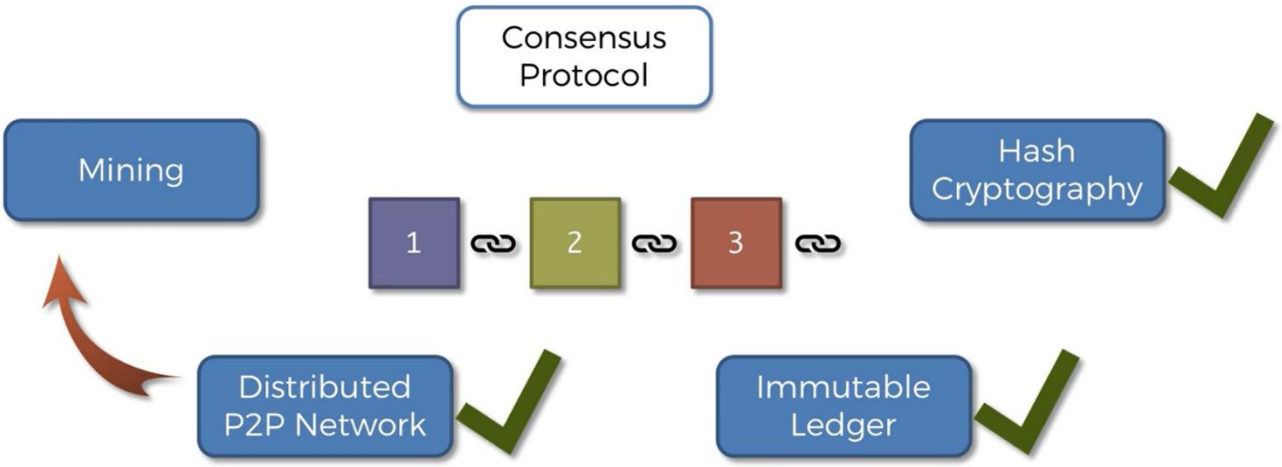
How Mining Works

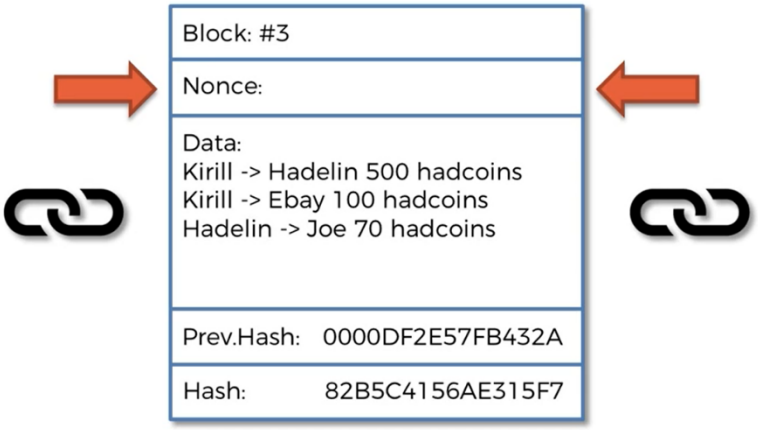
Hello and welcome back.

And today we're going to be talking about mining. It's going to be a two part in mining. All right so let's have a look where we are on our map.



We've talked about hash cryptography the immutable ledger. We've now also checked off distributed peer to peer networks. And finally we're moving on to the mining in this we're going to find out exactly what's the whole system is about why is there mining.

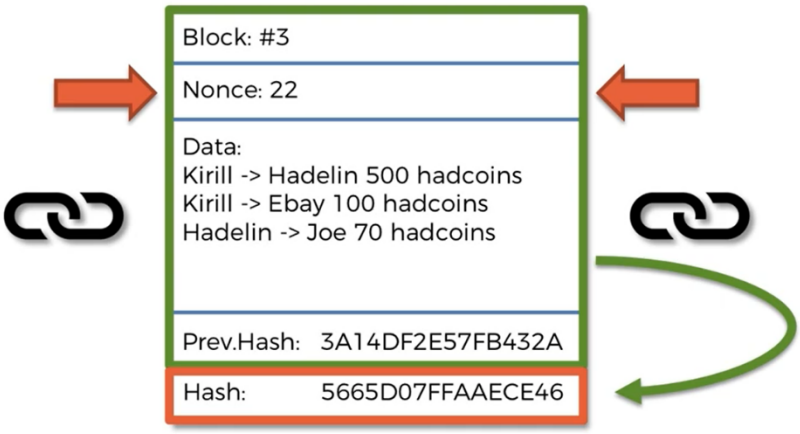
What's the competition that everybody's participating in. Why is so why are so many resources allocated or dedicated to mining block chain bitcoins and things like that so let's have a look.



Here is our block in a block chain. And as we discussed it's got a couple of fields so it's got the block number at the top. It's got some data. And as you can see here I put in some fake data where I said sent I Hadelin 500 odd coins. Then I bought something on ebay for a hundred odd coins at once and some person named Joe 70 odd coins and what I'd coin is is a cryptocurrency that you'll be creating together for on line.

