Blockchain / Cryptocurrency:

Important Links:
What is Bitcoin? A Brief and Easy Guide:
https://blockchaininformer.com/bitcoin/what-is-bitcoin/

Can I mine Bitcoin?
https://bitsonline.com/money-mining-bitcoins/

SHA256 Hash Generator:
https://demoblockchain.org/hash

Block Hashes Demo:
https://demoblockchain.org/block

Blocks in a Blockchain Demo:
https://demoblockchain.org/blockchain

Distributed Blockchain Demo:
https://demoblockchain.org/distributed

Bitcoin Block Explorer:
https://btc.com/

Block Explorer (IMPORTANT):
https://www.blockchain.com/explorer

Bitcoin Cash Project Website:
https://www.bitcoincash.org/

Block Explorer for BCH:
https://blockchair.com/bitcoin-cash/blocks

Cryptocurrency Market Capitalization:
https://coinmarketcop.com/

How Will We Get to 21 Million Bitcoins?
https://bitsonline.com/21-million-bitcoin/

First Retail Bitcoin Purchase:
https://bitcointalk.org/index.php?topic=137.0

Bitcoin VR:
https://bitcoin-vr.github.io/

Fiat Leak:
https://fiatleak.com/

Realtime Bitcoin:
https://www.buybitcoinworldwide.com/how-many-bitcoin-users/

Bitcoin Globe:
https://blocks.wizb.it/

Bit Bonkers:
https://privacypros.io/tools/bitbonkers/

Bit Listen:
https://www.bitlisten.com/

Cold Storage:
https://bitsonline.com/cold-storage-bitcoin-hard-fork/

Is your Bitcoin wallet prepared for a hard-fork?:
https://bitsonline.com/bitcoin-wallet-ready-hard-fork-august/

How to Keep Your Bitcoins Safe With Two-Factor Authentication (2FA):
https://bitsonline.com/keep-bitcoins-safe-2fa/

Blockchain Informer:
https://blockchaininformer.com/

==

Blockchain:

Block in a Blockchain:

Has the following fields:

Block Number, Nonce (Number used once), Data, Prev (Hash of previous block), Hash (Valid hash has 4 leading 0's)

Key areas of support:

Value:

Enables a unique asset to be transferred over the Internet without a middle, centralized agent.

Trust:

Creates a permanent, secure and unalterable record of who owns what. Using advanced cryptography, "Information Integrity" is preserved.

Reliability:

Decentralized network structure ensures that there is no single point of failure which could bring the entire system down.

Cryptocurrency:

Type of digital asset which can be used to exchange value between parties.

It used cryptography to secure how it is transferred and to control the creation of new units of that currency.

ex: Bitcoin (pseudonymous and slow), Litecoin (Fast, 2min per block generation), Z-Cash (anonymous), Monero (Anonymous), Dash (Digital Cash)

Digital Token:

A digital token is a digital asset that can represent anything.

ex: Securities, loyalty points and real-world assets.

Audiocoin - Cryptocurrency for music industry

Golem - Shared economy computing power

VeChain - Track supply chain on blockchain

Steemit - Rewards platform for content publishers

CryptoKitties - Collect and breed digital cats

Initial Coin Offerings (ICO) / Initial Token Offerings:

Form of investment, you buy digital token for that project and indirectly invest in it.

Smart Contracts:

Disintermediation of any contractual obligations (like a bank third party when you buy a house)

Automation

Self-Executing and Immutable

Cost Reduction

Nick Zabbo (Father of Smart Contracts)

DAO & DAC:

Decentralized Autonomous Organization and Decentralized Automation Corporation

Collection of smart contracts

Distributed Networks on a blockchain

Possibilities:

- IoT
- Artificial Intelligence

Business Use Cases of Blockchain Beyond Bitcoin:

Supply chain management (Walmart + IBM)

Real estate impacts (Australian Banks ANZ and Westpac + IBM)

Insurance (Maersk + Microsoft)

Certificates of Authenticity (DNV + Deloitte)

Humanitarian Aid (UN)

Limitations of Blockchain Technology:

Early Stage

Lack of Awareness

Limited Available Technical talent

It is immutable (No reversals or modifications)

Key Management

Scalability

Time to process

Common Misconceptions:

Bitcoin in Anonymous (False)

