BITCOIN : An Electronic Payment System, detailed explanation.

<table>
<thead>
<tr>
<th>1. What is it</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Overview</td>
</tr>
<tr>
<td>3. Controlling Money Supply</td>
</tr>
<tr>
<td>4. Robocoin</td>
</tr>
<tr>
<td>5. Suggested Readings</td>
</tr>
</tbody>
</table>

What is it?

An electronic payment system/ virtual currency system which means it is just a vehicle or conduit by which two parties transact over the internet.

Ex. A paying → B (over the internet)
Transaction between A and B amounts to a specifically constructed sequence of numbers which A will send to B.

Sequence of numbers has some mathematical properties which makes it hard for someone to conduct any fraud on system as it is cryptographically done.

Payment options under Bitcoin [Both the parties/users should have at-least one of them]:
1. Installing a software known as “Bitcoin Client” on the respective systems.
2. Third Party Service which may handle the transactions on behalf of users.

In return of the payment made by A, B can use the bitcoins to buy something over the internet or can get them converted into cash.

Question #1. Why would B wants to accept bitcoin (after all it’s just a sequence of system generated numbers)?

Answer: Bitcoin Exchanges: Places where bitcoins can be exchanged for cash/currency.
Ex. Mt. Cox where bitcoins can be sold for Euro/Dollar/INR etc.

Presently 1 Bitcoin is of around 780 US Dollar, but this value is fluctuating because it’s a new currency. As and when it gets more prominence in the market and is used more widely its value will tend to stabilise.
Question#2. Why not use other similar platforms like Paypal or E-cheques?

Answer: There are few better properties of Bitcoins over other platforms like:
   1. Privacy
   2. Open to All
   3. Decentralised

**Privacy:** Within Bitcoin network people can trade without actually disclosing who they are in real lives. (Remember it is just a sequence of numbers that will work as a pseudonym for A)
It is just like cash where nobody needs to disclose identity (ex. bank account details), unlike in other options like paypal or e-cheques where one needs to tie bank account details while transacting.
**Benefit over other platforms:** This property of Bitcoins is hugely beneficial to people who wants to buy commodities without disclosing the amount they have spent on it. (As bitcoin network allows you to deal with your sequence of numbers so generated not the name or any other details)

**Open to All:** Anyone with internet connection can get involved with Bitcoin network.
All one needs is to either download “Bitcoin Client” or use a Third Party Service like Mt.Cox which manages all the mechanics of the behalf of the user.
All details relating to the transactions are are open and quite clear to the users, the users just needs to enter the amount they want to transfer and the software takes cares of the mechanics involved.
**Benefit over other platforms:** If one wants to deal in electronic payments, typically one needs a Debit or Credit Card and a bank account whereas Bitcoin Network eliminates that too.

**Decentralised:** When A transacts with B over the bitcoin network that transaction won’t go to any other party like a bank or some other authority.
Therefore no one entity can control the money supply in Bitcoin network & so no one can reverse the transaction and transfer the sum to some other person’s account.
**Benefit over other platforms:** Traders who do not undertake online trade due to fear of online frauds can be assured of no frauds as bitcoin network makes it very hard to reverse the transaction.

Demerit of decentralisation: A central authority like a bank performs a very crucial role like validating the currency or transactions against fraud, so bitcoin is left quite vulnerable in this regard because of the absence of a central authority.

**Overview**

Two important features about bitcoin are that:
1. Bitcoin network is decentralised: Also known as Peer to Peer network (P2P)
2. It is sometimes referred to as Crypto-Currency: Being a network of just individual hosts, it involves a lot of cryptographic techniques to make it secure & safe.
Bitcoin can be compared basically to some sort of a global ledger.

For example:

A possesses 50 bitcoins with himself and he wants to transfer 30 of them to B and just like cash he transfers 50 coins to B and in return gets 18 back from B (2 coins being the transaction fee, to be discussed later in this article).

When A wants to transfer the bitcoins, he will have to apply digital signatures to the transaction. Digital Signatures are mathematical of tradition signs in a cryptographically strong way.

After the transaction is done from A’s side it will broadcast the details of the transactions to all the nodes in the P2P network known as **BITCOIN MINERS**.

**Question**: Why does he need to broadcast the information?

**Answer**: Because when B receives the information of the transaction, he might want to check some things before he accepts the coins like

1. If the numbers are quoted correctly
2. If they have been transferred to someone else too in the given course of time. (Because it is easy for a user to just copy the numbers and use them elsewhere too). This concept of A trying to spend coins twice in context of the digital cash is also known as **DOUBLE SPENDING**

So in order to have a mathematical assurance of the bitcoins and to avoid Double Spending, specific nodes in P2P network called the **bitcoin miners** plays an important role. They note down all the transactions (as every transaction is broadcasted) and compile them into a **TRANSACTION BLOCK** which is nothing but recording of all the transactions broadcasted.

So we can say that a single transactions is like → one ledger item

& a **Transaction Block** is like → an entire ledger page.
Bitcoin Miners also include a special transaction in the transaction block for themselves for the effort of doing this mining & so include a specially crafted sequence of numbers associated with the transaction which is called **PROOF OF WORK** in return of what they charge a **TRANSACTION FEE**.

The **proof of work** adds to the security in the network as it becomes very hard for a fraudulent activity to influence the network of bitcoin.

Transaction Block also contains encoding of previous Transaction Block which results in a chain of transaction blocks known as **TRANSACTION BLOCK CHAIN**.

**Question**: Why maintain Transaction Block Chains?
**Answer**: It will broadcast details of chains to all nodes/bitcoin miners and once a chain gets verified the miners take anything that hasn’t been processed and generate proof of work.

**NOTE**: The whole process of maintaining transaction block chains and generating proof of work is a decentralised process.

**Things to remember**:
- Transaction Block Chains
- Proof of work
- Transaction Fee
- Bit Coin Mining
- Double Spending

**Controlling Money Supply in Network**
Question: Is there an upper limit to Bitcoins Money Supply?

Answer: Yes, the Bitcoin Network is actually designed to so that there can be maximum 2,10,000,000 (2crore 10lakhs or 21 Million) Bitcoins ever generated in the system.

So some steps are required to check the money supply of bitcoins.

**Fractional Coins**: The Smallest possible unit for a bitcoin can be 0.00000001 Bit coin which is also known as a Satoshi which comes from Satoshi Nakamoto, a pseudonym for the inventor of bitcoin network (which is not necessarily a name of an individual)

**Reward Structure is decreasing**: When the bitcoin network was invented in Jan 2009 the reward which the miners got for generation of a transaction block was 50 bit coins.
And the current reward is reduced to its half as 25 bit coins.

So continuing with this pace it is estimated that approximately it requires 4 years to generate 2,10,000 new blocks (as generated from 2009 to 2013).
And it is assumed that for every new 2,10,000 new blocks the reward would be reduced to its half. And so the entire supply of 2,10,00,000 bitcoins would end by the year 2140.

**Robocoin**

The world’s first Bitcoin ATM machine which can transact digital currency – Bitcoins -for any official currency has been unveiled in Vancouver, Canada.

The ATM named Robocoin allows users to buy or sell the digital currency. The ATM in Vancouver is operated by Las Vegas-based Robocoin and Vancouver-based Bitcoiniacs.

**Suggested Readings:**

