Blockchain

What it is
How it works
Why it is important

Objectives

* Present basics of the blockchain
  * What it is
  * Why it is important
  * How it works
  * A few examples
* No attempt to defend Bitcoin or cryptocurrency, that is another brief

Simple Definition

* Distributed ledger of transactions
* Transactions can be of many different types including:
  * Cryptocurrency
  * Executable distributed code contracts (smart contracts)
  * Distributed intellectual property (IP) registry

Why it is important

* A distributed ledger, unlike a single computer, is very difficult to hack or disable
* Common blockchains are not controlled by a single company or government
  * Researchers Hanke and Busnell have verified 57 episodes of hyperinflation in history, i.e., 50% increase in price in 1 month
* Many systems used today were designed long ago, and are inefficient
  * Why does it take 9 days to transfer a few 529 college fund dollars from one account to another?

Side Story: Crypto Munitions

* In 1991 Phil Zimmermann created Pretty Good Protection (PGP) source code and gave it to a friend, who posted it to several electronic bulletin boards
* In 1993 Zimmermann became the formal target of a criminal investigation by the US Government for "munitions export without a license"
    * An attempt to control cryptography
* Zimmermann published the entire PGP source code in a hardcopy book.
* The export of books is protected by the First Amendment
* Remove the binder, scan pages with OCR, you get the PGP source code

Fundamental: Hash Function

data

bit string, fixed size

* It is a mathematical **algorithm** that **maps** data of arbitrary size to a **bit string** of a fixed size
* It is a one-way function, that is infeasible to invert
* Two sets of "data" can be determined the same from their hash signatures

SHA256

A Block Can Be Anything

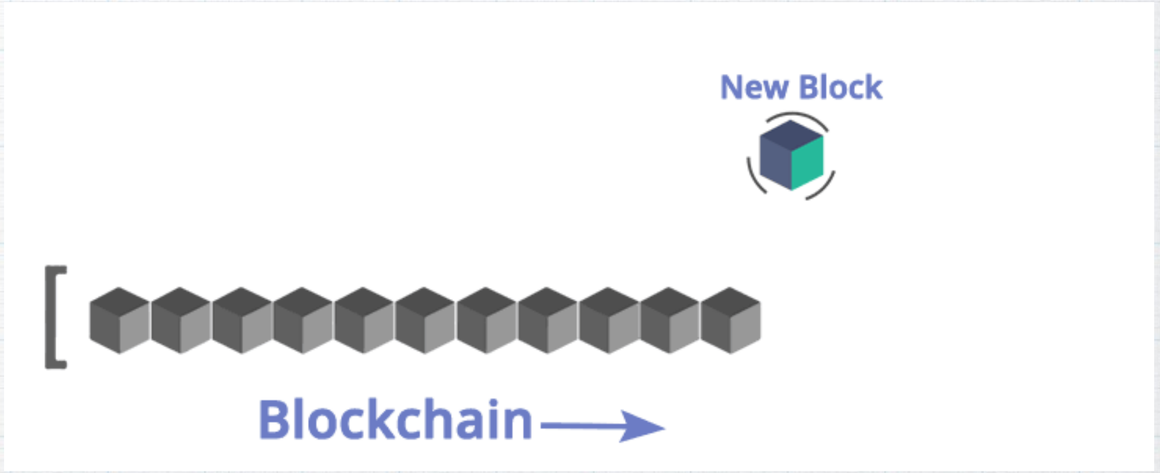
- A block is a collection of information, it can be anything
  - Any combination of numbers, letters, pictures, videos
  - GPS locations, place names, thing names, people names
  - Dates, times, amounts, account numbers...
  - Runs, hits, outs, ..., votes, results
  - Any binary sequence, anything that can be represented in a computer
- A finite size, generally blocks are all the same size
- Each block has a hash number
  - Makes it easy to compare two blocks

Blocks Are Immutable

- Blocks are immutable, meaning they are unchanging over time, or cannot be changed
  - The number 5 is unchanging, it is immutable
  - The variable X can change, and is not immutable

