

# **Internet Economics and Financial Technology**

Josh Felmeden

November 15, 2021

## Contents

<b>1</b>	<b>The Big Picture</b>	<b>4</b>
1.1	Expanding the big picture . . . . .	4
<b>2</b>	<b>Big Money</b>	<b>4</b>
2.1	Positive Feedback . . . . .	4
2.2	The Long Tail . . . . .	5
2.2.1	Power-Law distribution of popularity . . . . .	5
2.2.2	Criticism of The Long Tail . . . . .	5
2.2.3	Support for The Long Tail . . . . .	5
2.3	Disruptive Technology . . . . .	6
2.3.1	The Innovator's Dilemma . . . . .	6
<b>3</b>	<b>Internet Economics</b>	<b>7</b>
3.1	Micro Economics . . . . .	7
3.2	Production costs . . . . .	7
3.2.1	Competitive markets . . . . .	8
3.2.2	Monopolistic Markets . . . . .	8
3.3	Economics of the Internet . . . . .	8
3.3.1	Consumers . . . . .	9
3.3.2	Producers . . . . .	9
3.4	Pricing Strategies . . . . .	10
<b>4</b>	<b>Auctions</b>	<b>11</b>
4.1	Auction Theory . . . . .	11
4.1.1	Terminology . . . . .	11
4.1.2	Equivalent Auctions . . . . .	12
4.1.3	Revenue Equivalence Theorem (RET) . . . . .	13
4.2	Auctions in Practice . . . . .	13
4.3	Online Auctions . . . . .	14
4.3.1	Double Auction . . . . .	15
<b>5</b>	<b>Financial Technology</b>	<b>15</b>
5.1	Development Landscape . . . . .	15
5.1.1	LASIC . . . . .	16
<b>6</b>	<b>Economic Agents and Market Based systems</b>	<b>16</b>
6.1	Background Economics . . . . .	17
6.2	Market Metrics . . . . .	17
6.3	Maths Behind ZI-P . . . . .	18
<b>7</b>	<b>Empirical Methods</b>	<b>19</b>
7.1	Confidence intervals . . . . .	19
7.2	Comparing method A with method B . . . . .	19
7.3	Choosing a test . . . . .	19
7.3.1	Wilcoxon-Mann-Whitney U Test . . . . .	20
7.4	Adjacent Values . . . . .	21

<b>8 Options and Betting Markets</b>	<b>21</b>
8.1 Short-selling . . . . .	21
8.2 Derivative Contracts . . . . .	21
8.3 Equity Options . . . . .	22
8.4 Options Strategies . . . . .	23
8.5 Betting Exchanges . . . . .	23
<b>9 Economies of Gaming</b>	<b>23</b>
9.1 Economics of Game Development . . . . .	23
<b>10 Sentiment Analysis</b>	<b>24</b>
10.1 Unsupervised learning . . . . .	25
10.2 Aspect Level Sentiment Classification . . . . .	25
<b>11 Crowd Economics</b>	<b>25</b>
11.1 Prediction Markets . . . . .	25
11.1.1 Iowa Electronic Markets IEM - Winner Takes All . . . . .	26
11.1.2 Vote Share Market . . . . .	26
11.2 The Crowd Economy . . . . .	27
11.2.1 Crowdsourcing . . . . .	27
11.2.2 Crowdfunding . . . . .	27
<b>12 Blockchain and Bitcoin</b>	<b>28</b>
12.1 Anatomy of a block . . . . .	29
12.2 Nonce Values and Difficulty . . . . .	29
12.3 Successfully Verifying the transaction . . . . .	30
12.4 Bitcoin Concerns . . . . .	30
12.5 Blockchain Evolution . . . . .	30

# 1 The Big Picture

Based on past events, it is possible that we have reached the climax of the IT revolution. The migration to cloud technology is mirrored by the migration of electricity from home generators to power stations. From here, there have only been marginal improvements in this field, and this could be the same in the tech sector.

Similarly, this was seen in the explosion of the ‘.com boom’ seen later. This rapid growth was due to people investing lots of money in the technology; a mania. Again, this has been seen before in history with the development of canals.

Another bubble popping phenomena was the collapse of the American housing market, where the stock market collapsed. Humans are really good at messing up financially, and also inventing tech that can revolutionise the world.

Essentially, what I’m getting at is that in the financial sector, trading is mostly done by computers. Obviously, these computer traders have no common sense, which worries a lot of the big companies, and investigations have been done into this.

## 1.1 Expanding the big picture

This section is the only section where we will discuss the history of finance, so bear with me here. Looking at the last 250 years of technology ‘surges’, we can possibly gain insights about the current surge.

1. Industrial revolution (1770-1873)
2. Steam and railways (1829-1873)
3. Steel, electricity (1875-1918)
4. Oil, Car, Mass production (1908-1974)
5. IT and Telecoms (1971-??)

If the IT surge ends at the mean duration, then we can expect the surge to end in 2024. This end does not mean the end of the world, just that the time to make great fortunes has passed.

So, computer science is no longer *just* about computer science. Because of this surge, there is great interplay between this field and others, such as finance.

# 2 Big Money

## 2.1 Positive Feedback

Successful companies have won out for a whole host of factors, but history tends to focus on the winners. *Positive feedback* and *network externalities* can help to elevate a company or product to success, even if it has superior rivals.

## 2.2 The Long Tail

The long tail was named and popularised by Chris Anderson. In the old days, Retailers could make money on high-volume, low-margin goods or low-volume, high-margin goods. This is because shops had shelf volume that, if filled up by low-volume, low-margin goods, would be making a loss on these products, since physical space costs money. Thanks to the advent of online markets, 'shelf' space costs almost nothing, meaning that shops can now stock the low-volume, low-margin goods.

In examples such as the music industry, these less popular goods still have returns that would be beneficial for the vendor. In fact, no matter how far down the popularity graph you go, there is still money to be made. This tail is called the *long tail*.

### 2.2.1 Power-Law distribution of popularity

The power law appears a weirdly large amount in terms of popularity, which is of the form  $P = cR^{-v}$ . This makes the graph dip very sharply early on, but level off; never reaching zero.

As it turns out, the biggest money could be made in the smallest scales (if they are done large scale). The way to do it is:

1. Make everything available
2. Reduce prices
3. 'Help me find it'

### 2.2.2 Criticism of The Long Tail

Does the long-tail effect really exist? One observation is that the web actually *magnifies* the importance of 'blockbuster' hits. However, Anderson disagrees with this, stating that it is all about where you define the head and tail of the power-law curve and whether you use absolute values (since the criticism compares percentages).

Another criticism stated that music sales exhibited a log-normal distribution rather than a power-law curve. They reported that 80% of the music tracks they monitored sold NO copies at all over a one-year period. This was disputed poorly by Anderson.

