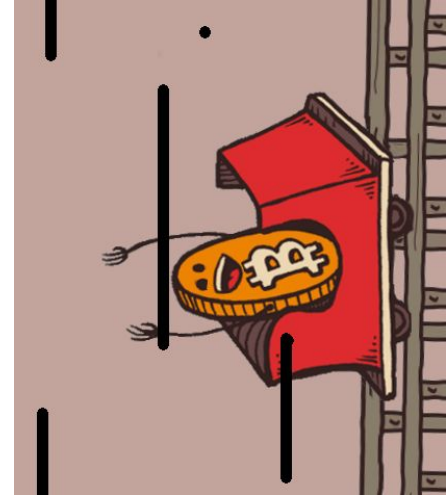
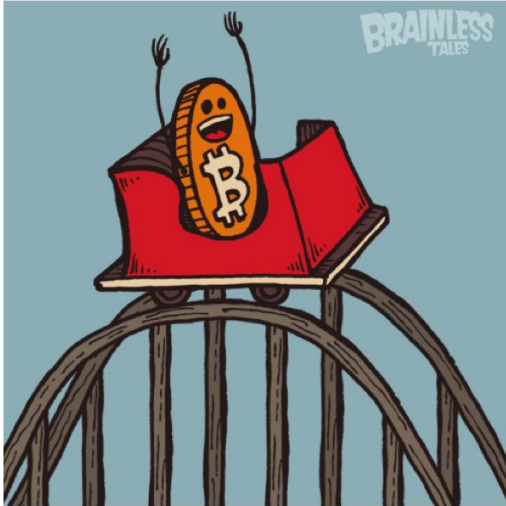


# Intro to Bitcoin Montreal

Alex Melville





Alex Melville

Software Engineer  
@BitGo

World Traveler

[github.com/Melvillian](https://github.com/Melvillian)



# Tonight

- 40 minute **intro** talk
  - 5 minutes for questions
  - 30 minute break
- 
- 40 minute **technical** talk
  - 5 minutes for questions
  - freedom!

# Intro to Bitcoin

- A Short History of Bitcoin
- Real World Examples
- What IS Bitcoin?
- How Do I Value Bitcoin?
- How It Works
  - Addresses, Blocks, Miners Developers
- Done!

