* Getting Technical: What is blockchain?
  + A distributed, public ledger.
  + Stores multiple copies of every transaction
    - This prevents attackers from modifying the transaction.
    - Eg: There are 10 copies of same transaction. Attacker finds out one of the transactions located and will attack that specific value. Blockchain will recognize that there were changes we’ve made and run and algorithm that will say all the current transactions regarding that single transaction and it will update the attack in modified transaction to the previous value that prevents the transaction from being falsified.
  + A history of every single transaction!
    - Since every transaction is recorded in the blockchain we actually have a way of tracing back to see every transactions that has been made. This actually provides the system with a lot of transparency in that every single transaction made can be tracked back to the person that made the changes.
  + “Miners” maintain and build the ledger.
* What is Ethereum?
  + Invented by Vitalik Buterin in 2013
  + Goes beyond a store of value to building “smart” contracts
    - The idea behind bitcoin is straight exchange of value. I send you bitcoin, you send me bitcoin. But nowadays we deal with money in a different way like contracts. Eg: you want to send money to me in exchange of my car, my house, or any rent. This is impossible in bitcoin. So Ethereum takes a different route called smart contracts
    - Smart contracts are pieces of code that can be written and added to the blockchain. Similar to token in that they are immutable. Once the code is in the blockchain their history can’t be changed
    - When you send money using Ethereum through smart contracts, it initiates the smart contract and smart contract will do something in exchange. Smart contract can create new tokens and tokens can represent things in real life with value , for instance, the car or the house.
  + Allows users to perform complex operations with their money
* What is DAO?
  + Decentralized Autonomous Organization
    - The idea is that you create an organization on the blockchain that isn’t controlled by any single person so the coders that created the DAO don’t actually control the DAO. The DAO makes decisions based on bylaws that are set in stone at the very beginning and they are immutable. So, once the DAO has been created it follows those rules and uses those rules to organize itself.
    - It was meant to control and organize the development of etherium. They wanted to create an organization that would manage it and would be responsible for hiring people that built out the blockchain.
  + A self organizing entity, that makes decisions by following simple by-laws
  + Simply code. Not controlled by its creators
  + Stored in the Blockchain, as a big Smart Contract
* ETHICAL ISSUE #1: THE DAO. How does it work?
  + Contractors submit Proposals to the DAO.
  + Curators select proposals to enact and fund.
    - Curators are people that are responsible for enforcing the by laws and they are the ones that choose which proposals are accepted and when they accept this proposal, the contractor is added tot a list of people who can receive Ethereum from the DAO for the work that they do.
  + Contractors selected are paid in Ether, by the DAO
  + Investors exchange Ether for DAO Tokens
  + Each DAO Token gives Holders a vote as shareholders which enables them to hire or fire the curators.
* BUT THEN DAO GOT HACKED
  + A bug in the code left an exploit
    - Small issue that allowed infinite recursion to occur in very specific scenario
    - A person could send a command to transfer funds and if they can get the same function to call split down the function that is being called again it would infinitely occur and transfer effectively as much money as you want in one location.
    - One guy figured it out and he effectively stole the entirety of the balance of the DAO. 55 million dollars.
    - The maintainers of the Ethereum did the mortal sin in the blockchain. They just forked the blockchain. That is you split the blockchain in a certain point in history. i.e. you decide that at this point all the transactions after that are invalid. The way they did was you just have to get the miners to agree in consensus that this is the new reality that these transaction never occurred.
    - The problem was that not all the miners agreed with that. In fact close to 40% of the miners didn’t agree with that. Because the intention behind cryptocurrency is an immutable blockchain and immutable ledger that can never be re-written except only for the miners to do this.And this set a precedent that a blockchain could be hard forked and that had never happened before. So, people were afraid of that and also didn’t want that to be the case. So, they insisted on keeping the DAO where it was and giving that money back to the hacker.
