Udemy Certified Bitcoin Professional Course

Section 2: History of Money and Ledger-Based Economics

Centralised Ledgers

- ○ Are controlled by a single entity —> i.e your bank's statement
- ○ A Bank could theoretically take your money away from you without your consent (i.e cyprus during economic meltdown)
- ○ Another disadvantage of centralized ledger — theoretically a bank could shut down and lose your transactions
- ○ In a decentralized system a single party cannot game the system and harm other users
- ○ Bitcoin is on a decentralized ledger that is made possible via proof of work

Functions of currency

Functions:

1) Medium of Exchange: Helps make transactions happens, its the facilator. Eliminate the bartering.

2) Store of Value: Holds value over a sustained period in time

3) Unit of Account: provides a measure for the value of a product

Distributed Consensus

Consens: Collective Decision Making Process Between Many People over what is right and what is wrong

- In the case of the Bitcoin Blockchain it isn't poeple mking consensus its computers on the the Blockchain called nodes
- Mining is how Bitcoin solves distributed consensus
- Forks -- separate branch
- Bitcoin's distributed consensus is determined by its hash rate, which is the number of calculations performed on the network.
- If a small number of calculations are performed the network is more vulnerable to attacks

History of Bitcoin

- In 2007 Satoshi nakamoto started working on bitcoin
- October 31st 2008, bitcoin whitepaper was published
- January 2009, first bitcoin transaction to place between satoshi and hal finney
- In November 2010 Bitcoin's market cap exceed $1Million dollars
- June 2011, great Bubble of 2011 huge
- September 2012 Bitcoin Foundation lauched
- 2013 market cap 1billion dollars
- Look up bitcoin's history timeline.
- https://www.coindesk.com/live-blog-satoshi-nakamoto-revealed/
-

Price Derivation

- Bitcoin has value simply because of Supply and Demand
- Exchanges bring together buyers and sellers

Section 3: Basic Cryptography

Terms and Definitions

- PDF

Hash functions

- SHA 256 - reward in bitcoins for solving each hash
- Utilizing hashing

Symmetric and Asymmetric Encryption

- Asymetric - Utilizes a pair of keys. Public and private keys
- If you encrypt data with the public key only the person who has the corresponding private key can decrypt it.
- They are super secure
- Symmetric encryption: 1 key for both encryption and decryption operations
- Pros and cons.
- Symetric advandages: more efficient can handle large amounts of data, shorter keys
- Assymetric advantages: very good for digital signature use cases and can stay in perfect working condition for years
-

Digital Signatures

- Non reputible transactions
- Everyone can verify the transactions
- Bitcoin wallets have a private and public keys -- private key, creates public keys which then creates the Bitcoin addresses

Section 4: Bitcoin Basics

Community

- Roles: User, Advocate
- User - without users the ecosystem wouldn’t be as strong as it is today, if you have wallet youre a user
- Advocates - educators teach others
- Marketers - help to promote Bitcoin
- Faucet owner - sites where you earn bitcoin for ads
- Miners -- Homebase mining is no longer profitable but ASIC specific hardware
- Investing - Day trading, long term investing, can influence the price of bitcoin if they are moving large amounts of Bitcoin
- Education, adoption and core development of Bitcoin

Bitcoin Addresses and Keys

- **Each Private Key has a Public Key**
- **Public key can be calculated from private key**
- **Address is a form of the public key**
-

Bitcoin Transactions

1. Input - Bitcoin Address used to send Bitcoins
2. Amount - Number of Botcoins being sent
3. Output - Bitcoin Address of the Recipient

- Bitcoin transactions don't have receipts
- Bitcoins aren't real

Bitcoin Blockchain

- The Bitcoin Blockchain is A Public Ledger of All the Bitcoin Transaction that have ever taken place
- As such the blockchain is ever evolving
- Each Block is added to the Blockchain in chronological order
- Ie-- The Blockchain is all the transctions of your Bank since your bank's inception
- The Blockchain is decentralized so anything that happens on the network happens as a whole
- Example: If you understand Google Docs you can understand Blockchain