### 2.2.3 Support for The Long Tail

The Long Tail has been proven to have grown longer over time. Niche books now account for around 37% of Amazon's sales. Additionally, a longer but also fatter tail has been observed on consumer software downloading patterns. However, this is only for software, which would behave differently than the entertainment sector.

## 2.3 Disruptive Technology

A technology company may have some form of technology and a projected performance. The company will also have an idea of the improvement required by the mainstream market. As long as the technology offered improves faster than the mainstream market's demands, the company is going to do fine. However, these are just predictions, and therefore this prediction must be monitored.

Some time into the future, a new technology appears with a much smaller performance and market than yours. However, it may have another benefit (smaller/cheaper/lighter), meaning that other companies invest in this. Because our company is already doing well, it is not a threat and we are not interested in it. The research team also conclude that the technology will not improve as fast as ours, therefore, our technology will always outperform the new one.

This prediction is true for a long time. At a certain point, the needs of the mainstream market are met by the new technology. Despite our technology being far above the needs of the consumer, the market is taken away from us, because our technology is far too advanced, and the new technology has other benefits that the mainstream market find more attractive, causing our company to be obsolete.

### 2.3.1 The Innovator's Dilemma

There are two different types of innovations:

- **Sustaining Innovations:** Incremental improvements on existing products or services that are attractive to existing customers and business models. Eventually, you offer more than the customer wants
- **Disruptive Innovations:** perform perform less well than existing products, perhaps being lower quality or less sophisticated, but they are also simpler, cheaper, or more user friendly.

These disruptive innovations can cause strong incumbent companies to fall or falter, not due to weaknesses in these companies, but because they do the right think short-term; leaving the lower end of the market to others.

The *dilemma* is the choice between doing what made the company a success in the first place, or investing in a lower quality prospect, meaning that sometimes successful incumbents need to invest in the 'wrong thing'.

Very often, this is the sequence of events:

- The disruptive technology is developed by the incumbent company
- The existing customers are unimpressed
- Therefore, the company stops developing the disruptive technology and instead concentrates on sustaining innovations
- New companies form (sometimes from disgruntled ex-employees of said company) and develop a new market for the disruptive technology
- As the disruptive technology matures and improves, it moves 'up the chain'
- The company then realises that there is significant demand, and attempts to enter as a late-comer. It fails to do this due to the lead built already by these new companies.

## 3 Internet Economics

### 3.1 Micro Economics

Micronomics studies the behaviour of individuals and businesses and how decisions are made based on the allocation of limited resources. This income can then be used to make or provide other resources, giving us a cycle. Consumers have a finite amount of resources, so the price of the goods needs to be well placed so the consumers will buy. But also, consumers have a finite amount of resources, so the supply also needs to be carefully placed. These interactions can become quite complicated quite quickly.

Supply and demand is at the heart of this. On the one hand, we have the amount demanded by the consumers, and on the other, the amount supplied by the producers. The **equilibrium** of these two values is when they are the same.

Excess demand means that consumers are fighting over the finite goods, meaning that the price rises; perhaps above the equilibrium. Some consumers will be unlikely to buy at this inflated price, meaning that the equilibrium returns.

Excess supply causes prices to fall, and some producers are unlikely to want to continue creating these goods, returning the equilibrium.

Every individual has a different amount of a certain good that they demand. If we aggregate these demands, we get a *demand curve*. The law of diminishing marginal benefit means that the demand will have a downward slope as we go up in quantity. The *gradient* of the curve tells us the **price elasticity** of demand. If the gradient is small (i.e. small elasticity) a small change in price results in a large change in quantity demanded. Conversely, *inelastic* demand means that a large change in price results in a small change in quantity demanded.

How quantity demanded changes in relation to a price:

- Horizontal demand: **perfect elasticity** (a change in quantity has no effect on price)
- Vertical demand: **perfect inelasticity** (fixed quantity demanded, regardless of price)
- 45-degrees: **unit elasticity** (percent change in price equals percent change in demand)

### 3.2 Production costs

Running a business has associated costs:

- **Fixed costs**: a company must incur fixed costs in order to operate. They are fixed during a short time period.
- **Variable costs**: these tend to rise with increased production
- **Semi-variable**: labour can be considered a variable cost, because if paying overtime hours, or if you decide to hire more people to cope with increased workload.

We can graph the costs against quantity produced. **Economies of scale** are increased profit when the company is first scaling. After this, we see **diminishing marginal returns**. The marginal cost

curve tends to be upwards sloping, and firms need to cover their marginal cost of each additional unit produced. Therefore, the minimum price they will supply their product is the MC. They also need to cover their AVC. The supply curve for a firm is the curve that appears above the production costs.

As with elastic price, there is also elastic supply. **Elastic supply** can accommodate a large change in supply for relatively small additional costs, while **inelastic supply** means an increase in supply requires high additional costs.

### 3.2.1 Competitive markets

A **competitive market** creates efficient allocation of resources at equilibrium where quantity generated matches the quantity demanded. If there is an excess of demand, the price will increase, and vice versa.

Supply and demand curves show the price-quantity relationship. A change in another factor can shift the demand/supply. This shift can be represented by a change in either line causing a new equilibrium.

### 3.2.2 Monopolistic Markets

Sometimes, as a single firm grows to take over an entire market. This firm would be called a *monopolist*. In the real world, complete monopoly is rare, and so if a firm owns more than a quarter of the market, it is considered a monopoly. In a competitive market, firms are price takers. Each firm supplies a very small proportion of the market so no matter how much they produce, there will only be demand at a price. Conversely, for a monopolist, they are the only provider, so the demand curve is the same as the market demand curve. They are able to set the price to whatever they like, since they have no competition.

## 3.3 Economics of the Internet

The internet has disrupted the business landscape:

- **Combinatorial innovation** — components can be combined and recombined to create new products or services — has accelerated due to the internet.
  - 1800s, standardised gears revolutionised manufacturing
  - Internet revolution — innovations are rapidly distributed globally, many innovations are open-source and standardisation is easier and more necessary.
- Economic laws have not fundamentally changed, but the characteristics of online business activities can result in different markets.

Online economic activities consist of:

- Digital goods
- Information goods



- Online purchasing of physical goods
- Online provision of services

Digital differences between digital and physical goods:

1. Digital goods tend to be costly to produce, but cheap to reproduce. Fixed costs are high, but variable costs are low
2. Most of the production costs are *sunk* (cannot be recovered) unlike a factory, for example, which can be resold after
3. There are no capacity constraints limiting the number of times something can be reproduced.
4. Digital goods are often *experience goods* (customer doesn't know the value without using them)
5. Searching online is easy, so search costs for the customer is very low
6. *Positive network externalities* are often strong — the value to you increases as more people use it.

### 3.3.1 Consumers

If the production and consumption of a good or service affects the third party who was not involved, then they are a *externality*. A **negative externality** imposes costs on the others (such as pollution). **Positive externality** has benefits (such as spending on education).

