




# Bitcoin invention

A photograph of Jeff Booth, a man with short brown hair, wearing a white button-down shirt. He is gesturing with his hands while speaking. The background is dark and out of focus.

“Bitcoin might just be humanity’s  
greatest invention”

*Jeff Booth*



A photograph of Larry Fink, CEO of Blackrock, speaking at a podium. He is wearing a dark suit, a light blue shirt, and a patterned tie. He has glasses and is looking slightly to his left. The background is a blue wall with the word "ECONOMIC" visible in white letters.

“Bitcoin will revolutionize finance”

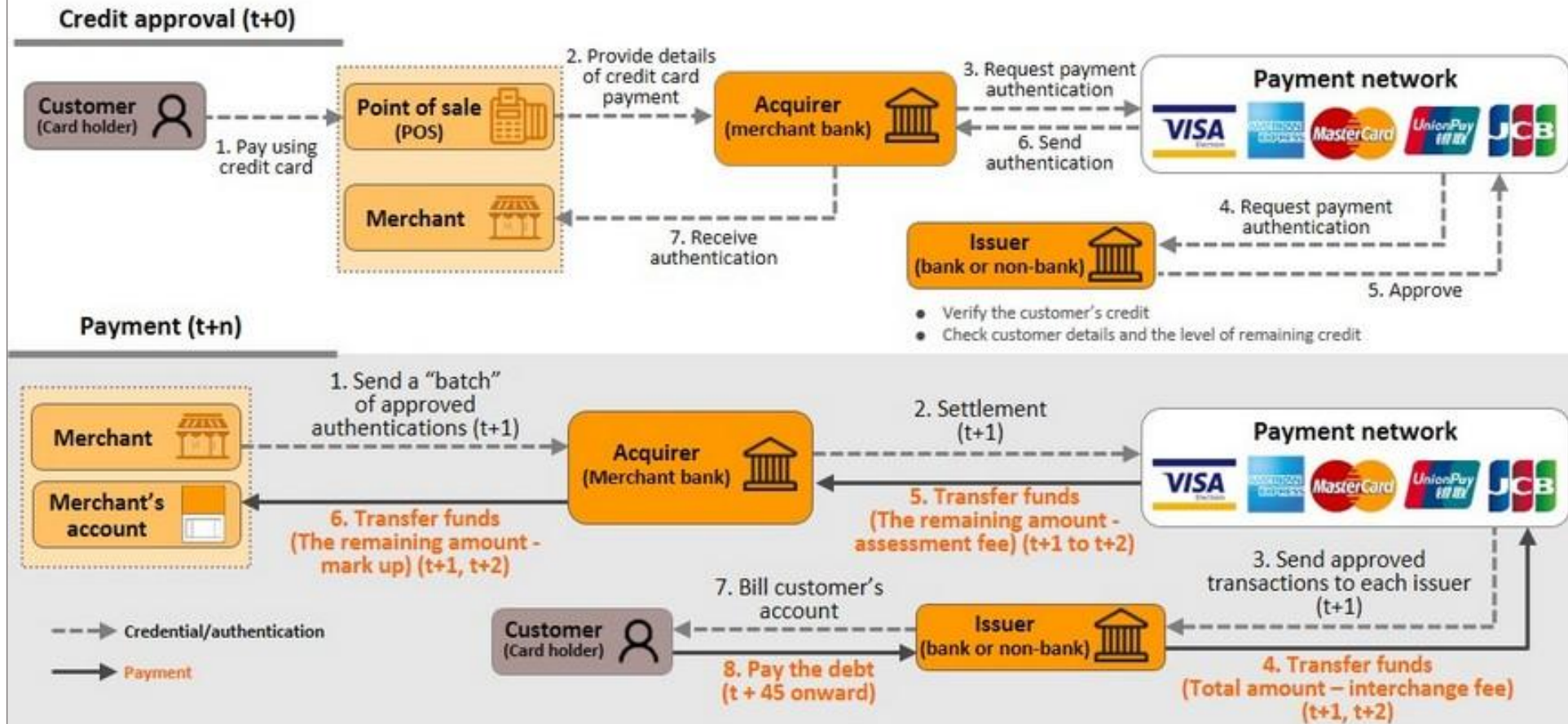
CEO Larry Fink

*Blackrock*

*world's largest asset manager*

*world's most powerful company*

Figure 2: Credit Card Payment Processing

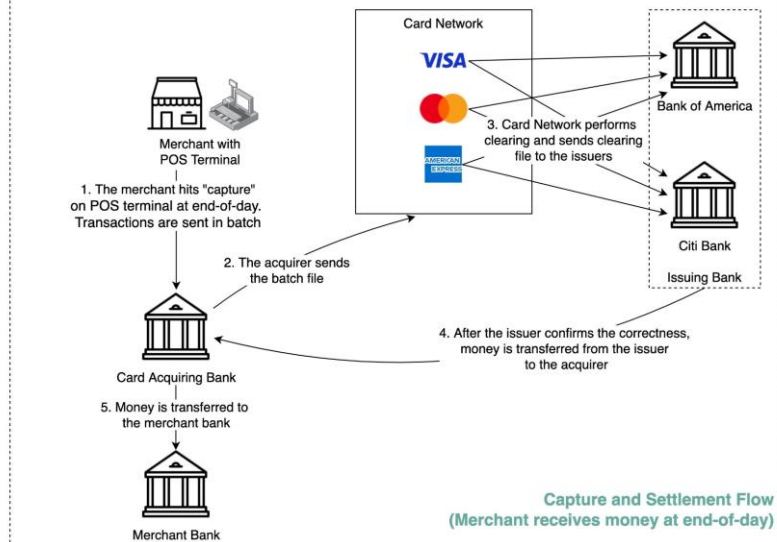
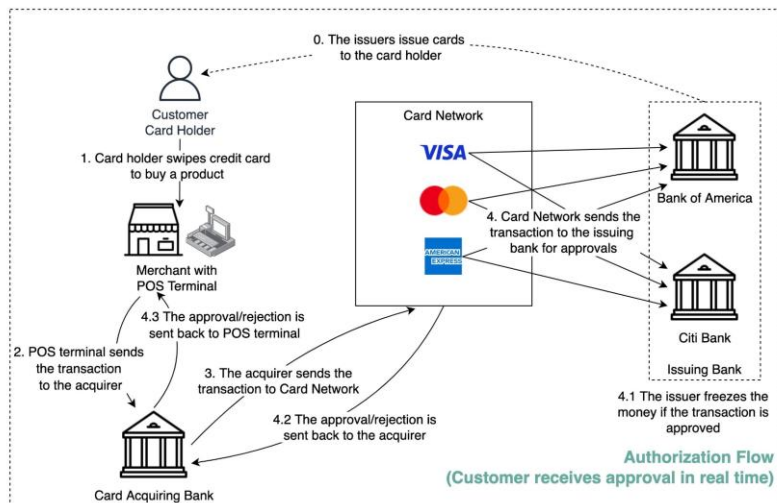


Source: Krungsri Research



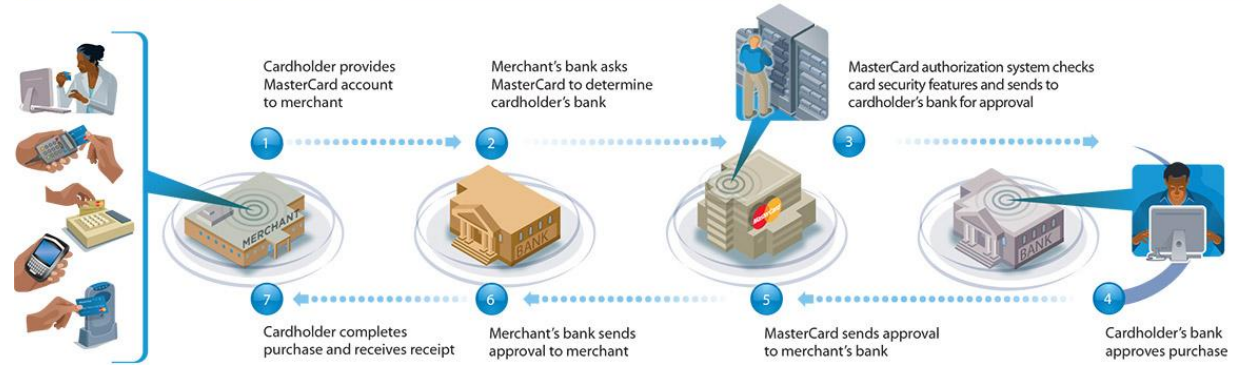
## How does VISA Work?