Bitcoin the Unit

- Bitcoin (caps) vs bitcoin (lowecase)
  - Bitcoin - payment system and Bitcoin Ecosystem.
  - Bitcoin - as a currency.
- BTC = one Bitcoin
- mBTC = Milli Bitcoin
- uBTC = Micro Bitcoin
- Satoshi

Bitcoin the Network, Bitcoin Improvement Protocols, Buying and Selling Bitcoin

- Decentralized peer to peer network, so if a node were to go down
- Routing: Validates and Pass on transaction sand blocks as well as discover and maintain connections to other nodes
- SPV - Simplified payment verification
- BIP: Bitcoin Improvement Proposal
- Developers make a proposal and miners vote on it
- Coinbase -- wallet an exchange
- Coinmama
- Selling via exchange sites
- Mt. Gox -- exchange liquidity issue
- Never keep your funds stored on exchanges

Bitcoin explorers

- Blockchain.info

UTXOs - Unspent Transaction Outputs - outputs of a transaction that aren't yet inputs of another transaction

Section 5: Mining

- **Blocks contain proof of work to be valid**
- **Anybody can be a Bitcoin miner**
- **Mining on your home computer. Mining can cause a lot of damage.**

Purpose and Function
Algorithm - *SHA256*

- Kilo hashes/sec
- Megahashes/sec
- Gigahashes/sec
- Terrahashes/sec
- Peta hashes/sec

Mining Pools
Mining Hardware
Security and Centralisation

Section 6: Wallets, Clients, and Key Management

- Hot wallet - in some way connected to the internet
- Cold wallet - Wallets that are strictly kept offline.
- Wallets vs. Clients
- Deterministic Wallets
- BIP38 - passphrase encrypted wallet
- BIP - Bitcoin Improvement proposal
- WIF - Wallet Import Format

Section 7: Bitcoin Commerce

- **P2p payments**
- **Bitcoin specific point of sale solutions**
- **Bitcoin Payment Processors**

Section 8:

Dictionary Of Bitcoin Related Terms

Section 3, Lecture 9

51% ATTACK

This could be described using the example of a ‘major shareholder’. Once a shareholder owns 51% of shares in a company they own it. In the bitcoin community, a 51% attack is a single miner or group having a controlling stake of the computing power in a cryptocurrency network.

This could enable them to issue transactions that could conflict with someone else’s, stop transactions going through, spend their currency multiple times over and prevent other miners from mining.

ADDRESS

A bitcoin address is the presence that allows you to send and receive transactions as part of the bitcoin network. It also acts as the public key to your bitcoins.

ALTCOIN

Altcoin is the name given to the group of ‘alternative’ cryptocurrencies separate to bitcoin. Examples of altcoins include Litecoin and Feathercoin.

AML

Bitcoin exchanges are subject to Anti-Money Laundering (AML) techniques. This ensures that all transactions on the network are being carried out by genuine traders and not those converting illegal funds.

ASIC

An Application Specific Integrated Circuit (ASIC) is designed specifically to process the SHA- 256 hashing equation used to mine bitcoins.

ASIC MINER

An Application Specific Integrated Circuit miner is the holy grail of bitcoin mining – able to calculate the SHA-256 equation far quicker than a CPU or GPU unit. ASIC miners are purpose- built and connect to the network via a wireless link or Ethernet connection.

BITCOIN INVESTMENT TRUST

A sort of bitcoin syndicate, the Bitcoin Investment Trust invests exclusively in this cryptocurrency, and uses secure protocols to keep them safe on behalf of members. This is one way to invest in bitcoin without purchasing the hardware required yourself.

BITCOIN PRICE INDEX (BPI)

The Bitcoin Price Index, devised by Coin Desk, shows the average bitcoin prices across the leading global currency exchanges.

