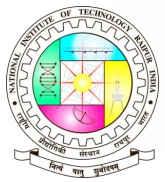
The Chain and the Longest Chain

Dr. Preeti Chandrakar
Assistant Professor

Department of Computer Science and Engineering
National Institute of Technology, Raipur
September 2021

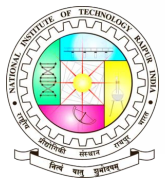
Outline

- Introduction
- The longest chain with more blocks
- Calculate the longest chain
- Adoption of the longest chain
- Miners and the longest chain
- Value of longest chain for transactions

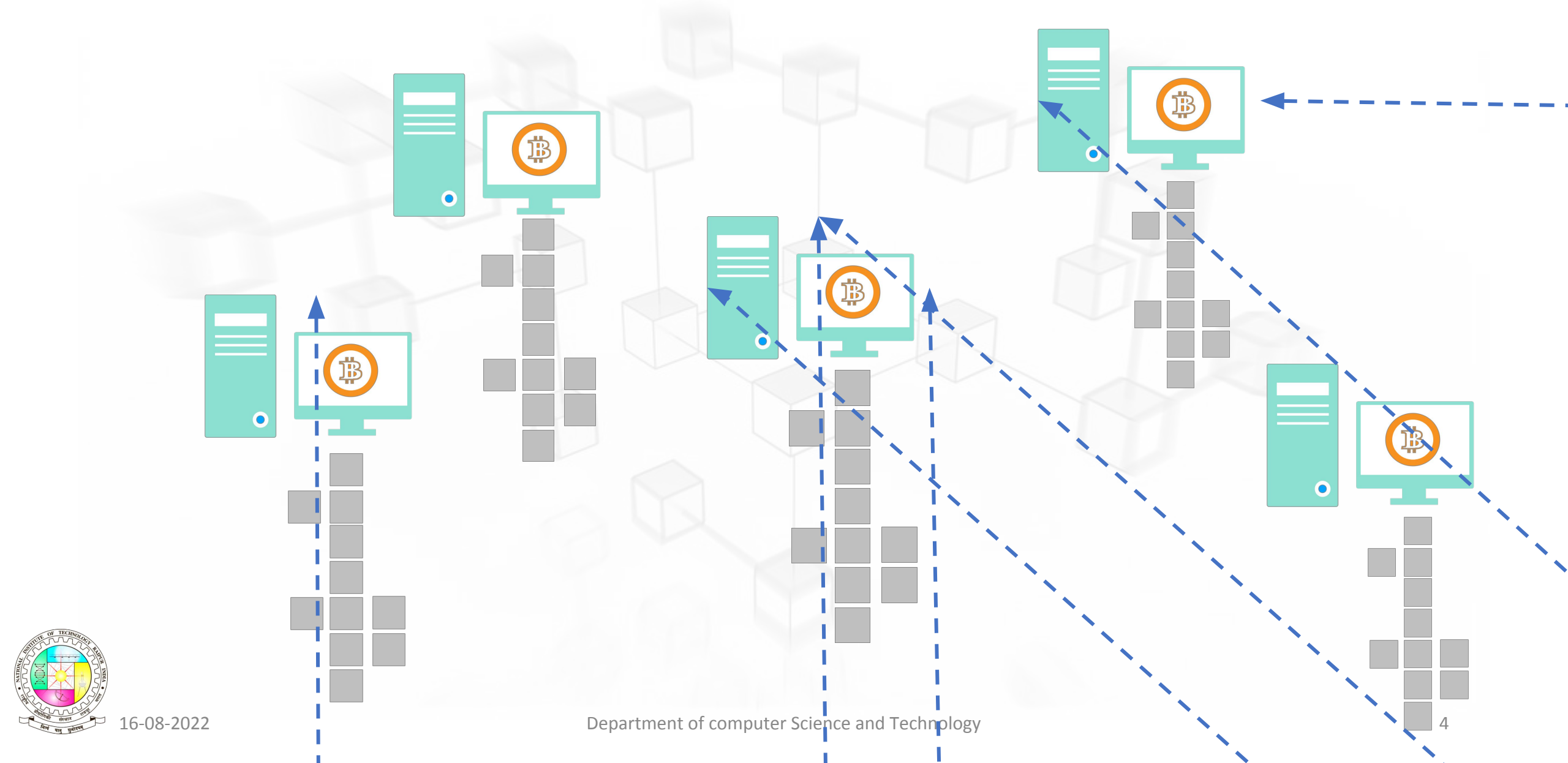


Introduction

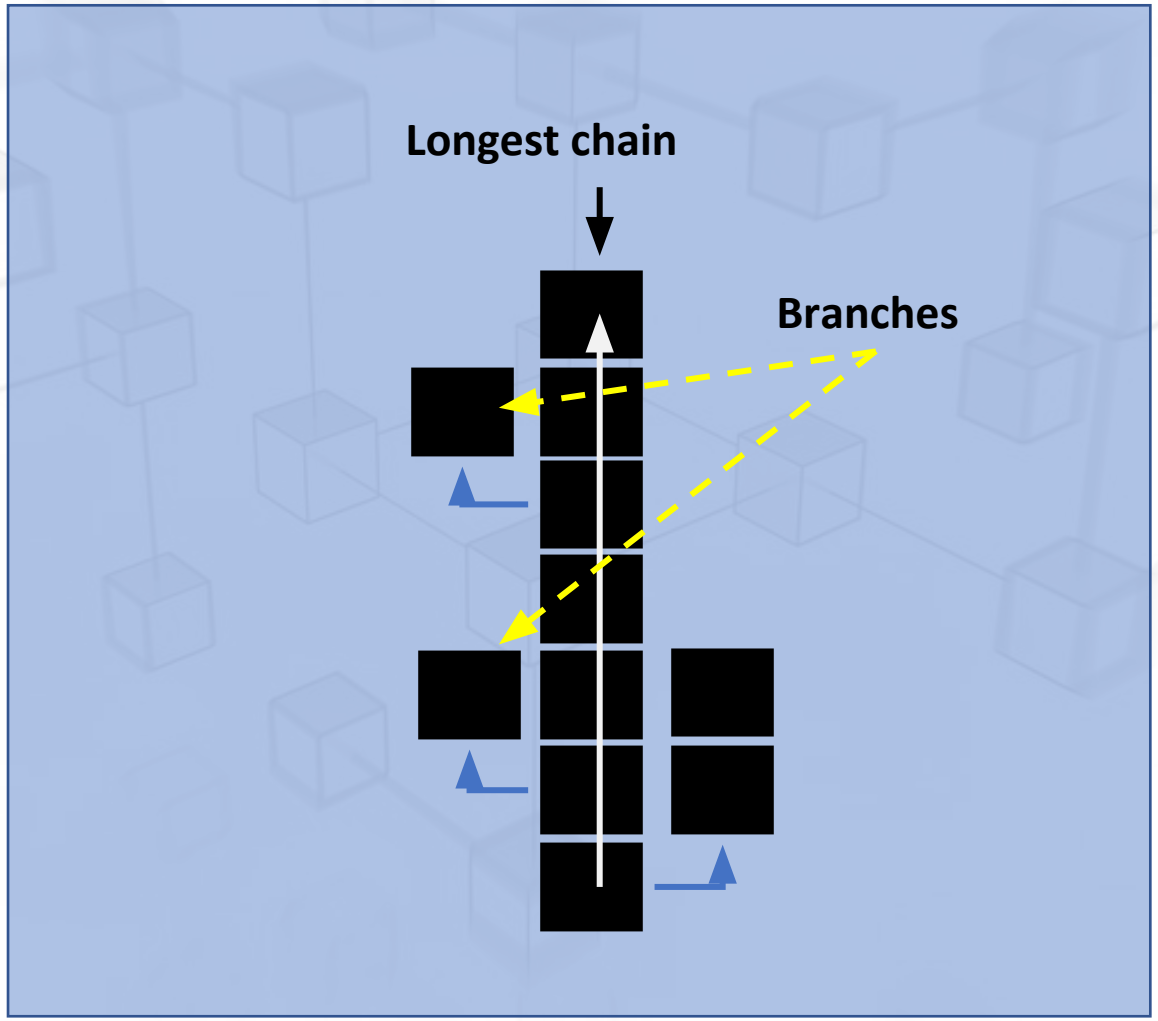
- **The chain** in the bitcoin network, is the *n* number of blocks connected with each other through hash of previous block and form a ledger
- That ledger is known as blockchain
- These blocks are mined and added to the ledger by the miner nodes
- The **longest chain** is what individual nodes accept as the valid version of the blockchain
- When a node adopts a longest chain of blocks, it allow each node to agree on the what's blockchain is looks like as rule of adoption
- Therefore, also must agree on the same transaction history of that longest chain.