# Why I'm Here Tonight

We're just getting started

Most exciting time to be in the cryptocurrency space is right now

Solving problems nobody has ever solved before

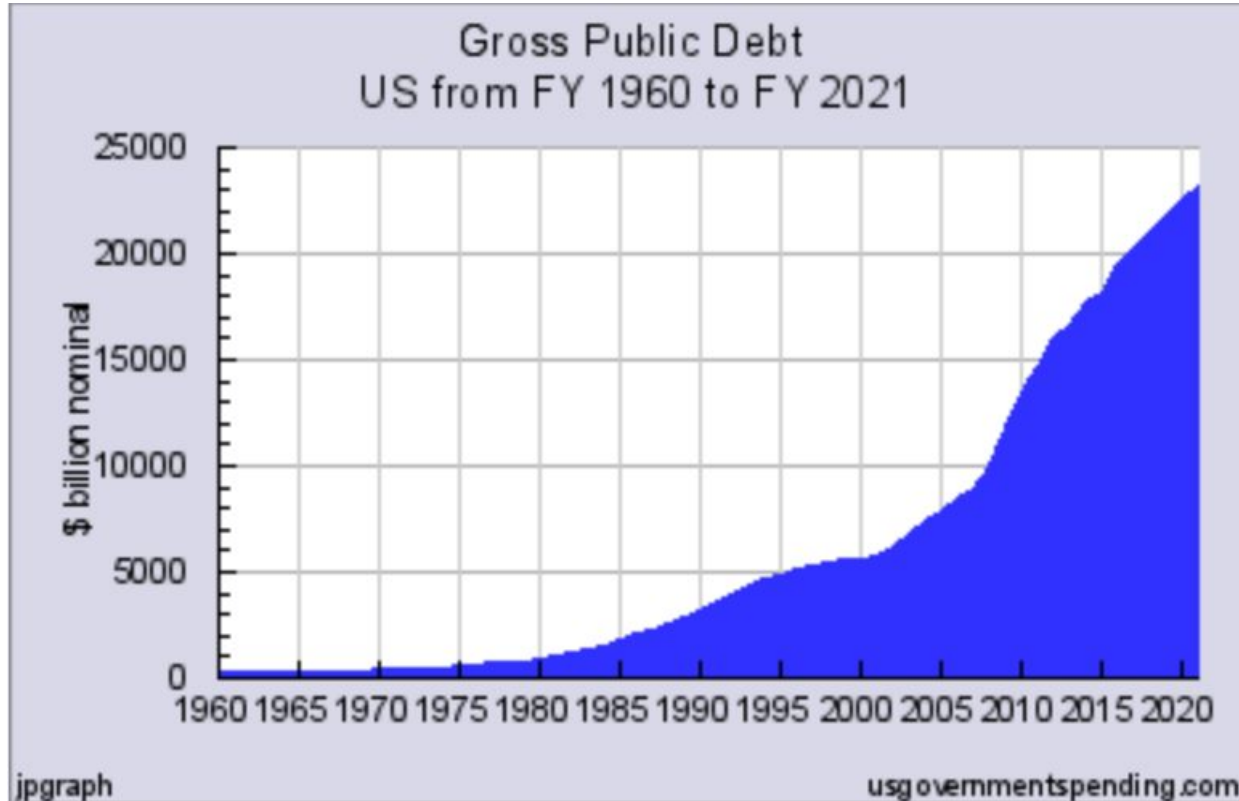
I love what I'm doing, and I want to share it with you so perhaps you can dive in and go from knowing nothing (like I did) to waking up each day thinking about what can I work on today

a story, a story...

# 2008 (The Great Recession)



# 2008 (The Great Recession)





2009 (Birth of Bitcoin)

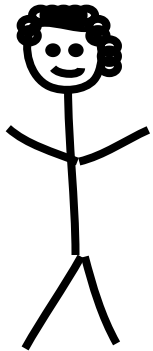
# Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto  
satoshin@gmx.com  
[www.bitcoin.org](http://www.bitcoin.org)

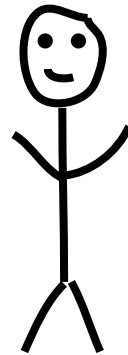
**Abstract.** A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a

