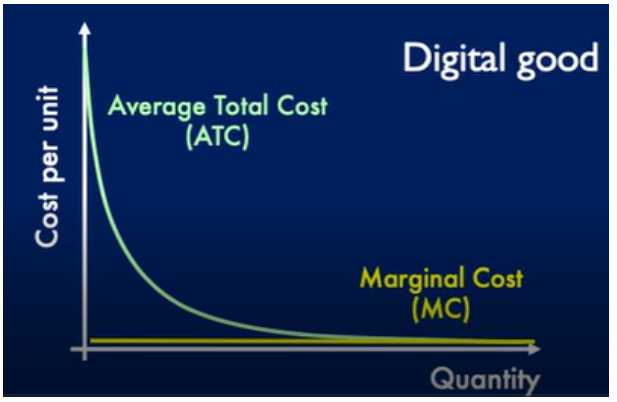


Figure 20: Consumer Surplus & Expenditure

Remark 4.5 - *Competition between Digital Companies*

- Due to low variable costs, companies with identical digital products will very quickly move prices to near-zero.
- New companies will struggle as fixed costs are high.
- Network effects & switching costs make it hard for new companies.

Due to these *barriers to entry* monopolies are common among digital companies. To succeed, a company needs to focus on product differentiation (i.e. innovation).

Remark 4.6 - *Formats*
Companies can make their software use *Proprietary Formats*, meaning the files cannot be used by other software. This increases switching costs for customers.

Using *Industry-Wide Standards* allow a user's files to be shared between providers. This can increase the network effect, potentially attracting new customers. Here companies have a trade-off between having a large part of a small pie, or a small part of a large pie.

Remark 4.7 - *How Standards Develop*
Industry-Wide Standards general develop in one of two ways

i). A *single (major) player* sets a standard by opening up their proprietary format (e.g. PDF).

ii). A *war* occurs between multiple standard setters. Generally detrimental to everyone involved.

iii). A *negotiation* occurs between multiple standard setters. There is a risk that one party may pull out of the deal and use their own proprietary format.

4.2 Price Discrimination Online

Remark 4.8 - *Personalised Pricing Online*

- Consumers tend perceive personalised pricing as *unfair*.
- Consumers like *transparency* (i.e. how a price is decided).
- European data protection laws *require* companies inform people about the specific purpose of processing their personal data.

Proposition 4.7 - *Digital Product Versioning*

- Digital versions are used extensively and creatively as they are easy to prepare and near-zero cost to duplicate.
- Buyers have a choice over which version to buy, so do not find the practice controversial.
- *Personalisation of Product* is an extreme typr of product versioning (becoming closer to 1^{st} degree price discrimination) as it allows user to specify many properties (e.g. screen quality, amount of ram & storage for a pc).
- People tend to *upsell* towards an "almost top option" when given a choice (the 2nd most expensive bottle of wine is often the most popular).
- Product versioning can cause you to *compete with yourself* as some people who would have payed the higher price, will go for the lower price.

Remark 4.9 - *Unbundling*
Bundling is common with physical software but there is also a practice of *unbundling*. Since there is no physical substrate online there is less commercial pressure to bundle. (e.g. publishers can sell individual articles rather than a full magazine).

Remark 4.10 - *'Free' Digital Versions*

As the duplication cost of digital goods is almost zero, many are given away for free. In these cases there are still several ways for producers to make money: cut-down versions encourage you to buy a full version; Artificial delay (e.g. stock feeds); Ads (or pay for no adds).

'Free' versions allow a customer to build a truer valuation of a product, particularly useful for *experience goods*.

Even if a user is on the free model they are building the *network effect* of the product and likely increasing the *swapping costs* they will experience if they want to change product.

Proposition 4.8 - *Freemium Model*
The *'Freemium'* business model is to offer different versions at different prices, *including a free one*. The hope is a consumer will *upgrade* to a paid version because they like the service.

4.3 Economics of Computer Games

Proposition 4.9 - *Virtual Game Economies*
Virtual game economies are generally stimulated by players collecting raw materials and then producing goods which they sell between themselves, very much like an IRL economy.

Virtual economies have many of the same issues as real economies. For a stable economy, a balance must be struck between currency sources (money entering) and skins (money leaving). If there is an imbalance then *MUDflation* can occur (Multi-User-Dungeon inflation?). Designing these stable economies (for MMORPGs) is hard.

Economic stability is important otherwise games can lose credibility. There are examples where players have developed *meta currencies* which are more stable to improve a games longevity.

Remark 4.11 - *IRL Game Economies*
There are real-world markets when players sell their in game items for IRL money. Essentially this a ForEX market.

Remark 4.12 - *Gold Farming*
As the value IRL market for a game's assets reaches it has been observed that people in developing nations will choose to grid the game (gold farm) in order to obtain items to then sell in an IRL market, rather than work a traditional job. This market is between the cash rich-time poor (americans) and cash poor-time rich (mexicans? sorry).

This typically against a games EULA, but it is hard to game makers to counter.

Remark 4.13 - *Game Development Budgets*
The number of people involved in making a game and the number of lines in a typical AAA game has grown exponentially, tracking the powerfulness of computers.

However, the *average* game budge has decreased as many games as small titles made on tight budgets or as passion projects.

Mid-size studios with projects budgets in the low millions are rare. This is typically due to either them being absorbed by bigger studios; or the mid-size studio breaks up into smaller teams.

The rise in *Content Costs* has increased due the number of many hours required to complete tasks and jobs have become much more specialised. Additional, game-developers now demand higher wages. Note that this is useful for big studios as they act as a barrier to entry.

5 Auction Theory

Remark 5.1 - *Why Use Auctions?*
Auctions allow an item to be sold for a price which is wholely decided by a consumer's willingness to spend. *Auctions* are a mechanism for first-degree *price discrimination*, this makes them particulary popular online.

Auctions are used when sellers are *uncertain* about the value consumers place on an object (common with one off items). In this case auctions are good as they allow for *price discovery*.

Auctions are easy to automate and a form of differential pricing.

Proposition 5.1 - *Auctions vs Posted Prices*
When a seller chooses to run either an auction or use posted prices, they are choosing whether between *price discovery* and *convenience*. Auctions are often favoured by unexperienced sellers and unique items. Auctions sell for less than a posted price listing (otherwise consumers would pay the posted price listing).