blog.bytebytego.com



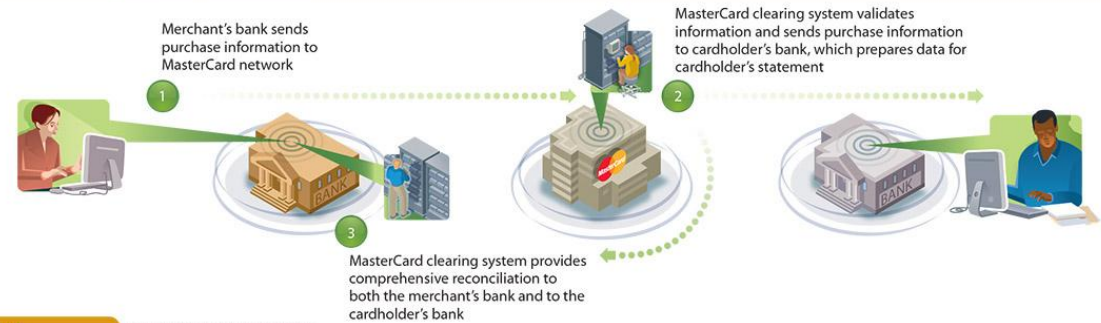
## AUTHORIZATION

TIME OF PURCHASE



## CLEARING

USUALLY WITHIN ONE DAY



## SETTLEMENT

USUALLY WITHIN TWO DAYS



AOTE-0707  
© 2007 MasterCard







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

Satoshi Nakamoto  
satoshin@gmx.com  
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 financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Bitcoin is digital money



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

Satoshi Nakamoto  
satoshin@gmx.com  
www.bitcoin.org

**Abstract.** A purely peer-to-peer version of electronic cash was needed to enable payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

- Scarce
- Digital
- Permissionless
- Borderless
- Un-censorable
- Fast
- Cheap
- Irreversible
- Decentralized
- Deflationary
- Private
- Programmable

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

Satoshi Nakamoto  
satoshin@gmx.com  
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 financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1

peer-to-peer



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

Satoshi Nakamoto  
satoshin@gmx.com  
www.bitcoin.org

electronic payments  
directly from one  
party to another

**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 financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.





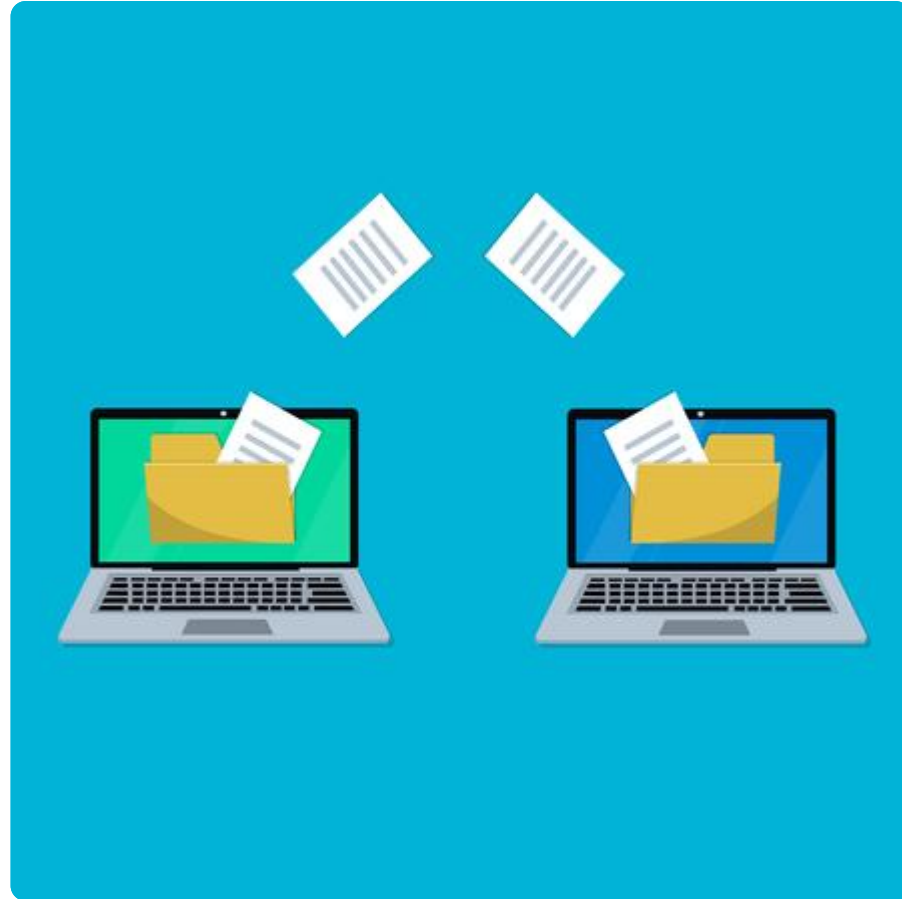
**peer to peer: yes**  
**electronic: no**



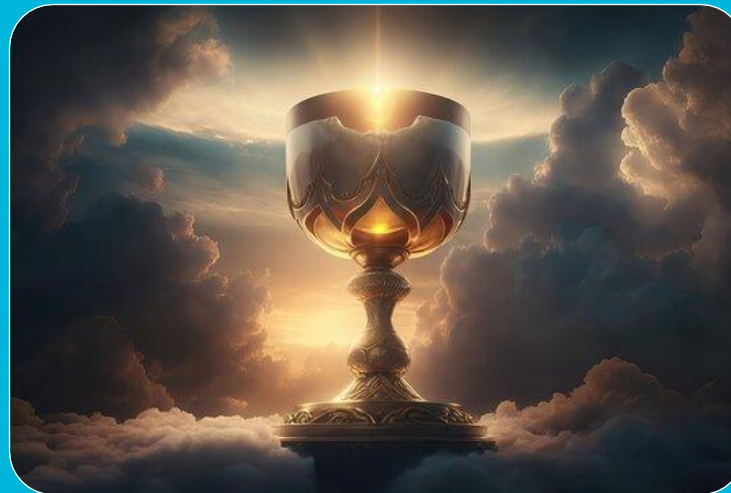
**electronic: yes  
peer to peer: no**











?

