CMSC 398F
Week #2
Bitcoin and Blockchain Structure

•••

Announcements

- Quiz 1 was due this morning
- Quiz 2 will be released soon
- Project #1 will be released next week
- Join the class Piazza!
  - piazza.com/umd/fall2022/cmsc398f

What is Bitcoin?

"

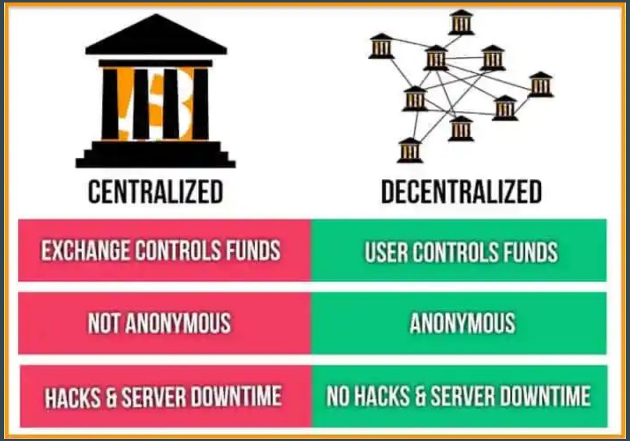
Bitcoin is a cryptocurrency, a virtual currency designed to act as money and a form of payment outside the control of any one person, group, or entity, and thus removing the need for third-party involvement in financial transactions.

Basic Concepts

- First and most widely used cryptocurrency
  - Completely digital, decentralized, built on principles of Computer Science, cryptography, and economics
- **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

Cypherphunk Movement

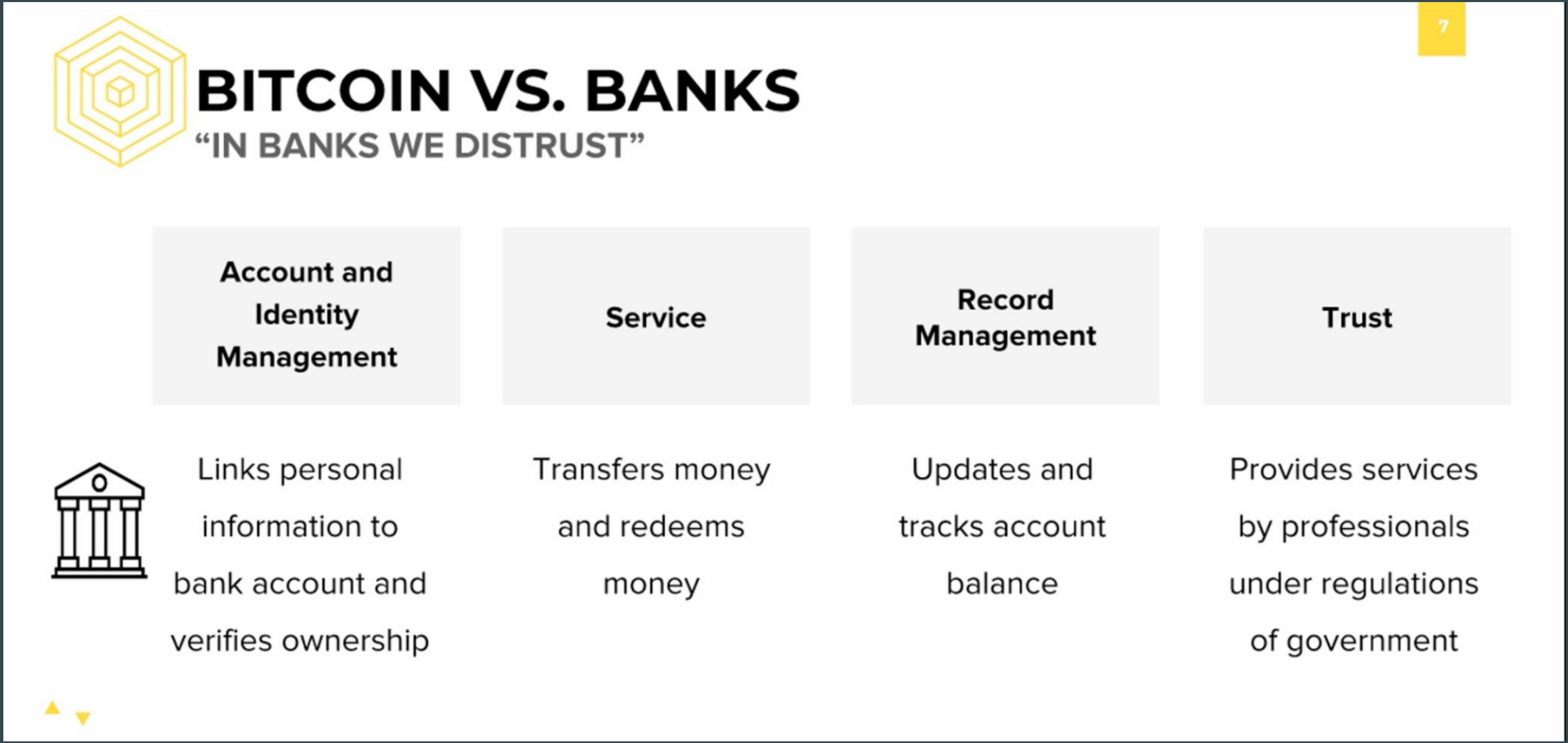
- Cypherphunks: a group of individuals who advocate for protection of privacy using cryptography
- Bitcoin was created by Satoshi Nakamoto in 2009
- He created the first ever decentralized, pseudonymous, and trustless system for transactions