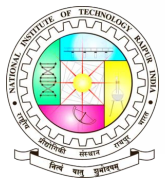
Bitcoin network with chain



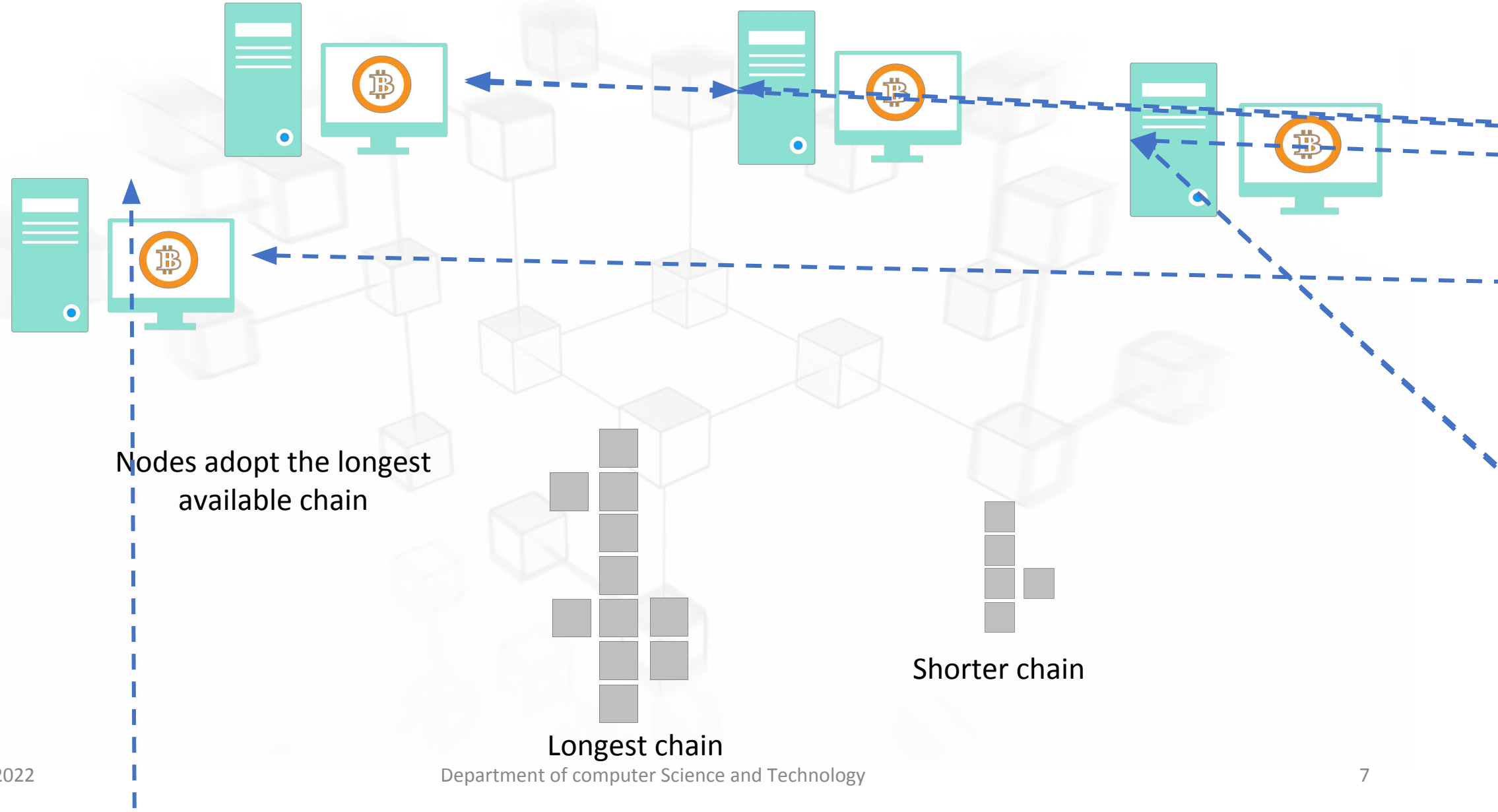
Bitcoin longest chain



- The longest chain is the chain of blocks that took the most effort to build
- To add a new block to the blockchain, need processing power
- Therefore, a blockchain with *more blocks* in it will have taken *more energy* to build than a chain with fewer blocks in it,
- As a rule, nodes will always adopt this chain over a “shorter” one
- So, *nodes will always adopt the chain that took the most energy to build*
- Which is what we mean when we refer to the “longest chain”