Definition 5.1 - *Private Value*
An object's *Private Value* is the value each consumer places on the object. Each bidder knows their private value for an object, but do not know the private value of others nor does knowledge of other bidders' private values affect your private value. This situation is common for consumable goods, less so with investments.

Definition 5.2 - *Interdependence*
Interdependence occurs when a bidder does know have a fixed value for an object and use other bids to improve their estimate of an objects value. This is common when other bidders may have more information.

Definition 5.3 - *Open Auction*
In an *Open Auction* all bids are known to all particpants.

Remark 5.2 - *Assumptions in Auction Theory*
In Auction theory several assumptions are made:

- All auctions are equally attractive (ie there are no auctions where no one turns up);
- There is no collusion between bidders;

These assumptions means auction theory often does not work well in practice.

Remark 5.3 - *Attendance at Auctions*
Entering an auction can be quite involved, so often bidders will skip auctions they don't think they can win.

Definition 5.4 - *Signalling*
During an auction a bidder may place a *'weird'* bid which signals their intent for the rest of the auction to other bidders. This is a form of collusion without any prior agreement necessary.

(Consider the T-Mobile - Mannesbane auction for parts of the german telephone network).

Definition 5.5 - *Reverse Auction*
Reverse Auctions are when multiple suppliers bid for a contract with a single consumer. This is commonly used for construction & suppliment contracts, (inc. by governments).

Often suppliers must be *qualified* in order to *offer* a price.

Definition 5.6 - *Double Auction*
In a *Double Auction* multiple buyers and multiple sellers take part. The sellers offer descending prices, and buyers bid ascending prices. When two prices meet a sale is made between those two parties.

Continuous Double Auctions all buyers and sellers to place bids at any time, and not necessarily in order. This is used in stock exchanges.

Double Auctions are very efficient for price discovery.

Proposition 5.2 - *Trading in the Dark*
Sometimes you do not want to give away your private information (e.g. You dont want to list a large stock sale on a public order book as this would affect the stock price).

Dark Pools are designed to keep your trading intensions secret so that it does not impact price. WARNING it is common for dark pool owners to use this information against their users.

Definition 5.7 - *Posted Auction*
A *Posted Auction* is one where the seller posts a price and then buyers have an option to buy at that price (and that price alone). This is how most shops work.

5.1 Open Auctions

Definition 5.8 - *English Auction*
AKA *Open Ascending-Price Auction*. Used in *Homes under the Hammer*.

i). The auctioneer announces a (low) price to everyone.

ii). If a bidder is happy to pay that price they raise their hand. (Price is reduced if no one bids).

iii). Auctioneer will announce that that bidder is currently winning and will announce a new, higher price.

iv). ii)-iii) repeat until no-one accepts the new higher price (ie no hands are raised)

v). The item is sold to the person who bid last, at the price of that last bid.

Bidders can infer information from when others drop out of an auction. However, with *Private Values* this will not change their strategy (it would for *Interdependence*).

Proposition 5.3 - *English Auction - Optimal Strategy*
Let v be the private value a bidder assigns to an object

- It is not optimal for a bidder to bid a price p if $p > v$ as the bidder makes a loss.

- It is not optimal for a bidder to drop out at a price $p < v$ as the bidder still has surplus demand.

Therefore, the optimal strategy is to bid on any price p that does not exceed v.

Remark 5.4 - *Weak Bidders*
It is harder for a weak bidder to win an English auction as stronger bidders can just accept the next price.

Definition 5.9 - *Dutch Auction*
AKA *Open Descending-Price Auction*. Used in *Dutch Flower Markets*.

i). The auctioneer announces a (high) price to every.

ii). The auctioneer keep reducing the price until someone bids (raises their hand).

iii). The item is sold to this (first) bidder, at the price the auction was stopped.

Proposition 5.4 - *Dutch Auction - Optimal Strategy*
Shade you bid. i.e. bid $p < v$ where v is your private value.

Remark 5.5 - *Robustness*
Collusion is much easier in an open auction, meaning the auction is less robust.

5.2 Sealed Auctions

Definition 5.10 - *Sealed Auction*
In a *Sealed Auction* bidding is done in private. Participants do not know what others have bid.

Definition 5.11 - *First-Price Sealed Bid Auction*
Used to buy *Houses in Scotland*.

i). Auctioneer announces the auction is open and how long it is open for.

ii). Each participant makes a single secret bit.

iii). The highest bid will win, and will pay that price. (ie pay *First-Price*)

Proposition 5.5 - *FPSB - Optimal Strategy*
Shade you bid. i.e. bid $p < v$ where v is your private value.

Definition 5.12 - *Second-Price Sealed Bid*
AKA a *Vickery Auction*

i). Auctioneer announces the auction is open and how long it is open for.

ii). Each participant makes a single secret bit.

iii). The highest bid will win, and will pay the price of the second highest bid. (ie pay *Second-Price*)

Proof 5.1 - *SPSB Auction - Optimal Strategy*
Let v be the private value a bidder assigns to an object, p be the value they bid and c be the greatest value of a competitor bid.

If $p = v$ then

- Bidder wins if $c < p = v$ for a profit of $(v - c)$.
- Does not win if $v = p < c$.

If $p < v$ then

- if $v > p > c$ then the bidder *still* wins with profit $v - c$.
- if $c > v > p$ then the bidder *still* loses.
- if $v > c > p$ then the bidder now loses (making less profit), where they wouldn't have with the previous strategy.

Therefore, bidding $p < v$ never increases a bidders profit. A similar argument can be made for not bidding $p > v$.
The optimal strategy is to bid $p = v$ (same as an *English Auction*)

Remark 5.6 - *Auctions for Sellers*
If buyers are risk averse (ie don't want to lose the opportunity of buying) then FPSB can increase revenues over SPSB auctions.

Remark 5.7 - *Robustness*
Sealed auctions are more robust as you cannot observe other bidders actions, and thus cannot punish a colluder who defects.

Remark 5.8 - *Weak Bidders*
Weak Bidders have a better chance of winning a sealed auction as other bidders may over-shade their bid.

5.3 Equivalent Auctions

Definition 5.13 - *Incentive Compatible*
Auctions are *Incentive Compatible* if they encourage bidders to bid their true value for an item. Incentive compatible auctions stop game playing between bidders as there is no advantage to second guess other users' values. This makes *Incentive Compatible* auctions more predictable and thus favourable for auctioneers.

