SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

COURSE NAME: 19CS622-Blockchain Technology

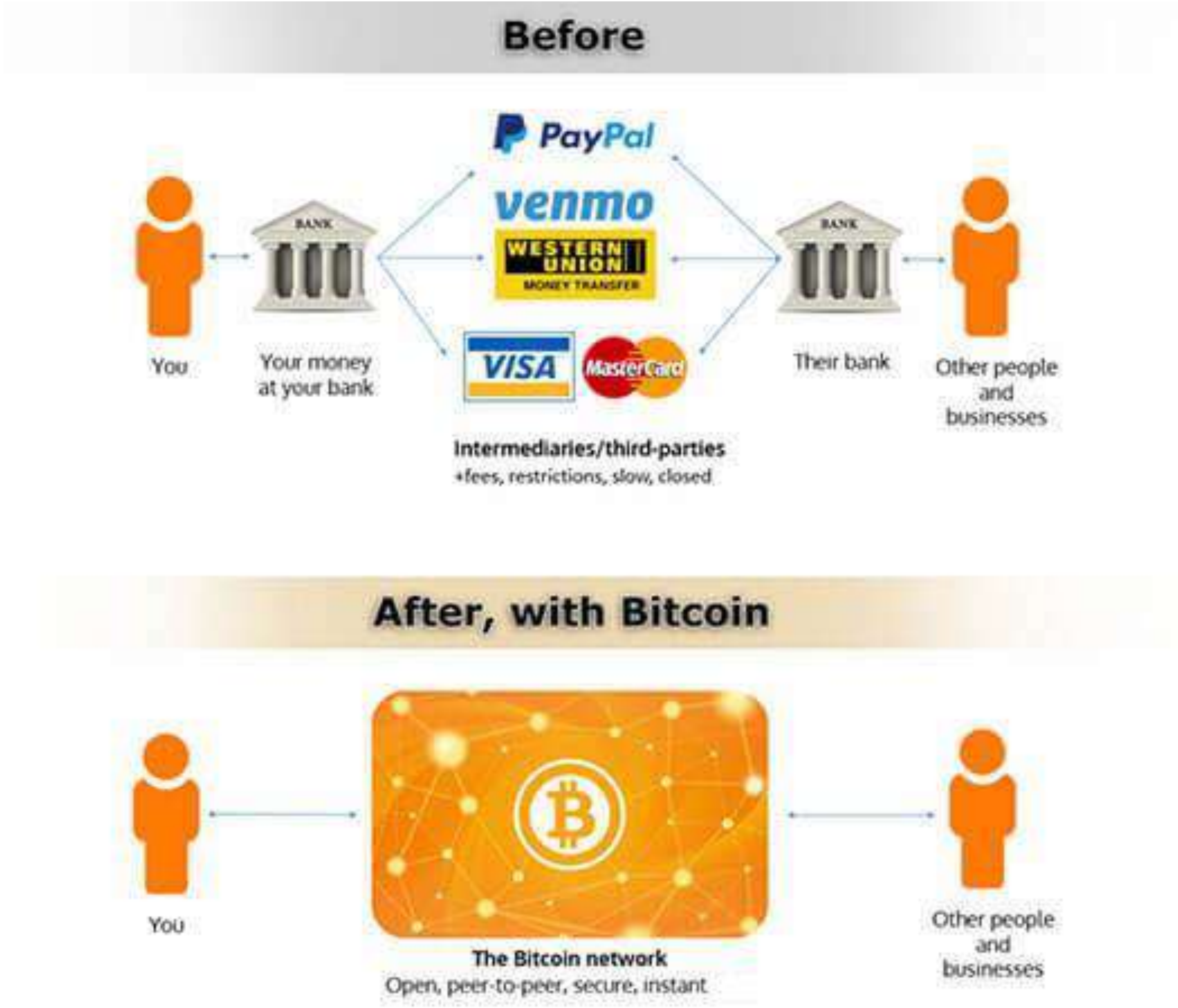
III YEAR /VI SEMESTER

Unit 2- CRYPTOCURRENCY

Topic 1 : BITCOIN

BITCOIN

- A distributed, decentralized digital currency system
- Released by Satoshi Nakamoto 2008
- Effectively a bank run by an ad hoc network
  - Digital checks
  - A distributed transaction log
- Number of BitCoins in circulation 11.8 million (December 2013)
- Total number of BitCoins generated cannot exceed 21 million
- Average price of a Bitcoin: around $300
  - Price has been unstable.
- Total balances held in BTC 1B$ compared with 1,200B$ circulating in USD.
- 30 Transactions per min. (Visa transaction 200,000 per minute.)

