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 1- INTRODUCTION TO BLOCKCHAIN

Topic 5: Consensus Algorithms & Types

Brain Storming

1. Blockchain terminologies
2. Define Distributed ledger.

Consensus components

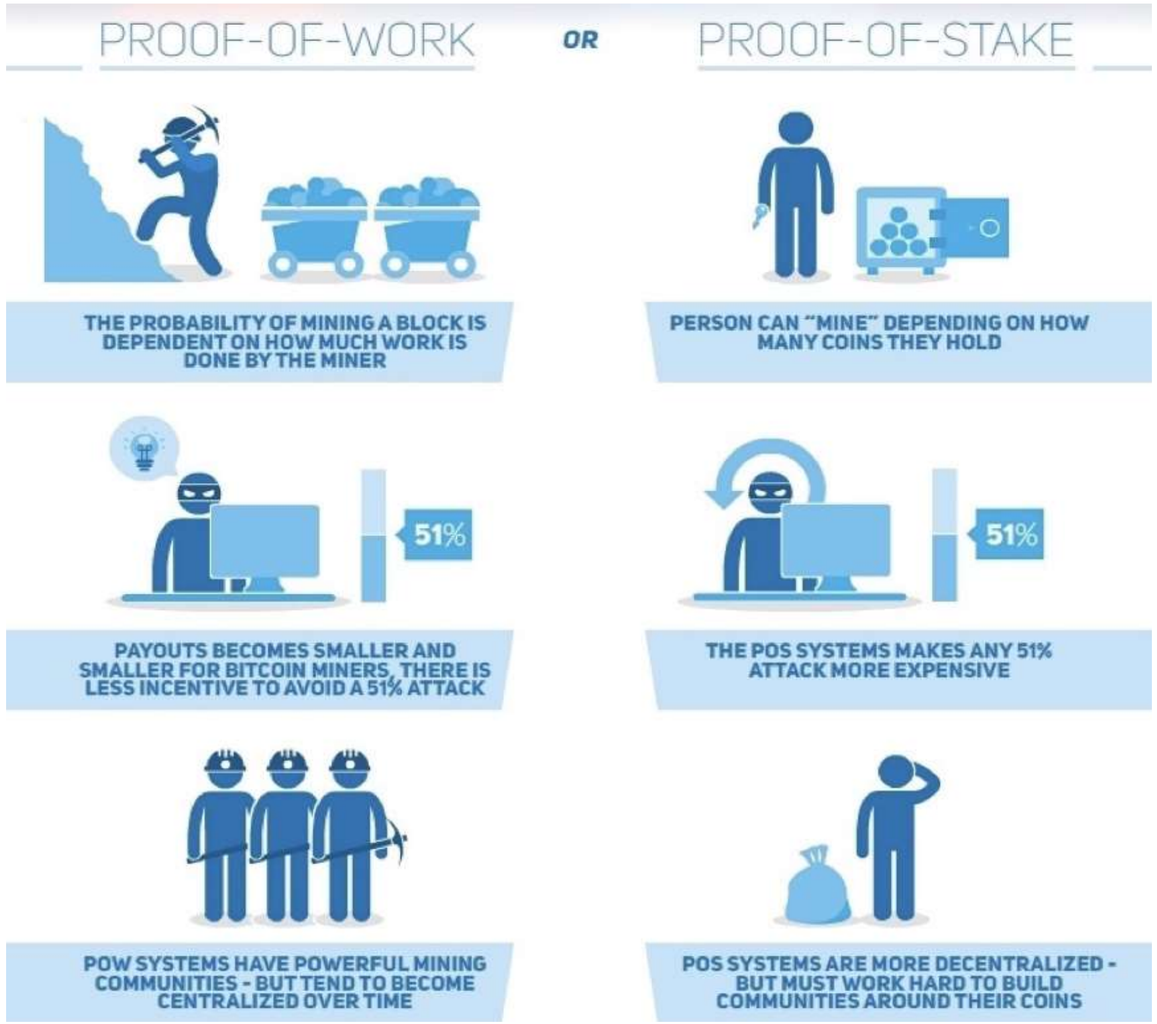
- **Principles and paradigms of distributed systems**
  - ***Byzantine fault tolerance*** (BFT): the dependability of a fault-tolerant computer system, particularly distributed computing systems, where components may fail and there is imperfect information on whether a component has failed.
  - The objective of BFT is to defend against failures of system components with or without symptoms that prevent other components of the system from reaching an agreement among themselves, where such an agreement is needed for the correct operation of the system.
  - One example of BFT in use is bitcoin. The bitcoin network works in parallel to generate a blockchain with proof-of-work allowing the system to overcome Byzantine failures and reach a coherent global view of the system's state.