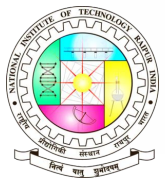


Bitcoin network with chain

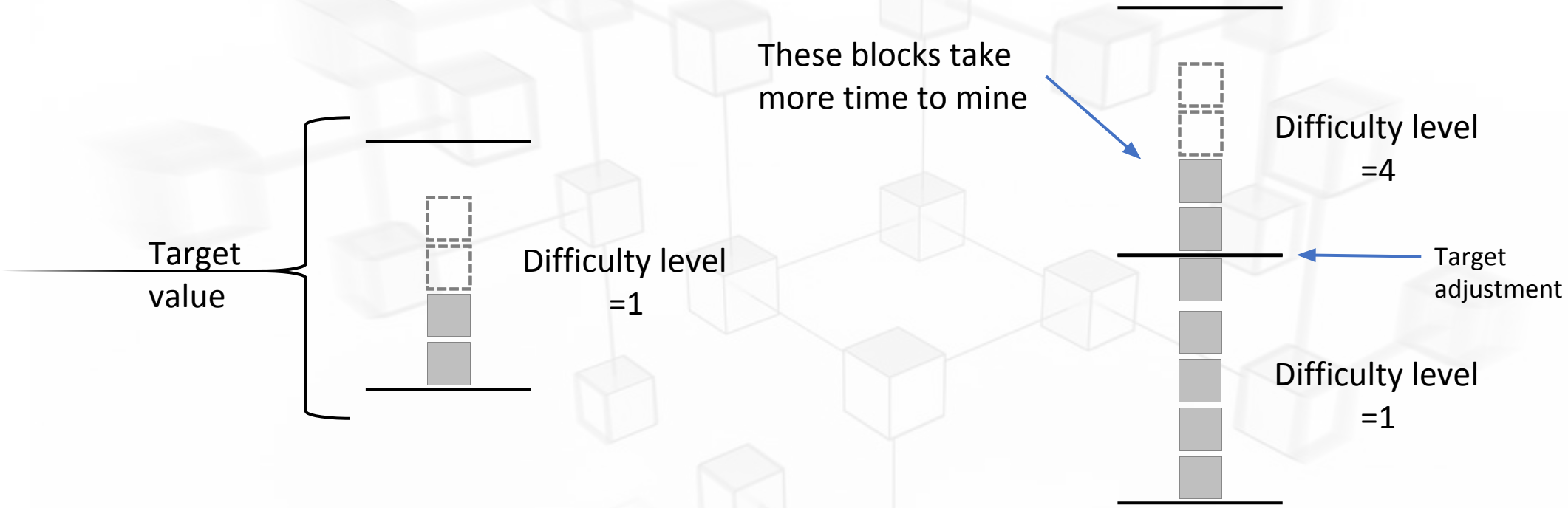


The longest chain with more blocks

- The chain that required the most energy to build, is not necessarily the one with the most blocks in it
- The difficulty changes mean that some blocks are going to require more energy to mine than others
- With the same difficulty period every new block requires the same amount of effort to mine,
- Therefore, adds the same amount of “work” to the chain
- However, if the difficulty increases (because blocks were mined more quickly than every 10 minutes on average)
- The blocks in the new difficulty period are going to take *more effort* to mine on to the blockchain
- Nodes adopt the chain with the most work, they wouldn’t adopt a chain with *more* blocks in it if it didn’t require as much work to build.

