BLOCKCHAIN TECHNOLOGY

Welcome to the decentralized world.

You have probably heard the term blockchain. There is a lot of buzz around this technology.

Let us attempt to understand its concept.

Blockchain is a technology.

It's not a piece of software.

It's not a single device.

It's a technology concept.

WHAT DOES THIS
TECHNOLOGY DO?

This technology changes the way we maintain our ledgers.

We seldom realize how important ledgers are to all of us.

If you have to name one thing that allows our species the capability of dominating this planet over other members of our animal world – it is the ledger.

Exactly, that is how important ledgers are.

Let's elaborate.

LEDGER
MAINTENANCE

Human society is a transactional society. We use our skills, in our competent areas, to create a surplus which we trade with other members of our society.

To maintain a balance in this trade or transaction – we keep a record.

This record is the single source of truth about our transactions which is used to settle our dues with other members, continuously.

We all trust this ledger therefore can go about doing our work in a better manner.

Now, if we all keep our own ledgers, we all will be kings, right?

But then, we will always end up fighting other similar kings claiming their ledgers to be correct.

So, as a responsible society, we gave up the job of maintaining the ledger to a single trusted third party whose job is to keep a record of our transactions on our behalf.

Whenever we need to settle between ourselves, we ask that guy to check our ledgers, tell us who needs to pay whom how much and we agree to whatever he says – because he had promised to be fair to all of us.

We all use and follow the authority of the trusted third party over our ledgers - we call them by several names through the course of time - chieftain, pharaoh, Maharaja, Samrat, etc.

They appointed other guys – some recording cash transactions, some recording land properties, some recording births and deaths, etc.

Everyone busy maintaining the ledgers for us.

Then the computers came, internet happened, networks were established and human society went on researching further into what technology can do for society.

Several baby steps were taken in technology leading to implementation of the Blockchain technology.

Perhaps, unknowingly of how this was going to be used in the future, in 1982 – David Chaum proposed a solution to the question that can technology be such that – mutually suspicious participants maintain a computer system among themselves without cheating each other? His system could do exactly that.

Then, in 1991 – Stuart Haber and Scott Stornetta proposed a technology to time-stamp digital documents in a tamper-proof manner!!!

The very next year, in 1992, the same duo along with Dave Bayer demonstrated how smartly Merkle Trees can be used to store the information of several documents – in such a manner that the documents would be immutable – cannot be changed!!!

In 2004, one of the most notable contributors to this technology – Hal Finney introduced a system called Reusable-Proof-of-Work to maintain the ledger without involving any trusted central third party.

With this system – we were inches close to the technology we now know as blockchain – but notable attempts – Nick Szabo's Bit Gold, Wei Dei's b-money all suffered the problem of not being able to solve the problem of "DOUBLE SPENDING".

Double Spending is a problem where a digital coin is incessantly copied and used over and over again giving unfair advantage to the issuer and pumping inflation into the system. Big Problem!!!

Then, in 2008 – an unknown Cypherpunk – who called himself/ (herself/themselves) Satoshi Nakamoto published a modest looking 9-page concept note called 'Bitcoin: A Peer to peer Electronic Cash system'.

He had used Chaum's Uncheatable Network systems, Stornetta-Haber's Timestamping, Stornetta-Haber-Bayer's Merkle Trees, Finney's RPOW – tinkered with them smartly and Bang!!! – created a system which took the imagination of the world by storm.

Today – it is known as the Blockchain Technology.

WHAT DOES BLOCKCHAIN TECHNOLOGY ACTUALLY DO?

It creates an uncheatable system, which can be used by people to record transactions among themselves without requiring a trusted third party.

The trust has shifted from the Kings and their men to the cryptographic proof that the transaction is valid!!!

That is the BIG DEAL – that is blockchain for you.

Disrupting the entire system as we know it – as we have become habituated to.

