Blockchain in Internet of Things

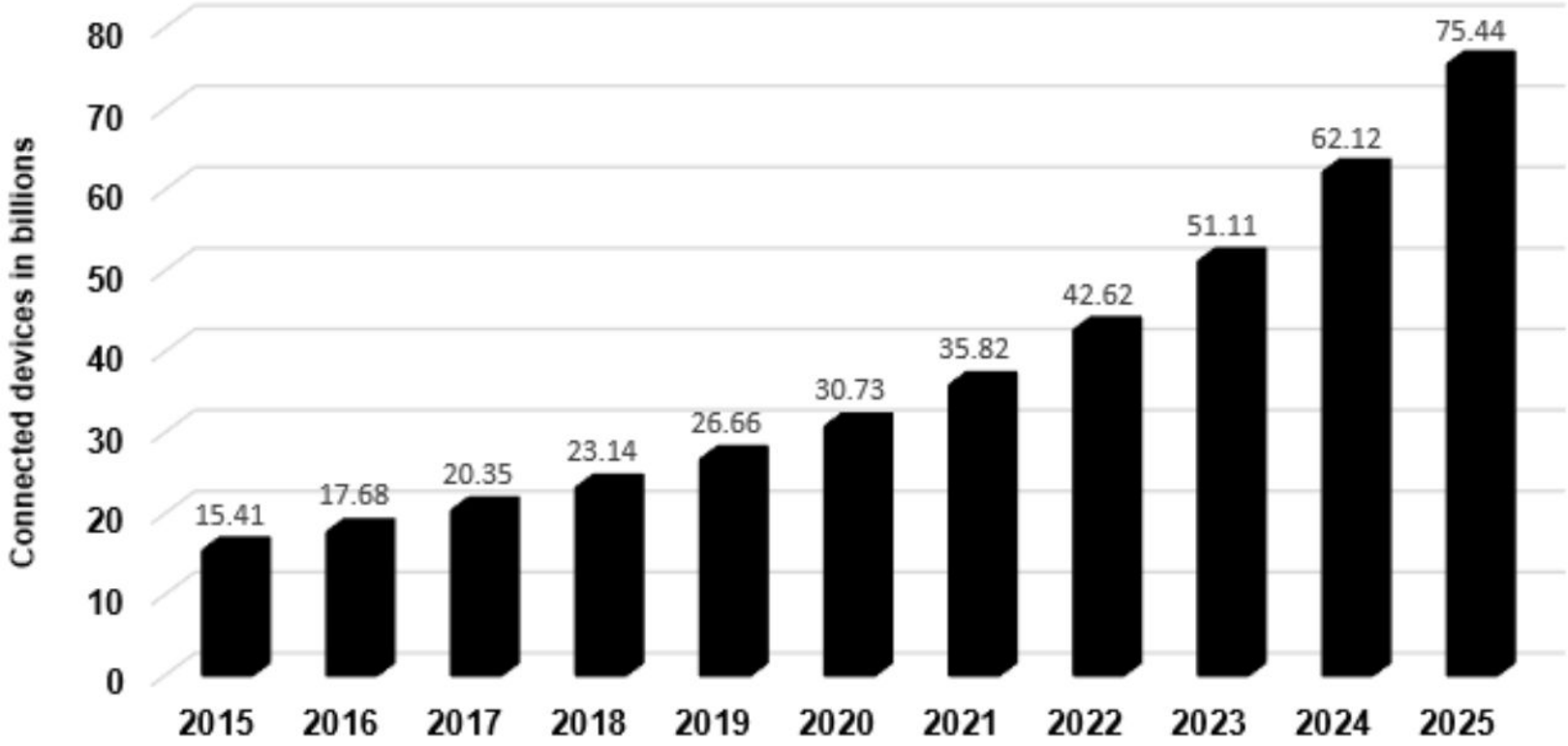
What is IOT[2]

definition of IOT

- “a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies”

ITU. “ITU-T Recommendation Database.
Recommendation ITU-T Y.2060 (06/2012).