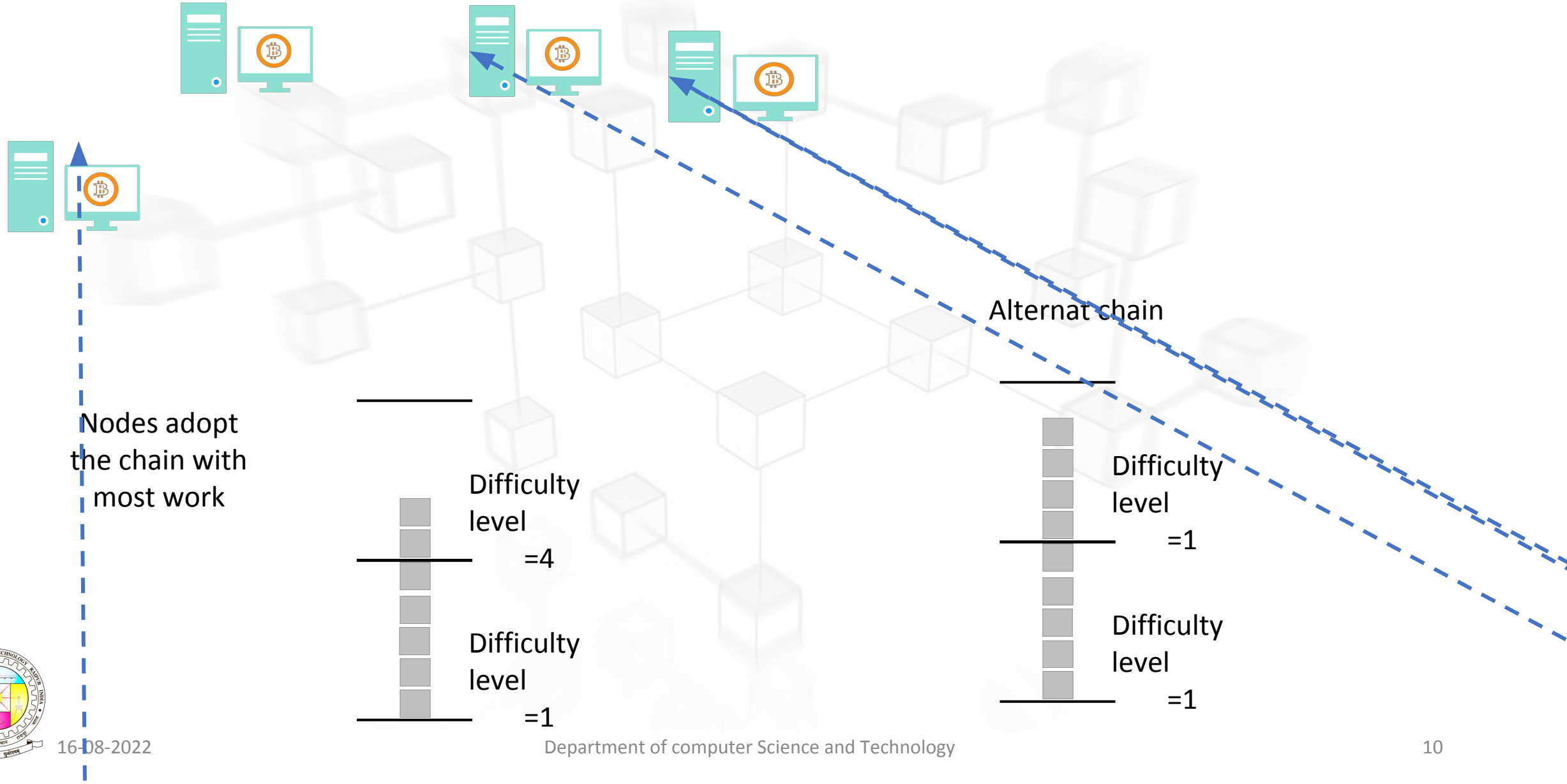


The longest chain with more blocks



*The **target** is what blocks must get under to be added on to the chain.

The longest chain with more blocks

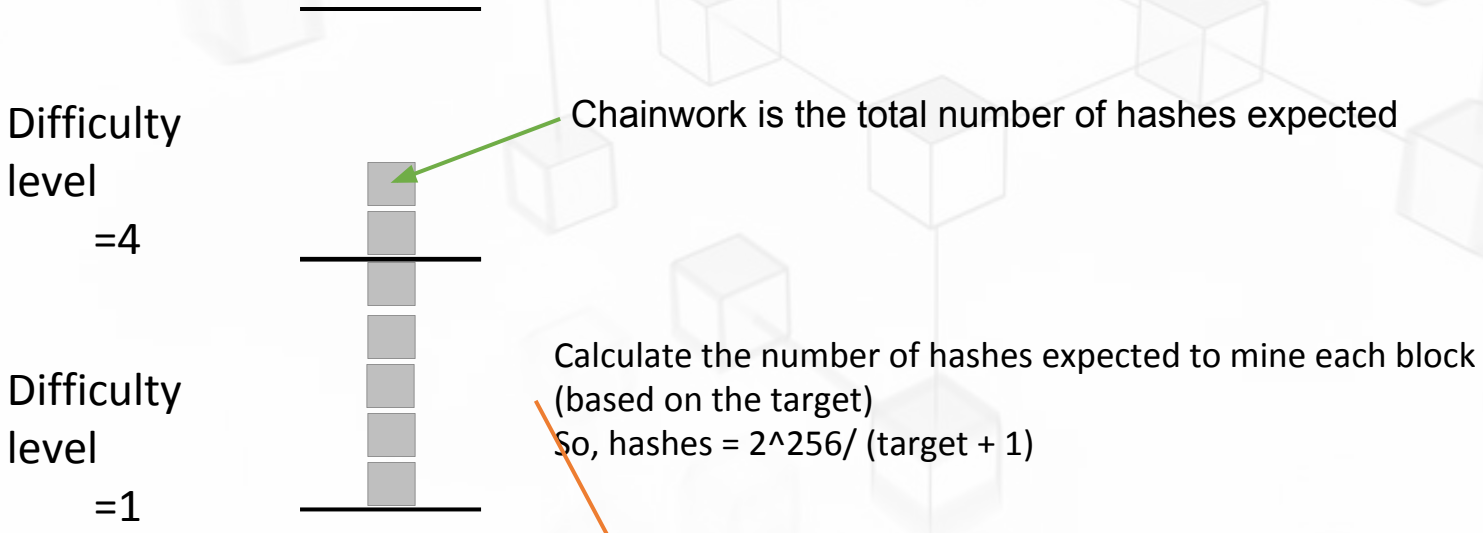


Calculate the longest chain

- The longest chain is measured by a metric called “chainwork”.
- **Chainwork** is the total number of hashes that are expected to have been necessary to produce the current chain.

