APRIL 3, 2019

INTRODUCTION TO BLOCKCHAIN
A BEGINNER'S GUIDE

ANAND A

Intended Audience : Beginners to Blockchain

CONTENTS

SHORT DESCRIPTION

Procure a basic understanding on the concept of blockchain which is fast becoming the technology to go to in banking domain and general information integrity maintenance.

PREFACE

There are a lot of buzzwords fluttering about in the tech community like IoT, Blockchain, Digital, Automation etc. One of the buzzword which has the potential to become a practical real world application is the Blockchain.

Blockchain is a concept that was proposed by a person or persons going by the pseudonym Satoshi Nakamoto. This concept was first published in the whitepaper "Bitcoin: A Peer-to-Peer Electronic Cash System" in 2008.

> *The Blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value."*
> *Don & Alex Tapscott, authors Blockchain Revolution (2016)*

DEFINITION

By definition Blockchain is a decentralized, distributed and public digital ledger that is used to record transactions permanently across many computers so that the transactions cannot be altered, without the alteration of all subsequent blocks.

- A ledger is a record of financial transactions, which is used to prepare financial statements for the organization.
- A distributed ledger is one that is accessed or modified by multiple parties and is synchronized at any point of time.
- A decentralized ledger is one which is stored in multiple locations and is updated simultaneously.

Table 1: Example of a simple ledger

Date	Description	Debit	Credit	Balance
Jan. 10, 2018	Inventory - Storage	Rs. 17,000		Rs. 17,000
Feb. 20, 2018	Logistics		Rs. 12,000	Rs. 29,000
Jun. 1, 2018	Parts outsourced	Rs 22,000		Rs. 7,000

Since alteration requires consensus of the majority of the network, it is practically impossible.

Each block is linked to the previous block by means of a cryptographic hash which is irreversible. A timestamp and transaction data completes the structure of the block.

Blockchain was created for the cryptocurrency, Bitcoin, though the tech community is now finding other potential and perhaps revolutionary uses for the technology.

BLOCKCHAIN JARGONS

- **Node:**

The computer that is connected to the Blockchain network using a client that performs the task of validating and relaying transactions. Every node gets a copy of the Blockchain, which gets downloaded automatically upon joining the Blockchain network.

- **Block:**

Group of transactions is referred to as a block.

- **Smart contracts:**

These are contracts which execute when a certain condition is met. For instance, an incentive could be paid out when an investment instrument meets certain milestone.

- **Block time:**

The *block time* is the average time it takes for the network to generate one extra block in the Blockchain. By the time of block completion, the updated data becomes verifiable

BLOCKCHAIN SIMPLIFIED

Pre-requisites:

- In simple words picture a spreadsheet or ledger which has been copied multiple times across a network of computers called nodes. These nodes are facilitated to update and verify the ledger.
- The information is held in a shared and continually synchronized database. The Blockchain database is not stored in any one node but is hosted on all the nodes in the network simultaneously.
- The information is available and verifiable to all on the network. The network self-audits every 10 minutes. Every node has full copy of ledger.

Process Flow:

1. The process begins by broadcasting the transaction across the network.
2. Each node has an incentive of earning a certain amount of cryptocurrency for processing and verifying transaction.
3. However certain nodes are assigned as 'Mining nodes' which validate the transaction.
4. The transactions cannot be altered since it requires overpowering all the other nodes.
5. Once a transaction is updated and verified, it is grouped together with other transactions forming a block.
6. This is broadcast to other nodes in the network.
7. This block is finally added to an existing Blockchain indicating the end of transaction.

Note: There are no centralized "official" copy and every user is assigned equal trust.

