E-Commerce

2. Foliensatz – Business Models

Business model - the architecture with which an organization creates value for customers, how it delivers that value, how it captures that value and how it defends value.
Business plan - the detailed implementation plan for your business model. Includes Company Goals, Resources required to achieve the goals, Methods used to achieve the goals, Timeline, Market size, market analysis, market fit, etc.

Business model examples:
Apple

- Traditional:
  Create: unique products -> deliver: devices own apps -> capture: hardware sales -> defend: brand
- Digital:
  Create: apps -> deliver: 3-party apps and accessories -> capture: hardware sales -> defend: developer ecosystems

Business Model Canvas – a canvas to describe, discuss, design, challenge, improve, innovate, invent, pivot, choose a business model. Has 9 blocks.
Blocks of Business Model Canvas (Example: Nespresso upd.):

- Customer Segments - For whom are we creating value? Who are our most important customers?
  Exp: households;
- Value Proposition - What value do we deliver to the customer? Which one of our customer's problems are we helping to solve? Which customer needs are we satisfying? What bundles of products and services are we offering to each Customer Segment?
  Exp: Nespresso machines, nespresso pods;
- Channels - Through which Channels do our Customer Segments want to be reached? How are we reaching them now? How are our Channels integrated? Which ones are most cost-efficient?
  Exp: retail, nespresso stores, website, mail order, call center;
- Customer Relationships - What type of relationship does each of our Customer Segments expect us to establish and maintain with them?
  Exp: equire & lock-in, nespresso club;
- Revenue Streams - For what do customers currently pay? For what value are our customers really willing to pay?
  Exp: 1 time machine sales, repetetive pod sales;
- Key Resources - What Key Resources does our Value Proposition require (Physical, Intelectual, Human, Financial)
  Exp: brand, patent, distribution channels

- Key Activities - What Key Activities does our Value Proposition require (Production, Problem Solving)
  Exp: B2C distribution, Marketing
- Key Partnerships - Who are our Key Partners? Who are our key suppliers? Which Key Resources are we acquiring from partners?
  Exp: Postal Service, Studios Exp: machine manufacturers, coffee growers
- Cost Structure - What are the most important costs inherent in our business model? Which Key Resources are most expensive? Which Key Activities are most expensive?
  Exp: marketing & branding, production, B2C distribution

Types of business Models:

- Freemium: a mix of free and paid services. To grow business and acquire customers, companies offer free (lite) versions to customers but for a limited time or with limited features. To unlock the upgraded features, the customer has to opt for paid services.
- Subscription: Allows the customer to get services by paying a fixed amount every month or year. Allows companies to segment the market and offer a specific number of items in its content under different plans and prices known as tiered offerings. -> Netflix
- Hidden revenue: A revenue generation system in which users don't have to pay for the services offered, but the company still earns revenue streams from other sources. -> Google with ads
- Razor and blade: One item (e.g. Razor) is sold at a low price while another associated item (e.g. blade) is sold at a premium price. -> Printers
- Reverse Razor and Blade: Offering low priced products to encourage customers to buy high priced items as well.
- User-generated content: Allowing users to generate quality content on websites for free to answer other users' questions and provide reviews. User-generated content is compiled and sold to companies seeking to exploit consumers' ideas and content to promote their brands.
- Data licensing: Data can be licensed to other companies to be used to improve their products. -> Twitter selling real-time data.
- Aggregator: A network model that provides collective information about a particular service and sells them under their brand name.

Enterprise - an enterprise is an organisational unit producing goods or services which has a certain degree of autonomy in decision- making. An enterprise can carry out more than one economic activity and it can be situated at more than one location. An enterprise may consist out of one or more legal units.
Strategy defines how a business is going to compete, what its goals should be, and what plans and policies will be needed to achieve these goals.

