**BLOCKCHAIN**

**What is blockchain?**

A blockchain is a continuously growing list of records,called blocks, which are linked and secured using cyptrography. -wikipedia

**Genesis block(1)**:

* For this prev has to be 0000000000000000000000000 64 hex chars.
* it never changes and is the starting block. Never add blocks to left,cascading only to right.

**Cryptographic hash**: SHA256 algorithm

Uses digits from 0 to 9 and a-f hexa decimal 64chars

**Five requirements for Hash algo:**

1.**Only One way** -> cant reconstruct from hash.i.e its just a pointer,a hacker cant get the doc that was hashed.

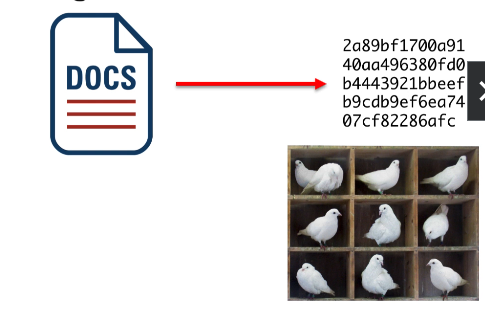
2. **Deterministic or reproducible**- > everytime u get same hash for same combination of content.

3. **Fast computation**

4.**Avalanche effect** -> if something is updated in intermediate fblock, every subsequent block after that prev hash and hash has to be changed as all are dependent on prev block starting from genesis block,even if it’s a punctuation marks extra,it completely changes hash.

5.**Must withstand collisions**(very imp concept behind Cryto Mining):->artificial collision is created to do mining by finding the hex pattern matching.

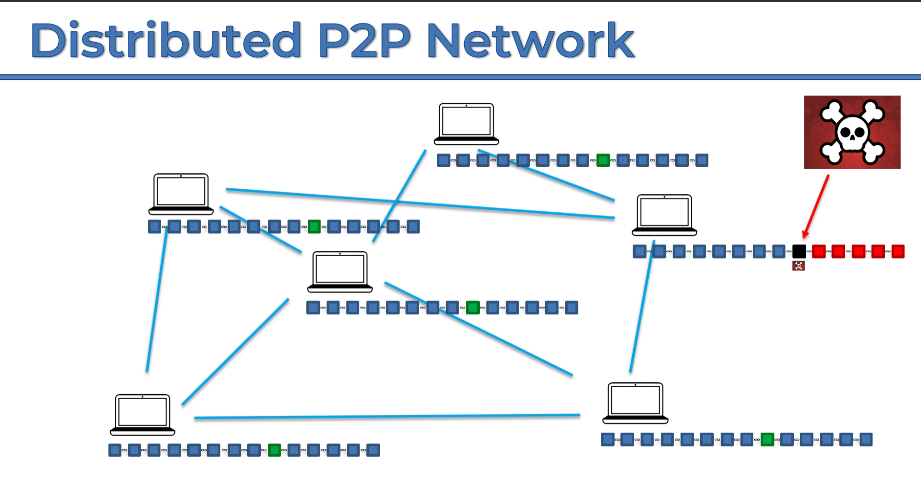
* Also referred as pigeon in the hole principle.if there is only 9 holes but 10 pigeons are there u have to fit in somehow so 2 pigeons in same hole is possible,so they there is chance that two docs or content might have same hashing.but its very rare case.



**Tool to visualise and practice hashing and blockchain working**:

<https://tools.superdatascience.com/blockchain/block>

**Distributed P2P network in Blockchain:**



* Initially our hashing is copied and maintained as pointer in distributed network ,so Lets say a hacker hacks the block that is marked as black in the pic, and he somehow updates the hashings in subsequent blocks that follows black.i.e red blocks.But as the other networks has the old hashing that is currently matching the node block hacked , so the network senses there is some threat and suddenly updates the hacked hash to old has,preventing hacker based on max node of network value.So hacking like this is impossible.
* Try P2P : <https://tools.superdatascience.com/blockchain/distributed>

**Bitcoin:**

* Every 4 yrs the value of mining got **halved** ,in 2020 it was 6.25$ by 2024 by 3.25$.Every transactions is transparent and borderless and no need for intermediaries like bank for safety

**Bitcoin Monetary policy (Mining):**

Same like current currency bitcoins is limited to avoid inflation.By 2140 ,it will be never ever more than 21Million bitcoins.Etherum block frequency is 15sec,averaged.

