CMSC 398F
Week #2
Bitcoin and Blockchain Structure
...

Announcements

- Quiz 2 will be released soon
- Join the class Piazza!

What is Bitcoin?

Bitcoin is a cryptocurrency, a virtual currency designed to act as money and a form of payment outside the control of any one person, group, or entity, and thus removing the need for third-party involvement in financial transactions.

Basic Concepts

- First and most widely used cryptocurrency
  - Completely digital, decentralized, built on principles of Computer Science, cryptography, and economics
- Bitcoin whitepaper published in 2008 by Satoshi Nakamoto
- **B**itcoin refers to the community, the network, and the software
- **b**itcoins: the currency itself, a unit
- **Inspiration for the blockchain**: the underlying data structure that stores a permanent history of all the transactions to ever occur in the history of Bitcoin

Satoshi Nakamoto's Innovation

- Bitcoin attempts to solve two problems that decentralized networks typically face
  - Inconsistent transaction records held by different nodes
  - Malicious pseudonymous actors might broadcast false messages and divide the network
- Double spending attack: asynchronous records held by different nodes
- The **blockchain** and **consensus protocol** are the solutions to these problems

BITCOIN VS. BANKS

"IN BANKS WE DISTRUST"

	Account and Identity Management	Service	Record Management	Trust
	Links personal information to bank account and verifies ownership	Transfers money and redeems money	Updates and tracks account balance	Provides services by professionals under regulations of government

BITCOIN VS. BANKS

"IN BITCOIN WE TRUST"

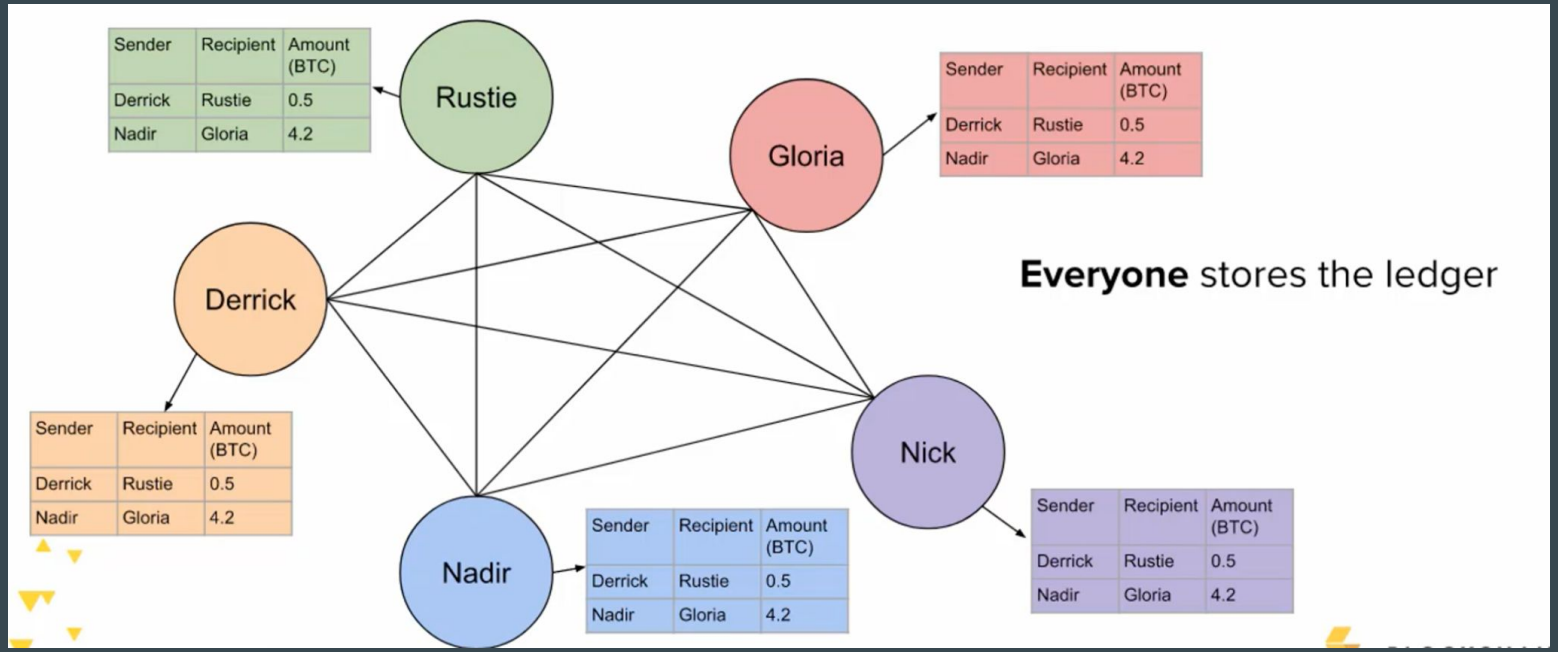
	Account and Identity Management	Service	Record Management	Trust
	Gives users autonomously created and managed identities	Sends funds between peers directly (P2P)	Updates every node, which keeps its own ledger (blockchain)	Provides trusted protocol which incentivizes actors to behave honestly

