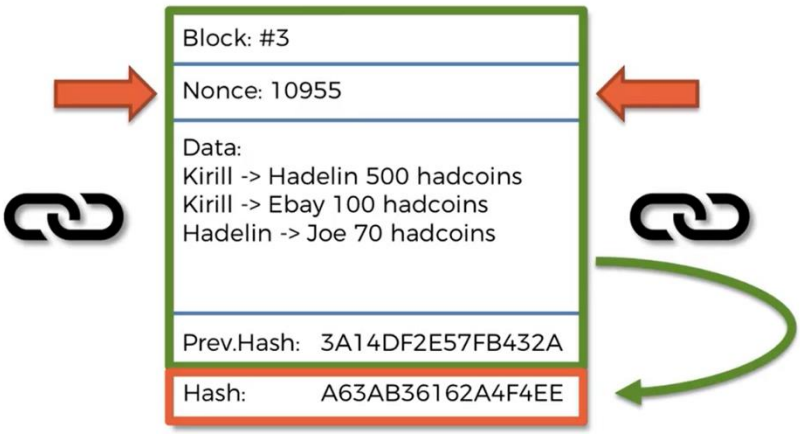
How Mining Works

All right part two how mining works. Let's have a look.

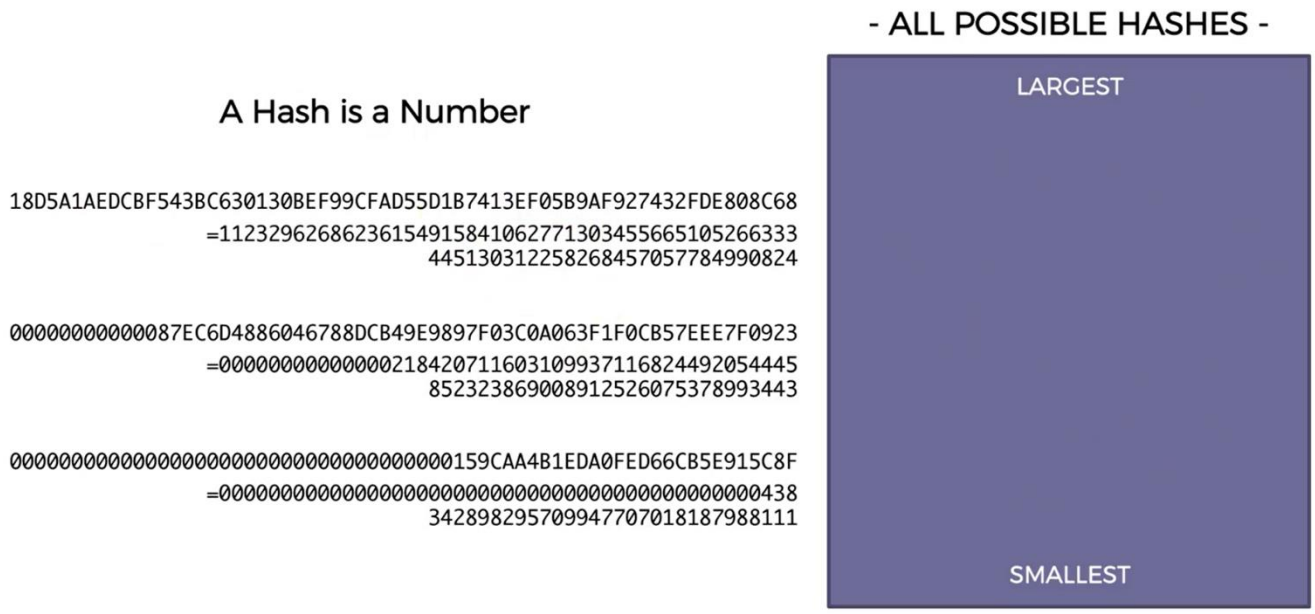


So we left off last summery here where we have this block and we now know that we can control or we can vary the hash of the block by varying the non-SS the number the actual field that we identified. OK so how does this tie in with money.

Well let's have a look.

The first thing that we're going to need to do is to make a statement. The statement is that a hash is a number. And if you already know this then this will just take like a minute if you don't and this will be very useful for us going forward.

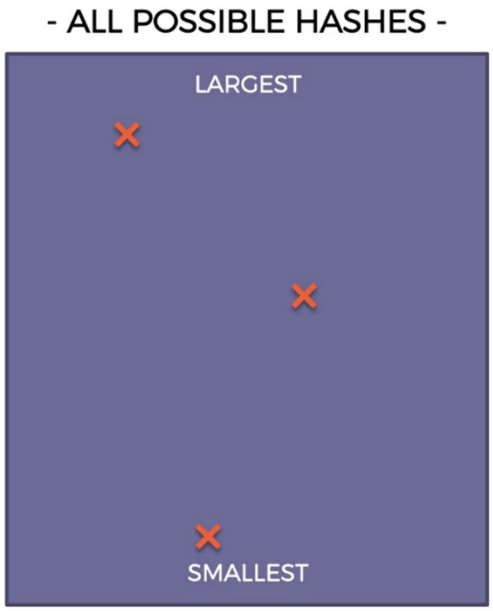
So here is an example of a hash.