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

Keep in mind that a block doesn't just store one single transaction or block stores multiple transactions so several transactions get put into a block. Then also in the block we've got a field for the previous hash or the hash of the previous block and this is a very important feature of block chains because that's how the cryptographic link is facilitated between them. And finally we've got a field for the hash of the current block.

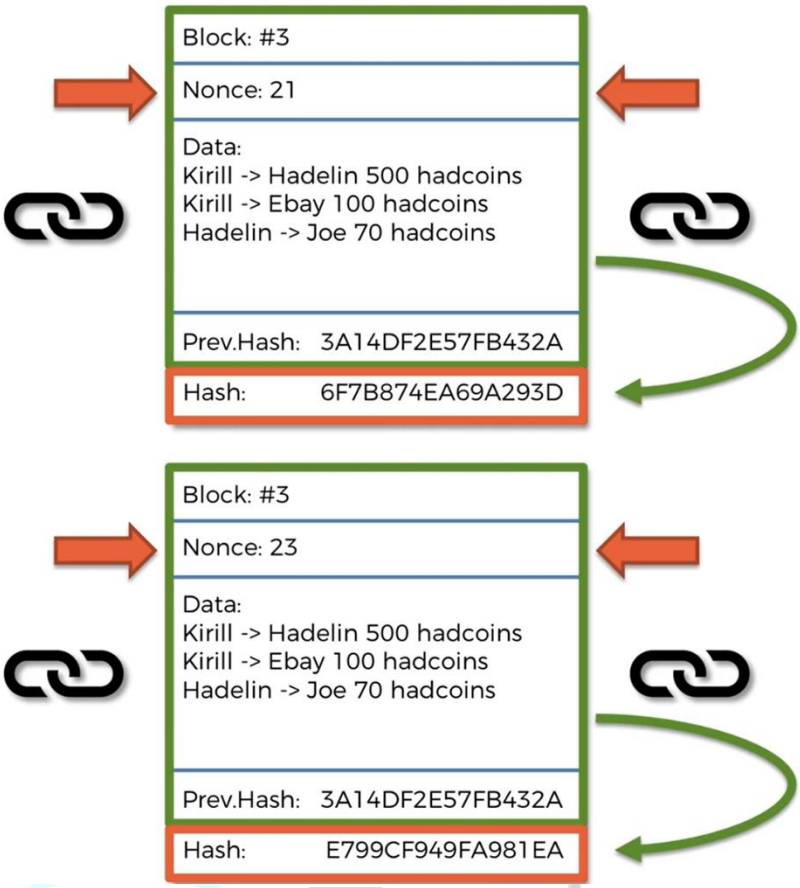


And how do we get the hash of the current block where we take the block number of the data and the previous hash put all of that into all that together into a hashing algorithm and it spits out a hash for us. And there it is. That's our hash. And so here this instantly asks for a question and the question is if it's so simple to just take the block number the data and the previous hash put into hashing algorithm and get a hash out like in which takes a half a second if it's so simple then how come black What's the whole fuss about mining.

How come there's so many like hundreds of thousands of mining rigs around the world are like nodes around the world and lots of mining rigs and a lot of competition powers dedicate to them.

Why is this all happening and what's this competition that everybody is in. If this is all there is to mining a block Well in reality it's not as simple as that. There is actually another field in a block and it's time to reveal this field. The field is called non-SS and not stands for number used on the once. And so this field is what mining is all about as we'll see from the story on the next one. Everybody is just changing this field all the time.

So to understand this let's have a look at what is it that now controls the hash. What is it that now dictates the hash of the block in this new updated structure that we see. Well it's these things how it in the Green Square. We've got the block number the non-SS is now included in that party.



And then we've got the data and the previous hash. So now we take all these four components we put them into a hashing algorithm and then it will split out the hash value. And so all of a sudden now what the non-SS gives us it gives us extra control gives us extra flexibility.

Now we can manipulate the hash value by changing the non-SS so we don't have to change the block and we can change the block number because the block number is the block where we can change the previous hash because it's linked directly to what we have in the previous block and we can change the data because that would mean we're tampering with the data and that would defeat the purpose of a blockade.

It has to be an immutable nature. We put in a nonce and it will spit out something that we cannot control the hash. But at least we can vary the hash by varying the not so let's have a look at how that works. We get a higher and different hash 20 different hash 21 again different hash 22 23 then we can do something I wanted to point out here so you can see that the hash is changing.

And also notice how where do we go from let's say 20 from 21 to 22. Notice how the hash is changing absolutely like dramatically. And why is that happening.

Or that's the avalanche effect in action. What's happening is in the block itself. Essentially we just changing one bit of information.

So if you write it out in binary code you will see that this block has like some combination of ones and zeros.

And to go we're just changing literally one bit somewhere from 0 to 1. And that is that's all the change we're doing. But at the same time the hash used is completely unrecognizable completely different to what we had before. And that is important and will be important why we'll see in the next part. But that's t\he avalanche effect and actually I just wanted to illustrate that.

OK. So that's how we change and also just take a random number this turn and 43 like there's ten thousand nine hundred fifty five.

So non-SS is a number that can go up to like four billion something. So it's quite a large number there's a lot of variety that you can play around with the nonce. And that gives you variability in the hash. So there we go that's a starts to mining. Now will end the first part and in the next part we will see how the mining works cryptographic Puzzle .

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