# Before Bitcoin

Alice



Bob

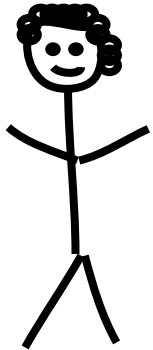


# Before Bitcoin

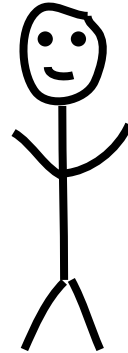


BANK OF CANADA

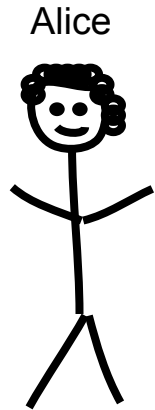
Alice



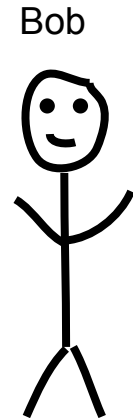
Bob



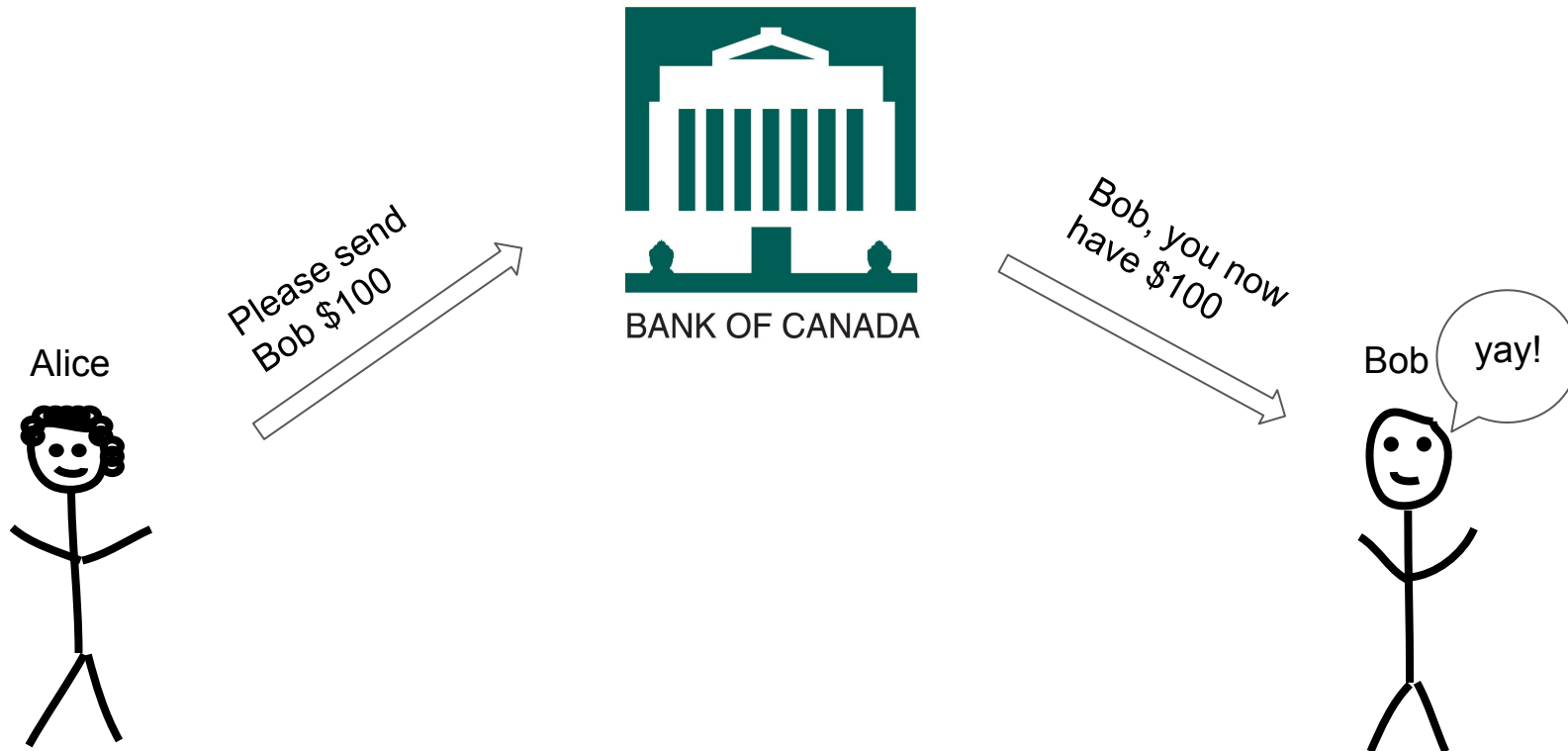
# Before Bitcoin



Please send  
Bob \$100

A white arrow with a black outline pointing from Alice towards the Bank of Canada.

