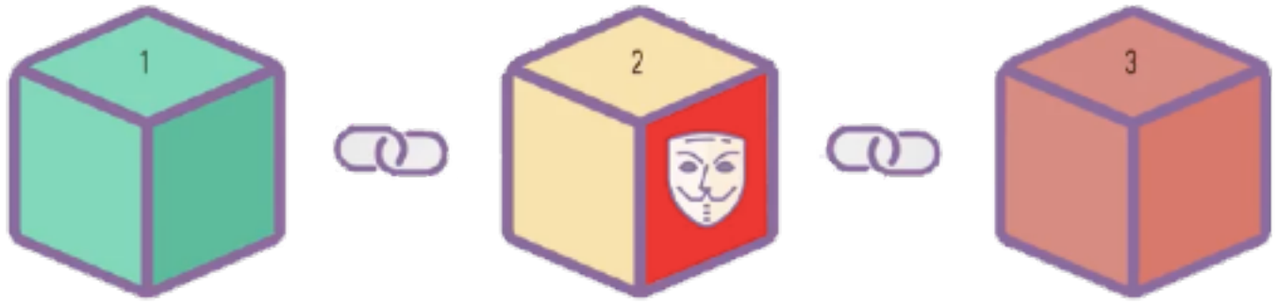
BLOCK CHAIN AND SECURITY:



Hash:	1Z8F	Hash:	~~6BQ1~~ H62Y	Hash:	3H4Q
Previous hash:	0000	Previous hash:	1Z8F	Previous hash:	6BQ1

Uh thats not right??

So, What if someone tamper with a block ?

This results in the change of the hash of the block so the following block will not point to the previous. So changing a single block will make all following blocks invalid

To make a block permanent you need to tamper all the blocks present in the chain

Case: *It takes around **10 min*** to calculate and verify hash of a single transaction in case of bitcoin so time to tamper a block and make it valid will take **10 x Number of blocks present in the chain***

REMEDY FOR TAMPING:

These days computer are highly efficient in calculating hash values so to mitigate

Tamping of the data blockchain have something called as ***proof-of-work.***

Proof-of-work: A mechanism which slows down the creating of new blocks.
So this makes it difficult to tamper a block

Slow and steady...

So, the Security of the block chain comes form its creative use of hashing and proof-of-work