Consensus components

- **Blockchain consensus algorithms**
  - Behind every cryptocurrency, there's a consensus algorithm. No consensus algorithm is perfect, but they each have their strengths. In the world of crypto, consensus algorithms exist to prevent double spending.

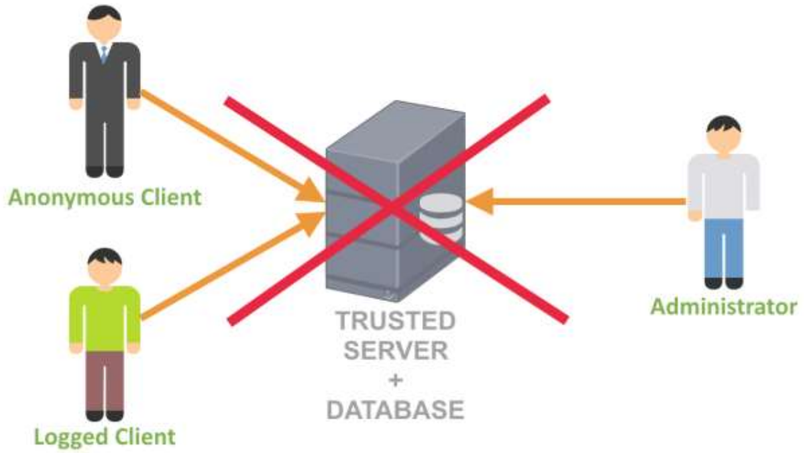
  - Proof of Work (PoW)
  - Proof of Stake (PoS)
  - Delegated Proof of Stake (DPOS)
  - Proof of Burn (PoB)
  - Practical Byzantine fault tolerant Mechanism (PBFT)
  - …