**Network externalities** is a kind of externality that occurs when the act of buying a product confers indirect cost or value on all those who already own the same product or service. A **Negative network externality** imposes costs on others who also own the product (such as car purchase increasing road congestion). **Positive network externality** provides benefit to others who also own the product or service (such as telephone that makes you available for others to call). The term *network effect* is often used in a positive way.

The network effect is a very powerful effect. The demand curve of this is initially upward sloping, meaning that the initial marginal cost is very large. This is because the network is growing, and so is of more benefit to the consumer. After a while, this tapers off, and the demand curve ends up looking hyperbolic. The midway point in the upward curve is the *critical mass*. This is the quantity of users that must be reached for the network to be viable.

**Switching** from one product from one product or service to another can have additional cost. When this cost becomes very high, a user is said to be *locked in*. In the digital domain:

- The consumer would have to retrain to learn another service or software
- The consumer would have to convince their friends/peers to switch too
- The software needs to be set up again
- There will be reduced quality of service in the short term because of the information that is stored by one company that will not be transferred to the other.

### 3.3.2 Producers

For the competitive markets:

- Short term: supply curve is MC above AVC (average variable cost)
- Long term: supply curve is MC above ATC (average total cost)

If two companies are competing with identical digital products as their variable costs are near zero, competition will drive the price down to near-zero. A new company won't want to risk competing with an existing company because the set up costs are high compared with the possible profits. The risk is further enhanced by the network effect as any new product must reach the critical mass or it will fail. Additionally, switching costs and lock in mean that users are less likely to swap to the new product. Therefore, for commodity digital goods, there is a tendency towards monopoly. To succeed, companies must therefore focus on product differentiation or competing for emerging future monopolies.

For digital products with a strong network effect and high switching costs, we expect to see monopolies occurring.

Producers greatly gain from having a monopoly and therefore will try to retain this. *Proprietary formats* are a powerful means of enforcing monopoly, such as the .doc format of Word. OpenOffice reverse engineered this, reducing lock-in, but switching costs meant that it was not widely uptaken. As a result, Word is still dominant, but OpenOffice is making inroads.

**Standards** help to stop this. Adopting industry-wider standards allows a user network to be shared between providers. This seems detrimental, but the network value is greatly increased. There are multiple ways a standard can be introduced:

1. Standards have a *leader*, that sets the standard for the industry
2. A *standard war*, where two or more producers compete to dominate
3. A *standards negotiation*, where two or more producers negotiate a standard collectively

### 3.4 Pricing Strategies

There are three degrees of **price discrimination**

- **First-degree:** Perfect price discrimination. The business charges the maximum possible price for each unit sold. It is hard to know everyone's individual spending habits, so is not often used anymore
- **Second-degree:** When a company charges a different quantity consumed, such as quantity discounts on bulk purchases, or versioning (premium, standard, free tiers). This means buyers self-select and reveal their type via their selection. Much easier to employ this in the digital world.
- **Third-degree:** Grouping a product by a certain group, such as cinema tickets with students, adults, children, etc. Buyers cannot choose their group.

For price discrimination to take place, a seller must satisfy three conditions:

- Distinguish between customers
- Have enough market power
- Resale must be impractical, costly, or forbidden

Price discrimination can also be controversial for a variety of reasons, and sometimes against the law.

Bundling is another form of versioning and is the practice of selling several goods together for a single price, such as Microsoft Office. It's used to sell to customers who would otherwise not buy. Can help to keep a monopoly.

## 4 Auctions

### 4.1 Auction Theory

There are four common auction types:

- Open Ascending-Price (English)
- Open Descending-price (Dutch)
- First-price sealed bid
- Second-price sealed bid (Vickrey)

Auctions are not new, and have been used since the era of the Babylonians. Auctions are used because the *seller is unsure* about the values that bidders attach to the object being sold. If the seller knew bidder values, he could just offer the object to the bidder with the highest value  $v$ , or just below.

#### 4.1.1 Terminology

##### **Private values:**

- Each bidder knows the value of the object to themselves at the time of the bidding
- No bidder knows with certainty the values attached by *other* bidders, and knowledge of the other bidders' values have no effect

This assumption is most plausible when the value of the object to a bidder is derived from its consumption or use alone, such as a pizza or a bicycle.

**Interdependence** is when the object worth may be *unknown* at the time of the auction to the bidder.

- Bidder may have only an *estimate* or some private signal that is correlated with the true value.
- Other bidders may possess *information* that, if known, would affect the value that a particular bidder attaches to the object.

We call this specification **interdependent values** which are values that are unknown at the time of the auction and may be affected by the information available to other bidders.

This assumption is most plausible for situations in which the object being sold that can possibly be resold after the auction, such as a Harry Potter first edition book.

### 4.1.2 Equivalent Auctions

- **First-price sealed-bid auction:**
  - The bidder's strategy maps private information to a bid
  - No information about other bidders is available as the auction is sealed
  - The bidder needs to consider what the bid, as they have no idea what other people might bid
- **Dutch auction:**
  - Conducted in the open, but offers no useful information to bidders
  - The only information available is that some bidder has agreed to buy at the current price, but that causes the auction to end.

These two are equivalent because bidding a certain amount in the FPSB auction is equivalent to offering to buy at that amount in a Dutch auction. Therefore, Dutch open descending price auction is strategically equivalent to the first-price sealed-bid auction.

**strategic Equivalence:** for every strategy in one game, a player has a strategy in another game that results in the same outcomes

- **English auction**
  - Offers information when other bidders drop out. By observing this, it may be possible to infer something about their privately known information
  - with *private values*, however, this information is of no use
- **English Auction Strategy**
  - It cannot be optimal to:
    - \* Stay in after the price,  $p$  exceeds the value  $v$  (incurring a loss)
    - \* Drop out before the price reaches the value (losing out on potential gains)
  - Therefore, the optimal strategy is to bid up to the value  $p = v$

the strategy for a **Second-price sealed-bid auction** is also the same:

- Bidder  $B$  with private value  $v$  bids a price  $p$ .
- The highest competing bid has price  $c$

So, the optimal bidding strategy for this auction is:

- If  $B$  bids at  $p = v$ :
  - $B$  wins if  $v = c$  (making profit  $v - c$ ) and does not win if  $v < c$ .
  - If  $v = c$ , assume  $B$  is indifferent between winning and losing
- Alternatively, if  $B$  bids  $p$  lower than  $v$  (i.e.  $p < v$ ):
  - If  $v > p > c$ , then  $B$  still wins and profit is still  $v - c$
  - If  $c > v > p$ , then  $B$  still loses, so also no change, BUT
  - If  $v > c > p$ , the  $B$  now loses, so makes less profit
  - Therefore, bidding  $p < v$  can never increase profit for  $B$  but can decrease profit.

We say that these auctions are **weakly equivalent** because the two auctions are not strategically equivalent, but the optimal strategies are the same if the values are private.