This is a proper shower 256 hash it takes up sixty four bits 64 digits. And the statement is that this is actually a number it's not just a word it's just a combination of characters and just

By: Vasu D,Techno Triumph IT Innovative Solution LLP,India
Email: vasukrishna131@gmail.com

the label. It's an actual numbers. You can increment it you can do both medical operations with it. And why is that. Well a hash is actually a hexadecimal number. So here you can see digits from 0 to 9. And also you can see some letters but the letters are limited to f as a b c d e f. And what a hexadecimal number is is it's like a decimal number. But instead of just having digits from 0 to 9 it also has those six extra ones so a stands for 10 B stands for 11 C stands for 12 D stands for 13 E stands for 14 F stands for 15. And so that's all there is to it. And we can actually convert this hexadecimal number into a normal decimal number and it will look like this.



18D5A1AEDCBF543BC630130BEF99CFAD55D1B7413EF05B9AF927432FDE808C68

00000000000087EC6D4886046788DCB49E9897F03C0A063F1F0CB57EEE7F0923

0000000000000000000000000000000000000159CAA4B1EDA0FED66CB5E915C8F

So there's our decimal representation of our hexadecimal number as you can see the number is visually longer and that's because in the decimal system we only have 9 digits whereas in the hexadecimal system .we have in the decimal system we have 10 digits.

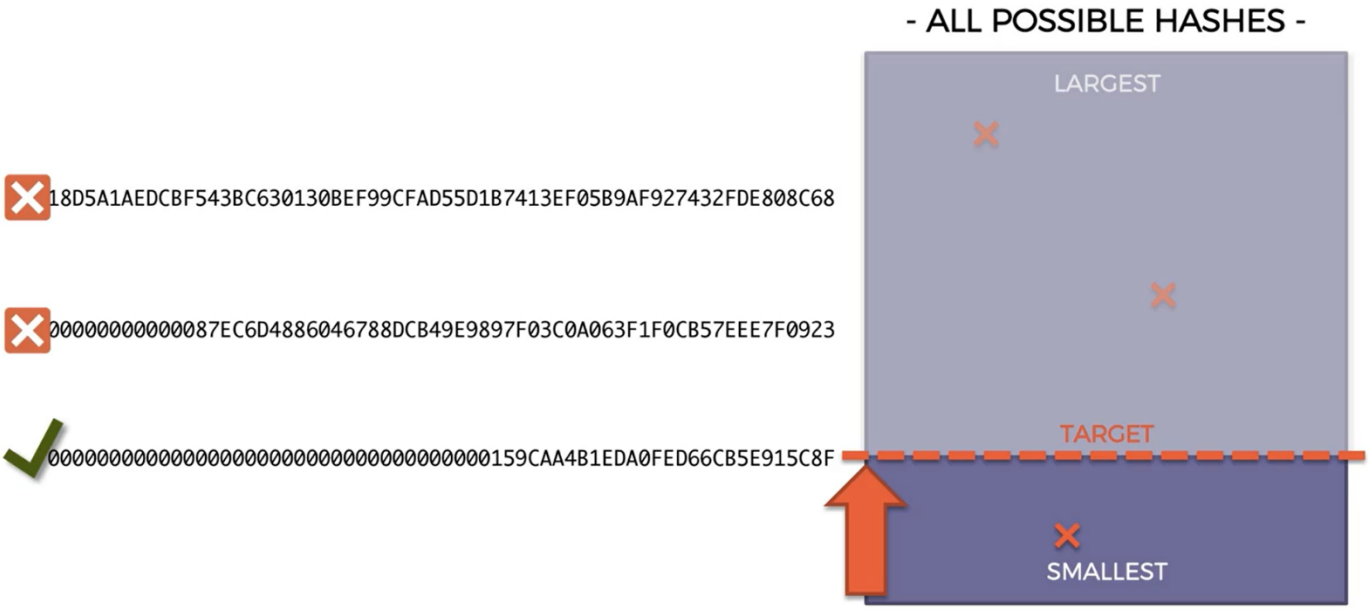
Funny but in the hexadecimal system we have 16 digits so therefore every digit can encode at a higher value. This is another SHA 256 hash as you can see at the start there is leading zeros. You don't have to write them out.

I included them here just to illustrate that the visual length of this number is the same as the previous one. It is also 64 characters or digits in length.

So how mining works is in essence the block chain system or the hash algorithm will set a target so, there's a target set for minors to accomplish a certain hash.

So let's say the targets are here marked in above figure target. There we go. That's our target. And the way it works is any hash. Higher than Target doesn't count. That's not good enough for the blocking. It has to in order to be include in the block. It has to be locked be below the target. And the important thing to know is this is completely arbitrary. There is no there is no economical reason for it.

