

# Introduction to Blockchain Technology

**Vinod Nigade**

Software Engineer

15<sup>th</sup> September, 2017

# Outline

- 1 Introduction
- 2 Background
- 3 Blockchain Technology
- 4 Miscellaneous

## Bitcoin

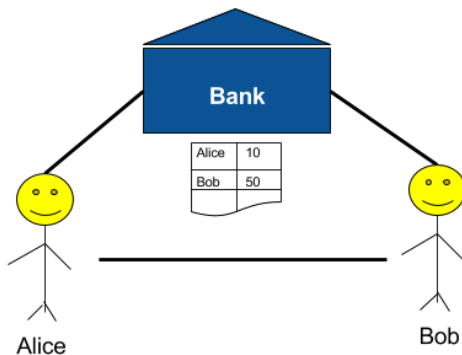
- A decentralized cryptocurrency [Nakamoto, 2008]
- No central authority

## Blockchain Technology

- A decentralized P2P trust-based distributed system
- Consensus is achieved through proof-of-work.

# Background

## Traditional Banking



- Maintains a ledger (record book)
- Verifies owner and recipient
- Validates every transaction

# Background

## Cryptographic Hash Function

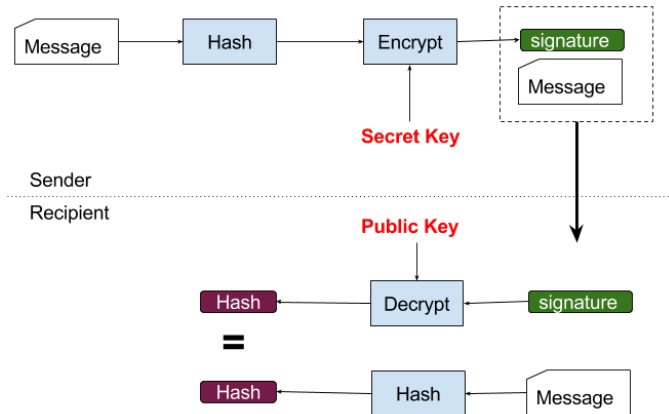


## Properties

- Collision resistant
- High entropy
- One-way function

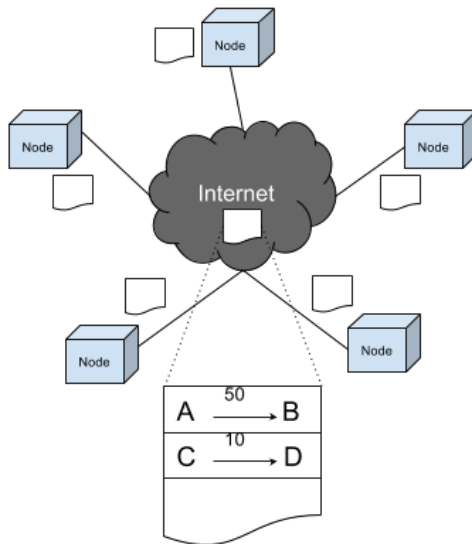
# Background

## Digital Signature



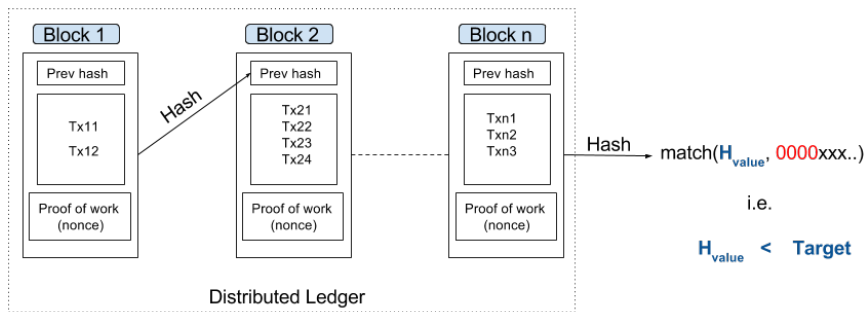
# Blockchain Technology

## Distributed and Replicated Ledger



# Blockchain Technology

## Blockchain

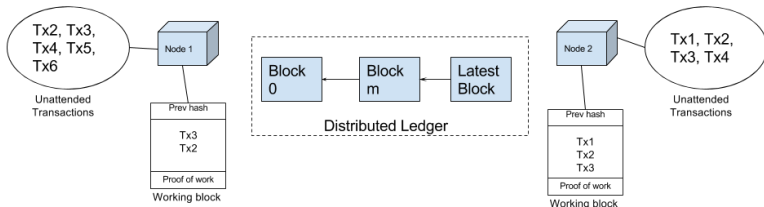


- The process of finding a block is called as Mining
- Highly compute intensive and power hungry
- Rewarded with some coins (newly added into the circulation) and transaction fee



# Blockchain Technology

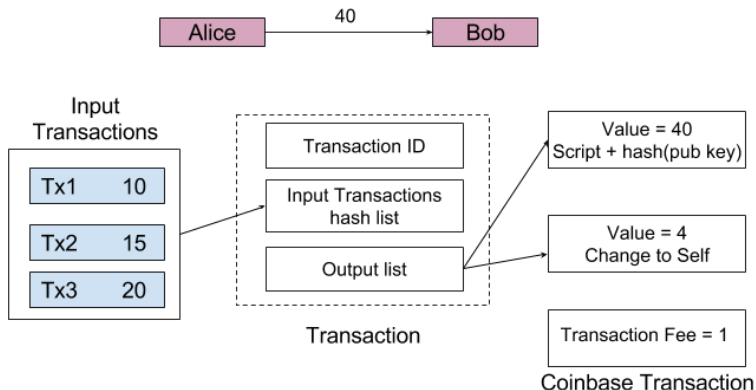
## Block Creation



- Group the broadcast transactions after every 10min interval
- Two nodes may find two different blocks simultaneously
- Conflict is resolved by selecting the longest forked chain. Thus, transaction in a block has to wait for next 6 blocks to get confirmed.

# Blockchain Technology

## Transaction



- Transactions are irreversible and non-encrypted
- Output is transferred to a bitcoin address (recipient's public key)

