Introduction to blockchain and cryptocurrency

Logic of blockchain technologies

Roman Matkovskyy, Rennes School of Business

TRANSACTING IN CRYPTOCURRENCY (BITCOIN)

Bitcoin Transactions

- **A transaction tells the network that the owner of some bitcoin value has authorized the transfer of that value to another owner**.
- The **new owner can spend the bitcoin by creating another transaction** that authorizes transfer to another owner, and so on, in a chain of ownership.
- Transactions are like lines in a double-entry bookkeeping ledger.
- Each transaction contains one or more “inputs,” which are like debits against a bitcoin account.
- On the other side of the transaction, there are one or more “outputs,” which are like credits added to a bitcoin account.
- **The inputs and outputs (debits and credits) do not necessarily add up to the same amount**. Instead, **outputs add up to slightly less than inputs and the difference represents an implied transaction fee, which is a small payment collected by the miner who includes the transaction in the ledger**.

Transacting in Bitcoin

- First, you need a **wallet** (for instance using Blockchain.info, Coinbase,…)
  - Wallet – a place to store your bitcoin credentials: namely your private key
- Private key – a 256-bit number, expressed as a hexadecimal and generated using cryptography
  - E9873D79C6D87DC0FB6A5778633389F4453213303DA61F20BD67FC233AA3326
- When people complain that they have lost their bitcoins, it means they have lost their private keys

Transacting in Bitcoin

- Without the private key – one has no way to access crypto-currencies
- If someone has your private key, then you have given them your cryptocurrencies
- Your private key can generate your unique address (which is public)

Transacting in Bitcoin

- Ways to transact in Bitcoin
  - Third-party software (example, Coinbase),
    - Provides the wallet and the access to a bitcoin exchange
  - One can separately choose a wallet and an exchange
  - You can buy with cash using a bitcoin ATM

Transacting in Bitcoin

- Once you own cryptocurency, you can:
  - purchase goods or services from other users of bitcoin using third party software, or directly (the list who accept bitcoin is here: https://99bitcoins.com/bitcoin/who-accepts/)
  - trade bitcoin back to euros/dollars…
- Bitcoin can be considered as a currency, similar to any other.
- But Bitcoin is not:
  - a stock, which is a claim to ownership in a company
  - a treasury bill, which is a claim to the income of taxpayers
- **Unless people believe that it can eventually function as a medium of exchange, in some states of the world, or store of value, bitcoin (or other similar crypocurrencies) has no inherent value.**

Transacting in Bitcoin

- Might Bitcoin function someday as a generalized and global medium of exchange?
  - First, **we need to consider what is currency**

Money: Bank money

Bank money has several notable characteristics:

- **Holding and using money requires a bank account**.
- **Any monetary transaction implies a movement between bank accounts**.
  - It is identifiable/traceable thus it be monitored and regulated.
- **Money is a legal claim on an identifiable entity: the bank**.
  - It is a liability of the bank.
  - *A bank deposit gives the holder legal rights on the bank, and an (indirect) claim on its assets.*
- **Bank customers have the right to convert their deposit into banknotes, which are legal tender.**
  - The Central Bank issues the currency serving as a "base" for the system, giving it its legal status.
- **Bank money is a form of "private" money.**
  - It is therefore vulnerable to a loss of confidence in the issuing bank.
- **Bank money nonetheless benefits in many ways from public backing through deposit insurance and/ or access to Central Bank refinancing**.
- Fiats are **backed by the power of the sovereign**
- The fiat of the US/EU/… governments does extend:
  - to private businesses accepting dollars for payment
  - to all of the transactions (both legal and illegal)

Money: e-money

- **E-money is not a new form of money, but is instead one of the modern forms that bank money takes**.
- **E-money**, in its current forms, **is simply a way to access and move money deposited in bank accounts**.

Money: Crypto currencies

- Crypto currencies are fundamentally **different** from bank money/e-money.
- **They have no intrinsic value**, **are privately created, and are totally dematerialized and digital**.
  - They are **purely private currencies**, are **not legal tender**, and are **not convertible at par.**
  - They are **created and circulate independently of any bank**;
  - They **do not represent a claim on any person or legal entity**.
    - They are “outside money”
  - Typically, they have **no physical, financial, or legal backing** of any kind (stable coins are exceptions).
  - They are denominated in specific units of account, unrelated to existing currencies (e.g., a **satoshi** is the smallest unit of Bitcoin currency. 1 satoshi = 0.00000001 BTC)

What does make a currency to be a currency?

- **The self-fulfilling equilibrium**:
  - We agree to take euros or other fiats because we believe that everyone will take them.
- Rests on the following fundamentals:
  - In fiats we can pay taxes and discharge debt
  - The rule of law
- Thus: **what makes a currency a currency are the common beliefs of the individual users!**

Credit cards?

- Nearly all merchants accept credit cards (Visa, Mastercard, Discover, American Express)
  - It is costly for the merchants due to a fee
  - Average credit card processing fees: 1.3% to 3.5% + $0.10
  - By law, merchants are not allowed to offer a discount for cash
    - Overall, credit card business is very profitable for the credit card companies
- We, as customers, demand these cards, so merchants suffer if they do not accept them
- Overall, price discrimination is not allowed by merchants.

Cards as centralized intermediary

- Transactions are done in terms of fiats (euros/ dollars, etc)…
- The credit card companies keep track of accounts and verify the legitimacy of the transaction (thus, a centralized ledger is maintained)

Why Cryptocurrency?

- To minimize power of centralized intermediaries
- Philosophical reasons to dislike centralized intermediaries
- A need to hide from the centralized intermediary
- Avoid inflation and other macroeconomics issues