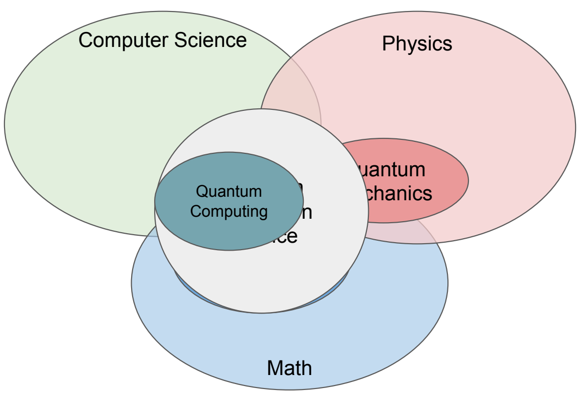
CMSC 22880 - Introduction to Quantum Computing

Diana Franklin

Teaching Staff

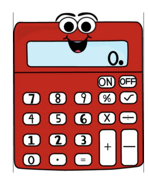
Instructors:
    Prof. Diana Franklin, dmfranklin@uchicago.edu
TAs:
    David Maldonado, dagm@uchicago.edu
    Sarang Joshi, sarongj@uchicago.edu

What is Quantum Computing?



CLASSICAL COMPUTERS

How it started

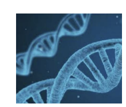


How it's going

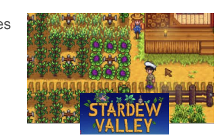
AI-generated images

Self-driving cars

Search engines



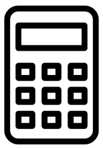
Genetic Analysis

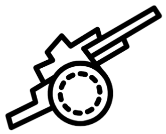


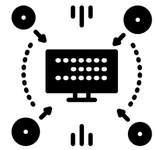
Video games

Smartphones

Development of Classical Computers







Designed for mathematical calculations

Ada Lovelace envisioned uses like composing music

Grace Hopper made them easier to program

Computers can do our calculations faster! → **Increase computer speed!** → **Increase storage space!** → **Google**

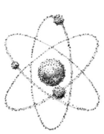
60 years of improvements

Limits on Classical Computation

- Classical computers solve many day-to-day problems efficiently, or at least faster than a human
- Many complex calculations, however, are still intractable with classical machines and software
  - ***Intractable problems require infinite resources/time to solve!***
- Example problems that are difficult for classical computers include:
  - Modeling natural processes
  - Selecting the 'correct' solution from an exponentially large set of potential solutions

QUANTUM

How it started



The behavior of **thousands of atoms** that we observe with our eyes does not capture what happens in **individual atoms**

How it's going

CHICKENS

Chicken Flock

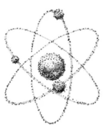
Will run to food

Chicken Pet

Brown one:
leader - led a garden escape one day
Loved the seeds from the clover weed
Never played with the chicken toys

Quantum

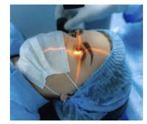
How it started



The behavior of **thousands of atoms** that we observe with our eyes does not capture what happens in **individual atoms**

How it's going

GPS



Lasers

Small computers

MRI machines

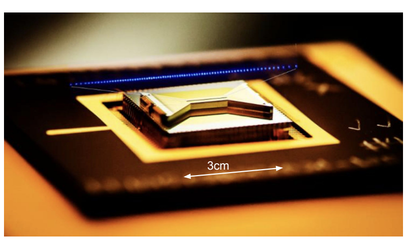
Quantum Computers

Wow! What an *interesting* *phenomenon*! → Look at all the *cool* *stuff* we can make! → Could we *compute* with it? → What can we compute *faster* than classical computing?

Quantum Computing: a hammer… looking for a nail!