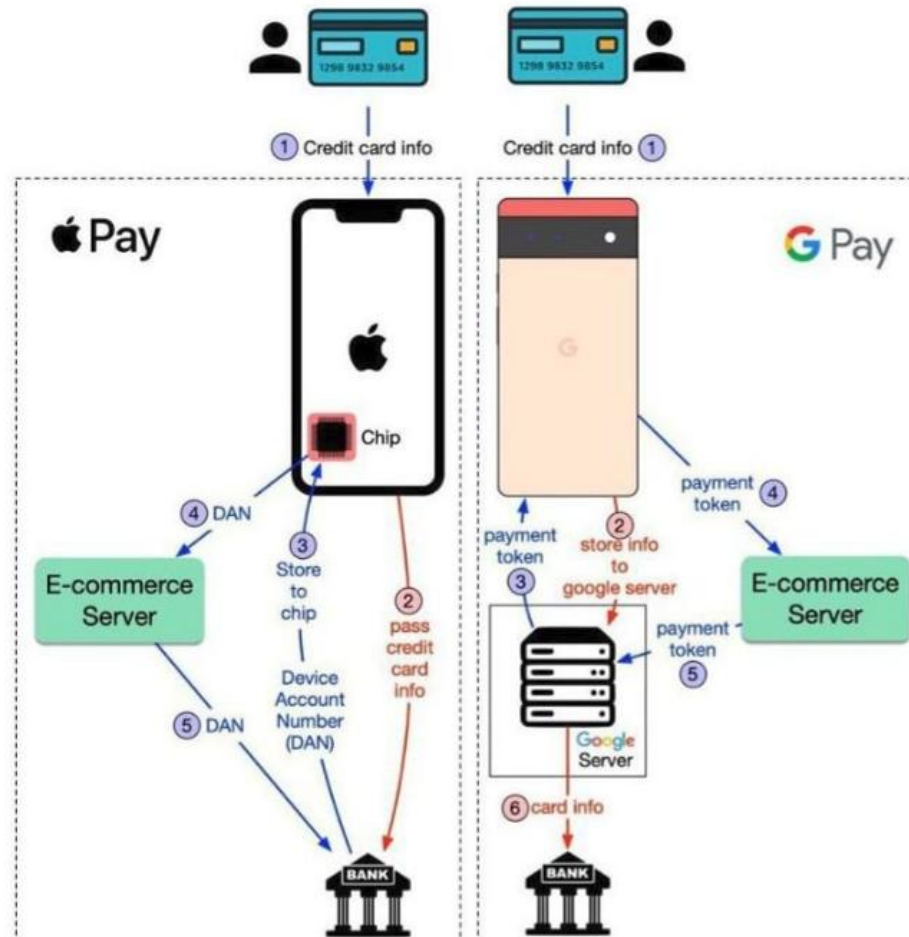


- Bank cheque
- EFT
- credit card
- Apple pay
- Venmo
- Wire transfer
- SWIFT
- Loyalty points
- Pre-paid card
- Gift Cards
- e-bucks



# Apple Pay

# Google Pay

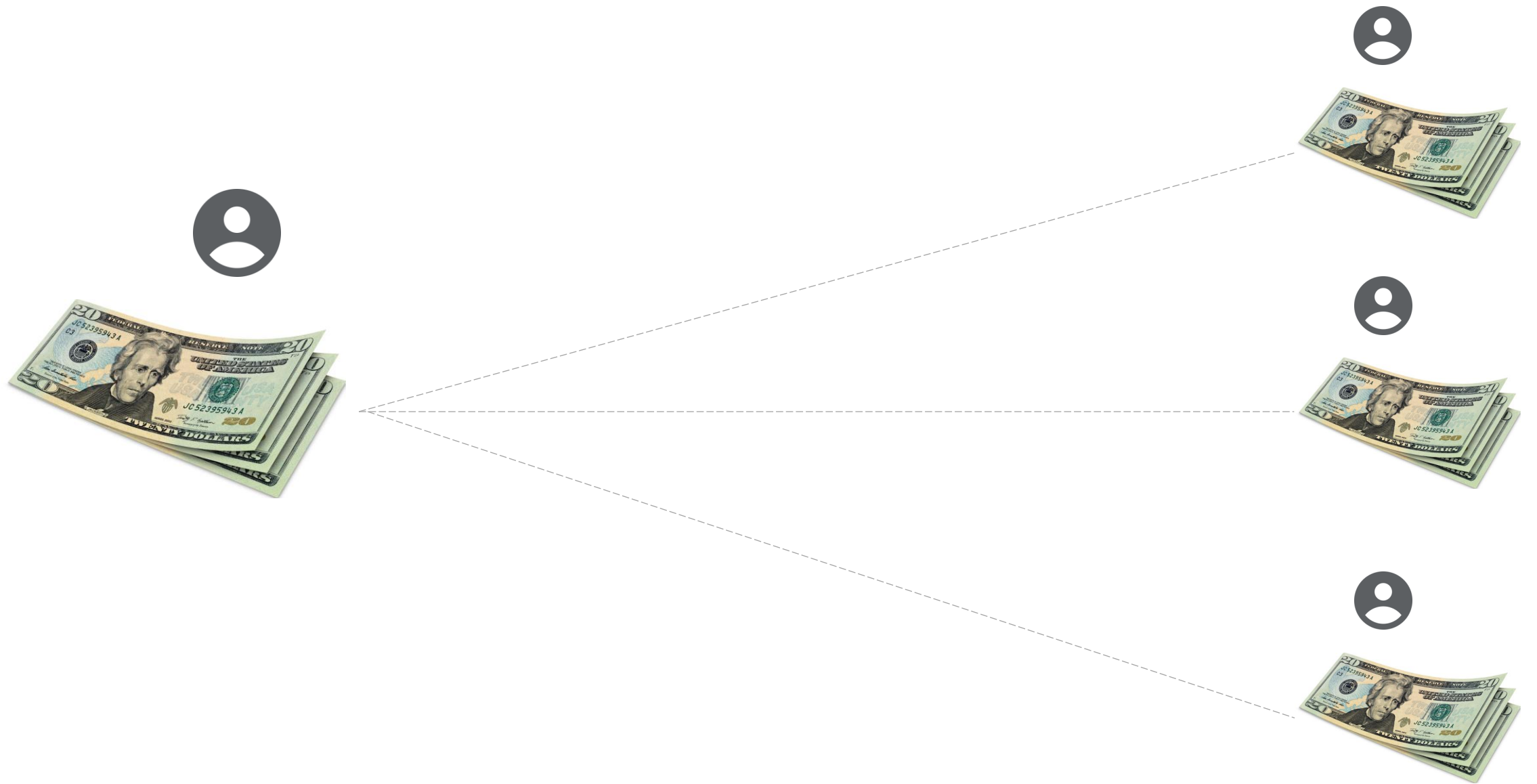












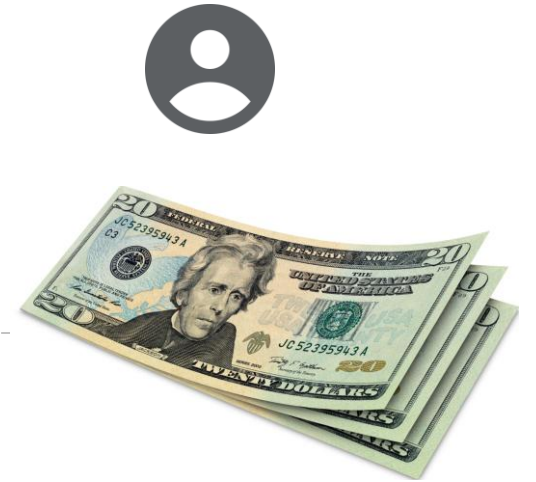
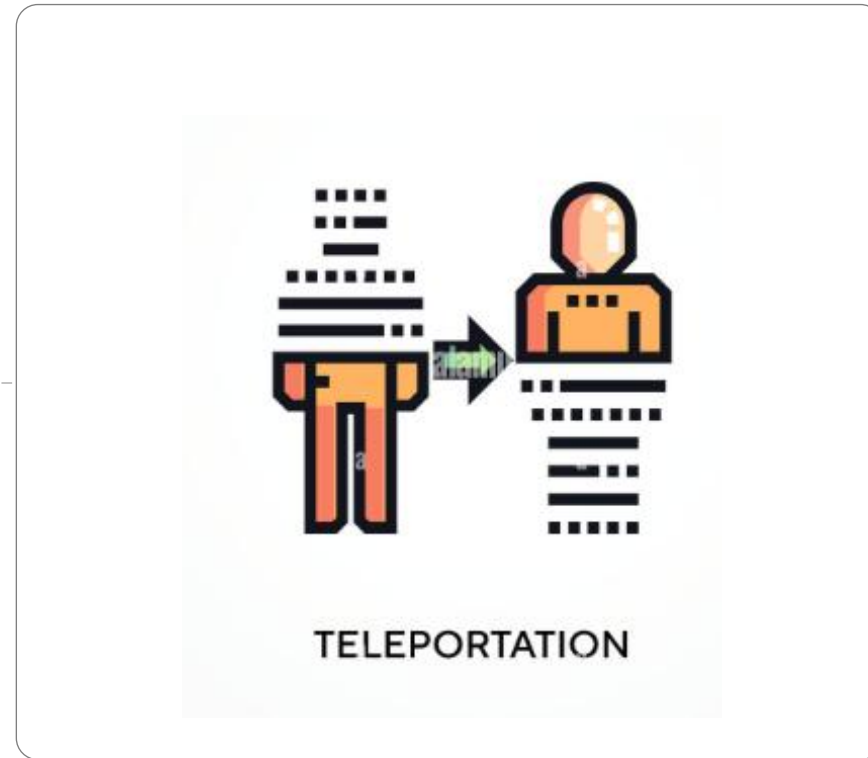
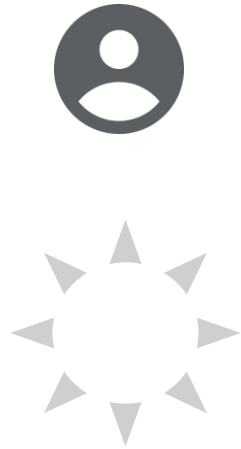
# Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto  
satoshin@gmx.com  
www.bitcoin.org

