The Bitcoin Cryptocurrency: Part 6

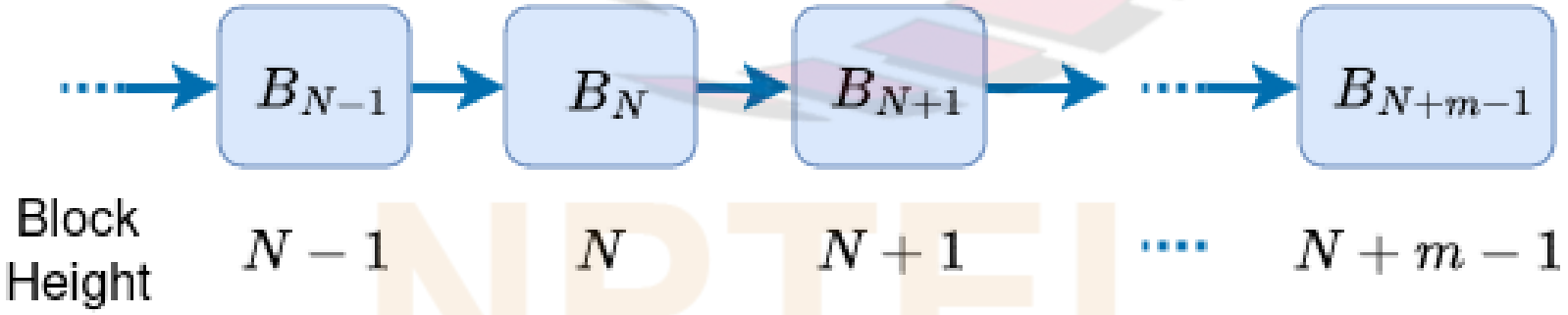
Gaurav S. Kasbekar
Dept. of Electrical Engineering
IIT Bombay

References

- Saravanan Vijayakumaran, "*An Introduction to Bitcoin*", Lecture notes, IIT Bombay, Oct. 4, 2017. Available at: https://www.ee.iitb.ac.in/~sarva/bitcoin.html
- A. Narayanan, J. Bonneau, E. Felten, A. Miller, S. Goldfeder, "*Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*", Princeton University Press, 2016