CENTRALIZED	DECENTRALIZED
EXCHANGE CONTROLS FUNDS	USER CONTROLS FUNDS
NOT ANONYMOUS	ANONYMOUS
HACKS & SERVER DOWNTIME	NO HACKS & SERVER DOWNTIME

Satoshi Nakamoto’s Innovation

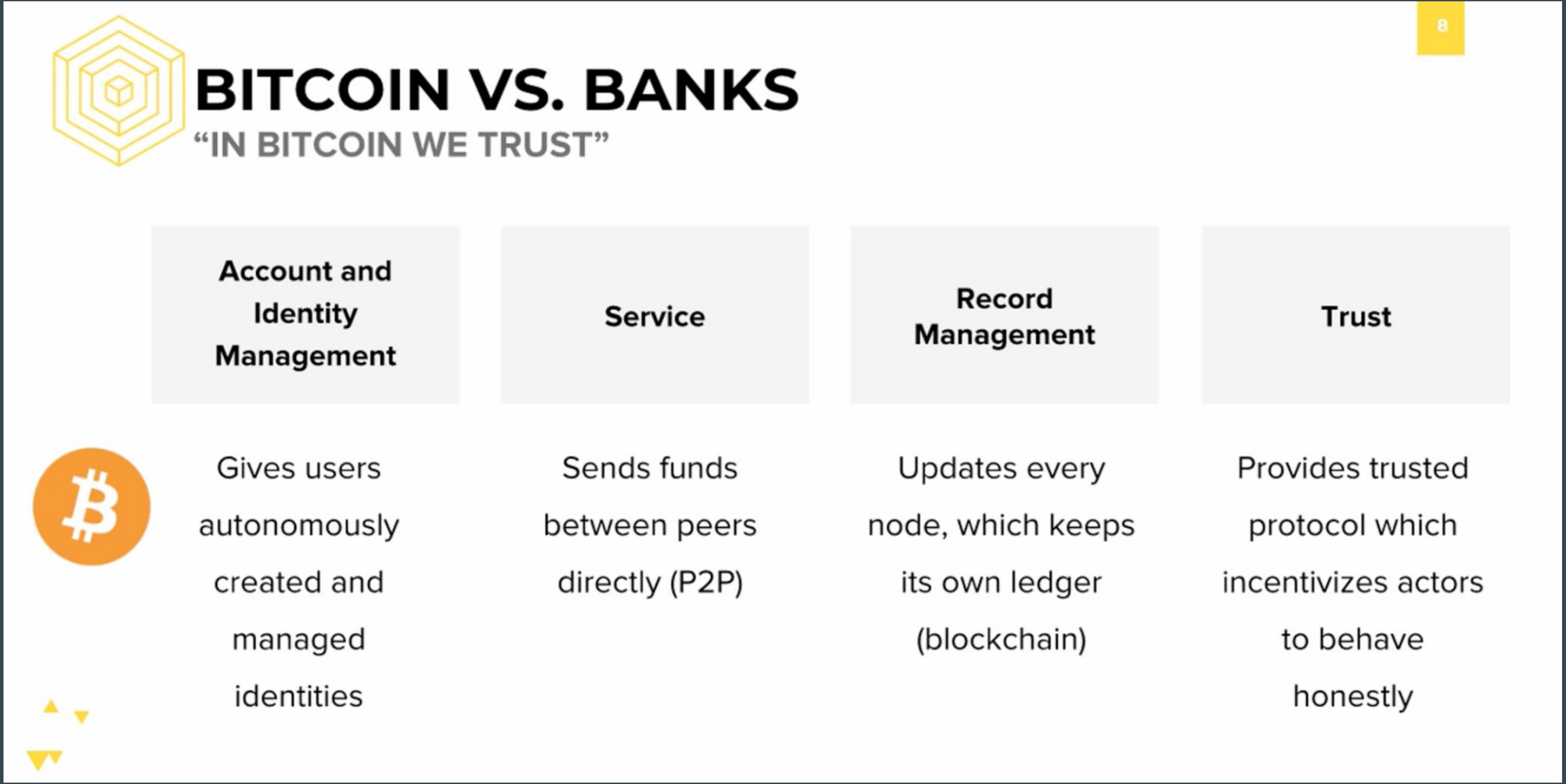
- Bitcoin attempts to solve two problems that decentralized networks typically face
    - Inconsistent transaction records held by different nodes
    - Malicious pseudonymous actors might broadcast false messages and divide the network
- Double spending attack: asynchronous records held by different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

