*****Go to www.bitgoldwallet.com for information on what bitcoin is and how to safely buy, use and store it, and how to choose a secure and memorable password*****

BITCOIN: A SIMPLE EXPLANATION
(17 April 2020)

How does bitcoin work? This article will try to explain bitcoin using words and examples which are easy to understand. To achieve this, the explanation may be very slightly inaccurate in some places, however this will make it easier to understand. By the end of this article, you will hopefully have a better understanding of bitcoin.

PART 1.1 : BITCOIN PUBLIC ADDRESSES

The first basic part of bitcoin which needs to be understood is what bitcoin public addresses are, how they are created, and how they work together with bitcoin private keys. A bitcoin public address is basically like a bank account number which holds people's bitcoins. An example of what it may look like is:

16er32qQe1Xi5ZEbqxvWJJN4GKC9kYnp1i

A real bitcoin public address like the one shown above is made up of capital and lowercase letters, as well as numbers that are arranged in a specific way.

In our simple explanation, I will instead give an example where 10 NUMBERS are used to represent a bitcoin public address. So our example bitcoin public address looks like the below:

8104940784

In order to receive bitcoins, you need to have a bitcoin public address which the bitcoin computer wallet program has created. This is the 'thing' you give to other people for them to send you the bitcoins. So how are bitcoin public addresses created?

PART 1.2: BITCOIN PRIVATE KEYS

A bitcoin public address is always created using a bitcoin private key. An example of what a bitcoin private key may look like is:

L4iLhJzUAvNfa6x3wyYGV9N6fCR3cMXN7EJ7RiC5ct4dZjmdhSmd

A real bitcoin private key like the one shown above is made up of capital and lowercase letters, as well as numbers that are arranged in a specific way.

In our explanation, I will instead give an example where 20 NUMBERS are used to represent a bitcoin private key. So our example bitcoin private key looks like the below:

16503429214399795533

To create a bitcoin private key, you would use a bitcoin computer wallet program. This bitcoin private key is like a password to your bitcoin public address that lets you send the bitcoins from the bitcoin public address you currently own to another person's bitcoin public address.

SO HOW ARE BITCOIN PRIVATE KEYS CREATED? This is where the magic starts.

All bitcoin private keys start as a very LARGE and very RANDOM number that is created by the bitcoin computer wallet program. This random number might be between 100 – 1000 numbers long or longer*. Think of a number so large that it is impossible for anyone or anything to guess this number. Imagine the entire universe was filled with computers placed side by side, all of them turned on and all of them repeatedly trying to guess this number, for all time and still failing. This is more or less the number that your computer creates.

The computer program you use will then convert this random number to a bitcoin private key. To a computer, all data is numbers represented by zeros and ones. So it can be seen that a computer program can easily convert any random number to a bitcoin private key with the correct formatting or structure.

The main thing to understand is that the bitcoin private key is infact a completely random set of characters and numbers. No one else on the planet knows the bitcoin private key except you because you created it randomly on your computer. If you created the bitcoin private key and only you know it, then this means you own the bitcoin private key.

(Note: in reality, security is a massive issue with the creation of bitcoin private keys due to the risk of this data being stolen and spied on, so many people, including beginners let reputable cryptocurrency exchanges handle the storage and creation of their bitcoin private keys for them).

So how is the bitcoin private key converted to the bitcoin public address?

The bitcoin computer wallet program does this by using an exact formula known as a SHA256 hash together with other steps. The formula used is one-way, meaning that once the bitcoin public address is created, no one can use the bitcoin public address to work out what the private key was. And the formula is always the same and always gets the same result for the same original character string.

In cryptography and in bitcoin, a one way hash like the SHA256 hash shown above is very important and is used a lot.

In our explanation, instead of using the SHA256 hash; to make the idea easier to understand, I will use a simple one way formula (or hash) which I have made up so you can see how the one way aspect might work. We will call this hash the MU-hash (Made up hash):

Our example MU-hash =

1) Take the first set of numbers, then 2) multiply this by 3141592654, then 3) remove the first 5 numbers from the result, and then 4) repeat this process 1000 times, and then after this is done, 5) only show the first 10 numbers and remove all the other numbers.

To simplify this further so that this can actually be done in an example, we will replace 4) repeat this process 1000 times with 4) repeat this process one time.

