NPTEL ONLINE CERTIFICATION COURSES

Blockchain and its applications

Prof. Shamik Sural

Department of Computer Science & Engineering

Indian Institute of Technology Kharagpur

Lecture 08: Blockchain Elements - I

CONCEPTS COVERED

- What is a Blockchain
- Blocks in a Blockchain
- Block Header

KEYWORDS

- Block Structure
- Block Header
- Mining a Block
- Block Generation Puzzle

What is Blockchain?

- A Platform for executing transactional services
- Spanned over multiple organizations or individuals who may not (need not) **trust** each other
- An append-only shared ledger of digitally signed and encrypted transactions replicated across a network of peer nodes

The Block in a Blockchain – Securing Data Cryptographically

- Digitally signed and encrypted transactions “**verified” by peers**

- **Cryptographic security** – Ensures that participants can only view information on the ledger that they are authorized to see

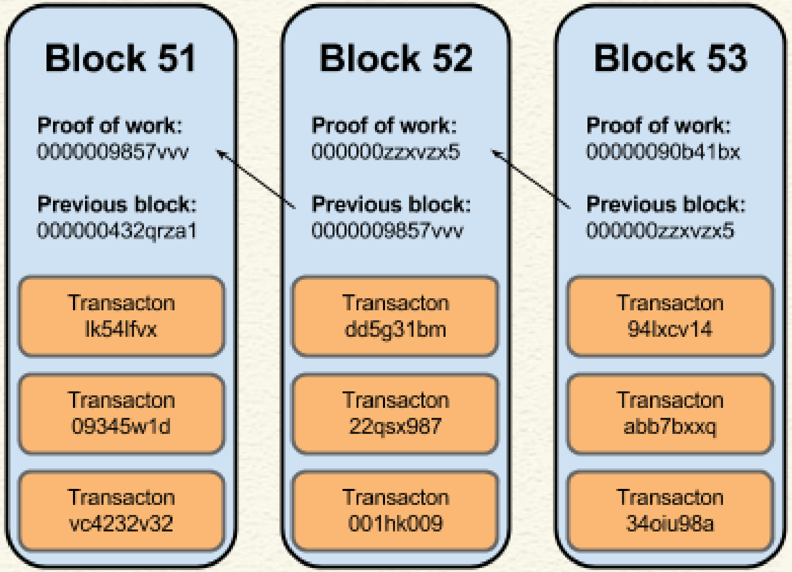


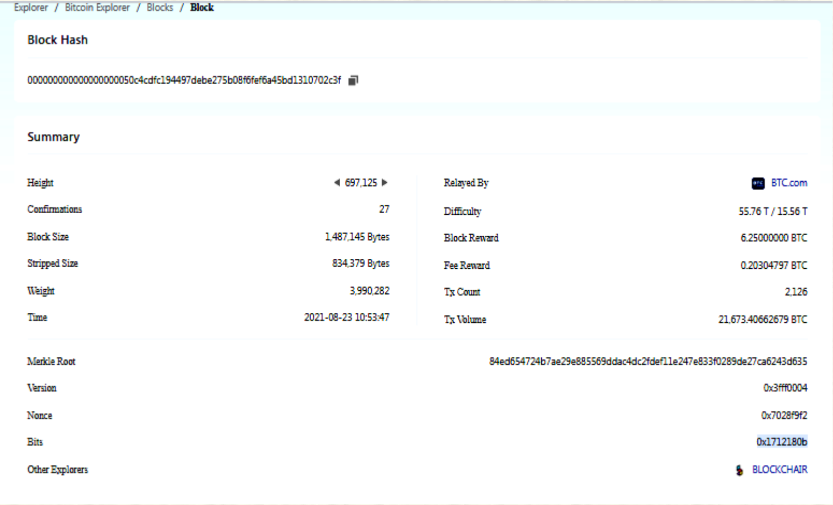
Image source: http://dataconomy.com/

Structure of a Block

- A block is a **container data structure** that contains a series of transactions
- **In Bitcoin:** A block may contain more than 500 transactions on average, the average size of a block is around 1 MB (an upper bound proposed by Satoshi Nakamoto in 2010)
  - May grow up to 8 MB or sometime higher (several conflicting views on this!!)
  - Larger blocks can help in processing large number of transactions in one go.
  - But longer time for verification and propagation

Structure of a Block (Reference: Bitcoin)

- Two components:
  - **Block Header**
  - **List of Transactions**



Explorer / Bitcoin Explorer / Blocks / **Block**

Block Hash

0000000000000000000050c4cdfc194497debe275b08f6fef6a45bd1310702c3f

Summary

Height	◀ 697,125 ▶	Relayed By	BTC.com
Confirmations	27	Difficulty	55.76 T / 15.56 T
Block Size	1,487,145 Bytes	Block Reward	6.25000000 BTC
Stripped Size	834,379 Bytes	Fee Reward	0.20304797 BTC
Weight	3,990,282	Tx Count	2,126
Time	2021-08-23 10:53:47	Tx Volume	21,673.40662679 BTC