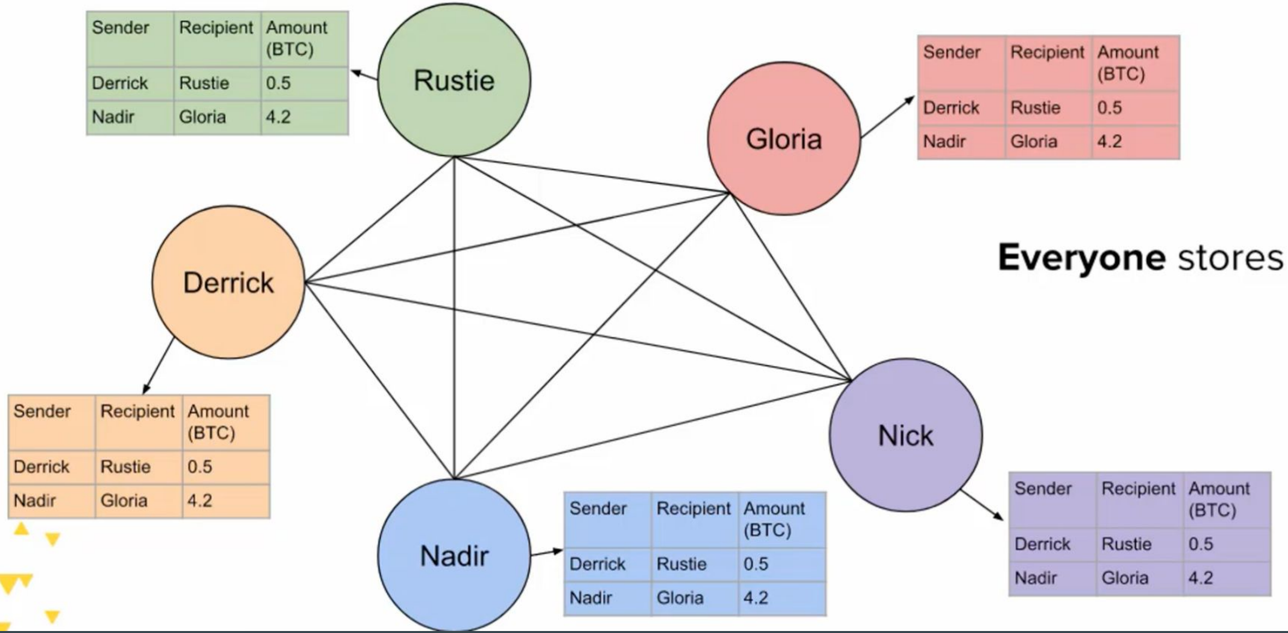
Bitcoin From the Ground Up: Identity

- 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?