Ok. So to summarize PART 1, the computer wallet program creates:

Random number > then creates Bitcoin private key [then uses one way hash] > to create Bitcoin public address

OK. So now we can start our example:

Start with Bitcoin private key = 16503429214399795533

Then hash this private key with our MU-hash =

1 & 2: 16503429214399795533 x 3141592654 = 518470519857673886665574814582

3: 518470519857673886665574814582 (remove first 5 numbers) = 051985767388665574814582 [take note that it is possible for zeros to be in the front of the number, and that it is rarer for these resulting numbers to have many consecutive zeros in front of it]

4: (repeat this process one time) = 051985767388665574814582 x 3141592654 = 16331810494078453270017822328062 8 (then remove first 5 numbers) = 810494078453270017822328062 8

5: (only show first 10 numbers and remove all the other numbers) = 8104940784 = Bitcoin public address

SO we are left with:

Bitcoin private key = 16503429214399795533 (and)
Bitcoin public address = 8104940784

Every single time we do this one way MU-hash on the same original bitcoin private key we will get the same bitcoin public address. And looking only at the bitcoin public address, it is impossible to calculate or guess what the original bitcoin private key was. For our simple example though with the MU-hash, a powerful computer organization might be able to guess or calculate our bitcoin private key through random guessing (because our numbers are fairly small) but for the real bitcoin private key this would be impossible to do.

At its simplest level, this is how bitcoin public addresses and bitcoin private keys work. If you know the bitcoin private key, you can always prove to the network that you own the bitcoin public address which contains the bitcoins and the network will always let you move the bitcoins even though they don't know who you are.

You can see now how anyone on the planet can, in the safety of their own homes, create their own bitcoin public addresses to give to people in order to receive and send bitcoins from. This is part of what makes bitcoin a decentralized digital currency which allows anyone to take part in, and which is hard to restrict or ban.

PART 2: THE BITCOIN BLOCKCHAIN

So the bitcoin private key and bitcoin public address holds the actual bitcoins. And you can see that these can be created and stored without limit by anyone knowledgeable enough. However, if we only have these, the bitcoins won't be of any use. We need a payment network which lets you send your bitcoins to different bitcoin addresses.

The bitcoin blockchain serves this purpose. The bitcoin blockchain is basically the list (or ledger) of all the transactions and all the used bitcoin public addresses that has ever been made in the bitcoin network. It is maintained by a large number of highly invested people and groups who take part in the network (known as miners)[**].

The easiest way to understand the bitcoin blockchain is to go back to the very beginning of bitcoin in the year 2009 at Block 0 known as the genesis block and then slowly build up from there. I will only need to describe up to Block 2 for you to get a good enough idea. I want to emphasize that these things didn't happen as described for the actual bitcoin blockchain but is rather a hypothetical scenario which fairly accurately explains how bitcoin mining and bitcoin transactions work[***].

BLOCK ZERO – GENESIS BLOCK

BLOCK ZERO basically has no transaction data. But it still has data such as the date it was created and some other data. This blockchain data is stored on the computers of individual people who have downloaded and run the original bitcoin wallet program (called nodes and/or miners). In our example we will assume there are only 3 participants which make up all the

users in the network: Participants A, B and C. In the future many new participants will join the network. The original bitcoin wallet program and all future variations of the program is free for anyone to download and use.

Each of these 3 participants would have had the option to mine bitcoins. And they would have been able to create bitcoin public addresses and private keys like described earlier.

When they ran the mining software for the first time at least one bitcoin public address was created by each of them. So assume:

Participant A has created bitcoin public address
1EcKp4Cv6QLV5kmCMEezERLXJYTaNVaLgs

Participant B has created bitcoin public address
14pP4zDquF3NE3BSjjpNbsCTz9tDs9cSN8

Participant C has created bitcoin public address
1J62KZfV2Z8653zv3ydW88YgjBZySj7CQm

Now all 3 Participants activate their mining software. Since there are currently no bitcoins in all the world, BLOCK ONE, the next block of the blockchain will not contain any transactions showing any movement of bitcoins, but it will show a balance of 50 new bitcoins created into one of the 3 bitcoin public addresses shown above owned by Participant A, B or C. New bitcoins enter the world after every mining round. The way the software decides which miner gets the 50 new bitcoins is based on a 'proof of work' system. On average new bitcoins enter the world every 10 minutes and this rate is set by the computer software.

