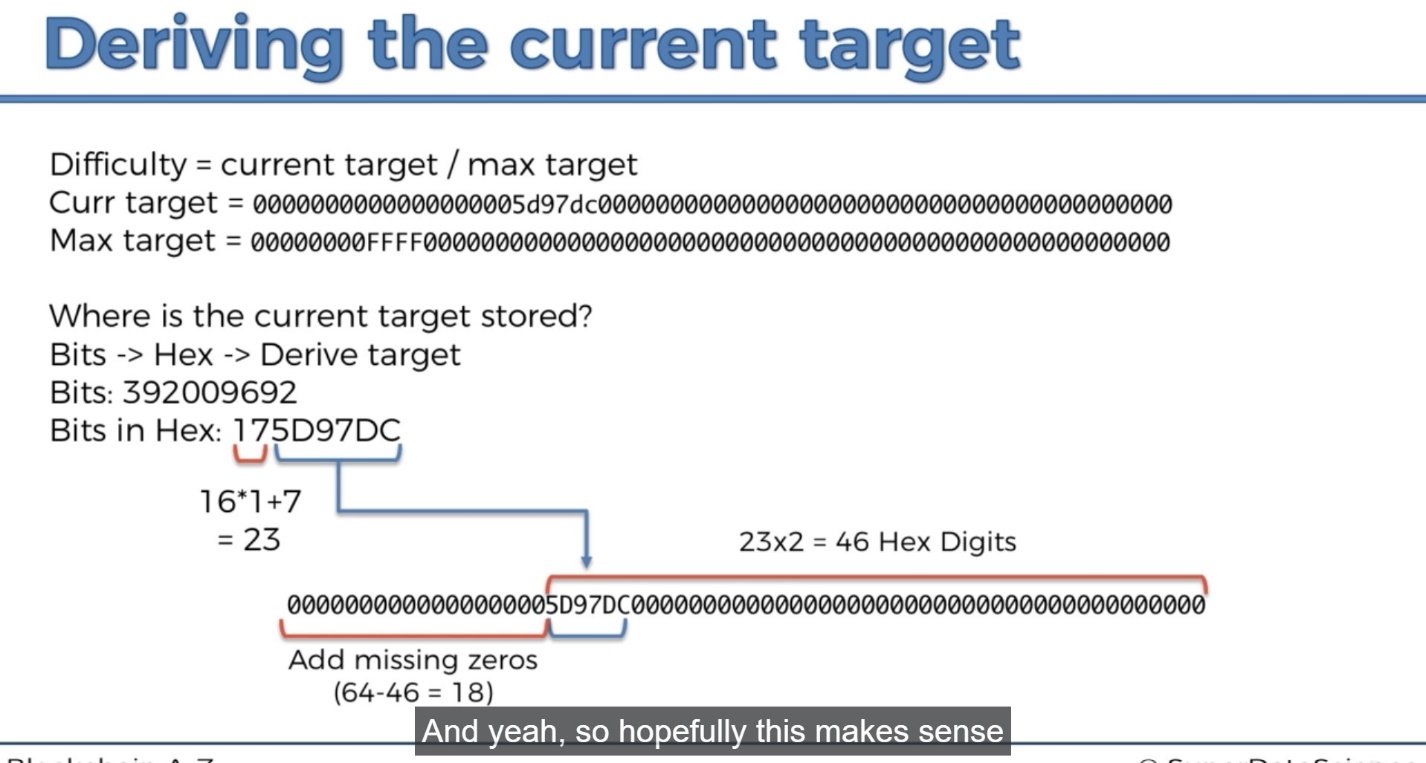
Blockchain🡪

* Blockchain intuition->
* Initial Concept: “How to time stamp a Document”->Haber Stornetta.
* Blocks(Data+previous hash->hash of block-64) which are cryptographically linked together.
* Genesius Block->First Block
* SHA256 Hash ->64 hash output(Hexa),  
  Hash Algorithms -> One-way, Deterministic, Fast, Avalanche Effect, Withstand collision.
* Immutable ledger -> Deed-ex, physical tracking of assets-ex, after block has previous hash.
* Distributed P2P Network-> change all blocks-issue, for restore data-issue,  
  every computer in the network has ledger, all synced and consensus occur and copied the consensus one, and if they must hack. they must hack more than 50% all at the same time.
* Mining-> Block(Multiple Transactions),  
  (BlockNumber+Data+PreviousHash+nonce(only once))->HashOfBlock,  
  vary the hash by nonce, Hash is a number->Decimal number encode to hexadecimal for shorter number, Lower Hash(Golden nonce) below the target, Cryptographic puzzle,
* Byzantine Fault Tolerance-> Consensus Algorithm(with Traitor), majority of information,  
  in case of 2 traitors-> no solution(more than 30%).
* Consensus Protocol(Prevent from -> Attackers, Competing Chains)->  
  (Proof of Work, Proof of stake)

Proof of Work-> Solution to cryptographic puzzle(hard to solve)  
(reward + transaction fee)  
every node check for new block.  
Two Block at the same time-> two chains -> Competing Chain-> Longest chain win(The part of network which has the highest hashing power-more than 50% has the),  
Orphaned Blocks -> left behind and no reward  
blockchain with money->Tokens and Coinbase

* Cryptocurrency intuition
* Technology(Blockchain), Protocol/coin(Bitcoin, ETH), Token()->from ICO
* Protocol: System in which people can transact with each other, Every Protocol has its coin.  
  No intermediaries in between.
* Monetary:   
  Halving-> Every 210,000(4 years) blocks the number of bitcoins reduced by 2x (21mill total), Block reward increase after the drop in bitcoin amount. Deflation in the currency  
  Block Frequency-> block came in how much time. 10min avg
* Mining Difficulty-> one leading zero reduce pool size by 16,   
  the probability of a golden nonce is extraordinarily low.  
  curr/max = Adjusted diff(every 2016 blocks in 2 weeks)->by node->no centralized
* Mining Pool-> for working against industrial asics(not double work), Reward to node on basis of hashing power  
