Blockchain Technology
(BITS F452)

BITS Pilani
Pilani Campus

Dr. Ashutosh Bhatia, Dr. Kamlesh Tiwari
Department of Computer Science and Information Systems

innovate achieve lead

BITS Pilani

Pilani Campus

Proof of Work

Remaining Problems

How to pick a random node?

How to avoid a free-for-all due to rewards?

How to prevent the Sybil attack?

Are of these problems are related and have same solution :
Proof of Work

Proof of Work

To approximate selecting a random node

select node in proportion to a resource that no one can monopolize (we hope)

- In proportion to computing power : Proof-of-Work
- In proportion to ownership: Proof-of-stake

Idea: allow nodes to compete with each other using their computing power that implies the nodes automatically being picked in that proportion

Equivalent views of POW

1. Select nodes in proporation to computing power

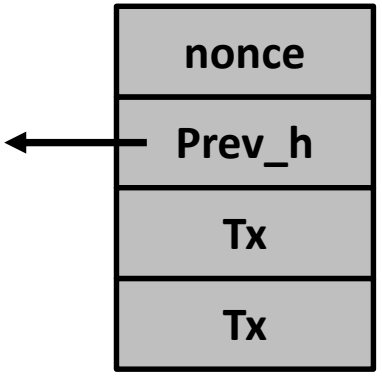
2. Let nodes compete for right to create blocks

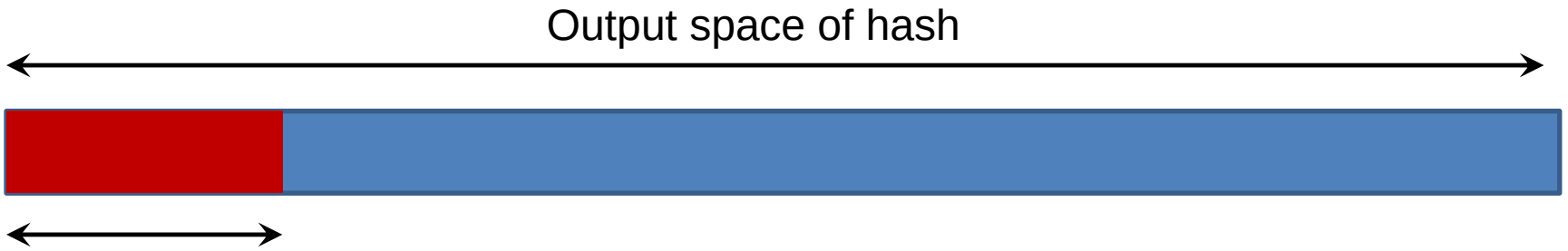
3. Make it moderately hard to create new identities
   protection against Sybill attack

Hash Puzzles

To create block, find nonce (a random value) such that

H(nonce || prev_hash || tx || tx || ... || tx) < target





If hash function is secure:
Only way to succeed is to try enough nonces until you get lucky

