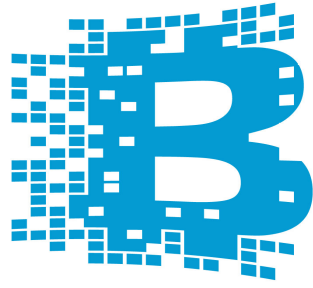# Blockchain
The future of Internet

Muhammad Moinur Rahman

moin@bofh.im

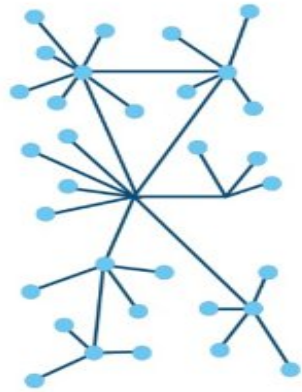Blockchain != Bitcoin/Cryptocurrency

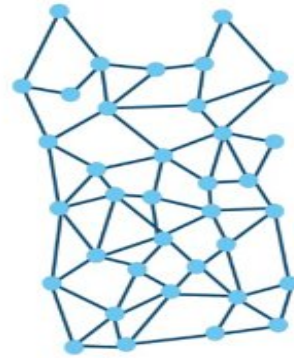# What is Blockchain?

- A distributed Database

- Decentralized

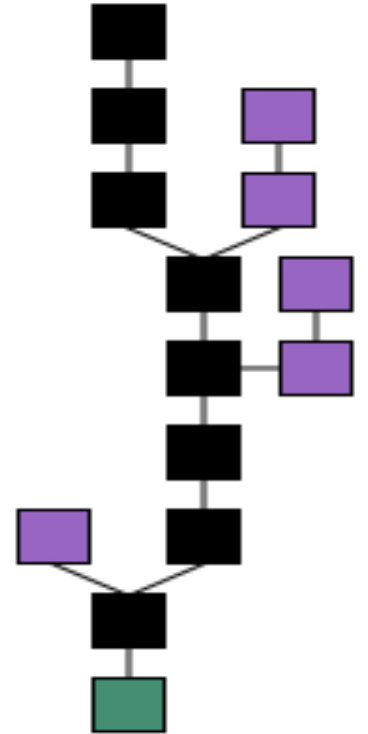- Mainly a list of always growing records

Centralized   Decentralized   Distributed
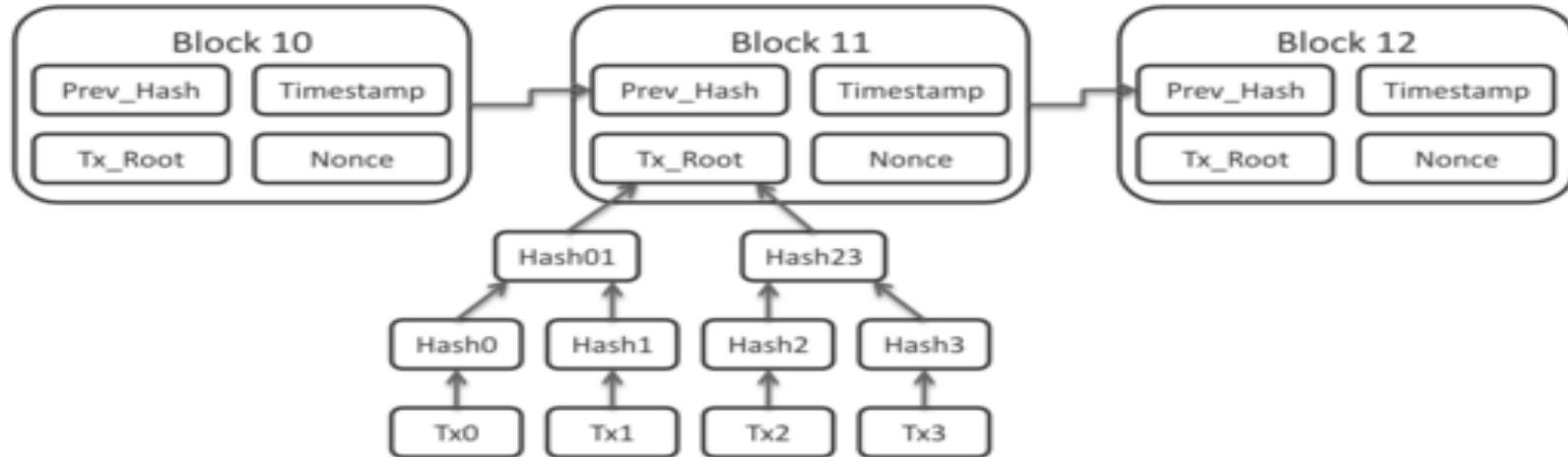
What is Blockchain? - Continued