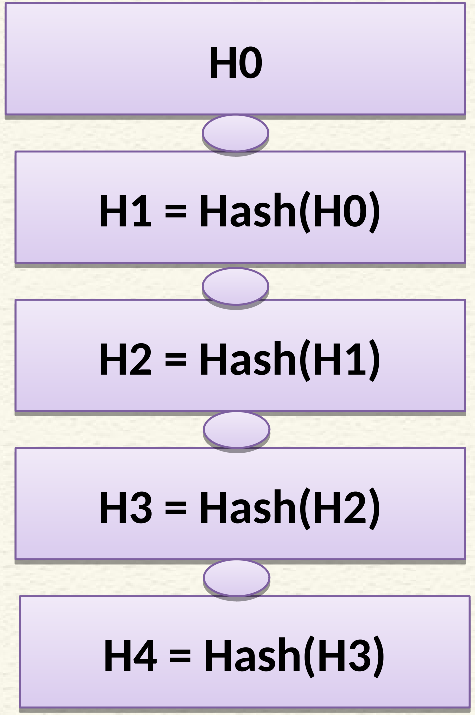
Merkle Root	84ed654724b7ae29e885569ddac4dc2fdef11e247e833f0289de27ca6243d635
Version	0x3fff0004
Nonce	0x7028f9f2
Bits	0x1712180b
Other Explorers	BLOCKCHAIR

Block Source: https://btc.com/btc/blocks OR https://blockchain.com/explorer

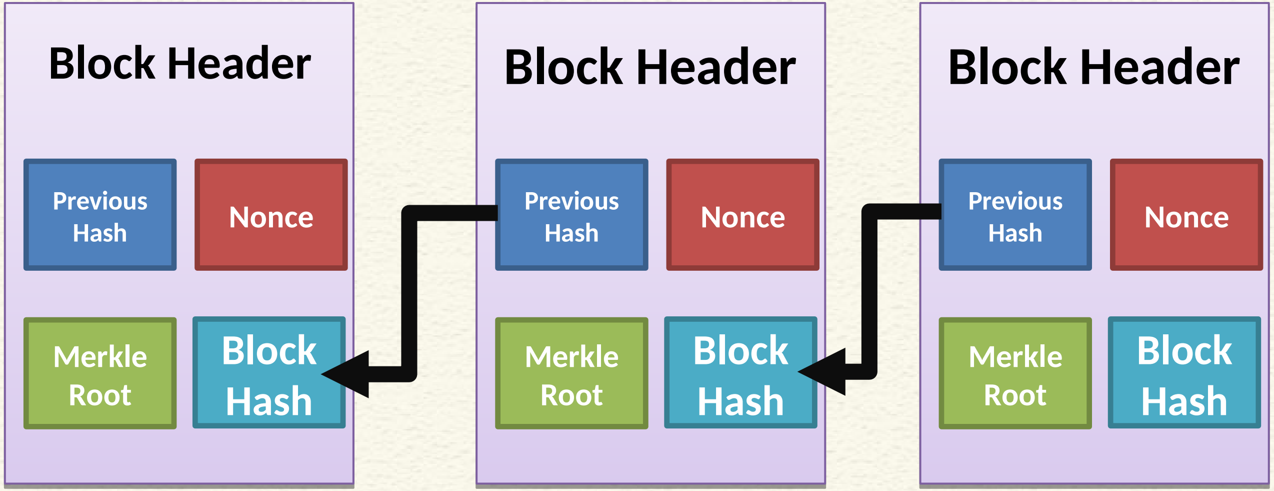
Block Header (Reference: Bitcoin)

- Metadata about a block – (1) Previous block hash, (2) Mining statistics used to construct the block, (3) Merkle tree root

- **Previous block hash:** Every block inherits from the previous block – we use previous block's hash to create the new block's hash – make the blockchain **tamper proof**



Block Generation Puzzle



Find out the nonce which generates the desired hash (certain number of zero bits at the prefix) - 00000000000000004a2b84f93a285b7a7………

Block Header (Reference: Bitcoin)

- **Mining** – the mechanism to generate the hash
  - The mechanism needs to be complicated enough, to make the blockchain **tamper proof**
  - **Bitcoin Mining:** $H_k = Hash(H_{k-1} \,||\, T \,||\, Nonce \,||\, Something\ more)$
  - Find the nonce such that H_k has certain predefined **complexity** (number of zeros at the prefix)
- The header contains mining statistics – timestamp, nonce and difficulty

Block Header (Reference: Bitcoin)

- Understanding Difficulty and Bits
- “Bits” written in Hex, e.g., 0x170e2632
  - First byte is index and next three bytes form coefficient
  - Target = Coefficient*2^(8*(index-3))
- Difficulty is the largest possible target (0x00000000FFFF0000000000000000000000000000000000000000000000000000) divided by the current target , e.g.,
- (0x0000000000000000000E2631FFFFFFFFFFFFFFFFFFFFFBB0C4B021913E000000)
- Remember: “Cost of Mining” – Pretty High (Computing Power and Energy)

[Number conversion utility: https://www.rapidtables.com/convert/number/hex-to-decimal.html]

Hashes in a Block Header (Reference: Bitcoin)

- Block identifier – the hash of the current block header (Hash algorithm: Double SHA256)
- Merkle Root
- Previous block hash is used to compute the current block hash
- Timestamp, Previous hash, Merkle root, Difficulty Bits, Nonce and Version used to compute current hash

Demonstration

https://dlt-repo.net/bitcoin-block-hash-verification-tool/

Block Source: https://btc.com/btc/blocks

CONCLUSIONS

- We have described the structure of a block in blockchain
- Main components of a block header
- How to solve block generation puzzle
- What is meant by mining of a block

REFERENCES

- Cryptography and Network Security – Principles and Practice by William Stallings, Pearson (2017)
- Blockchain Basics: A Non-Technical Introduction in 25 Steps by Daniel Drescher, Apress (2017)
- Any other standard textbook on blockchain/bitcoin

Thank you