Everyone stores the ledger



Sender	Recipient	Amount (BTC)
Derrick	Rustie	0.5
Nadir	Gloria	4.2

Sender	Recipient	Amount (BTC)
Derrick	Rustie	0.5
Nadir	Gloria	4.2

Sender	Recipient	Amount (BTC)
Derrick	Rustie	0.5
Nadir	Gloria	4.2

Sender	Recipient	Amount (BTC)
Derrick	Rustie	0.5
Nadir	Gloria	4.2

Sender	Recipient	Amount (BTC)
Derrick	Rustie	0.5
Nadir	Gloria	4.2

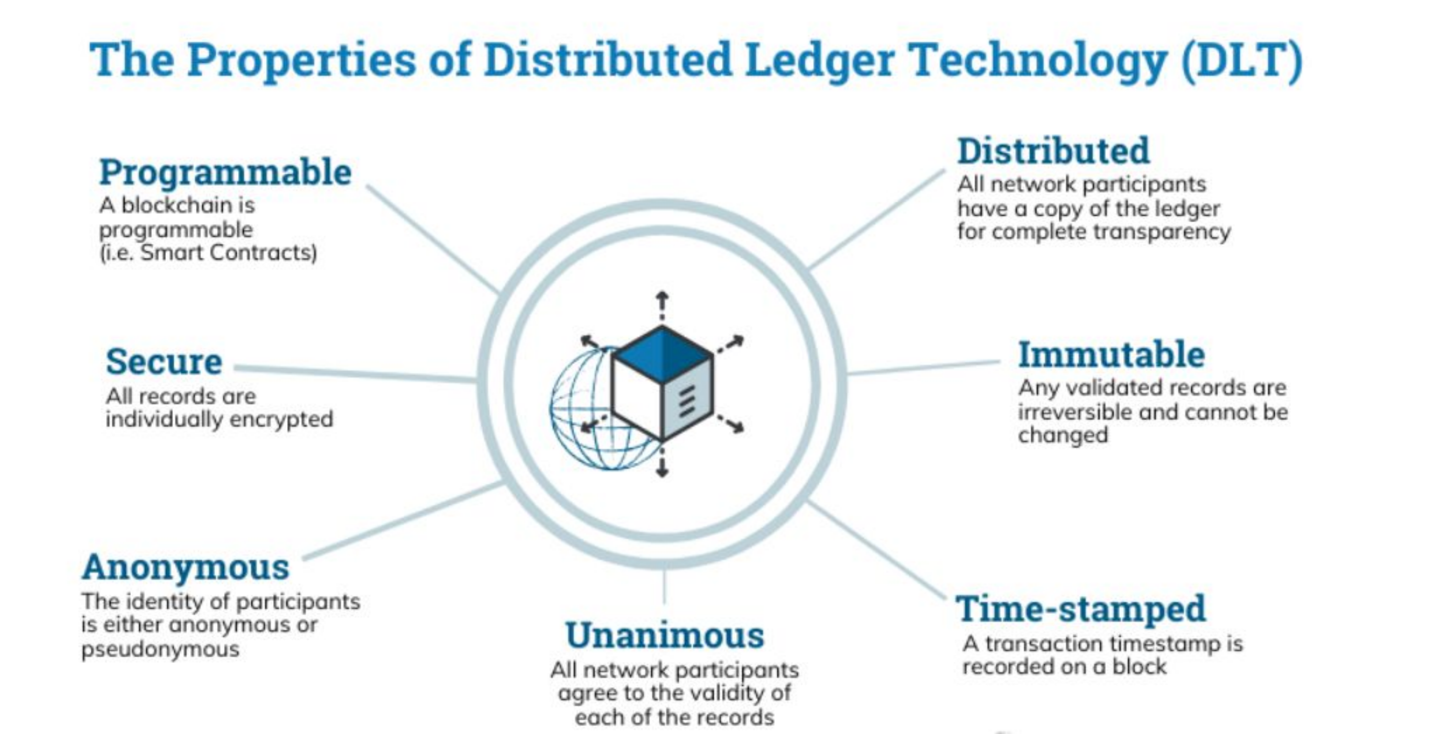
Record-Keeping

- 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)

