A Talk on

Web 3.0 : Bitcoin, Blockchain, Cryptocurrencies

"A **NEW** Decentralised Internet"

Friday 4 pm, 16th March 2018

Speaker : **Abhijit Roy**

Venue : Seminar Hall

Web 3.0 : Bitcoin, Blockchain, Cryptocurrencies

"A NEW Decentralized Internet"

Speaker : **Abhijit Roy**

Block.Hub

Questions ?

- Why Cryptocurrency is required ?
- What is Bitcoin ?
- What is Blockchain Technology ?
- Why so many cryptocurrencies ?
- What are the applications of Blockchain Tech. ?
- What's Govt's opinion on Blockchain technology ?
- The Future of Blockchain technology
- So on….

Why Crypto? - Fiat Currency problems

- Cash is not tamper-proof.
- Printing more currency is in the hands of Govt.
- Using money in form of digital wallets is not safe – Paytm, Olamoney, etc.
- Banks involved in Fraud, Loans are not recovered. Hence, become 'Bad loans'. Actually, any bank can modify the past record of loans.

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for

What is Bitcoin ?

- History → introduced after 2008 financial crisis
- A peer-to-peer cryptographic digital currency.
- The protocol is like **BitTorrent** i.e. decentralized. But no incentives for File upload (seeds) or staying as a live node.
- Consensus Algo. → Proof-of-work (PoW) introduced.
- PoW → Group of nodes competing against each other for getting the authority to validate a block of transactions.
- The node who validates a block, gets a reward in Bitcoins plus Tx fees. Currently, 12.5 B + 1.5 B = 14 B

PROOF OF WORK

How Bitcoin's total supply is 21 M ?

- Different rewards for different span of years. Reward gets halved every 4 yrs or 2,16,000 blocks.
- Puzzle solved every 10 minutes, otherwise difficulty level adjusted (↑ or ↓)
- 2009-2012(June) : 50 Bitcoins
- 2012-2016(June) : 25 Bitcoins
- So on….

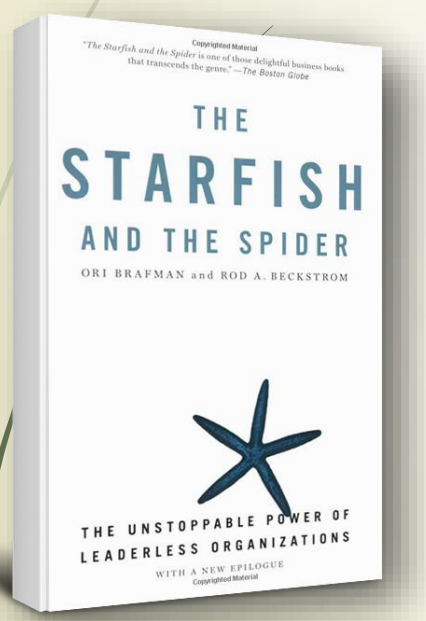
$$
\begin{aligned}
&(50*6*24*365*4)\\
+\ &(25*6*24*365*4)\\
+\ &(12.5*6*24*365*4)\\
+\ &(6.25*6*24*365*4)\\
&\vdots\\
+\ &(10^{-8}*6*24*365*4)
\end{aligned}
$$

= **21 millions by 2140 yr**

Bitcoin Facts

- 1st purchase– 2 pizzas bought using **10,000 Bitcoins**.
- ***Satoshi Nakamoto*** holds (mined) 1 M Bitcoins (5 % of total supply).
- CPU → GPU → ASIC (customized according to the cryptographic hash function).
- Currently, **16.5 M** bitcoins already mined.
- Electricity usage for a single Bitcoin block = Electricity spend in a city on a day.
- Tx speed → max. **3-5 / sec**. Not matching the VISA/Mastercard capacity (min.1000 txs/sec).
- **Problems** - Network slow, High Tx fees (by miners), Huge energy consumption.
- **Solutions** – Lightning, Segwit2x, etc. proposed.

What is Blockchain ?