Porters competitive forces model includes:

- Threat of New Entrants
- Threat of Substitutes

- Bargaining Power of Buyers
- Bargaining Power of Suppliers
- Industry Rivalry

Swot analysis inccludes:
    - Strengths (internal origin)
    - Weaknesess (internal origin)
    - Opportunities (external origin)
    - Threats (external origin)

General Strategy Issues
- Be a first mover or a follower
- Born-on-the-net or move-to-the-net
- Have a separate online company
- Have a separate online brand
- How to handle channel conflict (depends on existing distribution channels)
    - Let established distributors handle e-business fulfillment
    - Provide online services to intermediaries (e.g., by building portals for them)
    - Sell some products only online
    - Avoid channel conflict entirely by not selling online

Pricing issues:
- Easier price comparison
- Differentiated pricing
- Online and off-line goods can be priced differently

Pricing models:
- Customer characteristics: Pricing and differentiation of offers is based on customer profiles (micro-segmentation) or Personalized– sell to each user at a different price (*airline yield management*)
- Product features: Versioning – pricing based on product features or attributes. (e.g., information w.r.t. time, or region)
- Volume Discounts: Demand pooling gives individuals access to volume discounts, coordination costs must not exceed discounts
- Value-based pricing: Customer is enabled to influence the price by selecting the service level (customer-initiated service customization), Online car customisation

3. Foliensatz – Platforms

Traditional business is pipeline business. It includes step-by-step arrangement for creating and transferring value, with producers at one end and consumers at the other end.

Platforms bring together individuals and organizations so they can innovate or interact in ways not otherwise possible, with the potential for nonlinear increases in utility and value. Exp: malls, newspapers.
Platforms engage multiple sides of the market (buyers-sellers, application devs – hardware producers), generate network effects(negative networks effects also possible), solve a chicken or egg problem.
Engage multiple sides of the market : Facebook connects advertisers, applications and platform partners to users.
Network effects: The value one user experiences potentially increases as more people or organizations use the same product or service and as more complementary innovations appear. Strong network effects can lead to non-linear growth.
Chicken or egg problem: one side comes onboard first and provides something that attracts another side. Often a decision has to be made which market side to line up first.

Platform business models:

- Innovation Platforms: Usually create value by facilitating the development of new complementary products and services, sometimes built by the platform owner but mostly by third-party firms, usually without supplier contracts. Examples: Apple IOS, Google Android, Steam, Amazon AWS, Microsoft Azure.
- Transactional Platforms: intermediaries or online marketplaces that make it possible for people and organizations to share information or to buy, sell, or access a variety of goods and services. Exp: Snapchat, Airbnb, Uber, Amazon
- Hybrid conpanis: combine both. Apple, google, microsoft, Salesforce, amazon.

Alternative classification:
Exchange:

- Services marketplace: a service
- Product marketplace: a physical product
- Payments platform: monetary payment
- Investment platform: an investment/financial instrument (i.e., money exchanged for a financial instrument, be it equity or a loan, etc.)
- Social networking platform: a double-opt-in (friending) mode of social interaction
- Communication platform: 1: 1 direct social communication (e.g., messaging)
- Social gaming platform: a gaming interaction involving multiple users, either competing or cooperating

Maker:

- Content platform: a piece of content (a text article, photo, video, etc.)
- Development platform: a software program

Building Innovation Platform Business:

1. Chose market sides: complementors (use supplied tools to develop complementary products) or end users. Challenge is to identify complementors that will stimulate demand. Strategies: broadly expose APIs, encourage

complementors, Subsidise complementors, Create own complementary products.
2. Solve chicken-egg problem. Challenges: how to make the platform attractive for potential end users even with few complementary applications, How to persuade complementors to develop platform-specific applications if there is uncertainty about the number of end users. Strategies: to launch already with sufficient complementary applications, launch a platform to solve an industry-wide problem.
3. Design business model. Most innovation platforms generate profit by increasing customers' willingness to pay for the platform itself, taking a portion of the value of the sale of every complementary product sold.
4. Establish & enforce ecosystem rules. Define to what extent the platform competes with its complementors – do not destroy complementors's incentives to innovate.

Building Transaction Platform Business:

1. Choose market sides: Buyers-sellers, advertisers to subsidise internet search. Social Networks can be one-sided if all users are similar, and multi-sided if there are different user categories.
2. Solve chicken-egg problem. Bootstrap one side, Initially subsidise one side, Offer a useful service to one side. Bringing on both sides at the same time is more risky, as it often involves subsidising both sides.
3. Design business model. Transaction platforms tend to offer value and generate profit in 5 ways: matchmaking (buyers-sellers), reducing friction in transactions, complementary services, complementary technology sales, advertising.
4. Establish & enforce ecosystem rules. "community guidelines", reviews and evaluations, some platforms guarantee services.

