SNS COLLEGE OF TECHNOLOGY

Coimbatore-35
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 INFORMATION TECHNOLOGY

BLOCK CHAIN AND CRYPTOCURRENCY

IV YEAR - VII SEM

UNIT 3 - **DISTRIBUTED CONSENSUS & BLOCK CHAIN APPLICATIONS**

Recap of the Last Lecture

- Byzantine Generals Problem
- Definition of Byzantine adversary
  - **Byzantine:** Adversarial nodes can deviate from the protocol arbitrarily!
- Synchronous and asynchronous networks
  - **Synchronous network:** known upper bound Δ on network delay
- Byzantine Broadcast
- Dolev-Strong (1983)
- State Machine Replication (SMR)
- Security properties for SMR protocols: Safety and Liveness

Sybil Attack

How to select the nodes that participate in consensus?

Two variants:

- *Permissioned:* There is a *fixed* set of nodes (previous lecture).
- *Permissionless*: Anyone is free to join the protocol at any time.

Can we accept any node that has a signing key to participate in consensus?

Sybil Attack!

Sybil Attack

How to select the nodes that participate in consensus?

Two variants:

- *Permissioned:* There is a *fixed* set of nodes (previous lecture).
- *Permissionless*: Anyone is free to join the protocol at any time.

Can we accept any node that has a signing key to participate in consensus?

In a **sybil attack**, a single adversary impersonates many different nodes, outnumbering the honest nodes and potentially disrupting consensus.

Sybil Resistance

Consensus protocols with Sybil resistance are typically based on a bounded (scarce) resource:

	Resource dedicated to the protocol	Some Example Blockchains
Proof-of-Work	Total computational power	Bitcoin, PoW Ethereum…
Proof-of-Stake	Total number of coins	Algorand, Cardano, Cosmos, PoS Ethereum…
Proof-of-Space/Time	Total storage across time	Chia, Filecoin…

How does Proof-of-Work prevent Sybil attacks?

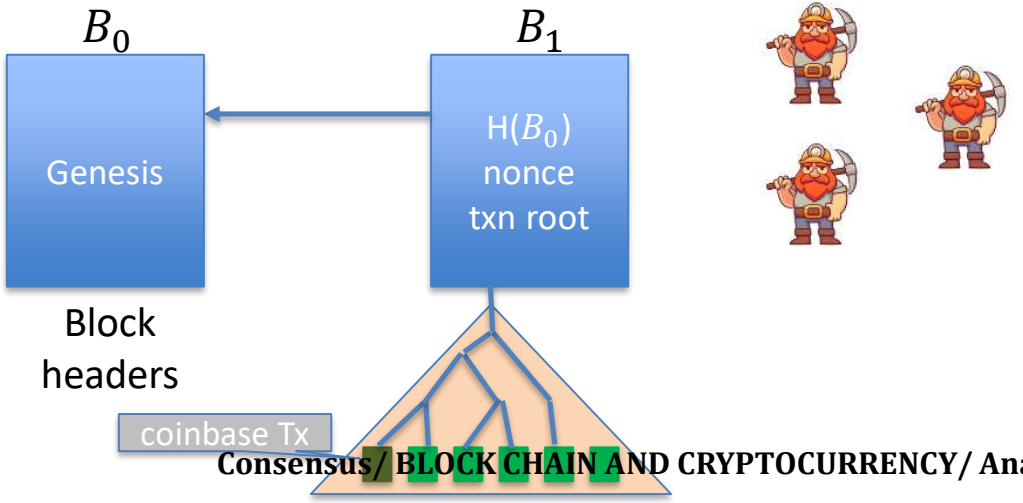
We assume that the adversary controls a small fraction of the scarce resource!
Resource gives the power to influence the protocol.
Adversary has less influence than honest nodes.

Bitcoin: Mining

To mine a new block, a miner must find *nonce* such that

$$H\left(h_{prev}, \text{txn root}, \text{nonce}\right) < \text{Target} = \frac{2^{256}}{D}$$

Each miner tries different nonces until one of them finds a nonce that satisfies the above equation.