Bitcoin From the Ground Up: Identity

- What's the role of identity in the context of currencies?
  - Authentication
    - Receiving
    - Claiming/Spending
    - Blame
  - Integrity
- In daily life?
  - Houses have addresses and **door keys**
  - Emails have aliases and **passwords**
  - Bitcoin uses public and **private keys**

Bitcoin From the Ground Up: Record-Keeping

- How do we keep track of the history of transactions?
  - Databases
- How do we keep a database of the transactions when there is no central authority?
  - Distributed databases
    - Information is not stored by one entity
    - Copy is stored with every user
- How does this look?


Sender
Recipient
Amount (BTC)
Derrick
Rustie
0.5
Nadir
Gloria
4.2
Rustie
Gloria
Derrick
Nick
Nadir
Everyone stores the ledger

Record-Keeping

- Making everyone their own ledger allows for maximum independence
  - Follows the intent of Bitcoin
- But what “data structure” would this database need to hold the transaction history?
  - Feasibly can’t store every transaction individually
  - Once a change is made for one entity, it must propagate throughout the entire network

What is a Blockchain?

What is a Blockchain?

- A blockchain is a distributed and immutable ledger that is shared among the nodes of a computer network.
- The innovation with a blockchain is that it guarantees the fidelity and security of a record of data and generates trust without the need for a trusted third party.
- How?
  - Prevents fraudulent transactions
  - Solves the double-spend problem
  - People can’t create their own currency

The Properties of Distributed Ledger Technology (DLT)

Programmable
A blockchain is programmable (i.e. Smart Contracts)

Secure
All records are individually encrypted

Anonymous
The identity of participants is either anonymous or pseudonymous

Distributed
All network participants have a copy of the ledger for complete transparency

Immutable
Any validated records are irreversible and cannot be changed

Time-stamped
A transaction timestamp is recorded on a block

Unanimous
All network participants agree to the validity of each of the records

Blockchain Structure

- A batch of transactions gets grouped into what are called “blocks”.
- Every block is built-off, or chained to, a previous block.
- Components of a Block:
  - Hash of the block
  - Hash of the previous block
  - Some Data
- The first block is called the **genesis block** in any blockchain

Bytesoft®

Genesis Block

Hash: **4X8G**	Hash: **3LFK**	Hash: **85KS**
Previous hash: **0010**	Previous hash: **4X8G**	Previous hash: **3LFK**

