

CTION

CONNECTION

ECTION

BLOCKCHAIN

PRESENTED BY: Mazhar K

Time to learn how *Blocks* are *Chained*?

Monetary System

Blockchain &
Bitcoin - Help?

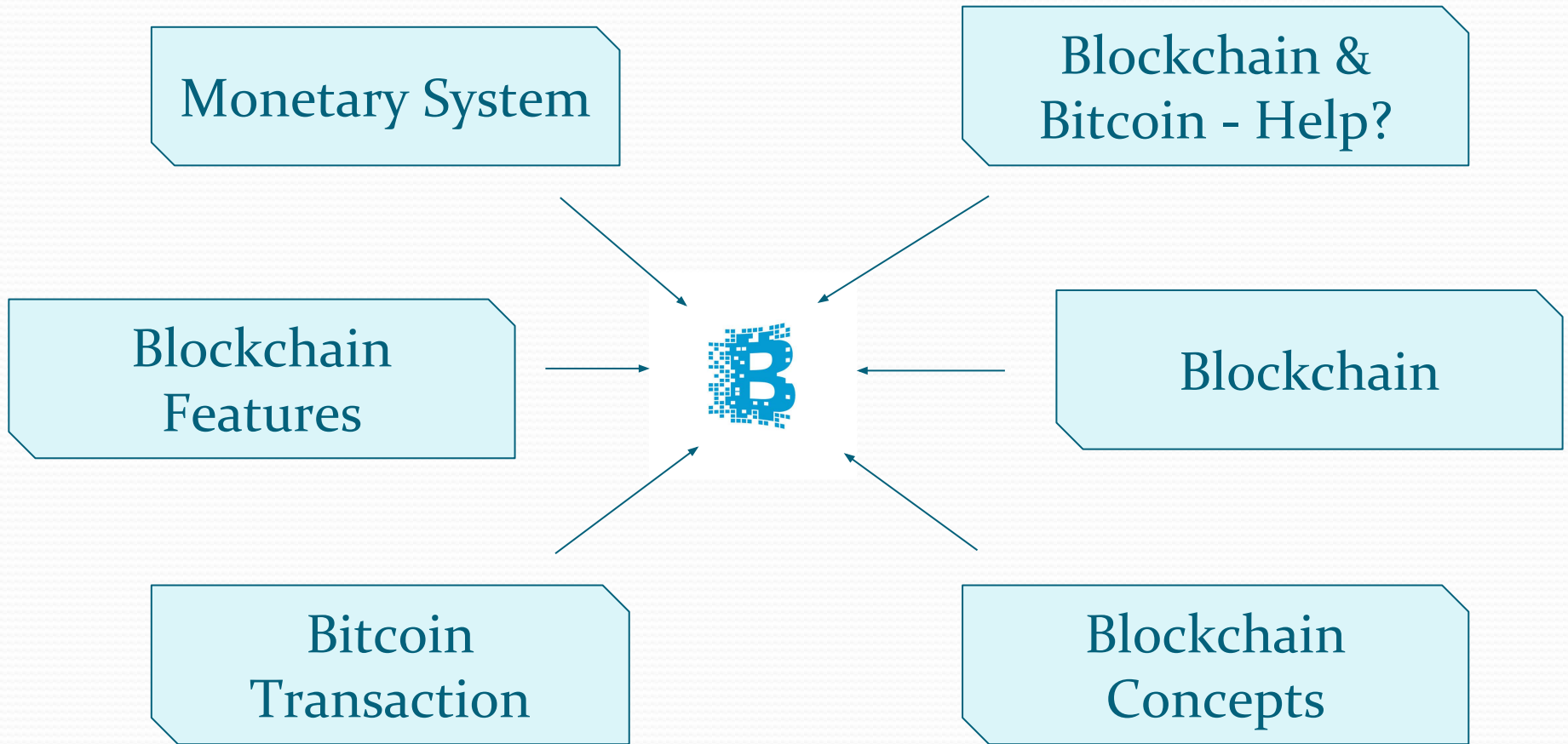
Blockchain
Features



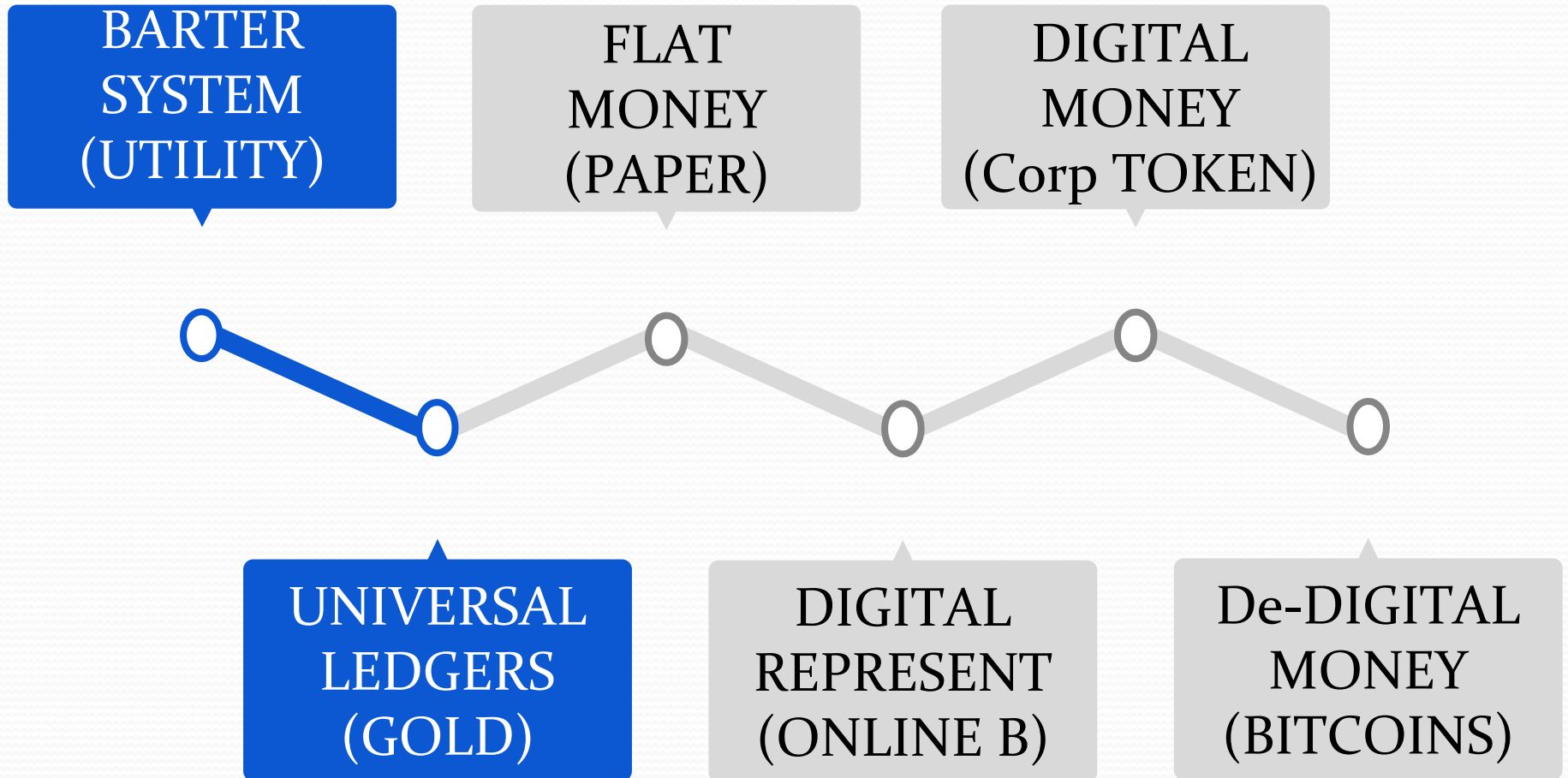