HOW MINING WORKS

So we will assume that all 3 participants turn on their mining software at the same time and everyone is using the exact same type of computer. These 3 miners all have the same copy of the bitcoin blockchain which in its entirety is currently BLOCK ZERO. The mining software now takes the BLOCK ZERO file data and adds the empty BLOCK ONE file data to it and then expresses this file as a number (we will call this the 'block one computer number'). Remember that all data files on a computer are zeros and ones. Then the software begins the mining process by taking a random number (called a nonce) and adding this random number to the end of the 'block one computer number'. Then it creates a one way (SHA256) hash of this new number and the result is recorded somewhere. Basically the rules of the program states that if this resulting number (or hash) has a certain number of consecutive zeros in front of it, then it proves that that computer has completed the 'proof of work' and the software automatically creates the 50 new bitcoins into that participant miner's bitcoin public address. If the random number doesn't lead to the required number of consecutive zeros then the computer tries again until it does find one. The proof of work here lies in the fact that mathematically, it

takes a certain number of random hashes by the computer before the computer will find one that meets the difficulty requirement of having a hash-result with the required number of consecutive zeros in front of it.

Every 2 weeks this difficulty is automatically adjusted by the bitcoin computer program which all the miners run by adding or reducing the number of consecutive zeros that are needed before new bitcoins can be awarded. The more zeros there are, the more difficult it is to solve****. The difficulty is changed so that on average about every 10 minutes a new block is solved, and this happens regardless of how many or how few computers are mining.

In our example each of the 3 miners have an equal chance of finding the correct hash first because everyone is running the same computer type and so each computer will create the same number of hashes per second. In modern day bitcoin mining though, different miners have vastly different hash producing abilities and this will directly impact on how many blocks they will solve compared to other miners. The more hashes they can make compared to the rest of the miners, the more blocks they will solve. Also, in modern day mining the number of hashes required is so huge now that only mining pools or centres with millions and millions of dollars worth of dedicated mining hardware in them can successfully solve new blocks.

So we will assume Participant A was the first to solve BLOCK ONE and their bitcoin wallet software now shows 50 bitcoins at address 1EcKp4Cv6QLV5kmCMEezERLXJYTaNVaLgs. Participant A will now broadcast this information to the entire network and Participants B and C will check that Participant A's hash number is correct by simply checking that the number they used leads to the correct hash in that new block (correct hash = proof that work has been done). If it is correct then their computers will now also show BLOCK ZERO + BLOCK ONE.

The bitcoin blockchain has now been updated and will look like the following:

BLOCK ZERO (date and time created) +

BLOCK ONE (date and time created)(50 NEW BTC at 1EcKp4C… as mining block reward) + Solved HASH of Block one

MAKING TRANSACTIONS

Lets say that participant A decides to spend their bitcoins right now by sending it to another bitcoin address. Participant C has given Participant A an address for him/her to send the bitcoins to (say address 18yACUJ3PaAWs41GoJU7aDZSTLEqwaBA4b).

So Participant A will now create a transaction on their computer. The transaction will be to:

SEND 20 BTC from 1EcKp4Cv6QLV5kmCMEezERLXJYTaNVaLgs to 18yACUJ3PaAWs41GoJU7aDZSTLEqwaBA4b and send the CHANGE 29 BTC back to

1EcKp4Cv6QLV5kmCMEezERLXJYTaNVaLgs, and give 1 BTC as the transaction fee to be sent to the miner that solves the next block.

This transaction will immediately enter the memory pool (called mempool) which can be picked up by any of the other miners in the network.

Now lets assume all three Participants A, B and C continue to try to solve the next block of the bitcoin blockchain called BLOCK TWO.

To do this they would take the current blockchain and then add any transactions they like from the mempool to create a new blockchain that includes BLOCK ZERO and BLOCK ONE and BLOCK TWO, which is then expressed as a 'block two computer number'. They will then attempt to solve the new block like before. None of the miners are required to add any transactions from the mempool and can continue to mine an empty block if they wanted, but they usually want to add transactions because they will receive the transaction fee that Participant A has included in the transaction.

So lets now assume this time Participant B successfully solves the next block.