- Tamper proof and Revision proof

- Open, permission less and public

- Byzantine Fault Tolerant

How Blockchain Works?

- A growing list of records called blocks

- Each block contains

  - A timestamp

  - A link to previous block

- Can be managed

  - Publicly or autonomously

    - Peer-to-peer network

    - Distributed Time-stamping

  - Privately

Uses of Blockchain

- Recording of events
- Medical Records
- Identity Management
- Transaction processing
- Documenting provenance
- Financial

- Marketplace
- Smart Contracts
- Digital Products Marketing
- Property Records
- Voting
- Cloud Storage

History of Blockchain

- 1991 – Stuart Haber & Scott Stornetta

- 1996 – Ross J. Anderson

- 1997 – Michael Doyle

- 1998 – Bruce Schneier

- 1998 – Nick Szabo – Bit Gold

- 2008 – Satoshi Nakamoto

- 2014 – Blockchain 2.0

Internet

- A 30 years old technology

- Based on IP routing and DNS

- Primary purpose was to share abundance of Data

- Now under mass surveillance

- Now censored by different governments to capitalize political benefits

- Always requires DNS information to make full

Internet

- Centralized by the so called ROOT DNS servers

- Secured by DNSSEC

- Web trust system is broken

- Under the control of around 1200+ CA

- Most of the https are weakly configured

- Prone to catastrophe, zombie apocalypse, alien invasion, Government shutdown

Words from ..

- "We didn't focus on how you could wreck this system intentionally," - **Vinton G. Cerf**.

- "I invented the web. Here are three things we need to change to save it
  - We've lost control of our personal data
  - It's too easy for misinformation to spread on the web
  - Political advertising online needs transparency and understanding" - **Sir Tim Berners Lee**

DNS

- A decentralized database maintained by root servers

- Secured implementation by DNSSEC(Hardly implemented by Domain owners)

- Web anchor of trust is based on CA(Run by large Companies, Controlled by Governments)

DNS in a Distributed Blockchain

- Censor-free

- Distributed, hard to knock down by a single attack or Government

- Supported by TOR or I2P

- Private

DNSchain - Implementation

- Namecoin – Bit DNS

- OKTurtle
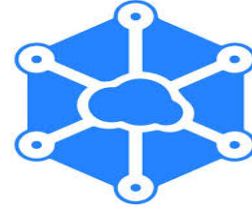
- Emercoin – EMCDNS

- And more ..

Data storage/Cloud Storage

- Privacy at stake for major Cloud Storage providers

- Personal information stored in clouds

- Accessible by Providers/Law Enforcement Agency/Governments

  - With Warrant

  - With Subpoena

- Ransomware

Data storage in Blockchain - Implementation

- storj

- sia.tech

Traffic Routing

- Always goes through an ISP

- Running Deep Packet Inspection

- National Firewall

- DNS Cache Poisoning

- Plain traffic is intercept-able

- Caching Data poisoning

- Comes with Privacy Demolished

Blockchain in routing(BGP) – What if

- Voting capability to avoid bad routes

- Overlay Network with Path Performance Computation

- A DHT maintaining RemyCC (Remy Congestion Control)

- Prefixes are added/removed/modified by DPKI

SDN in Blockchain

- SDN – Cutting Edge Technology

- Misconfigured Infrastructures by newbie uneducated engineers

- API/Programmability is vulnerable

- Flow Table can be modified remotely

SDN in Blockchain – What if ..