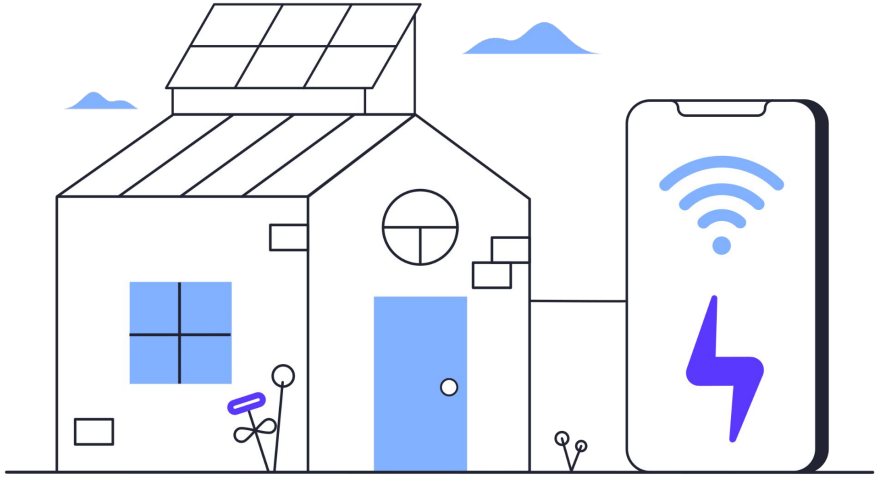
Expected Internet of Things growth from 2015 to 2025[3]



Examples of IoT

Smart House

- Security
- Heating & Cooling
- Kitchen

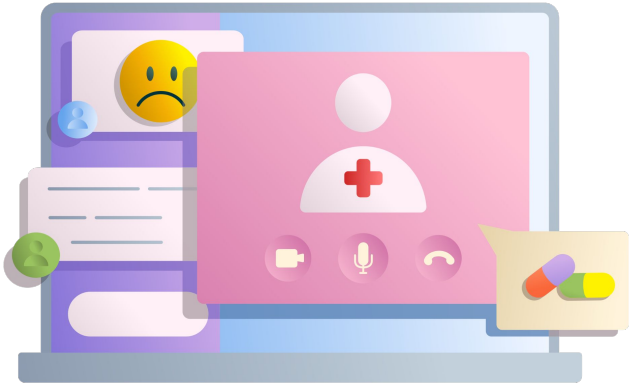


Smart Driving

- Self-driving car
- safety services such as General Motors' OnStar
- navigation

Healthcare

- health and wellness applications
- Internet of Medical Things (IOMT)
- Wearables