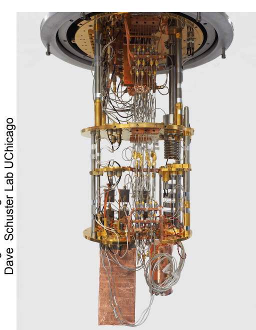
Competing quantum hardware technologies

Emily Edwards and Kai Hudek
Ken Brown STAQ Lab Duke



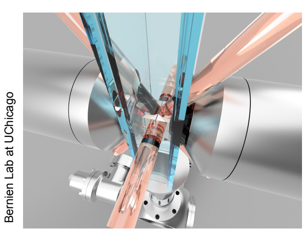
Trapped ion
(inset magnified view of ions 5×10^{-6} m spacing)

Yongshan Ding
Dave Schuster Lab UChicago



Superconducting

Bernien Lab at UChicago

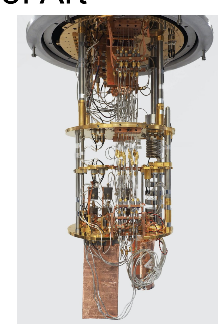


Neutral Atoms

Classical vs. Quantum Devices: State of Art

Carlos Jones/ORNL

Summit Supercomputer
~250×10^{15} Bytes of storage
(1 Byte = 8 bits)

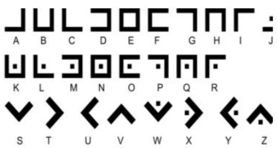


Schuster Quantum Computer (Stanford)
~10s of qubits of storage

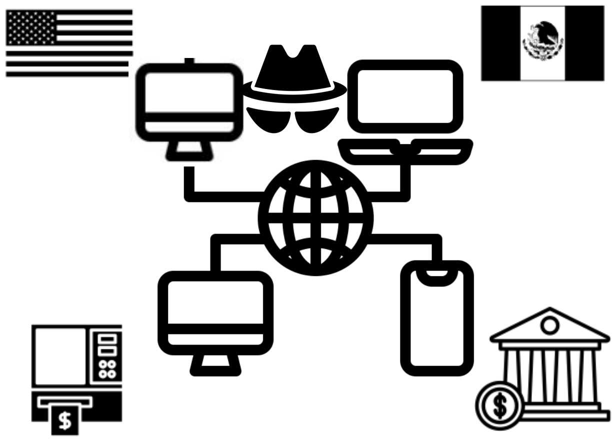
Commercial machines reaching < 1000 qubits

Poor connectivity, reliability

What problems may it solve?



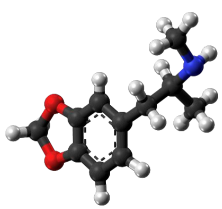
Cryptography



What problems may it solve?

Optimal routing

What problems may it solve?



Molecular simulation

Drug Design

Fertilizer Production

Chemistry Simulation

- Simulation of molecules
  - Understand metabolic processes
  - Develop of improved chemicals and materials
  - Develop better fertilizer
- Classical simulation techniques use ‘guess and check’ strategy
  - Theorists develop a hypothesis
  - Experiments are outlined and performed
  - Results are analyzed and new theories are developed
- The efficient simulation of atoms and simple molecules is a near-term quantum computing application

Moving Forward with Quantum Machines

- Many technical challenges to scaling the number of qubits
  - Short lifetime and error prone
  - Devices are sensitive to environment and each other
  - Limitations due to complex hardware and software
- Improved control and hardware will allow for more sophisticated systems and algorithms

Takeaways

- The impact of quantum computing could be widespread, revolutionizing computation for some types of problems
- Quantum will not replace classical computers, only supplement them
- In this course, you will learn more about why quantum information is different from classical information, and how it could change the world!

The FUN Approach

Gain intuition by connecting concept to daily life through cartoons, games

Show how it applies to quantum computing

This course is not for you if:
You have taken MENG 26400
You prefer a theoretical / mathematical approach

Course Goals and Outline

Introduce you to quantum computing key principles

Methods:

1) Intuition - explain the unique features of quantum computing through relatable activities
2) Math - provide the mathematical background so that you can calculate the results of quantum operations
3) Programming - Program quantum operations and quantum computer

Why broad audiences? All populations need to be on the design team - those left out suffer

Why the fun approach? Quantum Computing has a smugness problem that drives less confident people away

Airbags killed short people

Siri / Alexa didn't understand people with accents

Facial recognition misidentifies dark-skinned people

Machine learning perpetuates historical discrimination

Norms

Quantum Computing is a relatively new, different field, so confusion is normal.