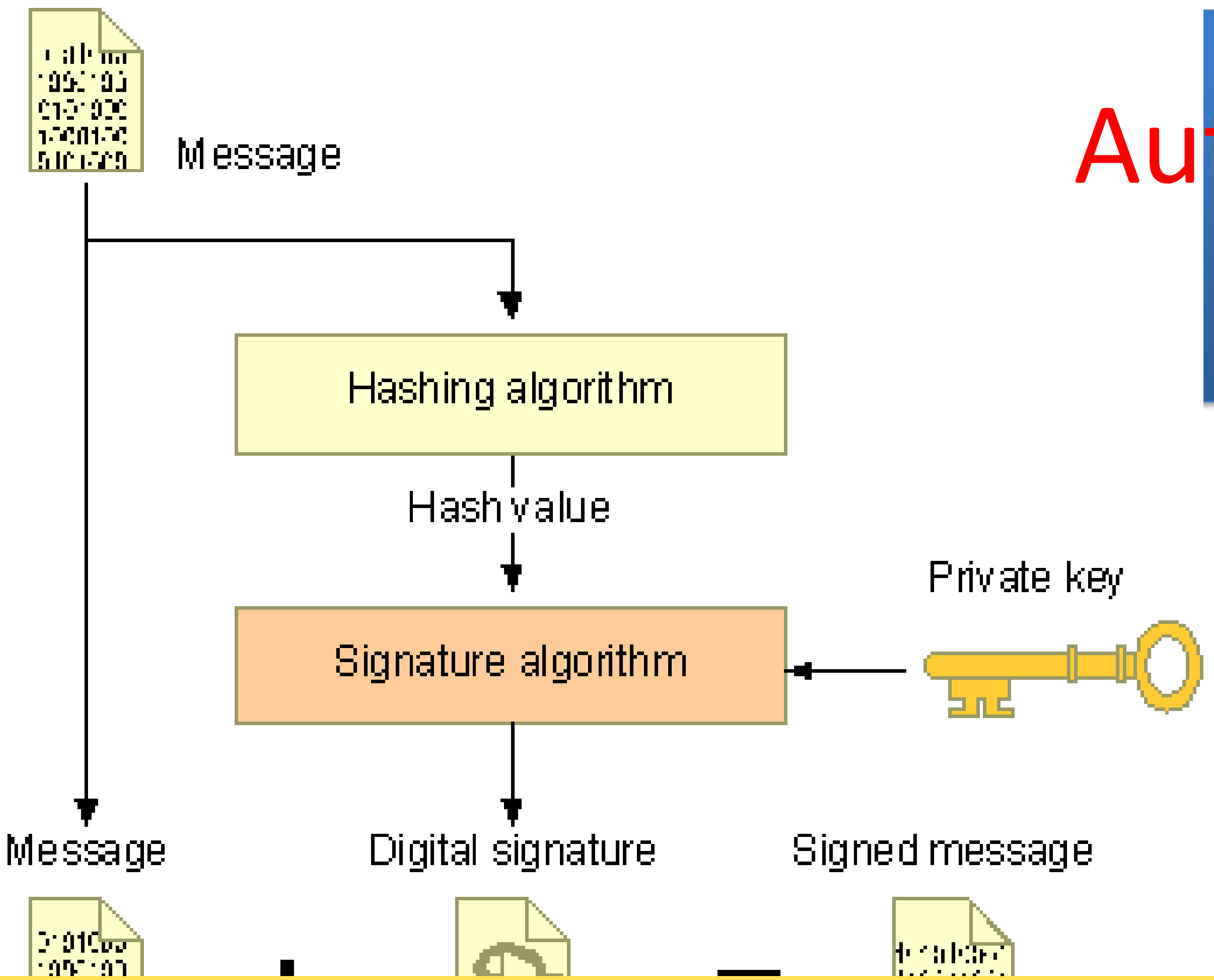

Before
You
Your money at your bank
PayPal
venmo
WESTERN UNION MONEY TRANSFER
VISA
MasterCard
Intermediaries/third-parties
+fees, restrictions, slow, closed
Their bank
Other people and businesses
BANK
BANK
After, with Bitcoin
You
The Bitcoin network
Open, peer-to-peer, secure, instant
Other people and businesses

SECURITY IN BITCOIN

- **Authentication □** **Public Key Crypto: Digital Signatures**
  - Am I paying the right person? Not some other impersonator?
- **Integrity □** **Digital Signatures and Cryptographic Hash**
  - Is the coin double-spent?
  - Can an attacker reverse or change transactions?
- **Availability□** **Broadcast messages to the P2P network**
  - Can I make a transaction anytime I want?
- **Confidentiality□** **Pseudonymity**
  - Are my transactions private? Anonymous?

Public Key Crypto: Digital Signature

First, create a message digest using a cryptographic hash
Then, encrypt the message digest with your private key