'Star fish & Spider' analogy for Decentralized & Centralized organization

Features

- Shared-database (distributed).
- Multiple nodes involved keeping record of all kinds of data – Txns, text, image, video, any format.
- Unlike BitTorrent, nodes are incentivized.

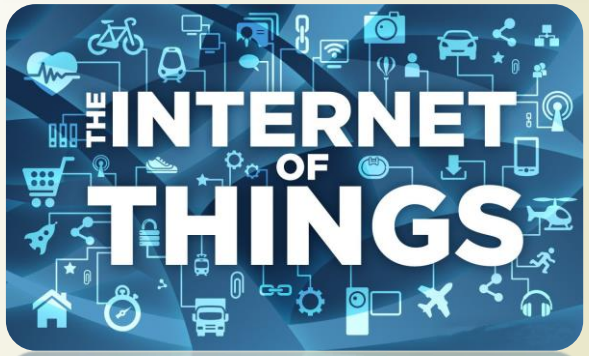
Blockchain's Use cases

- **Banking & payments** → Blockchain actually banks the unbanked, requires a smartphone & internet. That's it!!..

- **Cyber security** → Highly secure due to its decentralized & immutable nature.

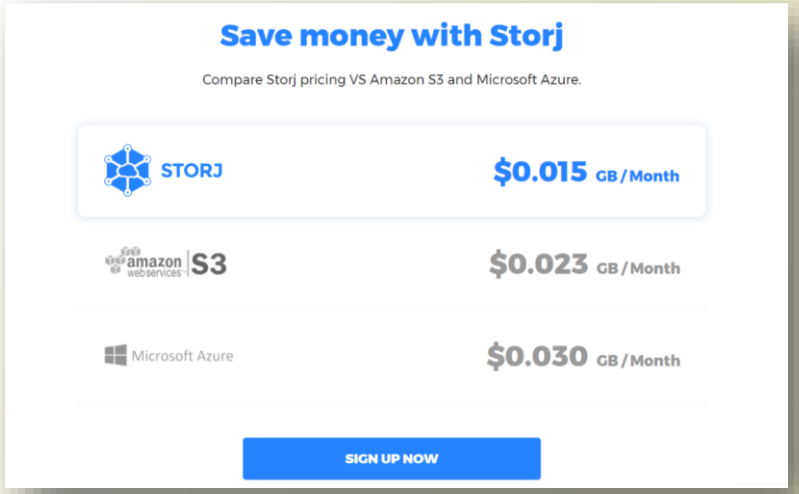
- **Supply Chain management** → Real-time tracking of goods & services using immutable record i.e. Blockchain.

- **Networking & IoT** → Samsung & IBM want to connect devices (car, household items – refrigerator, etc.) in a peer-to-peer way using Blockchain tech.



- **Private Transport & Ride sharing** → decentralized UBER, OLA. Taking the fare down significantly by reducing intermediaries & associated fees. Automatically pay for parking, tolls & fuel. Startups - UBS, ZF & INNOGY

- **Decentralised Storage Networks (DSNs)** → Eliminating Goggle, Amazon, Microsoft, cloud services.



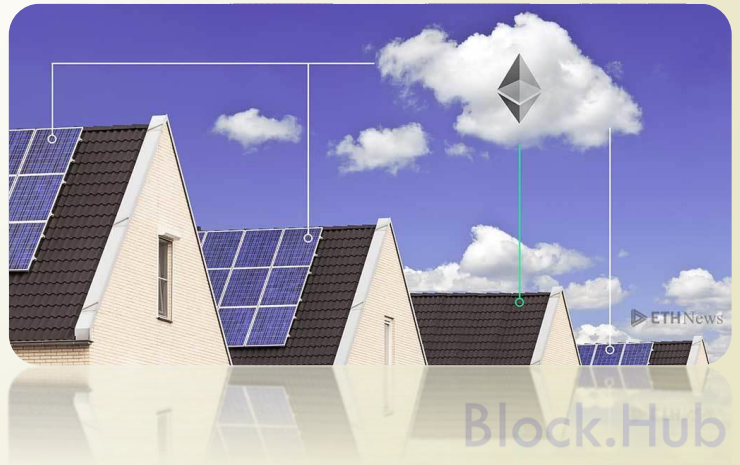
- **Charity** → people complain about inefficiency & corruption due to which the fund doesn't reach to those who are meant to have it. Blockchain shall allow to track donations to get where they're going. Startups- BITGIVE.