There is no like logical or computational mathematical cryptographically reason for it. It's just a way to put hurdles in the way of my mind has to create a challenge for them to solve. That's the only reason they're there is this started. No other is.And so in this case if a minor found this hash it wouldn't count to me not good enough there would not be allowed to create a block with this hash number.

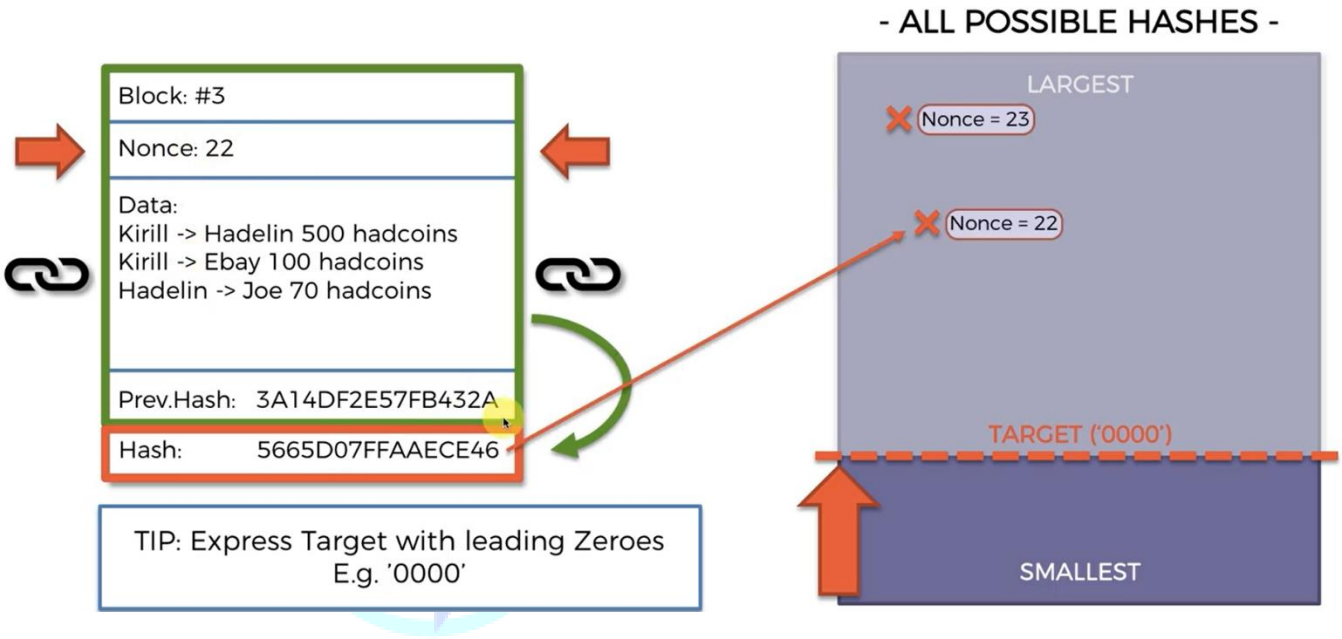


First hash is also not good enough. It's above the target.

By: Vasu D,Techno Triumph IT Innovative Solution LLP,India
Email: vasukrishna131@gmail.com

But if you found this hash you'd be welcome to create the block. You'll be allowed to create a block and that's when you will be considered the miner who actually mined the block because you found a hash like that and will like. This is like just in a high level we will go into detail like in a second in this but before we do I wanted to give you guys a small tip that a good way of thinking about the target is actually in terms of leading zeroes.

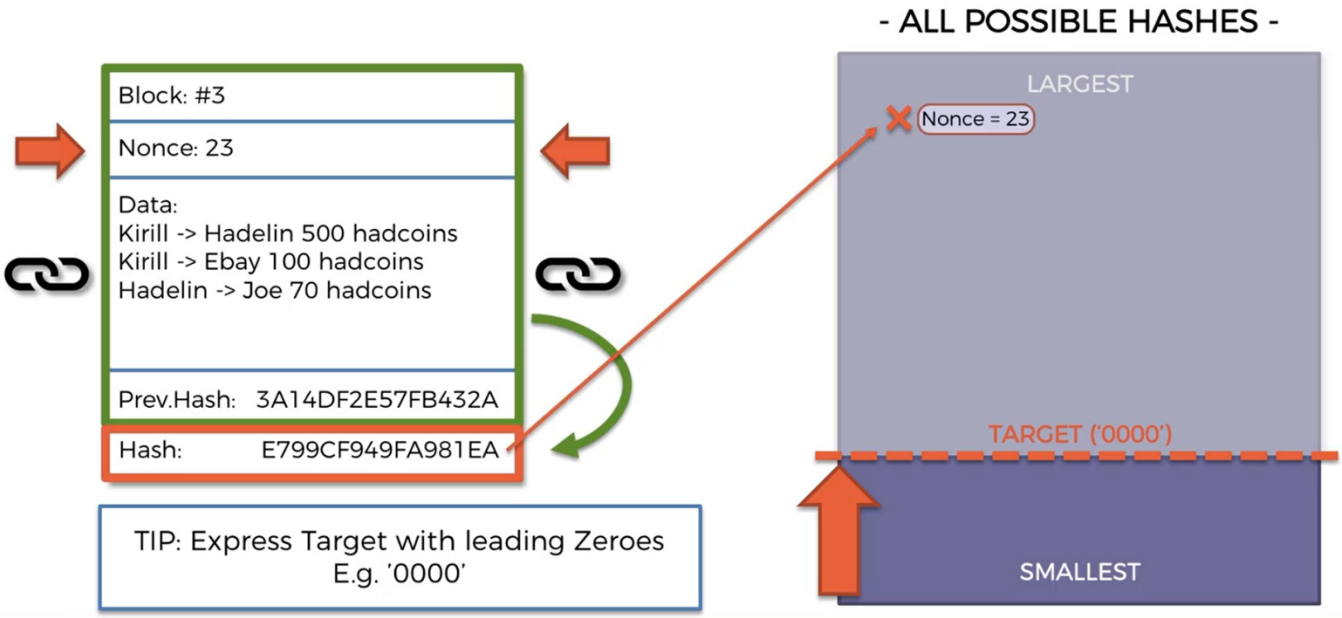
So as you can see the lower you are the smaller the number and the more leading zeros will be So if you think of the target rather than as it like I remember trying to remember what the target is in terms of hashing. Just remember the number of leading zeros for instance for eating zero. And now let's discuss what we just talked about the whole mining because I know it's right now.