Pieter Wuille

- To work out chainwork, you just need to work out how many hashes you would have needed to perform to mine each block in the chain, then add them up.

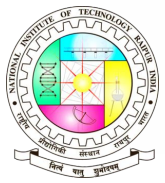


*The average expected number of hashes for each block depends on what the target was at the time.

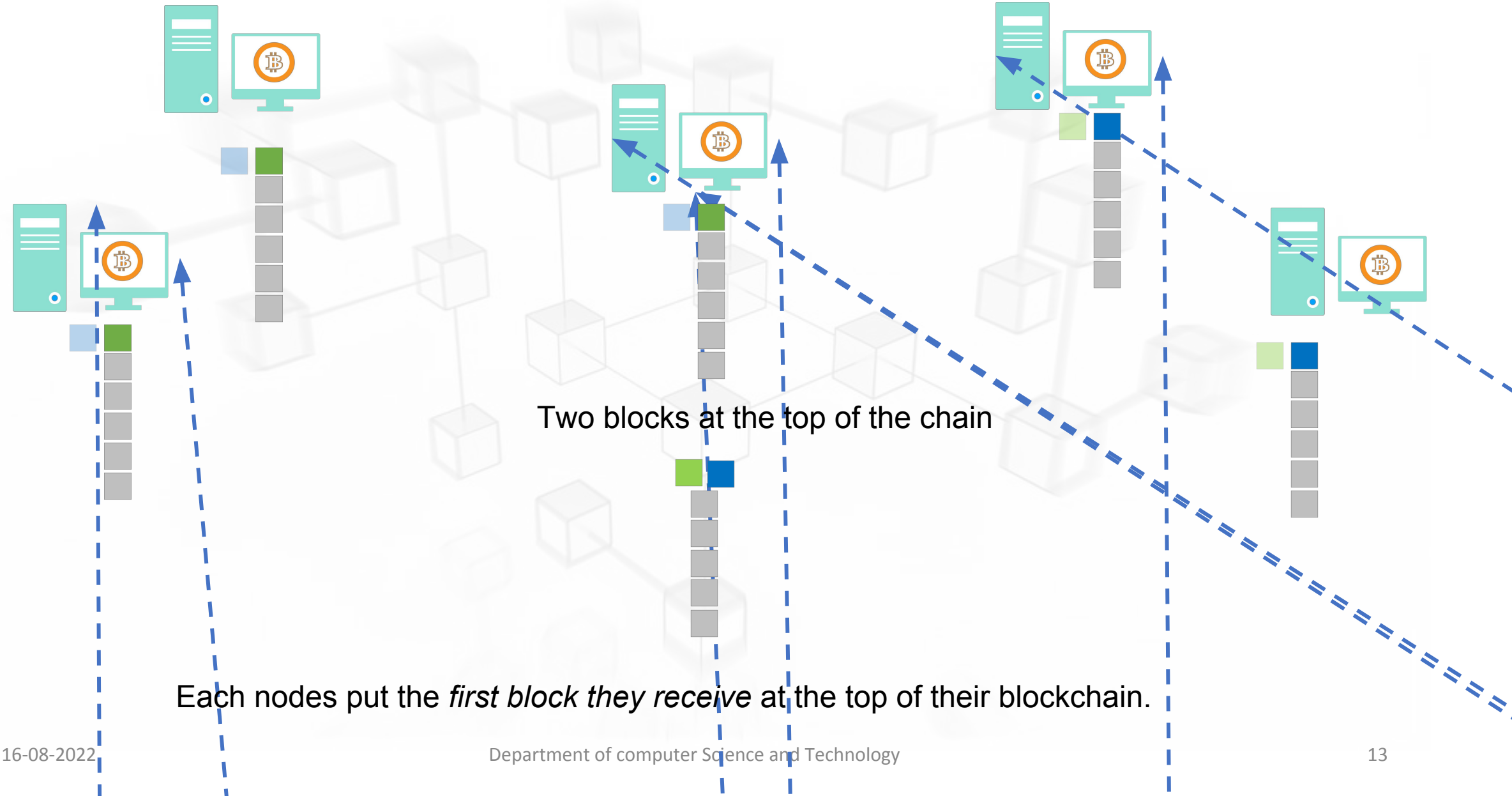
Adoption of the longest chain

- For a node, Adopting longest available chain allows to have same view of the blockchain
- Following two examples of prove why it is helpful in adding block in blockchain

1. **Resolving disagreements when two blocks are mined at the same time.**
   - When two block are generate at the same time then which one add to the longest chain ?
   - This situation can be resolved by having nodes adopt the longest chain of blocks.
   - This is because the **next block to be mined** will build upon *one* of these two blocks,
   - creating a new longest chain that all nodes on the network will be happy to adopt

