An introduction to Bitcoin

Ricardo Pérez-Marco (CNRS, IMJ-PRG, Paris 7)

Quantitative Methods for Financial Regulation

Stony Brook

September 10, 2016

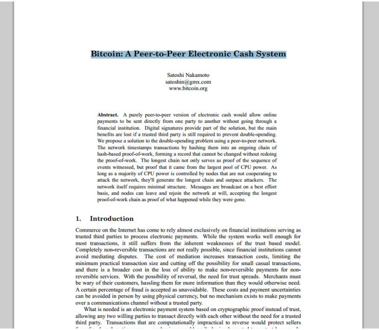
(*Bitcoin and Decentralized Trust Protocols*, Newsletter of the European Math. Soc., 100, June 2016. ArXiv 1601.05254)

An introduction to Bitcoin

Bitcoin paper

S. Nakamoto, November 1st 2008,

"Bitcoin: A peer-to-peer electronic cash system"



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. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers

Transparency Theorem

- Bitcoin is an electronic currency modelled by gold.

Transparency Theorem

- Bitcoin is an electronic currency modelled by gold.
- Bitcoin does not depend on any central authority.

Transparency Theorem

- Bitcoin is an electronic currency modelled by gold.
- Bitcoin does not depend on any central authority.
- Bitcoin protocol runs on open software.

Transparency Theorem

- Bitcoin is an electronic currency modelled by gold.
- Bitcoin does not depend on any central authority.
- Bitcoin protocol runs on open software.
- To avoid the **"double spend problem"** Bitcoin relies on a public ledger. This is general and necessary:

Theorem

Transparency Theorem: *An electronic decentralized currency must rely on a public ledger.*

The blockchain

- The public ledger is an incorruptible public database of all transactions called "**the blockchain**".

The blockchain

- The public ledger is an incorruptible public database of all transactions called "**the blockchain**".
- Anyone can write in the blockchain.

The blockchain

- The public ledger is an incorruptible public database of all transactions called "**the blockchain**".
- Anyone can write in the blockchain.
- Anyone can have a copy of the blockchain.

The blockchain

- The public ledger is an incorruptible public database of all transactions called “**the blockchain**”.
- Anyone can write in the blockchain.
- Anyone can have a copy of the blockchain.
- The blockchain is composed by a chronological sequence of cryptological chained blocks.

The blockchain

- The public ledger is an incorruptible public database of all transactions called **“the blockchain”**.
- Anyone can write in the blockchain.
- Anyone can have a copy of the blockchain.
- The blockchain is composed by a chronological sequence of cryptological chained blocks.
- Each block contains a set of transactions.

The blockchain

- The public ledger is an incorruptible public database of all transactions called "**the blockchain**".
- Anyone can write in the blockchain.
- Anyone can have a copy of the blockchain.
- The blockchain is composed by a chronological sequence of cryptological chained blocks.
- Each block contains a set of transactions.
- Each new block is generated in about 10 minutes.

The blockchain

- The public ledger is an incorruptible public database of all transactions called "**the blockchain**".
- Anyone can write in the blockchain.
- Anyone can have a copy of the blockchain.
- The blockchain is composed by a chronological sequence of cryptological chained blocks.
- Each block contains a set of transactions.
- Each new block is generated in about 10 minutes.
- The blocks are generated by "miners" that validate current transactions.

The Trust Machine

- The core of the Bitcoin protocol is the algorithm to ensure that this database cannot be forged.

The Trust Machine

- The core of the Bitcoin protocol is the algorithm to ensure that this database cannot be forged.
- The mechanism of consensus: "The trust machine".

Nodes

- The Bitcoin Network is composed by nodes that communicate with each other.

Nodes

- The Bitcoin Network is composed by nodes that communicate with each other.
- Nodes check and broadcast transactions.

Nodes

- The Bitcoin Network is composed by nodes that communicate with each other.
- Nodes check and broadcast transactions.
- Some nodes are miners that validate transactions.

Nodes

- The Bitcoin Network is composed by nodes that communicate with each other.
- Nodes check and broadcast transactions.
- Some nodes are miners that validate transactions.
- Anyone can join and participate in the network.

