IM 450-01 Issues in IM: *Blockchain, Cryptocurrency, NFTs*

Spring 2022

Class 7— February 10

-Blockchain summary and conclusion

(and a crypto-sneak peek)

Blockchain tech: What did you learn?

- How blockchain has been around for a lot longer than I was led to believe. I've learned Nakamoto's original paper was published in 2008 and that it is now just finally coming to fruition. Technology depends on the time and integration to become known and at least somewhat popular.
- In fact, "In 1991, Stuart Haber and W. Scott Stornetta invented the blockchain. Yes, 17 years before the release of the Bitcoin paper, the main idea behind cryptographically linking blocks in an append-only data structure was published in an academic paper. . . Haber and Stornetta's paper proposed calculating hash values of documents and saving them with a timestamp. The records are linked up in a data structure by including hashes of previous records' certificates. . . Whoever wrote the original Bitcoin paper did not "steal" this idea. In fact, Haber and Stornetta are cited three times in the Bitcoin paper."
- https://blocktelegraph.io/blockchain-before-bitcoin-history/
- 2021—1991--"30 year rule" from IM 355 and Blockchain is NOT YET fully developed/implemented/diffused.

Blockchain tech: What did you learn?

- An important takeaway from this section is that blockchain is not a technology that is only reserved for cryptocurrency. There are companies and even other industries that are already on their way to incorporating blockchain into business practices and even potential solutions to global issues.
- I was surprised to learn about the cryptography that helps secure Blockchains. I didn't know that the code in each block would change with even the smallest adjustments to trades.

Blockchain tech: What did you learn?

About potential drawbacks of blockchains, and how they could be misused or simply abused to give some people an edge over others. I still tend to view blockchains as being more secure and transparent than other forms of ledger or technology, and I believe it’s because the potential drawbacks are so rarely discussed. While some of these drawbacks relate to users lacking proper knowledge on the subject, or Ill-defined requirements, some of them are technical issues and can present serious problems if overlooked. For example, while be it unlikely, it’s possible for a large amount of users to pool together their computing power and essentially hijack control of the system through numbers. Or say, for a hacker to make use of enough computing power from several users and hijack additional control themselves. It really puts into perspective that new issues can arise from the solutions of old problems.

Blockchain tech: What did you learn?

- **I didn't know that Blockchains could be used for non-physical trades. My previous beliefs were that Blockchains were used only for cryptocurrency, and I was surprised to hear that transactions for real world items can be executed, validated, and recorded through blockchains.**
- **The possible environmental impact of this technology is very troubling. This could easily scale into a larger limiting factor in the future.**

Q&A? Blockchain

Final reading assignments on blockchain

11	8 am	Level 3 Material 3	
13	5 pm		Level 1 Material 1

Pre-Orientation to Cryptocurrencies (CCs) Stipulations

- **Most CCs are built and run on blockchain-tech (we will talk about the exceptions later).**
  - **As such, most CCs share the advantages and disadvantages of blockchain-tech.**
  - **CCs are the most ubiquitous current and recent use-cases for blockchain-tech.**
- **CCs consists of two basic processes:**
  - **Mining: the math-cryptographic work that accomplishes creating the basic CC units of value. The US government “mints and/or prints” money. CC processes mines units of value;**
  - **Speculative financial markets: units of CC value are traded in ways that are similar to money (banks and lenders), stocks (stock market), and commodities (corn, beef, etc.).**

Pre-Orientation to Cryptocurrencies (CCs)
BITCOIN

BITCOIN
(BTCUSD)

- A DIGITAL LEDGER OF TRANSACTIONS
    - The first miner to solve a complex, mathematical, cryptographic problem gets to add a set of transactions to the Bitcoin Blockchain.
    - That miner is paid for solving/adding with a portion of BTCUSD.
- Because the total # of Bitcoin are set (21M, a limit not yet reached, now=18.2m), “scarcity” raises value.
- Increased #s of minors = smaller mining rewards in fractional portions of Bitcoin= (from 50 to <6.5)

Pre-Orientation to Cryptocurrencies (CCs)

