Guest Lecture: An Introduction to bitcoin

Murch

2015-06-02

Introduction

What is Money?

What is Bitcoin?

History of Bitcoin

Introduction

What is Money?

What is Bitcoin?

History of Bitcoin

Who am I?

Name: Murch

Job: my job

Why here? Because I can’t stop talking and thinking about Bitcoin

Qualification: Spent lots of time reading and writing about Bitcoin

Introduction

What is Money?

What is Bitcoin?

History of Bitcoin

What is money?

Examples for Money?

What is money?

Examples for Money?

Properties of Money?

Definition of Money

Definition

Money is any object or verifiable record that is generally accepted as payment for goods and services and repayment of debts in a given socio-economic context or country.

The main functions of money are distinguished as:

- medium of exchange
- unit of account
- store of value

Definition [en.wikipedia.org/wiki/Money]

Definition of Money

Definition

Money is any object or verifiable record that is generally accepted as payment for goods and services and repayment of debts in a given socio-economic context or country.

The main functions of money are distinguished as:

- medium of exchange
- unit of account
- store of value

Definition [en.wikipedia.org/wiki/Money]

Money is a technology that facilitates trade.

Two Categories of Money

Two Categories of Money

Definition

Commodity Money is based on the inherent value of the exchange medium.

Examples:

Two Categories of Money

Definition

Commodity Money is based on the inherent value of the exchange medium.

Examples: Gold, Shells, Cigarettes, Livestock

Two Categories of Money

Definition

Commodity Money is based on the inherent value of the exchange medium.

Examples: Gold ▲, Shells 🐚, Cigarettes 🚬, Livestock

Definition

Fiat Money is inherently worthless, but derives value from being a promisory note issued by a nation or company.

Examples:

Two Categories of Money

Definition

Commodity Money is based on the inherent value of the exchange medium.

Examples: Gold, Shells, Cigarettes, Livestock

Definition

Fiat Money is inherently worthless, but derives value from being a promisory note issued by a nation or company.

Examples: US Dollar $, Euro €, Bank statement

What shortfalls does Money have?

So, Money is pretty useful, but...

What shortfalls does Money have?

So, Money is pretty useful, but...

What problems can you think of?

Currency is inefficient and slow

- Wire transfers take 2+ days
- Intercontinental wire transfers 7+ days
- Handling cash is inconvenient

Currency is expensive to maintain

- Cash has to be counted and transported
- Bills have to be replaced every 2-5 years
- After time coins’ value lower than production cost

Digital currency lacks privacy

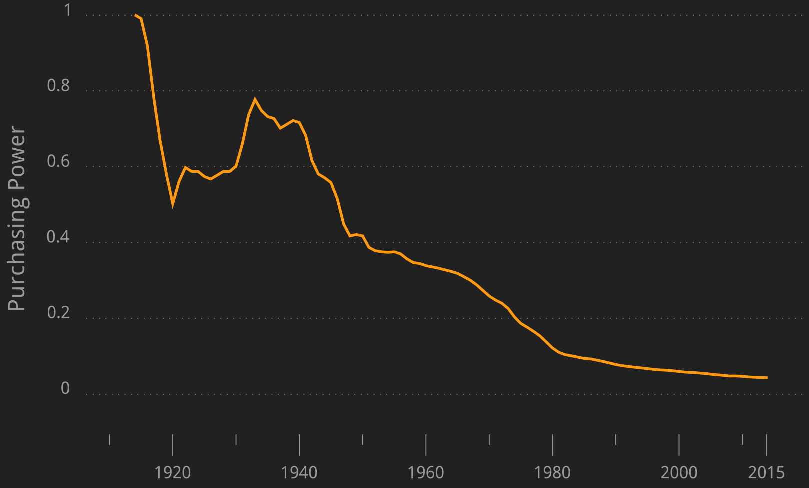
- Bank tracks your payments
- Credit Card Companies track your payments
- Government tracks your payments

Only cash is private.

Inflation

- Goverments set money policy
- Banks create additional money

Loss of Purchasing Power



Data: U.S. Bureau of Labor Statistics, Detailed CPI report 2015-04

Lack of Control

- Transfer and Storage controlled by third parties
- Limited Freedom to choose recipients
- Counter-party risk

Introduction

What is Money?

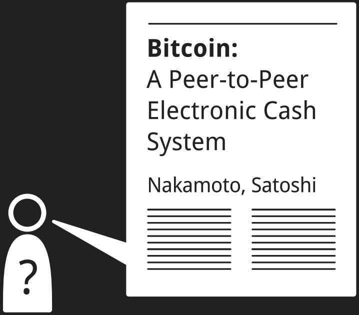
What is Bitcoin?

History of Bitcoin

What is the connection to Bitcoin?

Bitcoin is a new payment system designed to address these problems.