SHA256

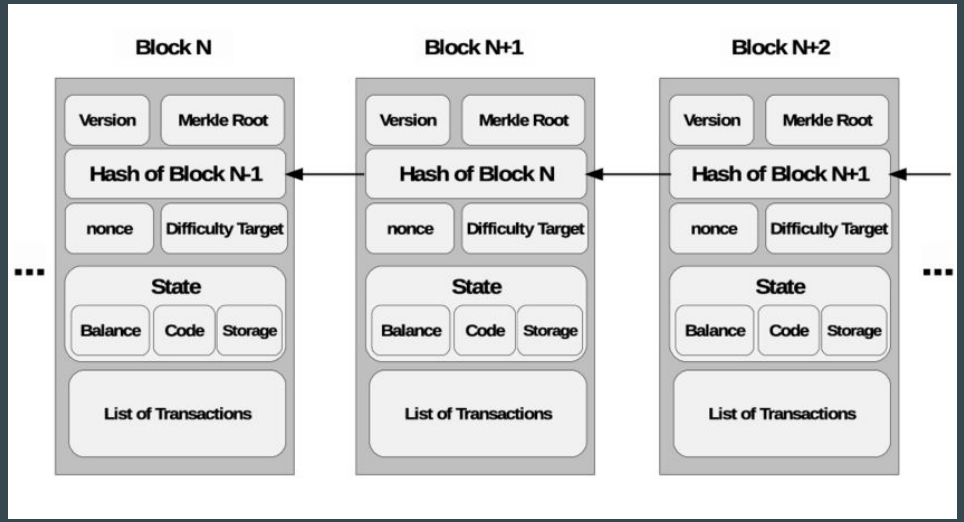
- Each block in the ledger contains a hash generated by SHA-256 referring to the preceding block in the chain
- SHA-256 is a patented cryptographic hash function that outputs a value that is 256 bits long
- Properties of SHA-256
  - Collision resistant - No two input values can produce the same hash output
  - Pre-image - The input can not be recreated given a hash value
    - Given a hash value: h, impossible to find input x such that hash(x) = h
  - Avalanche Effect - If there is a small change in the input, the output changes dramatically

SHA256

- Bitcoin uses double SHA-256, meaning that it applies the hash functions twice.
- Security - It’s nearly impossible to break SHA-256, which keeps transactions safe and secure on the network.
- Difficulty - takes a lot of computing power to find the right hash for a block, since similar inputs give vastly different hashes due to Avalanche effect
- Verification - anyone can verify the validity of a block by simply re-computing the hash of that block

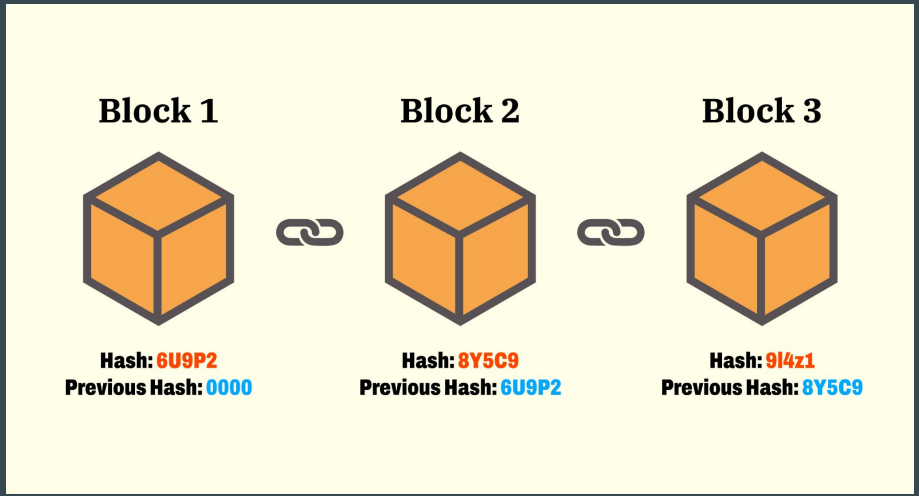
Blockchain Structure Overview: Components of a Block

- Block Header:
  - Previous Block Hash
  - Root hash of Merkle tree
  - Nonce
  - Other Metadata: Timestamp, the goal of the current difficulty
- Block Body
  - List of Transactions