Enshittification - the process by which a platform lures in and then captures end users (stage one), who serve as bait for business customers, who are also captured (stage two). Then the platform rug-pulls both groups and allocates all the value they generate and exchange to itself (stage three).

It is made possible by lack of platform intermobility and collective action.

4. Foliensatz – Customers

Personalisation – a set of techniques for providing a "tailor made" service to the customer (interface customisations, recommendations). Internet is an enabling technology (also for personalization). It facilitates the collection of information about client.
Levels: Product -> Presentation -> Communication.
Customer Pull means presonalization created by the customer. Basically Adaptibility - user modifies explicitly some parameters for own use.
Can include configurable communication, presentation of online content, individual service, dynamic customizable filters, product/ service selection and presentation.

Supplier push – adaptivity - system modifies parameters to user needs. Personalized communication, recommendations, context specific offers.
The long tail - economic model in which the market for non-hits (typically large numbers of low-volume items) could be significant and sometimes even greater than the market for big hits (typically small numbers of high-volume items).
Recommender System helps to make choices without sufficient personal experience of the alternatives (more than personalization). Preferences (user features, product features, user-product interaction data) are the input to the recommendation model. Recommenders can be:

- Non-personalized: use popularity, like people‘s ratings, sales data, accumulate rating data or transaction data. Recommend items with highest average rating.
- Demographic: use user features (age, gender, area), find users with similar features, recommend items that are preferred by similar users.
- Content based: use item features (genre, keywords), recommend items with highest similarity.
- Collaborative filtering: use user-item preferences. User ratings, transaction data, find highly correlated users, recommend items that are preferred by those users.
- Knowledge-based: Model „reflects“ the domain, use user preferences – item features. Build a model for prediction, recommend items by using the model.
- Context-aware: a style of computing in which situational and environmental information about people, places and things is used to anticipate immediate needs and proactively offer enriched, situation-aware and usable content.

The recommender ranks the items by their predicted ratings, but when the items are presented to the user their perceived value is determined by the interaction context: the presence of other competing options.
Marketing - the activity, set of institutions, and processes for creating, communicating, delivering, and exchanging offerings that have value for customers, clients, partners, and society at large.
Marketing mix: 4 P

- Product - refers to an item that satisfies the consumer's needs or wants (roduct design, branding, guaranties, etc),
- Price - the amount a customer pays for a product (price strategy, price tactics, allowance, discounts),
- Place - Refers to providing customer access (Franchising, Market coverage),
- Promotion - marketing communications (Channel/media strategy)

Digital marketing - marketing via digital channels. Advantages: targeted marketing, lower costs, performance metrics.

Impression – user viewing the advertisment
Click - user clicking on the ad
Action – user taking an action

CPM (Cost per Mille) - the advertiser pays the publisher a set fee for every one thousand impressions. (Good for brand awareness campaigns)
PPC (Pay Per Click) - the advertiser pays the publisher only when the ad is clicked. (Good for consideration campaigns)

PPA (Pay Per Action) - the advertiser pays the publisher only when the user performs some action. (good for driving action)

Reach – how many people saw the ad
CTR (click through rate) - total number of people who click an ad / total number of people who view an ad
Conversion Rate - total number of people who take an action / total number of people who click an ad
ROI - (Revenue - Cost)/Cost
ROAS - Revenue/Cost

DM Instruments:

- Online Advertising
- Search Engine Marketing (SEM) and Advertising (SEA): pay per click – keyword advertising. Allows efficient fulfillment of demand, market feedback and transparency of data. Exp: google ads. They do auction concept for ads. Advertiser can specify daily budget, and max CPC bid. Google Ads calculates a score, called Ad Rank, for every ad, which depends on bid, ad relevance, landing page experience.
- Search Engine Optimization (SEO) concerns the organic (=non-paid) search results, ranking of sites by search engines. On-Page optm: relevant keywords, discription of pictures, headlines, etc. Off-page optm: social signals(repost), linkbuilding (which domains link to the website, etc)
- Web Analytics: page view, visit, landing page, bounce rate, time on site, event, channel. Helps gain customer insights, product insights, performance evaluation.
- Remarketing & Retargeting: Remarketing is re-engaging customers, e.g. via email marketing. Retargeting is when ads are placed off-site targeting users that visited one's own site. -> Cookies use.
- Affiliate Marketing - Merchants promote their products or services via the network of a partner (the Affiliate). Google AdSense, Amazon Affiliate Program.
- Email Marketing - another communication channel to the customer; often opt-in. Can be transaction Emails, Newsletters or Stand alone campaigns. Ultimate goal: increase Customer Lifetime Value.