- Flowtable is maintained in a blockchain

- Modification of flowtable is authenticated against KSI(Keyless Signature Infrastructure) or DPKI

- Saving the events in a blockchain to track it down to its root

- Easier Log readability

- Authenticate agents, messages, control interfaces, devices, state of a service

IoT

- A trillion dollar Industry

- Billions of devices will be connected

- Interact in between them

- Going to be the most vulnerable systems from the prying eyes

- Decentralization is required, considering centralized infrastructure

IoT in Blockchain – What if

- Billions of ongoing transactions will be stored in blockchain

- Rather than centralizing the Data storage

- A single fail-proof network

- No MITM attack

- A single Tamper proof DHT(Distributed Hash Table)

- Blockchain is already a proven technology with billions of Dollar market for Cryptocurrencies

BlockStack

- Decentralized Internet

- A Full Stack of Apps

  - Identity

  - Storage

  - Payments

- With the possibility of

  - Decentralized Social Network

  - P2P Marketplace

  - Community Run Voting
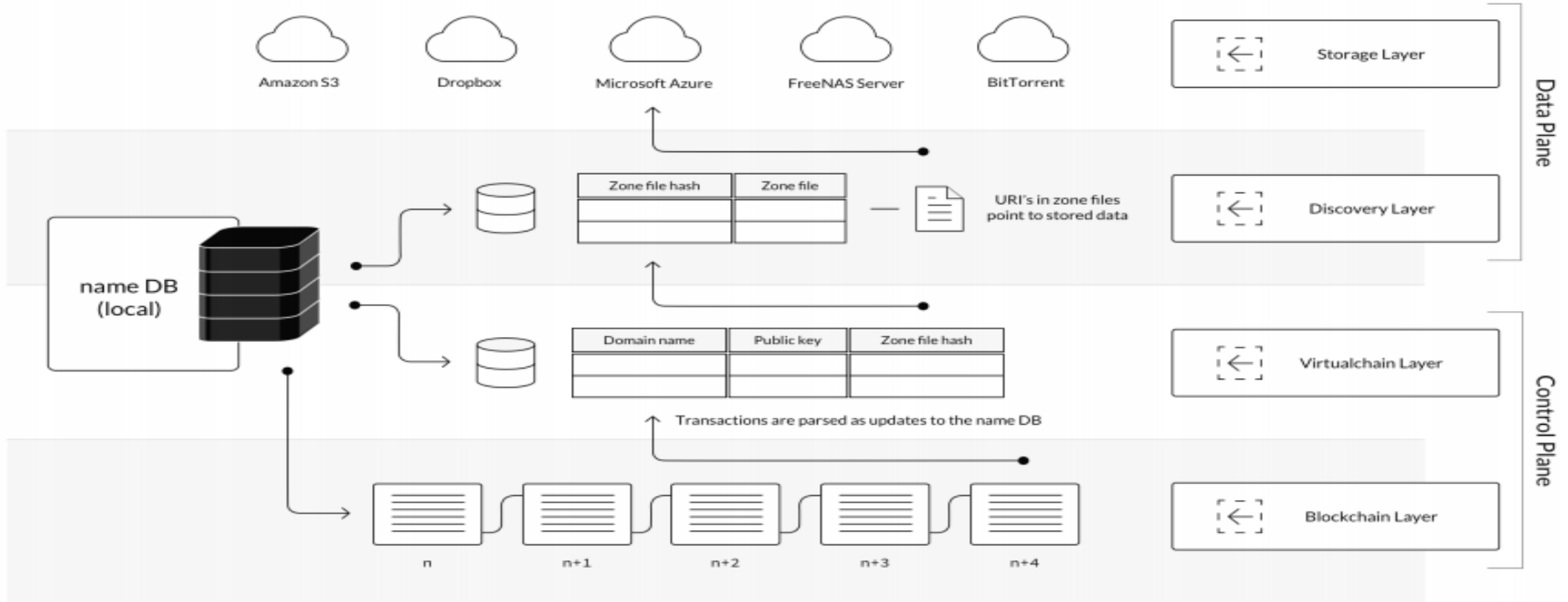
- Blockchain

BlockStack - Details

- Blockchain Layer

- Virtual chain Layer

- Discovery Layer

- Storage Layer

    - Any Cloud Storage Provider

    - Personal Storage at your bunker

- BNS

- ATLAS Network

BlockStack - Architecture

End Goal

- A Censorship free Internet

- Freedom of Speech

- Privacy in the Digital Age

Questions ..

- Thank you ..