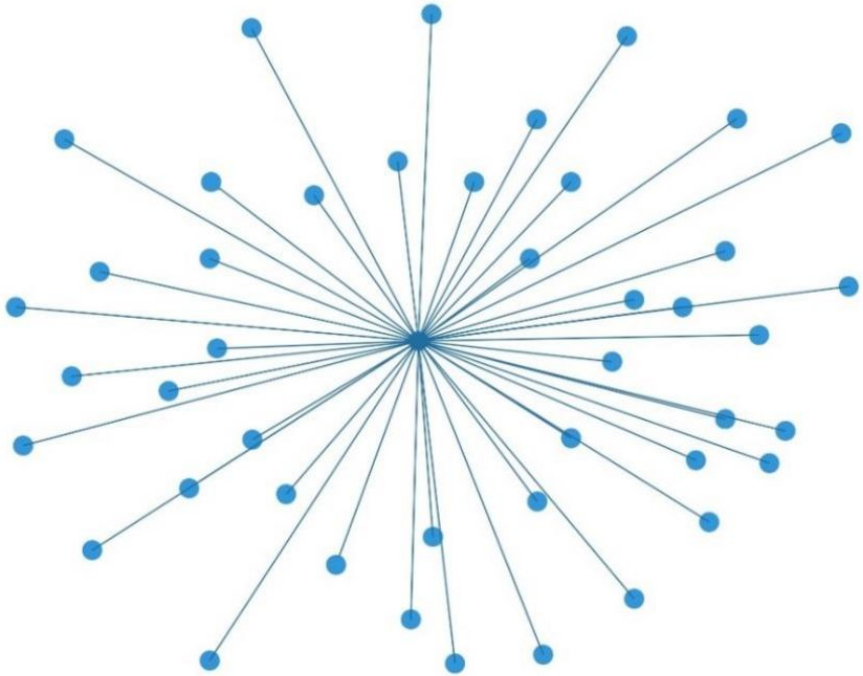


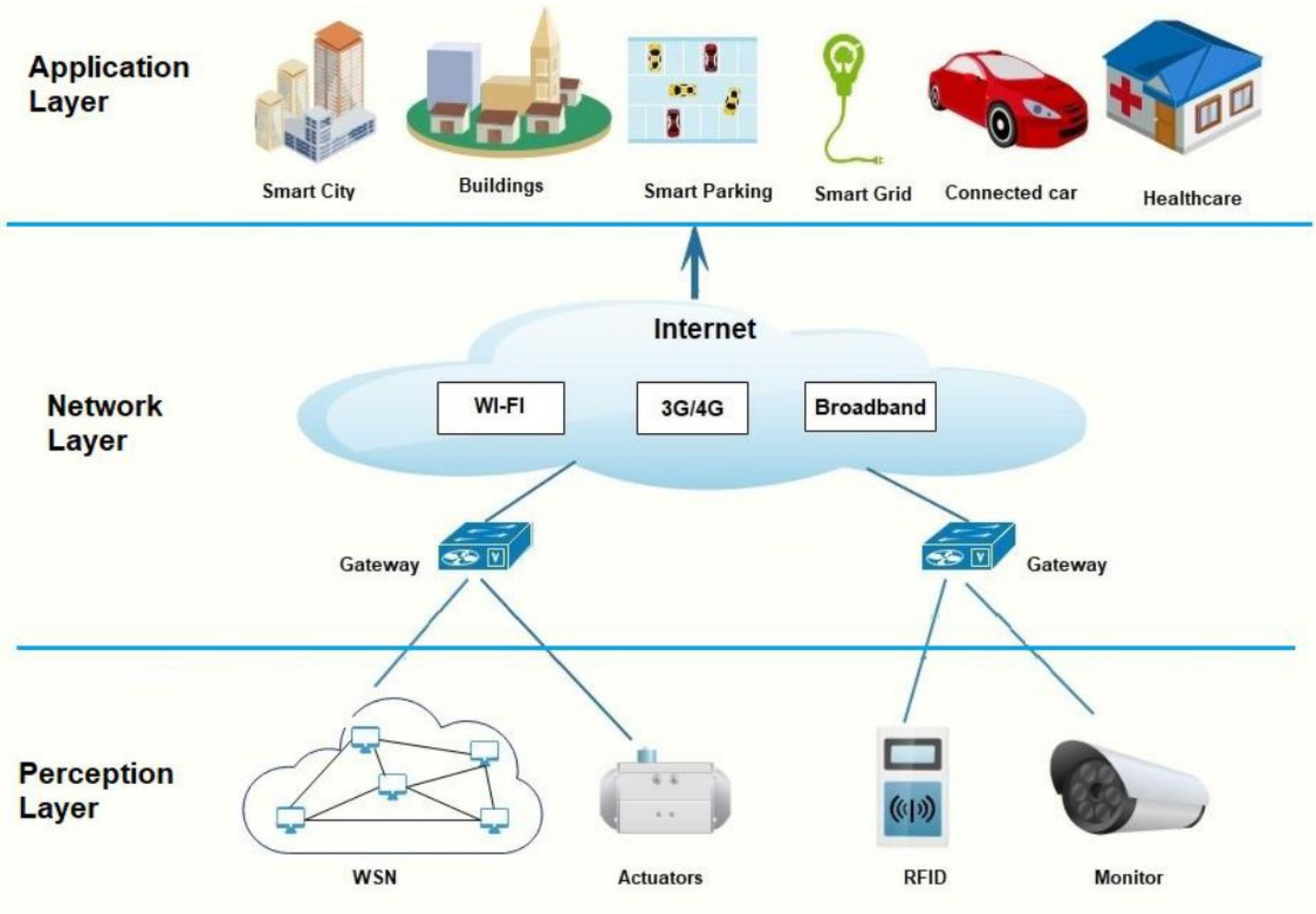
common features

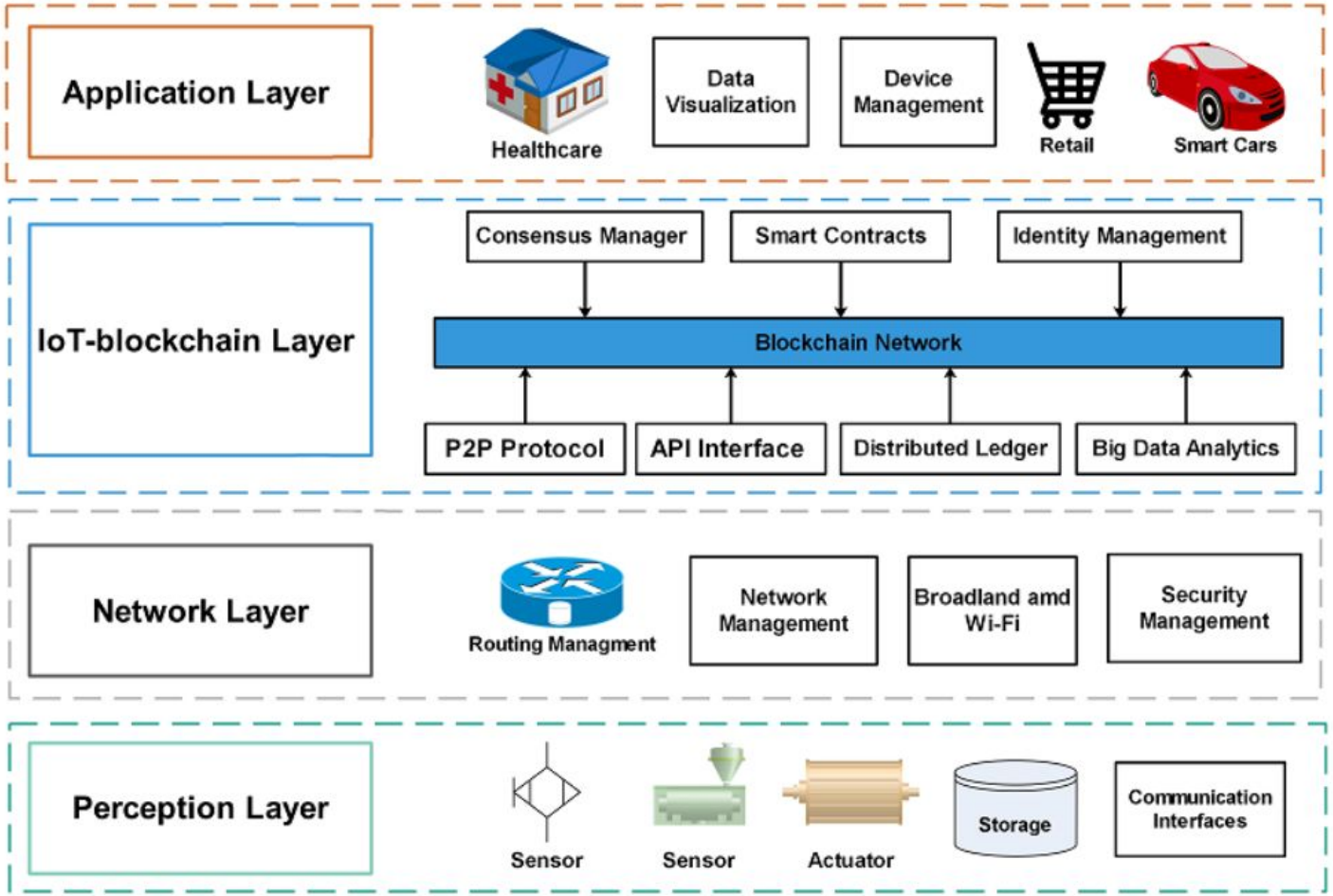
- Sensing capabilities
- Connectivity
- Large scale network
- Big data
- Heterogeneity

IoT Architecture

Centralized IoT Architecture




Application Layer
Smart City
Buildings
Smart Parking
Smart Grid
Connected car
Healthcare
Internet
Network Layer
WI-FI
3G/4G
Broadband
Gateway
Gateway
Perception Layer
WSN
Actuators
RFID
Monitor

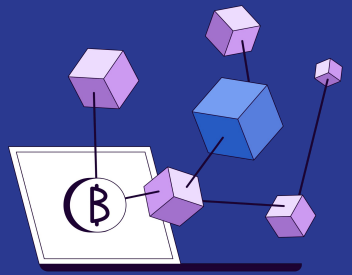


"Design and Implementation of an Integrated IoT Blockchain Platform for Sensing Data Integrity.[8]

challenges of the IoT centralized model[7,5]

- Single Point of Failure
- Security
- Privacy
- Scalability
- Address Space[4]
- Data Integrity
- Susceptibility to Manipulation

Blockchain Technology



Blockchain[6]

- a decentralized database containing sequential, cryptographically linked blocks of digitally signed asset transactions, governed by a consensus model