    - The easiest way to prevent that is to not create doubts or to ensure that the DAOs are secured. The real issue when they made the original DAO was that they got very ambitious. The entire code base was massive and it was really hard to maintain especially since once a contract is out there it’s immutable so they couldn’t update it, say for they could create a new entity of it on a blockchain but it’s hard to actually update the DAO because of the entire idea behind it like the DAO is not controlled by its creator, it’s controlled by itself and its community so to rewrite scripts on the DAO it has to be approved. So, inherently, the DAOs in the future if they are ever created need to be simple .
  + Ironically, the bug had been fixed, but the patch was not live
  + Once single hacker was able to siphon all the funds
  + 8 million Ether(Approximately 10% of all Ether at the time) stolen
* WHO WAS AFFECTED
  + The DAO Token Holders
  + Everyone who owned Ether
  + The Hacker
  + ETF
  + DAO contract authors
  + Contractors
  + The Miners
* Who is ethically responsible for the hack? What about the loss in currency following the hack?
  + The Ethereum Foundation
    - Chose to hard fork the blockchain causing the market to crash
  + DAO Contributors
    - Who wrote the faulty code
  + The hacker
    - Who stole the money
  + Miners
    - Who opted to continue along with old blockchain and forced the hard fork to cause a different value.
  + DAO contributors are most responsible for the incident. If you look at it from the perspective of utilitarianism, they did write the code and they may have intented well but they resulted in a bug that caused the actual hack to be able to be caused in the first place. If they had followed their responsibility and kept the project simple before developing extra rules, they might have prevented this entire thing from occurring.
  + Ethereum foundation was responsible for the reduction in currency. They clearly intended well but once again following the theory of utilitarianism they forced a fork in the blockchain breaking their own rules. This actually resulted in a loss of more money than was actually stolen by the hacker. This choice affected not just DAO contributors who had already lost their money but also everbody in the Ethereum network including those who had no intention of or support for the DAO
  + Looking at it from Locke’s perspective in that the governmet control should be restricted to that of protecting the rights of citizens by forking the blockchain they actually for went the positive rights of the citizen and in order to secure the funds for the DAO contributors they actually forced the entirety of community to lose their money.
  + It’s a very split argument. There is no clear person that is a hundred percent responsible for this. The blame can be shared across multiple people: hackers and the DAO in general.
* DISCUSSION (2/3)
  + Each smart contract is supposed to be a contract
  + Does this mean that the hacker was simply following the contract?
    - I think he had ill intent, he clearly wanted the money for himself. But at the same time, everybody should have been following the DAO a lot more carefully. In the end, it’s probably about more up to the DAO to make sure that their code was up to par.
    - The hacker knew that he was taking something that was allotted for somebody else. But he’s following the rule and that’s perfectly fine. According the ---- theory, even though you’re following the rules if it’s wrong, it’s wrong.
    - Looking at it from perspective of Utilitiranism, he did take advantage of the smart contracts. As a result, he found insecurities in the DAO and forced the community as a whole to look at what they were attempting to do. Prior to this, they had a lot of trust that smart contract would always operate as they expected and since there is a written word component to each contract, it’s hard for people to recognize that they do also have to consider the code and since the code was so complex that it allowed for something like this to occur, the 55 million dollars that he stole can be considered a sort of finder’s fee for having exposed this crack, this bug.
* DISUCSSION (3/3)
  + Since the collapse of the original DAO, there have been several attempts to create new DAOs.
  + As a computer scientists, how might we improve future DAO implementations?
    - Make sure that the code is very well tested. Given a larger time frame for testing the DAO
    - Always be aware that there could be errors in the code.
    - Focus on standard best practices such as the single responsibility principle . The idea being a piece of code should realistically only do one thing. The DAO attempted to do a lot and even thought it could have been tested better, it did ultimately attempt to do a lot. The code should be made simpler.
    - In the future, DAO may prefer to focus exclusively on payments and accepting payments as opposed to focusing so much on allowing universal contributions.
    - Ethereum organization should have had more oversight over the DAO and not have trusted things to go right all the time.
* Can you explain more about blockchain? Poker chips or cash
* If there is no one controlling the cryptocurrency, then who is keeping track and updating the blockchain? Miners