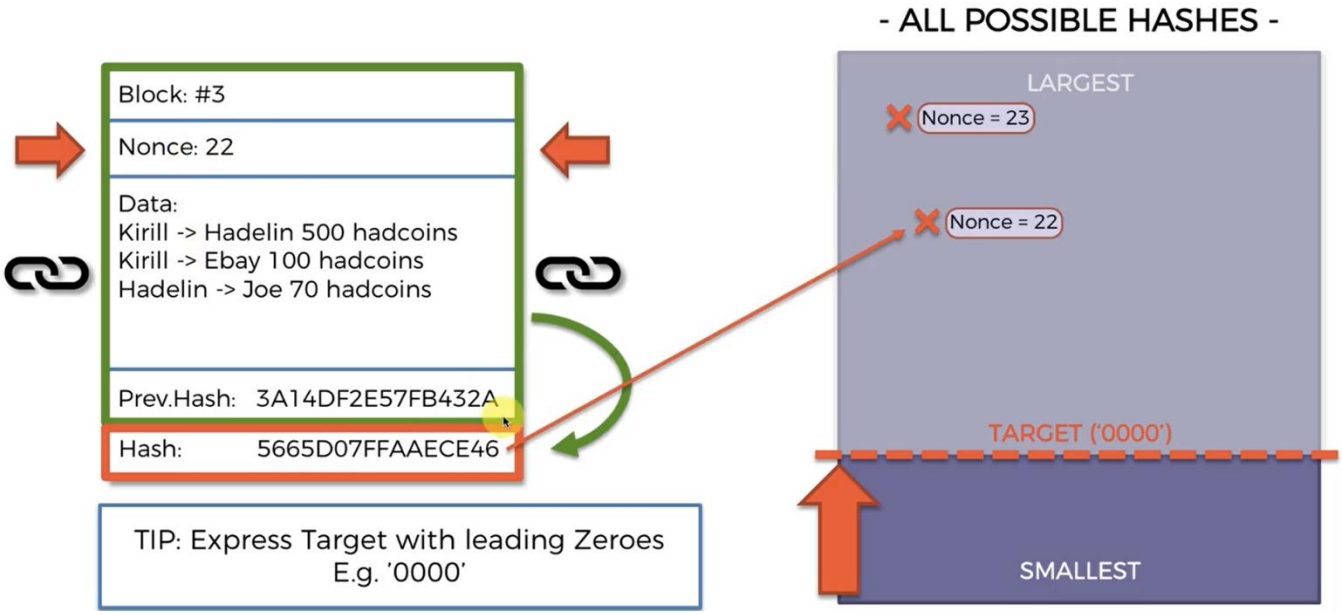


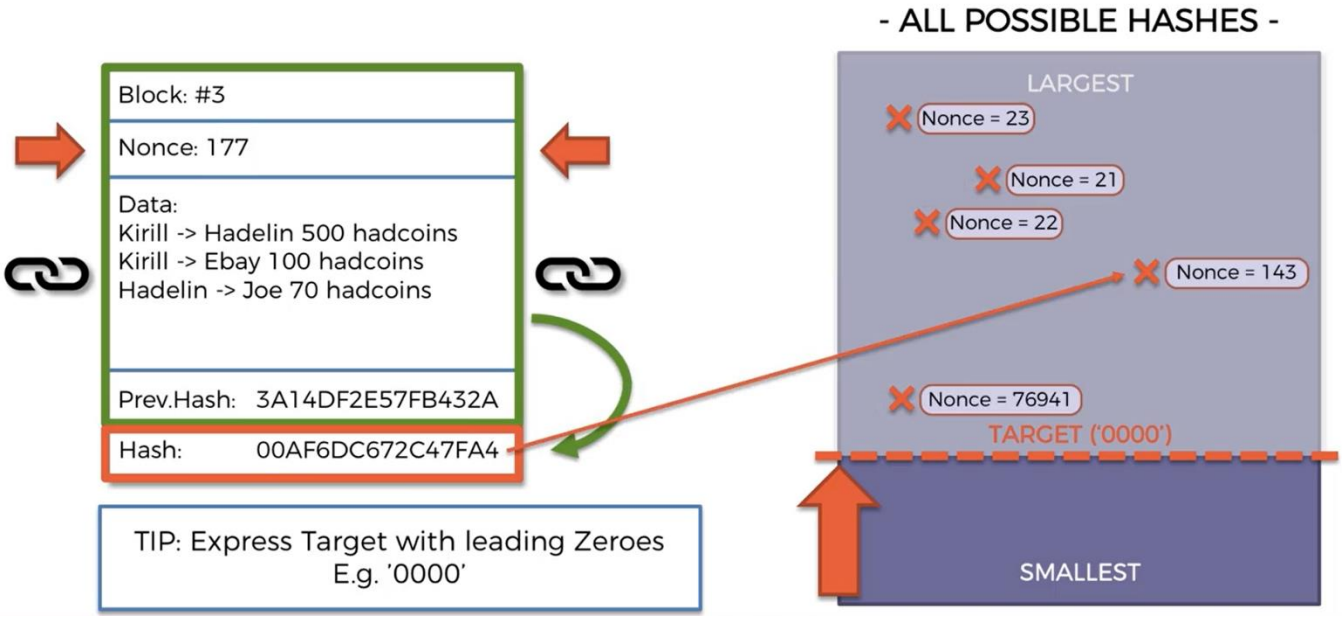
So we want to add and you block so we know that block number we're going to be adding block number three. So you can change that the data in the block. So as we discussed we don't want to change the data we can't change it.

But for now for us to understand how mining works is good enough to agree that we have this set of transactions that needs to go into the block and we cannot change it because if we agree that the list of transactions that then we cannot change any details of each section because we don't want to tamper with the data.