5. Foliensatz – Markets & Networks

Business transaction phases: Information phase -> Negotiation phase -> Settlement phase
Transaction – agreement between buyer and seller to exchange goods.
Transaction costs are expenses incurred when making a transaction.
Market is a medium that allows buyers and sellers of a specific good to interact in order to facilitate a transaction. Can be virtual.
Electronic markets - IT based market places for exchanging goods and services, supporting (all) phases of a transaction.

Perfect Competition - an idealized market structure where following assumptions hold:

- large number of buyers and sellers
- perfect information available to all actors; risk-taking is minimal
- rational actors take decisions to maximize self interest;
- no barriers to entry or exit
- homogeneous goods that are substitutes of each other
- zero transaction costs
- no externalities in transactions from third parties
- no government regulations, and no price setters

Transaction cost theory says that perfect competition does not exist in real markets and cannot explain the emergence of firms. Why are some transactions performed within firms rather than in the market -> to minimize the transaction costs.
Transaction costs are determined by asset specificity (The more specific an asset, the more difficult is to reuse), Frequency (How often trading actors perform transactions) and Uncertainty.
Hierarchy - coordination by some central power instance, based on longer lasting plans. Has lower transaction costs and less information problems. Hierarchical coordination is based on influence and control of a coordinating firm, it causes control cost, but it permits enforcement of interests of the coordinating firm and prevention of coordination problems.
The higher the asset specificity and the uncertainty(complexity) the more likely is the transaction to be organized in a hierarchy. -> IT questions the use of hierarchical organizations, since IT lowers communication cost, allows for more complex descriptions (reduces uncertainty) and IT reduces asset specificity.
Networks are organizational arrangements that use resources and/or governance structure from more than one organization. Networks are a "middle way" between the loose coupling of markets and tight relationships of hierarchies. The combination of cooperation and competition between participants of a network is called coopetition.
Exp: Long-term relations of a company to its law, consulting, accounting and banking firms.
Limitations that lead to intermediation:

- Search costs (on both sides)
- Match of demand and supply
- Incomplete information
- Contract risk
- Trust
- Pricing inefficiencies

Infomediaries - electronic intermediaries that control information flow, often aggregating information and selling it.

Intellectual property (IP) - creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce.
IP is protected in law by, for example, patents, copyright and trademarks.

Copyright should provide an incentive for the creation of new works of art. Copyright protection is automatic, it extends only to expressions of ideas, its valid for the life of the author + 70 years.

2 types of copyright:

- Moral rights: The right to be attributed as the author/creator, and to ensure that the work is reproduced in a manner that does not offend the author/creator.
- Economic rights: The right to produce copies and to make the work available. This includes the right to: reproduction of the work, distribution of the work, public display and performance of the work, transformation of the work.

The author as a rule owns both economic and moral rights to their work, but can sign away economic rights when for example publishing.
Code can be open source or open code (the opensource license must be attached to the code) or closed (trade secret, proprietary license).
Patents exist as incentive for inventors to reveal the workings of their inventions.
A patent is an exclusive right granted for an invention, which is a product or a process that provides, in general, a new way of doing something, or offers a new technical solution to a problem. In order to be patentable, the
invention must fulfill certain conditions:

- It must be of practical use;
- It must show an element of novelty
- It must show an inventive step which could not be deduced by a person with average knowledge of the technical field;
- Its subject matter must be accepted as "patentable" under law.

