freeknowledgemission-list@meetup.com

Bitcoins and Cryptocurrency

OR…

freeknowledgemission-list@meetup.com

If only I had bought them when they were cheap…

And I would not be doing this PPT!

freeknowledgemission-list@meetup.com

- Bitcoins and other cryptocurrencies are designed after the process implemented by the unknown person called Satoshi Nakamoto.
- Satoshi Nakamoto has disappeared. He (?) created the first reference application.
- Proof-of-work (POW) solutions require an entity to solve a math problem to have a resource (such as sending an email).
  - Generally cryptocurrencies use HASHCASH like process for POW
  - HASHCASH was invented to allow for a “cost” for each email or like process.
  - Byzantine fault tolerance (BFT) solution not needed.
  - The problem is hard, but it is easy to validate the solution and the solution may involve the date and time stamp and thus can’t be pre-computed.
- For Bitcoins a new “block chain” is validated by a POW from peers in a network of blockchain or hyperledger.
  - This is mining. Unlike HASHCASH the POW is made more and more difficult by increasing the number of bits.
  - According to social media the Bitcoins difficulty is set to allow for about six Bitcoins to be mined an hour

freeknowledgemission-list@meetup.com

- Bitcoins and generally cryptocurrencies use a shared ledger that records all of the transactions.
- To store the current transactions a blockchain must be created. To create a blockchain a newly minted Bitcoin is used to “prove” the block.
- As the generation of Bitcoin is unpredictable it is very hard to “hack” the underlying blockchain. The monetization of Bitcoins creates a community of miners.
- The peer in the network of shared ledger copies that presents a new Bitcoin takes over the updating of the ledger. Thus it is impossible to guess which peer gets to update the ledger next.
- Corrupting the ledger at one peer generally means the other peers will ignore the corrupt peer unless by some means it gets the next Bitcoin and can store the new transactions in a new blockchain.

freeknowledgemission-list@meetup.com

Currency

Or How Money Works

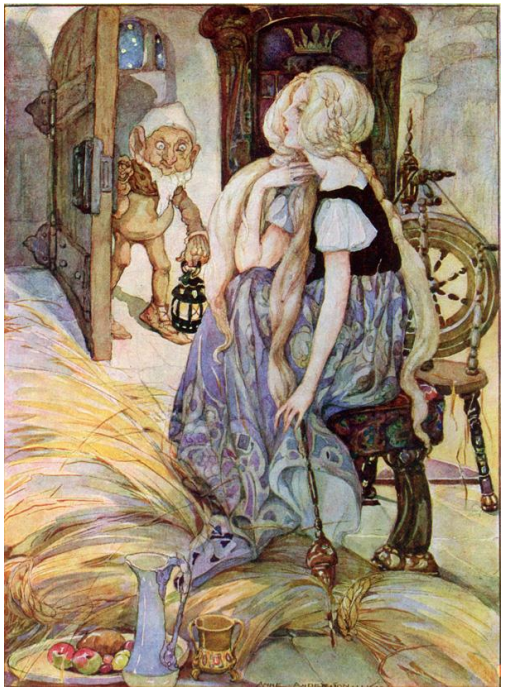
freeknowledgemission-list@meetup.com

- Currency is a medium of exchange and means to circulate.
- Currency can be fiat, that is the government or a central authority orders a value. Often this include make the currency “legal tender.” That is the currency must be accepts.
- US was on various fiat values. Famously the US moved from gold to silver to devalue the currency. The US left the gold standard in the “Nixon Shock” of 1971.
- Inflation generally exists in the US and is an accepted way of life. Everything is adjusted to inflation. Money gets worth less and we have more. Debt is usually available at an affordable price.
- Deflation exists in US when there is a financial melt-down. The recent Great Recession and the Great Depression starting in 1929 and lasting into World War 2. Money gets worth more and we have less of it. Debt is hard to get and is often at near zero interest.

freeknowledgemission-list@meetup.com

- Money, a form of currency, is liquid. It is accepted as payment. Actually it is against the law in most countries to refuse a local currency based payment.
- Illiquid forms of exchange: gold bars, silver bars, Old Master paintings, stamp collections, agriculture goods (grain, cows, copper, and so on), etc. That is the value of the item is based price that can be attained by selling it and this price can be different based on the moment (i.e. finding a buyer or “dumping” it to get whatever you can get for it).
- Bitcoins and crytocurrencies are illiquid—they are *not* legal tender, by definition.
- Cryptocurrencies are by definition deflationary.

freeknowledgemission-list@meetup.com



Futures

Or How to Turn Things into Cash

freeknowledgemission-list@meetup.com

- Futures are a legal agreement to buy or sell something at a predetermined price at a specified time in the future.
- The original use of futures contracts was to mitigate the risk of price or exchange rate movements by allowing parties to fix prices or rates in advance for future transactions.
- Thus if an exchange is created for a illiquid asset a futures allows prices to be known and values to be predicated in the future.
- Often a “future” requires only a percentage of ownership.
- The US and many other countries (UK has it own gold price, for example) have used futures and various versions of purchasing agreements to monetize risk and evaluate illiquid assets.
- Cryptocurrancies generally trade in an exchange using forms of futures.
- These are unregulated exchanges.

freeknowledgemission-list@meetup.com

- Exchanges charge for all transactions.
- Exchanges usually also get a small percentage of every transaction.
- Exchanges to be fair must (all of this is obvious):
  - Have many transactions. Thus evaluations are measureable any time.
  - Transactions must follow some order based on time. This can have some random components but must be clearly recorded.
  - Have large “customers” that buy outstanding orders so that prices do not go into a free-fall. This prevents shenanigans.
  - Not have large “customers” that are free to trade at any time with any amount. If it costs something then many shenanigans are prevented.
  - Have controls to stop free falls of prices during a “crisis of confidence.”
- Remember that most exchanges are immune from paying for errors and offer limited means of recompense when things wrong.
- And that an exchange needs a certain level of “churn” to make money.

freeknowledgemission-list@meetup.com

Cryptocurrency

Technology version of gold

freeknowledgemission-list@meetup.com

- Sold in exchanges.
- The peers in network are exchanges or are connected to the exchanges.
- The cryptocurrency is held on account in the exchanges.
- When you “mine” you turn over your solution to the exchange which then sends it to a peer.
  - Exchanges have been hacked and closed down for illegal activity
  - Kraken, an exchange, is offer zero fees this month to make up for problems
  - Ownership of Bitcoin and other cryptocurrency is managed through exchanges and this is where most of the losses have happened.
- The POW is NOT used for trading and thus there are reports in the press of “bots” schemes to increase prices.
- Cryptocurrencies:
  - Illiquid
  - Are managed by unregulated exchanges
  - The underlying technology (for those that use block-chains) is secure, but exchanges are another issue.

freeknowledgemission-list@meetup.com

- There are now multiple cryptocurrency many created, according to the press, by the Crypto Castle. Many fortunes created by Bitcoins have been used to create new cryptocurrencies.
- Litecoin (LTC) created in 2011 uses a different mining process and peer process than Bitcoin and is becoming more accepted (~$193)
- Ethereum (ETH) uses a distributed platform and uses smart contracts. It was created in 2015 (~$1050)
- Zcash (ZEC) is an open source block-chain with more security than Bitcoin created in 2016. (~$511)
- Dash offering untraceable transactions in 2014 but still using block-chain (~$852). Rebranded from “Darkcoins”
- Ripple (XRP) is not a block-chain and does not use mining (~$1.53)
- Bitcoin, the orginal, (~$12,400)

freeknowledgemission-list@meetup.com

Questions?