ETHEREUM

BITCOIN (BTCUSD)

A DIGITAL LEDGER OF TRANSACTIONS

ETHEREUM (ETH)

- **A DIGITAL LEDGER OF TRANSACTIONS**
- **“SMART CONTRACTS”**
- **EXECUTABLES**

- **A DIGITAL LEDGER OF TRANSACTIONS**
- **MAY CONTAIN “SMART CONTRACTS”**
  - **Your X ETH purchase is recorded on the ledger but also includes the contract term that “If the price/value of your ETH falls below 50% of investment, the seller will void the transaction and return your money”**
- **MAY CONTAIN EXECUTABLES**
  - **Your X ETH purchase is recorded on the ledger but also includes the executable that “If the price/value of your ETH falls below 50% of investment, your ETH will “split” by purchasing ETH X2 (so you’ll own twice as much). The original seller does nothing; the ETH itself executes the IF/THEN statement.**
- **The first miner to solve a complex, mathematical, cryptographic problem gets to add a set of transactions to the Ethereum Blockchain.**
- **That miner is paid for solving/adding with a portion of ETH.**
- **Because the total # of Ether are set (a limit not yet reached), “scarcity” raises value.**
- **Increased #s of minors = smaller mining rewards (fractional portions of ETH)**

Pre-Orientation to Cryptocurrencies (CCs)
STABLECOINS

BITCOIN (BTC)

A DIGITAL LEDGER OF TRANSACTIONS

ETHEREUM (ETH)

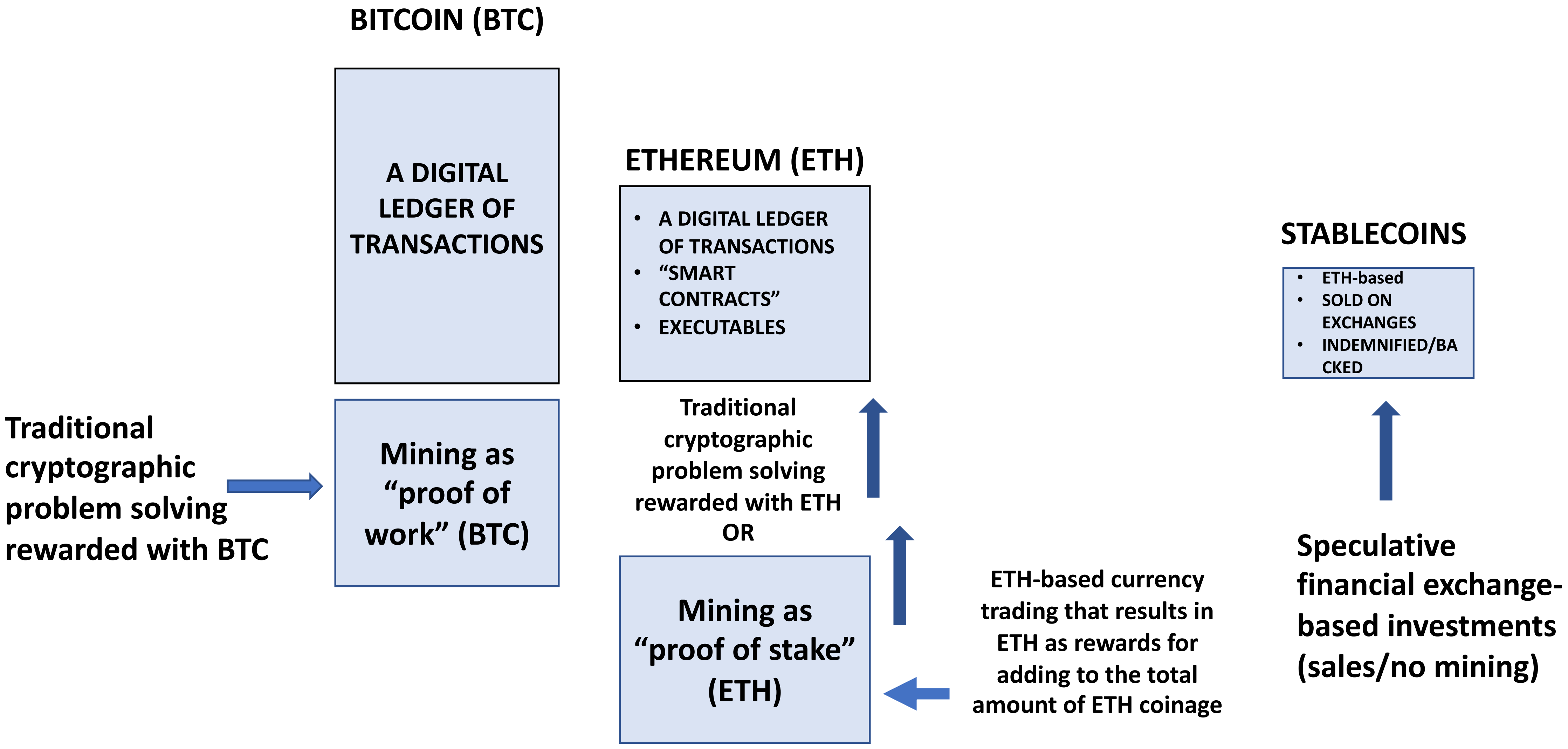
- **A DIGITAL LEDGER OF TRANSACTIONS**
- **“SMART CONTRACTS”**
- **EXECUTABLES**