A patent is an exclusive right granted for an invention, usually for 20 years. The patent owner may give permission or license the patent or sell the right to the invention to someone else. Once a patent expires, the protection ends, and an invention enters the public domain.
Trademarks exist as consumer protection: trademarks empower manufacturers to punish rivals who misleadingly market competing products or services that are like to cause confusion among their customers.
Digital rights management tools are a set of access control technologies for restricting the use of proprietary hardware and copyrighted works. Technologies include product keys, limited install activations, persistent online authentication, copying restriction.

Controversies: disappearing license authorities (If you buy a license to read a book on a platform, then there are various reasons that you could lose access to the book), unusual business models (add security chips to printer cartridges – identify and lock out refilled cartridges).

6. Foliensatz – Social, Political, Regulatory & Economic Environment

Imperfect markets can lead to market failure -> government steps in to regulate (consultations, policies, funding, taxation). Examples for policies: EU's digital services act (publishing transparancy reports, etc).

Data is the new oil/gold analogy: data is fool's gold; insight is pure gold.

Data access and reuse can generate social and econ benefits to 1 – 2,5% of GDP.

EU Strategy for data: data can flow within EU and across sectors, availability of high-quality data, EU rules and values fully respected, rules for access and use are fair, practical & clear.

Relevant Legislations: General Data Protection Regulation (GDPR) -> fines up to 20K or 4% of worldwide annual turnover, Data Governance Act, Data Act.

EU Data Governance Act

1. Mechanisms to facilitate the reuse of certain public sector data that cannot be made available as open data.
2. Measures to ensure that data intermediaries will function as trustworthy organisers of data sharing or pooling within the Common European Data Spaces.
3. Measures to make it easier for citizens and businesses to make their data available for the benefit of society (data altruism).
4. Measures to facilitate data sharing, in particular to make it possible for data to be used across sectors and borders, and to enable the right data to be found for the right purpose.

EU Data Act

• Measures to allow users of connected devices to gain access to data generated by them, and to share such data with third parties to provide aftermarket or other data-driven innovative services.
• Measures to rebalance negotiation power for SMEs by shielding them from unfair contractual terms imposed by a party with a significantly stronger bargaining position.
• Means for public sector bodies to access and use data held by the private sector that is necessary for exceptional circumstances, particularly in case of a public emergency.
• New rules allowing customers to effectively switch between different cloud data-processing service providers and putting in place safeguards against unlawful data transfer.

Open Government Data (OGD) is a philosophy – and increasingly a set of policies – that promotes transparency, accountability and value creation by making government data available to all. By encouraging the use, reuse and free distribution of datasets, governments promote business creation and innovative, citizen-centric services.
Difficulties

- Data out of date
- No guarantee that data source continues to be available
- Data quality
- Data available depends on various factors

Obsticle: majority of data remains locked in data silos, which do not share data outside of ist closed environment.

Main actors in data ecosystem:

- Data generators: primary source of data, f.e. users browsing the internet, consumers paying with their credit card, location data from GPS readings. May be able to ‘monetise’ this information;

- Data Services: The actual creation of value of data only occurs when that information is processed and analysed;
- Data Business Users: Companies and public administrations using the outcome of data analytics to improve performance;
- End Cusromers: Consumers, business customers or citizens dealing with companies or public administrations, are often also data generators themselves;

Data markets can be:
- Property Market: Data Sale negotiated between buyer and seller
- Consumer Market: Data bought off-the-shelf (Taxi demand map)

Callenges:
- Companies are not sure how valuable their data are
- Companies do not see their business as selling data
- Getting into selling data has high overheads
- Selling small amounts of data is not straightforward
- Companies are concerned about inadvertently revealing proprietary or personal information

EU Artificial Intelligence Act

The EU Parliament adopted the AI Act in March 2024 and the Council followed with its approval in May 2024. It will be fully applicable 24 months after entry into force, but some parts will be applicable sooner.