Enter Satoshi Nakamoto



Bitcoin:
A Peer-to-Peer Electronic Cash System

Nakamoto, Satoshi

Bitcoin in a nutshell

- New way to send payments via internet

Bitcoin in a nutshell

- New way to send payments via internet
- Agreement to treat digital tokens named bitcoins as money

Bitcoin in a nutshell

- New way to send payments via internet
- Agreement to treat digital tokens named bitcoins as money
- Digital cash: irreversible and no middlemen

Bitcoin in a nutshell

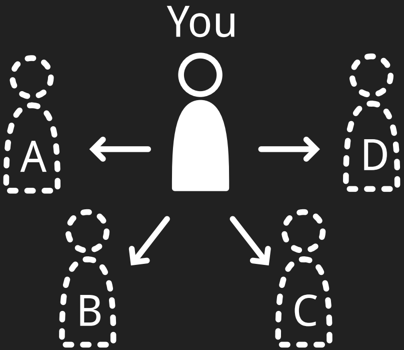
- New way to send payments via internet
- Agreement to treat digital tokens named bitcoins as money
- Digital cash: irreversible and no middlemen
- All transactions are publicly visible

Bitcoin in a nutshell

- New way to send payments via internet
- Agreement to treat digital tokens named bitcoins as money
- Digital cash: irreversible and no middlemen
- All transactions are publicly visible
- Users remain private