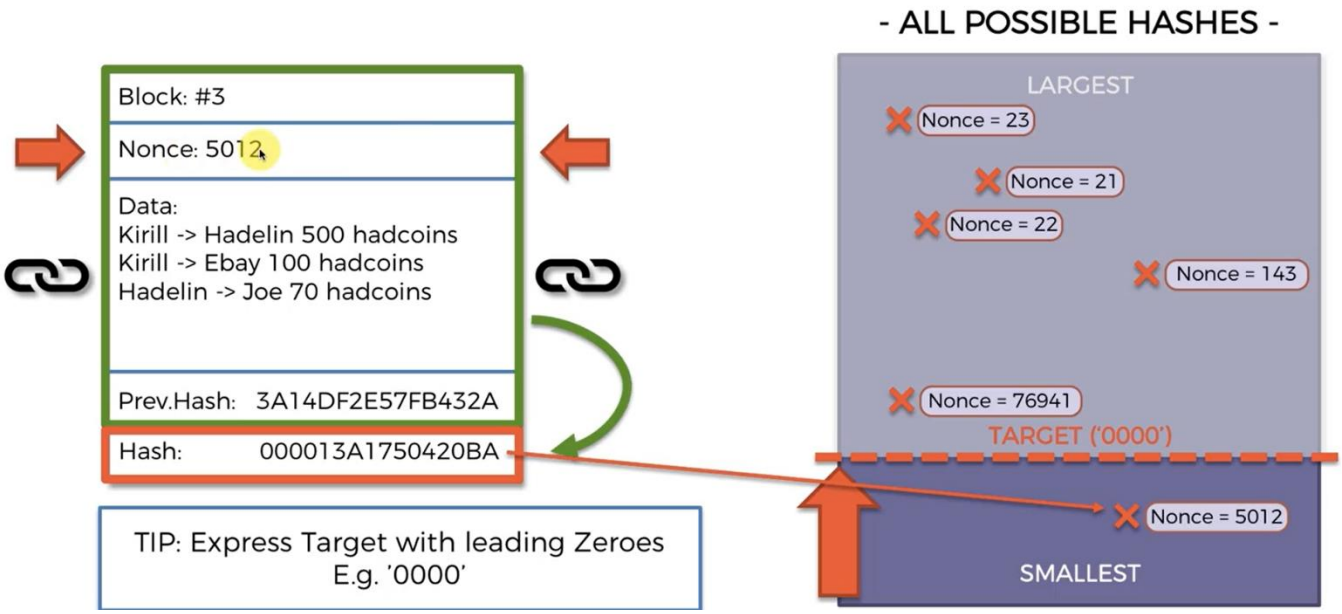
And that's the whole concept whole point of block chains that it's an immutable ledger. Then we can also change the hash of the previous block. Chant cannot change this value because it has to be cryptographically linked to the hash of the previous block. So the only thing that we can actually change in this whole block is the nonce let's us allows us to vary the hash of the card block. So let's see what that means for mining.