With interdependent values, the information available to others in the open auction is relevant to a

bidder's evaluation of worth. Seeing some other bidder drop out early may make the bidder realise that his own estimate is too great. Therefore, if the values are interdependent, the two auctions may not be equivalent from the perspective of the bidders.

An auction is said to be *incentive compatible* if it encourages bidders to bid their *true value of the good*

Both English and Vickrey are incentive compatible, since when values are private, the optimal strategy is to bid  $p = v$ .

However, Dutch and FPSB are not, since we want to bid lower than the true value; attempting to stop the auction just below the price of what other bidders value the good at.

Incentive compatible auctions stop game-playing between bidders.

#### 4.1.3 Revenue Equivalence Theorem (RET)

- In English/Vickrey auctions, bidders bid price  $p = v$ .
- In Dutch/FPSB, bidders price  $p < v$ .
- However, the expected revenue in a first-price auction is the same as the expected revenue in a second-price auction.

The revenue equivalence theorem states that if the values are private, and bidders are risk neutral, any standard auction will yield the **same expected revenue** to the seller.

The revenue equivalence theorem requires *risk neutral* bidders, meaning that they have no emotional attachment to the bids and they only seek to maximise expected profits. However, in reality, bidders are normally *risk averse*, meaning that they will bid higher, as they will buy *insurance* against the possibility of losing. When we take risk aversion into account, we get the result that the expected equivalence in the first-price auction is greater than that in a second-price auction.

The RET also requires private values, but in reality, the values are often interdependent, since we often change our valuations based on valuations from others. When we take interdependence into account, ordinary ascending auctions are more profitable than standard (first-price) auctions.

## 4.2 Auctions in Practice

Auctions don't always perform in the way that we expect. Too much economic knowledge can sometimes be a dangerous thing. Essentially, if you can't prove the mathematics in theory, then it's not worth having the theory in the first place.

There are two key implicit assumptions, where all auctions are equally attractive and there is no collusion between bidders. However, attractiveness and robustness to collusion are important in practical auction design. Profitability depends on the *number of bidders* who participate. Participating can be costly, so bidders will only enter if they feel they can win. In **ascending auctions**, a strong bidder can always top a weak bidder, so weak bidders are not likely to enter. On the other hand, in

a first-price sealed bid, a weaker bidder might win, because a stronger bidder is trying to cop a deal. Unfortunately, because bidders can't observe each other, they are not able to influence the auction.

It is possible to signal other bidders and collude with them to ensure that you both get a deal for a really cheap price.

### 4.3 Online Auctions

There are a lot of platforms for auctions online; allowing for auctions to be run quickly and cheaply. The auction rules are algorithmic, so there is no need for a physical auctioneer. Open auctions become easier and cheaper for both the seller and the buyer. Bidding and selling can both be automated. Online auctions are easily scaled, too. The internet, therefore, has created a golden age for auctions.

It was predicted that small businesses would no longer need intermediaries to sell their products and services. Because the cost of reaching customers is virtually zero, it would be easy. However, the cost of reaching people's attention suddenly became much greater, therefore revealing the need for an online market place.

**eBay** is one of the most famous auction venue online. Amazon tried to offer auctions, but eBay retained their title. The auctions on this website are open-ascending with a preset deadline. It's very similar to an English auction, but instead of waiting for a last bid, it has this set deadline. The time constraint has an affect on bidder behaviour, however. It can lead to a very intense last minute bid (sniping). The problem with sniping is that the majority of the bid length does not receive any attention, and then suddenly spike.

To combat this, eBay introduced their own 'sniper' software. They made it such that you can enter a value, and will increment slowly up to the limit. Another possible fix is to extend the deadline slightly whenever a bid is placed. Amazon used this approach.

The trade off between posted prices and auctions is a trade off between price discovery and convenience. Auctions are more likely to sell, but they will sell for a lower price than a fixed price. Auctions are particularly useful for when a seller is unsure of the value of an item.

While eBay holds a lot of auctions, **Google Ads** hold the highest volume of auctions. Due to the *idiosyncratic* nature of adverts, it is impossible to price an advert effectively. Therefore, Google sells them via auction. Advert quality depends on three factors:

- Historic click-through-rate
- Relevancy
- Landing page quality and load speed

The highest bidder might not win the auction, since the quality of the advert also matters.

Google used to use a first-price auction (pay what you bid). Unfortunately, Google noticed that bidders would load the servers by constantly monitoring the system to work out if they could reduce their bid. Instead, they went for a second-price value approach instead, meaning that they bid their true value.

As the price set depends on the number of bidders, Google make it easier for advertisers to match

(such as partial matching).

#### 4.3.1 Double Auction

A reverse auction is an auction whereby the sellers offer their goods at lower and lower values.

A double auction is a combination of this and a normal auction. When the offers match, we can match the buyer and seller (think GE).

## 5 Financial Technology

There are three dimensions of financial technology:

- The business functions offered
- Technologies and concepts
- Institutions in the space

This is sometimes called the *finance cube*.

The traditional banking and finance firms look to use technology to automate or improve a traditional business function. They want to increase productivity and efficiency; looking to maximise profit and overlay new services. It's a new form of incremental innovation. This advancement is **digitalisation**: leveraging digital technology to improve processes.

Start-up technology companies, on the other hand, look to introduce **new kinds** of financial services. The finance is redesigned from the ground up, making use of the technology possibilities. They want to disrupt traditional finance through new tech. This development is considered as **FinTech**.

Finally, big-tech companies already have a huge network of users. They want to streamline technology processes and lock in users. This development is considered as **TechFin**, leveraging current tech platforms to overlay financial services.

Note that these terms are **not used consistently**, which is not incorrect, but annoying for us, so we will stick to these definitions for ease of understanding.

Finance and technology have an old relationship. They have been in cahoots for a really long time.

### 5.1 Development Landscape

According to a 2015 survey, the peak age group of financial technology users are relatively young, with the highest users being between 25 and 34. This shouldn't come as much of a surprise. The users also tend to be wealthy. However, the survey was only conducted in Australia, Canada, HK, Singapore, UK and USA. This begs the question, does this skew the result?



These countries have access to banking, but 70% of the world's adult population are un/underbanked. This category of people need easy access, appropriate and attractive (to use) products.

Financial services have been regulated for a long time. This is to:

- Protect actors
- Improve efficiency
- Reduce risk
- Help build trust

These *financial regulators* are the reason that banks are more popular than giving your money to some random fella, and to stop them from just running away with your money. However, fintech/techfin is disruptive, so may not be initially regulated. Tech companies do not have expertise of regulatory compliance. Some regulators take a 'watch and see' approach (also called sandboxing).

### 5.1.1 LASIC

- **Low profit margin** — It is necessary to be able to maintain a low profit margin. These margins remain low at the user level, so high volumes are necessary.
- **Asset light** — Fixed costs should be kept low, so look to ride on existing infrastructure whenever possible
- **Scalable** — Easily scalable
- **Innovative** — Products and operations should be innovative, ideally a new business model
- **Compliance easy** — Governments want something that is easy to regulate.

