Learning Goals

- Understand what cloud computing is
- Understand the pros and cons of cloud computing
- Understand how cloud computing creates a backbone for cryptocurrency
- Describe how cryptocurrency works at a high level
Cloud computing is the notion where you use other servers connected to the Internet to do your work for you.

For example, you could ask other servers to do some operations for you (e.g., process data) or you can ask other servers to store data for you.
Types of Cloud Computing

• You can have:
  • Private clouds (where only a select few individuals (i.e., UBC’s own students or staff) can store information on the servers)
  • Public clouds (such as Google Drive where everyone can make an account to store information)
The cloud is great!

- **Convenience**
  - You can access your data anywhere you want as long as you remember your password
  - If you lose your computer/phone, it’s less of a hassle to restore what you have

- **Scale**
  - You don’t need to buy 10000 machines to get the power or processing capability you need. You can outsource and pay for that work.

- **Maintenance**
  - You don’t have to deal with fixing or updating software on a ton of machines
There are downsides too!

- You also depend on the infrastructure security of the company running the cloud service you are using
  - E.g., Equifax (July 2017) had a huge data breach which resulted in millions of people having their sensitive data (name, date of birth, SIN/SSN number, etc.) leaked
  - E.g., Celebrities were targeted using phishing attacks and the data they stored on iCloud (emails, photos, etc.) was leaked
There are downsides too!

- You also depend on the company itself to make sure your services or your data stays available
- If the company hosting all the servers you depend on goes down or has an outage, you are affected!
What can we do with cloud computing?

- Cloud computing is the backbone for cryptocurrency
- **Cryptocurrency** is a decentralized virtual currency
What can we do with cloud computing?

• Bitcoin was the first cryptocurrency but may others have come about afterwards

• These other types of cryptocurrency are sometimes called **altcoins**
  • E.g., Dogecoin, Ethereum

• Cryptocurrency is a type of digital currency and is not the same as electronic money
Cryptography

• The crypto portion refers to cryptography!
  • Information is run through an algorithm to encrypt it
  • It’s central to how cryptocurrency works! Even your own access to your “money” is guarded through cryptography
We’ve talked about encryption before

- When we were looking at how the Internet worked (and when we talked about Turing), we talked a bit about encryption.
- Here’s a refresher:
  - Encryption is basically a way to scramble information to prevent unauthorized individuals from accessing your data.
We’ve talked about encryption before

Let’s say you lock some confidential information in a box using a unique symmetric key and
How does this factor into cryptocurrencies?

- You aren’t sending messages like the video describes but cryptocurrencies use cryptography in a few ways
  - Hash data (more about this later)
  - Sign data
- Depending on the cryptocurrency you are looking at, different things are encrypted
  - E.g., Bitcoin doesn’t encrypt transaction logs but Monero and ZCash do
What do we currently do?

- The Bank of Canada controls how much currency we have in the economy
  - It decides whether we print more currency, what the interest rates should be, etc.
- We also have FINTRAC, a system that helps track monetary dealings, to prevent money laundering.
- This is a **centralized** system (i.e., one institution is managing our economy)
What does cryptocurrency do?

• Cryptocurrencies operate in a decentralized manner
  • There’s no one person or institution that decides on “creating” more of a cryptocurrency

• Cryptocurrencies are digital (think of it like a file)

• Most cryptocurrencies have a limited number of coins available
  • Each type of coin determines that number differently
Cryptocurrency

Each cryptocurrency is slightly different but they generally have these traits:

- Transactions are irreversible
- People using it are anonymous
- Transactions are quickly verified and are globally accessible
- Secure
- Limited supply
Wait…

• If cryptocurrencies are a file, what stops someone from using the same file twice?
• This is called the **double spending problem**
  • How do you know the cryptocurrency being sent to you right now hasn’t already been given to someone else?
• That’s where the blockchain comes in

[Wait…](http://www.dummies.com/personal-finance/what-is-cryptocurrency/)
How are transactions tamper proof?

- Records of who has done what with the currency is publicly available and distributed across different computers
  - These records are called **blocks**
- A block can contain hundreds of transactions
- Each block is linked to another block
  - The whole thing is called a **blockchain**
How are transactions tamper proof?

- Each block has a fancy math equation run on it to distill its contents down to 64 characters
  - This is called hashing and part of how cryptocurrencies use encryption!
- These 64 characters are included in the next block
- You can’t alter a block without altering all the blocks that come after it
  - This solves the double spending problem
What happens in a transaction?

- When someone wants to sell/exchange their currency, the network is scanned to see if that person owns the rights to it.
  - This is where the public/private key comes in!

- Since all the transactions are public knowledge, it’s a matter of having computers do the work.

- If the person does own the right to it, the transaction can continue. A new block is created and added to the end of the last block.
How is a transaction verified?

- **Mining** is the process of verifying and adding transactions to the blockchain.
- Each block contains an answer to some computationally expensive task.
- Transactions are verified by having miners use their computer find the solution to the current block they are looking at.
How is a transaction verified?

- The first to finish adds the block to the blockchain and is rewarded with some of the cryptocurrency.
- Everyone who has a copy of the blockchain will have their copy synced and updated.
How is a transaction verified?

- Each type of cryptocurrency has different standards for how hard it is to mine something.
  - E.g., Bitcoin uses the standard that it should take an average of 10 mins to mine something.
How is all this information stored?

- Trees!

- To handle all this data, a special type of tree is used (Merkle trees)
Real World Impact

- Prices for computer hardware (especially graphics cards) are going up because of the need for more computing power to mine cryptocurrencies
- Bitcoin mining used more electricity than all of Ireland
- Streaming sites have been found to insert code that make people who use the site mine for them

Learning Goals

• Understand what cloud computing is
• Understand the pros and cons of cloud computing
• Understand how cloud computing creates a backbone for cryptocurrency
• Describe how cryptocurrency works at a high level