Spontaneous emergence of decentralized crypto-monetary systems

Ricardo Pérez-Marco

(CNRS, IMJ-PRG, Paris 7)

Workshop on Fintech, Univ. Orléans

September 15, 2020
Spontaneous emergence of decentralized crypto-monetary systems

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

Workshop on Fintech, Univ. Orléans

September 15, 2020

Spontaneous emergence of decentralized crypto-monetary systems

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

Workshop on Fintech, Univ. Orléans

September 15, 2020


Bitcoin paper

S. Nakamoto, November 1st 2008,
Bitcoin paper

S. Nakamoto, November 1st 2008,

“Bitcoin: A peer-to-peer electronic cash system”
S. Nakamoto, November 1st 2008,

“Bitcoin: A peer-to-peer electronic cash system”
Transparency Theorem

- Bitcoin is an electronic currency modeled by gold.
Transparency Theorem

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

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

- Bitcoin is an electronic currency modeled 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.
Transparency Theorem

- Bitcoin is an electronic currency modeled 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:
Bitcoin is an electronic currency modeled 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 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”.

**Inside: A 12-page special report on Colombia**

The Economist

How the technology behind bitcoin could change the world

Our guide to America’s best colleges
Myanmar’s free-ish election
These ever-creative accountants
America takes the fight to Isis
Ceyxworld: the new superpredator
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.

Addresses:
- 14xuSZXtfGw5XqfYxEjp4crwYGYQDWmZ12
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
Monetary mass

- Each bitcoin is composed by 100 million satoshis (basic unit).
Monetary mass

- Each bitcoin is composed by 100 million satoshis (basic unit).
- Bitcoins are generated at each new validated block.
Monetary mass

- Each bitcoin is composed by 100 million satoshis (basic unit).
- 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

- Each bitcoin is composed by 100 million satoshis (basic unit).
- 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. Now 18.5 M exists.
Monetary mass

- Each bitcoin is composed by 100 million satoshis (basic unit).
- 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. Now 18.5 M exists.
- The last halving (the 4th) did happen in May 2020. Since then, 6.25 BTC are created in each new block.
Monetary mass

• Each bitcoin is composed by 100 million satoshis (basic unit).

• 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. Now 18.5 M exists.

• The last halving (the 4th) did happen in May 2020. Since then, 6.25 BTC are created in each new block.

• Bitcoin is a deflationary currency. Current monetary inflation ≈ 1.8%.
Monetary inflation
What is money?

Anything can be money
What is money?

Anything can be money

The distinction between good and bad money is CONFIDENCE
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 network computation power.
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 authenticable.
Properties of good money

• Good money is not easy to falsify or produce.
• Good money is easily authenticable.
• Good money is easily divisible.
Properties of good money

- Good money is not easy to falsify or produce.
- Good money is easily authenticable.
- 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 authenticable.
• 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 authenticable.
- 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 authenticable.
- 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 authenticable.
- 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 authenticable.
- 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.
BTC/USD year 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 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 can be used over insecure channels.
- **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 can be used over insecure channels.
- **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 can be used over insecure channels.
- Good money is anonymous.
- Good money is decentralized.
- 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 can be used over insecure channels.
- Good money is anonymous.
- Good money is decentralized.
- Good money is antifragile.
- 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 can be used over insecure channels.
- Good money is anonymous.
- Good money is decentralized.
- Good money is antifragile.
- Good money is useless (!)
- 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 can be used over insecure channels.
- Good money is anonymous.
- Good money is decentralized.
- Good money is antifragile.
- Good money is useless (!)
- Good money is programmable!
Spontaneous emergence

Spontaneous emergence of decentralized crypto-monetary systems
Spontaneous emergence

- New phenomenon: Spontaneous emergence of a global monetary system.
Spontaneous emergence

- New phenomenon: Spontaneous emergence of a global monetary system.
- Academic challenge: Understand the dynamics of this phenomenon.
Spontaneous emergence

• New phenomenon: Spontaneous emergence of a global monetary system.
• Academic challenge: Understand the dynamics of this phenomenon.
• Viral adoption. Sigmoid curve.
Spontaneous emergence

• New phenomenon: Spontaneous emergence of a global monetary system.
• Academic challenge: Understand the dynamics of this phenomenon.
• Viral adoption. Sigmoid curve. Typical from Internet technologies, social networks, etc.
Spontaneous emergence

- New phenomenon: Spontaneous emergence of a global monetary system.
- Academic challenge: Understand the dynamics of this phenomenon.
- Viral adoption. Sigmoid curve. Typical from Internet technologies, social networks, etc.
Adoption and price

The sigmoid adoption curve has an initial exponential phase (still there).