# Before Bitcoin

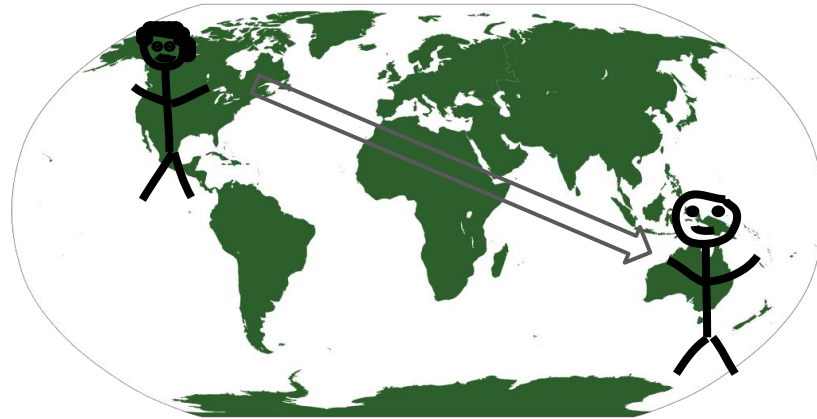


# After Bitcoin







BANK OF CANADA

Hey!



# 2010 (Last Post by Satoshi Nakamoto)

 Author	Topic: Added some DoS limits, removed safe mode (0.3.19) (Read 20253 times)
<b>satoshi</b> Founder Sr. Member  	<div data-bbox="318 305 985 354"> <b>Added some DoS limits, removed safe mode (0.3.19)</b> <u>December 12, 2010, 06:22:33 PM</u></div> <div data-bbox="1883 322 1922 343">#1</div> <hr/> <div data-bbox="309 371 1903 425">There's more work to do on DoS, but I'm doing a quick build of what I have so far in case it's needed, before venturing into more complex ideas. The build for this is version 0.3.19.</div>

# 2010-2013 (Software Growth, Mt. Gox Crash)





2013-Present (Too Many to Mention!)



Real World Examples (bread wallet)



bread

b43,920 = \$463.40



Sent **b300,000** 20 s  
to 38rrzX4kQEd...sJbMSz8LbSW  
Transfer to bitgo "bread receive"  
In progress: 40%

Sent **b1,022.23** 11/30/17  
to 1FqW9VM...1pq5T9rqYKwg  
Complete

Sent **b2,500** 09/15/17  
to 3GXgJvEQ...QQxAbWNdF  
Complete

Sent **b4.000** 09/11/17



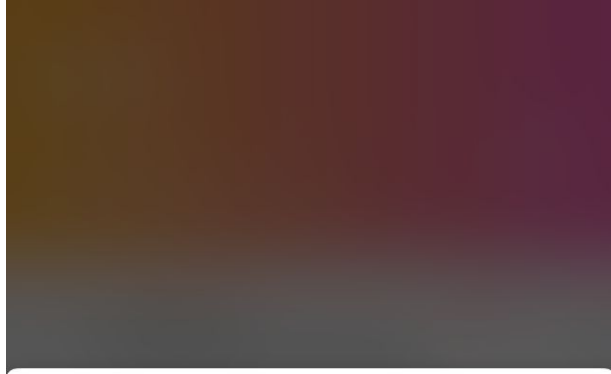
SEND



RECEIVE



MENU



Send



To

38rrzX4kQE...MSz8LbSW

Paste

Scan

₮1,000

Bits(₮)

Network Fee: ₮407 

Memo

Send



## Confirmation

Send

₮1,000 (\$10.55)

To

38rrzX4kQEd8...sJbMSz8LbSW

Processing time: This transaction is predicted to complete in 10-60 minutes.

Amount to Send:	₮1,000
Network Fee:	₮538
<b>Total Cost:</b>	<b>₮1,538</b>

Cancel



Send

bread

b43,920 = \$463.40



Sent **b300,000** 20 s  
to 38rrzX4kQEd...sJbMSz8LbSW  
Transfer to bitgo "bread receive"  
In progress: 40%

Sent **b1,022.23** 11/30/17  
to 1FqW9VM...1pq5T9rqYKwg  
Complete

Sent **b2,500** 09/15/17  
to 3GXgJvEQ...QQxAbWNdF  
Complete

Sent **b4.000** 09/11/17



SEND



RECEIVE



MENU



Receive



1AnFdz2niZgfC29ABKqggDZFjnf71NNyfW

 Share

Request an Amount

# What IS Bitcoin?



What IS Bitcoin?