By: Vasu D,Techno Triumph IT Innovative Solution LLP,India
Email: vasukrishna131@gmail.com



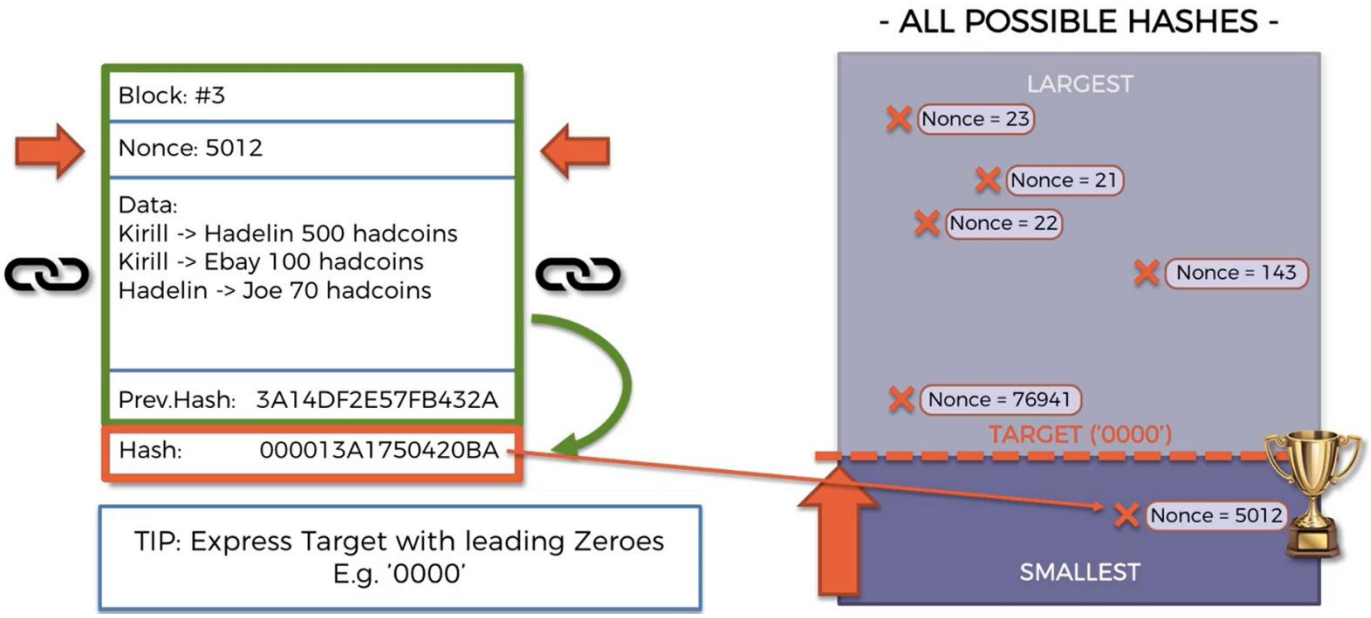
So let's see what that means for mining. Check the above mining figure one by one .

So if we plot this hash onto our map of hashes you'll see that it might be somewhere over there. It's hypothesized that it's over there. And that's the hash and this label is just to remind us that this hash was generated from this block when the nonce was 23. So next let's change and wants 22. Now you can see the hash is over here it's the smaller hash and that was generated by nonce 22.

And so we could just keep going doing that because we will not be allowed to add this block into the block chain until the hash is below the target. So all we can do is just keep guessing different nonces as you can see there we go. And that's essentially what miners do.