  Asics -> for bitcoin.
* Nonce Range-> 32-bit number(4 billion), not enough,  
   it also has time stamp(Unix time stamp), and every second is calculated new hash with respect to time. New nonce also try from 0 to 4B.  
  100MH/s vs hash pools, General hash rate: 22 million Trillian hashes.
* Transactions in Blockchain-> from mempool(staging environment) attach to every node, max limit that can fit in a block is 1MB(2000 transactions), fees (by the users themselves),  
  the miners pick the transactions with the highest fees to include in the block.  
  They calculate the hash with time stamp, nonce value but if they checked the whole 4B nonce variations then they can change the block Configuration by changing transactions(with the lowest fee).  
  After that we can find configuration in which the nonce is not fully consumed under a 1 sec.  
  Pools have the algorithmic logic to pick the transactions for us(we directed our hashing power to a pool).  
  You should add some fee for transaction processing if not then it stuck in the mempool and returned in 72 hours-> go to BTC.com  
  Highest fees for more Demand.
* CPU<10MH/s, GPU<1GH/s, ASIC(relay on circuit)>1000GH/s, Cloud Mining->  
  No bitcoin mining on GPU.
* ETH hash is memory heavy, and different rate.
* Mempool(staging area for transaction) is both for node and miner, every block contains 2000 transactions. Mempools has thousands of transactions.  
  out of mempool and added to block. And added to every node.
* Orphaned Block-> 51 percent has the highest hash rate, and this is the longest chain, and the orphand block transactions released back to the mempool.
* Wait for 6 confirmations otherwise (included it self) Double spend problem.
* 51 percent attack-> 51 percent of the hash rate, this also has double spent problem, means the orphaned block transactions released to the mempool, this have the power to add which transaction to the new block.
* Target value-> from bits metric, to hex number,   
  
* Transactions in Blockchain
* Transactions and UTXO’s(Unspent transaction outputs)->   
  In Blockchain the transaction lives on and until another transaction builds off of the utxo from that transaction, In Cryptocurrency generally there is no account.
* In Blockchain transaction-> the input transaction amount should be same as the output(UTXO) amount. If it’s extra, then send me back the remaining amount.
* The new transaction is piggy backing on the old transaction.