Bitcoin is about **Trust**

What IS Bitcoin?

# Bitcoin is about **Trust**

Let's you send money to anyone on the planet (with an Internet connection)  
without a third-party (bank)

# What IS Bitcoin?

- Ledger
- Global
- Decentralized
- Append-Only
- Cryptographic Security

# What IS Bitcoin?

- Ledger

View - General Ledger Entries - 5300 Office Supplies

CRONUS Navigator Demo Master 1 - Serenic\_2013R2\_Demo - k12p14...

General Ledger Entries

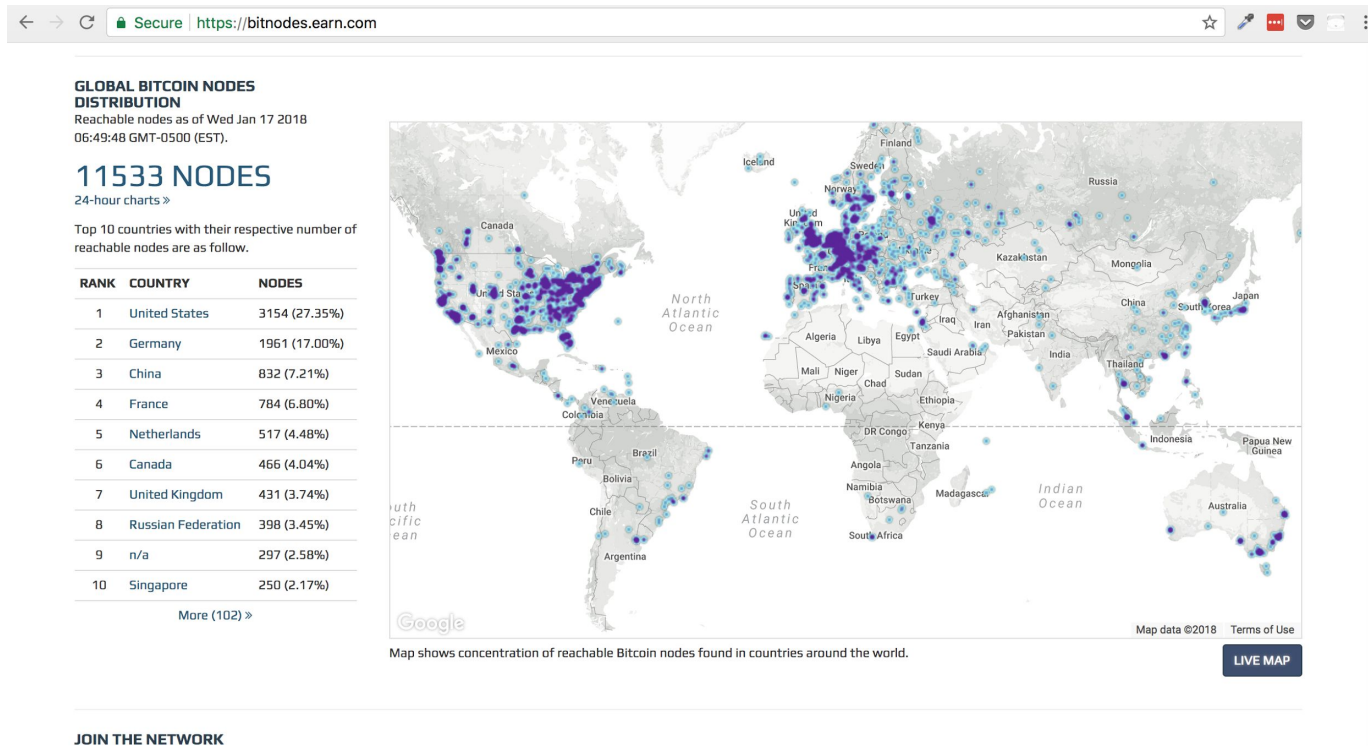
Type to filter (F3) Amount Filter: 5300 • Actual