The bitcoin blockchain will now look like the following:

BLOCK ZERO (date and time created) +

BLOCK ONE (date and time created)(50 NEW BTC at 1EcKp4C… as mining block reward) +
Solved HASH of Block one +

BLOCK TWO (date and time created)(20 BTC at 18yACU…. (1 confirmation) moved from 1EcKp4C…; 29 BTC at 1EcKp4C... (1 confirmation) moved from 1EcKp4C…; 1 BTC at miners address 14pP4zDq… as transaction fee reward moved from 1EcKp4C…; and 50 NEW BTC at miners address 14pP4zDq… as mining block reward) +
Solved HASH of Block two

A real world example of a 'Solved HASH of Block #593468' of the bitcoin blockchain is shown below (it is a hexadecimal base-16 number containing exactly 64 characters):

00000000000000000014fcb29e6e3b0ead3bd2e307d7f619a935f1d5323e9013

There is a lot more to all of this but this is the gist of what bitcoin mining and solving blocks involves. The entire system has been designed to be very secure and very stable and has been in continuous improvement since it started. A point to highlight is that only so many bitcoins can be added at a certain time and the rate of new bitcoins that can be added is halved about every four years. This is where bitcoin's programmed scarcity comes from and is a major reason why it is so valuable. There will only ever be a certain maximum number of bitcoins on the planet

and never anymore. The total number of all the bitcoins in the world is currently over 87% of its maximum possible number.

A FINAL LOOK AT TRANSACTIONS

When a transaction is created, the software you use will do a number of things. The most important of these is that it will sign the transaction with the bitcoin private key and then it will broadcast the transaction to the network.

The way your computer proves to the network that you are the rightful owner of the bitcoins stored at a particular bitcoin public address is by using one way hashes together with your bitcoin private key. And it does this without revealing your bitcoin private key to anyone except yourself.

To picture how this is possible, simply go back to our previous example of how your bitcoin private key was hashed to create the bitcoin public address. Now instead of:

Random number > then creates Bitcoin private key [then uses one way hash] > to create Bitcoin public address

We simply add ONE more hash step in between the bitcoin private key and bitcoin public address so that we have:

Random number > then creates Bitcoin private key [then uses one way hash] > ***to create SIGNATURE [then uses another one way hash]*** *> to create Bitcoin public address*

Now it is possible to show the network your SIGNATURE without revealing your bitcoin private key while still proving that you are the owner of the bitcoin private key. In practice, there is more to the signing process (such as public keys), and each signature will only work specifically to a particular transaction you have created, but you get the idea.

As soon as you have created the transaction and the bitcoin network has checked that it is valid, your transaction will enter the mempool in order to be picked up by a miner, and then eventually added to the next block of the blockchain.

Bitcoin transactions therefore can happen securely and discretely, with no need for you trust any particular third party (such as banking institutions). You only need to trust that your own creation, storage and transaction steps used to create and send the bitcoins were secure; and that the network of miners maintaining the network will continue to mine new blocks the way they have always mined them since the very beginning.

Slight inaccuracies explained:

* The actual random number only needs to be between 2^{128} (2 to the power of 128) and 2^{256} (2 to the power of 256) to meet unbreakable cryptography standards. This is roughly equal to a number containing between 39 and 78 numbers (decimal numbers).

** Not every miner who takes part in the bitcoin network needs to be highly invested. Many smaller miners who work as part of a larger mining pool have not necessarily spent huge amounts of money on their equipment. Many mining groups however are heavily invested and they are located all over the world.

*** The real bitcoin blockchain was originally mined mainly by its creator/s (Satoshi Nakamoto) for a period of up to 12 months before any significant number of other participants joined the network. The first block was mined on the 3 Jan 2009 and the first open source bitcoin client (or program) was released to the public on the 9 Jan 2009. The first bitcoin transaction was made on the 12 Jan 2009, about 10 days after the first block was mined. The huge majority of the estimated 1.6 million or so bitcoins which was mined in 2009 have never been moved and it is believed that the private keys to these have been lost.

**** The way the actual bitcoin mining difficulty is set is not by requiring the hashed number such as 000000000000000000014fcb29e6e3b0ead3bd2e307d7f619a935f1d5323e9013 to have a certain number of consecutive zeros in front of it, but for it to be smaller than a certain number that happens to have a lot of consecutive zeros in front of it. So for the above example, the hashed number might just need to be a number smaller than say 0000000000000000001500000000000000000000000000000000000000000000. Because of this, the difficulty can be set quite precisely.

Colour scheme explained:

Green text = real world examples of bitcoin public addresses, private keys and hashes

Blue text = made up examples of bitcoin public addresses, private keys, hashes, names and blockchain data used to make explaining how bitcoin works easier to understand

DISCLAIMER

The information presented in this document is presented as is, purely for information purposes. The authors and anyone involved in the making of this document accepts no liability whatsoever for any circumstance that may arise out of the information provided. We recommend the reader take personal responsibility and do their own research on the appropriate subjects.

*****Go to www.bitgoldwallet.com for information on what bitcoin is and how to safely buy, use and store it, and how to choose a secure and memorable password*****