Consensus components



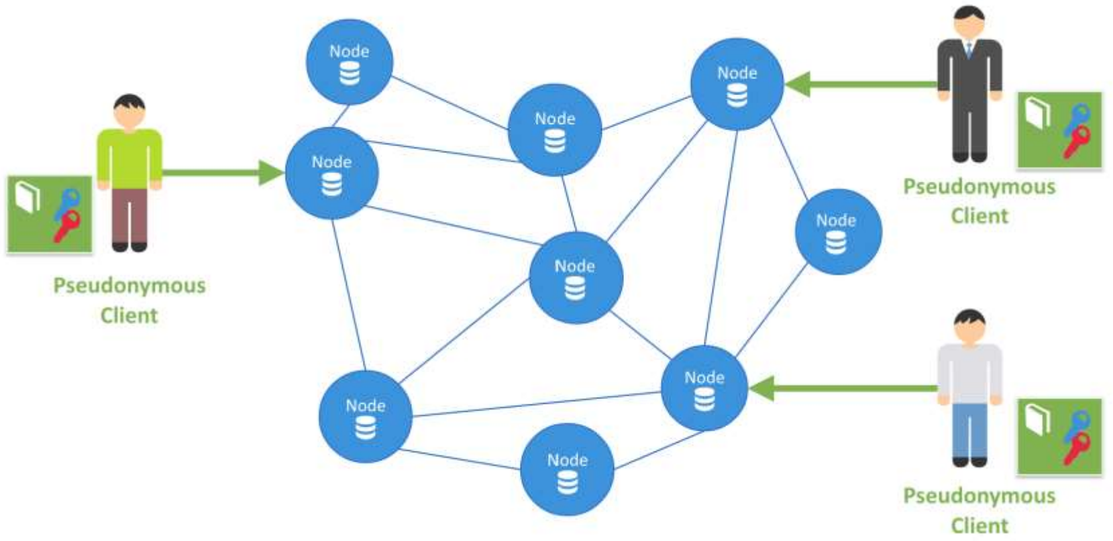
Consensus components

- **Blockchain structure**
  - No more client/server architecture with name roles



Consensus components

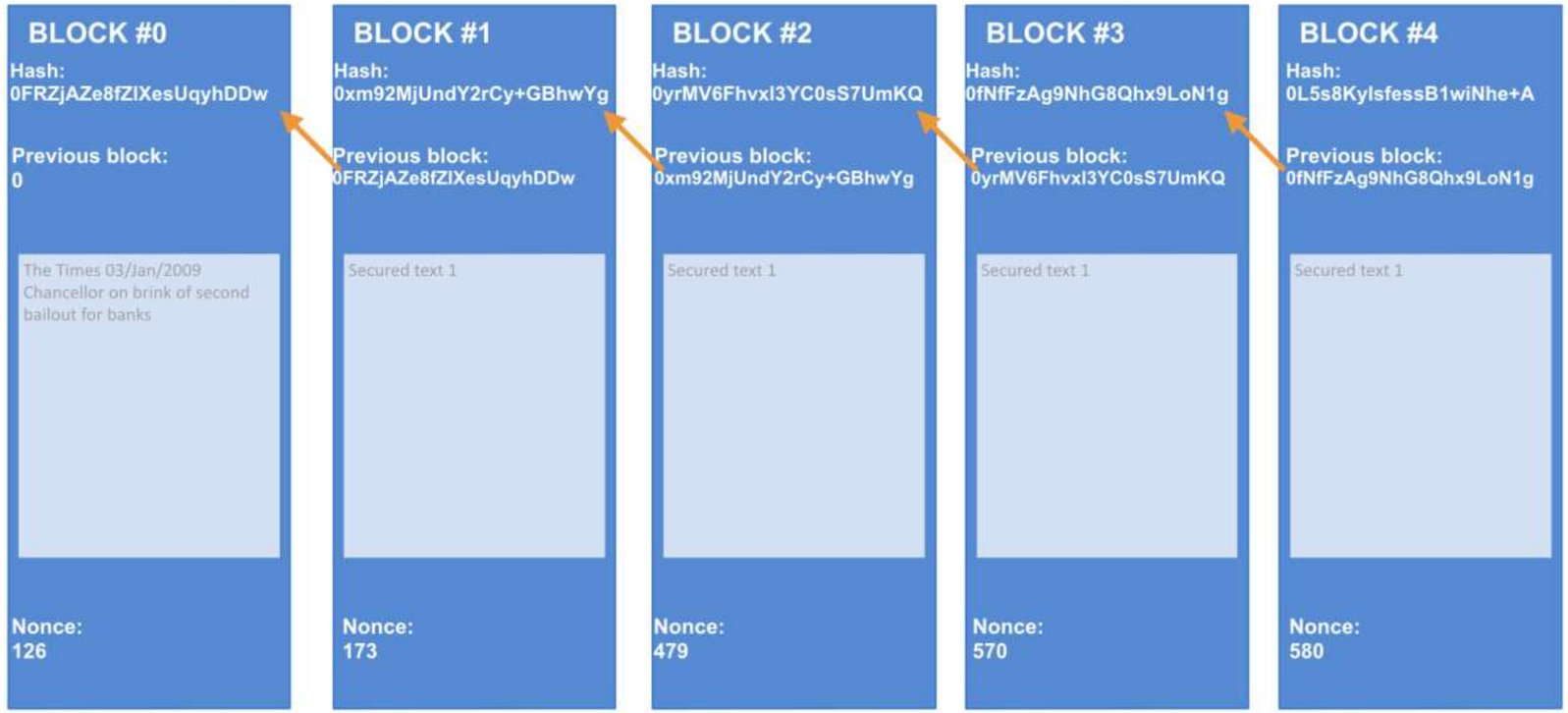
- **Blockchain structure**
  - Peer-to-peer Architecture with pseudonymous client bearing key pairs. Each node as a database copy.