Posting Date	Document Type	Document No.	External Document No.	G/L Account No.	Fund No.	Dept	Program	Description	Amount	Reason Code	Source Code	Source Type	Source No.
3/6/2015	Invoice	PPI00210		5300	F100	110		Office Supplies	108.00		GLRECLASS	Vendor	V200
3/9/2015	Invoice	PPI00212	PI-46466	5300	F100	100	100	Office Supplies	500.00		PURCHASES	Vendor	V200
3/9/2015	Invoice	PPI00212	PI-46466	5300	F100	100	100	Office Supplies	500.00		PURCHASES	Vendor	V200
3/9/2015	Invoice	PPI00213	PI-46464	5300	F100	200	100	Copy Machine Supplies	500.00		PURCHASES	Vendor	V110
3/9/2015	Invoice	PPI00213	PI-46464	5300	F100	200	200	Copy Machine Supplies	1,000.00		PURCHASES	Vendor	V110
3/9/2015	Invoice	PPI00215	454545	5300	F100	100	130	Supplies	451.22		PURCHASES	Vendor	V200
3/9/2015	Invoice	PPI00215	454545	5300	F100	100	100	Supplies	504.56		PURCHASES	Vendor	V200
3/9/2015	Invoice	PPI00216	33434	5300	F100	100	200	Office Supplies	500.00		PURCHASES	Vendor	V110
3/9/2015	Invoice	PPI00217	ABC123	5300	F100			Office Supplies	500.00		PURCHASES	Vendor	V200
3/9/2015	Invoice	PPI00218	PI-565656	5300	F100	100	200	Administrative Line Allocation	440.00		PURCHASES	Vendor	V110
3/9/2015	Invoice	PPI00218	PI-565656	5300	F100	110	200	Administrative Line Allocation	200.00		PURCHASES	Vendor	V110
3/9/2015	Invoice	PPI00218	PI-565656	5300	F100	200	200	Administrative Line Allocation	220.00		PURCHASES	Vendor	V110
3/9/2015	Invoice	PPI00218	PI-565656	5300	F100	140	200	Administrative Line Allocation	250.00		PURCHASES	Vendor	V110
3/9/2015	Invoice	PPI00218	PI-565656	5300	F100	140	200	Administrative Line Allocation	210.00		PURCHASES	Vendor	V110
3/9/2015	Invoice	PPI00218	PI-565656	5300	F100	120	200	Administrative Line Allocation	300.00		PURCHASES	Vendor	V110
3/9/2015	Invoice	PPI00218	PI-565656	5300	F100	130	200	Administrative Line Allocation	380.00		PURCHASES	Vendor	V110

Close

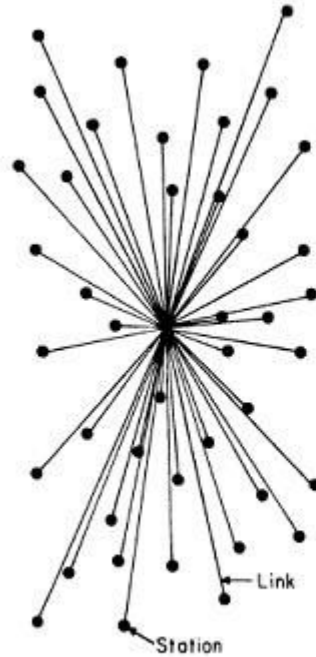
# What IS Bitcoin?