Privacy in Bitcoin

Privacy in Bitcoin

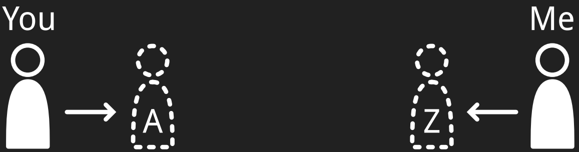


Spending bitcoins

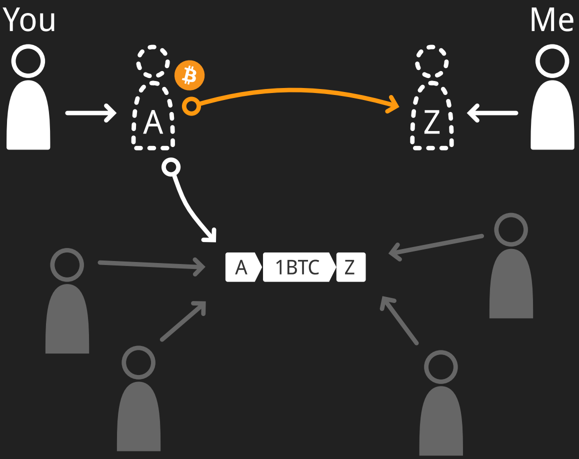
You

Me

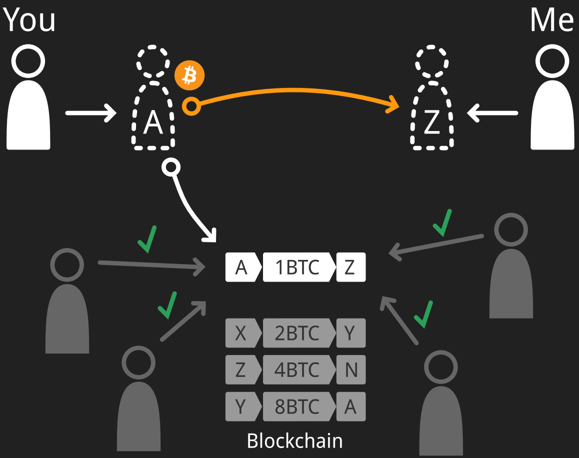
Spending bitcoins



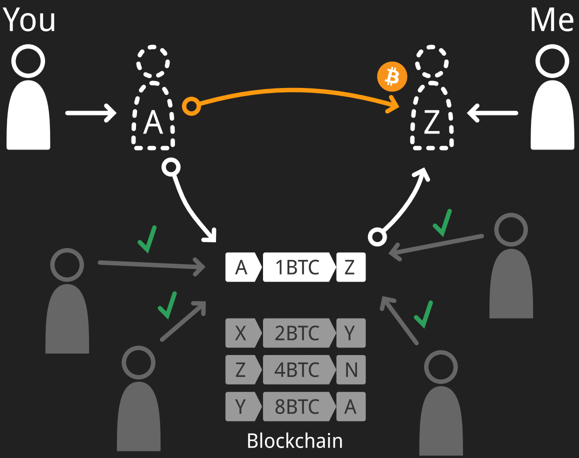
Spending bitcoins



Spending bitcoins



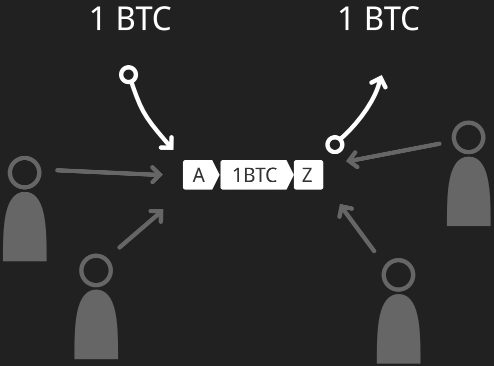
Spending bitcoins



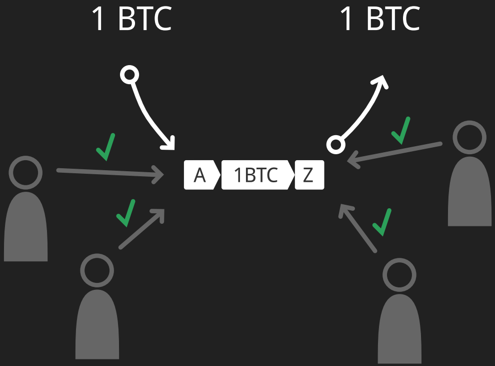
Let’s see this live

Address: 1LNHme4E5mrhUk4tbLpb75Q5aq81F8Mb95

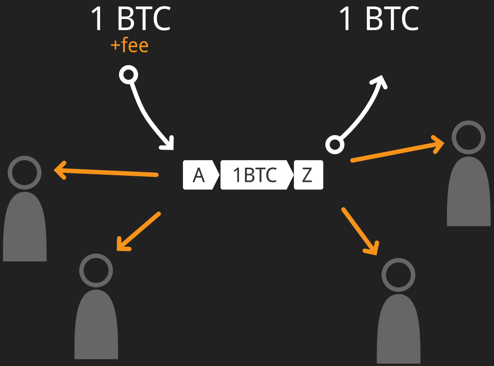
Who pays for Bitcoin?



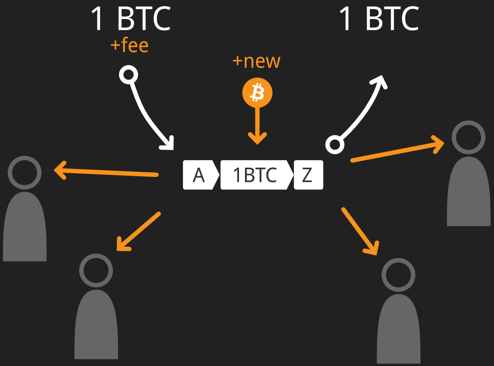
Who pays for Bitcoin?



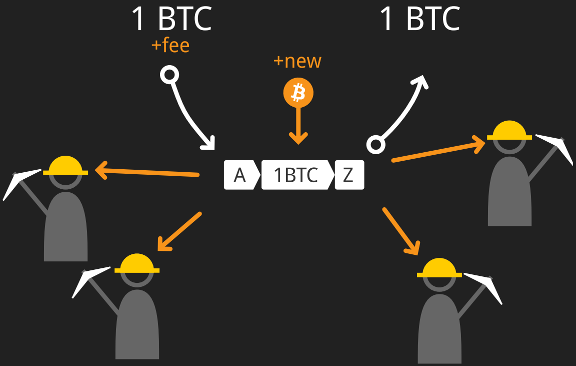
Who pays for Bitcoin?



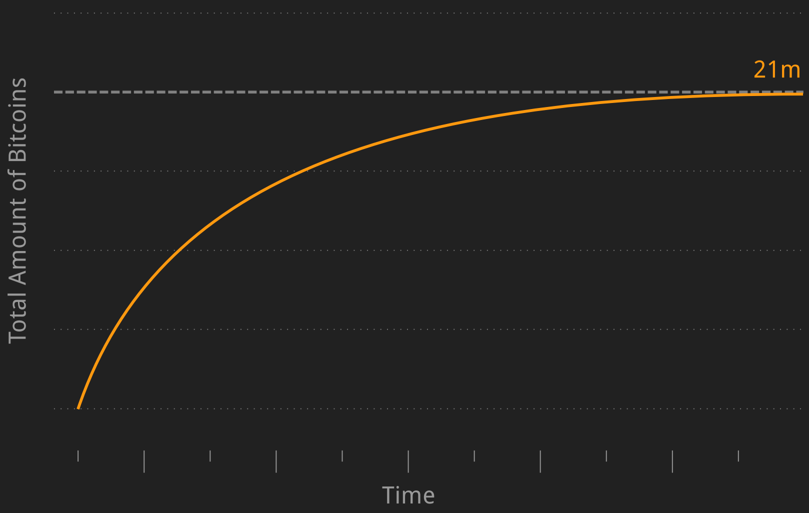
Who pays for Bitcoin?



Who pays for Bitcoin?



Bitcoin is a Limited Resource



Getting started with Bitcoin

Getting started with Bitcoin

1. Inform yourself: bitcoin.org

Getting started with Bitcoin

1. Inform yourself: bitcoin.org
2. Get a wallet

Desktop	MultiBit
Android	Bitcoin Wallet
iOS	breadwallet

Getting started with Bitcoin

1. Inform yourself: bitcoin.org
2. Get a wallet

Desktop	MultiBit
Android	Bitcoin Wallet
iOS	breadwallet

3. Get bitcoins

Getting started with Bitcoin

1. Inform yourself: bitcoin.org
2. Get a wallet

Desktop	MultiBit
Android	Bitcoin Wallet
iOS	breadwallet

3. Get bitcoins
4. Spend bitcoins

That’s how Bitcoin works

Any questions so far?

