

# Fintech And Crypto Currencies

## Exam Theory Answers

UCT MPhil Financial Technology

Christopher Maree - MRXCHR013

---

### Question 1.1:

Disruptive innovation describes a product or service that starts out as underrated but in time becomes popular enough to replace a conventional product or service. Some key characteristics of disruptive innovation are that the product begins at the low end of the market with normally a poor quality. This product can, but is not always, associated with often associated with the creation of a new technology. In time, due to lower costs and higher accessibility and market penetration, the product eventually becomes the most appealing product on the market. Usually a disruptive company is hard to spot before it becomes large because by its very definition it starts small and slowly grows until it is too big to be stopped by the companies that it will displace.

A key part of this is that the company needs to be creating a new market that did not exist before or fundamentally changing the market dynamics of an industry. It is not enough to simply make an improvement upon existing technology or markets (referred to as sustainable technologies/innovation). For this reason Netflix is considered a disruptive innovation as it fundamentally changed the market dynamics of movie rentals. However, Google is not a disruptive company as their tech was more of an improvement over previously existing search engines, and did not create a new market force or dynamic.

Finding a company that has not been labeled as disruptive is difficult as the media is willing to throw the word around to define any new and upcoming company that is making changes in its respective industry. To this end the company that I have chosen that will disrupt its target market in the next 5 years is **Impossible Foods**. They create a hemp based meat substitute that actually tastes really good and many people can't distinguish it from normal meat. Impossible Foods was founded in 2011 by a Stanford biochemist and is currently scaling the manufacturing of its Impossible Burger (ground beef substitute) and is developing other meat substitutes to replace animal agriculture at large. The impossible burger is currently sold in many restaurants around the world and its adoption is growing quickly.

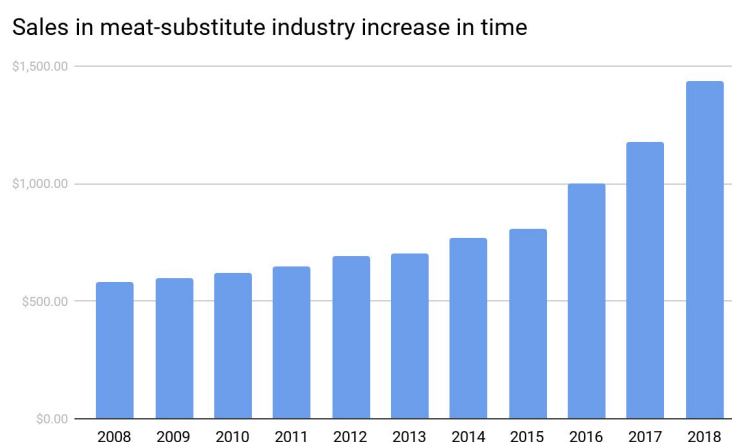
Despite the fact that Impossible Foods recently raised \$300 million in funding and currently has a \$2 billion in valuation I think that they still have massive potential to grow and fundamentally change the meat based foodstuffs marketplace. In alignment with the definition of a disruptive company, Impossible Foods started out by creating a product that caters to the low end of the market: fast food burgers. Putting their meat substitute in a burger is a great way to hide that the taste is not quite the same as beef as it can be masked by all the other flavours and textures in the burger. This has given them the opportunity to get a foot in the door of the industry at large and will enable them to slowly grow while they refine their technology in creating artificial meat based products. In time the quality of their produce will improve and they will be able to expand their offerings to more than just burgers and eventually they will be able to compete with any and every meat based product. At this point they will have gained enough market share at the low end that they can begin to compete at a higher end.

The main reason that Impossible Foods and synthetic meat based products are disruptive is because they can create *almost* the same product but at a fraction of the cost(in the future) and with a fraction of the footprint on the environment. Animal agriculture contributes ~ 30% of annual greenhouse emissions worldwide. According to the Impossible Foods “Impossible Burger uses 96 percent less land, 87 percent less water, and generates 89 percent fewer emissions compared to traditional beef”. Eventually Impossible Foods will be able to fundamentally change the market for meat products by offering a radically different alternative that before now was not even an option.

An additional market force which will contribute to the growth of meat-substitutes and thereby increase the ability for Impossible Foods to become a disruptor is fast food chains adopting their product and offering it to their customers. To this end, McDonalds has partnered with Impossible Foods to offer a vegetarian version of their product line which is based off Impossible Foods hemp-based meat patties. As Impossible Foods creates more and more partnerships they will be able to secure the foothold in the market which will enable them to grow to the point of disrupting the higher priced sections of the meat and animal based products market.