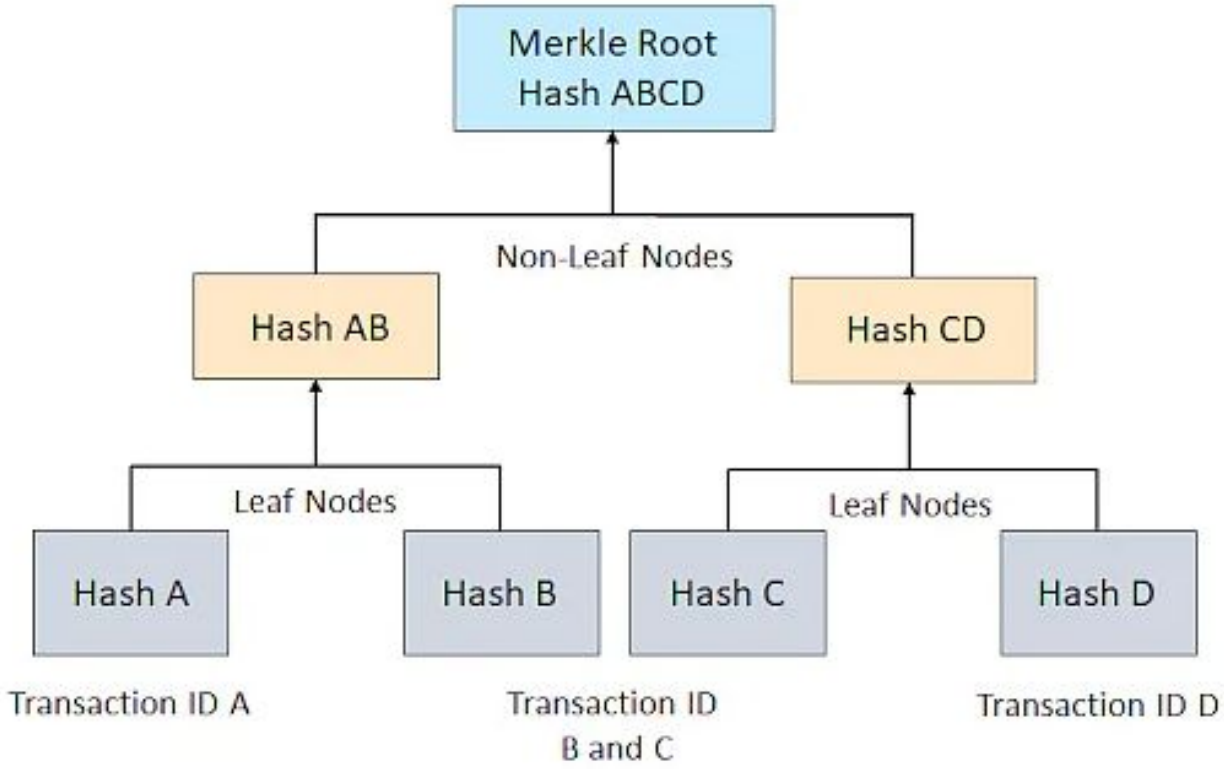
Components of a Block: Previous Block Hash

- The block header contains the hash to the previous block
  - This is the “chain” in blockchain
- Without this component, there would be no connection and chronology between each block.



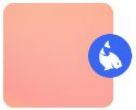
Components of a Block: List of Transactions

- Transactions are stored in the block with a so-called Merkle Tree
  - hash-based binary tree of transactions
- To develop this, transaction data is initially hashed. This hash then gets repeatedly hashed with other transactions hashes until a singular hash value remains
  - This value is called the “root hash”
- The root hash represents the information of all its “leaves” (individual transactions) and “branches” (hashes of the leaves)


Merkle Root
Hash ABCD
Non-Leaf Nodes
Hash AB
Hash CD
Leaf Nodes
Leaf Nodes
Hash A
Hash B
Hash C
Hash D
Transaction ID A
Transaction ID
B and C
Transaction ID D

Components of a Block: Nonce

- 32-bit integer that is included in the block
- The nonce will hash together with the previous block hash and merkle root hash to create the hash for the entire block
- A block hash is valid if it is less than a certain target, which usually means starting with a certain number of 0-bits (i.e., the hash must look like 0x0000000023FB23..., not 0x12FD23A123...)
  - Small exceptions to this
- If the block has the correct hash, we call that nonce the “winning” nonce



Bitcoin Block #754,276

Mined on 9/15/2022, 19:46:57 View all Blocks

This block was mined on 9/15/2022, 19:46:57 by F2Pool. A total of 15,427.88 BTC ($304,029,592) were sent in the block with the average transaction being 5.4631 BTC ($107,658). F2Pool earned a total reward of 6.25 BTC $123,165. The reward consisted of a base reward of 6.25 BTC $123,165 with an additional 0.1518 BTC ($2,991.45) reward paid as fees of the 2,824 transactions which were included in the block.