Blockchain

Bitcoin
Transaction

Blockchain
Concepts



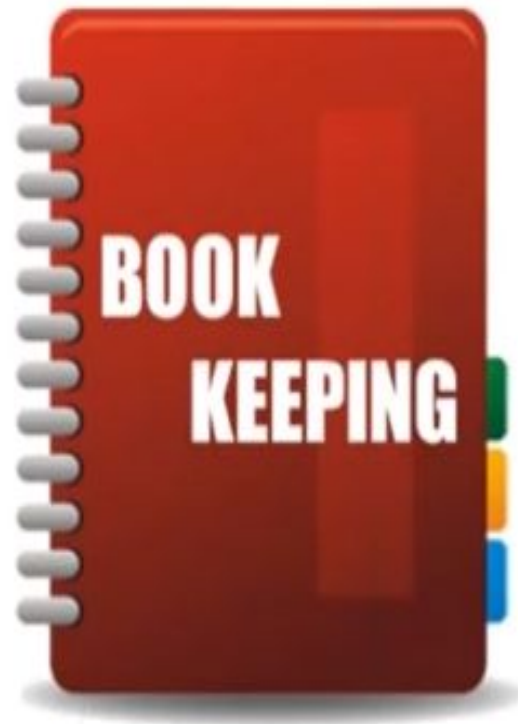
Change in Monetary System



How a Trade happens - Current System?



Trade is Recorded in Bookkeeping (An offline ledger where transaction details are stored)



Bookkeeping is isolated and closed to the public



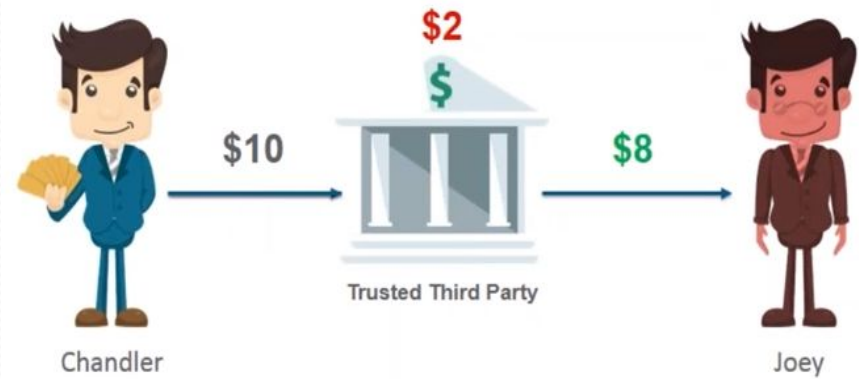
For this reason we use trusted third parties or middle men we trust to facilitate and approve our transactions

