

The background of the slide is a repeating pattern of 3D cubes in various colors (red, orange, green, purple, blue, yellow). Each cube has three arrows pointing downwards from its top face, suggesting a flow or sequence. A solid blue rectangle is centered on the slide, containing the title text.

The Blockchain Trevor Hyde

Bitcoin

- ▶ Bitcoin is a **cryptocurrency** introduced in 2009 by the mysterious Satoshi Nakamoto.



- ▶ Satoshi Nakamoto has never been publicly identified.

Bitcoin

- ▶ Over the past year the value of Bitcoin skyrocketed to nearly \$20,000 per coin.



- ▶ This rapid appreciation generated a lot of interest in **blockchains**, the technology underlying Bitcoin.

Blockchains Everywhere

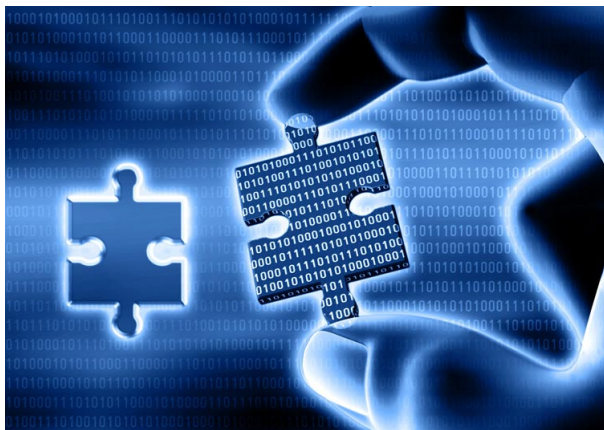
- Many new cryptocurrencies and other blockchain applications sprung up subsequently.



- While the blockchain bubble seems to have burst, the technology is here to stay!

Goals

- ▶ Blockchains somehow involve “miners”, cryptography, and lots of computers solving “difficult math puzzles”.



- ▶ My goal in this talk is to explain what blockchains are, how they work, and why they're awesome.

What problem do blockchains solve?

- ▶ A **public record** is a source of important public information.
- ▶ **Examples:**
 1. Property ownership: Who owns stuff?
 2. Voting/democracy: Who voted and for what?
 3. Government records: What are they up to?
 4. Monetary system: Who has money/credit?
 5. Stock market: How's Big Corp doing?
 6. Internet: Where's my website?

What problem do blockchains solve?

- ▶ A **public record** is any source of important public information.
- ▶ **Examples:**
 1. Property ownership (government)
 2. Voting/democracy (government)
 3. Government records (government)
 4. Monetary system (banks)
 5. Stock market (corporations)
 6. Internet (DNS servers, mostly in USA)
- ▶ **Major problem:** the public records need to have integrity in order for these systems to work, and this requires that we **trust the institutions** that maintain the public records!

Public Record Wish List

- ▶ We want a system of public records with the following properties:
 1. **Integrity:** Cannot be maliciously altered.
 2. **Decentralized:** Not maintained by a central authority.
 3. **Transparency:** Can easily be audited for integrity, including the underlying system.
- ▶ **Solution?**

Public Record Wish List

- ▶ We want a system of public records with the following properties:
 1. **Integrity:** Cannot be maliciously altered.
 2. **Decentralized:** Not maintained by a central authority.
 3. **Transparency:** Can easily be audited for integrity, including the underlying system.
- ▶ **Solution?**

Blockchains!

What is a blockchain?

- ▶ **Model for public records:** a long list of information which can be added to but not changed.
- ▶ Break list into **blocks** and **chain** them together in chronological order
= blockchain.
- ▶ **Important innovations:**
 1. How the blockchain is stored.
 2. How new blocks are added.



Who stores the blockchain?



Everyone stores the blockchain!

- ▶ There is no “official copy”, the record is constantly maintained by anyone and everyone.
- ▶ Redundancy prevents errors and makes it difficult to alter.
Think: DNA.

How are blocks added?

- ▶ Blocks are added to the blockchain by **miners**. The process of creating a block to add to the blockchain is called **mining**.



- ▶ The details of mining vary based on the application. I will focus on how it works for the **Bitcoin blockchain**.

What is the Bitcoin blockchain?

- ▶ The Bitcoin blockchain consists entirely of transactions of Bitcoin between addresses.