Core Components of Blockchain

- Transaction
- Block
- Chain
- Hash function
- Miners
- Consensus

common features

- Decentralization
- Transparency
- Immutability
- Better security

comparison between IoT and blockchain

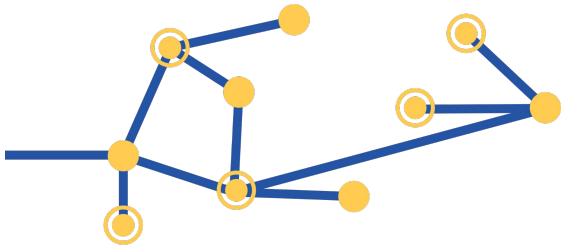
Items	IoT	Blockchain
Privacy	Lack of privacy	Ensures the privacy of the participating nodes
Bandwidth	IoT devices have limited bandwidth and resources	High bandwidth consumption
System Structure	Centralized	Decentralized
Scalability	IoT considered to contain a large number of devices	Scales poorly with a large network
Resources	Resource restricted	Resource consuming
Latency	Demands low latency	Block mining is time-consuming
Security	Security is an issue	Has better security

challenges of the IoT centralized model

- Single Point of Failure
- Security
- Privacy
- Scalability
- Address Space
- Data Integrity
- Susceptibility to Manipulation