# Blockchain Technology

## Transaction Example

### Input:

**Previous tx:** f5d8ee39a430901c91...

**Index:** 0

**scriptSig:** 304502206e21798a42fae0e854281abd...  
90db022100e2ac980643b0b82c0e88...

### Output:

**Value:** 5000000000

**scriptPubKey:** OP\_DUP OP\_HASH160  
404371705fa9bd789a2fcd52d2c580b65d35549d  
OP\_EQUALVERIFY OP\_CHECKSIG

- Bitcoins in circulation = 16,564,000 (13th September 2017 05:30)
- System hash rate = 8,715,089.78 TH/s
- Number of transactions per day = 263,320
- Blockchain height (number of blocks mined so far) = 485220 (14th September 2017 19:30 IST)
- Current block reward = 12.5 BTC(bitcoins)
- BTC price = \$3,480.26
- Avg. block size = 0.67MB

## Crypto Exchanges

poloniex, kraken, bittrex, coinbase etc.

## Altcoins

Ethereum (ETH), Litecoin (LTC), Dash, Zcash, Monero etc.


## Decentralized applications (DApps) on blockchain

Augur: A decentralized prediction market, Storj: A decentralized cloud storage, InterPlanetary File System (IPFS) etc.

# Summary


Bitcoin is a decentralized crypto currency implemented using

- P2P distributed networking
- Cryptography
- Proof-of-work concept

 (2017).  
Bitcoin Wiki .  
[https://en.bitcoin.it/wiki/Main\\_Page](https://en.bitcoin.it/wiki/Main_Page).  
[Online; accessed 14-September-2017].

 (2017).  
Current Blockchain Status.  
<https://blockchain.info/>.  
[Online; accessed 14-September-2017].

 (2017).  
A next-generation smart contract and decentralized application platform.  
<https://github.com/ethereum/wiki/wiki/White-Paper>.  
[Online; accessed 14-September-2017].

 Nakamoto, S. (2008).  
Bitcoin: A peer-to-peer electronic cash system.