It splits AI Systems into 4 tiers:
- minimal risk,
- transparency risk: Generative AI, like ChatGPT, will not be classified as high-risk, but will have to comply with transparency requirements and EU copyright law Disclosing that the content was generated by AI, Designing the model to prevent it from generating illegal content, Publishing summaries of copyrighted data used for training; Content that is either generated or modified with the help of AI images, audio or video files (for example deepfakes) – need to be clearly labelled as AI generated;
- high risk: AI systems that negatively affect safety or fundamental rights; AI systems that are used in products falling under the EU's product safety legislation or AI systems falling into specific areas that will have to be registered in an EU database: Management and operation of critical infrastructure, Education and vocational training, Employment, worker management and access to self-employment, Access to essential private services and public services and benefits, Law enforcement, Migration, asylum and border control management, Assistance in legal interpretation and application of the law;
- unacceptable risk

High-impact general-purpose AI (GPAI) models that might pose systemic risk, such as more advanced LLMs, would have to undergo thorough evaluations and any serious incidents would have to be reported to the European Commission.

7. Foliensatz – Privacy & Ethics

GDPR includes data anonymisation.

Netflix prize - Open competition for the best collaborative filtering algorithm to predict user ratings for films, based on previous ratings without any other information about the users or films. No information at all is provided about users. Some values are perturbed in the training set to protect privacy. Won in 2009. However, the anonymity of the Netflix prize dataset is easy to breake using movie database, Netflix record of known user can be identified.
Ethics: discriminatory algorithms -> GDPR
Dark patterns - user interface design choices that benefit an online service by coercing, steering, or deceiving users into making unintended and potentially harmful decisions.

- Sneaking - attempting to misrepresent user actions, or delay information that if made available to users, they would likely object to.
- Urgency - Imposing a deadline on a sale or deal, thereby accelerating user decision-making and purchases.
- Misdirection - Using visuals, language, or emotion to steer users toward or away from making a particular choice.
- Social Proof - Influencing users' behavior by describing the experiences and behavior of other users.
- Scarcity - Signaling that a product is likely to become unavailable, thereby increasing its desirability to users.
- Obstruction - Making it easy for the user to get into one situation but hard to get out of it.
- Forced Action - Forcing the user to do something tangential in order to complete their task.
- Price Steering - Changing the order of search results to highlight specific products
- Price Discrimination - Customizing prices for some users

Micro-targeting: splitting users into segments and targeting different segments.

GDPR Effects:

- Data Processing and Profiling: Organizations may not use personal data for a purpose other than the original intent without securing additional permission from the consumer; Robust anonymization processes must be used where possible;
- Right to an Explanation: There are good reasons to use interpretable techniques, in particular to avoid bias; GDPR should not limit the techniques used to train predictive models;
- Bias and Discrimination: Ensure fair and transparent processing; Use appropriate mathematical and statistical procedures; Establish measures to ensure the accuracy of subject data employed in decisions; Take into account data with potentially implicit bias, e.g. residential area.

OECD Fair Information Practices (1980):

- Collection Limitation: Data should be collected within limits, by lawful and fair means and with consent (where appropriate)
- Data Quality: Data should be relevant, accurate, complete and kept up-to-date
- Purpose Specification: The purposes of collection should be specified at the time of collection
- Use Limitation: Data should not be used or disclosed for other purposes except with consent or by the authority of law
- Security Safeguards: Personal data should be protected against unauthorized access, destruction, use, modification or disclosure
- Openness: Users should be able to know what data is being collected, who controls the data, and for what purposes they are used
- Individual Participation: An individual should be allowed to inspect the collected data about themselves, and have them erased, rectified, completed or amended
- Accountability: The collector of the data should be accountable for complying with the above measures

8. Foliensatz – Cryptocurrencies

Traditional financial arragements:

- barter (requires coordination)
- credit (gives good, gets favour; -: risk through being owed a debt; +: doesn't need "bootstrapping")
- cash (-: system needs to be "bootstrapped" with cash, +: can be precise about the worth of something)
- Blended System: debt is measured in the amount of cash it would take to settle it

Credit today:

- Need a centralised institution to handle money transfers for every transaction – fee to this institution
- Privacy concern – this institution has records about how much money is spent where for each client
- Possibility of fraud (fee usually includes insurance against this)

Credit cards are dominant today for payment on the internet:

- Direct payment: No intermediary, All details stored by the Seller
- Payment through Intermediary: Seller doesn't get credit card details (security risk), Seller doesn't need your identity (privacy), Seller does not deal with the "financial system"

Digital cash: Some sort of instrument, enabled by technology, that acts much like physical cash, with no transaction fees, fast exchange of funds, confidentiality for participants, no possibility of after-the-fact revocation of the payment

Ecash

- Needs banks to implement the protocol
- Clients are anonymous
- Merchants are not anonymous – they must return coins to the bank as soon as they get them
- Resulted into failure

Cryptocurrency - any form of currency that only exists digitally, usually has no central issuing or regulating authority but instead uses a decentralized system to record transactions and manage the issuance of new units, relies on cryptography to prevent counterfeiting and fraudulent transactions.