Issues - existing Monetary System

Double Spending



Standard Transaction Fees



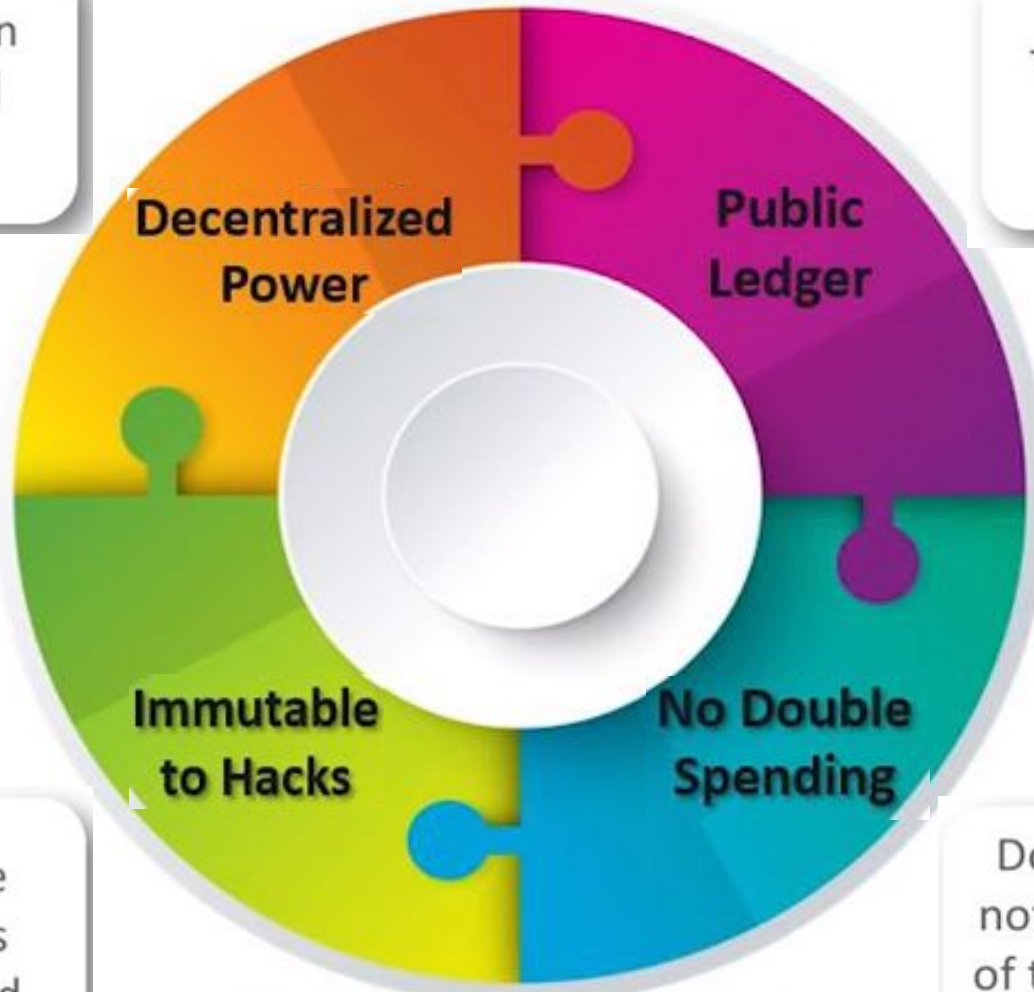
Transaction Delays



How can Blockchain & Bitcoin help?

Bitcoin Blockchain has a distributed ledger

The ledger is public for all to access



Transactions are immutable, thus cannot be hacked

Double spending is not allowed because of the basic structure of block transactions

