What is a bitcoin?

What is Bitcoin?

- A type of digital currency
- Can be transferred from one person to another in an instant

What is a bitcoin?

- A unit of currency
  - Like dollars, pounds..
- Every bitcoin is a sequence of 1s and 0s
  - This sequence of 1s and 0s is known as a bit string

How does Bitcoin prevent fraud?

- Can’t I just make up a bit string and call it a bitcoin?
  - A record of every exchange of bitcoins is sent to everyone that uses Bitcoin
    - This exchange is called a transaction
  - Transactions are stored in a ledger
  - When you try to pay Bob these “bitcoins” you made up, he will check the ledger
    - Since there no record of how you got the bitcoins, he will refuse to accept them

How does Bitcoin prevent fraud?

- If I receive a copy of every transaction, can't I spent other people's bitcoins?
  - Every user of Bitcoin has a public key
    - A series of alphanumeric characters
    - Like a credit card number, but not tied to your identity
  - Each public key has a private key associated with it
    - Like a password

How does Bitcoin prevent fraud?

- When Alice spends a bitcoin, she has to prove that she knows the private key associated with the public key
  - This private key is secret, and never displayed in the transaction
- If you want to spend Alice’s bitcoin, you need to know her private key
  - Similar to how you can’t use someone’s username without knowing their password

Advantages of Bitcoin

- Unlike credit cards, bitcoins are not tied to your identity
  - Just like regular cash!
  - Good choice if you want to remain anonymous online
- The value of bitcoins is the same everywhere in the world
  - “Global currency”
- They are much harder to steal
- The government cannot seize your bitcoins

How do I get bitcoins?

- You can exchange cash for bitcoins
  - Just like exchanging dollars for pounds
- You can accept bitcoins as payment
  - Like accepting dollars as payment
- You can “mine” bitcoins
  - This creates new bitcoins

How are new bitcoins created?

- There are a finite number of bitcoins
- They are uncovered by miners
  - Similar to how there is a finite amount of gold ore, which is then mined
- Miners select some transactions, verify them, and group them into a block
- This block is then added to the ledger once it is approved by a majority

How are new bitcoins created?

- When a block is added to the ledger, new bitcoins are created
  - Miners get to keep these bitcoins
- The process of verifying transactions involves solving a hard cryptographic problem
  - Cannot be solved by a person
  - Requires a ton of computing power and electricity
- This prevents all the bitcoins from being mined at once

Disadvantages of Bitcoin

- Bitcoins are not widely accepted
  - This may change in the future!
  - Or governments may pressure merchants to not use bitcoins
- They can be lost
  - To use a bitcoin, you need to have the public and private keys associated with it
  - If you lose the keys, you lose it forever
- The value of a bitcoin is volatile

Conclusion

- Bitcoins are a digital, global currency
- They protect your privacy
- There are mechanisms in place to guard against fraud
- They are volatile, not widely accepted, and can be lost