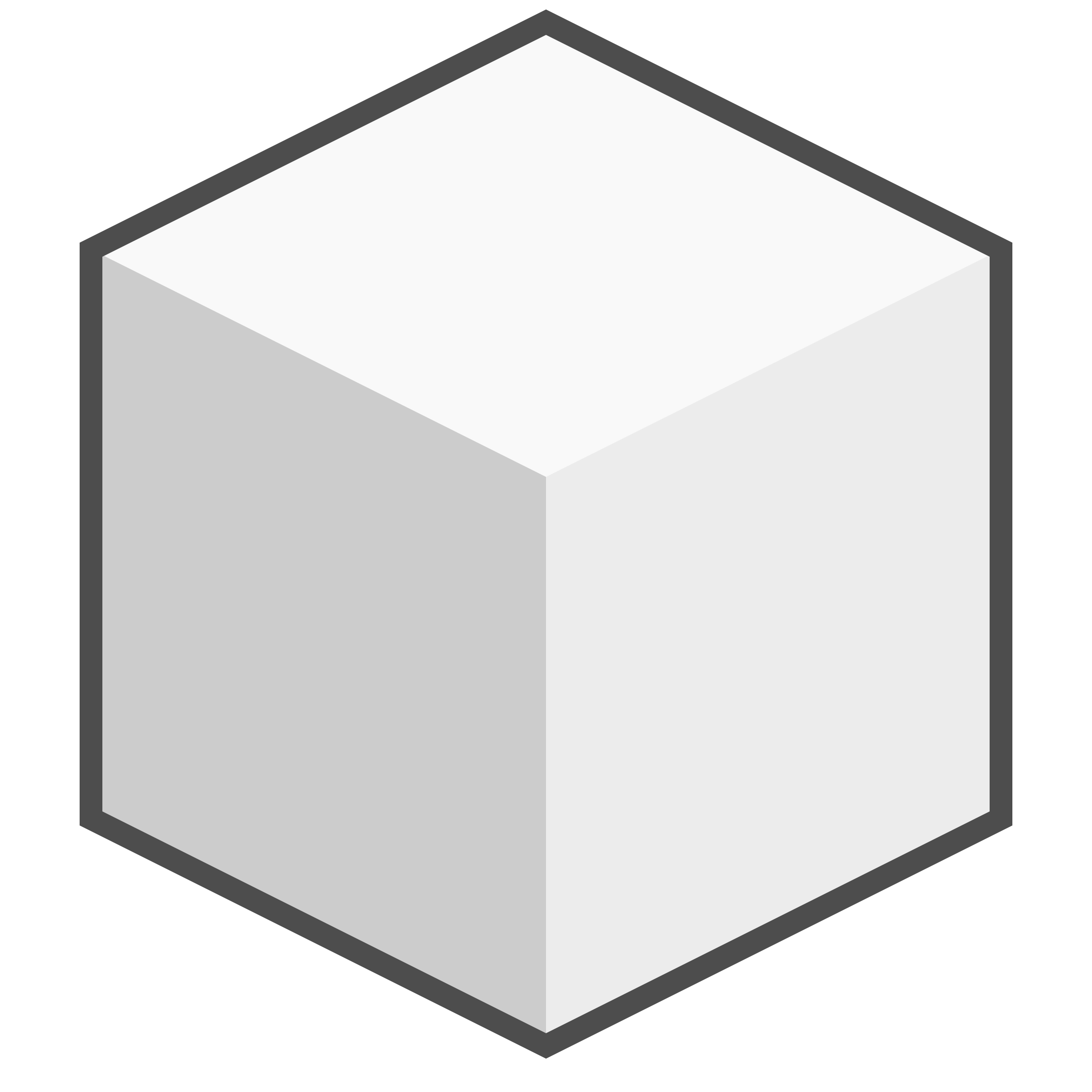
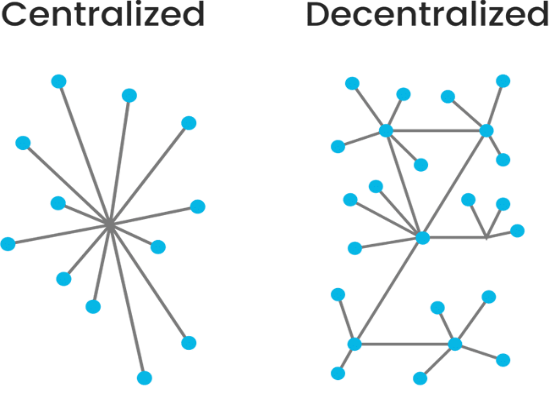
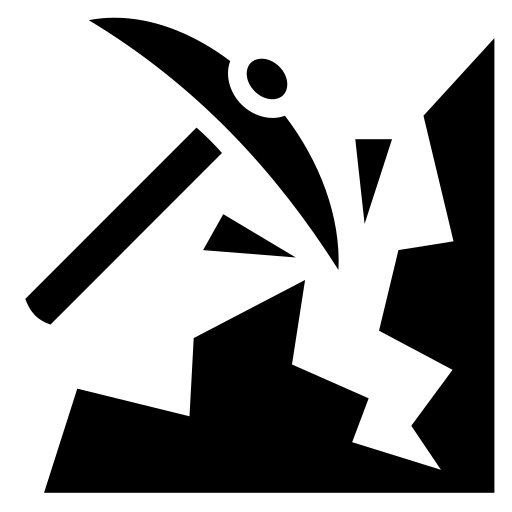
Research and Notes on Everything Blockchain