POW property 1: difficult to compute

innovate achieve lead

As of Feb 2022 the bitcoin difficulty is **26.69×10^{12}** hashes

It requires approximately **2.7×10^{15}** hashes to create one BITCOIN

Only some nodes bother to compete - minors

POW property 2: parameterizable cost

innovate achieve lead

Nodes automatically re-calculate the target every two weeks

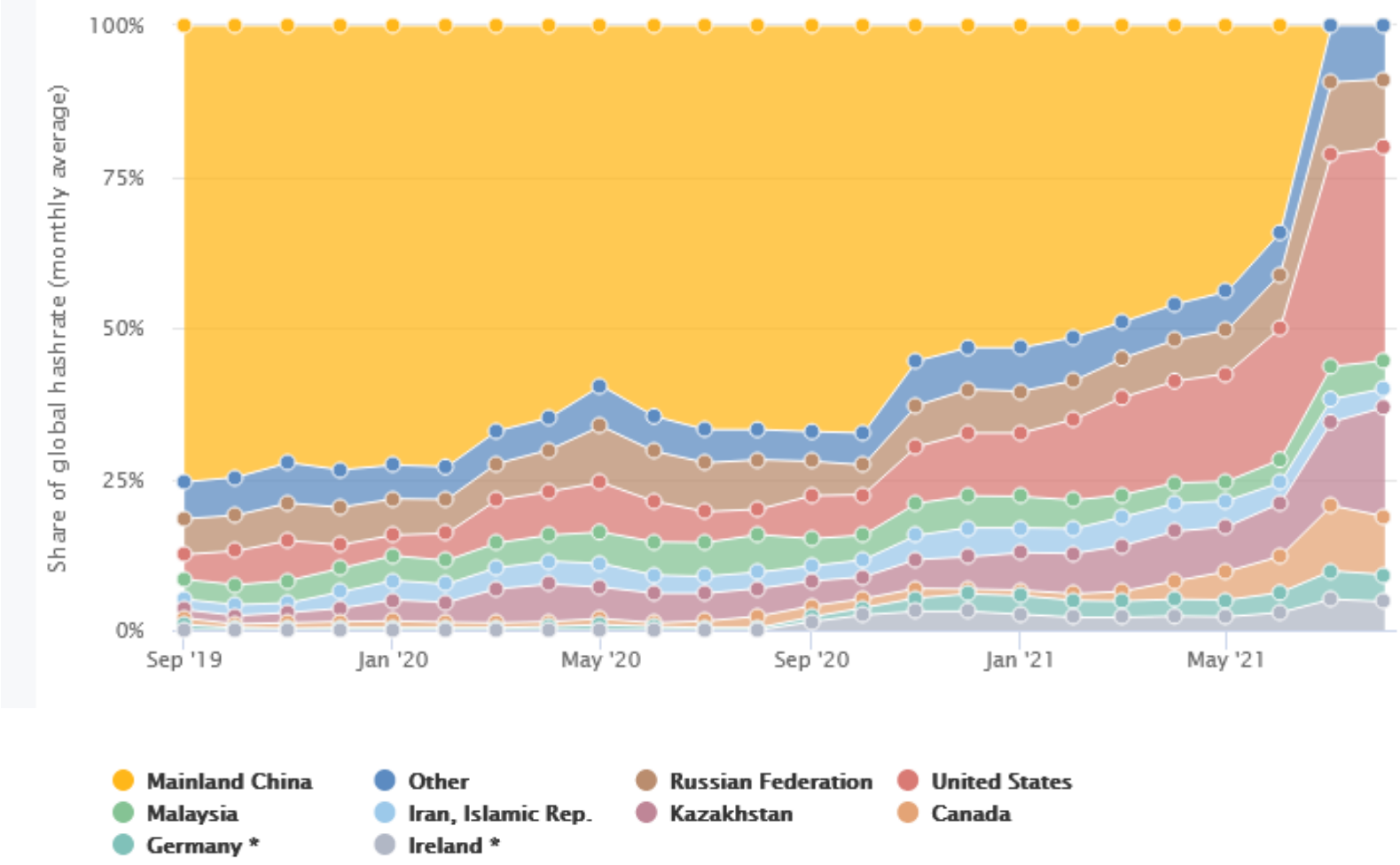
Goal average time between blocks = 10 minutes

Each 2016-block interval is known as a ***difficulty epoch***. At the beginning of every epoch the Bitcoin network recalculates the Current Target.

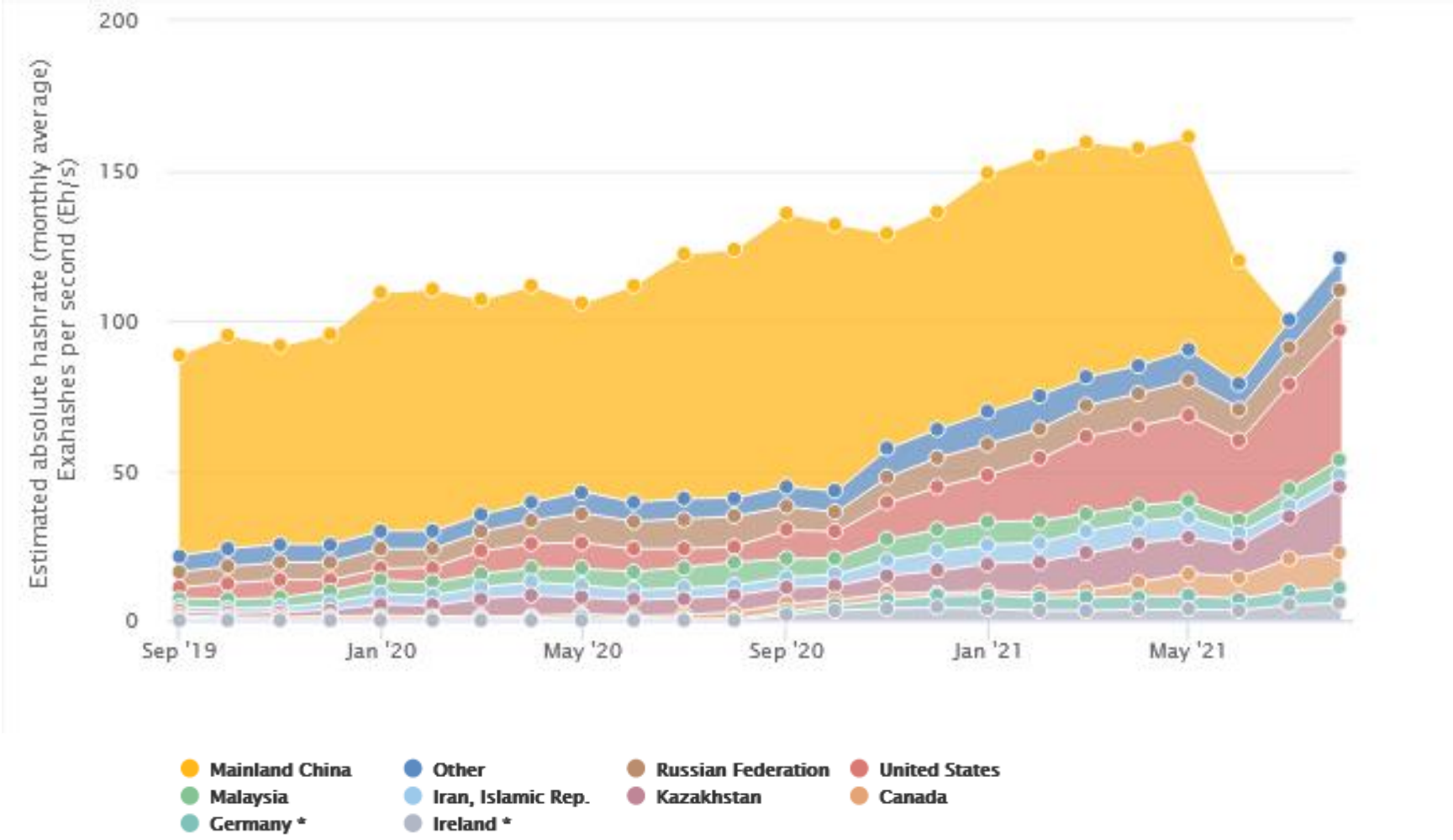
If if you put a fixed amount of H/W for mining the rate at which you find the block depends upon the total computer power available with others