Issues with centralized banks

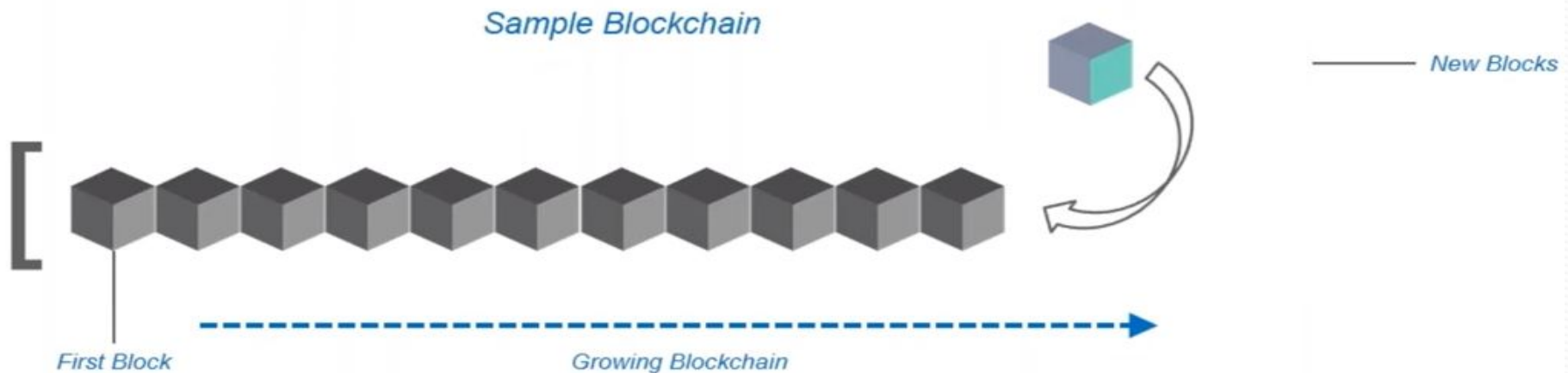
Blockchain & Bitcoin help? ...contd

And the **best part** of using such a cryptocurrency is that the **transaction fee** is **zero** or **very minimal** in comparison with **third parties** such as banks and digital transfer systems.



What is Blockchain?

Satoshi Nakamoto in 2008



- Block & Chain - 2 different terms
- Blockchain is the technology behind Bitcoin
- Public distributed database holding encrypted ledgers
- Block is the 'current' part of a blockchain which records some or all of the recent transactions, and once completed goes into the blockchain as permanent database. The first block is called "Genesis block".



Blockchain Overview



Blockchain uses Private Key Cryptography to secure identities and hash functions to make the blockchain immutable

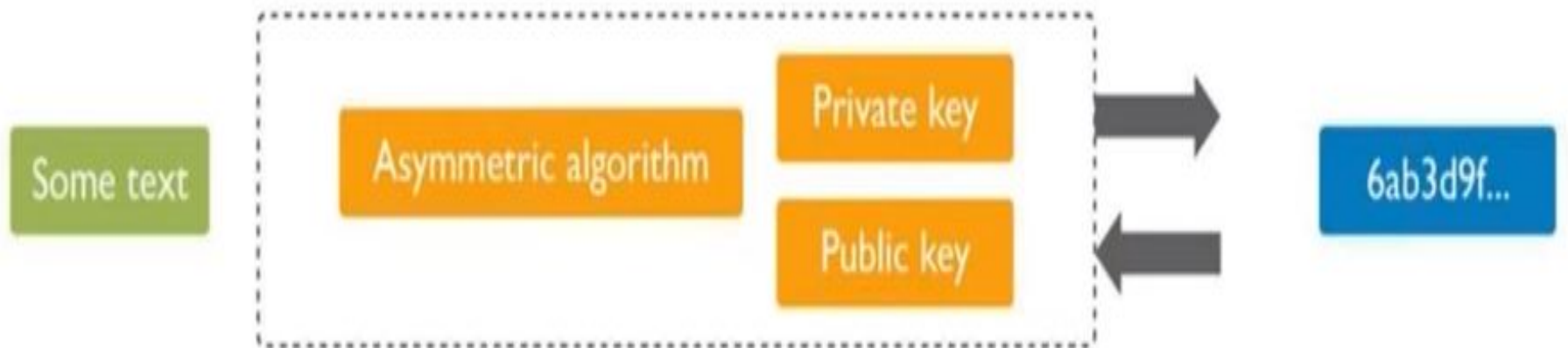
P2P machines on the network help in maintaining the consistency of the distributed ledger