Kira Boettcher - 7.2.2018

**What is a Blockchain?**  
 Blockchain is a virtual type of data storage. Most commonly used to record transactions, creating a digital ledger, in chronological order. The ‘Block’ refers to the way the data is stored, while ‘Chain’ refers to the way that each block is connected with it’s previous block.

**Blocks Contain** :  
 - Data: Such as details on a transactions, each detailed with a sender,   
 receiver, and currency transferred.   
.  
 - Hash: A unique identifier of a block and it's contents. As content changes,   
 the hash changes as well.   
.  
 - Previous Hash: Contains the previous block's hash identifier, connecting   
 and creating a 'chain' of 'blocks'

**Decentralized Network :**  
 Blockchains are not stored in a singular place, such as like at a data center. It is instead stored for the people, by the people, in a peer-to-peer network. When one decides to participate in the blockchain, their computer gets a copy of the entire chain and they become a node. When a cryptocurrency transaction are made and validated by miners, the nodes broadcasts their information to other known nodes, and the update continues to expand across the entire network, making   
the block final, preventing tampering, as everyone has a copy   
of the chain.

**Mining :** ‘Mining’ refers to the process of adding new blocks to the chain. This is done by:

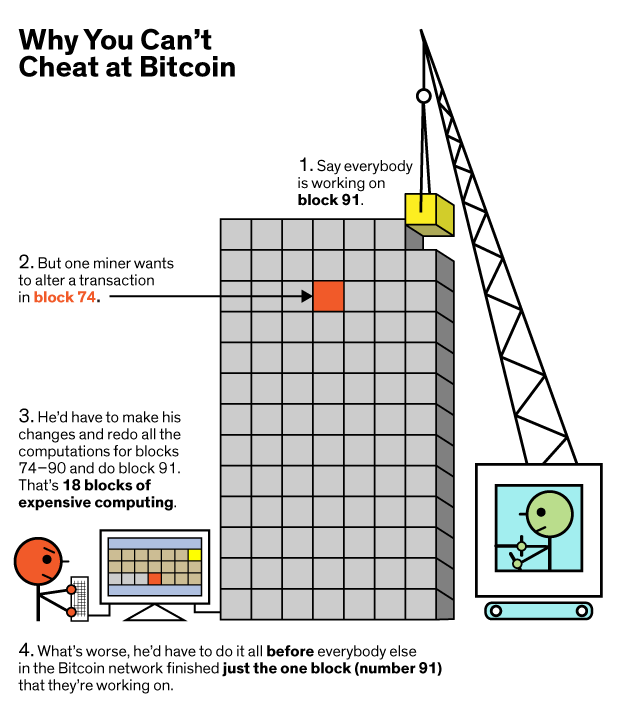
1. Proof of Work computations - This is the process of validating pending   
 data, such as pending cryptocurrency transactions between users.