BITCOIN WHITEPAPER

The bible of the bitcoin network, this whitepaper was written by the currency's 'founder', Satoshi Nakamoto, in 2008. It gives a comprehensive description of the bitcoin protocol, and is a good read for newbies and experienced bitcoin traders alike.

BITPAY

One of the payment channels that processes bitcoin transactions on behalf of merchants.

BITCOIN WHITE PAPER

The origins of bitcoin can be found in this paper that was posted on bitcoin.org back in 2008. The paper, titled ‘Bitcoin: A Peer-to-Peer Electronic Cash System’, described the peer-to-peer approach for generating ‘a system of electronic transactions without relying on trust’. This was the genesis of the cryptocurrency.

BITSTAMP

BitStamp is one of the fastest-growing bitcoin exchange platforms around.

BLOCK CHAIN

This records all of the individual bitcoin ‘blocks’ that have been mined since the inception of the currency. The chain is designed so that each block contains the ‘DNA’ of the one preceding it, which secures the chain against fraudulent mining activity.

BLOCK REWARD

A reward is given to each miner who completes a transaction block. It can take the form of coins or transaction fees – Bitcoin currently rewards 25 coins for each completed block. Once the threshold of blocks has been mined (which currently stands at 210,000 blocks) the reward is halved.

BTC

BTC is the abbreviated version of bitcoin, similar to USD and GBP in traditional currencies.

BUTTONWOOD

Buttonwood was a project designed to create a bitcoin exchange in New York’s Union Square. Named after the Buttonwood Agreement (upon which the New York Stock Exchange was formed). It was founded by bitcoin aficionado Josh Rossi.

CLIENT

This is the software program which connects a machine – whether a desktop computer, laptop or mobile device – to the bitcoin network. It may also be the home to your bitcoin wallet.

CONFIRMATION

A confirmation is the successful hashing of a bitcoin transaction into the block. It can take up to ten minutes, although larger transactions may require more than one confirmation, as more blocks need to be hashed and added to the block chain. Once another block is added to the chain the transaction will be confirmed again.

COLOURED COINS

The creation of coloured coins is a proposed new feature for bitcoin, and one which allow users to define their own attributes of the currency. The idea is that users could mark a bitcoin as a physical asset, which could then be traded as a token for other property.

CPU

This is the Central Processing Unit of a computer, and one that has been used in the past to mine bitcoin – before it was usurped by ASIC and GPU set-ups. CPU’s are still sometimes used to mine altcoins with less taxing hashing calculations.

COINBASE

CoinBase has two distinct meanings for the bitcoin community:

1. A name used for the input of a bitcoin’s transaction. Once a bitcoin has been mined, the reward is recorded as a transaction using this input data.

2. The name of a bitcoin wallet operator that offers payment processing for merchants, and acts as a ‘middle man’ in bitcoin exchanges.

COIN AGE

A coin’s age can be calculated by multiplying the currency amount by the period of time it’s been owned.

CRYPTOCURRENCY

A cryptocurrency is one that is deemed legal tender and based on mathematical formulas alone, rather than exchange rates.

CRYPTOGRAPHY

This is the name given to the process of using maths to create the codes used to conceal information. This is the basis of the mathematical equation inherent in bitcoin mining.

DDOS

DDoS stands for Distributed Denial of Service, and is a cyber-attack used to drain the resources of a target. This is done by sending small amounts of network traffic to tie up the target’s bandwidth – preventing it from providing its services to its clients. Bitcoin exchanges have been subject to sporadic DDoS attacks in the past.

DEFLATION

A deflation is experienced when the price of something decreases over time. This happens when the supply outweighs demand, or where there is only a finite amount of currency around.

DIFFICULTY

Each cryptocurrency has a difficulty ‘rating’, which highlights how difficult it is to hash a new block. The lower the number, the harder it is to produce a hash value that fits the block.