double spending  
problem

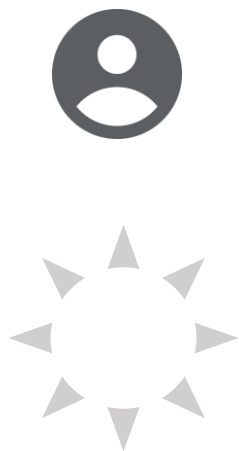
**Abstract.** A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.











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

Satoshi Nakamoto  
satoshin@gmx.com  
www.bitcoin.org

electronic **payments**  
directly from one  
party to another

**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 financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

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

Satoshi Nakamoto  
satoshin@gmx.com  
www.bitcoin.org

**Abstract.** A purely peer-to-peer version of electronic cash was proposed with payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1

peer-to-peer

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

Satoshi Nakamoto  
satoshin@gmx.com  
www.bitcoin.org

**Abstract.** A purely peer-to-peer version of electronic cash was proposed with payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

2

distributed  
consensus

ledger









## Pictographic Tablet Mesopotamia (3200 BC)



## The double-entry ledger (1340 AD)

Date		CK	Deposits	Bank	
1944		No		Paid	Outs
Dec 1	Balances forwarded				
	West End Bldg Loan Co. 687				10000
	First Federal Sav. & Loan 688				20000
	Poples Home & Savings Co. 689				20000
	West End Bldg Loan Co. 690				50000
	West End Bldg Loan Co. 691				10876
	Chas. F. Holdrege for Mission 692		11377		12146
	Rev. Allen B. Layman 693		17625		25000
	Frank Simons 694		13965		12080
	Mary G. Slade 695		20000		4400
21.	Chas. F. Holdrege 696		4000		12247
	Adam H. Bartel Co. 697		13202		220
	Light Plant 698		12247		1980
	The C & Ward Co. 699		27574		772
	Engineering Sales & Ser. Co. 700		1190		500
	Kepler Wall Paper Co. 701		2500		1730
	Earl M. Feltis 702		100.00		500
	Home Laundry 703				425
	Cash for Misc. 704				
	J. M. ... 705				

	A	B	C	D
1				
2		<b>Double Entry Accounting</b>		
3				
4		<b>Cash Purchase of Equipment</b>		
5		Account	Debit	Credit
6		Cash	--	\$250,000
7		Equipment	\$250,000	--
8				
9		<b>Credit Purchase of Inventory</b>		
10		Account	Debit	Credit
11		Inventory	\$50,000	--
12		Accounts Payable	--	\$50,000
13				
14		<b>Credit Sale to Customer</b>		
15		Account	Debit	Credit
16		Accounts Receivable	\$20,000	--
17		Sales Revenue	--	\$20,000























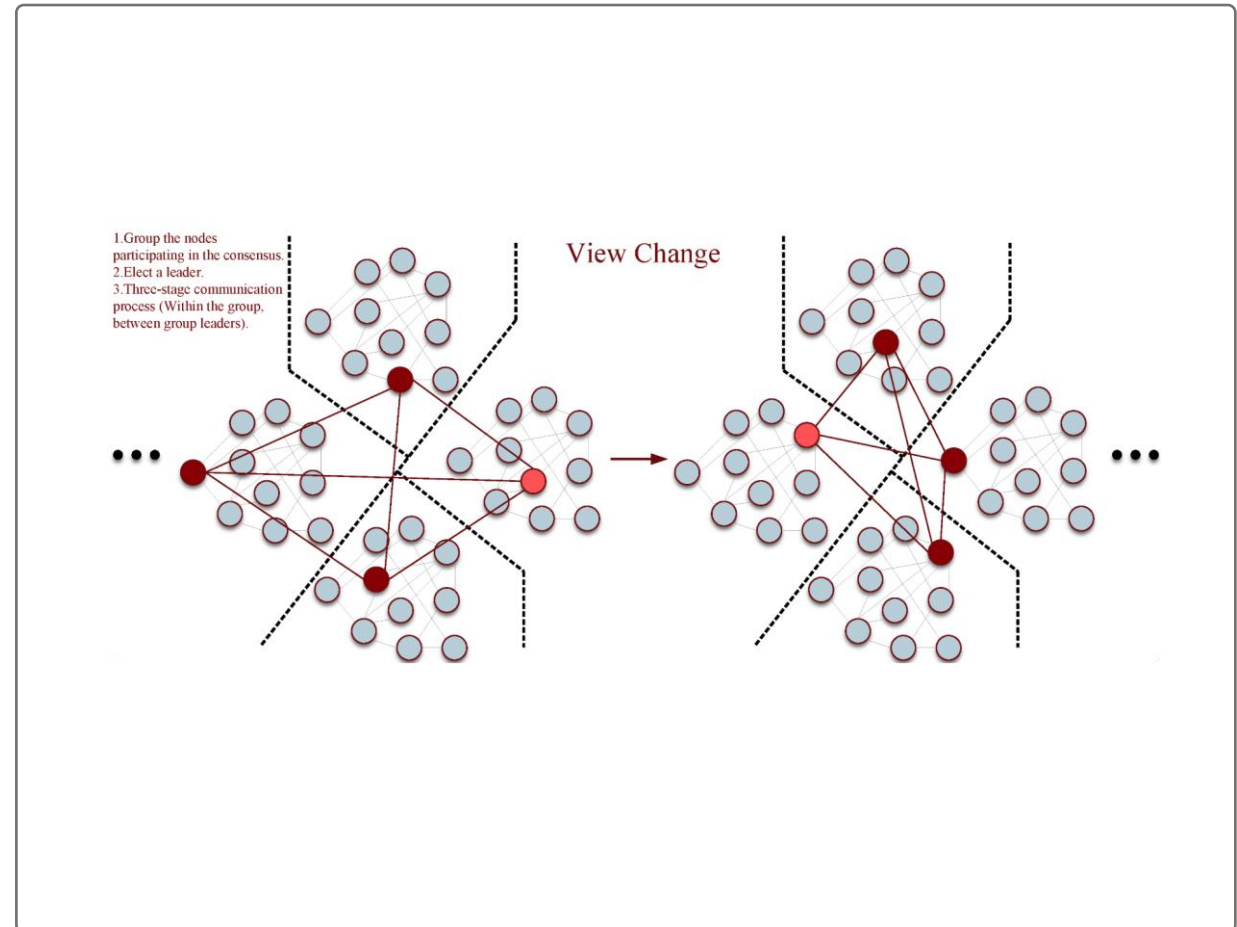
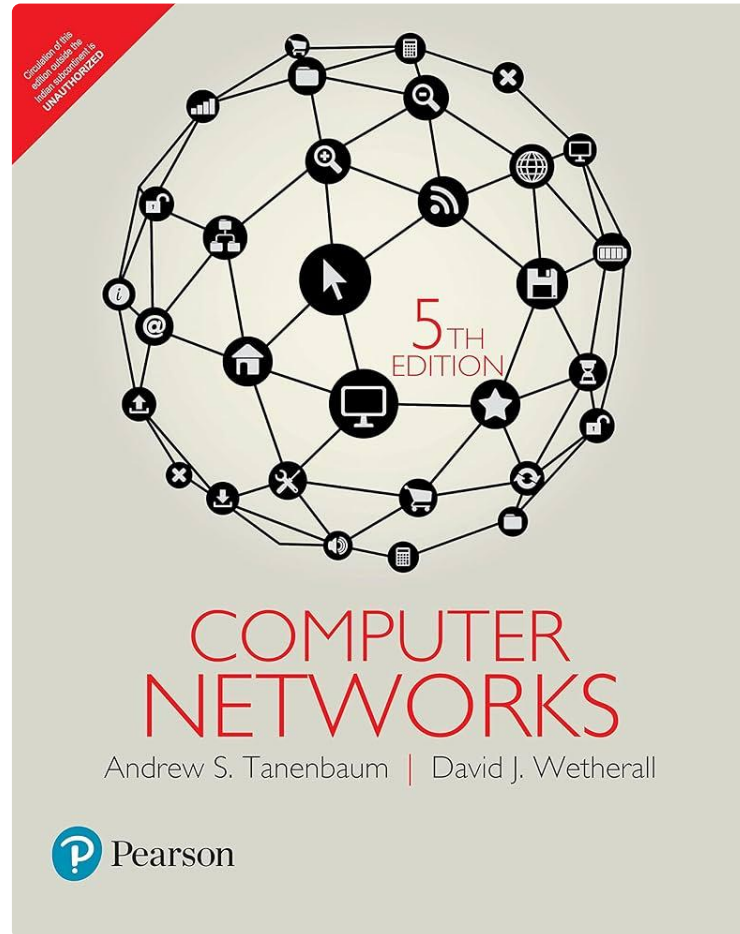