## 6 Economic Agents and Market Based systems

Market economics is an important metaphor for new methods in computer science or engineering, dealing with allocation of scarce resources. It requires software versions of both traders and market-places. Designing these things is hard, but can be done automatically.

It is useful to distinguish between **macro** and **microeconomics**. Macro is the high level stuff that we don't need, and micro is just maths, which is more useful for problem solving.

There are lots of really important resource limited systems:

- Telecom, computer OS, logistics, staffing, etc.
- Automating their control or regulation is attractive for the usual reasons
- and difficult for the usual reasons too

So, ideas from microeconomics could help us do automated dynamic resource allocation and control in engineered systems. Market based control is not a radical new idea, and has been around for a number of years. It happens that these automatically optimised robot traders and market mechanisms are originally intended for control of data centres and are of significant interest to major investment banks, buy-side funds, and exchange operators.



## 6.1 Background Economics

From everyday experience, we're used to the idea that if the demand for some tradable item exceeds the supply, then the price will rise. This is known as a **shortage**, or *seller's market*

Conversely, if the quantity supplied is greater than that demanded, the price will fall, known as a **surplus**, or *buyers market*

Formally, the price that buyers are prepared to pay at each possible quantity is referred to as the demand. This, when plotted, usually slopes downward. Similarly, the price that sellers are prepared to sell for at each possible quantity is referred to as the supply, and this will slope upward on a graph.

The price will balance at an intermediate price, where the quantity supplied will equal the quantity demanded.

This is known as *self-correcting*, and free markets will do this since transactions take place at prices away from equilibrium. Competition among buyers or seller will move prices back toward the equilibrium. At this equilibrium, traders have no incentive to change their prices.

Such market mechanisms can give efficient allocation of resources without a central controller or external intervention. A common ideal of efficient allocation is the notion of **Pareto efficiency**:

- An allocation is Pareto efficient if no-one can be made better off without someone being made worse off.
- Pareto efficient allocations can arise from free markets despite the fact that each trader in the market is acting only to serve his or her self-interest
- The traders appear to be led by an invisible hand
- Free markets are not guaranteed to achieve optimal allocations. conditions in which they fail are well known (such as a monopoly).

In reality, the supply and demand curve isn't as smooth as it is in theory. This is a simplification that is really useful for teaching purposes. However, in the markets that we will be looking at, things are gonna get more complicated. It looks more *stepped*. Each step in the supply curve represents an additional unit available for sale at the indicated price, while each step in the demand curve represents an additional unit desired at the indicated price. These curves also don't stand still because the buyers become saturated, or the sellers run out of stock. Even without transactions, traders dynamically alter their margins.

## 6.2 Market Metrics

- **Smith's  $\alpha$**  — Root mean square deviation of transaction prices around theoretical equilibrium price, expressed as a percentage (lower is better).

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

- **Allocative Efficiency** — Total utility (profit) earned by all traders, divided by theoretical max possible total utility (surplus), expressed as a percentage. Measures how effective the market is at extracting gains through trade.

- **Single Agent Efficiency** — Profit earned by an agent, divided by its expected profit if all trades take place at the equilibrium price (how effective a single trader is)

The results of an experiment of random agents creating artificial trades concluded that most of the intelligence is in the market, and not the traders. These 'zero-intelligence' agents were surprisingly human like when they were constrained to make offers and bids that would not make them a loss.

We have a better test for the kind of things we are looking at, which is called the RRO test (robust rank-order test), but we will not be covering it here. These results are actually gained, but they are **special cases**. We can actually predict when these ZI-C markets will fail to reach the equilibrium. For this reason, we can develop a better trader, known as a ZI-Plus trader.

These traders still work on their quota, as ZI-C does, but also use some machine learning; adjusting this using machine learning rules. They were able to succeed in markets where ZI-C failed.

### 6.3 Maths Behind ZI-P

ZI-C agents are hard bounded by the supply-demand curve. They are not able to offer prices that would breach this and cause them a loss. If we look at these curves, we get a probability density function (it would be equivalent to the area above the supply curve for sellers, or the area below the demand curve for buyers)

Transactions only occur when a bid and offer price cross. If we overlay the pdf for both supply and demand curve, we get the probability density function for the equilibrium price. Note that we are dealing with symmetric supply and demand curve here, which affects this slightly. The peak of this pdf is the equilibrium price. This means that it is not surprising that ZI-C agents reach equilibrium since this is the most likely value.

In asymmetric markets, the mid point (expected value) is no longer the peak. It could actually be the first point, if there is elastic supply, meaning ZI-C would fail to converge in these markets.

Very informally, the ZI-P sellers have a thing to sell, and a *limit price* such that it will not lose money. The price asked for  $P$  is  $L$  and some profit margin  $M$ :  $P = (1.0 + M)L$ .

- If we have price  $P$  and:
  - Sellers are accepting bids below  $P$  or
  - Sellers are making offers below  $P$
- then decrease  $M$  (not below zero). Otherwise:
  - If trades are happening at prices above  $P$  then increase  $M$  (even if we have nothing to sell)

Each ZI-P seller keeps their values private. The quantity in which the margin steps up or down is aiming for a target price, that is roughly the last quote price in the market. There is a little bit of randomness, too. ZI-P uses the Widrow-Hoff learning rule with **momentum (damping) factor**.

What makes a trader 'best'? It is really hard to compare them, so instead of analysing them, *empirical studies* are the method of choice. More on this later.

Testing agents in a *homogeneous* market is sometimes not good, since for things like financial mar-

kets, this is impossible. This exact problem is what led to MGD (modified GD agent). For this reason, the following tests were performed:

- **Homogeneous population test** — Tested in a market of a single agent
- **One-in-many test** — Tested in a market where all but one trader is using a different method, and only one instance of the agent
- **Balanced test** — Tested in a completely split market where each agent has a counterpart

## 7 Empirical Methods

### 7.1 Confidence intervals

If you have  $n$  sets of  $k$  samples, you have  $n$  estimates of the population mean  $\mu$ . You often are unable to get a perfect estimate in finite time, but you may be able to get bounds:  $c_1, c_2$  such that

$$Pr(c_1 < \mu < c_2) = 1 - a$$

$[c_1, c_2]$  is the *confidence interval*.  $a$  is the *significance level* ( $0 < a < 1$  and 0.1 is common)

One way to get a particular CI (confidence interval) is to take a lot of samples, and then compute the percentiles. Often, it is better to approximate via the *central limit theorem*: for large numbers of samples ( $n > 30$ ), sample means can be treated as coming from a normal distribution with mean =  $\mu$  and standard deviation =  $\sigma/\sqrt{n}$  (the standard error).  $(1 - a)$ CI then given by:

$$\left( \bar{x} - z_{1-\frac{a}{2}} \cdot \frac{s}{\sqrt{n}}, \bar{x} + z_{1-\frac{a}{2}} \cdot \frac{s}{\sqrt{n}} \right)$$

### 7.2 Comparing method A with method B

Calculate CI on samples from both A and B.

