**Lecture 7 Notes**

Slide 4

Transactions

* A transaction is when two parties exchange something. Humans have been looking for bet- ter and safer ways to transact with one another since the birth of trade. When our ancestors wanted something that someone else had, they had to be in possession of something their counterparty needed.
* For example, if they have some apples, and the other party has some fish then they may have been able to trade some of their apples for the other party’s fish. But that did not always work. As I’m sure, you can imagine this type of trade was difficult as the two parties had to have something the other wanted at the same moment. Human ingenuity in trying to solve this difficult trade and transaction problem led to the creation of money.

**The birth of money**

* The first forms of money were goods that everyone wanted all the time and did not de- teriorate over time like apples and fish. They were products like salt and beautiful shells.
* Thousands of years ago Greek slave traders often bartered salt for slaves. And you can still see remnants of these early transactions and money terminology. Expressions like “they are not worth their salt” and the word slave both come from this time. Salt is still used as money by nomads in Africa today.
* The next big evolution in terms of money was trusting a third party to hold your funds and protect it from thieves. The Knights Templar were a famous group that set up a network of banks. Their system allowed pilgrims to deposit assets in their home countries and withdraw funds in the Holy Land.
* It is believed that they used cryptography to ensure that no one cheated on the amount of funds they would request in their new location. Since the days of the Knights Templar, even more, elaborate schemes have been developed to protect people’s assets. The transfer of value is a vulnerable time for disintermediation and holding value of any kind leaves you open to theft.

Slide 5

**Trading promises**

* The notes that were used by pilgrims have evolved significantly. The note itself represented the option to retrieve value. Whoever held the note was in effect the owner of the deposited value that the third party promised to keep safe. This is known as a bearer instrument.
* Soon people figured out that they could directly trade notes for goods and services. The abstraction came because both parties agreed that the third party holding the funds was good for the promise and that the note represented a way for the holder to get the gold or silver that it represented if they wished.
* Money took another big leap when the United States in 1973 officially ended the gold standard. Many other industrialized nations did as well. Instead of banks holding a tangible asset like gold or silver, they facilitated an intangible asset.
* The intangible asset that modern money represents is the future work of people. Each currency is tied to the forthcoming production of a nation or coalition of countries like the EU. This means that currencies no longer have a fixed rate of exchange for gold. Our modern system of banking has floating rates that reflect public sentiment, war and trade agreements.

The idea of money has taken another exciting twist. Some countries like Switzerland and Australia recognize cryptocurrency as a currency. When you distill down why Cryptocurrencies have value, it is because they can be provably be exchanged from one individual to another. The blockchain secures the proof of exchange, and the blockchain’s consensus algorithm enforces the transfer rules. Cryptocurrencies are not backed by gold or the future output of a country like other currencies. Owning cryptocurrency means that you are in possession of a private key that allows you to send it to another public address.

Slide 6

**The public witness**

Another old human concept blockchain technology utilizes is the “public witness”. This is possibly the oldest “technology” humans created. A public witness is a person that isattesting to a fact or event. Their testimony allows others to believe that something took place. A witness is spreading their personal knowledge, so more people know and believe it.

* The first public witness may have occurred around an ancient campfire as a hunter retold an epic battle to their friends and family. You can see the evidence of these stories painted on the walls of caves across the world. Telling stories and sharing information is deeply human.

Slide 7

A public witness serves two main functions.

* It spreads knowledge to more than one individual and allows history to become persistent. The more people who know a story, the more persistent it becomes.
* The second purpose that a public witness provides is that it allows the individual to make a choice about the information they have been given. Each individual’s social norms influence that choice, for example, do they remember the history, do they pass on the information to more people, or do they take action?

Slide 8

Computers that witness

* Since their creation computers have been developed to do the work that once was only possible by the human mind. They have allowed us to replace countless numbers of once highly paid and skilled workers, such as the code breakers from World War II.
* Now networks of computers are doing what was only possible through groups of humans working cooperatively.
* Blockchain technology is an extension of the public witness concept in that it spreads knowledge, encourages persistence of information, and allows each individual node to make a choice with the information that they are given.
* Each node on a blockchain network is witnessing information. It is attesting to its accuracy and truthfulness later, much like how court houses, libraries and archives are places where people store information to reference at another point in time. Blockchains are a digital archive.
* Each node holds an independent archive of all the transactions that have occurred on its blockchain network. A node hears a “history” and then “chooses” what to do based on the rules of that blockchain.

Every blockchain creates standard rules for how to treat new information. The majority of nodes agrees to these rules and operates under them, but each node has a choice and some- times nodes break the rules or disagree. When only a few nodes disagree on the history of a blockchain, they are ignored.

However, when a large enough group of nodes no longer agree to the same rules, they will break off and start an independent blockchain. This is called a “hard fork”. Hard forking means there has been a radical modification to the protocol. The protocol is the set of rules that the majority of nodes agree to follow. Hard forks can make previously invalid blocks or transactions valid. This means that hard forks can, in effect, reverse transactions by changing the rules and rewriting the history of that blockchain.