- **Voting** → use Blockchain for Voter registration, identity verification & vote counting. Hence, make elections more fair and democratic. Startups – Democracy.Earth, Followmyvote.com

- **Healthcare** → need a secure platform to store and share sensitive data. Blockchain technology safely store medical records & share them with authorized doctors or patients.

- **Energy management system** → highly centralized industry for a long time. People can't buy from each other. Instead they have to go through the public grids.

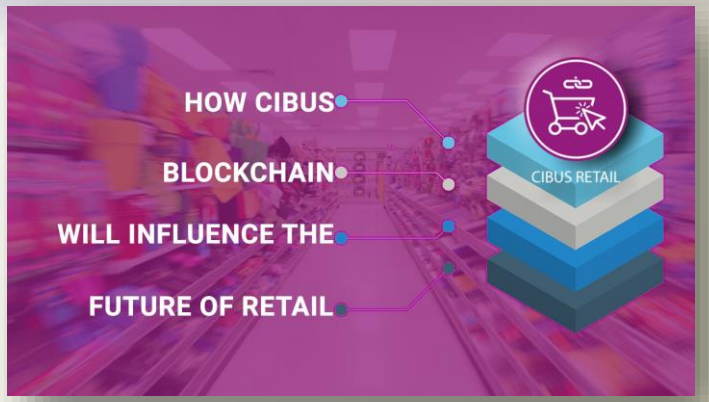
  Startups – TransactiveGrid (using Ethereum)



- **Music** → Blockchain startups are coming up with ways for musicians to get paid directly from their fans instead of paying to the intermediary record companies. SCs can solve licensing issues and catalog songs with their respective creators. Startups – Mycelia, Ujo music.

- **Retail** → Due to Blockchain tech - Better security, No fake goods, Lower costs, Greater speed.

Hence functioning w/o middlemen and associated fees. Startups – OpenBazaar, OB1



- **Real-estate** → Issues – bureaucracy, lack of transparency fraud, mistakes in public records. Blockchain can speed up transactions the need for paper-based record keeping. Also, tracking, verifying ownership, ensuring accuracy of docs, transferring property deeds (legal record). Startups – UBITQUITY.

- **Crowdfunding** → existing platforms take high fees. In Blockchain-based crowdfunding, trust is created through SCs removing middlemen. New projects can release their own tokens that can later be exchanged for products, services. E.g. ICOs

steemit beta

Trending | New | Hot | Promoted

All tags

life
photography
steemit
kr
art
busy
blog
introduceyourself
spanish
travel
bitcoin
esteem
steem
nature
cryptocurrency
story
funny
food
indonesia

Trending: All Tags

abrockman (63) in steem • 2 days ago

SteemSummer Tickets Now Available for May 25 to 27 in Palm Beach, Florida!

Imagine three full days of Steem in person. Rather than making your daily post onlin…

$682.04 | 969 | 277

chbartist (63) in life • yesterday

Building the road to success - Chapter 3

Hello Tribe of good intent On this chapter I would like to talk about the importance of…

$562.84 | 798 | 157

prameshtyagi (66) in bitcoin • 14 hours ago

All you Need to Know About Investing in Cryptocurrency in India

Image Courtesy - The Financial Express You call it a craze or simply curiosity, peopl…