- If the confidence levels don't overlap at all and one is clearly higher, we can conclude that the method higher is definitely better.
- However, if the confidence levels overlap and the means are in the bounds of the other's confidence levels, then at the stated confidence levels, there is no difference between A and B.
- If the CIs overlap, but neither mean is in the others confidence levels, we need to do a better test.

### 7.3 Choosing a test

**Parametric tests** require these assumptions usually:

- Independent observations (unless paired data)

- Observations are random draws from a normal/gaussian distribution
- Observed (dependent) variable is measured on at least an interval scale
- $n \geq 30$  usually advised
- Data are drawn from populations having equal variance
- Hypotheses usually about numeric values especially about the mean
- Often also requires
  - Symmetric, mesokurtic
  - Homoscedasticity
  - Equal cell-sizes in the data table

**Non-parametric** tests require these assumptions usually:

- Independent observations (unless paired data)
- Few assumptions regarding the population's distribution
- Scale of measurement of dependent variable may be normal or ordinal
- Primary focus is on rank-ordering and/or frequencies of data
- Hypotheses are usually about ranks, medians, or frequencies of data.
- Sample size requirements are less stringent than those for parametric tests

NB: Parametric tests are often described as 'distribution-free', but they're more accurately described as 'distribution-free-er'.

### 7.3.1 Wilcoxon-Mann-Whitney U Test

The U-test is:

- A powerful test for two independent samples on a continuous dependent variable
- Non-parametric version of the independent Student's t-test
- Like the t-test, it compares measures of central tendency
- Unlike the t-test, it uses medians instead of means, so no assumption of normal distribution
- Very commonly used

The method is as follows:

- Combine A and B into one list and sort, remembering which data from A and B
- Rank the list from highest to lowest, award average rank to ties
- Separate back into two samples and sum the ranks for A and B to get  $R_1, R_2$ .
- If the null hypothesis is true, the two rank sums should be 'similar'
- Compute  $U_1 = n_1.n_2 + ((n_1(n_1 + 1))/2) - R_1$
- Compute  $U_2 = n_1.n_2 + ((n_2(n_2 + 1))/2) - R_2$
- Compute  $U = \min(U_1, U_2)$
- Compare  $U$  to *critical value* for  $U_{n_1, n_2, \infty}$  (from a lookup table of critical values)
- If  $U < U_{n_1, n_2, \infty}$  then reject null hypothesis

To use this test, we need:

- Independent variable has two groups
- Dependent variables measurement scale is at least ordinal

- Data are randomly selected samples from two independent groups
- Population distributions of the dependent variable for the two groups share a similar (unspecified) shape but have differences in measures of central tendency

NOTE: Avoid  $N$  multiple pairwise tests, as accuracy falls off really quickly.

## 7.4 Adjacent Values

Adjacent values are indicators of the extent of *tails* of the distribution. The *upper adjacent values* is the largest actual value in the data-set that is less than twice the inter-quartile range greater than the median. The *lower adjacent value* is the smallest actual value in the data-set that is greater than the point twice the inter-quartile range less than the median.

## 8 Options and Betting Markets

So far, we have looked at how to make money, which simply has been buy low, sell high. This only works (and is profitable) when prices are rising. If prices are falling, with our current knowledge there is no good time to buy. We will look at this here.

### 8.1 Short-selling

To *go long* on X means to buy X, expecting the price to rise (a *bullish* position). To *go short* on X means to sell X, expecting the price to fall (a *bearish* position). This is often abbreviated to just long/short.

Short-selling:

1. Borrow  $n \cdot XYZ$  from a lender
2. Sell  $n \cdot XYZ$  now (time =  $t_1$ ) at price  $P_1$
3. Price of XYZ falls to  $P_2$
4. At time =  $t_2$  buy  $n \cdot XYZ$  at  $P_2$  and return to lender
5. Profit =  $n \cdot (P_1 - P_2) - \text{LenderFee} - \text{costs}$  (could be storage/insurance/transport)

### 8.2 Derivative Contracts

There are contracts that keep track of this called *derivative contracts*. These are contracts that *derive* their value from some other asset (known as underlying). There are lots of types, but we will look at two:

- **Future:** contract that *will* be executed by/on a set delivery date
  - Futures contracts are required to be executed
  - When issued, it specifies the forward price

- On the delivery, the contract is executed at the forward price
- The buyer of the forward is called the *long position* and the seller is the *short position*
- **Option:** contract that *may* be executed by/on the expiry date
  - Options contracts confer a right (but not obligation) to execute
  - Option specifies a strike price (or strike) aka the exercise price
  - Options to sell are puts, options to buy are calls

Both futures and options are *standardised* (size of contract and expiry date are prespecified) and *exchange-traded* (traded in a secondary market on an exchange, just like stocks and shares).

### 8.3 Equity Options

One options contract is right to buy/sell N shares ( $N=100$ ). the price of the option depends on the price of underlying, strike and risk premium. The **Strike price** is the price at which you can buy or sell underlying on exercise. The **Expiry** is the last date on which you can exercise option (two types, *American* options, where exercise happens any date up to expiry and *European* options, where exercise happens only on the expiry date also called maturity). The option is written/issued by its seller, and held/exercised by its buyer.

The option price is determined by three factors:

- **Intrinsic value:** money received if the option is exercised now
- **Volatility premium:** dependent on underlying's price volatility
- **Time value:** potential risk-free return on money saved wrt buying underlying.

Call options:

- Right to buy N units of underlying
- Option-holder can buy at strike price
- If exercised, option writer must sell N shares at strike price
- In-the-money if the underlying price is greater than the strike price
- Out-of-the-money if the underlying price is less than the strike
- At-the-money if underlying is the same as strike

Puts options:

- Right to sell N units of underlying
- Option-holder can sell at strike price
- If exercised, option-writer must buy N shares at strike price
- In-the-money if the underlying price is greater than the strike price
- Out-of-the-money if the underlying price is less than the strike
- At-the-money if underlying is the same as strike

## 8.4 Options Strategies

Of course, multiple options can be combined to create a different strategy. For example, a *bullish spread* is a combination of a long call and a short call, meaning both losses and profits are capped, but prices are still going to rise. This could also be created with short and long puts. On the contrary, a *bearish spread* can be created, equally from short and long put/calls, but this time the prices are going to fall. If you think the prices are not going to move much, you can create a *long butterfly*, and this is created by a long call, 2 short calls, and another long call.

There are lots more combinations of these, but I won't go into them here.

## 8.5 Betting Exchanges

Betting exchanges are electronic marketplaces where gamblers interact to find someone to take the opposite side of their bet: they 'buy' (*back*) or 'sell' (*lay*) the outcome of the event.