Another key element is that Impossible Foods’ technology is still a work in progress and still needs refinement until it will be truly disruptive. This can potentially happen in the next 5 years wherein a meat substitute is as tasty as normal but without all the negative environmental implications of traditional meat products while at a lower cost. At this point there will be a fundamental redistribution of the market capture shifting away from beef based product and towards non-beef alternatives. All while they are developing their technology they are gaining market traction in the bottom end of the market through their Impossible Burger.

Looking at the market growth of meat-substitutes we can see that in the last 3 years there has been a sizable increase in meat-substitutes. The graph below (data taken from <https://www.euromonitor.com/>) shows the total revenue (in US millions) over the last 10 years. This trend shows the beginning of a shift towards commercial acceptance and demand for meat-substitutes. This increase will also be coupled with the increase in quality and decrease in costs of meat-substitutes as technology improves. Another contributor to this will be people around the world becoming more aware of the impact of their eating habits on the environment and in time this will also contribute to market growth of meat-substitutes. Ultimately the disruption of plant based meat alternatives will be as a result of the product being cheaper, more sustainable, healthier and quicker to produce.



## Question 1.2:

A lot of companies will use blockchain to just ride on the hype of the buzzword. Practically 9 out of 10 times a traditional database would be more than sufficient for an application. Blockchains are slow and inefficient, hard to code on and difficult to maintain. Getting a product to market is difficult and so you better be sure that you need a blockchain in your product if you want to use one.

Even though blockchain does not allow for modification of data that is stored on chain (immutability) it has no way to ensure that data is entered into the blockchain is valid. This means that many applications that touch the real world have fundamental levels of trust required to be baked into them. Normally, this kind of information is fed to the blockchain using an oracle. This helps the situation somewhat but you still have to *trust* the oracle. For example, supply chain management, object authenticity guaranteed, proof of authorship and even land registry all require to trust the physical entity that entered the data onto the platform and so the fundamental use of blockchain in these cases is questionable. Granted blockchain can make these industries more *transparent* and harder to tamper with, which is definitely a plus but there will always be some level of trust required at the core place where blockchain touches the real world.

An example of a company that uses blockchain but shouldn't is the **Sun Exchange**. Their core product is using blockchain for solar project insurance. The basic premise of the idea is to issue an ERC20 token (Called SUNEX) which users can stake within a "solar project insurance fund" (or SPIF). The SPIF acts as a mechanism to own an investment within solar projects, thereby granting the SUNEX tokens fractional ownership within the solar projects. The funds within the SPIF are "backed by the physical hardware of the solar panels".

While this all sounds great in theory, there is one massive problem with how they conducted their token sale and their fundamental business model which means that it should not use blockchain. The problem is that they (the Sun Exchange) need to be trusted at every point along the supply and funding phases of each and every project. Therefore claiming that the blockchain makes their project more secure is actually a complete misnomer. This misdirection can be seen from the fact that:

1. The sun exchange claims that they took all the money they raised in the ICO and exchanged it to FIAT then invested it in sovereign debt. This debt was then used to protect the solar panes against default of the solar panel projects. This is where the insurance comes in.
2. They then claim that they pay out parts of profits generated from the solar farms using a profit sharing model to investors in *either* Bitcoin or FIAT over the 20-year lifespan of the farms.

As the money they raised from the ICO is sitting in FIAT sovereign debt and the Sun Exchange pays out to investors using either Bitcoin or FIAT the connection between the blockchain and SUNEX token is completely and utterly controlled and operated by The Sun Exchange. This means that they can artificially inflate the supply of tokens or lie about the value of money in the bank or where they sent the sovereign debt and no one would be the wizer.

They have not been audited and have no plans to be so there is no way to know what's going on under the hood in their system. For this reason there is no point in the Sun Exchange to have a blockchain within their product as you ultimately have to trust the weakest link in any trust chain and this resides with the company itself.

They could implement the exact same system without a blockchain and with a database to track people's balances as ultimately they control every aspect of their ecosystem. The trust properties of a completely centralized solution are exactly the same. In their case the blockchain adds zero value. For this reason the sun exchange should not use a blockchain. They can still accept and make crypto payments but their use of the blockchain as an account tracking mechanism makes no sense as it is expensive and slow when compared to other systems with the same trust & security characteristics.

### Question 1.3:

An initial coin offering (ICO) is a type of fundraising used by blockchain projects where before a platform launches founders sell tokens (coins) which will be used on the platform when it is launched. In this way the ICO is a source of capital for the startup to help in building out the platform. Normally ICOs are public where any investor can contribute and tokens tend to start selling at a discounted rate. After a period of time the tokens can be traded in secondary markets like crypto exchanges.