Prob (Alice wins the next block) = fraction of global hash power she controls

- Distribution of Bitcoin mining by country



BITCOIN Global Hashrate



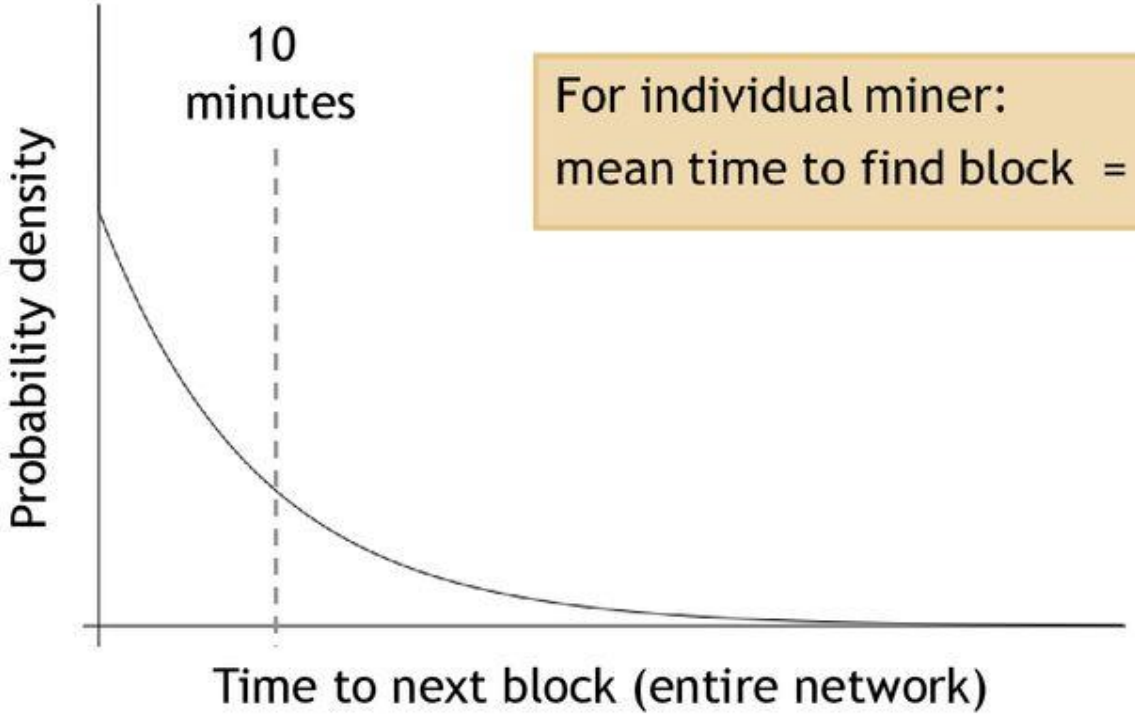
Key Security Assumptions

innovate achieve lead

Attacs infeasible if majority of minors weighted by hash power follow the protocol

This will ensure a more than 50% chance that the next node is proposed by a honest node

Solving hash puzzles is probabilistic



For individual miner:

$$\text{mean time to find block} = \frac{10 \text{ minutes}}{\text{fraction of hash power}}$$

PoW property 3: trivial to verify

Nonce must be published as part of block

Other miners simply verify that
H(nonce prev_hash tx … tx) < target

Advantage?

No centralized verifier needed! Any node or miner can verify that the block was correctly mined

Mining economics

If mining reward (block reward + Tx fees)	>	mining cost (hardware + electricity cost)	→	Profit

Complications:

- Fixed (hardware) vs. variable (electricity) costs
- Reward depends on rate at which miners propose blocks (ratio of their hash rate to the global hash rate)
- Cost in dollars, but reward in BTC → profit depends on exchange rate

Recap

Identities

Transactions

P2P network

Block chain & consensus

Hash puzzles & mining

Bitcoin has three types of consensus

- Value
- State
- Rules

Bitcoin is bootstrapped