- ▶ You can imagine a room full of transparent safety deposit boxes filled with money.
- ▶ The boxes do not belong to anyone, all you need is a secret password to take Bitcoin out of a box.

What is the Bitcoin blockchain?

- ▶ Bitcoin never leaves this room!
- ▶ Transactions slipped into the room and carried out by miners.
- ▶ All transactions are recorded on the blockchain.
- ▶ Since the Bitcoin never leaves the room, it doesn't matter if it exists!
- ▶ In reality, there are no boxes with money, there is only the **record** of the transactions!

Mining blocks

- ▶ Pending transactions are submitted to a public pool.
- ▶ Miners collect a bunch of these transactions and put them together into a block.
- ▶ Miners have a complete copy of the blockchain. They use this to check that all the transactions are valid.
- ▶ Miners include one more transaction giving themselves some Bitcoin for doing such good work.
 - ▶ This Bitcoin comes from nowhere!
 - ▶ This is how all Bitcoins are made.

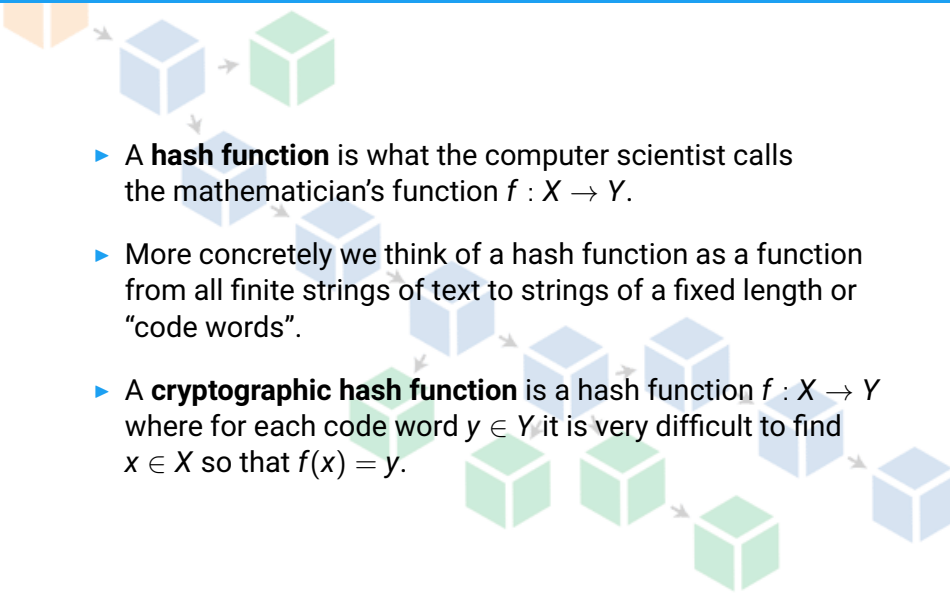
Mining blocks

- ▶ Finally comes the hard part: miners have to find a **key** to “lock the block”.
- ▶ Once they find the key, they announce their success to the world and the new block is added to the blockchain!
 - ▶ The transactions in the block become Official.
 - ▶ The new bitcoin is now real and belongs to the miner.
 - ▶ Everyone starts working on the next block.

Lock that Block

- ▶ “Locking” is accomplished by adding a special key to the block which verifies that nothing in the block has been changed.
- ▶ Finding this key takes a long time for a computer, but can be easily checked once found.
- ▶ This process is called **proof of work**. It requires a **cryptographic hash function**.

Cryptographic Hash Functions

- 
- ▶ A **hash function** is what the computer scientist calls the mathematician's function $f : X \rightarrow Y$.
 - ▶ More concretely we think of a hash function as a function from all finite strings of text to strings of a fixed length or "code words".
 - ▶ A **cryptographic hash function** is a hash function $f : X \rightarrow Y$ where for each code word $y \in Y$ it is very difficult to find $x \in X$ so that $f(x) = y$.

Example: SHA-256

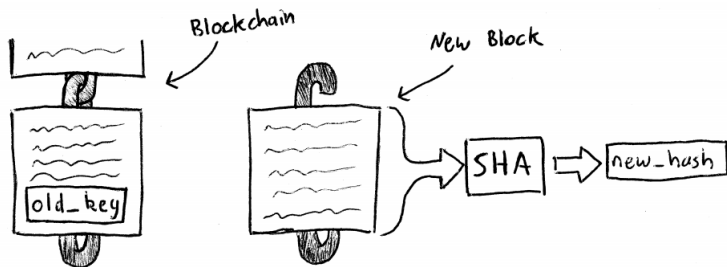
- ▶ **Secure Hash Algorithm** with 256-bit output.