MANDALA: A scalable blockchain model with mesh-and-spoke network and H-PBFT consensus algorithm[1]

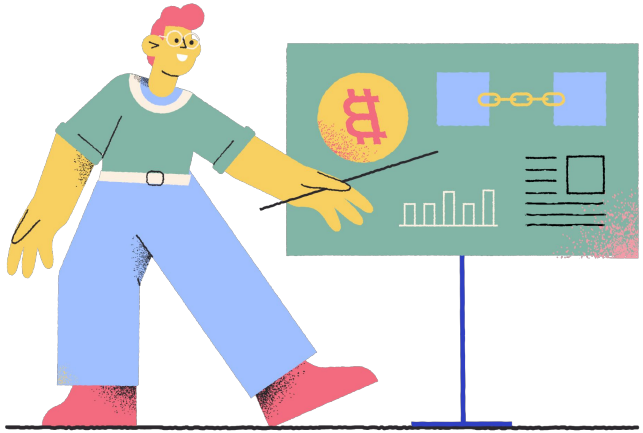
MANDALA Model



- The Mesh-and-Spoke network
- Hierarchical Practical Byzantine Fault Tolerance (H-PBFT)

Blockchain issue

- Poor scalability
- Blockchain cannot keep up with high-frequency operations
  - Bitcoin : 7 transaction per second (tps)
  - Ethereum : 20 ~ 30 transaction per second



network structure adopted by blockchain

- Centralized
  - hub -and-spoke
  - E.g. Napster , Fastpass
- Unstructured
  - organization method of random graph to form a mesh network
  - E.g. Bitcoin, R2trust
- Structured
  - Distributed Hash Table to manage nodes
  - E.g. Ethereum , IoT Scalable Model
- Hybrid
  - selects nodes with higher performance as supernodes to handle search tasks.
  - E.g. RCANE , EOS

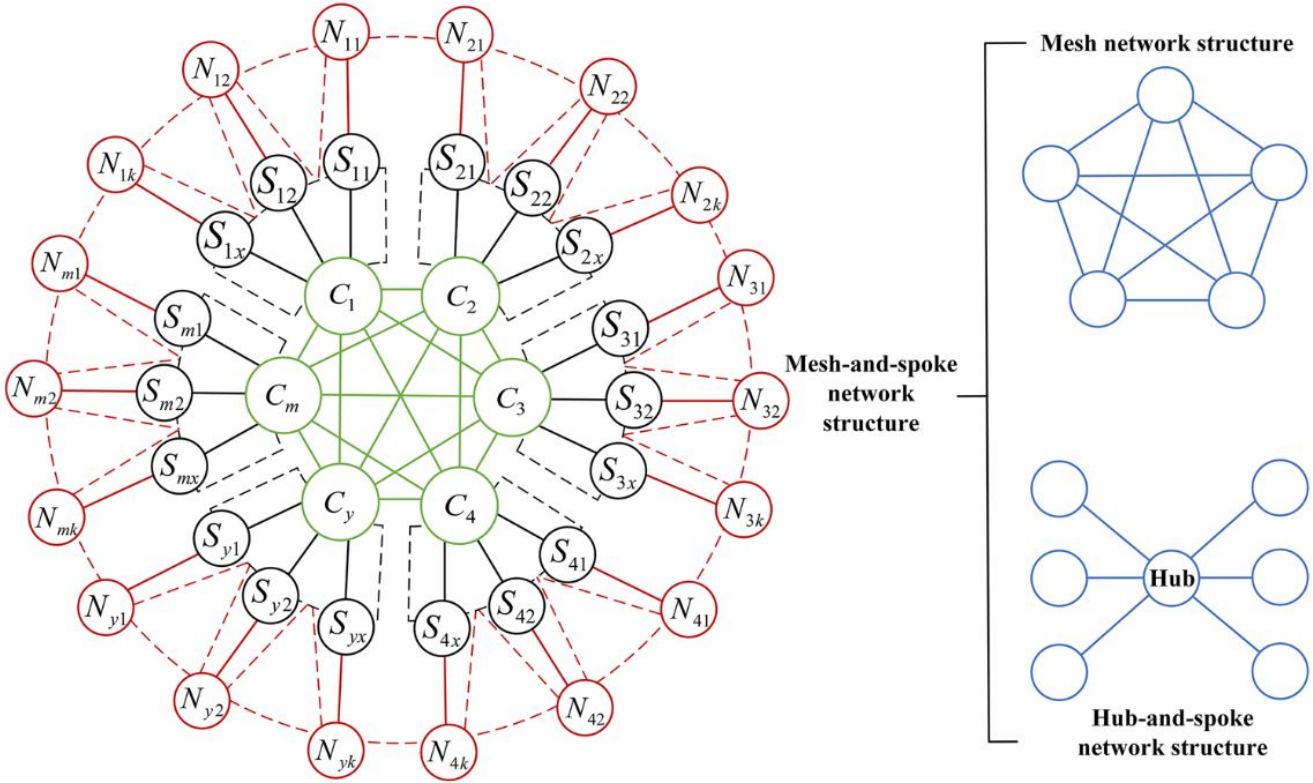
practical Byzantine Fault Tolerance(pBFT)