The program gives the blockchain its protocol based on the requirement

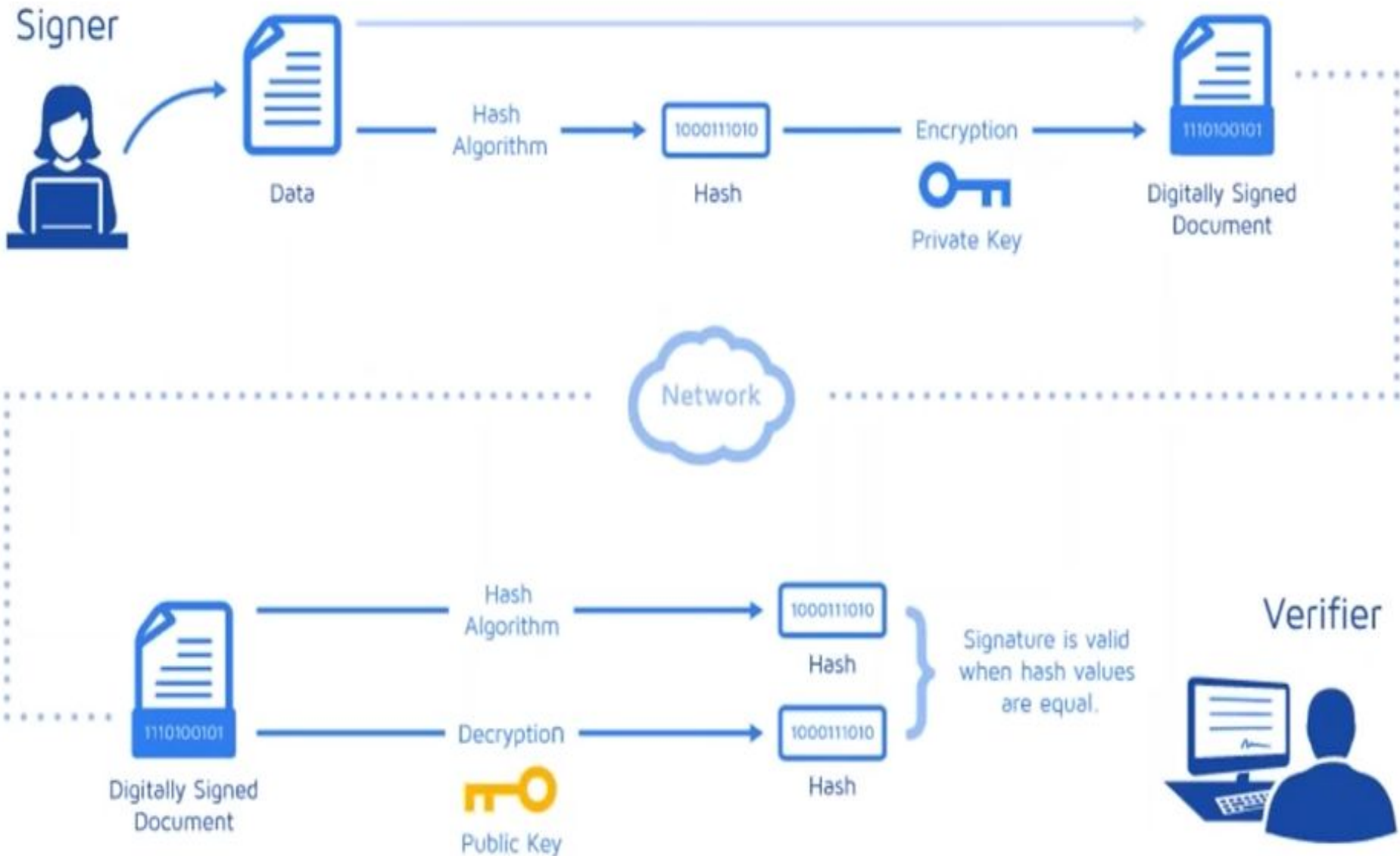
Cryptography

Involves 2 different keys:

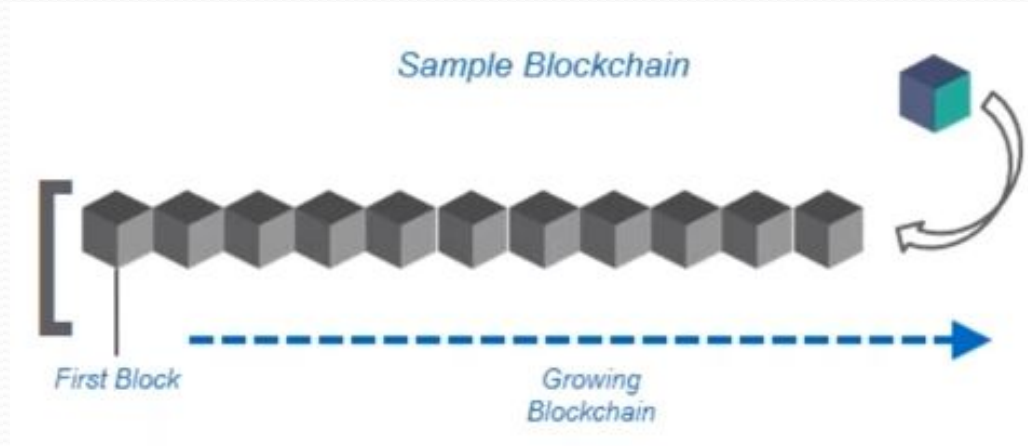
- Private
- Public
- *Private key to encrypt then public key can decrypt*
- *Public key to encrypt then private key can decrypt*
 - Asymmetric encryption



P2P System - Digital Signature



Blockchain Program



The Blockchain is the way of implementing any solution/ use case

Blockchain is a concept and can be implemented by any language

Solidity is the most preferred default for writing programs in Blockchain

List of Cryptocurrency

- Bitcoin
- Litecoin
- Ethereum
- BTC & BTG
- Ripple (XRP)
- IOTA
- Darkcoin (DASH)

What is Bitcoin?



The first decentralized digital currency

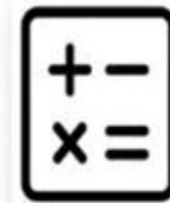
Uses cryptography to control its creation and management