English & SPSB auctions are incentive compatible.

Remark 5.9 - *Equivalence of English & Second-Price Sealed Bid Auctions*
English & SPSB auctions are weakly equivalent as the optimal strategies are only the same if values are *private* (i.e. there is no *interdependence*).

Remark 5.10 - *Strategic Equivalence of Dutch & First-Price Sealed Bid Auctions*
Bidding a certain amount in a FPSB auction is equivalent to offering to buy at that amount in a Dutch auction. Thus they are *Straegically Equivalent* (for all strategies in one game there is

a strategy in the other which will produce the same outcome).

Theorem 5.1 - *Revenue Equivalence Theorem*
If private values are iid and all bidders are risk neutral, then any standard auction yields the same expected revenue to the seller.

Remark 5.11 - *Revenue Equivalence Theorem*
In practice the *Revenue Equivalence Theorem* does not hold since bidders are not risk neutral (they do have an emotional attachment to goods) and interdependence exists.

5.4 Online Auctions

Remark 5.12 - *Auctions Online*
Due to the algorithmic nature of auction rules & no need for a physical auctioneer or room, the internet enables auctions to be run quickly and cheaply.

Bidding can be automated too, and more complex auction rules can be implemented.

The only limit to online auctions is server capacity and bandwidth.

Remark 5.13 - *Intermediates*
In the beginning of the Internet it was believed that small businesses (e.g. farmer) would be able to sell to customers directly, without the need of an intermediary (e.g. supermarket). This has not been realised as it is much harder to get customers attention online. So *Online Marketplaces* (e.g. amazon, ebay) sprung up to act as intermediaries.

Online marketplaces not host listings but also ease payments and improve trustworthiness of both sellers & buyers.

Remark 5.14 - *eBay*
eBay is one of the most famous online auctioneers. Mainly does consumer-to-consumer and business-to-consumer auctions, but also some business-to-business.

Reviews of sellers act as a lock-in mechanism and part of why *eBay* has an effective monopoly.

eBay auctions are open-ascending auctions with a deadline set before the auction begins (similar to an english auction, but with a time line).

Remark 5.15 - *Snipping*
The timelimit on eBay auctions has lead to phenomena of *snipping*, where bidders wait to place their bid till near the end of an auction in the hope it is too late for anyone else to join (and so as not to give away information about their value).

eBay don't like this as there is hidden information.

To combat this eBay introduced a 'proxy' bidding functionality (if everyone uses this then it is similar to a SPS auction). Alternatively, they could have extended the time limit each time someone bid (similar to a true english auction)

Proposition 5.6 - *Estimating Demand for Dynamic Pricing in Electronic Markets*

i). Track bidders and *'recover'* missing bidders (who could not bid as the price was too high when they first entered). Use this data to estimate a demand curve.

ii). Build a demand and supply curve.

iii). Calculate supplier costs and estimate revenues.

iv). Determine optimal sales quantity/strategy using the revenue and cost curves.

Remark 5.16 - *Google Ad Auctions*
Google understands their customer very well as they know exactly what they are looking for. Adverts for webpages are highly idiosyncratic and thus hard to compare.

Google uses auctions on its ad-space in order to perform price discovery. Multiple auctions are done for each user search (60k auctions per second). Google considers both the *bid price* and the *advert quality* when choosing the winner of an auction, as they don't want their users to get loads of shit adds.

Advert quality is assessed using: Historic click-through-rate; relevancy; and landing page quality (inc. load speed).

This type of auction works best for the seller when there is lots of competition in the auction. To encourage this Google relax the strictness of their keyword matching.

Originally, Google used FPSB auctions but this lead to their servers being overloaded with advertisers checking the results of auctions (to see if they could lower their price). Google then switch to SPSB auctions, solving the server overload problem, as this is *incentive compatible*.

6 Financial Technology

6.1 Financial Technology Firms

Proposition 6.1 - *Key Player - Traditional Banking and Finance*
Traditional Banking and Finance are using technology to automate/improve their traditional business functions (e.g. online banking), this is *digitisation*. Their aim is to increase productivity, efficiency, profit maximization and overlay new services. This is a form of *incremental innovation*.

Proposition 6.2 - *Key Player - Start-Up Technology Companies (FinTechs)*
Start-Up Tech Firms are using technology to introduce new kinds of financial services models. They redesign finance from the ground-up in order to use the technology. Their aim is to disrupt traditional finance through new technology.

Proposition 6.3 - *Key Player - Big Tech (TechFins)*
Big Tech Firms are using their technology dominance to move into financial services. Their aim is to streamline technology processes and lock-in customers. They are leveraging their positive network externalities and customer data.

Remark 6.1 - *Public Perception*
Changes in public perception of who is capable/should provide financial services (partly due to 2008 crash) has allowed for greater competition in the market.

Remark 6.2 - *Underbanked*
Studies have shown that *in the western world* fintech users tend to be young (under 35) and that the more someone earns the more likely it is they will use a fintech product.

But, around 70% of the world do not have access to basic banking facilities. These people of prime customers for certain fintechs. It is important to note that the products these people need are not necessarily the same as richer people. They generally want easy-to-use, simple products (savings accounts and short-term loans are generally inappropriate).

Mobile phones are common, even among low income communities. Thus, fintechs which use mobiles phones have a good chance to reach these customers.

Definition 6.1 - *Financial Regulation*
Financial services have long-since been regulated by government & regulatory bodies. These institutions define rules and directives to control and manage the financial services. The goal of these regulations are to: *protect* actors; improve *competitive efficiency* (ie antitrust lasts & prevention of monopolies); reduce *risk*; and build *trust*.

Remark 6.3 - *Regulation & FinTechs*
Financial Technology is subject to regulation but due to its often novel nature it may require new regulation. Some regulators are much more welcoming to new technologies than others. Some regulators take a *"watch and see"* approach where they allow a new technology to enter a market and then work with the firm to implement regulations (This is known as *Sandboxing*).

Regulators tend to only get involved once a product reaches a certain size.