- Ledger
- Global

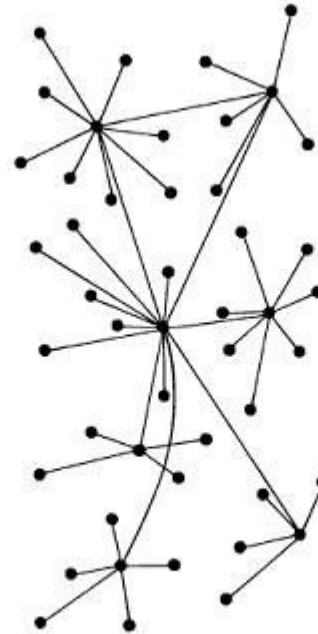


# What IS Bitcoin?

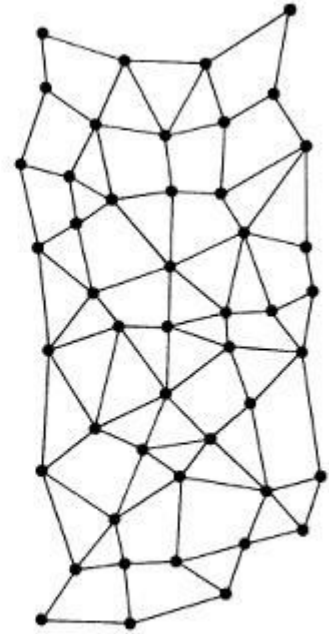
- Ledger
- Global
- **Decentralized**



CENTRALIZED  
(A)



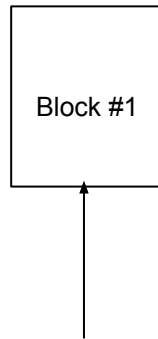
DECENTRALIZED  
(B)



DISTRIBUTED  
(C)

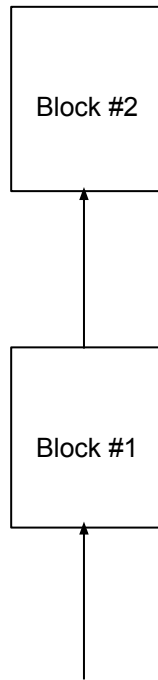
# What IS Bitcoin?

- Ledger
- Global
- Decentralized
- **Append-Only**



# What IS Bitcoin?

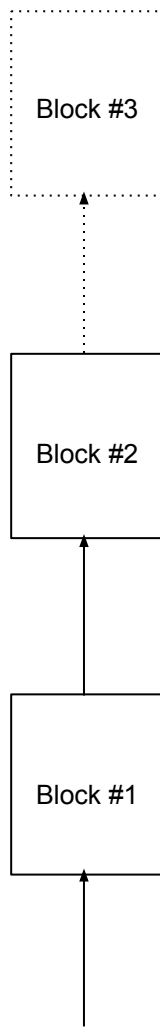
- Ledger
- Global
- Decentralized
- **Append-Only**





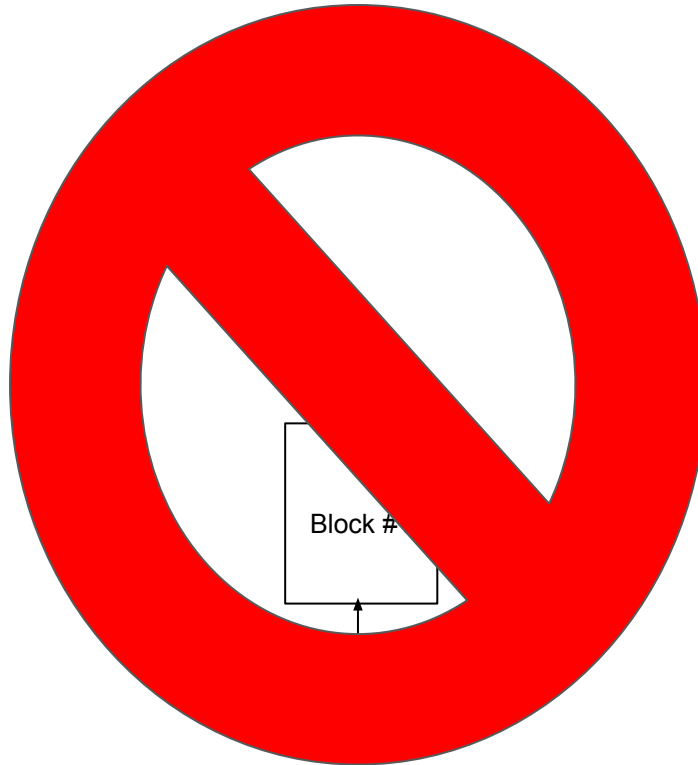
# What IS Bitcoin?