- feature of a distributed network to reach consensus even when some of the nodes in the network fail to respond or respond with incorrect information
- doesn't consume many computing resources
- communication complexity is as high as $O(N^2)$
  - overhead will increase rapidly

Hierarchical Practical Byzantine Fault Tolerance

- It divides the consensus into several sub-layers
- reduces the communication complexity and improves fault tolerance
- $O(N^{4/3})$

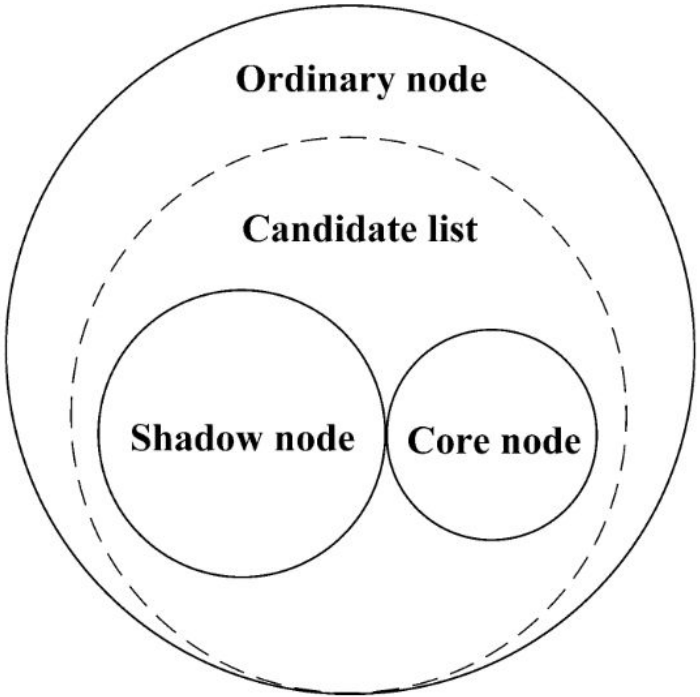
Mesh-and-Spoke network structure