This classroom should be a safe learning place

Respect. Be respectful.

Kind. Always be kind and helpful.

No smugness / intimidation. Don't show off your knowledge, just help

Course Organization

Lectures:

- Live lectures (best)
- Out of date pre-recorded videos
  - If you are sick and need to miss class. Better than nothing.

Homework on Gradescope:

- Short-answer or multiple-choice questions
- Programming labs - required for everyone

Final Project: Choose your own adventure

- Educational activity for novices / broad audience
  - Program a game that uses a quantum computer
  - Program a game that is inspired by quantum principles
  - Create a zine, infographic, etc., that does not already exist
  - Create a hands-on activity that does not already exist
  - Create something else pre-approved by me
- Deep dive into a topic we did not cover
  - 10-minute slide deck, speaker notes, video
  - Must assume same knowledge as what we covered in class
  - Must go beyond and provide real, technical material for a full 10 minutes

Grading

- Weekly homework problems: 15%
- Programming assignments: 26-30%,
- Lab *attendance*: 0-4%
- Final Project: 10%
- Midterm 20%,
- Final 25%

Homeworks are due every Wednesday night

Programming assignments are due every Tuesday night

Final project is due last day of instruction (prior to finals week)

Look smart for Family and Friends

How will quantum break cryptography?

Look smart for Family and Friends

Set time to 1 minute!!!

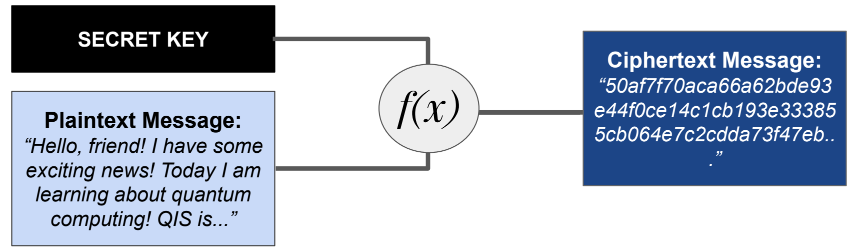
Multiply: How many in 1 min?

31x29	67x89
29x43	97x83
41x47	113x127
53x37	149x139
73x47	109x163

Factor: How many in 1 min?

143	4767
713	6889
989	9797
1763	14279
2881	18923

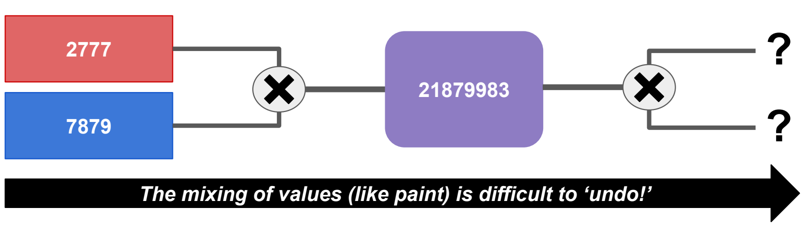
Encryption: A Bird's Eye View



Most modern encryption schemes 'scramble' the text so that the message content seems random and unusable. The 'scrambling' technique depends on a secret key and function that causes ***plaintext*** to convert to ***ciphertext***.

How is Encryption Secure?