$SHA(\text{password}) = 5e884898da28047151d0e56f8dc62927$
 $73603d0d6aabbdd62a11ef721d1542d8$

$SHA(\text{Password}) = e7cf3ef4f17c3999a94f2c6f612e8a88$
 $8e5b1026878e4e19398b23bd38ec221a$

$SHA(\text{pass word}) = 78980e257f412437fbf9343787bc00ec$
 $5b10636429bc000b290107335b089786$

Proof of Work



- ▶ Let `old_key` be the last key on the blockchain and let `new_hash` be the hash value of our new block.
- ▶ We look for a string `key` so that

$SHA(\text{old_key} + \text{new_hash} + \text{key})$ starts with n zeros.

- ▶ The larger n is, the harder it is to find `key`.

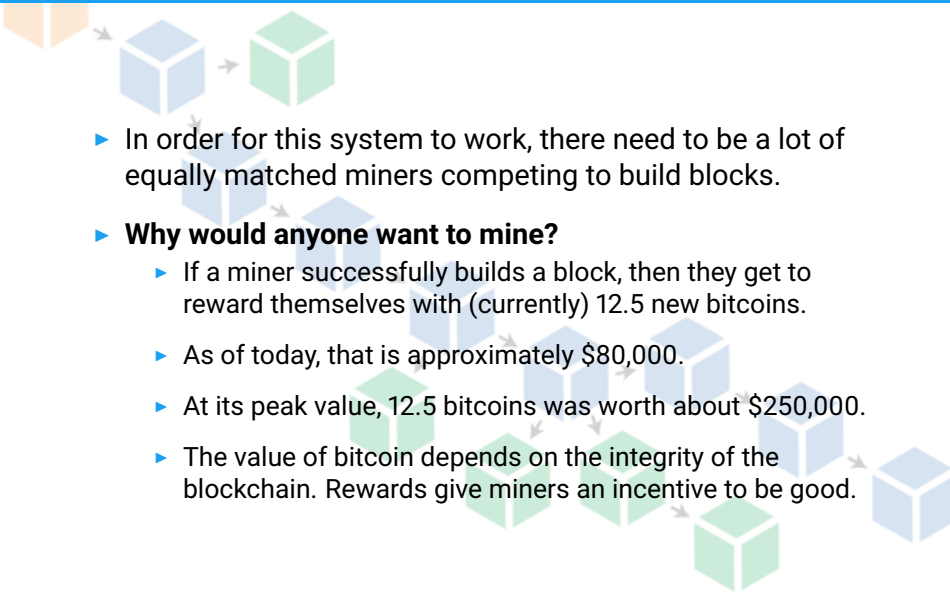
Proof of Work

- ▶ The most efficient way to find `key` is by trial and error, which takes a long time!
- ▶ People build “mining farms” to search for `key`.




- ▶ Once `key` is found, it is easy for anyone to check that it is correct.

Why mine?

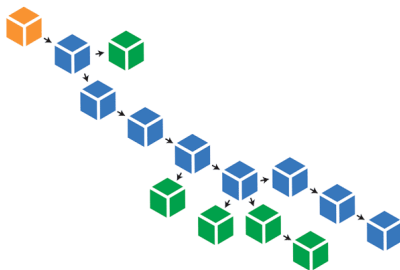
- 
- ▶ In order for this system to work, there need to be a lot of equally matched miners competing to build blocks.
 - ▶ **Why would anyone want to mine?**
 - ▶ If a miner successfully builds a block, then they get to reward themselves with (currently) 12.5 new bitcoins.
 - ▶ As of today, that is approximately \$80,000.
 - ▶ At its peak value, 12.5 bitcoins was worth about \$250,000.
 - ▶ The value of bitcoin depends on the integrity of the blockchain. Rewards give miners an incentive to be good.

Why not build blocks in a bubble?