Cryptographic Hash Function For a hash function to be cryptographically secure, we require Collision Resistance, Hiding, Puzzle Friendliness.
A hash function H is said to be collision resistant if it is infeasible to find two values, x and y, such that $x \neq y$, yet $H(x) = H(y)$.
Hiding : If we're given the output of the hash function $y = H(x)$, there is no feasible way to figure out what the input, x, was.
A hash function H is said to be puzzle friendly if for every possible n-bit output value y, if r is chosen from a distribution with high min-entropy, then it is infeasible to find x such that $H(r \| x) = y$ in time significantly less than 2^n.

Digital Signatures

Only you can make your signature, but anyone who sees it can verify that it is valid. The signature should be tied to a particular document. Signatures are existentially unforgeable – no matter what algorithm is used, the chance of successfully forging a signature is so small that we can assume it will never happen in practice.
There is a limit on the size of the message that are able to be signed -> sign the hash of the message, rather than the message itself
Public keys can be equated to an identity. you can make new identities whenever you want.

Bitcoin

First cryptocurrency to be invented, blockchain was utilized for the first time, Priced at ~€93.740/BTC as of end 2025.
A wishes to transfer M BTC to B -> a public ledger called the
Blockchain acting 3rd party -> The blockchain is a publicly available record of all the transactions made since the beginning of the Bitcoin -> The blockchain reveals whether A owns M BTC -> Other Bitcoin users confirm the transaction and add it to the
Blockchain-> No private information is revealed in the process.
Each transaction has a unique identifier, inputs are the coins consumed which were created in a previous transaction, outputs are the coins being created.
A blockchain consists of linked blocks, Each block contains many transactions, Each block is linked to the previous one, A new block is added to the blockchain every 10 minutes through the process of mining, Every block has been validated as legitimate, Once a block enters the blockchain it cannot be changed, No central authority controls the blockchain, Blockchain utilizes Cryptographic Hash Algorithm SHA-256, which produces a string of 64 characters (32 bytes).

Bitcoin Mining: The process with which legitimate blocks are added to the Blockchain, performed by miners. Requires a lot of processing power, expensive hardware and electricity, the miner that succeeds gets rewarded with bitcoins.

Mining Process :

- Transactions Picking
- Proof of Work: a hash output (aka signature) that starts with a certain number of 0s

- Validation and Addition to the Chain

- Listen for transactions – validate them
- Maintain the block chain and listen for new blocks – validate each block received by validating each transaction and checking the validity of the nonce
- Assemble a candidate block – group validated transactions into a block
- Find a nonce to make the block valid – requires the most work
- Hope your block is accepted – other miners have to have a consensus to accept your block

Estimated that the Bitcoin network generates 11.5 kilotons of e-waste each year.

Etherium

Running on a blockchain

Ether (ETH) is the cryptocurrency circulating within the platform.

Its distinguishing feature is the smart contract - Automatically executable lines of code that are stored on a blockchain which contain predetermined rules. Either A or B or both will write the code that implements the transaction. Both will digitally sign it and it will enter the blockchain. No third party required to enforce the contract.

Crypto: community & policy

Three types of consensus in bitcoin: about rules, about history and that coins are valuable.

Stakeholders:

- Core developers — write the rulebook and almost everybody uses their code
- Miners — write history and decide which transactions are valid
- Merchants and their customers — generate the primary demand that drives the price of the currency
- Investors — buy and hold bitcoins, so it's the investors who decide whether Bitcoin has any value
- Payment services — handle transactions and decide which currencies to select – maybe drive primary demand

Bitcoin vs. Government:

Capital controls - laws that a country has in place that are designed to limit the flow of capital (money and other assets) into or out of the country

Bitcoin can easily be used to circumvent these .

Crime crimes like kidnapping and extortion become easier, tax evasion, sale of illegal items