Fig:1 Flow diagram indicating Blockchain transaction
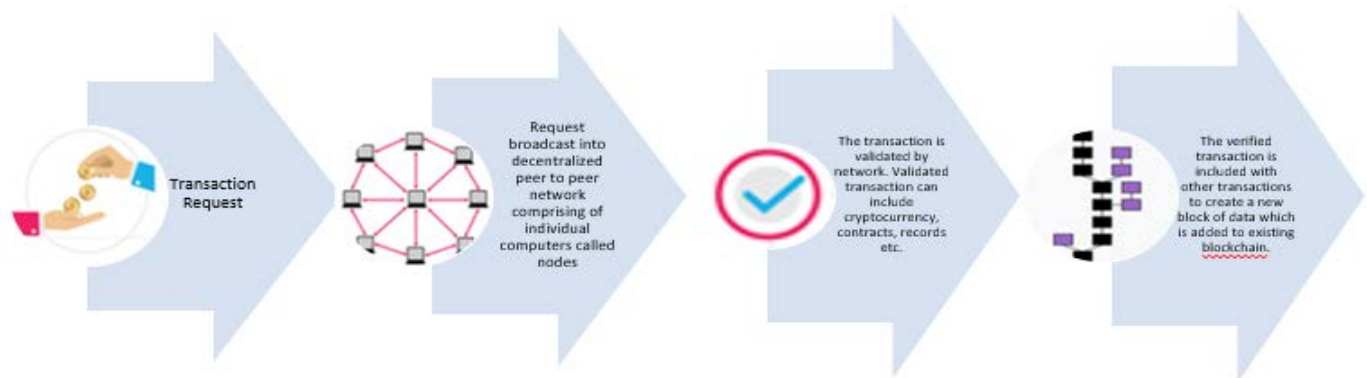
APPLICATIONS OF BLOCKCHAIN

- **Stock Markets**

Blockchain can deem interceders like clearing house, auditors and custodians irrelevant. Stocks can be bought and sold in a matter of few minutes as opposed to the current time consuming process.

- **Public record of land registry**

Blockchain can maintain property related records like Titles, Land Deeds and other transactions in a publicly accessible and tamper-proof manner.

- **Election**

Elections can be made fair and transparent since a vote once cast cannot be rectified and the public has full access to the results. Also if clubbed with identity management, multiple votes cannot be cast.

- **Insurance**

The insurance terms can be made transparent. This will eliminate any false claims and fair payouts. Payouts can be automated using smart contracts.

- **Copyright**

Blockchain enable creative content creators to monetize their efforts by automating payment everytime their contents are utilized.

- **Sharing Economy**

Users can directly interact with cab drivers or boarding partners thus eliminating aggregation.

- **Crowd-sourced Venture Capital Funds**

Users can participate in investing in an idea or a product

- **Supply Chain**

Blockchain enables the manufacturer, distributor, wholesaler, and retailer to be connected to the transactions between them. Smart contracts can make the payments automated while transactions can maintain its sanctity.

- **File Sharing**

Files can be stored in a distributed network ensuring robustness and easy accessibility.

- **Identity Management**

Blockchain enables users to store their digitized ID proofs making identity centric process easy.

- **IoT**

Internet of Things involve network-controlled management of certain types of electronic devices — for instance, the monitoring of air humidity in an irrigation facility. Smart contracts make the automation of these networks possible.

- **Medical History Management**

Blockchain can enable both doctors and patients to streamline treatment by quickly accessing medical history.

FEATURES OF BLOCKCHAIN:
- *Decentralized* – Since each node is an administrator
- *Robust* – Since there is multiple data replication nodes
- *Secure and incorruptible* – Since it lacks centralized points of vulnerability, transactions cannot be erased
- *Transparent* – Since it is a public ledger
- *Data integrity* – Since data quality is maintained by massive database replication and computational trust.

.

TYPES OF BLOCKCHAINS

Public Blockchains
A public Blockchain has absolutely no access restrictions. These networks hand out incentives to users who secure the network integrity.

E.g. Bitcoin and Ethereum.

Private Blockchains
A private Blockchain is the one where one has to be invited by network admins in order to be a member. It is generally used by corporates as an internal network.

Used by Banks

Consortium Blockchains

A consortium Blockchain is a network where there are multiple network admins. This eliminates any prejudicial entry.

CONCLUSION

Blockchain can become an all pervasive technology especially in the domain of finance. It can become the next internet comprising of highly secure information highway.