Bitcoin is used to launder money

Blockchain is a better database
Blockchain is bitcoin
You need to buy a full bitcoin

Merkle Tree:

Mathematical Data Structure composed of hashes of different blocks of data, and which serves as a summary of all the transactions in a block
Also referred as Hash Tree
Named after Ralph Merkle
It is possible to create a blockchain without a Merkle Tree
Merkle Root is a Hash value that provides the summary of all the transactions. If anything is changed within a block, Markle Root Hash also
changes and hence it serves as an added layer of integrity

==

Bitcoin:

First transaction:

January 3rd, 2009

White Papers:

"Bitcoin: A peer-to-peer electronic cash system" by Satoshi Nakamoto
"New directions in cryptography" - 1976 Mutual Distributed Ledgers (MDL)
Ecash - 1983
Hashcash Proof-of-Work - 1997
b-money - 1997
Bitgold - 1998

4 Components:

Software, Cryptography, Hardware, Gaming Theory

How it works (High Level):

Bitcoin Software issues new Cryptography challenge approx. every 10 mins
Global Bitcoin miner community races to solve the challenge (Find a nonce that satisfies a valid hash)
A miner solves the crypto challenge first
The rest of the miner community verifies the validity of the new block mined
The new block of transaction is added to the Bitcoin blockchain
The winning miner earns a reward for solving the challenge first (Currently 6.25 bitcoin)

Key Concepts:

Disintermediated:

Act of removing the middleman. Peer to Peer money transfer and no third party (Bitcoin Network takes care of confirming and verifying)

Distributed:

The entire network runs on thousands of distributed computers that share the work. More reliable.

De-centralized:

No central control. Hence, no central point of failure.

Trustless:

No need to have a third party to certify and bring trust to the process of transaction. The blockchain enables the trust.

Done via "Distributed trustless Consensus". All the nodes have to agree that a transaction took place.

Bitcoin Forks, Transactions and Segregated Witness (SegWit):

Fork:

A fork takes place when a blockchain splits into two different paths forward.

Hard Fork:

Introduces a change that forces everyone to upgrade

Soft Fork:

Introduces change that is backwards compatible

Interesting Facts about Forks:

Forks on Bitcoin happen on a regular basis
Two or more miners solve a block at the same time - for a while there are extra chains
Eventually one of the chains wins over the other
Orphan block - Back to Mempool

SegWit Soft Fork:

UASF: User Activated Soft Fork
Locked in on 8th August 2017, at block #479,707
Official Activation on August 24th at block #481,824
Did not cause split in chain
Replaces Block Size Limit with Block Weight Limit
SegWit is a like new functionality on a Bitcoin block / new feature

What is SegWit?

Protocol Upgrade
Improves scalability of Bitcoin without increasing Block size
Addressed Transaction Malleability
Does not require upgrading to remain on the blockchain
Did not cause a split on the chain

Contents of a Bitcoin Transaction:

Input
Amount
Output
Digital Signature: Transactions must be digitally signed using the owner's private key

In a SegWit transaction:

Signature data (Witness) is "segregated" to an extended block
Frees up approx 60-63% data
It includes input and amount as part of this extracted digital signature

Future of Bitcoin:

Number of bitcoins currently in circulation: 18.373 million
Total number that can be mined: 21 million
Reward currently with every new block: 6 bitcoins
Transaction fee also received (Keeps it alive)

The Halving:

Algorithm by which every 210,000 blocks or approx. every 4 years, the Bitcoin reward for mining a block is halved.

Important Dates in Bitcoin:

Oct 31st, 2008: Bitcoin Whitepaper
Jan 3rd, 2009: Genesis Block
May 22nd, 2010: First Retail Purchase (2 Pizza's for 10,000 BTC)
Nov 28th, 2013: 1 BTC > $1000
Mar 2nd, 2017: 1 BTC > 1 Oz Gold

==

Bitcoin Cash:

New crypto-currency developed from a "Hard-fork" in the Bitcoin Blockchain
Increases block size to 8MB from 1MB limit prior to the fork
Also, de-centralized and run by a global community
August 1st, 2017 -> Hard Fork -> Block Number 478,558
ViaBTC pool produced a 1.9MB block, which is not valid in the legacy Bitcoin Network. Caused a split which is not Bitcoin Cash.
Bitcoin and Bitcoin Cash are NOT compatible

==