Proposition 6.4 - *LASIC Principles*
Less & Teo proposed set of principles for a FinTech to succeed:

- *Low Margin*. Allows the business to service whilst offering very low prices to encourage customers.
- *Asset Light*. Reduce fixed costs. Can be done by utilising exists infrastructure (such as mobile phones).
- *Scalable*. The technology and business model must be able to scale (without affect efficiency or costs) in order to reap positive network effects.
- *Innovative*. Encourage adoption.
- *Compliance Easy*. Otherwise model may not be scalable.

6.2 National Banking Maturity

Proposition 6.5 - *National Banking Maturity*
The viability for new financial technologies will vary by country. If we consider the prevalence of banking in a country and the amount of venture capital investment in that country (as a ration of GDP) we can derive four categories which partition countries:

i). *Bank Dominant* - High prevalence, low investment. (e.g. Eastern Europe).
Traditional banking is well established and likely to continue to dominate. Most competition is likely to occur between existing businesses (and not from new FinTechs)

ii). *Partnering* - High prevalence, High investment. (e.g. Western Europe).
Traditional banking is well established, but there is also a strong technology ecosystem. This means it is possible for competition to come from outside traditional banks. It is possible for FinTechs to do well in this environment, although it is likely easier for them to partner with established banks.

iii). *Tech Dominance* - Low prevalence, High investment. (e.g. India & China).
A well-developed tech eco-system exists, while banks underserve the population. This is ideal for FinTechs as there are few established players in the market. Technology and Financial firms may partner in the future so they can utilise each other.

iv). *Race to the Finish* - low prevalence, low investment. (e.g. Sub-Saharan Africa).
Due to under-development technolgy and banking prevelance, telecom companies are often the most significant tech firms in these countries. Meaning, mobile phones are the key technology to utilise to gain a foothold in these markets.

Remark 6.4 - *China*
China uses a *Development-led* approach where it allows technologies to develop first and then adds regulation later (once it is clear where it is needed).

Remark 6.5 - *India*
India uses a *Devlopment-Lagged* approach where regulators largely restrict financial technologies until it it well understood.

7 Bristol Stock Exchange

Remark 7.1 - *BSE*
The *Bristol Stock Exchange* is an open-source piece of software which simulates a stock exchange.

Remark 7.2 - *Visualisation*
There are several ways to visualise prices in a stock market.

- Plot the supply and demand curves for current orders. This lines will be stepped.
- Plot a *lollypop graph* which is a "bar" chart of price against quantity, with bid & ask orders distinguished by different colours.

Definition 7.1 - *Bid-Offer Spread*
The *Bid-Offer Spread* is the absolute difference in value between the highest bid price and the lowest ask price.

$$P_{\text{min ask}} - P_{\text{max bid}}$$

Definition 7.2 - *Midprice*
The *Midprice* is the midpoint (arithmetic mean) between the highest bid price and the lowest ask price. The *Midprice* is an estimate of the market equilibrium price.

$$\frac{P_{\text{min ask}} + P_{\text{max bid}}}{2}$$

The *Midprice* does not consider the quantities available at these prices, meaning a single stray bid can alter the *midprice* dramatically.

Definition 7.3 - *Microprice*

The *Microprice* is the mean value of the highest bid price and the lowest ask price, each weighted by the quantity of the other class of stocks available at that price.

$$\frac{Q(P_{\text{max bid}}) \cdot P_{\text{min ask}} + Q(P_{\text{min ask}}) \cdot P_{\text{max bid}}}{Q(P_{\text{max bid}}) + Q(P_{\text{min ask}})}$$

where $Q(P_c)$ is the number of shares of class c (bid or ask) available at price P.

Definition 7.4 - *Depth*
The *Price Depth* for a specific stock is the number of price levels available.

Volume Depth is the total quantity of a specific stock available.

Proposition 7.1 - *Order Types*
The Bristol Stock Exchange only allows for *Limit Orders* & *Market Orders*.

There are several other order types which are common at other markets

GFD *Good For Day*. Limit order which expires at the end of the trading session/day.

FOK *Fill or Kill*. Only executes if it can be immediately filled in full.

AON *All Or Nothing*. Only executes if it can be filled in full, does not need to be immediate.

IOC *Immediate or Cancel*. Must be filled immediately, but not necessarily in full.

ICE *Iceberg*. Slice a big order into small chunks, each executed sequentially.

LOO *Limit On Open*. Limit order added as a market opens.

LOC *Limit On Close*. Limit order added as a market closes.

MOO *Market On Open*. Market order added as a market opens.

MOC *Market On CLose*. Market order added as a market closes.

OCO *One-Cancels-Other*. A pair of orders, once one is executed the other is cancelled.

OSO *One-Sends-Other*. A pair of orders, once the first is executed the second is sent.

Definition 7.5 - *LSE - Turquoise Plato*
Some exchanges offer sub-exchanges. *Turquoise Plato* is a sub-exchange of the London Stock Exchange. The key features of *Turquoise Plato* are

- It is a *dark pool*, which does not publish a Limit-order book.
- Orders need to be above a certain size in order to be routed to the dark pool.
- Orders in the dark pool are processed in size priority.
- Transactions happening in either the lit or dark pool are published upon completion.
- Larger orders are allowed to specify a minimum execution size.
- Orders have a duration.
- Allows for *Block-indication* orders, followed by *Order Submission Request* (OSR), followed by the actual *Qualifying Block Order* (QBO). This is known as the *Block Discovery Process*.
- Reputation of traders is tracked. If a trader follows a BI order with appropriate QBOs then their reputation goes up. Otherwise it goes down. If their reputation falls too low, the trader is excluded from the block discovery process.

8 Sentiment Analysis

8.1 Theory

Definition 8.1 - *Sentiment*
Sentiment is an individuals attitude or option towards something (i.e. How much they like or dislike it).

Typically *Sentiment* is measured using a *Polarity Value* between -1 (hate) and 1 (love).

Proposition 8.1 - *Importance of Sentiment*
Everyone has an option and can easily share it on the internet (e.g. tweets & reviews). These opinions can have significant economic effects and be drivers for social change.

The CMA estimated $23.3bn$ of uk consumer spending was influence by online review (many in travel and tourism).

Proposition 8.2 - *Yelp Reviews & Restaurants*
The reviews a restaurant receives can seriously affect its business

- A one-star increase on Yelp leads to an $\approx 5\% - 9\%$ increase in revenue.
- The effect is only really seen by independent restaurants (not chains).
- Market share of chain restaurants have decreased, likely due to Yelp helping independent restaurants penetrate the market.
- Consumer response was mainly affected by the number of ratings and the average rating. Some highly rated reviewers have greater swing power.