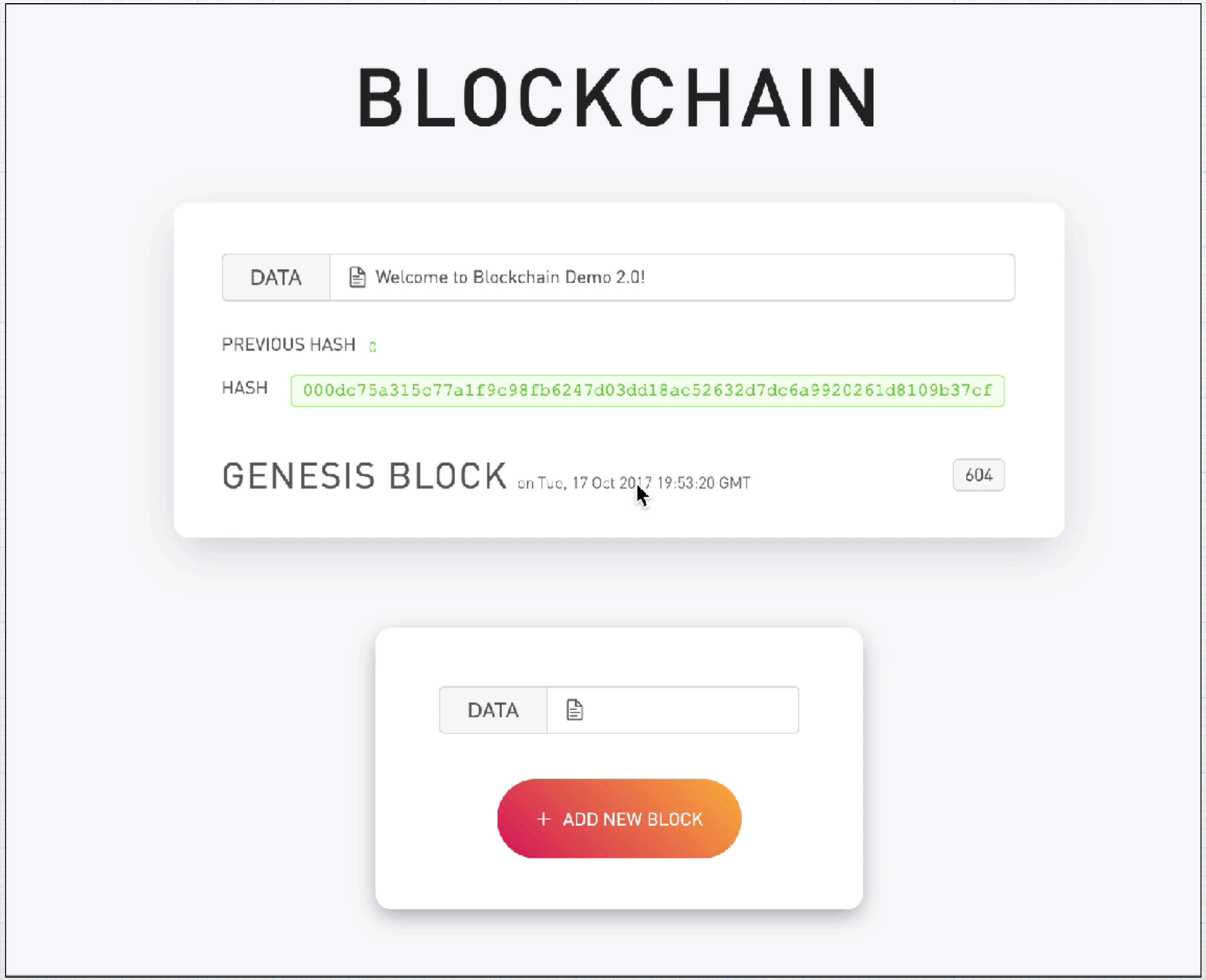
Chain of Blocks

* Blockchain is a collection of blocks
* Latest block has hash of all previous block hashes



* The blockchain can be confirmed to be accurate by recalculating hashes

Blockchain Demo



https://
blockchaindemo.io/

Blockchain Cost

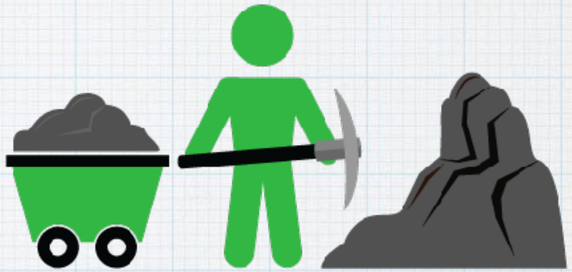
* Global power consumption for the servers that run bitcoin is about of 2.5 gigawatts
    * Ireland uses a similar amount of electricity
* Data centers are located where it is cold and energy is cheap, such as Iceland, Sweden, and Russia
* New protocols such as Proof-of-Stake will reduce power costs significantly

6 GPUs per computer
6 computers per row
6 rows per bay

Crypto Economics

* Typical public blockchain runs from 10s of thousands to billions of computers called **miners**
* Each computer is trying to earn rewards
  * For creating the next block
  * For verifying a transaction
  * Field of study is called **crypto economics**
* If there is no main computer, who controls how rewards are earned?