## Lecture 23 — The Byzantine Generals Problem

Jeff Zarnett  
jzarnett@uwaterloo.ca

Department of Electrical and Computer Engineering  
University of Waterloo

April 8, 2020



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

Satoshi Nakamoto  
satoshin@gmx.com  
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 financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network.

The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

distributed  
consensus

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

Satoshi Nakamoto  
satoshin@gmx.com  
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 financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network.

The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. blockchain

2. proof of work









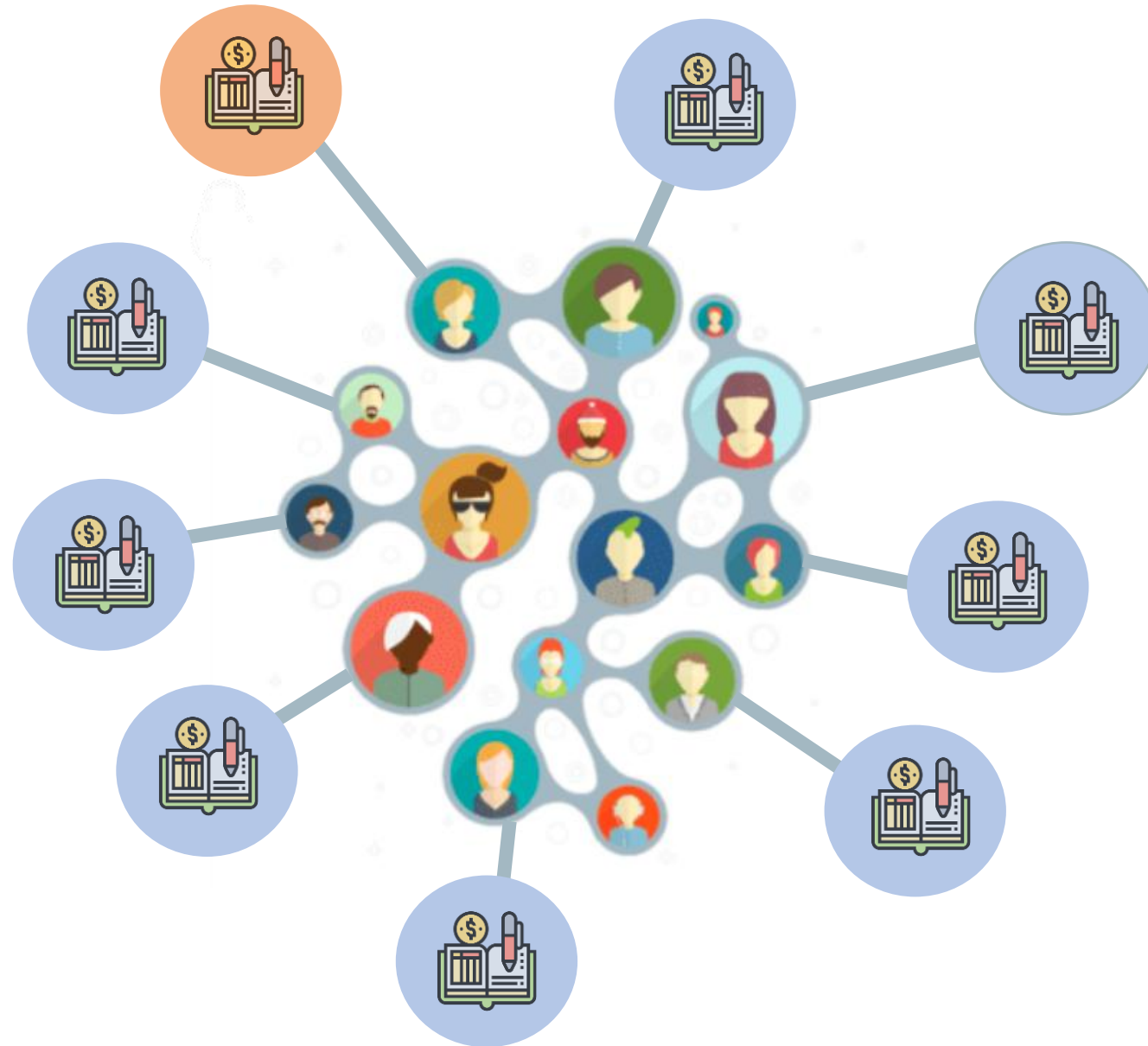


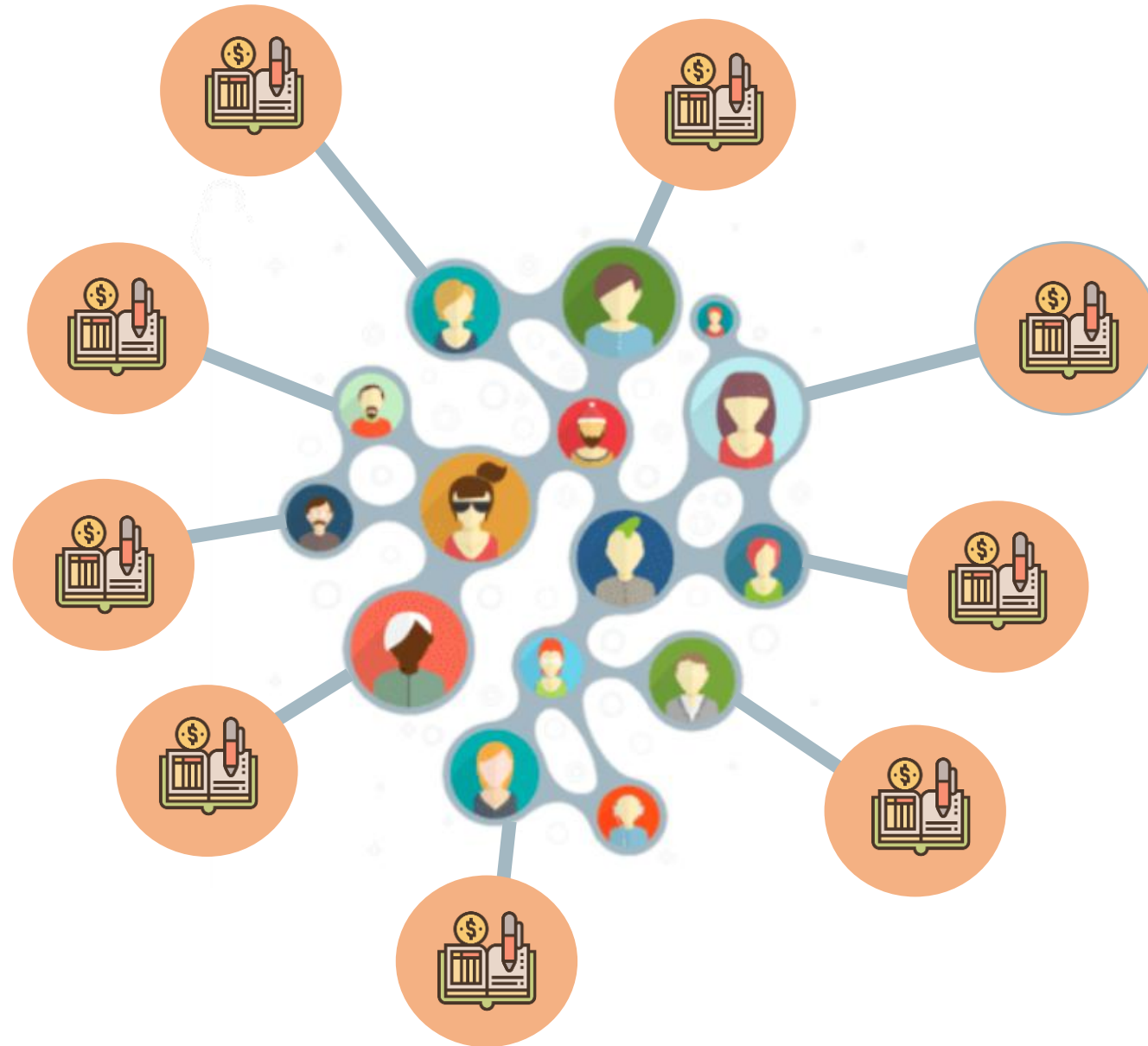












## Bitcoin Whitepaper (p.7)

The receiver generates a new key pair and gives the public key to the sender shortly before signing. This prevents the sender from preparing a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far enough ahead, then executing the transaction at that moment. Once the transaction is sent, the dishonest sender starts working in secret on a parallel chain containing an alternate version of his transaction.

The recipient waits until the transaction has been added to a block and  $z$  blocks have been linked after it. He doesn't know the exact amount of progress the attacker has made, but assuming the honest blocks took the average expected time per block, the attacker's potential progress will be a Poisson distribution with expected value:

$$\lambda = z \frac{q}{p}$$

To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \begin{cases} (q/p)^{(z-k)} & \text{if } k \leq z \\ 1 & \text{if } k > z \end{cases}$$

Rearranging to avoid summing the infinite tail of the distribution...

$$1 - \sum_{k=0}^z \frac{\lambda^k e^{-\lambda}}{k!} (1 - (q/p)^{(z-k)})$$

## Bitcoin Whitepaper (p.7)

The receiver generates a new key pair and gives the public key to the sender shortly before signing. This prevents the sender from preparing a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far enough ahead, then executing the transaction at that moment. Once the transaction is sent, the dishonest sender starts working in secret on a parallel chain containing an alternate version of his transaction.