Remark 8.1 - *Sentiment and Government Policy*
The sentiment of the general public to topics (such as gay rights) are driving factors towards change in government policy.

Proposition 8.3 - *Collecting Public Opinion*
There are a few ways to collect data on public opinion

Traditional Focus groups, customer surveys, opinion polls. These are expensive and time consuming.

Sentiment Analysis Analyse public opinion from online postings. This is hard.

Definition 8.2 - *Sentiment Analysis*
Sentitment Analysis is the process of computationally identifying and categorising opinions expressed in a piece of text. Particularly, to determine whether the author's attitude towards a particular topic is positive, negative, or neutral.

Definition 8.3 - *Topic Modelling*
Topic Modelling is the practice of computationally identifying the topic of a document through text classification.

Remark 8.2 - *Topic Modelling v Sentiment Analysis*
Topic Modelling is typically much easier than *Sentiment Analysis* as it can be done by identifying keywords. *Sentiment Analysis* is much more subtle as there may not be words

which are explicitly positive or negative.

Proposition 8.4 - *Levels of Sentiment Analysis*

Document-Level For a given document, identify the overall attitude to the object under discussion.

Sentence-Level For a given sentence, identify if it expresses a positive, negative, or neutral option.

Aspect-Level For a given document, identify all opinions expressed about a particular aspect of a topic.

Proposition 8.5 - *Document-Level Sentiment Analysis - Supervised ML*
Supervised Machine Learning requires labelled training data. There are some good sources of labelled training data online as many review sites allow authors to give an overall rating to their review (e.g. star rating).

A common approach to sentiment analysis in SML is the *bag of words* approach, which just considers the frequency of words in a sentence (ignoring context). Traditional machine learning techniques (e.g. Naïve Bayes & Support Vector Machine) can be applied to the *bag of words*.

Proposition 8.6 - *Document-Level Sentiment Analysis - Unsupervised ML*
Unsupervised Machine Learning does not required labelled training data.

An approach to sentiment analysis in UML is to consider the relationship between words (how often they co-occur). Classification is then based on *Semantic Orientation*, calculated from mutual information between given phrases in the review and words with explicit sentiment (e.g. excellent or poor).

i). Extract phrases (consecutive words) where the first word is an adjective (the sentiment) and the second is a noun (the context).

ii). Calculate *Pointwise Mutual Information* (PMI) for each of words. PMI determines how strongly words are semantically associated.

iii). Calculate *Semantic Orientation* (SO) for each phrase $PMI_p - PMI_n$ where PMI_p is the PMI of the phrase wrt some strictly positive word (e.g. excellent) and PMI_n is the PMI of the phrase wrt some strictly negative word (e.g. poor).

iv). SO is estimated by querying a search engine and noting the number of hits where the phrase is near (within 10 words) to the reference word (excellent or poor).

v). Calculate the average SO of the document. If the average is positive then the document is likely positive (and visa-versa).

Proposition 8.7 - *Aspect-Level Sentiment Analysis*
A document may contain multiple expression of sentiment regarding different aspects of multiple topic. It is hard to determine which object is being referred to, especially when phrases refer to multiple aspects or topics.

For each phrase there are 5 features which need to be determined

i). The object of the topic.

ii). The aspect of the topic begin discussed.

iii). The sentiment towards the aspect.

iv). Who is expressing this sentiment.

v). When the sentiment was expressed.

Proposition 8.8 - *Aspect-Level Sentiment Analysis - Algorithm*

i). Mark sentiment words and phrases using a lexicon. (i.e. Assign +1 to positive words and -1 to negative).

ii). Identify sentiment shifters (e.g. not, never, cannot) and flip the sentiment value for the words which are shifted.

iii). Identify *"but"* phrases: If the sentiment to one side of the phrase cannot be identified, then it can be considered the opposite of the other side.

iv). Sum the sentiment scores, weighted by the distance a word is from the aspect word.

v). If the weighted sum is positive then the sentiment to the aspect is positive.

8.2 Practice

Proposition 8.9 - *Twitter Sentiment*
There have been successful demonstrations of using sentiment analysis on public tweets to determine outcome of events. Including

- Predicting box office revenues for a movie by consider the number of tweets about a move, per hour, in the week prior to release.
- Predicting the election results. (Although there have been notable failures when trying to replicate).
- Stock market movements using the mood of tweets. Tweets were assigned one of six moods: Calm, alert, sure, vital, kind and happy. The topic of the tweets was ignored but the mood across all tweets was used to predict the directional movement of indexed stocks (e.g. S&P500, FTSE100). (Again there have been failures to replicate)

Remark 8.3 - *Correlation is not Causation.*
Proposition 8.10 - *Gaming The System*
As it has been shown that online sentiment has affect on business, some people have tried to game the system by artificially inflating the online sentiment about their business in order to stimulate sales.

Definition 8.4 - *Brushing*
Brushing is a scam which is popular on amazon where sellers try to get lots of positive reviews.

The general process is

i). The amazon sellers gets the name and address of a customer.

ii). The seller "purchases" an item from their own range and sends it to the customer, stating it is a gift.

iii). Amazon allows individuals who purchase a gift to leave a review for that item, so the seller leaves a very positive review for their own item.

iv). The review is listed as a "verified buyer" on Amazon. Thus giving it greater authority.

v). This artificially inflates the rating of the item and boosts is search ranking.

Remark 8.4 - *Fake Reviews*

- Yelp states if filters out 25% of all posted reviews as they suspected of being fake.
- Samsumg was fined for paying people to leave positive reviews for their products and to criticise HTC products.

Definition 8.5 - *Sockpuppetry*
A *Sockpuppet* is an online identity used for purposes of deception. The *Sockpuppet* poses as an independent third-party who is unaffiliate with actual account operator. The *Sockpuppet* account is then used to praise, defend or support the actual account operator and thus manipulate public opinion.

Sockpuppetry works as people default to crowd opinion. There are several types of *Sockpuppetry* practices

- *Ballot Stuffing* were multiple votes are submitted in online polls to favour the puppeteer.
- *Sybil Attack* where multiple false identities are used to create influence within a peer-to-peer online network.
- *Stealth Marketing* where multiple sockpuppets, each claim to be enthusiastic supporters of a product/service.
- *Starman Sockpuppet* where sockpuppets are used to make a particular point of view look foolish in order to generate negative sentiment; or, for the puppeteer to easily refute.
- *Astroturfing* using sockpuppets to make it appear that a particular message is coming from a grassroot support, rather than from a large company.