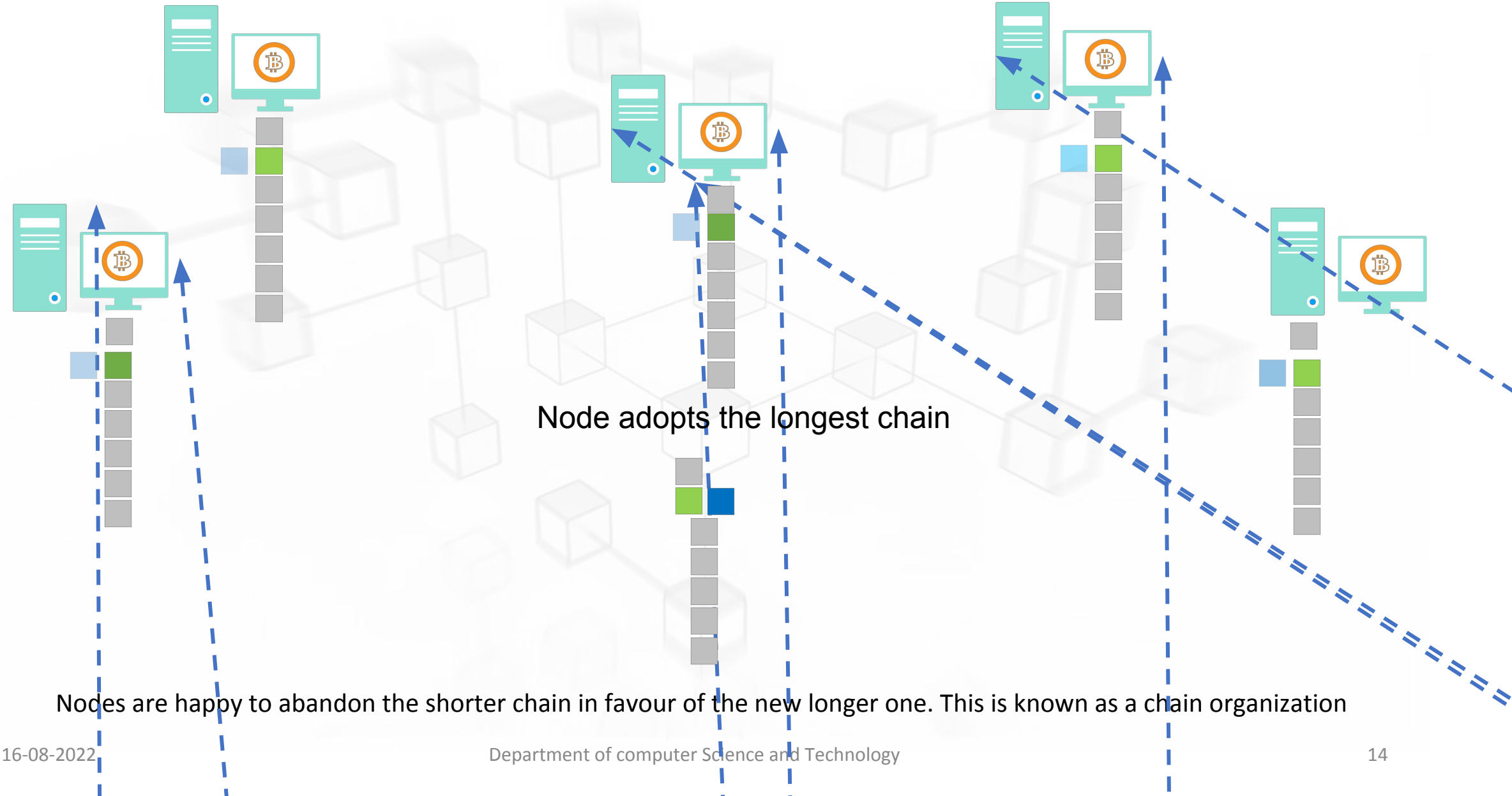


Adoption of the longest chain



Each nodes put the *first block they receive* at the top of their blockchain.

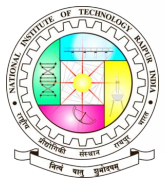
Adoption of the longest chain



Nodes are happy to abandon the shorter chain in favour of the new longer one. This is known as a chain organization

Adoption of the longest chain

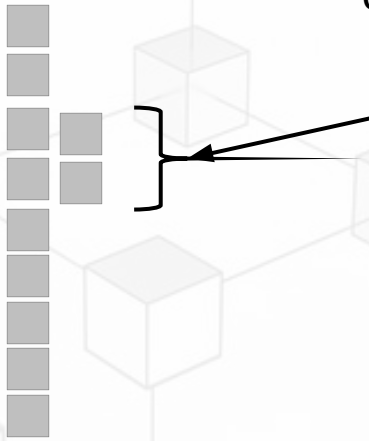
2. **Protecting blocks already mined on to the blockchain.**
    - The fact that nodes always adopt the longest chain as the valid version of the blockchain
    - If anyone wanted to replace a transaction in the blockchain,
    - they would need to work to build a *new longest chain* *to replace the current one*
    - However, if the majority of miners are continually working to extend the same current longest known chain
    - An individual miner won't be able to compete to outwork all of the other miners
    - The combined effort of miners protects existing blocks and transactions from being replaced by a single miner.



