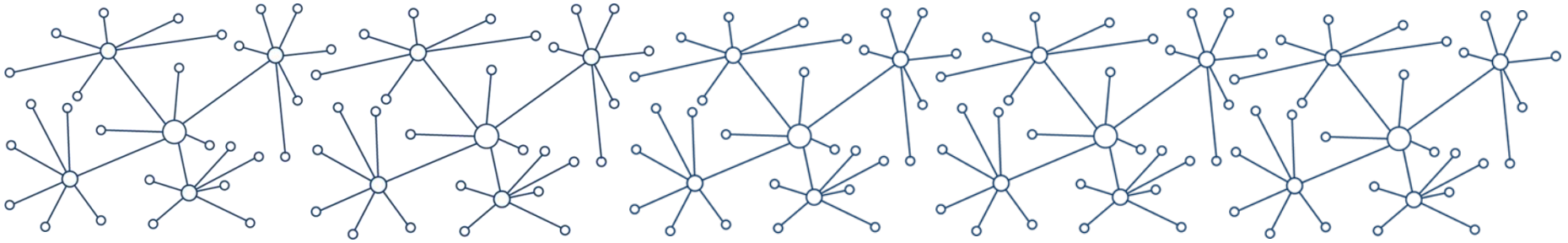


Blockchain Technology

Open Elective @ VJTI - Fall 2019

Lecture#4 (1 August 2019)