2. Validated data is then grouped and stored into a singular block (which   
 is roughly about 1,000 - 2,500 transactions) with a limit of 1 MB size.

3. After the block is made, the miner(s) have to randomly guess a   
 number (a nonce) that’d satisfy a complex mathematical equation,   
 which’ll create a hash number to commit the block into the chain.

This process is very computationally laborious and expensive, so miners get rewarded the system’s cryptocurrency for their contribution. The system remains fair by regulating the amount of blocks made within a time period with changing the difficulty of the puzzle. The system also pays out in correlation to the amount of work your system preformed to compute the answer (IE. Miners can’t commit a block with a single transaction and expect a good pay-out. )



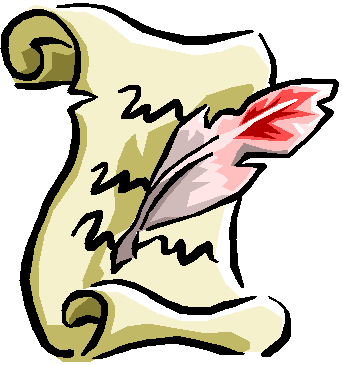
**Security** :  
 Saving data onto a blockchain is arguable the most secure way of saving data digitally. The complexity of regulations and the widespread decentralized network create a very safe, and difficult space for tampering, by outside or inside hacking   
(IE. external and internal theft). Examples of the security measures are:

* **Decentralized Network:** Blockchain is not located in singular place. Recorded and copied into the system (node) of each user.
* **Hashing:** Block hashes change when content changes, which affects subsequent blocks, that would need to be re-hashed as well. This makes changing just a singular block impossible.
* **Proof-of-Work (PoW):** Data validation through Miner’s computations. This system makes changing data even more laborious, as the ‘hacker’ has to compute the new hashes for each preceding block, which takes time and expensive computing power (<- See picture to left).  
    *Or*
* **Proof-of-Stake (PoS):** Data validation through a singular miner being chosen to validate pending data based upon amount of currency owned. -> No competition, more resourceful.

**Types of Data :**

Most common type of data blockchains track is digital currency and transactions (Often described as a digital ledger). Blockchain can be expanded though to store nearly any type of data.

**- Cryptocurrency**  
 Also known as digital currency or sometimes tokens. This is currency paid out to block miners after they successfully create a block. It’s found and stored within the blockchain, and is accessible by having its public and private keys.  
 **- Transactions**   
 Transactions are the transference of cryptocurrency for goods or service. This is where the public and private keys of a currency are used. Public keys are given to verify digital signature’s to a transaction. Private keys are exclusive to the owner of the specific token(s), and are what enables access to said token(s), and are used to authenticate a transaction via a encrypted digital signature, that could only be verified by the public key.

**- Smart Contracts**  
 Also known as self executing contracts/blockchain contracts/digital contracts. These are programs that enforce programmed rules and penalties in a transaction or agreement. The idea is to cut out a ‘middle-man’, or a person that’d connect you to a product, and instead have the transaction automated. This system ensures both ‘consumers’ and ‘commerce’ are guaranteed what they agreed upon.

Resources (most used/pulled from)

Blockchain Explained: <https://www.fool.com/investing/2018/01/10/the-basics-of-blockchain-technology-explained-in-p.aspx>   
Bitcoin Mining: <https://www.coindesk.com/information/how-bitcoin-mining-works/>   
PoW/PoS: <https://medium.com/loom-network/understanding-blockchain-fundamentals-part-2-proof-of-work-proof-of-stake-b6ae907c7edb>   
Public/Private Keys: <https://www.globalsign.com/en/ssl-information-center/what-is-public-key-cryptography/>   
Smart Contracts: <https://blockgeeks.com/guides/smart-contracts/>