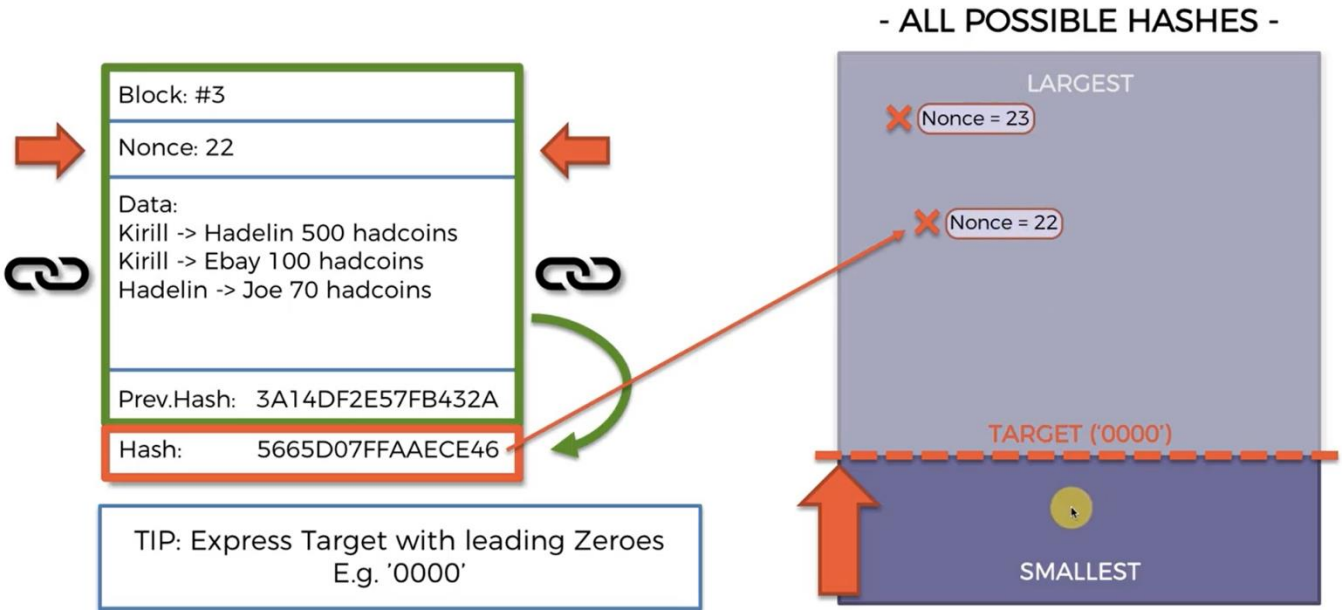
Miners just sit there and they change this field they changed the nonce in order to try guess a value of the non said will generate a hash below the target. That's as simple as that. And once they do generate such value So for instance they find unknowns at some point at random by accident through brute forcing they find the nonce.

For instance 5012 that generates a hash below the value. Then they win that's it. They get this nonces commonly called among miners.

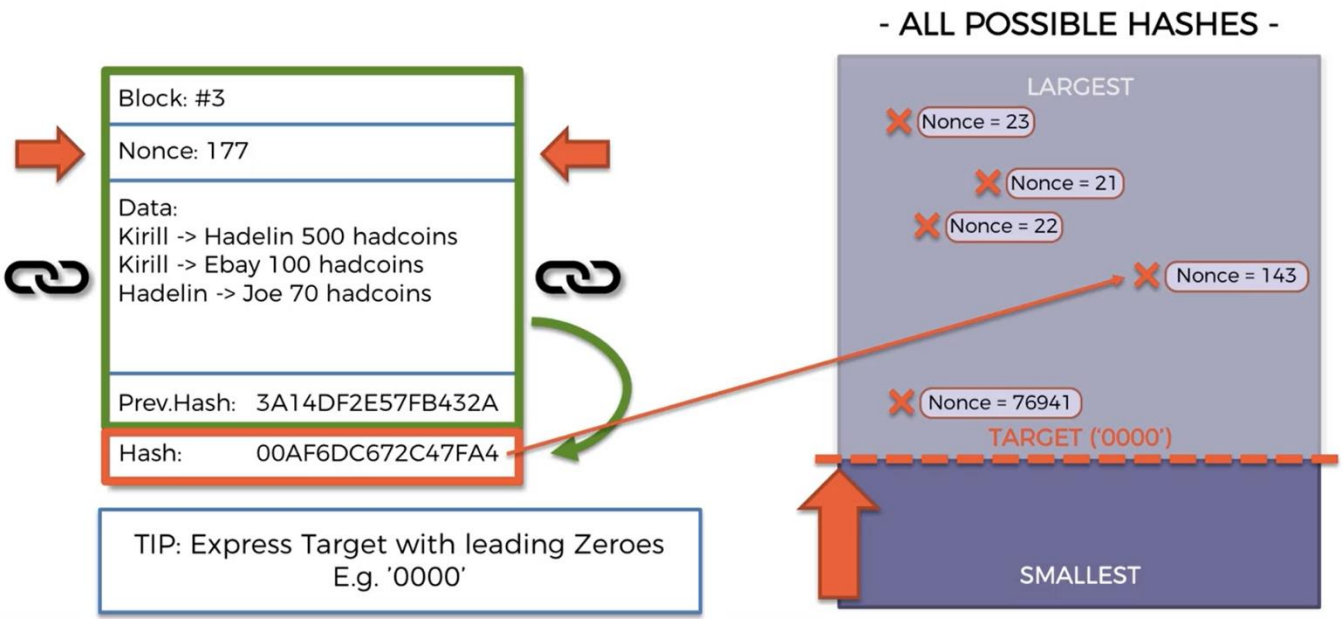


It's called the golden knots and because it generated that has military as you can see as those four leading zeros is below the target. And that said so then once that's done they're allowed to add the block to the block chain and they get the reward which again will discuss much a lot better.

So here you can see that the hash 4:23 was up here then the hash 4:22 is down as mentioned in figure below



. And if for instance if changing the notions a little bit would change the hash a little bit that would allow miners to predict that. Looks like by changing by reducing the odds the hash is going down so we'll have to go is 21 2019 18 and finally I'll get below the target.