- Encryption is based on one-way cryptographic functions
  - ***One-way function***: easy compute, difficult to invert
  - Multiplication is a one way function...factoring is hard!
- Multiplication of prime numbers used for key generation
  - Knowledge of the ***key*** or ***key factors*** allows for ***data decryption***



How Quantum Disrupts Modern Encryption

- Keys for modern encryption are large (>1000 bits), so data stays safe as long as the key and factors are secret
  - 1024 bit key → 309 decimal digits and intractable to factor for even the best classical factoring algorithms
- **Encryption only works if the inverse operation is computationally expensive!**
- ***Shor's algorithm*** is a quantum algorithm that factors numbers exponentially faster than the best classical algorithm
  - All encrypted messages, past and present, will be vulnerable

COLLAPSING -QUBITS-

Introducing **quantum vocabulary** and **concepts** through game play

COLLAPSING -QUBITS-

GOAL Be the last player with a working quantum program!

Avoid DISASTER EVENTS, which collapse your qubits!

COLLAPSING -QUBITS-

TIP! The total shield protects against ALL disasters!

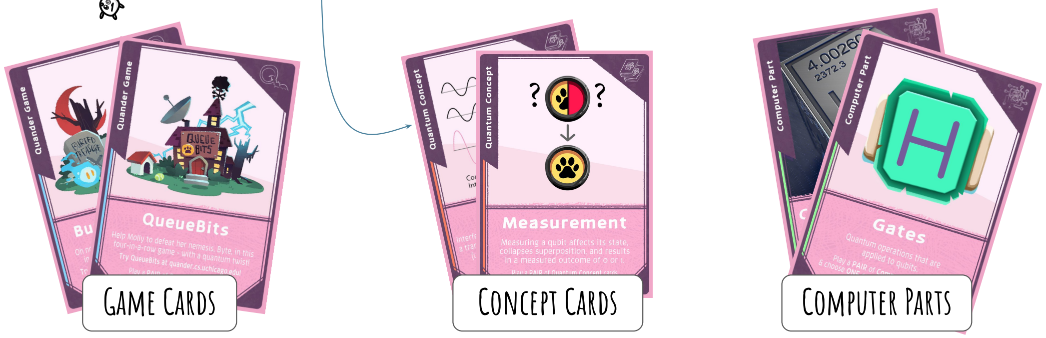
Use SHIELDS, to protect your qubits!

COLLAPSING -QUBITS-

Use QUANTUM PHENOMENA to:
Thwart other players
Improve your chances

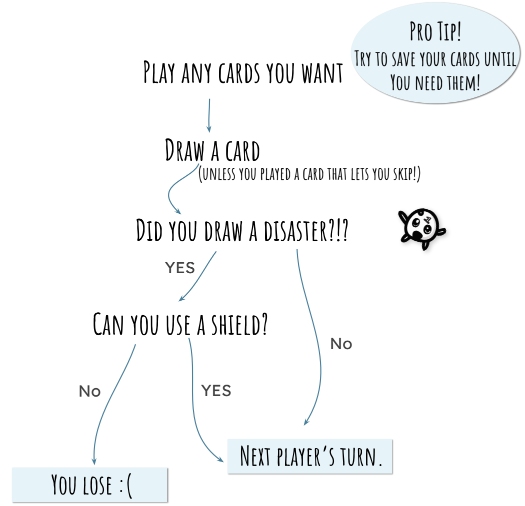
COLLAPSING -QUBITS-

RULE! Make sure to check the card type!
Only pairs of the same **type** count



Use pairs of pink cards with the same type
to steal a card from your opponents!

COLLAPSING -QUBITS-



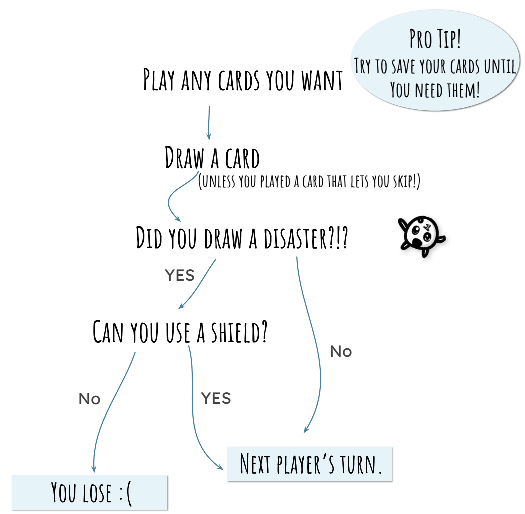
COLLAPSING -QUBITS-

GETTING READY

Before starting make sure to:

1. Remove all the **total shield** and **disaster** cards from the deck
2. Deal 5 cards to each player
3. Distribute 1 **total shield** card to each player
4. Shuffle the remaining **total shield** and **disaster** cards back into the deck

COLLAPSING -QUBITS-



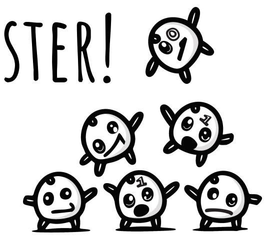
PLAY ANY CARDS YOU WANT
PRO TIP!
TRY TO SAVE YOUR CARDS UNTIL YOU NEED THEM!
DRAW A CARD
(UNLESS YOU PLAYED A CARD THAT LETS YOU SKIP!)
DID YOU DRAW A DISASTER?!?
YES
No
CAN YOU USE A SHIELD?
No
YES
YOU LOSE :(
NEXT PLAYER'S TURN.

COLLAPSING -QUBITS-

Reflection

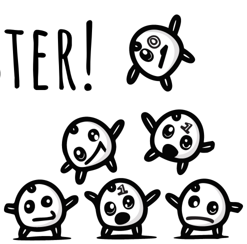
*Note: If you already know the answers from elsewhere, please do not answer quickly. The purpose is to give people time to think, suggest, etc. The goal is not to get the **right** answers.*

DISASTER!



What were some of the disasters that you remember?

DISASTER!



Can you come up with a new source for each disaster?

- Vibration
- Heat
- Magnetism
- Radiation

What do you think **superposition** is?

If we applied superposition to computers, what might it mean?

Quantum Computing Connection!

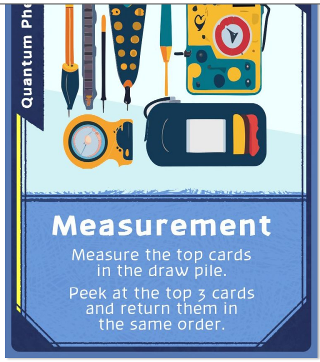
- Quantum computers use quantum bits (qubits!).
- Unlike classical bits which can only be either 0 or 1, qubits can be 0, 1 or a **superposition!**
- Superposition means qubits can be both 0 **and** 1 at the same time!

What **advantages** might superposition provide?

What is being **measured** when a player uses this card?

When might **measurement** happen in a quantum computer?

Quantum Computing Connection!



- When you **measure** a qubit it becomes either 0 or 1
- After **measuring** a qubit it is no longer in superposition
- Quantum operations can change the likelihood, or probability, of a qubit **measuring** either 0 or 1

Adjusting probabilities and increasing likelihood of the correct answer is the key to quantum algorithms

What happened when you **entangled** yourself with a different player?

How might **entanglement** apply to a quantum computer?

Quantum Computing Connection!

- If two qubits are **entangled** then *measuring* one qubit will reveal information about the other qubit as well!
- **Entanglement** is key to some of quantum computing's ability to solve problems in unique ways

If two qubits are **same entangled** what do you think will happen when you measure both of them?

Class Ended Here

Quantum Computation Basics

Quantum Concepts and the Gates they Influence

Superposition: Two things at once

Rabbit or Duck?

"There can be no peace until they renounce their Rabbit God and accept our Duck God."

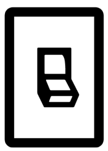
Vase or Faces?