Nodes

- The Bitcoin Network is composed by nodes that communicate with each other.
- Nodes check and broadcast transactions.
- Some nodes are miners that validate transactions.
- Anyone can join and participate in the network.
- To avoid Sybil attacks a “Proof of Work” (PoW) for miners is required.

Nodes

- The Bitcoin Network is composed by nodes that communicate with each other.
- Nodes check and broadcast transactions.
- Some nodes are miners that validate transactions.
- Anyone can join and participate in the network.
- To avoid Sybil attacks a “Proof of Work” (PoW) for miners is required.

Reaching consensus

- How to reach consensus in a network with insecure communications and malicious nodes but a majority of honest agents?

Reaching consensus

- How to reach consensus in a network with insecure communications and malicious nodes but a majority of honest agents?

The Byzantine Generals Problem.
The situation can be described as the siege of a city by a group of generals of the Byzantine army. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach an agreement.

Reaching consensus

- How to reach consensus in a network with insecure communications and malicious nodes but a majority of honest agents?

The Byzantine Generals Problem.
The situation can be described as the siege of a city by a group of generals of the Byzantine army. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach an agreement.

- **Nakamoto Byzantine Generals Problem:** The number of generals is not fixed.

Reaching consensus

• How to reach consensus in a network with insecure communications and malicious nodes but a majority of honest agents?

The Byzantine Generals Problem.
The situation can be described as the siege of a city by a group of generals of the Byzantine army. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach an agreement.

• **Nakamoto Byzantine Generals Problem:** The number of generals is not fixed.

Reaching Consensus

- The idea is to select randomly who validates the next block of transactions.

Reaching Consensus

- The idea is to select randomly who validates the next block of transactions.
- A decentralized “lottery” is set by the PoW.

Reaching Consensus

- The idea is to select randomly who validates the next block of transactions.
- A decentralized "lottery" is set by the PoW.
- A computationally intensive problem is set to validate a block.

Reaching Consensus

- The idea is to select randomly who validates the next block of transactions.
- A decentralized “lottery” is set by the PoW.
- A computationally intensive problem is set to validate a block.
- The problem is difficult to solve, but the solution is easy to check.

Reaching Consensus

- The idea is to select randomly who validates the next block of transactions.
- A decentralized “lottery” is set by the PoW.
- A computationally intensive problem is set to validate a block.
- The problem is difficult to solve, but the solution is easy to check.
- The difficulty is adjusted to find a solution in about 10 minutes.

Reaching Consensus

- The idea is to select randomly who validates the next block of transactions.
- A decentralized “lottery” is set by the PoW.
- A computationally intensive problem is set to validate a block.
- The problem is difficult to solve, but the solution is easy to check.
- The difficulty is adjusted to find a solution in about 10 minutes.
- The miner that solves it receives an award in newly created bitcoins.

Generation

- Addresses are generated from a random 256 bit seed.

Generation

- Addresses are generated from a random 256 bit seed.
- Addresses have a public address and a secret key.

Generation

- Addresses are generated from a random 256 bit seed.
- Addresses have a public address and a secret key.
- The secret key is used to validate spend transactions.

Generation

- Addresses are generated from a random 256 bit seed.
- Addresses have a public address and a secret key.
- The secret key is used to validate spend transactions.

- Public address: 14xuSZXtfGw5XqfYxEjp4crwYGYQDWmZ12

14xuSZXtfGw5XqfYxEjp4crwYGYQDWmZ12

Monetary mass

- Bitcoins are generated at each new validated block.

Monetary mass

- Bitcoins are generated at each new validated block.
- The reward for miners was 50 BTC for the first 210.000 blocks (about 4 years), then 25 BTC for the next 210.000, and so on.

Monetary mass

- Bitcoins are generated at each new validated block.
- The reward for miners was 50 BTC for the first 210.000 blocks (about 4 years), then 25 BTC for the next 210.000, and so on.
- The production of bitcoins decreases geometrically: A finite total of 21 million will be created and no more.