Review: Definition of Money

Definition

Money is any object or verifiable record that is generally accepted as payment for goods and services and repayment of debts in a given socio-economic context or country.

The main functions of money are distinguished as:

- medium of exchange
- unit of account
- store of value

Definition [en.wikipedia.org/wiki/Money]

Is Bitcoin Money?

- Verifiable Record
- Acceptance
- Medium of Exchange
- Unit of Account
- Store of Value

Is Bitcoin Money?

- Verifiable Record
- Acceptance
- Medium of Exchange
- Unit of Account
- Store of Value

Bitcoin is not *legal tender*, but a complementary currency. It shares aspects of both *commodity money* and *fiat money*.

Is Bitcoin Money?

- Verifiable Record ✓
- Acceptance
- Medium of Exchange
- Unit of Account
- Store of Value

Bitcoin is not *legal tender*, but a complementary currency. It shares aspects of both *commodity money* and *fiat money*.

Is Bitcoin Money?

- Verifiable Record ✓
- Acceptance ✓/ ✗
- Medium of Exchange
- Unit of Account
- Store of Value

Bitcoin is not *legal tender*, but a complementary currency. It shares aspects of both *commodity money* and *fiat money*.

Is Bitcoin Money?

- Verifiable Record ✓
- Acceptance ✓/ ✗
- Medium of Exchange ✓
- Unit of Account
- Store of Value

Bitcoin is not *legal tender*, but a complementary currency. It shares aspects of both *commodity money* and *fiat money*.

Is Bitcoin Money?

- Verifiable Record ✓
- Acceptance ✓/ ✗
- Medium of Exchange ✓
- Unit of Account ✓
- Store of Value

Bitcoin is not *legal tender*, but a complementary currency. It shares aspects of both *commodity money* and *fiat money*.

Is Bitcoin Money?

- Verifiable Record ✓
- Acceptance ✓/ ✗
- Medium of Exchange ✓
- Unit of Account ✓
- Store of Value ✓/ ✗

Bitcoin is not *legal tender*, but a complementary currency. It shares aspects of both *commodity money* and *fiat money*.

Does Bitcoin solve other Moneys’ shortfalls?

Issue	Bitcoin
Slow	Fast
Expensive to maintain	Network pays for itself
Lack of Privacy	Private/Pseudonymous
Inflated	Limited Supply
Lack of Control	Puts user in control

What makes bitcoins valuable?

Bitcoin is a limited resource and useful/convenient.

What are the downsides to Bitcoin?

What are the downsides to Bitcoin?

- Responsibility

What are the downsides to Bitcoin?

- Responsibility
- Limited Acceptance

What are the downsides to Bitcoin?

- Responsibility
- Limited Acceptance
- Legal status to be determined

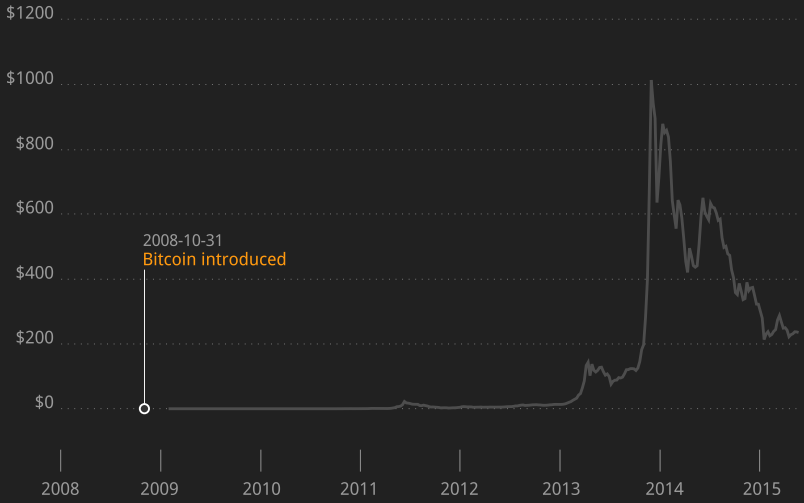
What are the downsides to Bitcoin?

- Responsibility
- Limited Acceptance
- Legal status to be determined
- Volatility and no inherent value

What are the downsides to Bitcoin?

- Responsibility
- Limited Acceptance
- Legal status to be determined
- Volatility and no inherent value
- Reputation

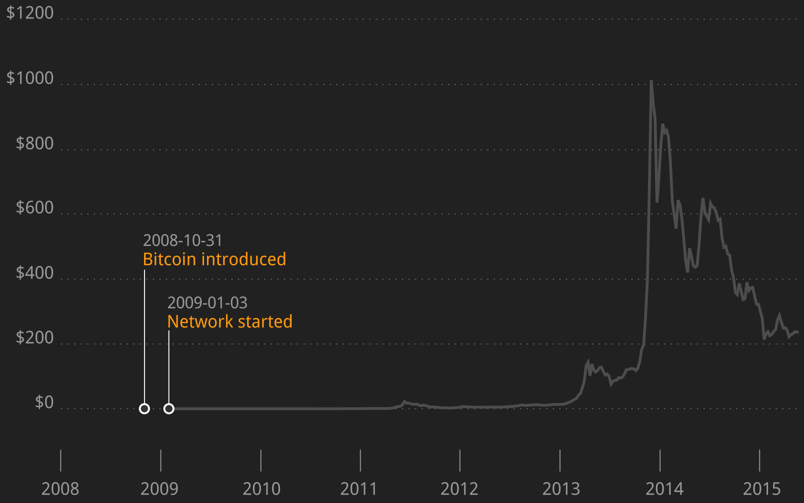
A Brief History of Bitcoin



2008-10-31
Bitcoin introduced

Marketdata: [CoinDesk.com] | Events: [HistoryOfBitcoin.org]