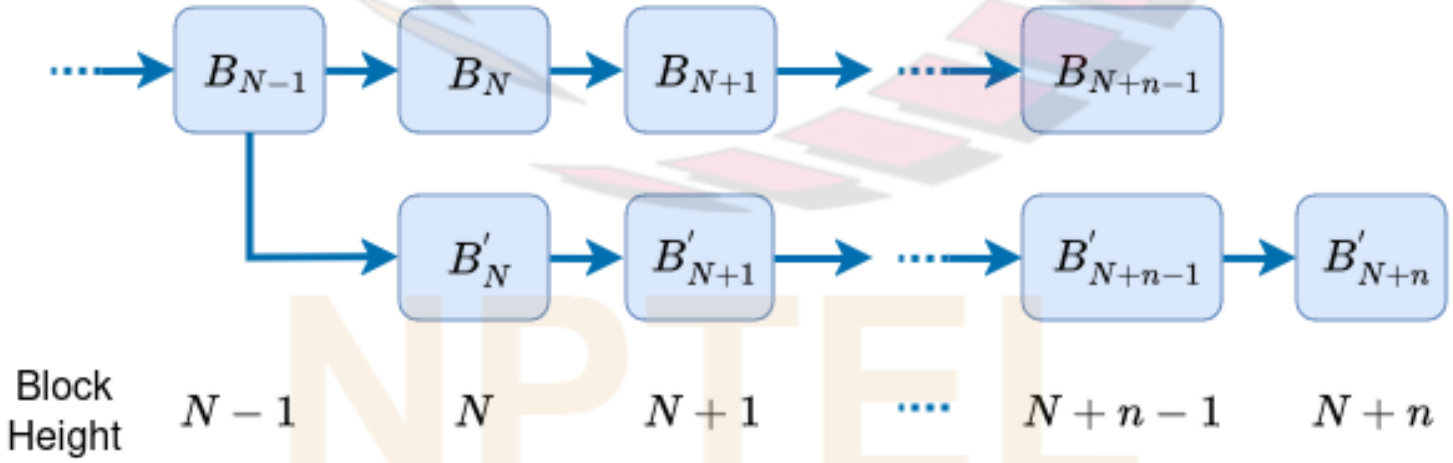
Blockchain Integrity

- Suppose Alice wants to modify an existing block B_N, which:
  - ❑is at height N in blockchain
  - ❑has received m confirmations
- E.g., Alice may want to delete a transaction from B_N
- Let B'_N be the modified block



Bitcoin Integrity (contd.)

- To replace B_N with B'_N in all the copies of the blockchain stored across the Bitcoin network, Alice must:
  - ❑ create a branch containing B'_N which is longer than branch containing B_N and broadcast it
    - once all the nodes in the Bitcoin network switch to the branch containing B'_N, it will become the block at height N in blockchain
- However, assuming that Alice controls less than 50% of the network hash rate:
  - ❑ the larger the value of m, the less likely it is that Alice is able to create a branch containing B'_N which is longer than branch containing B_N
- E.g.: assuming Alice controls a fraction of the network hash rate which is less than 0.4, it is nearly impossible for her (probability less than 1.05×10^{-9}) to tamper with blocks which have received 50 or more confirmations



Blockchain Integrity (contd.)

- Suppose a block contains a transaction where Bob transfers some bitcoins to Carol
- Such a transaction will have:
  - an input which unlocks a UTXO owned by Bob
  - an output which creates a UTXO that can be unlocked only by Carol
- Can Alice modify this transaction to make herself the recipient of bitcoins instead of Carol?
  - No, since the response script Bob uses to unlock his UTXO requires a digital signature which can only be generated using Bob's private key
  - The output of the transaction which specifies Carol as the recipient is part of the message that is used to generate the signature
  - If Alice replaces this output with an output which specifies herself as the recipient, the message used to generate the signature changes and Bob's private key is needed to generate the new signature

The 51% Attacker

- An attacker who controls more than 50% of the network hash rate called a "51% attacker" in the Bitcoin literature
- A 51% attacker can, with probability 1:
  - launch double spending attacks
  - and delete transactions from old blocks

  irrespective of the number of confirmations received
- A 51% attacker can also launch other, more serious, attacks
- Suppose a 51% attacker performs mining like a regular mining node, except that he/ she does not switch to longer branches which are announced by the rest of the network
  - since the branch mined by the attacker will eventually become the longest branch of the blockchain, all new bitcoins generated as part of the block subsidy will be owned by him/ her
  - this will make mining financially unviable for the other miners in the network and they may stop mining
  - attacker will then become the only miner in the network
  - Bitcoin system will then resemble a centralized system controlled by the 51% attacker

The 51% Attacker (contd.)

- Recall: under above attack, Bitcoin system will resemble a centralized system controlled by the 51% attacker
- Then, the attacker can harm the Bitcoin system as follows:
  - Can unilaterally decide which transactions get recorded on the blockchain
    - E.g., the attacker can censor transactions which transfer bitcoins to a merchant by not including such transactions in new blocks
  - Can decide the minimum fee rate for transactions by not including those transactions which pay less than this minimum rate into new blocks
  - Can cause Bitcoin system to stop functioning as a payment system by mining only empty blocks
    - "empty blocks" are blocks which contain only the coinbase transaction and no regular transactions
    - without any new regular transactions appearing on the blockchain, the Bitcoin currency would be worthless

The 51% Attacker (contd.)

- Recall: presence of a 51% attacker can lead to collapse of Bitcoin system
- However, such an event is unlikely since:
  - the costs (e.g., acquiring mining equipment, electricity, cooling) involved in generating a majority of network hash rate are prohibitive
  - the 51% attacker cannot hope to recover these costs by selling bitcoins since the attack itself will drive the price of bitcoins to zero