ICO's have been associated with a lot of fraud, manipulation and pump and dump schemes. Additionally, many ICO's fail soon after the token launch. One such ICO that was both a scam and failed is **OneCoin**. Onecoin was one of the worst ICOs of 2017 and managed to execute a near textbook perfect scam.

The core concept of one coin was to sell educational material used in trading. Members were able to buy packages of educational materials ranging from 100 to over 100 000 euros which were represented as "tokens" (with the label OFC). Later these tokens could be converted into OneCoins (with the label ONE) which was to be used on their merchant platform. After the initial token sale there was no way to convert your OFC's to other crypto currencies or FIAT. OneCoin had a dodgy website full of spelling and grammar mistakes, the team had a history with other scams and the Founder and COO falsified her qualifications on the site. Despite all these red flags they managed to scam investors out of almost \$4 billion in worldwide revenue. To date 98 people have been prosecuted for the scam, many are in prison and many more are still on the run. *Was it possible to identify that OneCoin was a scam by only looking at their white paper?*

One can analyze the OneCoin white paper to see a number of red flags that should have informed investors to steer clear of the OneCoin ICO. The sections below examine some of the major doggy parts of the white paper. Numbers in square brackets reference screenshots of the white paper that follows.

- 1) To begin with out of the 35 page white paper only 11 pages are about the actual product. The remaining pages are legal disclaimers. While this is not dodgy in and of itself, it does give the feeling that the authors are trying to hide something.
- 2) There is little to no technical description of the OneCoin platform.
  - a) The parts that do talk about the technical details of a centralized proof-of-work (POW) based system[1] that runs on top of AWS[2].

- b) This makes absolutely no sense to do. You would never run a centralized solution using POW as your consensus algorithm. It is just simply the wrong setup. If you are running a centralized solution you would either use proof of authority or if you wanted there to be a token based incentive structure proof of stake but definitely not proof of work which is running in an AWS.
- 3) They make outlandish claims about the scalability of the platform which could only be achieved with a centralized SQL like solution; not a blockchain based solution[3] (at the time of writing no other blockchain could achieve this kind of performance so how could they?).
- 4) They refer to “running backups of the blockchain” [4,5] to ensure that users don’t lose funds. This fundamentally is not required if they have an immutable ledger.
- 5) Refer to the implementation of a “Disaster Recovery plan” to “recover the IT infrastructure in the case of an event or disaster” to mitigate the loss of user funds in the case of a hack. Again this is a massive red flag because you should never need to recover your “blockchain” using a “backup” if it is immutable.

#	White paper extract
1	<p>OneCoin blockchain use proof-of-work (POW) that involves scanning for a value. When hashed, such as with SHA-256, the hash begins with a needed target (for example a number of zero bits). The proof-of-work is implemented by incrementing a nonce in the block until a value is found that gives the block's hash the required target. Once the CPU effort has been expended to make it satisfy the POW, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.</p>
2	<p>Since the OneCoin blockchain is centralized, the system uses one copy of blockchain data for several wallets. That means that if there are 4 or more wallets in a decentralized cryptocurrency, then there must be the same number of copies of the blockchain data. In the case of a centralized blockchain, however, it would be necessary to have, for example, only 2 copies of the data, so 3 wallets would be able to work with one copy, and other wallets with other copy. In this case, instead of performing a 4-times verification, only 2-times verification on 2 nodes is enough and will still be as true as 4 times verification of 4 different nodes.</p> <p>The OneCoin Blockchain can handle millions of user accounts on standard high-spec hardware (e.g. equivalent to current AWS 2xlarge instances) and this can be scaled up by upgrading to more powerful hardware (e.g. equivalent to AWS 4xlarge, 8xlarge, 16xlarge instances or higher) as required.</p>
3	 <p><b>SCALABLE</b></p> <p>The OneCoin blockchain can handle millions of user accounts. It has the capacity to process cross- border global payments and the capability to make unbounded transaction processing. The private management of the blockchain keeps the storage costs under control and prevents possible scalability issues that usually pertain to public blockchain.</p>
4	 <p><b>SAFE</b></p> <p>Based on cryptography, OneCoin cryptocurrency is safe and difficult to counterfeit. The ongoing data- backups performed by the company guarantee that there is low risk of stolen coins.</p>

**SECURE**

Because the company performs ongoing **data-backups**, there is a low risk of lost coins due to, for example, malfunction of the user's hardware or theft of coins.