STABLECOINS

- **ETH-based**
- **SOLD ON EXCHANGES**
- **INDEMNIFIED/BACKED**

- **CURRENTLY BASED ON ETHEREUM (Bitcoin stablecoin systems are developing)**
- **SOLD ON EXCHANGES (generally not mined directly although COULD BE given as mining rewards)**
- **“BACKED” BY COLLATERAL PROVIDED BY THE EXCHANGE THAT ISSUES THE STABLECOIN**
  - **Generally with the currency of the host country (say, USD)**
  - **COULD BE ”backed” by holdings of cryptocurrency, but this defeats the purpose of stablecoins and makes such an item less stable.**
  - **The “backing” makes stablecoins less volatile investments.**
    - **Much less risk than non-backed currencies;**
    - **Much lower potential returns than non-backed currencies;**
    - **Are the most direct “targets” for regulators because the “backing” might be a form of traditional ”security” that is regulated In a given country.**

Pre-Orientation to Cryptocurrencies (CCs)
MAKING AND MOVING



BITCOIN (BTC)

A DIGITAL LEDGER OF TRANSACTIONS

Traditional cryptographic problem solving rewarded with BTC

Mining as "proof of work" (BTC)

ETHEREUM (ETH)

- A DIGITAL LEDGER OF TRANSACTIONS
- "SMART CONTRACTS"
- EXECUTABLES

Traditional cryptographic problem solving rewarded with ETH

OR

Mining as "proof of stake" (ETH)