A Brief History of Bitcoin

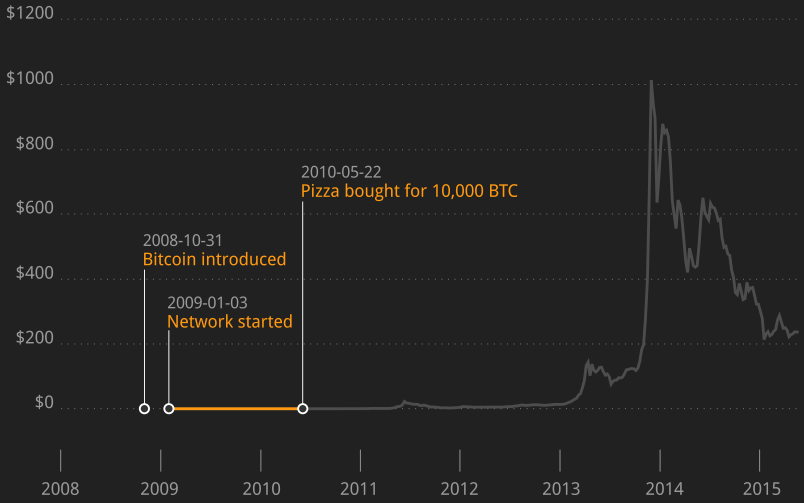


2008-10-31
Bitcoin introduced

2009-01-03
Network started

Marketdata: [CoinDesk.com] | Events: [HistoryOfBitcoin.org]

A Brief History of Bitcoin



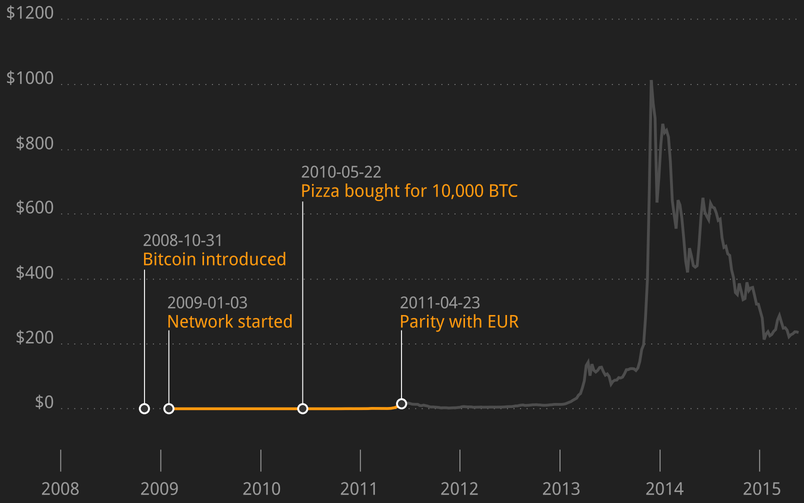
2010-05-22
Pizza bought for 10,000 BTC

2008-10-31
Bitcoin introduced

2009-01-03
Network started

Marketdata: [CoinDesk.com] | Events: [HistoryOfBitcoin.org]

A Brief History of Bitcoin



2008-10-31
Bitcoin introduced

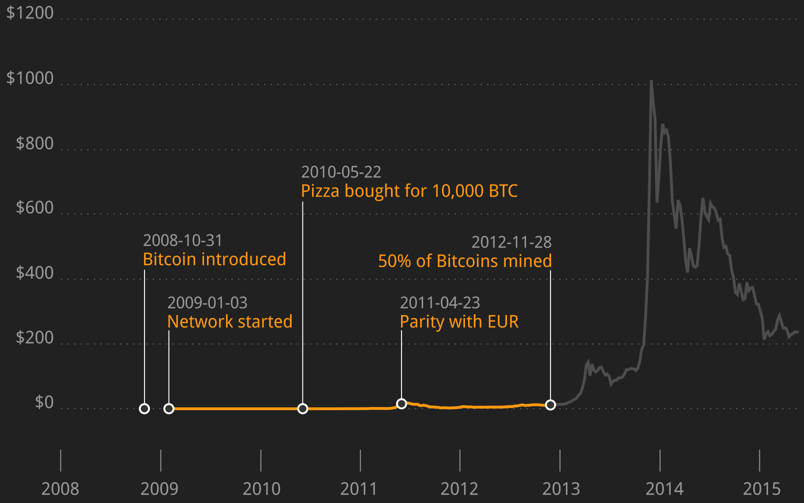
2009-01-03
Network started

2010-05-22
Pizza bought for 10,000 BTC

2011-04-23
Parity with EUR

Marketdata: [CoinDesk.com] | Events: [HistoryOfBitcoin.org]