Except live monitoring of the system and regular ongoing of backups of the whole system, the OneCoin blockchain implements DRP (Disaster Recovery Plan) to be able to respond adequately and in time when a disaster such as natural, environmental or man-made occurs (for example, an act of attack).

DRP is a set of procedures to recover and protect a business IT infrastructure in the event of a disaster.

Despite OneCoins super secure and safe ongoing data-backup system they managed to lose millions of user account balances when they were raided in Jan 2018. All these technology red flags in their white paper showed that their implementation was completely bogus and was a doomed centralized solution which has no inherent security. It is amazing that they were able to raise as much money as they did with such an outlandish whitepaper. The number of red flags makes it very clear that they were not intending to build a blockchain at all and claiming that their "centralized AWS blockchain" was secure and safe is without a doubt very dodgy.

### Question 1.4:

Proof of work (PoW) is a consensus algorithm which uses a computationally difficult puzzle to randomize and distribute the creation of new blocks within blockchains such as Bitcoin and Ethereum (Eth1.x). Upon finding a valid POW nonce a miner publishes their newly found block to the rest of the network where it is validated and then added to the blockchain. They are then paid a block reward for their efforts. This decentralized nature of finding new blocks makes it hard to centralize the mining process within the network while aligning the incentives of the miners with the network users. Ultimately POW solves the classic double spend problem that plagued all previous digital cash solutions before its initial usage in Bitcoin.

Proof of Stake (POS) on the other hand, does not require the expenditure of physical resources in mining blocks to secure the network. Rather, POS uses bonded collateral of the native token within the blockchain as a "stake" in the mining process of blocks. In this way, if a block proposer generates an invalid block or breaks one of the other consensus rules their stake can be slashed as penalty. Proof of stake fundamentally changes the economic mechanisms and incentives used to secure the network: In a POW based model you have to pay up front to mine a block (expenditure of electricity). However, in a POS based model you don't pay anything directly up front but there is the threat of a harsh penalty if you misbehave. This transition results in a number of major complexities when it comes to building out truly decentralized and censorship resistant POS based system, such as nothing at stake attacks, long range attacks and biasable randomness problems.

**Libra** is Facebook's blockchain implementation of a cryptocurrency which utilizes their own variant of proof of stake called LibraBFT. LibraBFT is a Byzantine-Fault-Tolerant (BFT) implementation which is a variant of the HotStuff framework<sup>2</sup> which was initially released in 2018 by VMWare Research. Libra's blockchain security depends on a byzantine agreement of  $\frac{2}{3}$  of the nodes to all agree on the output of a state change. In theory the framework would allow for future interoperability with other chains that make use of BFT consensus. Like all

other blockchain based solutions, Libra uses pseudonymous wallets with an associated public and private key pairing to perform transactions.

Libra uses a two token system: the Libra Investment Token(LIT) which acts as a governance token and offers participation in the governance of the network and the Libra token itself which is a stable token backed by a basket of FIAT currencies. Facebook is creating their own wallet, called Calibra, which will give Libra first class integration into the Facebook ecosystem with apps like Whatsapp, Instagram and Messenger all having their own wallets built in.

Libra is a permissioned blockchain. This means that a selected group of about 100 founding members act as validators on the network and need to be trusted in adding new transactions to the blockchain. This permissioned configuration is better than just having one centralized company run the network but it still requires some level of trust in operation. Libra has stated that they plan to transition to a permissionless system. However they have stated that this will depend on a number of technical and organizational issues which have yet to be resolved.

Existing traditional blockchains like Ethereum and Bitcoin use *blocks* as a central unit of storage within the system. Each miner combines a number of transactions together to form a block (after finding a valid proof of work). In Libra however the data structure does not contain blocks. For this reason, one might say that Libra is in fact not really a blockchain. It is rather more of a “decentralized programmable database”. In Libra the core data structure is a sequence of transactions that are incrementally stored in Merkel trees. The root of the tree contains an *authenticator value* which acts almost like a block hash from traditional blockchains. The  $i + 1$  authenticator value depends on the authenticator from transaction  $i$ .

Libra uses an account based model, similar to Ethereum. Fees are charged on the network when moving funds around or interacting with smart contracts. Similar to Ethereum, Libra has a gas price to quantify the cost of performing network operations. Internal structure of a transaction is similar to Ethereum containing: a sender address, amount of tokens to transact, maximum gas to be used by the invocation, a nonce, arbitrary code and a signature.

Smart contracts on Libra will be written in a new programming language called Move. This compiles down to bytecode which will be interpreted by a virtual machine. Move is a functional programming language with strict separation of code and data.