Difficulty is fluid and can change based on the amount of computing power in the network. So if large numbers of people left the network its difficulty would decrease. If a currency grows in popularity then its difficulty increases as computing power expands.

DOUBLE SPENDING

This is the immoral act of spending the same bitcoins twice. The user completes a transaction using their bitcoins and then makes a second trade from someone else using the same coins. The user must then convince the network that only one transaction has taken place by hashing it in a block. This is why zero-confirmation transactions are risky.

DUST TRANSACTION

This is a transaction that takes up space in the block chain but is ultimately worth very little. The developers of bitcoin are taking steps to minimise the amount of dust transactions that take place by introducing a minimum transaction amount.

ECDSA

ECDSA stands for Elliptic Curve Digital Signature Algorithm, and is the formula in the Bitcoin protocol used to sign transactions.

ESCROW

An escrow is a type of online wallet that holds funds securely to protect them during a transaction. It is used where two parties cannot exchange bitcoins in public, and want the added reassurance that their currency cannot be ‘stolen’ digitally.

EXCHANGE

An exchange is where users can come together and swap different cryptocurrencies. A bitcoin exchange will generally see its users swap bitcoin for traditional ‘fiat’ currencies.

FAUCET

A faucet is the method of mining a pre-defined number of coins when launching a new cryptocurrency, and then giving these away in order to kick-start interest.

FEATHERCOIN

A popular altcoin based on the Scrypt algorithm, and one that is thus suitable for CPU and GPU rigs.

FIAT CURRENCY

A Fiat currency is another name for money used across the world that has a value inferred by its owner. This is commonly used in money laundering and illegal activities.

FINCEN

This is the Financial Crimes Enforcement Network, a US Treasury Department agency created to impose regulations on bitcoin exchanges.

FORK

When one set of miners starts hashing a different set of transaction blocks it is known as a ‘fork’. This can be a malicious tactic or undertaken accidentally. It can even be a deliberate ploy where the bitcoin development team introduces a new version of the client. A fork is considered successful if it goes on to become the longer version of the chain.

FPGA

A Field Programmable Gate Array is another form of processing chip that can be tailored to bitcoin mining. As these are sold in larger numbers ‘off the shelf’ and then re-configured after sale, they are usually far cheaper to buy than ASIC chips, although they are less effective.

FREICOIN

Another type of cryptocurrency created by Silvio Gessell, and founded on the principle of being inflation-free.

GENESIS BLOCK

The original block in a chain.

GIGAHASHES/SEC

This is the measurement that determines how quickly your machine can mine – it is the number of hashtag attempts possible per second, measures in a billion hashes (a Gigahash).

GPU

This is a graphical processing unit, as found in your standard PC graphics card. As a GPU is designed specifically to render polygons in pixel-heavy computer games, they are also perfect for the calculations required in cryptocurrency mining.

HASH

A hash is the mathematical process required in bitcoin mining. It is complex – to protect the sanctity of the currency – and hard to decipher and alter the output.

HASH RATE

The number of hash calculations that can be performed per second. This generally dictates how successful a miner is likely to be.

INFLATION

The opposite of deflation: as the value of money drops, the price of goods and services increases exponentially. This gives consumers less purchasing power, so there’s more motivation to spend a currency quicker.

INPUT

This is where a bitcoin transaction starts, and will be denoted by a bitcoin address. That is unless it is a generation transaction of a newly-mined bitcoin.

KILOHASHES/SEC

The number of hashes calculated per second in thousands of hashes (a Kilohash).

KYC

This is Know Your Client, a regulation that forces financial institutions to thoroughly vet the people they do business with to ensure they are legit.

LEVERAGE

Utilising leverage in foreign currency trading enables you to multiply your ‘real funds’ and achieve significant profit. Leverage can be used by a trader to essentially lend another person funds, which they can then earn back in commission.

LIBERTY RESERVE

A former giant of the digital currency processing world, Liberty Reserve was shut down by the US government after it was found to be money laundering.

LITECOIN

A type of altcoin that uses the Scrypt hashing formula.