Superposition: Holds multiple values at once

Superposition:
Holds 2 values at once

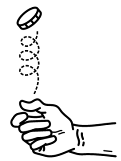
A bit: Stores either the value 0 or 1 at any given time

X = 5;



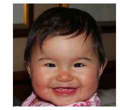
A qubit: Stores several things, including both 0 and 1

X = 5 and 8 and 12;



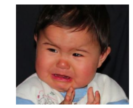
Heisenberg Uncertainty Principle: You Can't Accurately **Measure** / Read out the Complete State

Superposition:
Holds 2 values at once
Cannot read full state



Happy

Proud
Excited



Sad

Hungry
Tired
Angry
Bored
Anxious

Heisenberg Uncertainty Principle: You Can't Accurately **Measure** / Read out the Complete State

Superposition:
Holds 2 values at once
Cannot read full state

A bit: Stores either the value 0 or 1 at any given time

Int x = 5;
println("X = " + X);

```
>> java cstate
>> X = 5
>> java cstate
>> X = 5
>> java cstate
>> X = 5
```

A qubit: Stores several things, including both 0 and 1

X = 5 and 8 and 12;

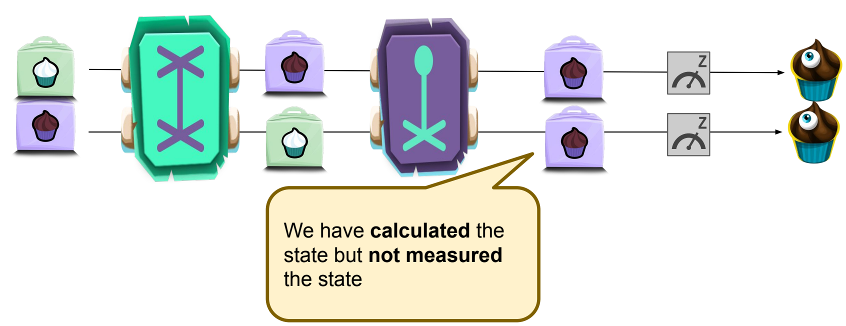
println("X = " + X);

```
>> java cstate
>> X = 5
>> java cstate
>> X = 12
>> java cstate
>> X = 5
```

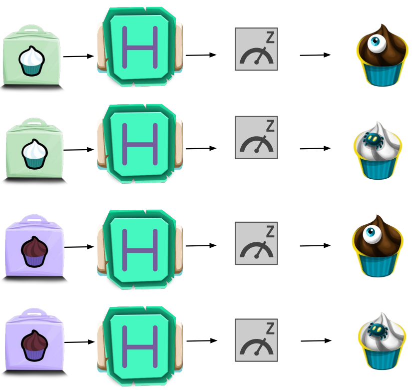
X has three values, but we only read one of them

Flu or COVID?

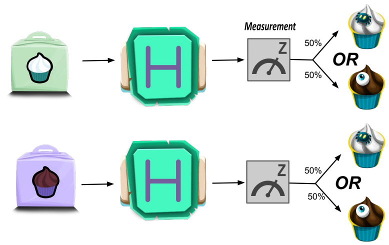
Update our model:
Measurement outcome is different from **state**



New Gate: The **H** Gate

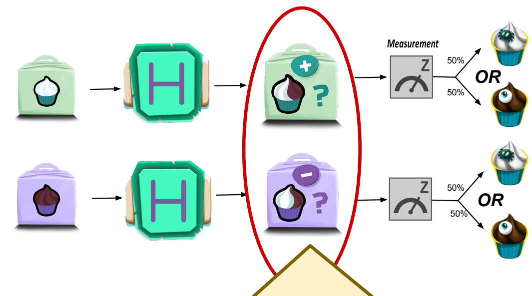


Observed outcome from single gate is random!



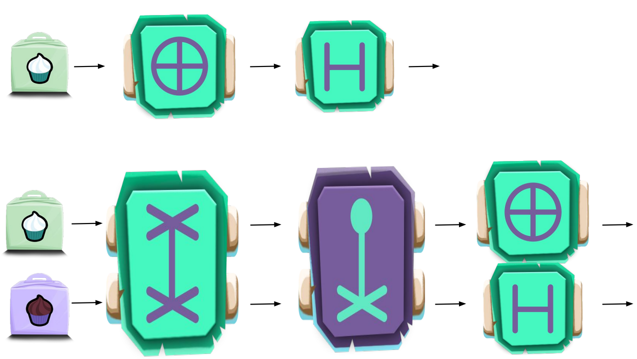
Probability (e.g. 50%), not outcome, **is predictable**.