Price BTC/USD shows the exponential increase.

We observe periodic bubbles. These are not "speculative bubbles."

Typical of the unstability of the exponential phase (and abrupt monetary halvings).

Bubbles are self-similar (see Mandelbrot's ideas).
Adoption and price

- The sigmoid adoption curve has an initial exponential phase (still there).
Adoption and price

- The sigmoid adoption curve has an initial exponential phase (still there).
- Price BTC/USD shows the exponential increase.
Adoption and price

- The sigmoid adoption curve has an initial exponential phase (still there).
- Price BTC/USD shows the exponential increase.
- We observe periodic bubbles.
Adoption and price

- The sigmoid adoption curve has an initial exponential phase (still there).
- Price BTC/USD shows the exponential increase.
- We observe periodic bubbles. These are not “speculative bubbles”.
Adoption and price

- The sigmoid adoption curve has an initial exponential phase (still there).
- Price BTC/USD shows the exponential increase.
- We observe periodic bubbles. These are not “speculative bubbles”. Typical of the unstability of the exponential phase (and abrupt monetary halvings).
Adoption and price

- The sigmoid adoption curve has an initial exponential phase (still there).
- Price BTC/USD shows the exponential increase.
- We observe periodic bubbles. These are not “speculative bubbles”. Typical of the unstability of the exponential phase (and abrupt monetary halvings).
- Bubbles are self-similar (see Mandelbrot’s ideas).
Adoption and price

- The sigmoid adoption curve has an initial exponential phase (still there).
- Price BTC/USD shows the exponential increase.
- We observe periodic bubbles. These are not “speculative bubbles”. Typical of the unstability of the exponential phase (and abrupt monetary halvings).
- Bubbles are self-similar (see Mandelbrot’s ideas).
New bimetallism and regulations

• Competition of Bitcoin and other crypto-currencies with classical currencies.
• Similar to gold/silver historical competition since the antiquity to the XIXth century.
• Renewed interest in bimetallic theory.
• New regulation needed.

Limitations: Regulation cannot regulate mathematics (nor physical laws)
• Gold and XIXth century bimetallic regulation can be helpful.
New bimetallism and regulations

- Competition of Bitcoin and other crypto-currencies with classical currencies.
New bimetallism and regulations

- Competition of Bitcoin and other crypto-currencies with classical currencies.
- Similar to gold/silver historical competition since the antiquity to the XIXth century.
New bimetallism and regulations

- Competition of Bitcoin and other crypto-currencies with classical currencies.
- Similar to gold/silver historical competition since the antiquity to the XIXth century.
- Renewed interest in bimetallic theory.
New bimetallism and regulations

• Competition of Bitcoin and other crypto-currencies with classical currencies.

• Similar to gold/silver historical competition since the antiquity to the XIXth century.

• Renewed interest in bimetallic theory.

• New regulation needed.
New bimetallism and regulations

- Competition of Bitcoin and other crypto-currencies with classical currencies.
- Similar to gold/silver historical competition since the antiquity to the XIXth century.
- Renewed interest in bimetallic theory.
- New regulation needed.
- Limitations: Regulation cannot regulate mathematics (nor physical laws)
New bimetallism and regulations

- Competition of Bitcoin and other crypto-currencies with classical currencies.
- Similar to gold/silver historical competition since the antiquity to the XIXth century.
- Renewed interest in bimetallic theory.
- New regulation needed.
- Limitations: Regulation cannot regulate mathematics (nor physical laws)
- Gold and XIXth century bimetallic regulation can be helpful.
New bimetallism and regulations

- Competition of Bitcoin and other crypto-currencies with classical currencies.

- Similar to gold/silver historical competition since the antiquity to the XIXth century.

- Renewed interest in bimetallic theory.

- New regulation needed.

- Limitations: Regulation cannot regulate mathematics (nor physical laws)

- Gold and XIXth century bimetallic regulation can be helpful.
Spontaneous emergence of decentralized crypto-monetary systems
Thank you for your attention!
Thank you for your attention!