Details

Hash	00000-f459b	Size	1,504,453
Depth	1	Version	0×32540004
Capacity	143.48%	Merkle Root	cb-31
Distance	37m 0s	Difficulty	32,045,359,565,303.15
BTC	15,427.8760	Nonce	3,299,940,922
Value	$304,029,592	Bits	386,451,604
Value Today	$302,620,255	Weight	3,998,203 WU
Average Value	5.4631288839 BTC	Median Time	Sep 15, 2022, 7:35:29 PM
Median Value	0.02475929 BTC	Minted	6.25 BTC
Input Value	15,428.03 BTC	Reward	6.40178696 BTC
Output Value	15,434.28 BTC	Mined on	Sep 15, 2022, 7:46:57 PM
Transactions	2,824	Height	754,276
Witness Tx's	2,349	Confirmations	1
Inputs	6,561	Miner	F2Pool
Outputs	10,962	Coinbase	,z>mm R 8-;@mrA oS b@ga 2 5k {e% 6 p /F2Pool/s F c
Fees	0.15178696 BTC		
Fees Kb	0.0001009 BTC		
Fees kWU	0.0000380 BTC		
Fee Range	1-422 sat/vByte		
Average Fee	0.00005375		
Median Fee	0.00002535		

Transactions

Last | First | ↗ Value | ↘ Value | ↗ Fee | ↘ Fee

TX 0 • Hash 80ff-7ab3 9/15/2022, 19:46:57	6.40178696 BTC $126,156 Fee 0 Sats $0.00
TX 1 • Hash cdb3-7d57 9/15/2022, 19:28:16	0.06386663 BTC $1,258.59 Fee 94.5K Sats $18.63
TX 2 • Hash 4357-c1a6 9/15/2022, 19:37:22	0.57668996 BTC $11,364.55 Fee 90.0K Sats $17.74
TX 3 • Hash 8b73-1fb2 9/15/2022, 19:43:03	0.41246284 BTC $8,128.20 Fee 70.0K Sats $13.79
TX 4 • Hash 3862-c5a8 9/15/2022, 19:42:31	7.76752636 BTC $153,070 Fee 204.6K Sats $40.32
TX 5 • Hash bccf-90c7 9/15/2022, 19:30:39	0.42307228 BTC $8,337.28 Fee 36.7K Sats $7.22
TX 6 • Hash f95f-dec5 9/15/2022, 19:36:36	0.26019150 BTC $5,127.47 Fee 50.0K Sats $9.85
TX 7 • Hash be63-2eb6 9/15/2022, 19:45:39	0.25230550 BTC $4,972.06 Fee 50.0K Sats $9.85
TX 8 • Hash 17f0-7be9 9/15/2022, 19:35:35	0.63245205 BTC $12,463.42 Fee 24.4K Sats $4.81
TX 9 • Hash ae6c-b3d7 9/15/2022, 19:34:36	0.02152068 BTC $424.10 Fee 40.0K Sats $7.88
TX 10 • Hash 0496-b9c0 9/15/2022, 19:46:44	3.99880000 BTC $78,802.39 Fee 63.8K Sats $12.56

Summary

- Cryptocurrency is a digital payment system that doesn't rely on banks or an authority to verify transactions
- Identical copies of the blockchain are hosted on computers around the world that run the Bitcoin software. These computers are known as nodes.
- Satoshi Nakamoto wrote the white paper on Bitcoin in 2009.
- Covered a general overview of Bitcoin along with its inspiration and blockchain structure
  - SHA-256
  - Nonce
  - Merkle roots
-