A Brief History of Bitcoin



2008-10-31
Bitcoin introduced

2009-01-03
Network started

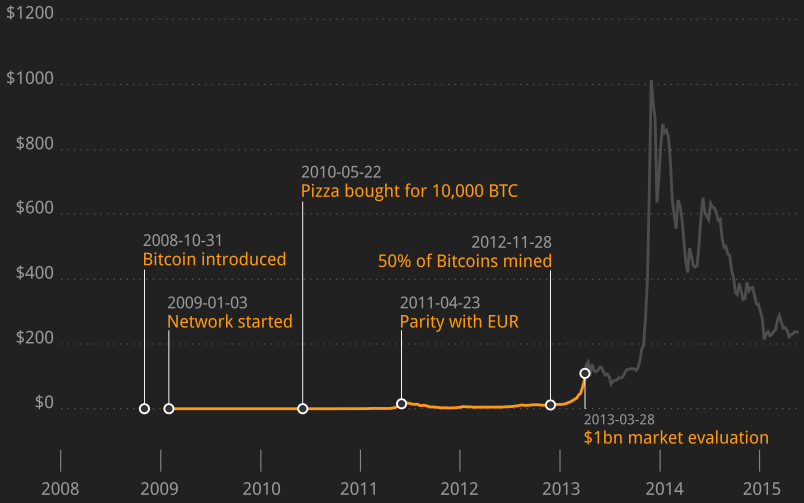
2010-05-22
Pizza bought for 10,000 BTC

2011-04-23
Parity with EUR

2012-11-28
50% of Bitcoins mined

Marketdata: [CoinDesk.com] | Events: [HistoryOfBitcoin.org]

A Brief History of Bitcoin



2008-10-31
Bitcoin introduced

2009-01-03
Network started

2010-05-22
Pizza bought for 10,000 BTC

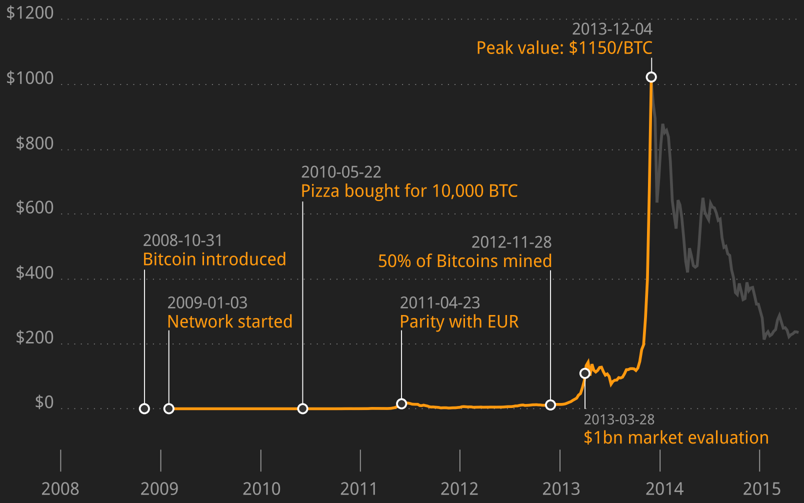
2011-04-23
Parity with EUR

2012-11-28
50% of Bitcoins mined

2013-03-28
$1bn market evaluation

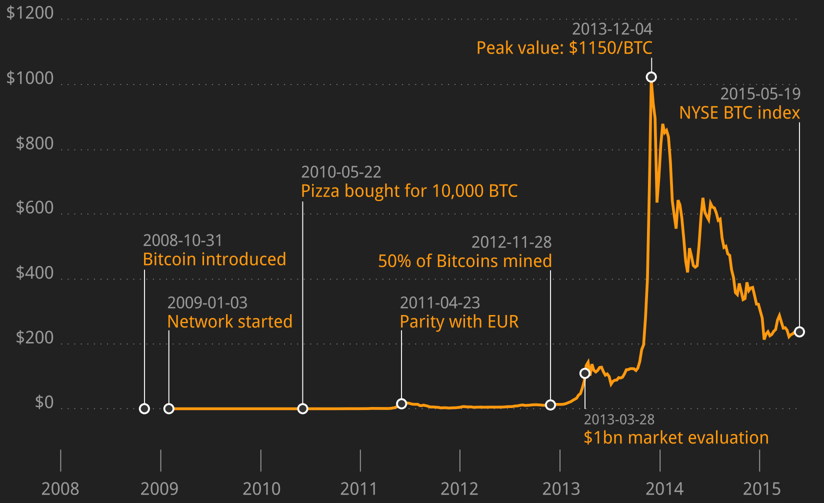
Marketdata: [CoinDesk.com] | Events: [HistoryOfBitcoin.org]

