TODO This needs some cleanup

What is Blockchain?

You've heard that blockchain is going to disrupt nearly everything from banking to voting to real estate. The term "blockchain" is often overused, that can have different meanings in different contexts. Blockchain technology has 3 major components that together really make it an innovation. Strictly speaking, a **blockchain** is just a data structure similar to a linked list. Blocks of data reference their previous block by including their digital fingerprint or hash in their block of data. If a previous block is modified, then all the following hashes will be different and it is easy to detect if the data has been tampered with. Even more importantly, is that this establishes an order to when events took place, in the case of Bitcoin, these events are transactions. The final piece is a consensus mechanism that allows participants on a public distributed network to all agree on a chain of blocks.

Consensus

A consensus mechanism extends the blockchain data structure by providing rules (agreed to by network participants) that enforce how blocks are accepted by the network as a whole. For example, with the proof-of-work consensus, there is an agreed upon amount of work that must be done before a block is accepted as valid (it must meet a maximum value threshold). The lower the threshold, the more work must have been done (on average) to calculate the block hash. Providing a valid block hash becomes a proof-of-work. This can make it much more difficult to modify past blocks, as the same amount of work must be done in order for the network to accept it as valid, thus distributed consensus can be achieved. This is why "blockchain technology" was invented, to achieve distributed consensus without relying on a third party. "Blockchain technology" is not really that interesting without the proof-of-work component and so it depends on what your definition of "blockchain technology" happens to be.

Bitcoin

Bitcoin was initially proposed in 2008 1 on a cryptography mailing list by a person or persons under the pseudonym Satoshi Nakamoto, who's real identity remains unknown. The proposal outlines a new innovative way to create a decentralized digital money. There are a few major problems that prevented this from working in the past, which the proposal claims to have solved.

1. Issuing new coins without a 3rd party
2. Handling transactions without a 3rd party
3. Preventing double spends

Since the goal of the project was to "allow online payments to be sent directly from one party to another without going through a financial institution", Bitcoin was designed as a decentralized application. This means it is not hosted on a central server controlled by a company or government. In fact, anyone can run the application and process transactions and mint new coins. Since there are so many participants, you can see how it would be difficult for participants to trust each other that no one is making fake coins and stealing money. A central server can easily establish these things, by acting as the authority with which all participants must agree. The problem is that this gives too much control to a third party who might be manipulated or have their own intentions. Bitcoin proposes a different approach.

In order to mint new coins and establish new transactions, a user must take a block, which contains the latest transactions on the network for all users, and compute a hash using the double SHA256 hash function (more on this later). If a user is able to do this, they are rewarded with new coins. The computed value, the hash, must be a number lower than or equal to the current network target value. To achieve this, you can keep changing a nonce within the block until the output value is a valid solution.

Let's assume the network target value is `00000000ffffffffffffffffffffffffffffffffffffffffffffffffffffffff`. This is an example of an output from the SHA256 hash function. It is an extremely large (256 bit) number represented as hexidecimal (base 16). Here is an example of a valid solution:

Input	Algorithm	Output
Block Header	double SHA256	000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

One quick way to verify is to count the number of zeros at the beginning and compare. If they are the same, see if the first nonzero value is less that the first nonzero target value. This is in fact the hash of the first bitcoin block and would take a normal laptop all day (12 hours at 100k Hashes/s) to compute. It would in fact have to guess, on average, 4.3 trillion times before a solution is found. You can see this takes the computer considerable work. Thus, when a solution is found it is considered a proof-of-work. This term refers to the amount of work a given hash value took to compute. In order to change a block in the past, one must redo this work for that block and any blocks afterwards. This makes it extremely difficult to modify or hack the blockchain by undoing a transaction, for example. Each new block creates another "transaction confirmation" and makes it more and more difficult to undo a past transaction, further securing the transaction order and history.

One of the Bitcoin-specific rules for the blockchain is that the longest chain (the one with the most proof-of-work) will always be considered the valid chain. Users will share this blockchain with others and they will compare all of the blockchains they receive from the peers they connect to and regard the longest as the source of truth for the network. All minted coins and transactions are validated and agreed upon by the whole network by checking the proof of work and accepting the longest chain.