The recipient waits until the transaction has been added to a block and  $z$  blocks have been linked after it. He doesn't know the exact amount of progress the attacker has made, but assuming the honest blocks took the average expected time per block, the attacker's potential progress will be a Poisson distribution with expected value:

$$\lambda = z \frac{q}{p}$$

To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \begin{cases} (q/p)^{(z-k)} & \text{if } k \leq z \\ 1 & \text{if } k > z \end{cases}$$

Rearranging to avoid summing the infinite tail of the distribution...

$$1 - \sum_{k=0}^z \frac{\lambda^k e^{-\lambda}}{k!} (1 - (q/p)^{(z-k)})$$

## Laws of Physics

### equations of rotation

$$\begin{aligned}\omega &= \omega_0 + \alpha t \\ \theta &= \theta_0 + \omega_0 t + \frac{1}{2} \alpha t^2 \\ \omega^2 &= \omega_0^2 + 2\alpha(\theta - \theta_0) \\ \bar{\omega} &= \frac{1}{2}(\omega + \omega_0)\end{aligned}$$

### rotational work

$$\begin{aligned}W &= \bar{\tau} \Delta \theta \\ W &= \int \tau \cdot d\theta\end{aligned}$$

### universal gravitation

$$\mathbf{F}_g = -\frac{Gm_1 m_2}{r^2} \hat{\mathbf{r}}$$

### orbital speed

$$v = \sqrt{\frac{Gm}{r}}$$

### 2nd law for rotation

$$\begin{aligned}\sum \tau &= I \alpha \\ \sum \tau &= \frac{d\mathbf{L}}{dt}\end{aligned}$$

### rotational power

$$\begin{aligned}P &= \tau \omega \cos \theta \\ P &= \boldsymbol{\tau} \cdot \boldsymbol{\omega}\end{aligned}$$

### gravitational field

$$\mathbf{g} = -\frac{Gm}{r^2} \hat{\mathbf{r}}$$

### escape speed

$$v = \sqrt{\frac{2Gm}{r}}$$

### torque

$$\begin{aligned}\tau &= rF \sin \theta \\ \boldsymbol{\tau} &= \mathbf{r} \times \mathbf{F}\end{aligned}$$

### rotational k.e.

$$K = \frac{1}{2} I \omega^2$$

### gravitational p.e.

$$U_g = -\frac{Gm_1 m_2}{r}$$

### hooke's law

$$\mathbf{F} = -k \Delta \mathbf{x}$$

### moment of inertia

$$\begin{aligned}I &= \sum mr^2 \\ I &= \int r^2 dm\end{aligned}$$

### angular momentum

$$\begin{aligned}L &= mrv \sin \theta \\ \mathbf{L} &= \mathbf{r} \times \mathbf{p} \\ \mathbf{L} &= I \boldsymbol{\omega}\end{aligned}$$

