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

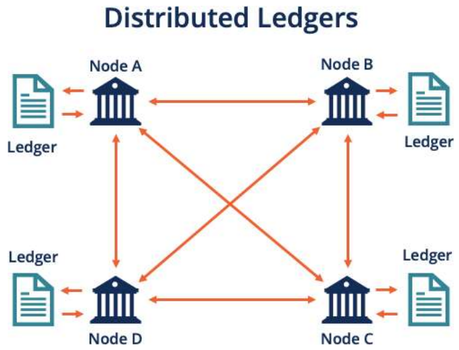
COURSE NAME: 19CS622-Blockchain Technology

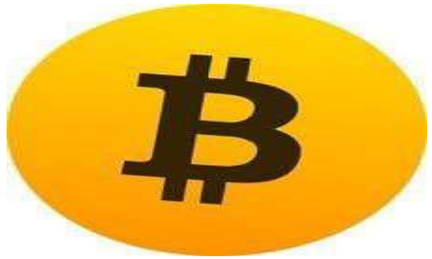
III YEAR /VI SEMESTER

Unit 2- CRYPTOCURRENCY

Analysis of Bitcoin transactions

Bitcoin Transactions

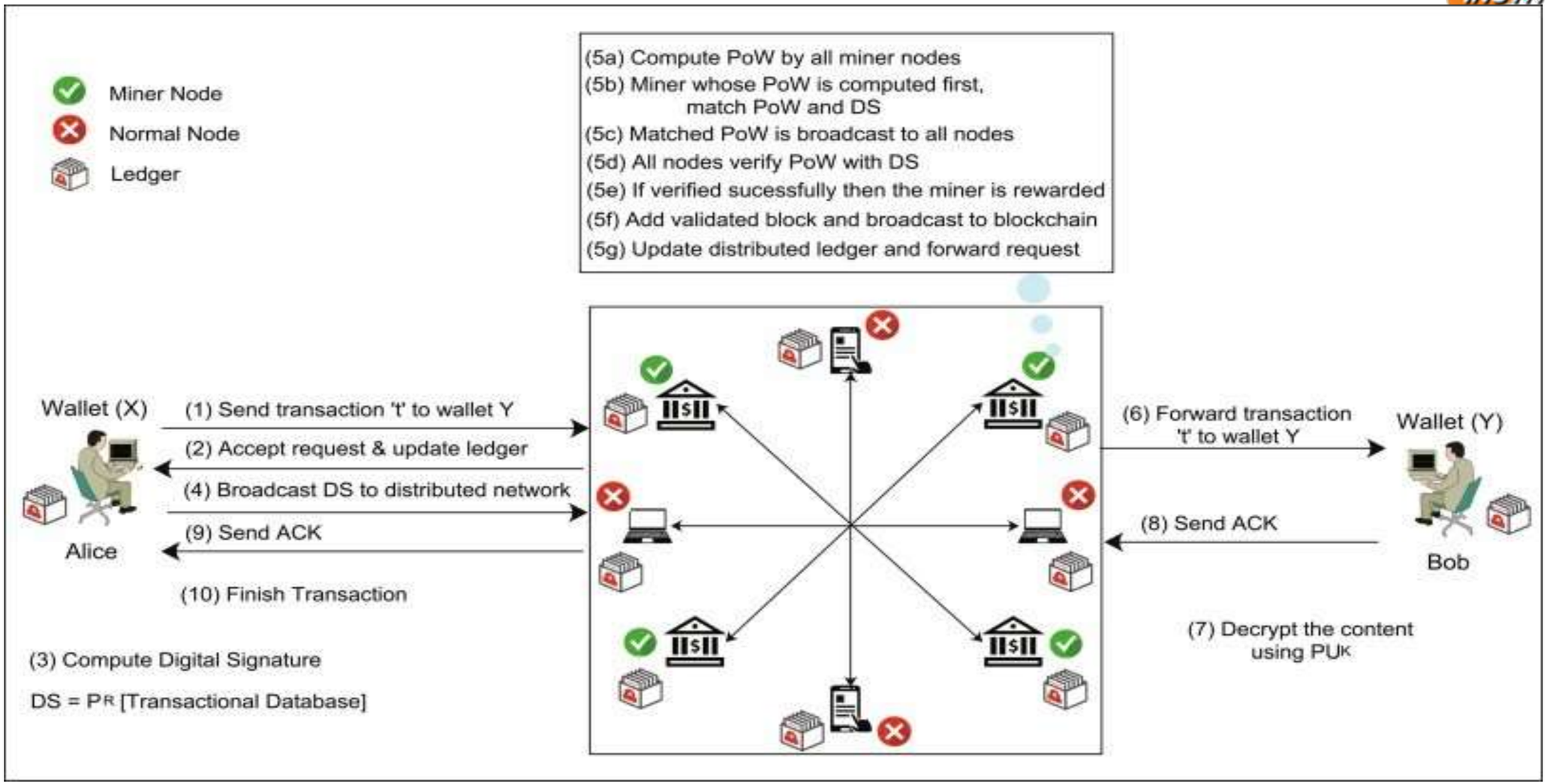




Bitcoin is a decentralized digital currency. Bitcoin transactions are verified by network nodes through cryptography and recorded in a public distributed ledger called a blockchain.

The cryptocurrency was invented in 2008 by an unknown entity under the name Satoshi Nakamoto.

Bitcoin Transactions



Bitcoin Transactions

Two parties *Alice and Bob* who want to communicate with each other for funds transfer over an insecure channel, Internet.

- If *Alice* wants to send some coins from her wallet *X* to *Bob's* wallet *Y*, then a request of transactional data "*t*" is sent to *Bob*.
- This request is broadcasted in the entire network.
- The distributed nodes accept the request and update their ledgers with the transactional information of *Alice–Bob*.
- After updating ledgers, Alice computes digital signature (*DS*) and broadcasts it in the network.
- A miner node is selected to verify and validate the transaction

Bitcoin Transactions

- It computes proof-of- work (PoW) to match the *DS* received.
- If PoW is successfully matched with *DS*, then the result is broadcast to all the nodes for verification and validation.
- The other miner nodes also verify the PoW with *DS*.
- If the verification is successful, then the miner node is (financially) rewarded for computing the PoW.

Bitcoin Transactions

- The validated block is added in the validated chain and the transaction is broadcasted to the entire blockchain.
- Using the validated transaction "*t*," the bitcoins are added to wallet*Y* of *Bob.*
- *Bob* decrypts the content using the paired public key (*PUK*) of Alice and sends the acknowledgment (*ACK*) to *Alice*.
- The transaction is finished once Alice receives the transaction acknowledgment.

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