LIQUIDITY

Liquidity ensures that the price of a good stays similar amongst all trades, ensuring that it is easy to buy and sell. If there’s a decent-sized community of traders then the price will remain stable and ‘liquid’. An illiquid market results in extreme price fluctuations, ad makes it harder to value a good.

MARGIN CALL

A margin call will take place when an exchange believes a trader does not have sufficient funds to cover their leveraged trades.

MEGAHASHES/SEC

The number of hashes possible per second measured in millions of hashes (a Megahash).

MARKET ORDER

A market order can be placed at an exchange when you want to buy or sell bitcoins instantly, and at the going market rate.

MBTC

A miniscule amount: one thousandth of a bitcoin (0.001 BTC).

MICRO-TRANSACTION

Paying a minute amount as part of a transaction online, these are hard to carry out under conventional payment systems. Imagine paying for a bag of crisps with your credit card.

MINING

Mining can be undertaken by anyone wanted to generate some new bitcoins for their wallet. You must solve cryptographic equations using the relevant algorithm.

MIXING SERVICE

The art of mixing in your bitcoins with another person’s, and then sending you back the same amount but with different inputs and outputs. This is a measure that helps protect the privacy of your account, as your currency cannot be traced back to you.

MT. GOX

This was perhaps the original bitcoin exchange back in 2010, and was certainly the most popular at the time. Based in Japan, Mt. Gox has subsequently gone into administration and closed.

NAMECOIN

Namecoin is a unique altcoin that provides an alternative to standard Domain Name Systems (DNS). Users can utilise .bit domains – only accessible via proxy servers – by paying with Namecoin.

NODE

Each computer that is connected to the bitcoin network and relays transactions to others is considered a node.

NONCE

A nonce is the random set of data used as an input when hashing a block. The nonce is the part that tries to fit the numerical parameters enforced by the difficulty of bitcoin. A different nonce is used for each attempt at hashing.

ORPHAN BLOCK

Any block that was part of a fork that has since been discarded is known as an orphan block. This is not part of the valid chain.

OTC EXCHANGE

A trader-to-trader exchange that doesn’t employ the services of a central mediator.

OUTPUT

The output is the destination address of a bitcoin transaction. There can often be more than one output for each transaction.

P2P

P2P, or Peer-to-Peer, interactions happen between two or more users in a network.

PAPER WALLET

This is a physical recognition of your public bitcoin addresses and their private keys. Your wallet can literally be a sheet of paper, and presents a safer way to store bitcoins that cannot be hacked or corrupted.

POOL

The collective name for a group of miners. These users will work together to mine a block, and then share the reward out accordingly. Mining pools increase your chances of successfully completing a block.

PP COIN

Sometimes known as peer coin or P2P coin, this is an altcoin that uses a ‘proof of stake’ calculation alongside proof of work.

PRE-MINING

A pre-mine is an operation carried out by a cryptocurrency’s founder prior to it ‘going live’.

PRIMECOIN

Primecoin uses a proof-of-work calculation to calculate prime numbers, and was founded by Sunny King.

PRIVATE KEY

The private key is crucial to keeping your bitcoins safe. This is unique to you, and only you should know your private key. It takes the form of a string that signs a digital communication once hashed with your public key.

PSP

The Payment Service Provider (PSP) offers processing services for merchants who accept bitcoin as a currency.

PUMP AND DUMP

This is a naughty tactic that artificially bumps up the price of an asset that has been purchased cheaply, with the aim of selling it on at a profit. The aggressive publicity causes others to buy it, which then of course forces up its value.

PROCESS NODE

Process nodes are present in nanometers, which are produced during the chip fabrication process. The smaller the node the more effective it is.

PROOF OF STAKE

The proof of stake is an alternative to proof of work, and calculates the amount of a currency you can mine based on your existing stake in it.

PROOF OF WORK

This calculation links mining ability to computer power. It takes a good amount of time and effort to hash a block successfully, and this is seen as a proof of work.