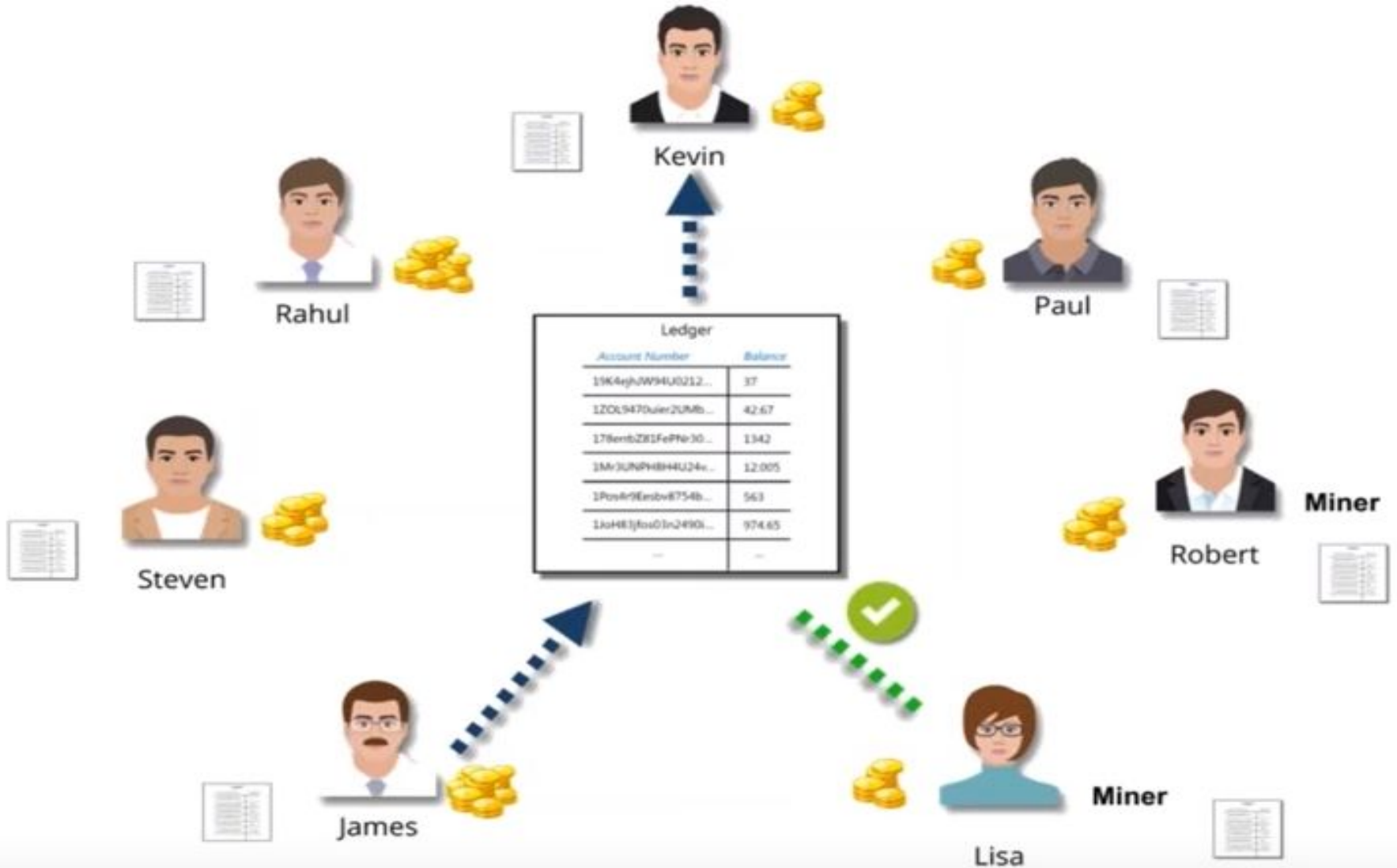
Account Number	Balance
19Kqj/W9WU212..	37
120L9679ue2JMb..	42.67
179erh2K1eP6u3D..	842
13h3LNP8H6U2h..	112.005
1Pou49eub8754b..	563
12uH8Juo09c2490..	974.05

Created and held electronically in a peer to peer open ledger called the blockchain

Ledger is produced by people using software that solves mathematical problems



Bitcoin Transaction



Bitcoin Transaction - Flow Diagram



Someone requests a transaction

The transaction is broadcast to the P2P network



Validation
The network of nodes validate the transaction



The transaction is complete



The new block is then added to the existing blockchain

Once verified, the transaction becomes a part of new block for the ledger



Blockchain Types

- ❑ *Public:* The ledgers are visible to everyone on the internet and anyone can verify and add a block of transactions to the block chain.

Examples – Bitcoin, Ethereum, Dash, Factom

- ❑ *Private:* All permissions are kept centralized to an organization. Only specific people in the organization to verify and add transaction blocks but everyone on the internet is generally allowed to view.

Examples- Multichain, Blockstack

- ❑ *Consortium:* Controlled by a consortium of members. Only predefined set of nodes have access to write the data or block.

Examples- Ripple and R3

Blockchain Use Cases

- Settlements
- Change of supplier
- Meter data
- Real-time capacity matching



- Autonomous network configuration
- Self-serve maintenance
- Asset and inventory tracking
- Cross asset/industry data sharing

- EV charging
- Peer-to-peer trading
- Demand-side management
- Network services

- Eligibility for social tariffs
- Safety authorisations and permit to work
- Fraud detection
- Loyalty schemes

Latest Updates

AWS launches a managed blockchain service:

<https://techcrunch.com/2018/11/28/aws-launches-a-managed-blockchain-service/>

Blockchain used in another industry (Mining industry):

<https://drive.google.com/open?id=182gzS7abEzr-f4SgcusKbqJDwMnZ7P1G>