Persona Mangement Software help manage sockpuppets by

- Creaing diverse & plausible online personas with static IP addresses.
- Allowing puppeteers to randomly select different personas each day.
- Blend traffic in with users from outside the organisation to provide cover & plausible-deniability.

Proposition 8.11 - *Sockpuppet detection*
An approach to detecting sockpuppets is to create a network which links online personas based on each time they express a similar view. Identify clusters within this network. Analyse the writing styles within the clusters, with those that match likely to be sockpuppets.

Common trends of sockpuppets is

- Similar IP addresses.
- Similar online names.
- Similar registration times.
- Similar login patterns.

Proposition 8.12 - *Likely Fakes*
The following are cases where a review is likely to be fake

- It is a duplicate review. Further
  - Negative outlier reviews are more commonly spammed, than positive outliers.
  - Singleton reviews are often fake.
  - Top-ranked reviewers are more likely to post fake reviews.
- Identify atypical behaviours. E.g.
  - Promoting or victimising a few target products.
  - Targeting a group of products in a short period of time.
  - Tending to give polarised scores.
  - Given ratings which deviate from those of other reviews of the same product.

9 The Crowd Economy

Definition 9.1 - *The Crowd Economy*
The Crowd Economy is the group of platforms which rely on active participation from large crowds of people online. (e.g. wikipedia & AirBnB).

Definition 9.2 - *Crowdsourcing*
Crowdsourcing uses crowds for to reach certain (non-monetary) goals

- Citizen engagement.
- Mass Collaboration.
- Crowd tasks.

Proposition 9.1 - *When to use Crowdsourcing*
Crowdsourcing is good when a task is difficult for a computer to perform: such as labelling images.

Proposition 9.2 - *Crowdsourcing - Finding Participants*
There are a few ways to get people to partake in crowdsourcing tasks

- Pay them.
- Trick them into doing it, generally as a side effect of something they want to do (e.g. CAPTCHA).
- Motivate volunteers. Generally by making it worthwhile/fun.

Definition 9.3 - *Crowdfunding*
Crowdfunding uses crowds to raise money. This can take several forms

- Donation Based.
- Reward Based. Funders receive a reward based on how much they pledge (typically the product the company will product).
- Equity Based. Funders become share holders.

- Debt Based. (Peer-to-Peer Lending). Cheap loans relative to traditional banks. Risk of debtor defaulting.

In the UK both *Equity Based* and *Debt Based* crowdfunding is regulated by the FCA, in the same way as traditional providers.

Definition 9.4 - *Mechanical Turk*
Mechnaical Turk is Amazon's crowd-based "job" market. Companies can post jobs and then users can choose to complete then for a fee.

10 Prediction Markets

Definition 10.1 - *Prediction Markets*
Prediction Markets use the knowledge of crowds to predict the outcome of some future event which has an uncertain outcome (but it is verifiable after the event whether the prediction was correct).

These markets require on participants being honest & unbiased. This is generally done by getting people to "put their money where their mouth is" (i.e. pay-to-play).

Proposition 10.1 - *Types of Market*
There are two ways a *Prediction Market* can pay out

- *Winner-Takes-All* where a fixed value is payout if a particular event happens (e.g. wins an election). Here the sum price of all contracts should equal the fixed value payout.
- *Vote Share* where payout percentage is based on a quantitative outcome (e.g. number of MPs won).

Example 10.1 - *Prediction Market*
Consider a future event with two possible future outcomes: X and Y.
Suppose we create two futures contracts: one paying if X occurs, and the other if Y occurs (Winner-Takes-All Market). These contracts can be traded and their values with vary over time. The Winner-takes-All market keeps traders honest as they have nothing to gain by choosing an event they believe to be sub-optimal.

If a CDA is used to trade these contracts then the relative current trade price can be considered as a measure of the collective market's belief of an event occurring.

Since traders want to make a profit, traders should buy a contract that they believe to be underpriced and sell a contract their believe is overprice. This means they don't necessarily buy the contract they believe is most likely to pay out, but the one which they believe is most under valued.

Definition 10.2 - *Arbitrage*
Arbitrage is the act of simultaneously buying/selling across markets to make a risk-free profit.

Consider a *Winner-Takes-All* market which pays 1 to whichever of two events occurs. If the sum price to buy a contract for each event is below 1 then you are guaranteed to make a profit. In this event you should buy as many pairs of shares as you can.

Arbitrage opportunities don't last for long as the increased demand causes the price of both contracts to rise, thus removing the guaranteed profit. Thus *Arbitrage* opportunities often only

occur when trading the same event in different markets.

11 Blockchain

Remark 11.1 - *Limitations of Current Set up*

- There are intermediary fees between seller & buyer transactions. Meaning neither gets full value of a transaction, and thus this could be considered an inefficency.

Remark 11.2 - *Which is the true chain*
If there are two conflicting blockchains, then the longer one is accepted as the truer version. (As it takes less work to add the conflicting nodes of the shorter chain onto the longer chain than visa-versa).

11.1 Evolution - Road to BitCoin

Remark 11.3 - *Road to Bitcoin*
Early in the internet secure HTTP protocols were not fully developed, meaning any only payments would be done without good encryption (very risky). There were many attempts to create secure payment systems, some of the major steps a laid out here.

Proposition 11.1 - *Credit Based Architectures*
There were two main early *credit based architectures* for secure payments

- *FirstVirtual* - An intermediary credit-based architecture (similar to PayPal). Limitation was that customers had a 90 day dispute window, and companies did not receive money until after this period.
- *SET Architecture Standard* (Visa & MasterCard) - Avoided the need for customers to enrol with an intermediary. Users install a shopping app onto their machine and store their details there. When a purchase is made, the app encrypts the details and then sends to an intermediary (Visa/Mastercard) to decrypt. Limitation was that it required end-user certification which was complicated and no-one could be bothered.

Proposition 11.2 - *Cash Based Systems*
DigiCash was a cash based system for payments which used *eCash* coins. Users bought eCash which they could then spend with merchants, merchants could then redeem the eCash for a fiat currency. The value of eCash is pegged to the value of the fiat currency. This is similar to many premium currencies in video games.