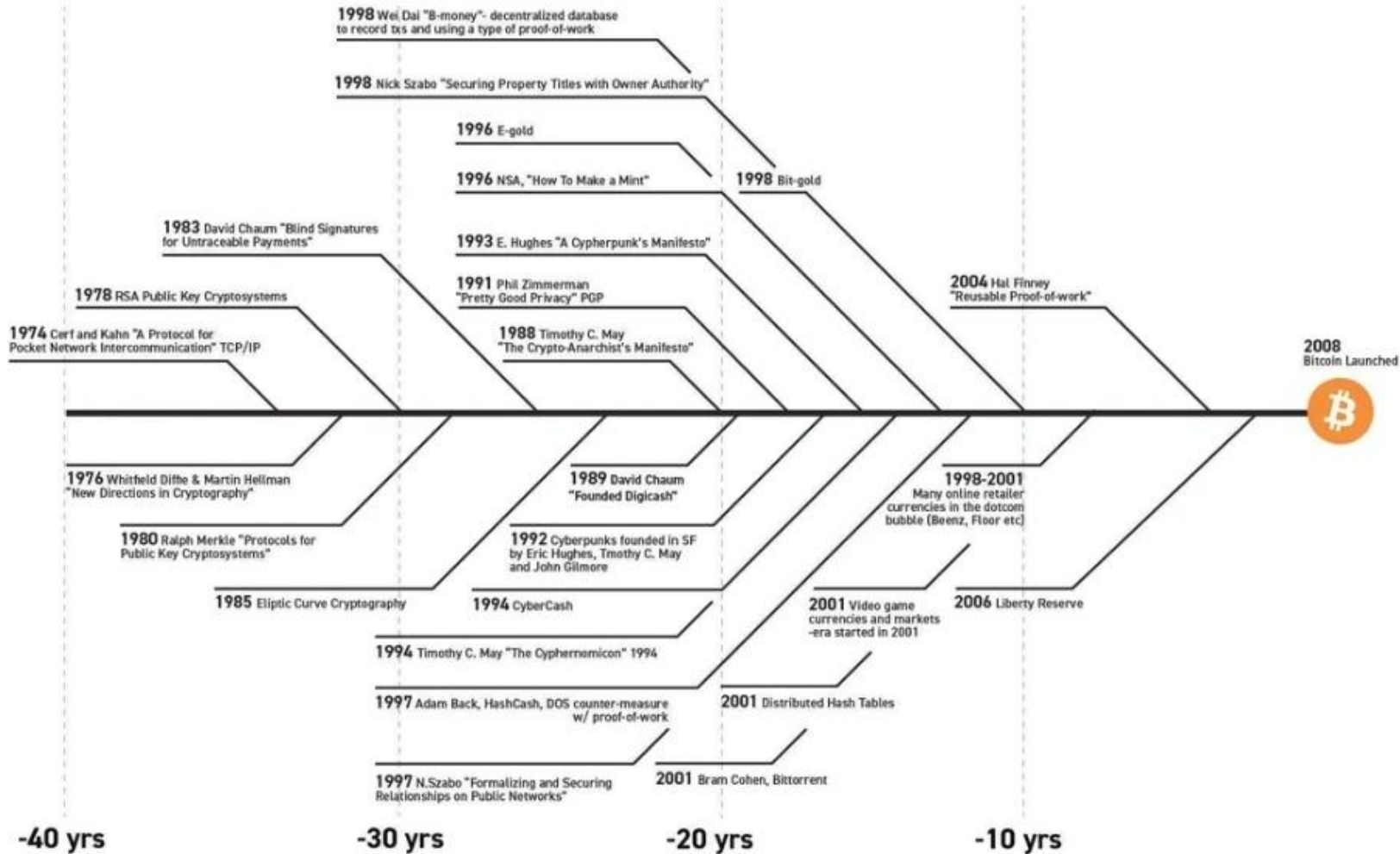
### gravitational potential

$$V_g = -\frac{Gm}{r}$$

### elastic p.e.

$$U_s = \frac{1}{2} k \Delta x^2$$

## Bitcoin prehistory - It's the result of 40 years of research, development and demand



## Bitcoin transactions

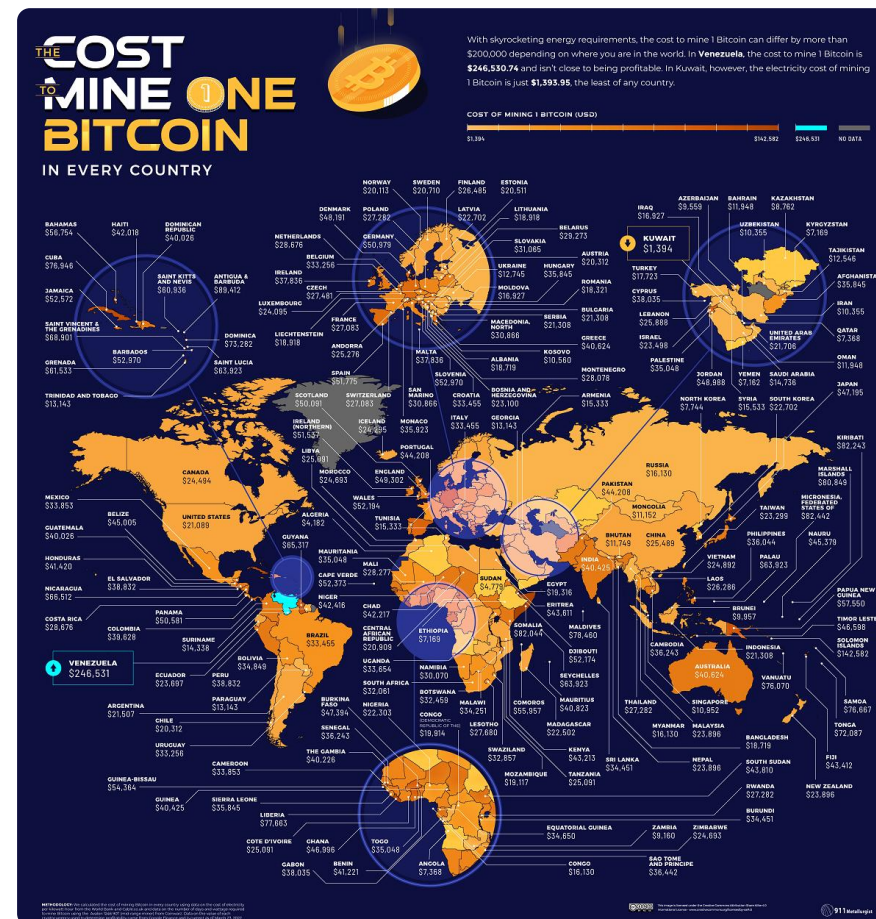
Network	16 yrs
Countries	118
Users	400 million (1:20)
Market cap	\$2 trillion
Transactions	1.2 billion
Transactions / day :	400 000
Value transactions / day:	\$60 billion
Value transactions / min:	\$10 million
Value transactions (all):	\$105 trillion



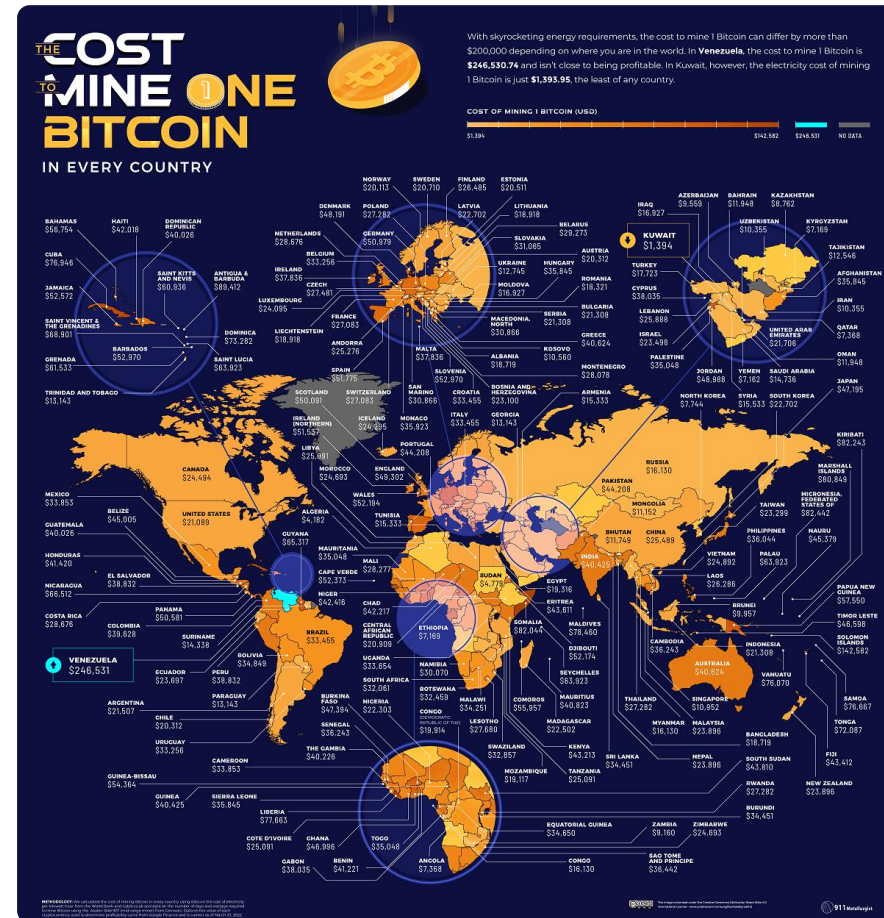




From 2013: "The bitcoin network is now more powerful than the top 500 supercomputers, combined".