Update our model: Superposition State

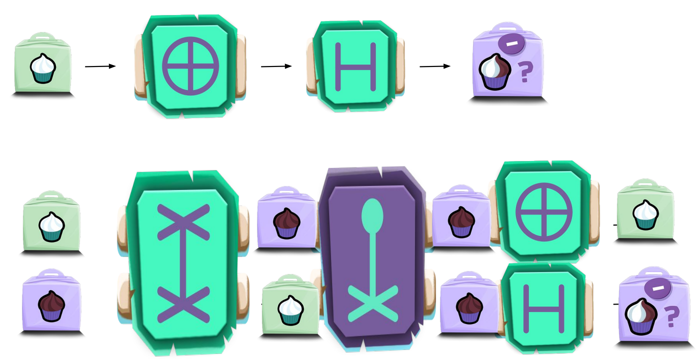


Superposition State - 50/50 probability of measuring chocolate or vanilla

What are the outcomes?

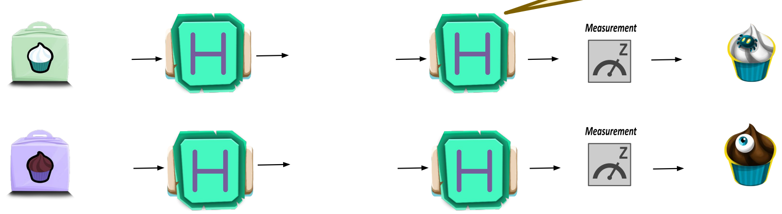


What are the outcomes?



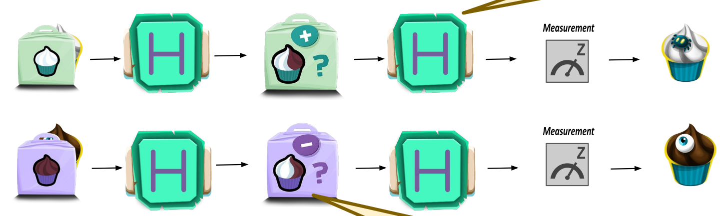
Look what happens?!?

H gate also reverses itself



Update our model: Phase

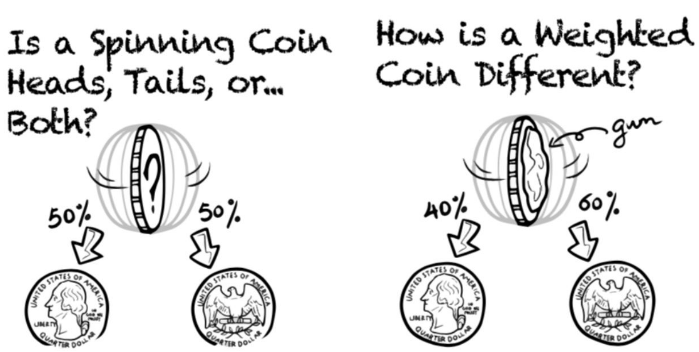
H gate also reverses itself



Must be a difference between these two states - it is **phase**

You Can **Control the Probability** of each Quantum State Value being Measured

Superposition:
Holds 0 & 1 at once
Control probability of measuring outcome
Cannot read full state



Measurement vs State: Sometimes state wins

Measurement:
Does not capture entire state

Measurement vs State: Sometimes state loses

Measurement:
Does not capture entire state

(unless you are a trained free diver)

Measurement disturbs state

Superposition:
Holds 2 values at once
Cannot read full state

A bit: Stores either the value 0 or 1 at any given time

Int x = 5;
println("X = " + X);
println("X = " + X);

```
>> java cstate
>> X = 5
>> X = 5
>> java cstate
>> X = 5
>> X = 5
```