I'll get over here but that's not the case. As you can see at 21 it goes up here you know 76000 is here but 143 is here is this completely all over the place is completely unpredictable and that's a very important feature. Now we can see that why that's such an important feature of the hash why the avalanche effect is so important in the hash because we thought that this whole cryptographic puzzle this concept of finding the hash is called the right hash is called as cryptographic puzzle.

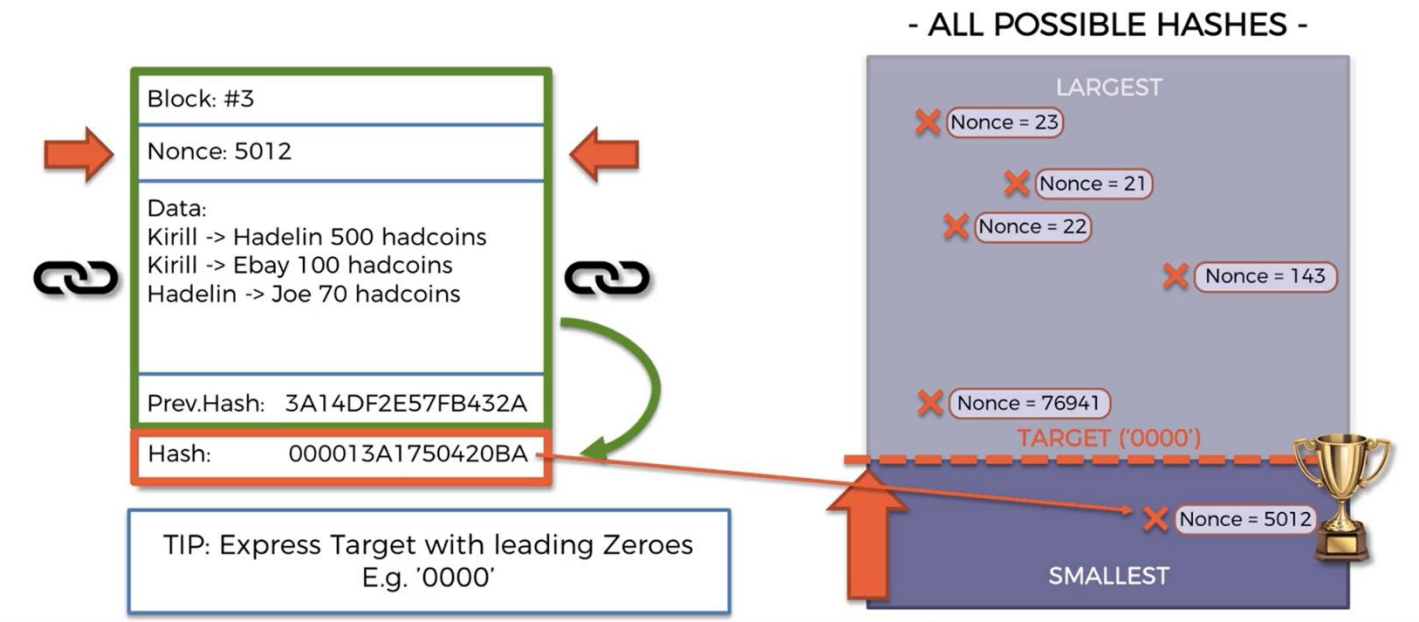
This whole cryptographic puzzle would not even exist because you could just like find the way you find your way like a shortcut into getting a small astronaut. And that even further illustrates the importance of the hashing algorithm like the reason for us using a hashing algorithm is because you cannot reverse engineer it.

You cannot crack it and predict what hash you will get based on the nonce input as soon as somebody is able to do that. The whole of this concept is going to fall apart because people will be just being able to predict the nonce and then just put in and they'll know what hash they get so they won't have to put in the work in order you know put in like hours and hours and hours of machine time in order to crack unknowns in order to get the right hash below the target. and that's it.

They will put in the block. So that's what the 256 promise is that nobody's been able to crack it. There's been attempts lots and lots of attempts to do that people but people haven't gotten even close to cracking it. So those are some important features to remember about or to know about the hashing algorithm why it's so important in Blockchain.

So that's the second important thing that we needed to point out here. So there we go that's our golden Nonce at the bottom. And yeah so that's in essence how mining works.

You just need to keep iterating the nonce until you get a hash below the target then you get to add that block or whoever gets there first guess at that block and then the whole thing starts again for the next for the next block.



I hope that now it's clear how mining works and what this whole fuss is about what the cryptographic challenge is why people are racing to get to the best the golden nonce and why there's so many miners around the world why they need the computation power and I can't wait to see how the next external.

That’s all for today until then enjoy blockchains.

Techno TRIUMPH
IT Innovative Solution LLP

By: Vasu D,Techno Triumph IT Innovative Solution LLP,India
Email: vasukrishna131@gmail.com

By: Vasu D,Techno Triumph IT Innovative Solution LLP,India
Email: vasukrishna131@gmail.com