Each coin had a unique ID and a central database was used to prevent double-spending. Ownership of coins was secure as users chose the ID number for their coin (ideally something long and unique).

Limitations were that only buyers were anonymous, not sellers (and coins had to be returned to the centralised system by sellers), and it was hard to do user-to-user transactions. Moreover, it was hard to persuade people to use so it did not reach critical mass.

Remark 11.4 - *Free-Floating Digital Currency*

A *Free-Floating Digital Currency* is a digital currency which is not pegged to a fiat currency. These have value due to scarcity (by design). Digital currencies are made scarce by making minting money hard (e.g. make it a hard puzzle).

Remark 11.5 - *HashCash*
HashCash was a computational puzzle intended to limit spam emails.

The puzzle for each email depended upon the sender, receiver, content and time (each puzzle is unique and independent). The sender has to solve the puzzle (taking a minute or so) before sending, but it is easy for the receiver to verify the solution. If the senders solution is wrong then the email is deleted.

The difficulty can be adjusted to combat improved hardware.

HashCash disappeared due to improved spam filters.

Remark 11.6 - *Ledgers for Timestamping*
Haber & Stornetta introduced the idea of using ledgers to timestamp documents in 1991. This prevents the timestamp from being changed.

Clients send documents to a trusted server to be stamped, a copy of the document is saved and a certificate of validation is issued. Much like a Notary.

To make this more efficient, documents were linked into a tree structure creating a block, and then linking blocks to create a chain.

Proposition 11.3 - *BitCoin - Generation 1*
The first generation of *BitCoin* learnt from the flaws of the previous systems.

- No centralised "trusted" server (Unlike Haber & Stornetta).
- Enable user-to-user transactions and anonymity in order to help reach critical mass (Unlike DigiCash).
- Simple to secure and use (Unlike FirstVirtual and SET)
- Used mining to regular currency creation (An attaptation of HashCash)

The novel features of BitCoin was that it had a decentralised mining process which did not require trusted servers. Also, it was open-source and part of that community became passionate about BitCoin, helping it reach critical mass.

Remark 11.7 - *BitCoin - A libertarian dream*
Due to the decentralised and anonymous nature of Bitcoin, it became a bit of a libertarian dream. No one can see how, or tell you how to spend you BitCoins (no tax! Hype!).

Infamously, these same features lead to bitcoin being popular for illegal and illicit activity (e.g. Silk Road).

Remark 11.8 - *Can you track bitcoin payments?*
BitCoin is pseudo-anonymous rather than fully anonymous. Users can be identified by their wallet IDs, but it is hard to get ahold of this information. As the ledger is public, if you known someone's wallet ID you can see and track all their payments.

11.2 Bitcoin

Definition 11.1 - *Bitcoin*
Bitcoin is a digital currency based on blockchain.

Definition 11.2 - *Blockchain Block*
Each *Block* on the *Blockchain* has a *header* containing the following

i). Timestamp and version number.

ii). A hash of the previous block header. This links this block into the chain.

iii). A *merkle root* summarising the new transactions that the block contains - this means every block will contain a history of all bitcoin transactions. (This makes it hard for someone to change the block as this value would be inconsistent with other blocks in the chain).

iv). A *nonce value* chosen by the miner such that when the header is hashed using $SHA256^2$ the resulting 256-bit hash has at least x leading 0s. The greater the value of x the harder the nonce discovery step is. This step generally requires a lot of brute force work to find a *golden nonce value*.

Using $SHA256^2$ makes the hashing practically irreversible.

After the header, there is a list of transaction that are recorded by the block (and summarised in the block's header), including the transactions that pays the miner their fee.

Definition 11.3 - *Bitcoin Miner*
Bitcoin Miners can add transaction onto the blockchain. They compete to be the first to mine a block in order to keep the fee from all the transactions in the block (and a block reward (new bitcoins added into the economy)).

Miners stop mining a block once they are told that the blockchain has been extended.

Definition 11.4 - *Bitcoin Rewards*
The rewards payed to miners act as a way for new bitcoins to enter circulation and encourage miners to complete the computation difficult process of mining. The value of the reward is regular decreased (halved every 10,000 blocks 4yrs) in order to control money flow.

Mining is meant to be hard, as this acts as "proof of work", keeping blockchain consistent and reliable.

Proposition 11.4 - *Bitcoin Transaction Step*
For a *Bitcoin* Transaction to occur the following need to be fulfilled.

i). Two parties agree a transaction. (ie what value will be transacted). Typically a "fee" is added to the transaction in order to encourage bitcoin miners to complete their transaction quickly (the miner keeps the fee).

ii). Create a transaction message. The message is created by the purchaser and has three components

(a) A reference to the transaction in which the purchaser gained the bitcoins they will now spend.

(b) The addresses involved in the payment (purchaser and seller).

(c) Amounts to be be payed to each address (change is payed to the purchaser).

iii). Sign the transaction message. The purchaser signs the message by encrypting it using their private key. (Others can confirm that the message was made by this purchaser by using the purchaser's public key to decryt it).

iv). Broadcast the transaction message (along with the purchasers public key) across the distributed network of bitcoin participants. Each peer in the network validates the transaction meets certain constraints. (Note the transaction is not on the ledger yet).

v). Verify the transaction message.

Remark 11.9 - *Forks*
Suppose block Z is the globally agreed end of the chain. Now suppose two nodes complete mining different blocks at the same time R and G respectively. They will propagate these sucessful minings out and that they should be placed after block Z. The network is no longer globally consistent as some notes will have $Z \to R$ and some $Z \to G$ as the end of their version of the chain.

Now suppose a node, which has $Z \to G$ as the end of its chain, successfully mines block P and propogates it out as occuring after block G. This will cause a *fork* at nodes which have $Z \to R$ as the end of their chain. For these nodes, block R is orphaned (and needs re-mining) and the end of their chain now looks like $Z \to G \to P$.

Definition 11.5 - *Blockchain*
Blockchain is a distributed ledger.

Remark 11.10 - *R3 CEV LLp*
R3 is a consortium of banks which are developing a blockchain technology for recording inter-bank transactions. This has been criticised as blockchain tech is often slower and more expensive than the existing tech.