Traditionally, the bookmaker sells a lay to the customer. Traditional bookies have argued that allowing anonymous customers to lay events encourages corruption because it's easier to throw a race than it is to win it.

Betfair was the company that really drove this market forward.

# 9 Economies of Gaming

Essentially RuneScape GE LOOOOL.

## 9.1 Economics of Game Development

Games have gotten exponentially bigger over time, both in terms of development teams and actual size of the codebase. This is only for the AAA games. The average game budget of the average game is on a shoe string budget, and only a tiny fraction become noteworthy/profitable successes, while the rest fall by the wayside. It's a big shift: the loss of mid sized studios as a result of absorption by a gorilla company or fragmented into small companies. This shift is theorised to have come about as a result of growth in content cost and marketing costs.

The problem is that it becomes really hard to take creative risks when you're borrowing so much money to make the game. Therefore, the well known succeeds. It is much the same in Hollywood.

## 10 Sentiment Analysis

Sentiment can be an *attitude* or *opinion* towards X. We can assign a numeric value to this sentiment from -1 to 1.

In the internet age, opinions are really important. Everybody has an opinion and can broadcast these opinions to the world really easy. Additionally, these opinions really influence spending. For example, a one-star increase in Yelp rating leads to a 5-9% increase in revenue. It also allows smaller restaurants to prosper because these reviews can substitute for more traditional forms of reputation.

Given the value of public sentiment is so valuable, gathering these opinions is really useful. This is called *sentiment analysis* and is the process of computationally identifying and categorising opinions expressed in a piece of text, especially in order to determine whether the writer's attitude towards a particular topic, product, service, etc is positive, negative, or neutral.

Sentiment analysis is a difficult challenge. There are three levels of analysis:

1. **Document-level:** For a given document, identify the overall attitude to the object under discussion
  - Supervised Learning
    - It's possible to use supervised learning to use this (but this needs a ground truth) to learn from
    - Features: 'bag of words' approach. Simply using the frequency or presence of words in the review as input (rather than the raw text)
    - After this, its possible to use a naive Bayes classifier, or support vector machine
    - The performance accuracy is around 81/82%, which is better than the performance of a human-generated feature set but not as high as reported on other non-opinion machine learning tasks due to the difficulty of sentiment classification.
  - Unsupervised learning
    - Unsupervised learning does not need tagged or labelled data to learn from in a supervised fashion, so probabilities of word and phrase co-occurrences calculated using search engine results. Classification is predicted using semantic orientation calculated as mutual information.
    - This was quite good for some things, but bad for movies, since some words could sound bad but be good.
2. **Sentence (or phrase) level:** For a given sentence, identify if it expresses a positive, negative or neutral opinion
3. **Aspect level:** For a given document, identify all opinions expressed regarding any aspect of any object.
  - A document may contain multiple expressions of sentiment regarding different aspects. A bag of words approach that treats words as independent features will not perform well in some sentences, since the context is lost.
  - Aspect level analysis corrects these failings.
  - For a given document, every quintuple of sentiment is identified:
    - The object
    - The aspect
    - The sentiment
    - Who holds the sentiment



- When it was expressed

## 10.1 Unsupervised learning

An example of unsupervised learning is using phrases containing adjectives or adverbs followed by a noun. From this, the **pointwise mutual information** of a pair of words calculates how strongly those words are semantically associated. Then, the **semantic orientation** of each phrase is calculated using the PMI of the *phrase* with reference words 'excellent' (often used in 5-star reviews) and 'poor' (often used in 1-star reviews). SO is estimated by issuing queries to a search engine, noting the number of hits (matching documents) where the phrase is near to the reference words. Finally, the average SO of phrases is calculated and assigned a final + or - value based on this.

## 10.2 Aspect Level Sentiment Classification

A simple algorithm might look something like this:

1. Mark sentiment words and phrases using a lexicon
  - Positive words or phrases assigned +1 and negatives -1
2. Identify sentiment shifters: (e.g. not, never, cannot)
  - Swap sentiment values for shifted words
3. Identify 'but' phrases
  - Heuristic states that if the sentiment on one side cannot be identified, it is considered opposite to the other side
4. Sum sentiment scores, weighted by word distance from aspect word

# 11 Crowd Economics

## 11.1 Prediction Markets

We can harness the intelligence of crowds to help us make *predictions*. It is important that people are honest, and to enforce honesty, we can use *pay-to-play* to avoid any bias, and discourage those with little knowledge or those who want to sabotage. This is what a prediction market is.

### Prediction Market

Trading a future event with two mutually exclusive uncertain outcomes Y and R.

We create two contracts, Y and R and these are traded for even outcomes Y and R. Contracts trade until some deadline when outcomes become known. At the deadline, contracts pay out based on the outcome of a real-world event.

- In **winner-takes-all** markets,  $N$  contracts corresponding to  $N$  mutually exclusive outcomes for a future event. Contracts have a fixed value payout if the event occurs and 0 otherwise

The market is run as a CDA and a LOB, just like a financial market. *Current trade price* of a contract is considered a measure of the (*believed*) probability of a given event by traders.

Since traders want to make a profit, traders should buy a contract when they believe it is underpriced and sell when they believe it is overpriced. Basic trading strategy is that if your own private belief that outcome  $Y$  will occur with probability  $p$  then:

- Buy  $Y$  when  $Y < p$ , Buy  $R$  when  $R < 1 - p$
- Sell  $Y$  when price  $Y > p$ , Sell  $R$  when price  $C_b > 1 - p$

These markets shift often to accommodate for news and real world events.

### 11.1.1 Iowa Electronic Markets IEM - Winner Takes All

This market offers real-money futures market where *contract payoffs* depend on future events:

- Not-for-profit: research and teaching
- Stakes are small
- Relatively low number of traders

IEM offers two kinds of markets:

- Winner-takes all
- **Vote share**: % payout based on a quantitative outcome (such as share of seats in election)

Prediction markets work equally well with multiple outcomes. WTA issues a contract for each separate (mutually exclusive) outcome.

#### Arbitrage Opportunity

Arbitrage is the act of simultaneously buying/selling across markets for risk free profit. For example, if a 2 contract WTA has a trade price of \$0.60/\$0.30, the cost of both is \$0.90. But, you know that one of them is guaranteed to pay \$1.00 at the end of the contract. So, we should buy as many as possible

Buying these will raise the price. Once the market equilibrates at \$1, we say the signal is *arbed* away.

Arbitrage also works when contracts are over-priced, too.

### 11.1.2 Vote Share Market

A VS market runs in a similar fashion to a WTA market. The only difference is the description of the payouts of the futures contracts. A VS contract pays out in proportion to the percentage of the final result. For example, IEM's VS market for the 2020 US presidential election has two contracts, defined

as follows:

- UDEM20\_VS: pays \$1 times the democratic Nominee's share of the two party vote
- UREP20\_VS: pays \$1 times the republican Nominee's share of the two party vote
- If, for example, the final result of the election is 55% democrat, then UDEM20\_VS pays \$0.55, and UREP20\_VS pays \$0.45.