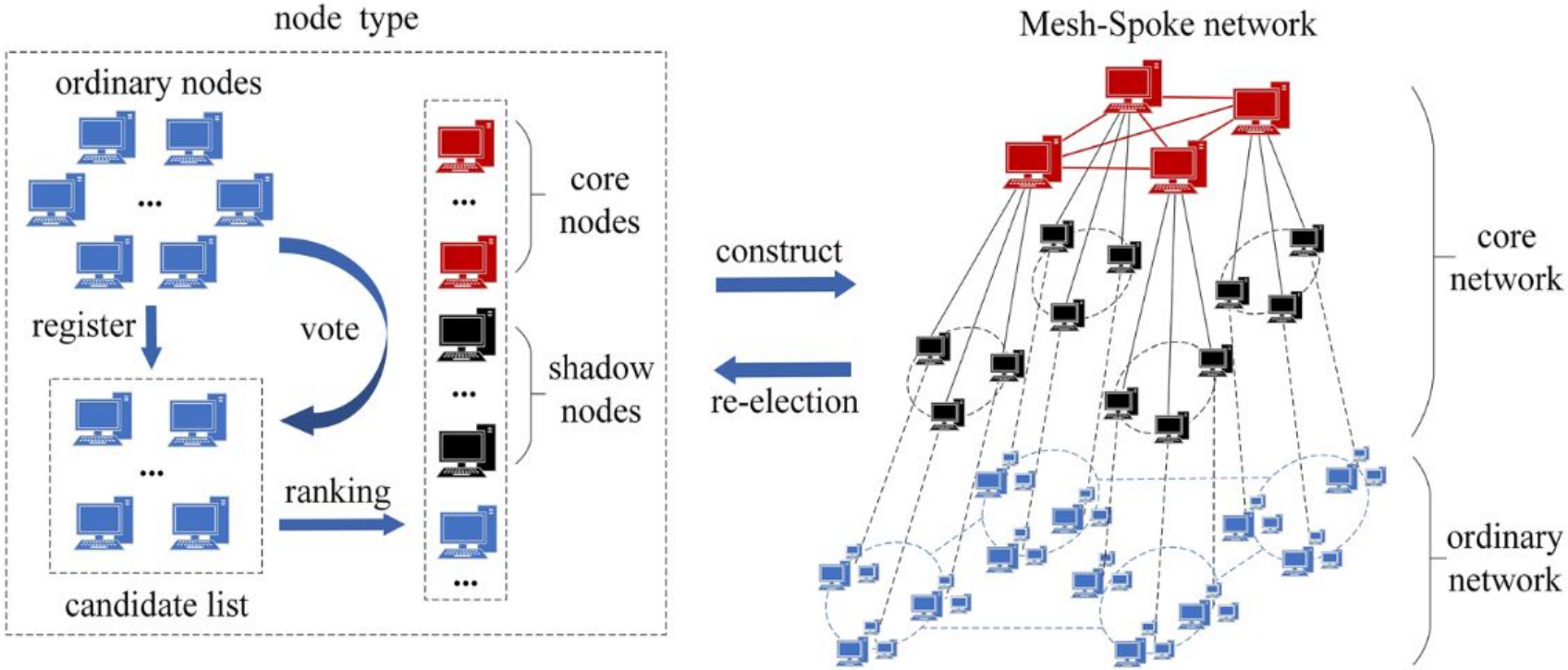
Mesh-and-spoke network

- Core nodes
  - Runs the H-PBFT to generate blocks and reach consensus
  - Receive and verify transactions from shadow nodes
- Shadow Nodes
  - pass messages between core nodes and normal nodes.
  - participate in the consensus and act as a candidate for the core node
- Ordinary
  - sending transactions to the core network
  - Receiving new blocks that have reached consensus

Logical relationship between nodes

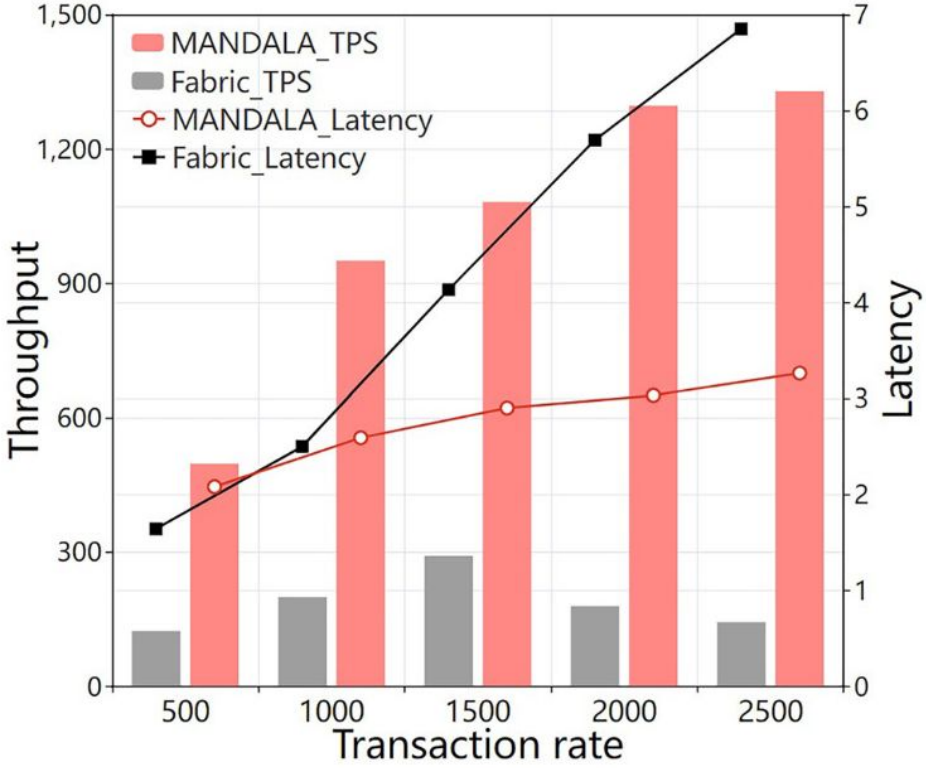


Mesh-and-spoke network(con’t)

