Introduction to blockchain

- What is a blockchain
- Proof of Work
- Smart Contracts

- Jason Corless
- jcorless@uvic.ca

What is a blockchain?

- An append only *distributed ledger* that groups *transactions* into *blocks*

- A *block* is a collection of zero or more *transactions*

- A *transaction* changes the state of the ledger, often by sending “money” between participants

Internet “money”

- Most blockchains introduce a currency that is used to transact on the blockchain
- For example:
  - the Bitcoin blockchain has bitcoin (XBT)
  - the Ethereum blockchain has Ether (ETH)
- Blockchain currencies can be traded for Fiat currencies (CAD, USD, EUR) at exchanges

Proof of Work

- A mechanism for securing the blockchain and an incentive structure for rewarding participants that help with the security.
- The two largest blockchains are currently secured by Proof of Work
  - alternatives exist, but none have been proven at scale

Background: Hash Functions

- A *hash function* takes arbitrary input and produces a fixed size output

- "Easy" to compute forwards
- "Impossible" to compute backwards
- Changing a single bit in the input should change the computed hash

Proof of work example

- Follow along at

- https://emn178.github.io/online-tools/keccak_256.html

Proof of Work

- New “unconfirmed” transactions are broadcast by participants to the network
- *Miners* collect new transactions and group them into a block
- All miners are competing with each other to find the next block
- The network rewards the miner who finds the next block

Mining Rewards

- Ethereum targets a new block every 15 seconds and reward is 3 ETH:
  - March 2018: ~$3000 USD
  - July 2018: ~$1200 USD
  - December 2018: ~$330 USD
- Bitcoin targets a new block every 10 minutes and reward is 12.5 XBT
  - March 2018: ~$115,000 USD
  - July 2018: ~$76,000 USD
  - December 2018: ~$53,000 USD

Network Difficulty

- The network sets the difficulty based on how long it is taking to find a new block
  - Increase the difficulty if blocks are happening too fast
  - Decrease the difficulty if blocks are happening too slow
- Our “difficulty” will be the number of 0s at the start of our computed hash.
  - more 0s == more difficult

Proof of Work

- Once a miner finds a guess which results in a hash less than the current difficulty, it broadcasts the block to the network
  - block includes the miner's address, so they receive the reward
  - It is easy to confirm that the hash is valid
- The latest block is the least secure
  - best to wait "a few" more blocks to be sure
    - ~ 12 blocks for Ethereum
    - ~ 6 blocks for Bitcoin

Real world example

- Go to: http://www.ethstats.net
- At the time of writing the slides, there were:
  - 214,000,000,000,000 guesses EVERY SECOND
- An average GPU (GTX 1070) can perform:
  - 30,000,000 guesses every second
- ~ 8.5 million GPUs
- ~ $5 billion in hardware

Why is it secure?

- The network always chooses the longest chain as the valid chain
- An attacker needs to present a longer chain than the “real” chain
- Technically possible if an attacker controls 51% or more of the mining hardware
  - invest $2.5 billion and you can attack Ethereum

Ethereum changed computing

- Prior to Ethereum, most blockchains only included transactions or limited “scripts”
- Ethereum allows turing-complete code to be stored and executed on the blockchain
- Because a blockchain is immutable, code deployed to the network cannot be changed.
  - this solves some problems, but introduces others

Simple Example

- I will sell your music on my website and take 10% of the income, you receive the other 90%
  - Do you trust me? [HINT: You shouldn't]
- Existing payment methods rely on so called "payment processors" that handle credit cards, bank cards and other methods
  - payment processors take up to 30% of the transaction

Audits, chargebacks

- When a customer buys your music, the money goes to me
  - you have to audit me to confirm that I'm not cheating
  - stolen credit cards result in you losing money
  - fees for payment processors reduce your profit

Smart Contracts

- Ethereum allows functions to accept ETH:

```
function buySong (uint32 songId)
 payable {
  yourAddress += msg.value * 0.9
  myAddress += msg.value * 0.1
  }
```

- You get your money the instant it is received*
- Above is pseudo-code, a LOT more detail and care is required.

Want to learn more?

- This is a fun tutorial to learn how Ethereum and smart contracts work:
- https://cryptozombies.io/

History

- March 2018 – CSC 106
- July 2018 – CSC 106