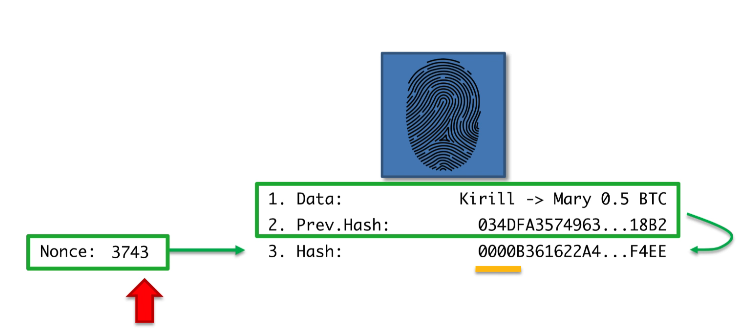
<https://hackernoon.com/this-time-is-different-part-2-what-bitcoin-really-is-ae58c69b3bf0>

**Nonce**: #number used only once -> purpose to manipulate the hash to get bitcoin reward.

* A random, unique number added to a block header before hashing.
* It's like a cryptographic puzzle that miners need to solve to validate a block and earn rewards.
* Data and prev hash cant be changed as its randomly gen,but nonce can be determined by miner by

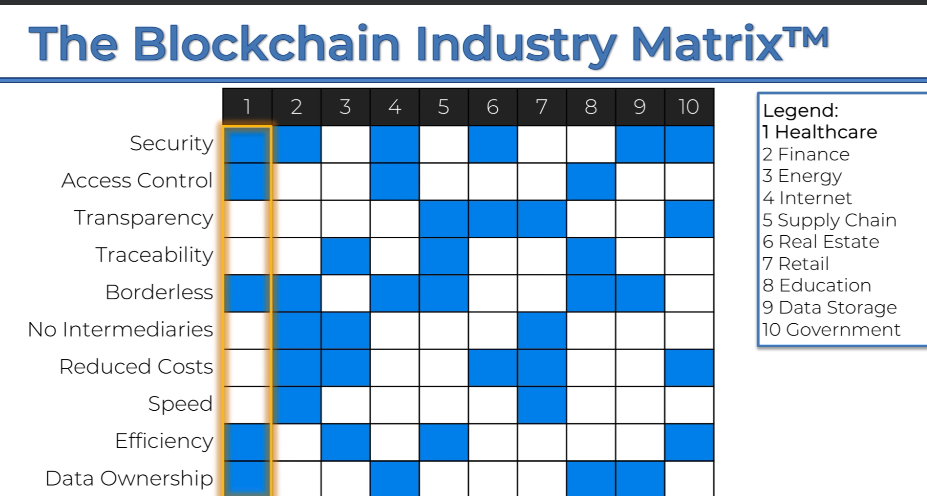
Continuous iterations of combinations to get hash like first 18 hex digits is 0, like 0000000…act8787 and so on.-> Currently req first 18hexs of 0 would the one who gets reward.updates once every 10min for bitcoin.

Block chain hashing depends on Nounce,prev hash,data. -> Simple math is tons of iterations to match hex-> GPUs



Try mining demo here: <https://tools.superdatascience.com/blockchain/blockchain>

**Blockchain Industry Matrix:**



Implementations of Blockchain industry wise:

**Healthcare:**

Health records: <https://medicalchain.com/en/> <https://www.linkedin.com/company/doc.ai/>

DNA with blockchain store: <https://nebula.org/whole-genome-sequencing-dna-test/>

**Finance:**

<https://ripple.com/solutions/cross-border-payments/>

**Energy:** <https://www.powerledger.io/>

**Internet:** Social media with blockchain backend: <https://steemit.com/>

<https://d.tube/>

Why web 3 matters: <https://medium.com/@Matzago/why-the-web-3-0-matters-and-you-should-know-about-it-a5851d63c949>

**Supply chain:** [**https://www.provenance.org/solutions**](https://www.provenance.org/solutions)

[**https://www.ibm.com/blockchain-supply-chain**](https://www.ibm.com/blockchain-supply-chain)

**Retail:**

[**https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/ConsumerIndustrialProducts/deloitte-uk-blockchain-in-retail-and-cpg.pdf**](https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/ConsumerIndustrialProducts/deloitte-uk-blockchain-in-retail-and-cpg.pdf)

**Education** [**https://www.accredible.com/**](https://www.accredible.com/)

[**https://www.blockcerts.org/**](https://www.blockcerts.org/)

**Data Storage:** [**https://sia.tech/**](https://sia.tech/)