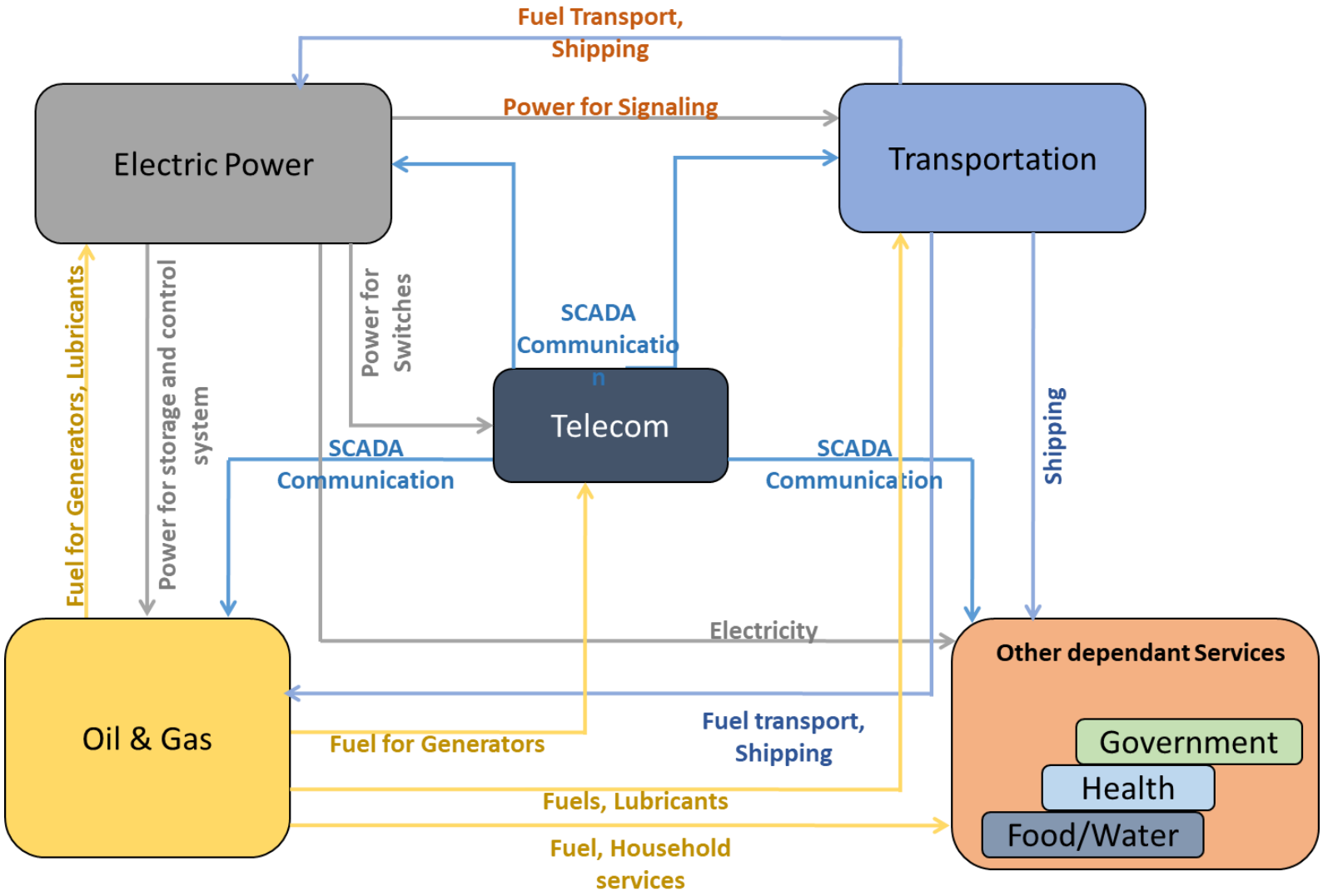
Dhiren Patel

VJTI Mumbai

Concluding Remark of last lecture

- Security: Looking Back
- The historical focus has been to try to build a "wall of protection" around the system or network to protect it from external threats
- this approach worked when organizations were more centralized
- Today – highly connected world!!!!!

CIP (Critical Infrastructure Protection)



Blockchain

- Blockchain is a distributed ledger with confirmed and validated blocks organized in an append-only chain using cryptographic links
- Form of a database (replicated across nodes)
- Transaction(s) → Blocks → Blockchain
- Append-only tree data structure
- Managing the append of the new valid blocks
- Blockchain must contain only blocks that satisfy a given predicate
- Crypto Signature, Hash function, Merkle tree

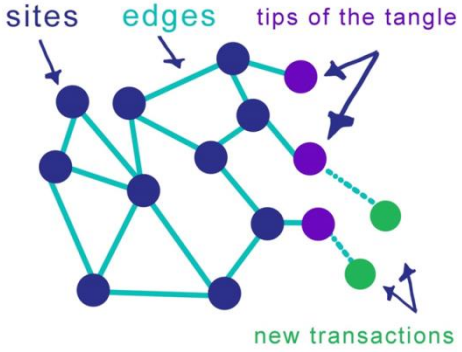
Blockchain characteristics

- Blockchain/DLT (Distibuted Ledger Technology) offers four unique inherent characteristics under certain conditions depending on design and/or implementation:
- Immutability
- Traceability
- Transparency
- Distributed

Blockchain properties (requirements)

- Validation and Synchronization
- Consensus and Update Agreement
- Partition-prone message-passing system
- A formalization of distributed ledgers
- the Monotonic Prefix Consistency
- Distributed maintenance of the Blockchain by many (distrusting) parties makes it achieving “distributed consensus” in real time

Addressing issues Different Blockchains



- Scalability, Security, Sustainability, Usability,
- Community ???
- Bitcoin to Ethereum - Scalability
- Hyperledger – semi-centralized – permissioned Blockchain
- Ripple, Hashgraph, IOTA
- QLDB (Amazon) v/s Blockchain
- (Centralized ledger <transactions history, crypto for signing and verification, centralized>)

Scalability factors

- Consensus mechanism
- Block generation / production (Incentive v/s Energy consumption (difficulty level))
- Block size
- Network Delay
- Transaction Finalization Time (TFT)
- No of blocks required for Confirmation
- Block level or Transaction level confirmation (tangle, hash graph, hyper ledger)
- Extension innovations (Main chain, Side chain, off chain etc.)

Consensus Mechanisms

- Based on Behaviours, Risk factors, and Governance model
- (majority <percentage> is predefined by a policy, Collaborative, Cooperative, Inclusive, Participatory)
- Proof of Work (PoW) //processing time, difficulty level
- Proof of Stake (PoS) //to hold stake
- Proof of Elapsed Time (PoET) //wait time
- Delegated Proof of Stake (DPoS) //approval to selected
- Proof of Activity – mix between PoW and PoS, Proof of Stake Velocity (PoSV), Proof of Importance (PoI)
- Proof of Reputation (PoR) //to keep network secure
- Proof of Authority (PoA) with ZKP (Zero Knowledge Proof)
- Artificial Intelligence Delegated Proof of Contribution (AI-DPoC)

Reference Book

- Mastering Bitcoin (Andreas Antonopoulos, O'Reilly)
- Soft copy on GitHub