A Brief History of Bitcoin



Marketdata: [CoinDesk.com] | Events: [HistoryOfBitcoin.org]

A Brief History of Bitcoin



Marketdata: [CoinDesk.com] | Events: [HistoryOfBitcoin.org]

Bitcoin Today

Bitcoin Today

- Still experimental

Bitcoin Today

- Still experimental
- Estimated Userbase: $\sim$500.000 - 2.000.000

Bitcoin Today

- Still experimental
- Estimated Userbase: ∼500.000 - 2.000.000
- Transactions per day: ∼110.000

Bitcoin Today

- Still experimental
- Estimated Userbase: $\sim$500.000 - 2.000.000
- Transactions per day: $\sim$110.000
- Accepted by 100.000+ merchants, including Microsoft, Dell, Lieferservice.de

Bitcoin Today

- Still experimental
- Estimated Userbase: $\sim$500.000 - 2.000.000
- Transactions per day: $\sim$110.000
- Accepted by 100.000+ merchants, including Microsoft, Dell, Lieferservice.de
- Regulation in progress

Bitcoin Today

- Still experimental
- Estimated Userbase: $\sim$500.000 - 2.000.000
- Transactions per day: $\sim$110.000
- Accepted by 100.000+ merchants, including Microsoft, Dell, Lieferservice.de
- Regulation in progress
- Altcoins: $\sim$725, e.g. , , , ,

Thank you for your attention

Thank you for your attention

Any more questions?

Byzantine Generals’ Problem

Bitcoin solves the *Byzantine Generals’ Problem*: How to achieve consensus in a distributed network with potential adversaries.

Alternative Bitcoin Definition

Definition

Bitcoin is a payment protocol that provides a public ledger maintained by a decentral peer-to-peer network secured with cryptographic proof.

Alternative Bitcoin Definition

Definition

Bitcoin is a payment protocol that provides a public ledger maintained by a decentral peer-to-peer network secured with cryptographic proof.

... quite a mouthful, huh?

Alternative Bitcoin Definition

Definition

Bitcoin is a payment protocol that provides a public ledger maintained by a decentral peer-to-peer network secured with cryptographic proof.

What is most important about that is:

- It’s open-source software.

Alternative Bitcoin Definition

Definition

Bitcoin is a payment protocol that provides a public ledger maintained by a decentral peer-to-peer network secured with cryptographic proof.

What is most important about that is:

- It’s open-source software.
- Very little trust required in other participants of the network.

Alternative Bitcoin Definition

Definition

Bitcoin is a payment protocol that provides a public ledger maintained by a decentral peer-to-peer network secured with cryptographic proof.

What is most important about that is:

- It’s open-source software.
- Very little trust required in other participants of the network.
- No one entity controls the network.

Alternative Bitcoin Definition

Definition

Bitcoin is a payment protocol that provides a public ledger maintained by a decentral peer-to-peer network secured with cryptographic proof.

What is most important about that is:

- It’s open-source software.
- Very little trust required in other participants of the network.
- No one entity controls the network.
- Any user can send money directly to peers.

Alternative Bitcoin Definition

Definition

Bitcoin is a payment protocol that provides a public ledger maintained by a decentral peer-to-peer network secured with cryptographic proof.

What is most important about that is:

- It's open-source software.
- Very little trust required in other participants of the network.
- No one entity controls the network.
- Any user can send money directly to peers.
- Solves the double-spend problem, and counterfeiting.

What makes bitcoins valuable?

Bitcoin recombines some of the best features of *Cash*, *Credit Cards*, and *Wire transfers*.

What makes bitcoins valuable?

Bitcoin recombines some of the best features of *Cash*, *Credit Cards*, and *Wire transfers*.

Global Anyone with an internet connection can use it.

What makes bitcoins valuable?

Bitcoin recombines some of the best features of *Cash*, *Credit Cards*, and *Wire transfers*.

- Global: Anyone with an internet connection can use it.
- Fast: Visible within seconds, confirmed after minutes.

What makes bitcoins valuable?

Bitcoin recombines some of the best features of *Cash*, *Credit Cards*, and *Wire transfers*.

Global Anyone with an internet connection can use it.

Fast Visible within seconds, confirmed after minutes.

Secure Doesn’t require you to reveal your secret to spend money.

What makes bitcoins valuable?

Bitcoin recombines some of the best features of *Cash*, *Credit Cards*, and *Wire transfers*.

Global Anyone with an internet connection can use it.

Fast Visible within seconds, confirmed after minutes.

Secure Doesn’t require you to reveal your secret to spend money.

Scarce Limited to 21 Million units.

What makes bitcoins valuable?

Bitcoin recombines some of the best features of *Cash*, *Credit Cards*, and *Wire transfers*.

Global Anyone with an internet connection can use it.

Fast Visible within seconds, confirmed after minutes.

Secure Doesn’t require you to reveal your secret to spend money.

Scarce Limited to 21 Million units.

Peer-to-peer Payments go directly from user to user.

What makes bitcoins valuable?

