LECTURE NOTES

Bitcoins

1. What is Bitcoin?

- Is one of many crypto-currencies
    - Currency: (1) common means of exchange, (2) store of value, (3) unit of account
    - Crypto: from cryptography applied to a digital currency
    - Transactions are done *peer-to-peer* with no intermediaries
    - Instead of taking 1USD from my wallet and putting into your wallet, I take 1B from my digital wallet and transfer it to your digital wallet
    - Problem? How to avoid a "copy and paste" of Bitcoins as we can do with different digital files (word, excel, pdf, etc.)?
        - What defines Bitcoin is the particular solution to this problem

2. Demand

- Why demand Bitcoins?
- Be careful: money demand is demand to hoard money, not just to make an exchange and then acquire another currency (i.e. USD).
    - Is there demand for Bitcoins, or demand for easier and cheaper transactions?
- Bitcoin has a demand to perform transactions
- Bitcoin is a technological improvement for peer-to-peer transactions
    - No need for an intermediary
    - Banks, and the Federal Reserve, are studying the possibility of applying a Bitcoin technology/rule (more on this below) to reduce transaction costs

3. Supply

- Supply of Bitcoins is pre-defined by the "Bitcoin rule" or what would be the "Bitcoin constitution"
- Clearing transactions. How to avoid double use of money?
    - Transfer of money across bank account are centrally managed (by the same bank if the two accounts are in the same bank, or by the Federal Reserves if it is across different banks)
- But Bitcoin is a decentralized system. How to avoid the double use of money?
    - The block chain (this is Bitcoin's innovation)
    - There is one ledger that tracks all the historical transactions done with any Bitcoin
    - One user A transfers Bitcoins to user B, the computers logged into the, let's call it, "Bitcoin core" need to verify that the history of transactions in the Bitcoin transferred coincide with the history in the ledger
    - Computers that verify the authenticity of a Bitcoin are called miners
    - To do this requires to solve a cryptographic problem (think of a very complicated numerical problem)
        - Example: Calculate the number *pi* or *n* up to the 1,000 decimal, or see how fast you can calculated 1,000 decimals in the number *pi* or *n* (or any known irrational number)
    - How are Bitcoins created?
        - If you use your computer or server to verify the Bitcoin authenticity, and if you are the first to do so, then you're rewarded with a number of Bitcoins
        - The complexity of the problem to solve automatically adjusts to the number of "miners" logged and to the computational power in the "Bitcoin core" such that the evolution of Bitcoins created follows the pre-defined path.


14-05-14 15:03:52] Stratum from pool 0 requested work update
14-05-14 15:03:52] Stratum from pool 0 requested work update
14-05-14 15:04:01] Accepted 04d5e33e ICA 0 Diff 52/8
14-05-14 15:04:10] Stratum from pool 0 requested work update
SAMSUNG
ViewHD

4. Bitcoin as money

- Is Bitcoin money?
    - (1) Generally accepted means of exchange?
        - Bitcoin has a similar capitalization than the currency of small countries, but has a much bigger geographical reach
    - (2) Store of value
        - Does its purchasing power oscillate too much?
        - If supply is fixed, then price volatility depends on demand instability
    - (3) Unit of account
        - Are prices denominated in Bitcoins?
- Assume its money. What type of money would Bitcoin be?
    - Is it a commodity (like gold or silver)?
    - Does it have a non-monetary use, like commodity money has?
    - Is its supply constrained by law (contingent) or a physical or natural condition (absolute)?

Scarcity	*Nonmonetary Use?*	**Yes**	**No**
	Absolute	Commodity	Synthetic Commodity
	Contingent	Coase Durable	Fiat

5. Can Bitcoin become money?

- Two challenges
    - (1) Network effects
    - (2) Natural monopoly
    - (3) Supply elasticity
- (1) Network effects
    - Money is a network good (it is not a public good)
    - The utility of network goods depend positively on the number of uses plugged into the networl
    - Examples: Fax, telephones, Facebook, etc.
    - The network advantage of using a certain money is that there is a large network of users that will accept it as a means of exchange
    - Why use Bitcoin if no one is accepting it?
    - If there's no nonmonetary use, where does its original value come from? (Mises's regression theorem)?
        - (1) Small group of users that value the "use of Bitcoin" (techs, crypto-anarcho-capitalists, etc.)
        - (2) Alternative use of computational power of servers
    - For Bitcoin to be become currency $U(B) > U(USD) + switching\ cost$
    - There's an increase if Bitcoin intermediaries
        - Example: Wordpress, your blog host, accepts Bitcoins. You pay the annual fee in Bitcoin "to" Wordpress. However, there is an intermediary between you and Wordpress that takes the Bitcoins and gives USD to Wordpress
- (2) Natural monopoly
    - The difficulty of the cryptographic problem to solve increases with time
    - This means that the cost to produce new Bitcoin increases
    - This means that the production of Bitcoin can become a natural monopoly
    - Then the block-chain (the ledger) becomes centralized and can be re-written by the natural monopolist without the double-check from other "miners"
    - The natural monopoly outcome defeats the purpose of the "Bitcoin constitution"

- (3) Supply elasticity
    - A good money is one that is neither too inelastic (deflation) nor too elastic (inflation)
    - Recall: $MV = Py$
    - Three types of money
        - Gold (G)
        - Fiat (F)
        - Bitcoin (B)
        - M (money) can be: *G*, *F*, or *B*
    - Then
        - $(Gm)V = PY$
        - $(Fm)V = PY$
        - $(Bm)V = PY$
    - In "free banking" *m* adjust automatically such that $\overline{MV} = constant\ per\ capita$
        - In gold standard, this happens through deposits and adverse clearing. Gold used as money is endogenous to the market (it depends on market forces)
        - In fiat currency systems, the central bank needs to adjust *F*. The supply of *F* is exogenous (it does not depend on market forces)
        - In Bitcoin there are no banks, therefore *m* =1. Then: $BV = PY$
            - Because *B* is predefined, it cannot adjust to changes in *V*
            - What if Bitcoin demand grows too fast (or too slow)
            - Potential solution, development of banks that would issue convertible banknotes to Bitcoins (a classic Bitcoin-standard rather than a classic gold standard)
            - But why use Banknotes, Bitcoins are already convenient enough