The cost of recording these transactions were sky-rocketing – as economic activity expands, the number of transactions go ballistic – so workload becomes heavy and they charge us more.
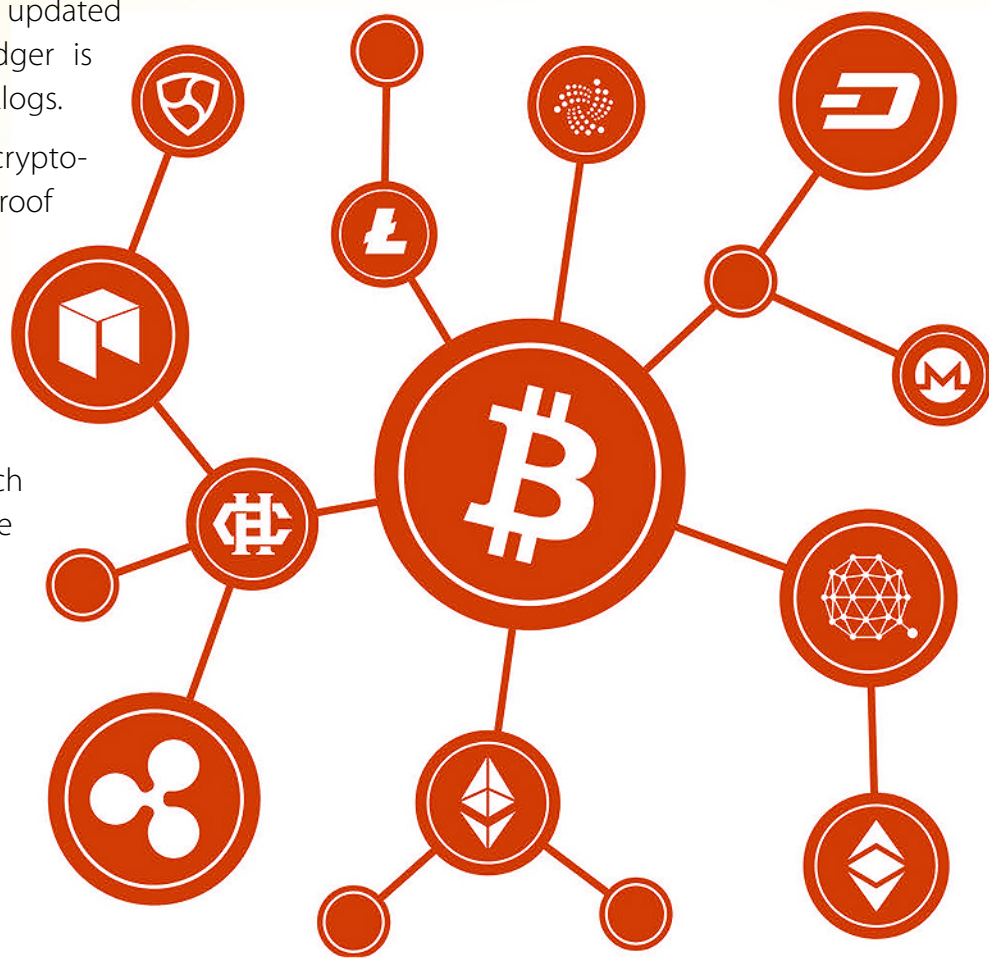
In a system without them, we do the record of our transactions all by ourselves - which keeps the costs down.

The cryptographic trust comes from everyone having the same ledger with themselves – so, transparency of the system improves.

The ledger has a copy with each participant – which needs to be simultaneously updated – which means that this ledger is always up-to-date – zero backlogs.

The transaction records are crypto-protected to be hack-proof – making these ledgers immutable – tamper proof / non-changeable.

The system necessitates a consensus within the group of participants – which makes everyone equal and the system remains fair for every participant – egalitarian!!!

Also – it makes the system safe – any one bad actor cannot hack the system – he needs more than half of the community to agree on his ideas!!! And even if someone hacks into one ledger, the community will find out the one single which is different from others – which means – the hacker will have to hack every copy of the ledger which is with everyone in the community.

So, a system – which is low cost, hack-proof, transparent and uncheatable was created by Satoshi – this is the technology which is today known as Blockchain.

In its improved form using Smart Contracts to do Smart Business and disrupting almost all sectors of business and life in general.

One final and very important point – **Bitcoin is not Blockchain**

Bitcoin is the first application of Blockchain Technology.

Also, you'll be surprised to know – Satoshi Nakamoto isn't credited to be the creator of Blockchain – It is Dr. Scott Stornetta who is popularly known as Father of Blockchain!!!

We hope this helps you understand the concept about blockchain technology and renders some context to how it is going to impact your life, business – everything.

For more details you can always check out our numerous programmes on Crypto University.

cryptowire ™

Knowledge, Information and Data Platform

www.cryptowire.in