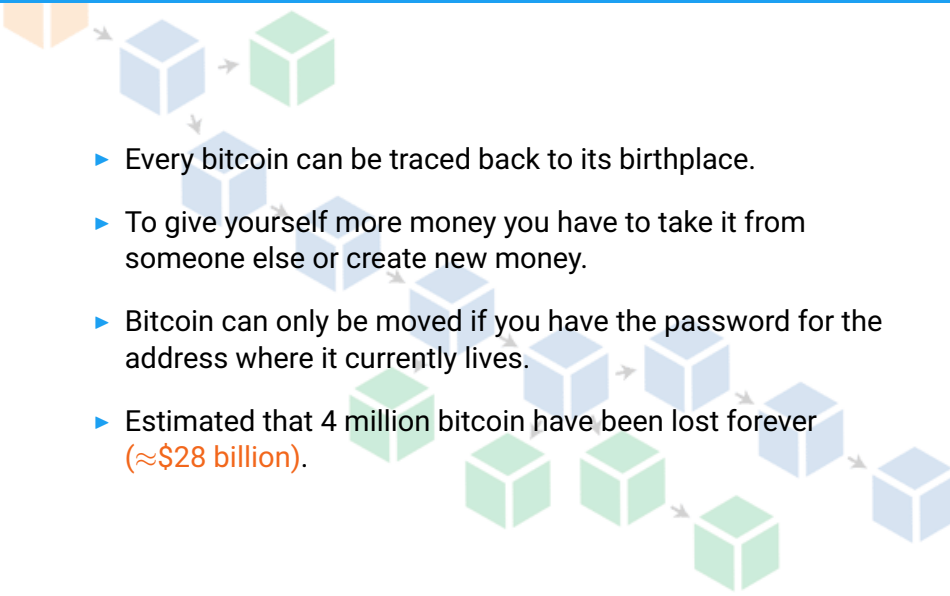
- 
- ▶ Miners constantly compete to build the next block.
 - ▶ When a miner successfully builds a block, they announce it to the world and everyone starts working on the next block.
 - ▶ **Why not ignore the blocks built by others and just keep working on your own?**
 - ▶ General protocol: go with the longest legitimate version of the blockchain.
 - ▶ You have to finish your current block and the subsequent block before anyone else finishes the next block.
 - ▶ Since mining takes so long and competition is strong, this is a bad strategy.

What if two blocks are made at the same time?

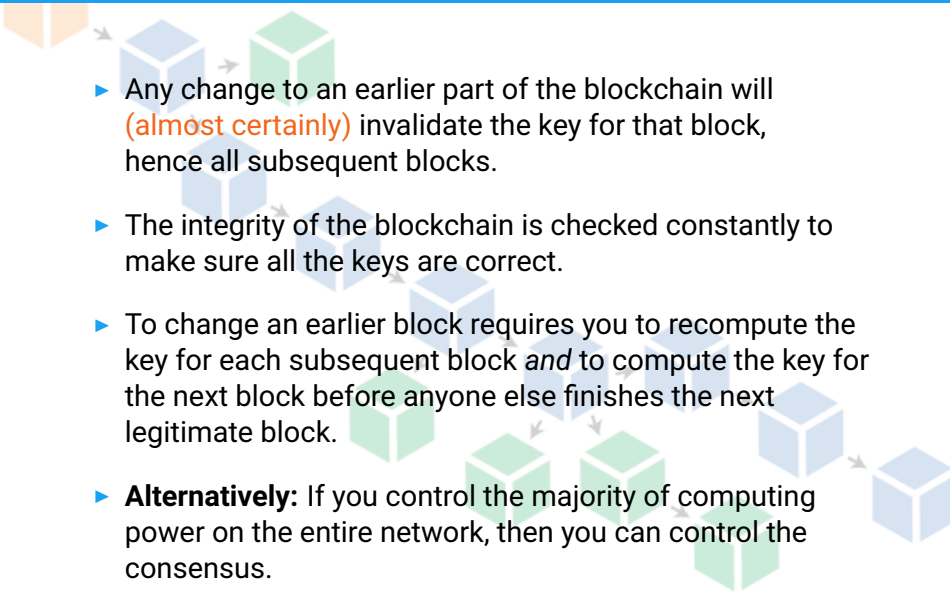
- ▶ Each miner works on the first legitimate version of the blockchain they encounter and switch only when a longer chain becomes available.
- ▶ The bitcoin universe temporarily splits into two parallel realities competing for existence.
- ▶ Whichever one succeeds first lives and the other dies.



Why not give yourself more money?

- 
- ▶ Every bitcoin can be traced back to its birthplace.
 - ▶ To give yourself more money you have to take it from someone else or create new money.
 - ▶ Bitcoin can only be moved if you have the password for the address where it currently lives.
 - ▶ Estimated that 4 million bitcoin have been lost forever (**≈\$28 billion**).