It is important to distinguish generic Proof Of Stake based systems with Libra’s permissioned Proof of stake system. Because Libra is a permissioned blockchain network which only pre-authorized validators there is trust required to be placed within this group of validators. Public permissionless networks on the other hand do not have this requirement and enable anyone to join and contribute to the security and validation of the network. Below some pros and cons of Proof-of work, generic Proof of stake and Libra’s implementation of proof of stake are discussed. These points specifically are looking at the consensus algorithm.

**Proof of work advantages:**

- Blockchain properties: Censorship resistant, immutable, partition tolerant, decentralized, transparent, strong liveness properties.
- Consensus properties: elegantly solves a number of hard problems of



decentralized system consensus such as selection of block proposers and selection of valid chain through longest chain rule (or GHOST in the case of ETH)

**Proof of work disadvantages:**

- To achieve decentralized consensus in a non biasable and immutable way requires to be inefficient by design
  - Therefore proof of work uses a lot of energy to validate transactions
- Slow throughput and poor scalability properties (BTC has 3tps & Ethereum 7tps)
- High barrier to entry to start mining with need for physical mining hardware
- Economies of scale make centralization of mining easier.

**Generic Proof of stake advantages:**

- Aims to maintain most of the blockchain properties of POW (some are hard to achieve though, such as partition tolerance and liveness)
- Democratization of mining as no longer require specific hardware
- Low energy requirements. Should be able to stake from smartphone or low power electronics.
- In theory can be highly scalable. Reaching higher very high tps.

**Generic Proof of stake disadvantages:**

- Hard to reach all three elements of the decentralized trilemma (scalability, security and decentralization) and so many solutions sacrifice on some of these properties.
  - For example many POS blockchains use delegated POS which sacrifices the decentralization and security to increase the scalability
  - POW on the other hand manages to address many of these issues.
- High cost in native currency (required bond) to start staking.

**Libra's implementation of Proof of stake Advantages:**

- Uses far less energy than POW.
- Far more scalable than POW with much higher tps
- Potentially easier interoperability with other blockchain systems

**Libra's Implementation of Proof of stake disadvantages:**

- Requires trust to be placed in centralized consortium members who run the blockchain network
- Transactions can be tracked, monitored and censored by consortium
- Impossible to publically contribute to consensus process.

## Question 1.5

I was part of group 4, project UniCoin. UniCoin enables academics to commercialise their work through auctioning off licences to companies that would want to implement their ideas. Publications are always left as free and accessible to the open science community for other non-commercial research. Researchers can select to share a proportion of their revenue with others who contributed to the research. In theory this is a great idea but there are a number of serious regulatory obstacles that would need to be overcome in order to make UniCoin a reality. Some of these are discussed below.

### 1) Validity of intellectual property claim through non-fungible licences

The core premise of UniCoin is the creation of blockchain based licences which represent permission from the content creator to monetize her work in the name of the company that holds the licence. The problem here comes in from a legal perspective in defending the licence in a court of law. This non-fungible licence, while cryptographically unique and guaranteed to originate from the content creator, is not a legal construct that can be used to defend the claim of explicit permission granting from the content creator to licence holder.



Fundamental regulatory changes would be required in the legal framework to make this a reality.

## **2) Verification of authorship of academic publication**

A second premise of UniCoin is that only the author of the publication should be able to publish her work on the platform. This means that I should not be able to go and get someone else's paper and publish it, claiming it as my own and ultimately profiting from it. This premise is based upon having a sufficiently strong legal framework that could sue individuals that broke this assumption and stole others IP on the platform. How this regulatory obstacle can be overcome in real life remains an open ended problem and is not unique to UniCoin. It is a very common blockchain problem.

## **3) Association of publication with underlying comertilizable intellectual property**

Within the UniCoin platform users buy access to an academic publication and then are allowed to commertialize the ideas within it with explicit permission of the author. This, however, makes the assumption that the intellectual property within the publication originated from the publication itself. There is no mechanism to prevent someone from taking an idea, putting it in a paper they write and then claiming that the publication was the source of the idea. Fundamentally this why the process of getting a patent in the real world takes so long and is so expensive. There needs to be proof of the novelty and originality of the idea. UniCoin does not enforce this at all and so this would need to be implemented through some external non blockchain regulatory framework to ensure that this premise will hold up in a court of law.

## **4) Legal framework to pursue violators of licence agreement**

There is no way to pursue people legally that do not follow the licence agreements laid out on the UniCoin platform. This means that someone could just find an idea, download the paper for open-science usage and then commercialize the idea anyways. There is literally nothing stopping users from doing this. As a result, a regulatory framework would be required to provide assurance that people who violate the licence agreements will be pursued in a court of law to enforce the agreements.