$350.40 | 261 | 65

chbartist (63) in life • 5 hours ago

It's never too late

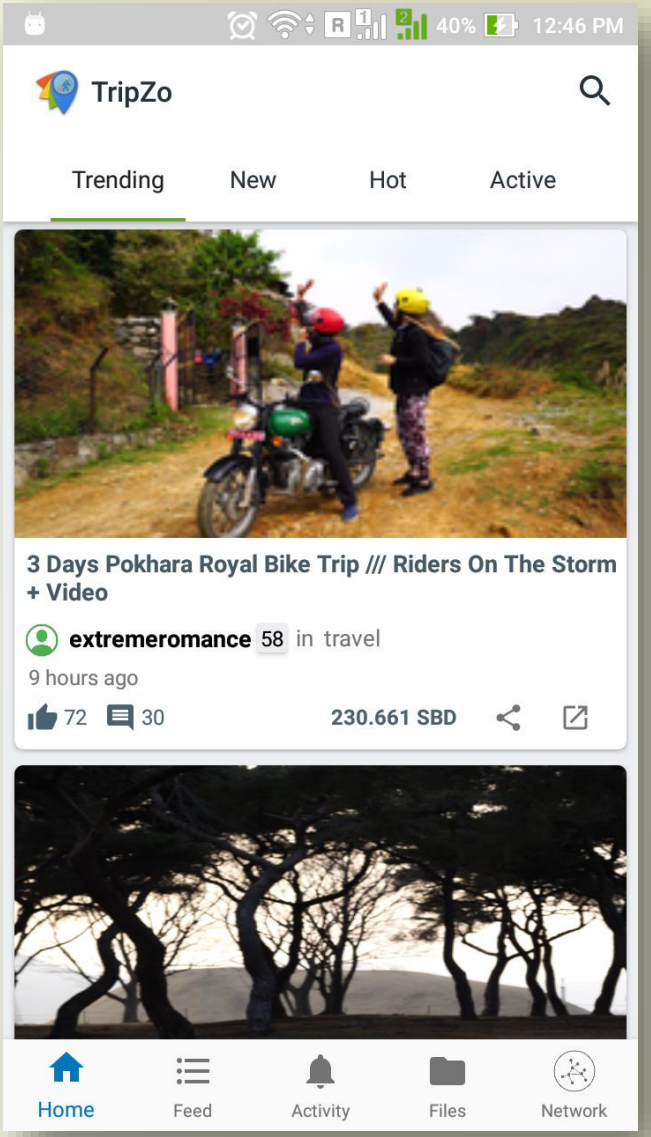
If you have ever felt like it's too late to follow your dreams, that it's too late to discov…

Links

My feed
My blog
My wallet

- **TripZo** - A p2p incentivized social platform for travel community.

- It's built over **Steem Blockchain**.
- Store files (photos, videos) in p2p platform.
- One can search for contents related to a place.
- People incentivized for giving information about places on Map, etc.



Block.Hub

Types of Cryptocurrencies

- **Payment tokens only** → Bitcoin, Litecoin, Dash, Dogecoin, Ripple, Bitcoin-cash, Bitcoin-diamond, etc.
- **Programmable Blockchain platforms** → Ethereum, Stratis, Nxt, Ethereum-classic, Lisk, Neo, Cardano, IOTA, etc.
- **dApps** → Lunyr, Steemit, Golem, Wings, Storj, Bancor, BAT, etc.

What is Smart Contract ?

- They are programs describing ‘set of rules’, stored on an account address.
- The program has built-in logic inside which is immutable once recorded in Blockchain.
- **Future** - There will be smart contract programmers, who will replace Lawyers (existing ones) because of the fact - “Code is Law”.


HOW WOULD A SMART CONTRACT WORLD LOOK LIKE?
Block.Hub

You want to buy a '*used car*'

You go to a dealer/individual to verify information about the car

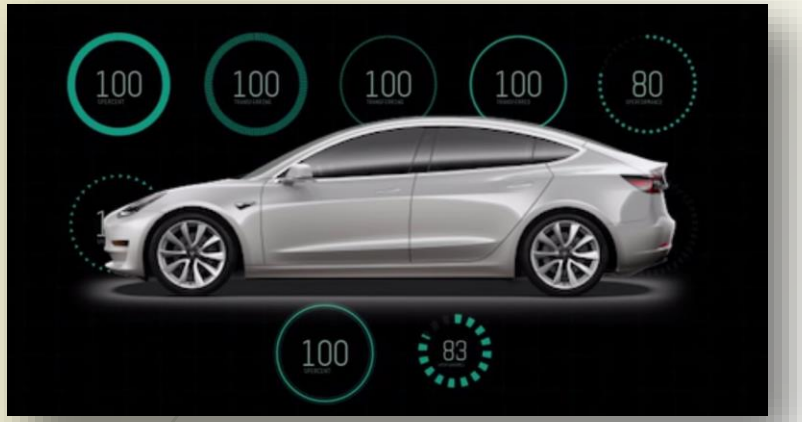
You do the payment and sign lots of documents, wait for the money to clear

Finally, you have the car.