# Terawulf Energizes First Nuclear-Powered Bitcoin Mining Facility in the US, Plans to Expand Operations



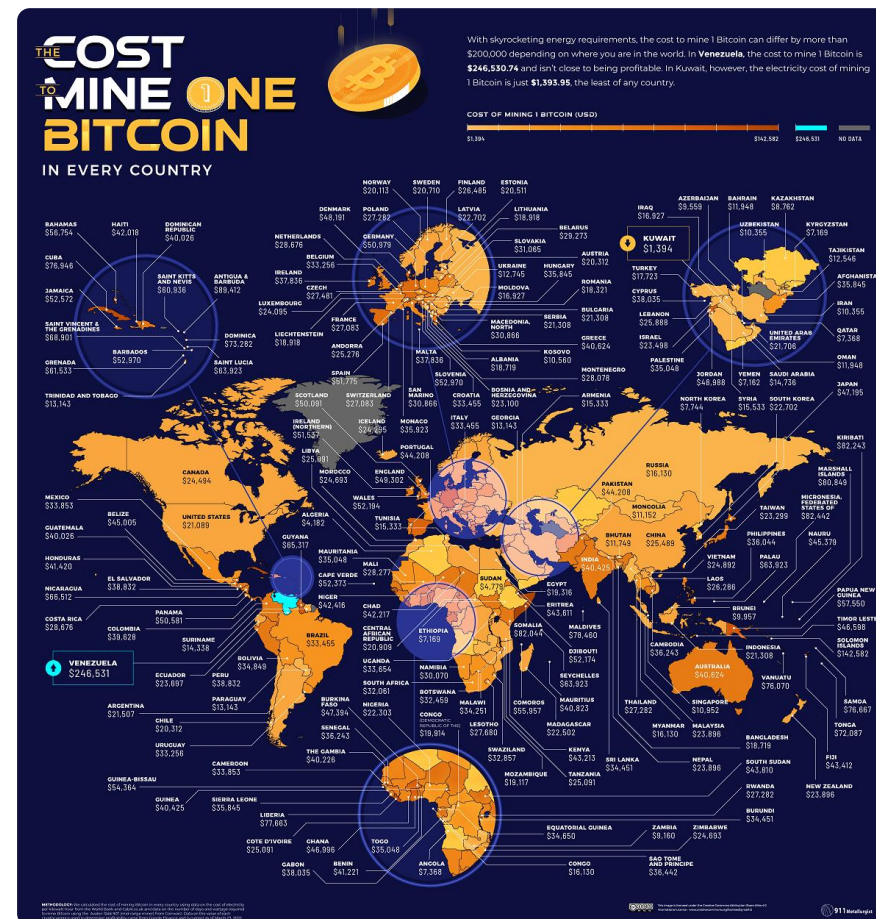


# Volcanoes are being harnessed to power Bitcoin mining in El Salvador in this new pilot project



Published by Danielkenz in NEWS

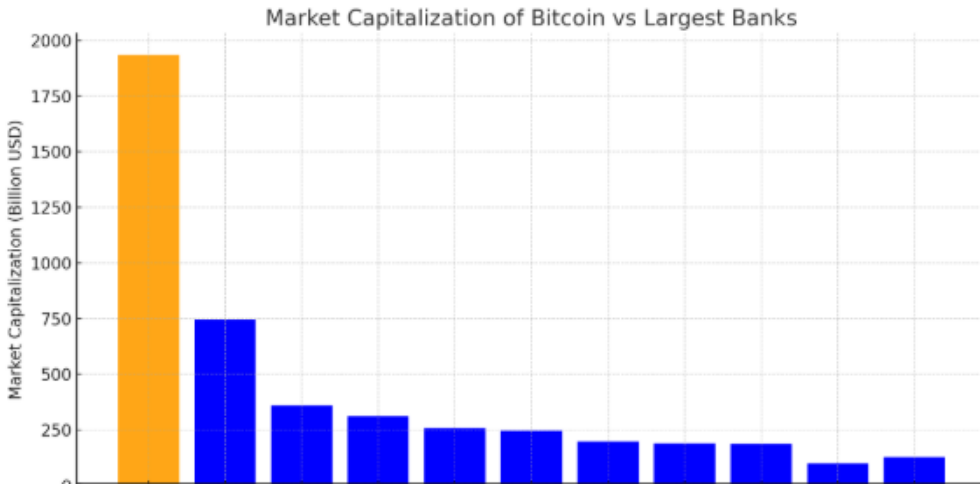
## Blockstream Satellite 2.0 Allows Users to Synchronize Bitcoin Node Without Internet Connection



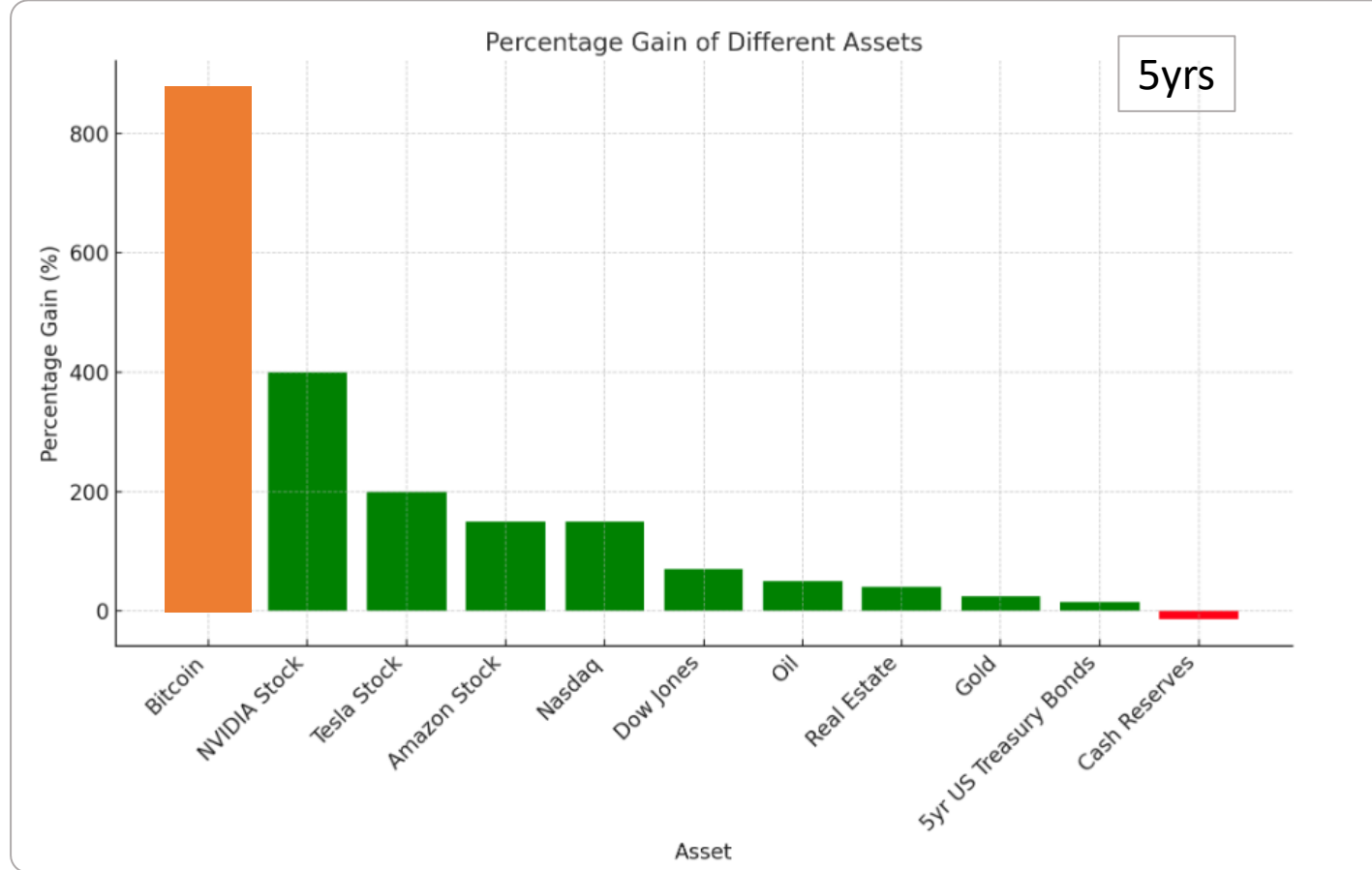
# Bitcoin becomes world's largest bank

 by **Kamsi King** — November 21, 2020

2 min read



JPMorgan Chase & Co.	\$743.74 billion
Bank of America Corp.	\$358.39 billion
Industrial and Commercial Bank of China Ltd.	\$310.34 billion
Wells Fargo & Co.	\$256.34 billion
Agricultural Bank of China	\$244.58 billion
China Construction Bank	\$197.15 billion
Bank of China	\$187.79 billion
HSBC Holdings plc	\$185.83 billion
Citigroup Inc.	\$98.45 billion
Goldman Sachs Group Inc.	\$125.80 billion







BitcoinBadger.net