PUBLIC KEY

A public key is a bitcoin address, the information of which is accessible to all. When hashed with a private key it secures a digital communication.

QR CODE

A QR Code is a 2D graphic that contains a sequence of data. These codes can be scanned by mobile phones, and are used to encode bitcoin addresses and to facilitate physical bitcoin exchanges.

RIPPLE

Ripple is a payment network on which users can transfer any currency. Payments are on an ‘IOU’ basis and based on trust. The network is made up of nodes and gateways operated by an official authority.

SATOSHI

Satoshi, which is the name of the creator of bitcoin, is also the smallest denomination available at 0.00000001 BTC.

SATOSHI NAKAMOTO

Satoshi was the original creator of the Bitcoin Protocol back in 2008. He left the project in 2010.

SCAM COIN

Scamcoins use pump and dump and pre-mining together in order to make money for the creator. A Scamcoin is an altcoin developed purely for its profit-making potential.

SCRYPT

A proof of work system designed for altcoin miners, and one that is slightly-less complex and more forgiving than SHA-256; hence why altcoins utilising Scrypt are more widely mined by those with CPU and GPU set-ups.

SIGNATURE

When private and public keys are hashed together they create a digital signature, which proves which address a bitcoin transaction came from.

SILK ROAD

Silk Road was an online marketplace that generally traded cryptocurrencies for illicit purchases. It was closed down in 2013 after it owner, Ross Ulbricht, was arrested.

SEPA

This is the Single European Payments Area; which is an EU-led agreement to make transferring funds between member states easier – and thus make bitcoin exchanges go a bit smoother.

SHA-256

The standard cryptographic equation used in the proof of work system of mining bitcoin.

SPV

The Simplified Payment Verification enables users to verify their transactions without the need to download the significantly-sized full block chain. Instead, users simply download the block headers.

STALE

Once a bitcoin block has been hashed it becomes ‘stale’, and therefore can’t be hashed again. This name is also given to a hashing job in a mining pool that has already been finished.

TAINT

When a particular bitcoin is held by two closely-related addresses it is the taint analysis that determines the steps it took. This also identifies addresses known for trading stolen coins.

TERAHASHES/SEC

The number of hashes possible per second measured in a trillion hashes (a Terahash).

TESTNET

This is a block chain used solely for testing.

TOR

Bitcoin traders and miners who want to conceal their identity often use this anonymous routing protocol.

TRANSACTION BLOCK

The transaction block is the record of transactions which are then collated and hashed, and then added to the block chain.

TRANSACTION FEE

Some bitcoin transactions will have a small fee imposed on them when sent across the network. This fee is awarded to the miner who has successfully hashed the block to make the transaction a possibility.

UBTC

Another small denomination of bitcoin; a uBTC is a ‘microbitcoin’ (0.000001 BTC).

VANITY ADDRESS

A vanity address is the bitcoin answer to a personalised number plate. The string will have a desired patter, such as a recognisable name.

VIRGIN BITCOIN

These are bitcoins offered as a reward to miners that have yet to be spent.

VOLATILITY

The fluctuations in price of an asset such as bitcoin are described as its volatility.

WALLET

In much the same way as you might store cash in a wallet, so to do bitcoin owners in either an online or paper wallet. The wallet holds the keys to each bitcoin, keeping them safe and free from fraudulent activity.

WIRE TRANSFER

A wire transfer is the preferred method of sending and/or receiving currency from a bitcoin exchange. This transfer is conducted electronically, and can be secured to a bank account pretty much anywhere on the globe.

ZERO COIN

An anonymous protocol designed to keep the identities of cryptocurrency exchangers secret.

ZERO-CONFIRMATION TRANSACTION

Where a merchant agrees the sale of a product or service in return for a bitcoin payment, yet the transaction cannot yet be confirmed by a miner or added to the chain. This is where ‘double spending’ can become a problem.