Why not erase transactions?

- 
- ▶ Any change to an earlier part of the blockchain will **(almost certainly)** invalidate the key for that block, hence all subsequent blocks.
 - ▶ The integrity of the blockchain is checked constantly to make sure all the keys are correct.
 - ▶ To change an earlier block requires you to recompute the key for each subsequent block *and* to compute the key for the next block before anyone else finishes the next legitimate block.
 - ▶ **Alternatively:** If you control the majority of computing power on the entire network, then you can control the consensus.

Problems

- 
- ▶ Proof of Work combined with intense competition maintains the blockchain's integrity.
 - ▶ **Problem:** Mining consumes a lot of resources.
 - ▶ **Problem:** How do you give cryptocurrency value?
 - ▶ **Problem:** Anonymous money promotes crime and terror.
 - ▶ **Alternative Problem:** Bitcoin isn't anonymous enough!

- ▶ Bitcoin was the first blockchain, but since then many new applications of blockchain have been found.
- ▶ One of the most interesting is **Ethereum**.
- ▶ The Ethereum blockchain stores the state of a **virtual machine**.



ETHEREUM

- ▶ Think of the Ethereum blockchain as the memory for a **decentralized computer**.
- ▶ Programs called **smart contracts** live and operate on this virtual machine.
- ▶ Instead of money transactions, people submit new programs or interactions with existing programs.
- ▶ Miners = CPU. Miners process the instructions and update the state of the machine.
- ▶ Ethereum blockchain can do *anything* a blockchain can possibly do!

Example: DAO

- ▶ DAO = **D**ecentralized **A**utonomous **O**rganization.
- ▶ Company/organization/government with no central leader.
- ▶ Shareholders/members/citizens vote through a smart contract to make decisions collectively.
- ▶ **Example:** a DAO investment fund could use “collective wisdom” to make smart investments.

Example: CryptoKitties

- ▶ **CryptoKitties** is a game running on Ethereum where users can buy, sell, trade, and breed unique virtual cats.
- ▶ In December 2017, a CryptoKitty sold for \$100,000.



Example: EtherTweet

- ▶ Tweet on the blockchain.
- ▶ Use policies encoded by a smart contract.
- ▶ Censorship impossible!
- ▶ Good? Bad?

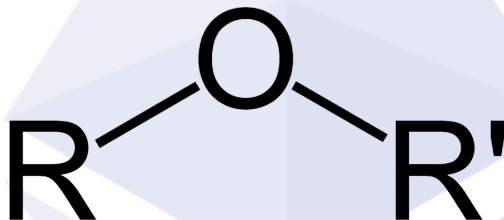
Halting Problem

- ▶ What's to stop someone from flooding the virtual machine with malicious programs?
- ▶ What if a mistake is made and a smart contract gets stuck in an infinite loop?
- ▶ Turing proved that no program can detect infinite loops in all programs.



- ▶ Ethereum solves these problems by putting a cost on all computations.
- ▶ Computations on the Ethereum virtual machine require **Ether** to run.
- ▶ Ether is paid to miners for the work of processing the computations.
- ▶ Ether can be bought and sold like Bitcoin, but unlike Bitcoin it also has a specific purpose which gives it value.

- ▶ If someone wants to run malicious programs to clog the Ethereum network, they have to pay for it.
- ▶ If a mistake pushes a smart contract into an infinite loop, it eventually run out of Ether and stop.



Explore the Blockchain and SHA-256

- ▶ Explore the Bitcoin or Ethereum blockchain yourself!
 - ▶ **Bitcoin:** <https://www.blockchain.com/explorer>
 - ▶ **Ethereum:** <https://etherscan.io/>
- ▶ Compute SHA-256 hash values!
 - ▶ **SHA-256 with Java implementation:**
<https://www.movable-type.co.uk/scripts/sha256.html>
- ▶ Read the original white papers!
 - ▶ **Bitcoin:** <https://bitcoin.org/bitcoin.pdf>
 - ▶ **Ethereum:**
<https://github.com/ethereum/wiki/wiki/White-Paper>

The background of the slide is a repeating pattern of 3D cubes in various colors (red, orange, green, purple, blue, yellow). Each cube has three arrows pointing downwards from its top face, creating a sense of flow or descent.

Thanks!