A qubit: Stores several things, including both 0 and 1

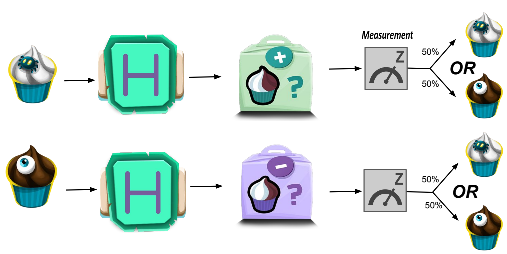
X = 5 and 8 and 12;

println("X = " + X);
println("X = " + X);

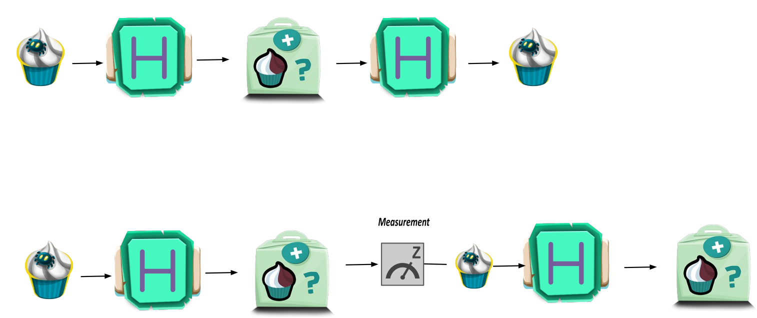
```
>> java cstate
>> X = 5
>> X = 5
>> java cstate
>> X = 12
>> X = 12
```

Once read, it no longer holds all 3 and will get the same result without resetting the program.

Measurement Changes State!!



Let's compare....



Summary

Just like classical computers, quantum computers store values in bits

Bits work together to be numbers or other data

Quantum computers have some extra operations and states - with superposition

Superposition can be very powerful, allowing **more data to be stored** at once and **more operations to be performed** at once.

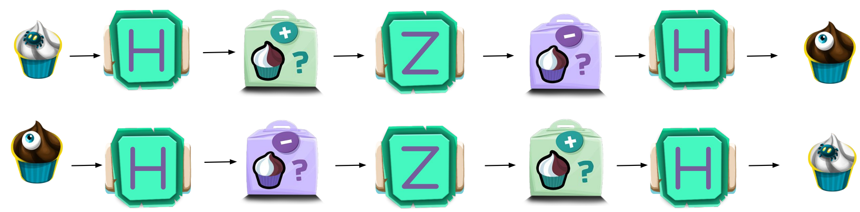
Quantum state is locked in the quantum bit - measurement does not reveal the whole state

Measurement collapses superposition, change the value of the qubit

Games, cartoons, analogies can help novices learn these concepts

Quander.cs.uchicago.edu - our games for middle & high school students (you have to give consent for us to use your gameplay data)

Z Gate toggles the phase



Measurement corollary: No cloning

Measurement:
Does not capture entire state
Collapses state
Cannot copy state

We CAN make qubits have a particular state that is known a-priori

We CAN NOT take a qubit of unknown state and copy it.

No Cloning Theorem: You can't copy state

Measurement:
Does not capture entire state
Collapses state
Cannot copy state

A bit: Stores either the value 0 or 1 at any given time

```
Int x = 5;
Y = X;
println("X = " + X);
println("Y = " + Y);
```

A qubit: Stores several things, including both 0 and 1

```
X = 5 and 8 and 13;
Y = X
println("X = " + X);
println("Y = " + Y);
```

To play: http://quander-lite.s3-website-us-east-1.amazonaws.com/

THE UNIVERSITY OF CHICAGO

EPiQC

@EPiQCExpedition

http://quander-lite.s3-website-us-east-1.amazonaws.com/
http://epiqc.cs.uchicago.edu/resources

Quantum Ops that act like Classical Ops