Proof Of Work



* Proof of work is a consensus algorithm
* All **miners** are on a peer to peer network, and are equally important
* **Miners** are all presented with the same transaction challenge
* The **miner** that finishes first, gets to create the next block and gets a reward
* Other **miners** that validate the transaction, by getting the same result within a time window, also get a reward
* At least 51% of the **miners** must agree with the result, or it is invalid

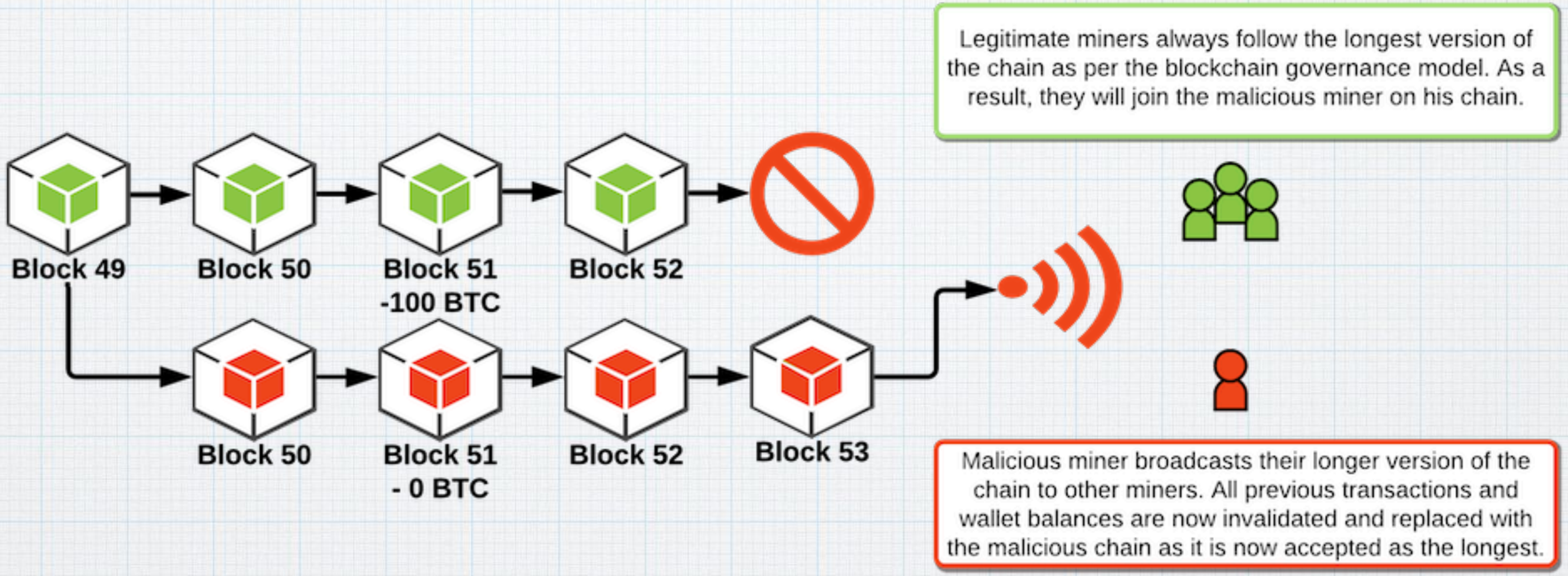
Blockchain Applications

* Money
* Insurance
* Government
* Financial Services
* Healthcare
* Music
* Real Estate
* Supply Chain

Risks

- In 10 years since it's creation, the Bitcoin blockchain has never been hacked
- Exchanges have been hacked
  - Exchanges are typically owned by a company and are prone to insider activity
- Individual crypto-wallets have been hacked
- Recently the Ethereum Classic blockchain was hacked
  - Someone exploited a bug in the software, gained 51% of the computing power, re-wrote transactions, and double spent currency

51% Attack



* If 51% or more have the same answer, the transaction is considered valid
* If 51% or more have the same WRONG answer, the transaction is considered valid

Discussion

* The 50 largest public companies are exploring blockchain
* Each marketplace will likely adopt blockchain when threatened with extinction

Fundamental: Public Key Cryptography

* Public key: shared with others
  * Used to encrypt things
* Private key: kept as a secret by the user
  * Used to decrypt things