- Ledger
- Global
- Decentralized
- **Append-Only**



# What IS Bitcoin?

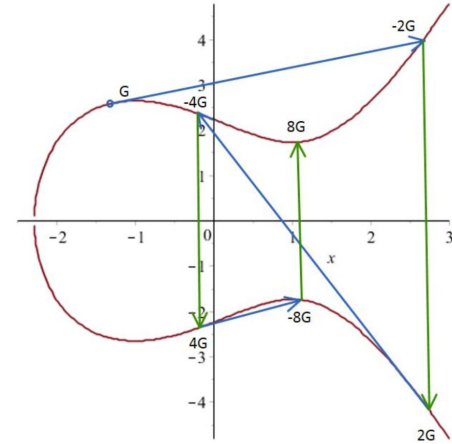
- Ledger
- Global
- Decentralized
- **Append-Only**



# What IS Bitcoin?

- Ledger
- Global
- Decentralized
- Append-Only
- **Cryptographic Security**

Digital Signatures



Cryptographic  
Hash Functions

Message



Hash Algorithm

SHA256



Hash Value

c323e4c2dc58224583767  
1faa90ed390dbd105fbeb29bd  
bf66673bcbe580fbf

SHA1 vs SHA 256

# How Do I Value Bitcoin?

# How Do I Value Bitcoin?

- Tough Question



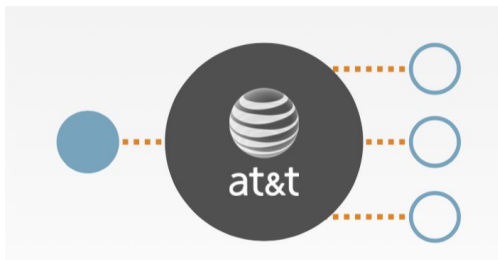
# How Do I Value Bitcoin?

- Tough Question
- Attempt #1: Cost to secure the network (Miner cost)

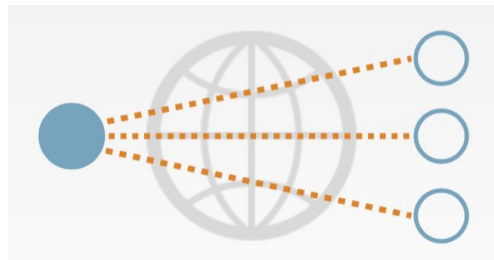
# How Do I Value Bitcoin?

- Tough Question
- Attempt #1: Cost to secure the network (Miner cost)
- Attempt #2: What's the value in being able to programmatically transact with anyone who has an Internet connection?

Before Internet



After Internet



# How Do I Value Bitcoin?

- Tough Question
- Attempt #1: Cost to secure the network (Miner cost)
- Attempt #2: What's the value in being able to programmatically transact with anyone who has an Internet connection?

Before Bitcoin



After Bitcoin





# Thanks! Stick Around For More On...

- Blockchain
- Cryptography
- Miners
- Addresses
- Smart Contracts
- ... And More!

# Resources

- Usgovernmentspending.com
- finance.google.com
- <https://cointelegraph.com/news/five-bitcoin-crashes-and-what-you-can-learn-from-them>
- Balaji Srinivasan “Bitcoin: A Overview”