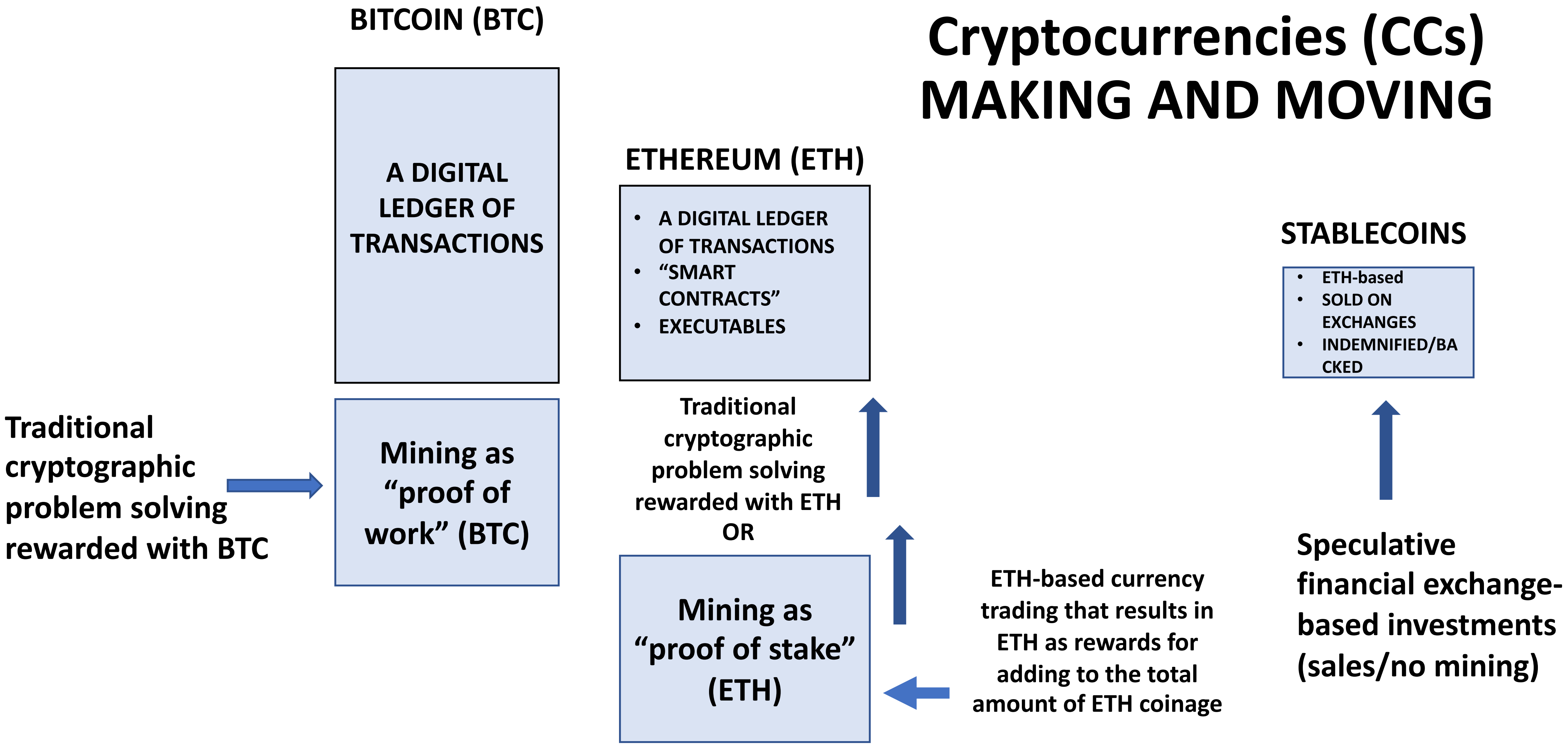
ETH-based currency trading that results in ETH as rewards for adding to the total amount of ETH coinage

STABLECOINS

- ETH-based
- SOLD ON EXCHANGES
- INDEMNIFIED/BACKED

Speculative financial exchange-based investments (sales/no mining)

Pre-Orientation to Cryptocurrencies (CCs) MAKING AND MOVING



BITCOIN (BTC)

A DIGITAL LEDGER OF TRANSACTIONS

Mining as "proof of work" (BTC)

Traditional cryptographic problem solving rewarded with BTC

ETHEREUM (ETH)

- A DIGITAL LEDGER OF TRANSACTIONS
- "SMART CONTRACTS"
- EXECUTABLES

Traditional cryptographic problem solving rewarded with ETH OR

Mining as "proof of stake" (ETH)

ETH-based currency trading that results in ETH as rewards for adding to the total amount of ETH coinage

STABLECOINS

- ETH-based
- SOLD ON EXCHANGES
- INDEMNIFIED/BACKED

Speculative financial exchange-based investments (sales/no mining)

Cryptocurrency Exchanges:

Buy/Sell the Underlying CC
Divide/Subdivide the Underlying CC
"Mint" coinage representing fractional portions of CCs

Hopefully, the Exchange rightly owned the underlying CC
Exchanges often don't work directly on the underlying blockchain so are open to attack/hacking/fraud.

Have a great weekend: Next week CRYPTO