Monetary mass

- Bitcoins are generated at each new validated block.
- The reward for miners was 50 BTC for the first 210.000 blocks (about 4 years), then 25 BTC for the next 210.000, and so on.
- The production of bitcoins decreases geometrically: A finite total of 21 million will be created and no more.
- The next halving in production of bitcoins will be next July 2016. Then 12.5 will be created with each new block.

Monetary mass

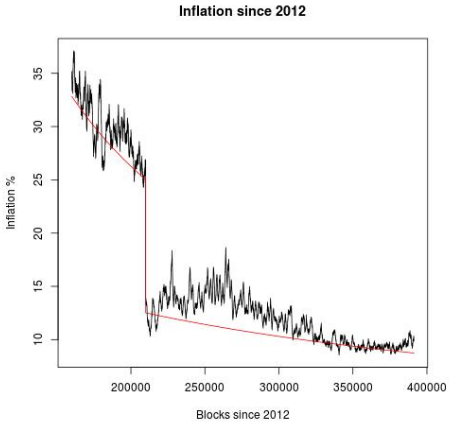
- Bitcoins are generated at each new validated block.
- The reward for miners was 50 BTC for the first 210.000 blocks (about 4 years), then 25 BTC for the next 210.000, and so on.
- The production of bitcoins decreases geometrically: A finite total of 21 million will be created and no more.
- The next halving in production of bitcoins will be next July 2016. Then 12.5 will be created with each new block.
- Bitcoin is a deflationnary currency.

Monetary mass

- Bitcoins are generated at each new validated block.
- The reward for miners was 50 BTC for the first 210.000 blocks (about 4 years), then 25 BTC for the next 210.000, and so on.
- The production of bitcoins decreases geometrically: A finite total of 21 million will be created and no more.
- The next halving in production of bitcoins will be next July 2016. Then 12.5 will be created with each new block.
- Bitcoin is a deflationnary currency.
- Each bitcoin is composed by 100 million satoshis (basic unit).

Monetary inflation

Bitcoin monetary inflation tends to 0



What is money?

$\boxed{\boxed{\textbf{Anything can be money}}}$

What is money?

Anything can be money

The distinction between good and bad money is CONFIDENCE

- Confidence to be able to spend it in the future keeping its value.

What is money?

Anything can be money

The distinction between good and bad money is CONFIDENCE

- Confidence to be able to spend it in the future keeping its value.
- Good money is backed by universally recognized structures:

What is money?

Anything can be money

The distinction between good and bad money is CONFIDENCE

- Confidence to be able to spend it in the future keeping its value.
- Good money is backed by universally recognized structures:
  1. Fiat money is backed by the state and central banks.

What is money?

Anything can be money

The distinction between good and bad money is CONFIDENCE

- Confidence to be able to spend it in the future keeping its value.
- Good money is backed by universally recognized structures:

1. Fiat money is backed by the state and central banks.
2. Gold is backed by its physical properties.

What is money?

Anything can be money

The distinction between good and bad money is CONFIDENCE

- Confidence to be able to spend it in the future keeping its value.
- Good money is backed by universally recognized structures:
  1. Fiat money is backed by the state and central banks.
  2. Gold is backed by its physical properties.
  3. Bitcoin is backed by mathematics and the computation power of the network.

Properties of good money

- Good money is not easy to falsify or produce.

Properties of good money

- Good money is not easy to falsify or produce.
- Good money is easily authenticatable.

Properties of good money

- Good money is not easy to falsify or produce.
- Good money is easily authenticatable.
- Good money is easily divisible.

Properties of good money

- Good money is not easy to falsify or produce.
- Good money is easily authenticatable.
- Good money is easily divisible.
- Good money is easily transportable.

Properties of good money

- Good money is not easy to falsify or produce.
- Good money is easily authenticatable.
- Good money is easily divisible.
- Good money is easily transportable.
- Good money enables fast payment settlements.

Properties of good money

- Good money is not easy to falsify or produce.
- Good money is easily authenticatable.
- Good money is easily divisible.
- Good money is easily transportable.
- Good money enables fast payment settlements.
- Good money is scarce.