Predictions can be really quite accurate, because money talks. There is less psychological bias and game playing, which is what we see in opinion polls. However, they are *not* always correct. For example, in the Clinton/Trump election campaign, the market predicted that Clinton would win.

IEM is the only prediction market in the US since it is essentially gambling. But, since IEM is not for profit, it is allowed to operate exempt from gambling restrictions.

## 11.2 The Crowd Economy

The crowd economy is an economy that requires interaction from the users of the service, such as Wikipedia.

There are two key economic roles of a crowd:

- **Crowdsourcing**: an alternative to traditional companies. Used for doing work/solving a problem
- **Crowdfunding**: An alternative to traditional financial intermediaries (like banks). Used for raising money

### 11.2.1 Crowdsourcing

Crowdsourcing has several forms:

1. Citizen Engagement
2. Mass Collaboration
3. Crowd Tasks

Crowdsourcing is really useful for tasks that are currently too difficult for a computer to perform. For example, labelling images for supervised learning. These tasks are often tedious and repetitive.

The simplest method for recruiting people to do these tasks is to either pay them. The other two methods are to trick them into doing the work (reCAPTCHA), or even ask them to do it for free (either make it worthwhile or make it fun).

### 11.2.2 Crowdfunding

Crowdfunding also has several forms:

1. Donation-based

2. Reward-based
3. Equity-based
4. Debt-based (P2P lending)

Equity and P2P based crowdfunding are regulated.

Crowdfunding is really useful to use instead of banks because banks will say 'no' if your idea is too risky (poor credit history, a wacky start-up, etc).

Multiple ways to encourage investment:

- Make it for a good cause
- Give them an exciting reward
- Give them a share of your new company
- Give them a high fixed interest rate

## 12 Blockchain and Bitcoin

Transactions using bitcoin are of a similar structure to that of real money:

1. Agree the transaction
  - A and B agree on some price
  - Adding a small 'fee' to her payment makes it more likely to be processed quickly because the fee will be 'earned' by the miner that mines the block that A's transaction is included in
  - A will spend a fraction of a bitcoin on this fee
  - Fee is not necessary, but incentivises the miners
2. Create the transaction message
  - A creates a message that includes three components
    - a) A reference to the earlier transaction that paid A the set price
    - b) A list of addresses of recipients of the payment, since the transaction pays the change back
    - c) A list of amounts to pay the addresses
  - A will split the input between two addresses, B, who is paid for the product, and A who gets her change back.
  - If amounts are greater than the agreed price, the remainder is the fee for a miner (but we don't know who's getting that yet.)
3. Sign the transaction message
  - A signs the message using her private key.
  - Easy to confirm that the message was made by A because public key can be used to decrypt it
  - No-one can encrypt it the same way without private key.
  - Similar to a royal seal
4. Broadcast the transaction message
  - A then broadcasts the encrypted message along with her public key (for decryption)
  - A initiates the broadcast by spreading the message to A's immediate peers in p2p network
  - Before broadcasting it to their peers, they verify the message
  - A's transaction is one of a number on the network that have not yet been included in the

## Blockchain

## 5. Verify the transaction message

- Miners now compete to be the first to mine a block containing transactions that haven't yet been added to the blockchain
- Winner is the one who keeps the fee and gets to include a payment to themselves in the block
- Mining is hard work, taking many compute cycles to win the competition. Proof of work is what keeps the blockchain consistent and reliable

## 6. Transaction success

**12.1 Anatomy of a block**

Each block in the Blockchain has a *header* formed of:

- Timestamp and version number
- A hash of the previous block header (linking new blocks in the chain)
- A *merkle root* summarising the new transactions that the block contains (meaning each block has a history of all bitcoin transactions)
- A *nonce value* chosen by the miner such that when the header is hashed (using SHA256) the resulting 256-bit hash has at least  $x$  leading 0s

**12.2 Nonce Values and Difficulty**

SHA256 hashes any data into an arbitrary 256-bit string.  $\text{SHA256}^2$  just applies SHA256 twice.

If you wanted to  $\text{SHA256}^2$  to have D into  $S = 000 \dots 011$  you could add an arbitrary nonce value to the end of D and keep changing this value until  $\text{SHA256}^2$  gave you a bit string that evaluated to 3.

If you are only happy with one specific 256-bit string, you will be waiting a long time before you find the right nonce, but if you just want to get a hash  $S$  such that  $S < 2^{200}$ , then things are easier. Even easier if you're happy with  $S < 2^{250}$ .

Checking whether a nonce 'works' is really quick:

- It requires one execution of  $\text{SHA256}^2$  on D and a comparison operation: is S satisfactory
- It's just like checking whether a sudoku solution is really easy, even if the sudoku is huge or difficult

*Finding* the nonce is really slow

- Many executions of  $\text{SHA256}^2$  depending on how small the subset of allowable hash strings is
- It's like solving a sudoku. Very difficult, especially when large.

The similarity between sudoku and finding nonce values is limited; you can't get better at finding nonce values. The only way to improve the chance of finding the right nonce value is to just *check more possibilities*. There's no trick. A correct nonce is the proof of work.

### 12.3 Successfully Verifying the transaction

After some time, a miner  $M$  will find the **golden nonce**.  $M$  gets the transaction fees and the standard fee for finding this.  $M$  broadcasts the new block to the p2p network. The nodes all add the new block to their copies of the blockchain, and miners start to mine the next new block. B can check that the transaction is verified in the blockchain and complete the transaction with A.

These steps are really important to avoid *double spending*. Nothing really stops someone from spending their digital bitcoin twice, so Blockchain avoids this:

- The blockchain stores this single agreed history of every transaction
- Nodes check to see if a bitcoin has already been spent.
- If so, the transaction isn't included in the block being mined.
- If a coin is spent twice simultaneously on different parts of the p2p network, a 'fork' in the Blockchain can occur temporarily
- But, the blockchain will identify and correct this fork quickly and without need for centralised control or co-ordination.

### 12.4 Bitcoin Concerns

Some of the critiques of Bitcoin are not unique to cryptocurrencies, such as theft or loss etc. However, there are some unique problems, and the main one is that mining bitcoin is incredibly demanding from an energy standpoint, due to the computational difficulty of finding the correct nonce value.

The Blockchain is an example of a log that is *intentionally slow/costly* because of the assumption of zero trust. There are far more approaches that exist and are much faster or less wasteful. Therefore, Blockchain is literally only useful for cryptocurrencies, and not much else.

### 12.5 Blockchain Evolution

Bitcoin did not appear in a vacuum. Many attempts at cryptographic payment systems and electronic cash were made during the 1990s, but many were not very functional.