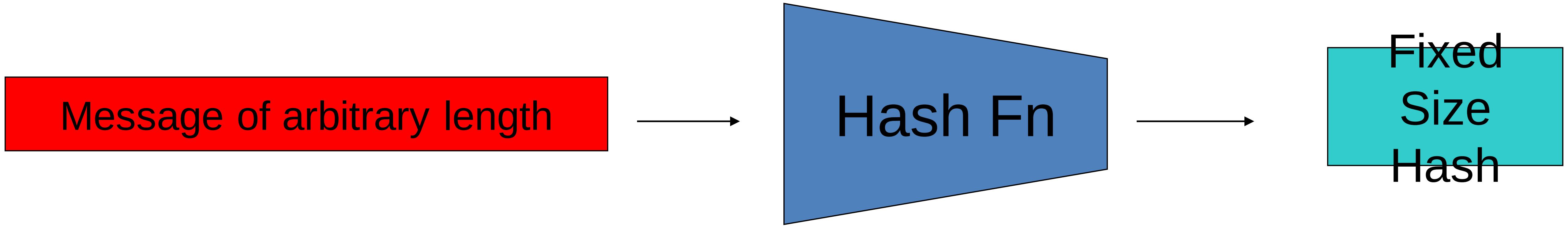
Authentication

Integrity

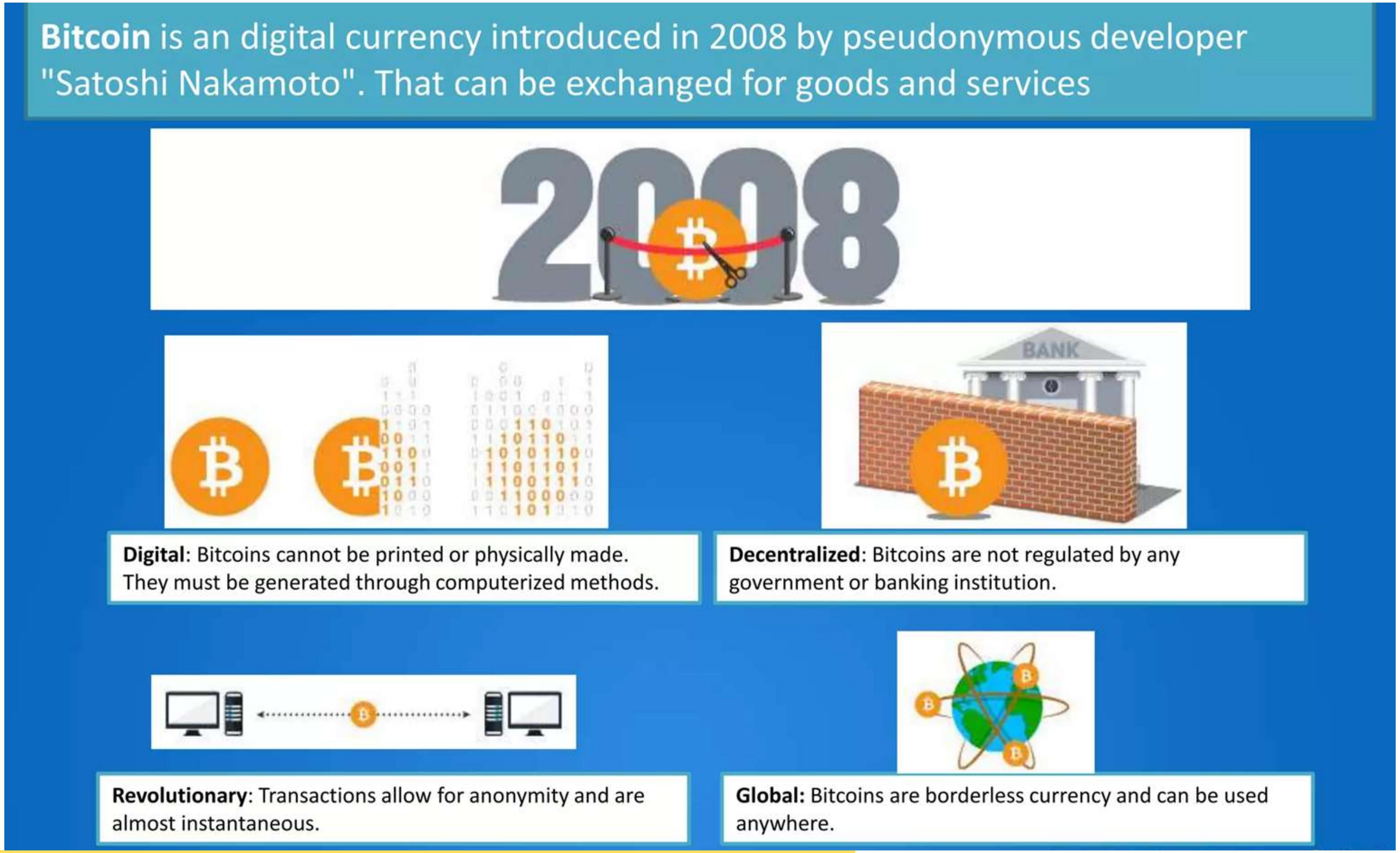
Non-repudiation

Cryptographic Hash Functions

- Consistent: hash(X) always yields same result
- One-way: given Y, hard to find X s.t. hash(X) = Y
- Collision resistant: given hash(W) = Z, hard to find X such that hash(X) = Z



BITCOIN



Bitcoin is an digital currency introduced in 2008 by pseudonymous developer "Satoshi Nakamoto". That can be exchanged for goods and services

Digital: Bitcoins cannot be printed or physically made. They must be generated through computerized methods.

Decentralized: Bitcoins are not regulated by any government or banking institution.

Revolutionary: Transactions allow for anonymity and are almost instantaneous.

Global: Bitcoins are borderless currency and can be used anywhere.

Summary

References

TEXT BOOKS

1. Mastering Bitcoin: Unlocking Digital Cryptocurrencies, by Andreas M Antonopoulos 2018
2. Imran Bashir, “Mastering Blockchain: Distributed Ledger Technology, Decentralization and Smart Contracts Explained”, Second Edition, Packt Publishing, 2018.
3. https://101blockchains.com/blockchain-vs-database-the-difference/

REFERENCES

1. William Mougayar, “Business Blockchain Promise, Practice and Application of the Next Internet Technology, John Wiley & Sons 2016.
2. Josh Thompson, ‘Blockchain: The Blockchain for Beginnings, Guild to Blockchain Technology and Blockchain Programming’, Create Space Independent Publishing Platform, 2017.
3. Arvind Narayanan, “Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction”, Princeton University Press, July 19, 2016.
4. Henning Diedrich, Ethereum: Block chains, Digital Assets, Smart Contracts, Decentralized Autonomous Organizations-2016

Thank You