This actually takes few days to do.

With Blockchain, using SC, you can have all these carried out in real-time.

Block.Hub



Seller would upload the car (sale, record) onto the Blockchain

the car's history can be verified using Blockchain record. And via SC, your payment is done using cryptocurrency

The car is now attached to owner using the Unique identity system.

And the information of the Car's current owner is updated

Blockchain's limitation

- Facing **scalibility** issue. E.g. – Bitcoin (3-5 txns/sec), Ethereum (15-20 txns/sec), Steem (10,000 txns/sec)
- Centralised entities' speed – Paypal (193 txns/sec), Visa/Master card (1000-4000 txns/sec), Facebook (50,000 likes/sec).
- Upcoming are Blockchains with **nearly 1 M txns/sec**. Shall arrive by this year 2018.

Which Blockchain platform will win ?

- Depends on network speed.
- **For developers** – Rewards and programming language available on the platform.
- **For users** - depends on number of Apps available on the platform e.g. Chrome.

Internet vs Blockchain

- Data Transport Protocol – Insecure & Secure.
- Internet of information | Internet of value i.e. assets.
- **Business Model** → Freemium (with Ads) vs Incentivized (w/o Ads).

Govt.'s stand on Crypto

- Indian Govt. has banned Crypto-trading officially. But, it supports the Blockchain technology.


In an interview earlier this month, KFTC Chairman, Kim Sang-Joo, stated:

> *"[Shutting down cryptocurrency exchanges] is not realistically possible. Based on electronic commerce law, the government does not have the authority to close down cryptocurrency trading platforms."*

And not just law, but the fact that it is so decentralized would make it virtually impossible. Many people would continue to use regardless, which the government is also surely aware of.

For Users

- Don't get intimidated by news saying "Earn in these cryptocurrencies to make your money multi-fold".
- Learn non-technical books on '*Blockchain',* if interested.
- Invest your money on real platforms (value-adding ones), not on fud coins because chances of success is less, but failure rate is very high there.
- Invest time on real platforms. Unlike Facebook, Quora, Reddit, try to explore Blockchain platforms – Steemit, Dtube, etc.
- Please change your thought to this i.e. "Whatever time you spend on, make some earning as well". Remember – "*Money isn't everything, but important*".

For Developers

- **Basics -** Learn programming languages – C++ , Java, Python, Go, ….
- Understand Blockchain architecture which is completely different than the traditional server-client model. Learning too much of cryptography is not required.
- If you are building Apps on centralized database, chances are that you are involved in something that is dated.

- **Quote** - "Do not build what you can build, build what you should build".

Future…

- of **Technology** – Blockchain & AI are the **Yin** & **Yang** of the Future.

- of **Jobs** – A Japanese concept called ***'ikigai'***. It means ***"a reason for being"***.

How the technology is relevant for SCL ?

- **Blockchain** - Upgrading the existing **server-client** data architecture to **Blockchain-based** architecture. No more Hacking issues. Options – *Private* (privacy) or *public* (transparent) Blockchains.
- **Data analytics** - Here, in FAB division, we have huge datasets getting generated everyday. We need real *data-analysts* (programmers) in huge no.
- **Artificial Intelligence (AI)** - Infact, there is a huge scope for *AI enthusiasts* for projects related to **"Image recognition of defects using AI models".**

“Let’s make the world Decentralized …..”

Email ID – dalvath3700@gmail.com

https://www.facebook.com/abhi3700

https://twitter.com/abhi3700

https://github.com/abhi3700

https://steemit.com/@abhi3700