Consensus components

- **Blockchain structure**
  - Data structure:

    31st, 2008



Consensus components

- **Blockchain structure**
  - Blocks of data:

```
yallet@tyler:~/.bitcoin/blocks$ find . -name 'blk*.dat' -mtime -7 -ls
26610095 130688 -rw-------   1 yallet   yallet   133819048 Nov 23 20:37 ./blk00688.dat
26610563 130556 -rw-------   1 yallet   yallet   133682935 Nov 25 16:30 ./blk00690.dat
26611820 130992 -rw-------   1 yallet   yallet   134128511 Nov 24 17:53 ./blk00689.dat
26609041 131076 -rw-------   1 yallet   yallet   134217422 Nov 22 21:51 ./blk00687.dat
26610902 130840 -rw-------   1 yallet   yallet   133975212 Nov 21 20:41 ./blk00686.dat
26612258 130460 -rw-------   1 yallet   yallet   133583976 Nov 26 13:46 ./blk00691.dat
26611825 114692 -rw-------   1 yallet   yallet   117440512 Nov 28 09:34 ./blk00693.dat
26611491 130112 -rw-------   1 yallet   yallet   133230159 Nov 27 14:49 ./blk00692.dat
yallet@tyler:~/.bitcoin/blocks$ hexdump -C blk00691.dat | head -n 15
00000000  f9 be b4 d9 53 3a 0f 00  00 00 00 20 f3 48 e2 80  |....S:..... .H..|
00000010  bb 89 03 22 dd e9 93 ad  9e bc fd 7e 53 14 45 7a  |..."........~S.Ez|
00000020  b5 f2 97 00 00 00 00 00  00 00 00 00 1f 5b e2 c0  |.............[..|
00000030  d1 7d cb 96 9a 37 86 21  c4 a8 af 5a ad a0 ad 0b  |.}...7.!...Z....|
00000040  b2 d2 ef 15 75 c3 3a c6  67 6e 46 0e de 58 38 58  |....u.:.gnF..X8X|
00000050  d4 e6 03 18 3e c5 4e e3  fd 45 0b 01 00 00 00 01  |....>.N..E......|
00000060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000080  ff ff ff ff 49 03 d0 b8  06 2f 48 61 6f 42 54 43  |....I..../HaoBTC|
00000090  2f e7 94 bb e5 9b be e7  9c 81 e8 af 86 e6 98 a5  |/...............|
000000a0  e9 a3 8e e9 9d a2 ef bc  8c e7 8e af e4 bd a9 e7  |................|
000000b0  a9 ba e5 bd 92 e6 9c 88  e5 a4 9c e9 ad 82 e3 80  |................|
000000c0  82 2f 06 74 7d 3d e3 b3  1d 9c f7 99 01 00 ff ff  |./.t}=..........|
000000d0  ff ff 01 4b 1d d3 4e 00  00 00 00 19 76 a9 14 bf  |...K..N.....v...|
000000e0  d3 eb b5 48 5b 49 a6 cf  16 57 82 46 23 ea d6 93  |...H[I...W.F#...|
yallet@tyler:~/.bitcoin/blocks$
```

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