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

Secure
All records are individually encrypted

Immutable
Any validated records are irreversible and cannot be changed

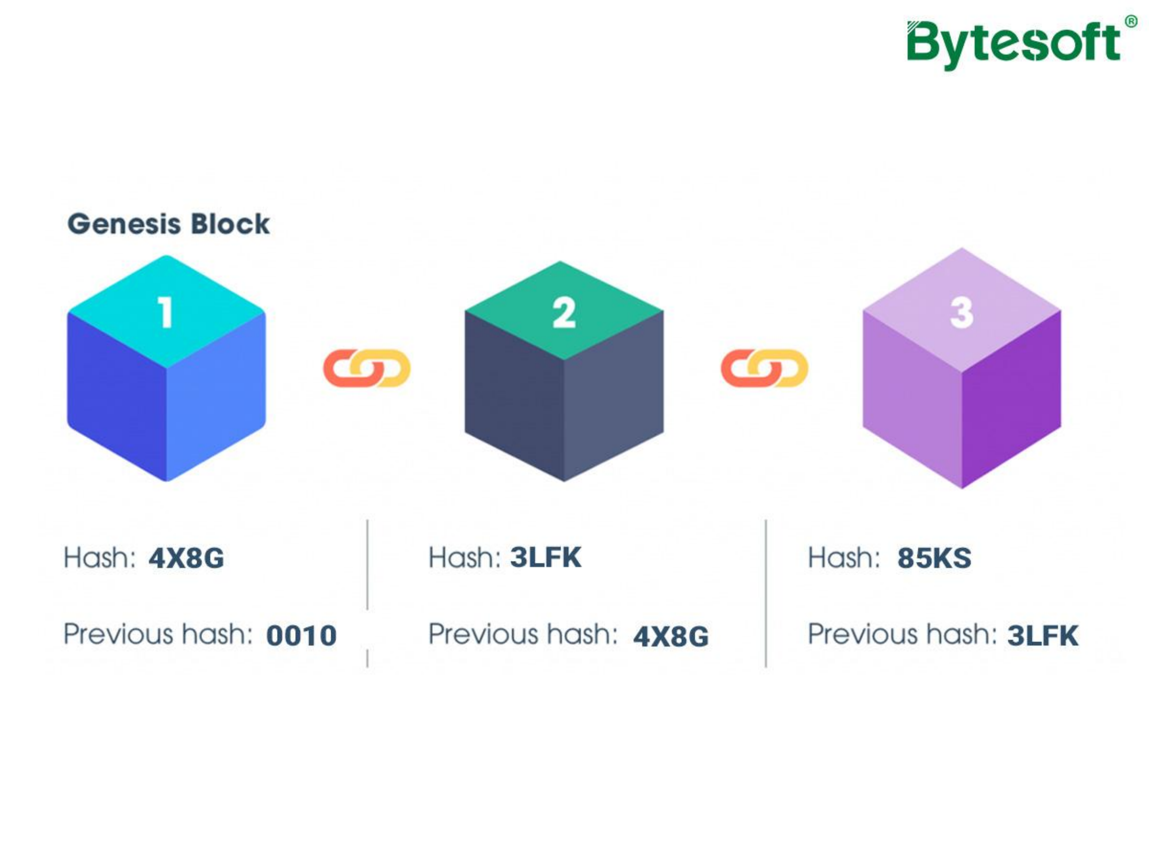
Anonymous
The identity of participants is either anonymous or pseudonymous

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

Time-stamped
A transaction timestamp is recorded on a block

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



Hash: **4X8G**

Previous hash: **0010**

Hash: **3LFK**

Previous hash: **4X8G**

Hash: **85KS**

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 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
- Verification - anyone can verify the validity of a block by simply re-computing the hash of that block

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