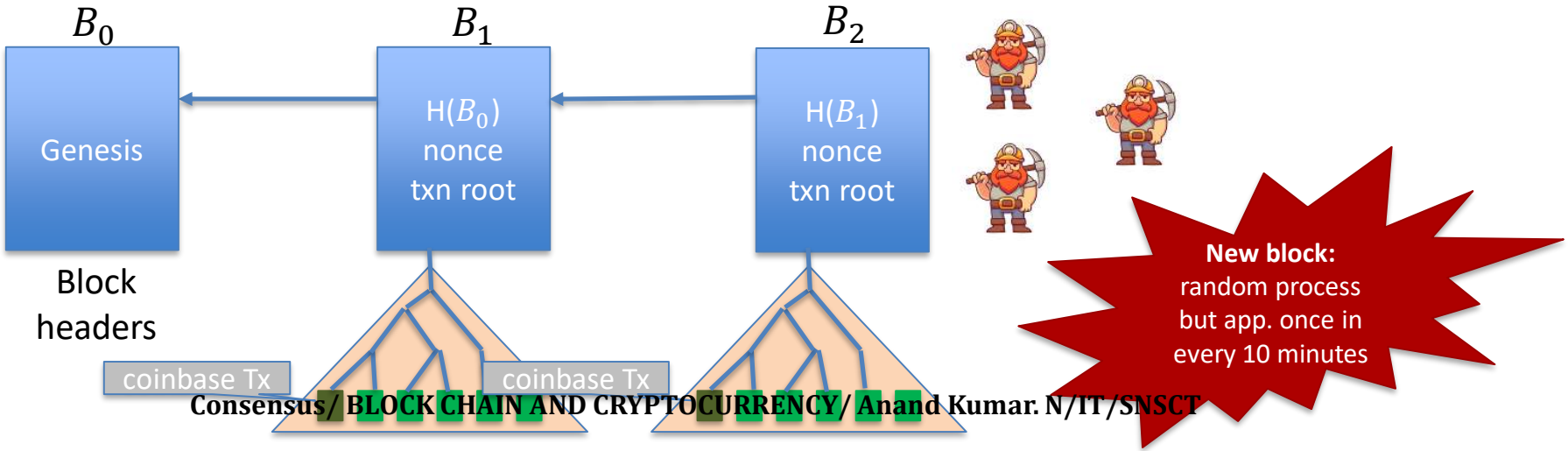
Bitcoin: Mining

To mine a new block, a miner must find *nonce* such that

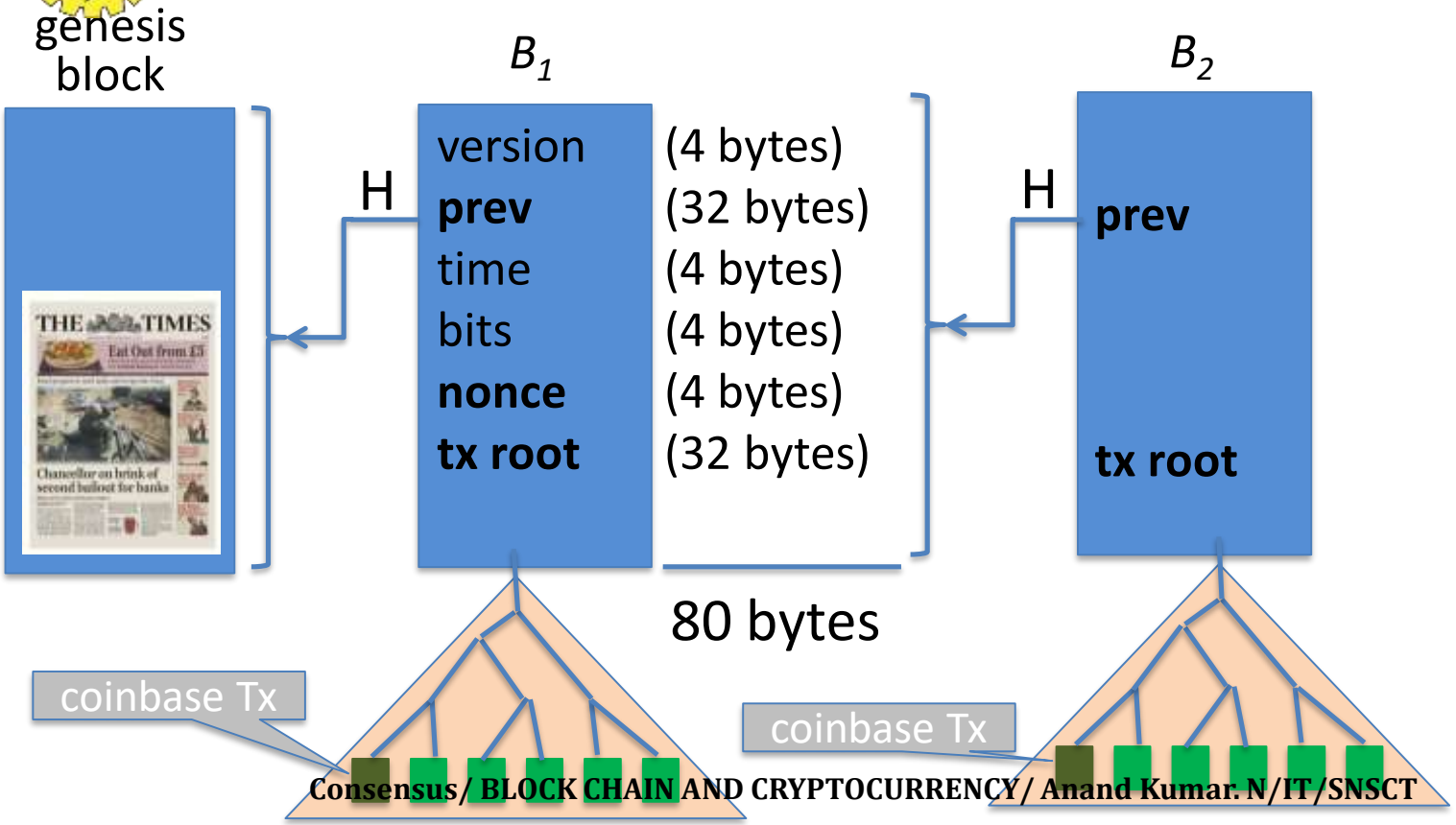
$$H(h_{prev}, \text{txn root}, \text{nonce}) < \text{Target} = \frac{2^{256}}{D}$$

Difficulty: How many nonces on average miners try until finding a block?

Each miner tries different nonces until one of them finds a nonce that satisfies the above equation.



Bitcoin: Mining



Bitcoin: Mining