Understanding Bitcoin Transactions

In this article we will discuss the complex issue of a Bitcoin transaction. Bitcoins are exchanged and transferred digitally through a computer generated code. To ensure that these transactions are completed safely and securely users use keys.
Two keys are always required for any transaction:
1. Public Key
2. Private Key
The public key is the one that is used for the actual transfer of the Bitcoin. Because this key is public it allows anyone to verify the transaction. Before the transfer can take place the senders account is verified, this ensures that they have enough Bitcoins in their account to cover the transaction. Once this first verification is done the transaction enters into the Block Chain. Think of this as the public ledger displayed in a transparent glass layer. People can see but they can't touch it!
This first verification step prevents anyone from trying to send the same transaction to two different people at the same time. If anyone attempts this type of process it is referred to as double spending. Having the two different keys prevents this from happening.
The end user then uses their private key to unlock the transaction, once it has been verified. The Bitcoin then gets deposited into their Wallet. A wallet is simply an online bank account. Because the system uses two keys all activity in the network can be easily traced. The process of verification often occurs multiple times before the receiver deposits the Bitcoin.
All of these transactions are available in the Block Chain, every transaction ever made is accounted for here. Plus anyone can view it if they wish to.
How the Blockchain is Created
Let's look at how the blockchain is created. As we described above it takes several verifications for each transaction to proceed. At this time the current number of verifications required is six. Before a transaction enters into the Blockchain a new block is formed first. The first step in this process is to verify that the person sending the Bitcoin has the currency available in their wallet. Now this is where it can get complicated, but we will try to keep it as simple as possible for you. To create a block, a process known as hash creation, has to occur. Think of this as small nodes that are attached to a block each time it is verified. So what happens is that the original block gets a little longer.
As this is all done on via a mathematical software program zeros are added at the beginning of the block. As each new block, verification, is completed more zeros are added on. The largest block is always taken to be the authenticated block. Once this verification process has occurred six times this block enters into the BlockChain. As it enters a timestamp is associated with it. This is how you can easily see all the transactions that have ever occurred. No records are ever removed from the Blockchain and it will continue to grow in size
Words 505