Properties of good money

- Good money is not easy to falsify or produce.
- Good money is easily authenticatable.
- Good money is easily divisible.
- Good money is easily transportable.
- Good money enables fast payment settlements.
- Good money is scarce.
- Good money is international.

Properties of good money

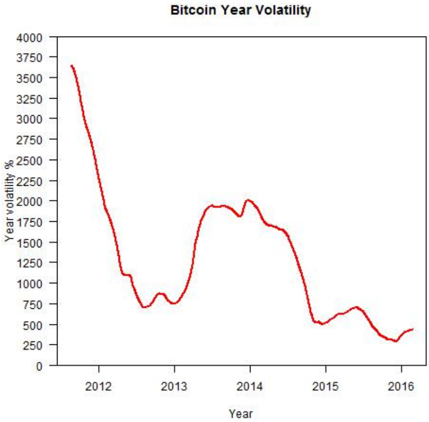
- Good money is not easy to falsify or produce.
- Good money is easily authenticatable.
- Good money is easily divisible.
- Good money is easily transportable.
- Good money enables fast payment settlements.
- Good money is scarce.
- Good money is international.
- Good money preserves or increases its value over time.

Properties of good money

- Good money is not easy to falsify or produce.
- Good money is easily authenticatable.
- Good money is easily divisible.
- Good money is easily transportable.
- Good money enables fast payment settlements.
- Good money is scarce.
- Good money is international.
- Good money preserves or increases its value over time.
- Good money is not volatile.

Bitcoin volatility

Bitcoin exchange rate volatility is high but decreases over time



Properties of good money

- Good money is fungible.

Properties of good money

- Good money is fungible.
- Good money does not decay over time.

Properties of good money

- Good money is fungible.
- Good money does not decay over time.
- Good money has a large base of users.

Properties of good money

- Good money is fungible.
- Good money does not decay over time.
- Good money has a large base of users.
- Good money is liquid.

Properties of good money

- Good money is fungible.
- Good money does not decay over time.
- Good money has a large base of users.
- Good money is liquid.
- Good money is easy to store securely.

Properties of good money

- Good money is fungible.
- Good money does not decay over time.
- Good money has a large base of users.
- Good money is liquid.
- Good money is easy to store securely.
- Good money is anonymous.

Properties of good money

- Good money is fungible.
- Good money does not decay over time.
- Good money has a large base of users.
- Good money is liquid.
- Good money is easy to store securely.
- Good money is anonymous.
- Good money is decentralized.

Properties of good money

- Good money is fungible.
- Good money does not decay over time.
- Good money has a large base of users.
- Good money is liquid.
- Good money is easy to store securely.
- Good money is anonymous.
- Good money is decentralized.
- Good money is useless (!)

Properties of good money

- Good money is fungible.
- Good money does not decay over time.
- Good money has a large base of users.
- Good money is liquid.
- Good money is easy to store securely.
- Good money is anonymous.
- Good money is decentralized.
- Good money is useless (!)
- Good money is antifragile.

Properties of good money

- Good money is fungible.
- Good money does not decay over time.
- Good money has a large base of users.
- Good money is liquid.
- Good money is easy to store securely.
- Good money is anonymous.
- Good money is decentralized.
- Good money is useless (!)
- Good money is antifragile.
- Good money can be used over insecure channels.

Properties of good money

- Good money is fungible.
- Good money does not decay over time.
- Good money has a large base of users.
- Good money is liquid.
- Good money is easy to store securely.
- Good money is anonymous.
- Good money is decentralized.
- Good money is useless (!)
- Good money is antifragile.
- Good money can be used over insecure channels.
- Good money is programmable!

Properties of good money

- Good money is fungible.
- Good money does not decay over time.
- Good money has a large base of users.
- Good money is liquid.
- Good money is easy to store securely.
- Good money is anonymous.
- Good money is decentralized.
- Good money is useless (!)
- Good money is antifragile.
- Good money can be used over insecure channels.
- Good money is programmable!