Adoption of the longest chain

All miners work to extend the current longest chain

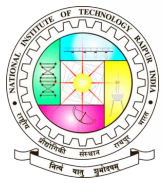
It is not possible to a single miner that he can replace the current longest chain



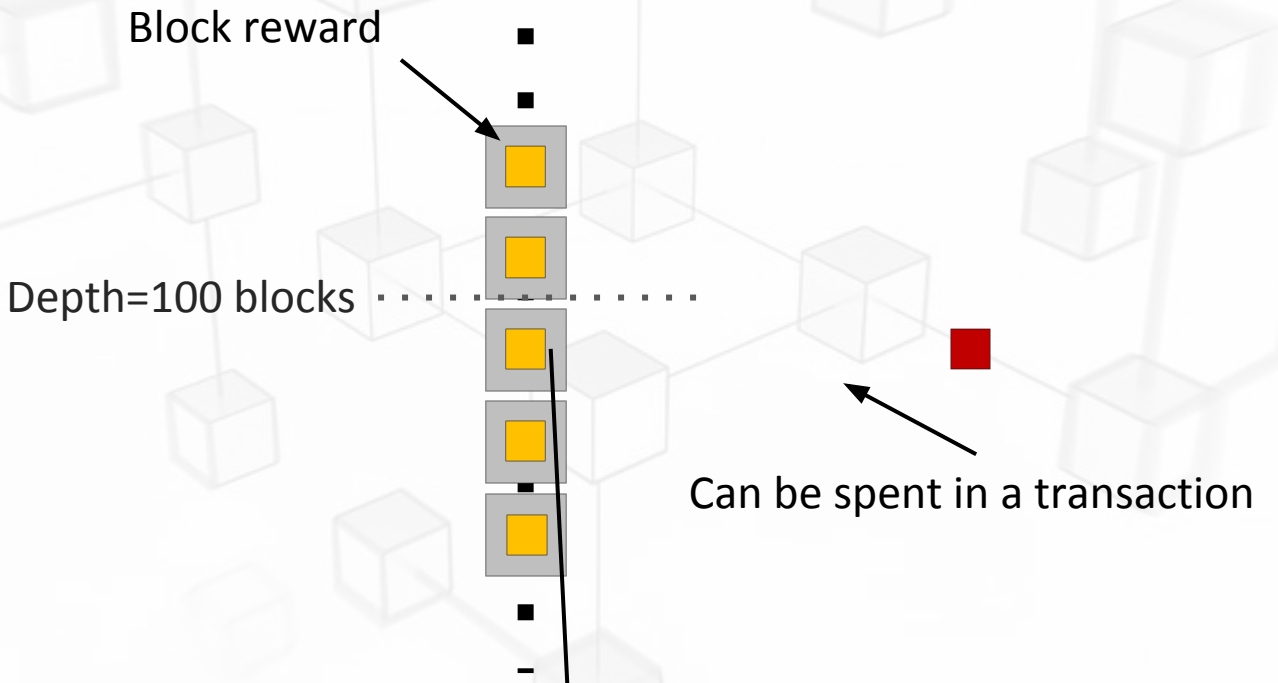
The majority of mining power to be able to out-run all other miners and build a new longest chain is known as a 51% attack.

Miners and the longest chain

- Because a miner can claim a block reward if they are able to mine a block.
- Furthermore, the bitcoins from this block reward can only be spent if the block becomes 100 blocks deep in the longest chain.
- Therefore, this block reward incentivizes miners to always try and mine new blocks that will become part of the longest chain (by always trying to build on to the current longest one).



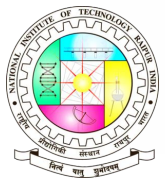
Miners and the longest chain



A block reward can only be spent if the block is part of the longest chain.

Value of longest chain for transactions

- A transaction inside a block that is not part of the longest chain is invalid, If any node try to spend the bitcoins from a transaction that is not in the longest chain
- Nodes would not accept it nor try to mine it into a block
- This is because nodes only consider the longest chain the valid history of transactions
- Anything outside of that is not a valid transaction



Value of longest chain for transactions