Remark 11.11 - *Concerns around Bitcoin*
There are several concerns about bitcoins (although many are shared with physical currency).

- Theft or loss of private keys. (Equivalent to loosing physical wallet or forgetting pin).
- Loss of anonymity.
- Attacks (DDos & Sybil Attacks).
- Overall energy consumption.
- Illegal content on the block chain.
- EMP bomb.
- Exchange/Value collapse.
- Future behaviour of bitcoiners is uncertain.

Moreover, many academics believe that blockchain itself is flawed (or at least very overhyped).

Remark 11.12 - *Blockchain is a Libertarians dream*

Due its decentralised nature. Although, there is still a concentration of people who perform most the work and thus hold most the power in the blockchain (And these people are, generally, anonymous!)!

Proposition 11.5 - *Technological Context of Blockchain*
Blockchain is a small subset of *Distributed Systems Tech.*

Definition 11.6 - *BitCoin Scripts*
BitCoin Scripts is a scripting language for BitCoin transactions.

BitCoin Scripts are simple and compact, with native support for cryptographic operations. It is stack-based, so every instruction is execute only once in a linear manner (ie no loops). It is not turing complete

There is an upper bound on the number of instructions in a script and the memory usage of a script, ensuring there are no infinite loops which miners could get trapped in.

The script contains basic instructions (arithmetic, if-else etc.) and crypto instructions for hashing and signature verification. You can specify arbitrary conditions which must be met in order to spend a coin.

Here are some of the instructions

T-of-N MULTISIG requires T signatures of N public-keys to agree to determine the outcome of the transaction. A 2-of-3 MULTISIG is common as only the buyer and seller need to sign (and if there is a dispute a third party can decide).

Remark 11.13 - *MULTISIG creates escrows and allows for smart contracts, without laws.*
Definition 11.7 - *FPGAs*
Field Programmable Gate Arrays allow for a configurable system which get close to the performance of custom hardware. *FPGAs* are an alterative to GPUs in bitcoin mining, they are quicker but the cost-per-performance-gain is marginal.

Remark 11.14 - *Who is mining*
Howadays most mining is done professionally which has lead to a centralisation of mining power (not very libertarian!). Over 70% of all mining occurs in China.

The annual electricity consumption of these mining operations is greater than that of many developed countries, including Switzerland & Czechia.

Proposition 11.6 - *Bitcoin Mining Limitations*
Bitcoin is designed to be time-consuming (for proof-of-work) taking around 10 minutes to mine each block. As each block contains at most 4,000 transactions this means the average throughput is 7 transactions a second. (Note that visa averages 2,000 per second and peaks at 10,000).

Proposition 11.7 - *Can you update BitCoin protocols*
Updating BitCoin protocols requires a hard-fork of the blockchain. This is unviable, as the global community are unlikely. Meaning the only solution is to start again.

11.3 Replacements to BitCoin

Proposition 11.8 - *Replacements to BitCoin*

There have been several new cryptocurrencies which seek to fix some of the limitations of BitCoin.

Ethereum 2.0 has a turing complete scripting language, which can write smart contracts of any complexity.

Cardano 3.0 has an efficient proof-of-stake mining process.

HyperLedger Fabric allows for private & permission based ledgers, specifically with business uses in mind.

Proposition 11.9 - *Ethereum 2.0 (2015)*
Ethereum mainly extends the ability to write and perform code, directly in the blockchain. This is done by having a turing complete decentralised virtual machine (EthereumVM) which can execute code using a network of public nodes. This allows for a sophisticated smart contracts and decentralised applications (DApps).

Smart Contracts are code which can be executed in the blockchain. DApps are a collection of one or more smart contracts and a front-end interface which allow users to interact with the system.

Ethereum is limited due to inefficiency in proof-of-work computations.

Proposition 11.10 - *Loops in Ethereum*
Ethereum allows for loops. But to prevent infinite loops it introduces the idea of "Gas". Each VM instruction requires a small payment of "Gas" (paid in etherum) to run. Different instructions cost different amounts (persistent storage is expensive). "Gas" is paid to the miner who executes the contract query (similar to the transaction fee in BitCoin).

A "Gas Limit" causes the program to halt when reached, preventing infinite loops.

Proposition 11.11 - *Decentralised Applications, DApps*
DApps are decentralised applications which have a web interface (typically a standard website) plus one or more smart contracts (for executing instructions on the ethereum blockchain). A users account for a DApp is a digital blockchain key which is stored on a computer's drive. This allows users to have more control over their data.

DApps typically raise money by selling their services (in the form of tokens).

Proposition 11.12 - *Decentralised Autonomous Organisation, DAO*
A *Decentralised Autonomous Organisation* (DAO) is an organisation which is fully represented by code which is transparent, controled by share holders and not influenced by a central government. (ie a whole organisation of a DApp).

Proposition 11.13 - *Cardano 3.0 (2015)*
Cardano 3.0 intoduced the following developments

- *Multi-Layered Approach* - Separating transactions/tokens from code & contracts. This helps scalability.
- Uses a proof-of-stake protocol rather than a proof-of-work protocol. This is much more efficient whilst still being secure. (Specifically the *Ouroboros Protocol*)
- Introduced *Permissions* to enable private networks.

Proposition 11.14 - *Proof-of-Stake Protocol*
The *Proof-of-Stake Protocol* does the following

- Calculate all miners "stake" in the cryptocurrency, by using the ledger to count the verified tokens each miner owns.
- Select the next miner m at random with the probability of a miner being picked being equal to the ratio of their stake to the total stake (of all miners).

Provided the random process is fair, we have a system that is equivalent to proof-of-work (ie as secure as), without the wasteful need to do any work.

Proposition 11.15 - *Ouroboros Protocol*
The *Ouroboros Protocol* is the *proof-of-stake* protocol used by Cardano. *Ouroboros* ensures true randomness by implementing a secure multiparty implementation of a coin-flipping protocol.

Proposition 11.16 - *HyperLedger Fabric*
HyperLedger is an open-source standard designed for cross-industry blockchain standards. It is hosted by the *Linux Foundation*.

HyperLedger Fabric is an enterprise-grade, distributed ledger platform that offers modularity and versatility for a broad set of industry use cases. THe modular architecture accommodates the diversity of enterprise use cases through plug-and-play components (inc. consensus, privacy and membership services).