Getting started with Blockchain: -

Chapter 1: - Why it all Started

“*A lack of transparency results in distrust and a deep sense of insecurity*.”

More important than learning about any technology or working on any project is its, ***why?***

When the reasons are clear we tend to learn fast.

So, A proper Financial system started around the ***3000 B.C*** when *Chanakya* an Indian mentor and guru created a system of first documented accounting system. That was the Single Ledger system. This system did fine, up until the *1600* A.C. when trade was mostly national, and no international business or routes were laid. Then the mankind took a leap forward we started exploring. *Columbus* started exploring the Central and South American coasts. Trade started between nations and sea routes were developed.

It was the time a little distrust among the people arose. Let us say that England had to do business with France, so one ledger system fails here as there is no central authority between the England and France. They both were separate identities.

This was the time when Double ledger system developed by Romans in 70 AD “***Tabulae Rationum***” come into the action. This system kept two separate records one for disbursements and other for the receipts, and trade went fine till the day both these match and people knew something is missing on ledger mismatch.

Then the Blockchain come to life when in *1992* *Haber*, *Stornetta* and *Dave Bayer* theorised the ***Merkle tree*** and incorporated it to the designs. Although, the first blockchain was incorporated by *Satoshi Nakamoto* in *2008* in the form of a digital currency called ***Bitcoin***.

Well, I assumed here that you know Bitcoin and Blockchain are different. If not, it is not an issue, we are going to discuss it in detail in upcoming chapters.

This is not a theoretical only textbook but still to clear all the terms and better understanding definitions are provided for important terms.

“*Blockchain is a digital record of transactions that represent the trade of underlying asset which can be anything from a cryptocurrency to the land or hospital records, all of which are on a peer-to-peer network that can either be public or private*”.

You may not understand it completely though it is indeed the best how blockchain can be defined.

So, the concept of blockchain was there from the *1992* but was only came into light or used for the real-life products after the success of Bitcoin. The first and most powerful blockchain built yet. At the time I am writing this book cost of *1 BTC* is up to *$34000* *USD*.

Now, let us have a look at some of the problems we have without blockchain. Or some of the ideas where you can work on using blockchain.

***Problem 1. Identity Theft: -*** *What is your identity*?

It is nothing more than a collection of claims regarding you as a person. This includes data on where you live, your passport number, driving license, social security number, and so on. All these are data points that are used by governments and stored in centralized databases.

And this gave birth to many problems like carding and bank frauds. 96% of the internet is operated using *Onion* and *Darknet,* so can you really trust someone with their identity whom you just met online minutes ago.

Well, don’t you feel the need to do something about it?

**Problem 2: - Cross border payments.** Have you noticed the costs?

So, you are based in Australia and did a business with a Canadian. Let us say you sold a wooden artifact for $100. Now your government would want a piece of this and take it as sales tax. In the meantime, the Canadian started the money transfer. Now there is a transaction fee of 2-3% that too with gross conversion rates. So, pick up a calculator and just do a paper transection that how much you lost in the process of selling. Just because there is trustable centralized authority in between does not mean you should pay around 15 % to sell. The problem is you do not trust the person on other side and the same goes with the other side.

Well, can we establish trust between them?

**Problem 3: - Unfairness in E-sports and Digital Copywrites.** Well have you wondered if algorithms behind those E sports are truly fair, or any course, art, work you publish is secure on the internet?

Well, I can neither confirm or deny my access to some of most famous and costlier courses on internet for free, just because they were not safe enough to protect them from cyber thefts. But with blockchain we can create a private network where no one can enter without a key. That key can be a transaction ID, in this way your work will never be stolen from the web again.

There are still many cons in our current system I can go on, but I must discuss solutions not problems.

***Features of Blockchain: -***

***1. Immutability: -*** “Once written on blockchain can only be changed by wrath of God”. Well, its just a saying but it is true to its core. Once a transaction or any asset is transferred on the blockchain its record is immutable It can not be undone or changed. Let us say Rohit and Kevin made a deal and to witness there was one man Peter. Now after deal Peter gets greedy and take money from Kevin to betray Rohit. What can Rohit do in this case? Or they could have announced the deal on the newspaper, so now the whole city knows about it and it cannot be changed. Same is the deal with the blockchain once a transaction is done whole network knows about it and it becomes impossible to change.

***2.*** ***Faster Settlement: -*** On Blockchain you can close a deal with proper work and trust in seconds where as conventional paperwork can take days to do the same. That too at highly reduced rates of the transactions.

***3. Security: -*** There are many systems in blockchain that makes the network essentially unhackable. Why does hacker’s hack? To steal data: - Not possible only nodes can access it. That too hashed in the SHA-256-bit encryption at least and several other hashing algorithms. What else anyone would want to access your system? To change data: - Not possible theoretically we need the 51% of the total computing power of the whole network to change it.

In the case of the bitcoin, it would be more power then all the supercomputers on the world working combined. Thus, making it practically impossible to do so.

***4. Decentralized system: -*** Are you obsessed with the fact that a single person (CEO) has all the power as what to do with your data in an organization. Well, this is not the case in the blockchain. A coder or the initiator may define the set of rules, but data and the controls will not be in hand of single person. Every member on the node is equally responsible for the data and integrity of the code.

I believe its enough to understand why blockchain is needed and what its true potential is.

We will start with the algorithms and deep concepts in the upcoming chapter but first we need to see a few things. Difference between the blockchain of the Ethereum and Bitcoin. Some terms that will be frequent like Gas, Nonce, Hash, Keys, Wallets, UTXO’s, Cryptography and many more. The fun is just beginning. Let us dive deep into the network and learn.