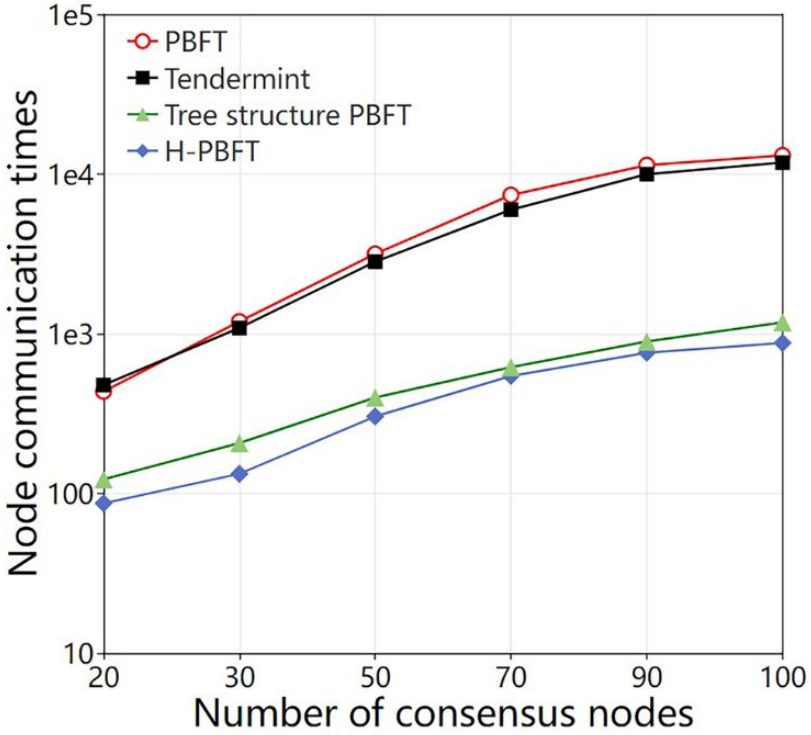


Throughput and latency

- 16 nodes participating in the consensus
- the total number of transactions is fixed at 10,000



Node communication times for consensus process



references

1. Atlam, Hany F., Muhammad Ajmal Azad, Ahmed G. Alzahrani, and Gary Wills. “A Review of Blockchain in Internet of Things and AI.” *Big Data and Cognitive Computing* 4, no. 4 (December 2020): 28. https://doi.org/10.3390/bdcc4040028.
2. Li, Jinze, Xiaofeng Li, He Zhao, Bin Yu, Tong Zhou, Haotian Cheng, and Nianzu Sheng. “MANDALA: A Scalable Blockchain Model with Mesh-and-Spoke Network and H-PBFT Consensus Algorithm.” *Peer-to-Peer Networking and Applications*, October 4, 2022. https://doi.org/10.1007/s12083-022-01373-w.
3. Atlam, Hany, Ahmed Alenezi, Madini Alassafi, and Gary Wills. “Blockchain with Internet of Things: Benefits, Challenges and Future Directions.” *International Journal of Intelligent Systems and Applications* 10 (June 1, 2018). https://doi.org/10.5815/ijisa.2018.06.05.
4. “Blockchain in IoT Security: A Survey | Request PDF.” Accessed December 17, 2022. https://www.researchgate.net/publication/330473352_Blockchain_in_IoT_Security_A_Survey.
5. Fernández-Caramés, Tiago, and Paula Fraga-Lamas. “A Review on the Use of Blockchain for the Internet of Things.” *IEEE Access* 6 (May 31, 2018): 32979–1. https://doi.org/10.1109/ACCESS.2018.2842685.
6. Sultan, Karim, Umar Ruhi, and Rubina Lakhani. *Conceptualizing Blockchains: Characteristics & Applications*, 2018.
7. “A Scalable Blockchain Network Model with Transmission Paths and Neighbor Node Subareas | SpringerLink.” Accessed December 17, 2022. https://link.springer.com/article/10.1007/s00607-021-00913-1.
8. Hang, Lei, and Do-Hyeun Kim. “Design and Implementation of an Integrated IoT Blockchain Platform for Sensing Data Integrity.” Sensors 19, no. 10 (January 2019): 2228. https://doi.org/10.3390/s19102228.