Bitcoin recombines some of the best features of *Cash*, *Credit Cards*, and *Wire transfers*.

Global Anyone with an internet connection can use it.

Fast Visible within seconds, confirmed after minutes.

Secure Doesn’t require you to reveal your secret to spend money.

Scarce Limited to 21 Million units.

Peer-to-peer Payments go directly from user to user.

Cheap Send any amount of money for less than one cent.

What makes bitcoins valuable?

Bitcoin recombines some of the best features of *Cash*, *Credit Cards*, and *Wire transfers*.

Global Anyone with an internet connection can use it.

Fast Visible within seconds, confirmed after minutes.

Secure Doesn’t require you to reveal your secret to spend money.

Scarce Limited to 21 Million units.

Peer-to-peer Payments go directly from user to user.

Cheap Send any amount of money for less than one cent.

Open No consent required to use it.

What makes bitcoins valuable?

Bitcoin recombines some of the best features of *Cash*, *Credit Cards*, and *Wire transfers*.

Global Anyone with an internet connection can use it.

Fast Visible within seconds, confirmed after minutes.

Secure Doesn't require you to reveal your secret to spend money.

Scarce Limited to 21 Million units.

Peer-to-peer Payments go directly from user to user.

Cheap Send any amount of money for less than one cent.

Open No consent required to use it.

Conclusion

As the Bitcoin network is useful, but not owned by any

Detailed Comparison to other forms of Money

Transaction Cost	Precious Metals	Fiat Currencies	Bitcoin
Storage	0.15% to 1% p.a.	Subsidized by FRB	Free
Transportation	Expensive	Inconvenient	Easy & Free
Fiduciary Media	Inevitable	Inherent	Impossible
Recordkeeping	Manual	Mostly manual	Automatic
Issuance	Mining	Politics	Algorithm
Payment Clearing	Expensive	Centralized	Cheap & Distributed
Scarcity	High	Arbitrary	Fixed - 21 million
Authentication	Expensive Assay	Trust counterparty	Built-in
Security	Physical	Institutional	Cryptographic

Addresses in Detail

Transactions in Detail

Blocks in Detail

Private Keys in Detail

Transactions in Detail

Blockchain in Detail

Who controls Bitcoin?

Is Bitcoin a Pyramid Scheme?

How is Scarcity Implemented?

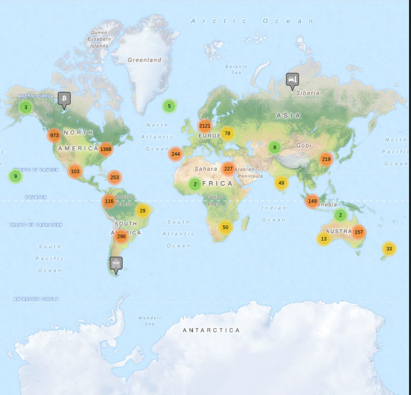
Why can't bitcoins be counterfeited?

Who is *Satoshi Nakamoto*?

Hardly any personal information available.
Commits during US east coast working times
used British and American spelling at times
Probably not a cryptographer by trade -> source
Combination of Economics, Computer Science,
Programming, Ideology

Where can one spend Bitcoin?

A range of internet merchants already accepts Bitcoin such as: Microsoft, Dell, Overstock,...
Brick-and-mortar store adoption is coming more slowly:



How does one obtain Bitcoin?

- Buy them on Exchanges, such as Bitstamp.com
- Offer goods or services for Bitcoin
- Mining (only on industrial scale today)

Is Bitcoin anonymous?

No. Bitcoin is private, but completely transparent. Therefore, it is not anonymous per se, but rather pseudonymous.

Strategies to maintain privacy in the network:

- Use every address only once, i.e. especially don't get your salary always paid to the same address.
- Don't spend transaction outputs together from accounts that should not be linked.

Nodes don't have identities. Addresses can be changed frequently, mining is performed almost independently of either of those.

Identity in the Bitcoin Network

- Addresses stand in as *Identities* in the Bitcoin network.
- Only the owner can speak for the identity as only the owner of the secret key can validly sign messages

Why is it easy to verify blocks, but hard to find them?

- To find a block one has to find a combination of the block content and a random value which maps to a subset of the possible hashoutputs

Double-Spending

Double-Spending: How do you know that you are the sole owner of a digital good? I.e. images are easy to copy and distribute. The problem is to create a distributed consensus.

Bitcoin solves the Double-Spending problem. This happens by publishing updates to the balances in the network through a blockchain. The blockchain is immutable, because it is secured by Proof of Work.

What is a Cryptographic Hashfunction?

How does Bitcoin achieve decentralization?

Who maintains the ledger? Who has authority over transaction validity? Who creates new bitcoins? Who determines changes in the rules of the Bitcoin systems? Why are Bitcoins valuable?

Distributed Consensus

Goal

When the protocol terminates, all correct nodes decide on the same value.

Challenges

- Malicious Nodes
- Latency and no "global time"
- Byzantine generals problem
- not all nodes interconnected / online at all times

Solution

Embraces randomness
Incentivizes good behavior