Blockchain time and Heisenberg Uncertainty Principle

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

Computing Conference 2018
London

July 11, 2018

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

Blockchain time and Heisenberg Uncertainty Principle

Bitcoin paper

Bitcoin paper

S. Nakamoto, November 1st 2008,

Bitcoin paper

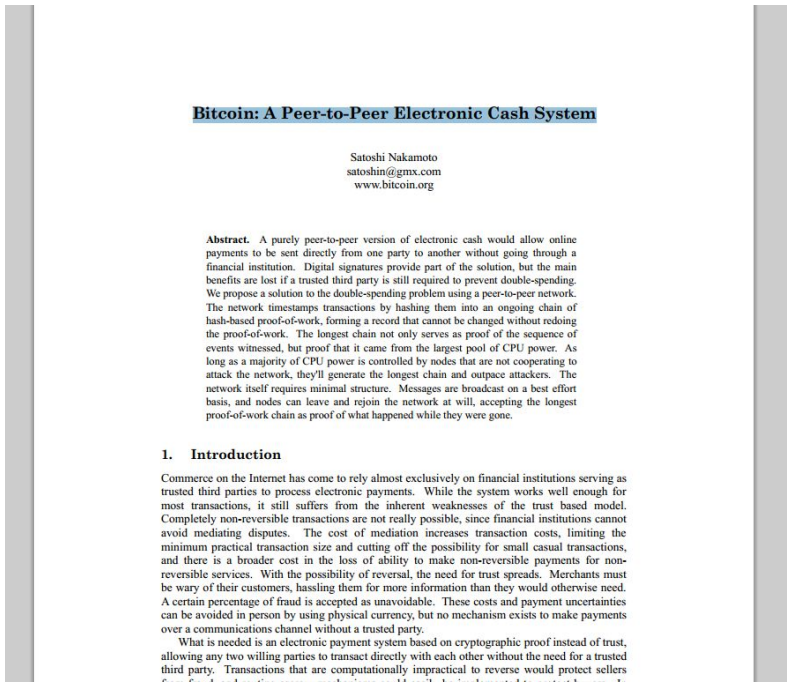
S. Nakamoto, November 1st 2008,

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

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

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:

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:

Theorem (Transparency Theorem)

A decentralized e-currency must rely on a public ledger.

The blockchain

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 ordered 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 ordered 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 ordered 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 ordered 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 by iterating hashes (Proof-of-Work).

Decentralized time

Decentralized time

- The solution to the “Double spend problem” will be trivial if a universal and decentralized time existed.

Decentralized time

- The solution to the “Double spend problem” will be trivial if a universal and decentralized time existed.

We would only need to crytographically timestamp transactions to prioritized them and avoid double spends.

Decentralized time

- The solution to the “Double spend problem” will be trivial if a universal and decentralized time existed.

We would only need to crytographically timestamp transactions to prioritized them and avoid double spends.

- Before the Bitcoin protocol no universal decentralized time server existed in the Internet.

Decentralized time

- The solution to the “Double spend problem” will be trivial if a universal and decentralized time existed.

We would only need to crytographically timestamp transactions to prioritized them and avoid double spends.

- Before the Bitcoin protocol no universal decentralized time server existed in the Internet.
- The Bitcoin network provides (a posteriori!) a decentralized time.

Decentralized time

- The solution to the “Double spend problem” will be trivial if a universal and decentralized time existed.

We would only need to crytographically timestamp transactions to prioritized them and avoid double spends.

- Before the Bitcoin protocol no universal decentralized time server existed in the Internet.
- The Bitcoin network provides (a posteriori!) a decentralized time.
- Each validated blocks is the “tick” of the clock.

The Trust Machine

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

The Trust Machine

- The core of the Bitcoin protocol is the algorithm to ensure that the blockchain cannot be forged.
- The mechanism of consensus: “The trust machine”.

Byzantine Generals Problem

Byzantine Generals Problem

Problem: How to reach an honest consensus and prevent malicious attacks?

Byzantine Generals Problem

Problem: How to reach an honest consensus and prevent malicious attacks?

Byzantine Generals Problem (BGP)

Byzantine Generals Problem

Problem: How to reach an honest consensus and prevent malicious attacks?

Byzantine Generals Problem (BGP)

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.

Byzantine Generals Problem

Problem: How to reach an honest consensus and prevent malicious attacks?

Byzantine Generals Problem (BGP)

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

Nakamoto Byzantine Generals Problem

Nakamoto Byzantine Generals Problem (NBGP)

Nakamoto Byzantine Generals Problem

Nakamoto Byzantine Generals Problem (NBGP)

The number of generals is not fixed. Anyone can participate in the decision network.

Nakamoto Byzantine Generals Problem

Nakamoto Byzantine Generals Problem (NBGP)

The number of generals is not fixed. Anyone can participate in the decision network.

Definition (Decentralized Consensus Protocol)

A **Decentralized Consensus Protocol (DCP)** is a solution to NBGP.

Thermodynamic conjecture

Thermodynamic conjecture

- The Bitcoin protocol solves NBGP.

Thermodynamic conjecture

- The Bitcoin protocol solves NBGP.

This is necessary to make sure that a minority cannot corrupt the blockchain.

Thermodynamic conjecture

- The Bitcoin protocol solves NBGP.

This is necessary to make sure that a minority cannot corrupt the blockchain.

- Only known solution to NBGP is based on a PoW.

Thermodynamic conjecture

- The Bitcoin protocol solves NBGP.

This is necessary to make sure that a minority cannot corrupt the blockchain.

- Only known solution to NBGP is based on a PoW.

In particular to defend from a Sybil attack.

Thermodynamic conjecture

- The Bitcoin protocol solves NBGP.

This is necessary to make sure that a minority cannot corrupt the blockchain.

- Only known solution to NBGP is based on a PoW.

In particular to defend from a Sybil attack.

- Security relies on a PoW.

Thermodynamic conjecture

- The Bitcoin protocol solves NBGP.

This is necessary to make sure that a minority cannot corrupt the blockchain.

- Only known solution to NBGP is based on a PoW.

In particular to defend from a Sybil attack.

- Security relies on a PoW.

Thermodynamical Conjecture: There is no solution to NBGP without external input of energy.

Thermodynamic conjecture

- The Bitcoin protocol solves NBGP.

This is necessary to make sure that a minority cannot corrupt the blockchain.

- Only known solution to NBGP is based on a PoW.

In particular to defend from a Sybil attack.

- Security relies on a PoW.

Thermodynamical Conjecture: There is no solution to NBGP without external input of energy.

Thermodynamic proof: We cannot have an isolated system with decreasing entropy by the 2nd Law of Thermodynamics.

Strong Thermodynamic Conjecture

Strong Thermodynamic Conjecture

Strong Thermodynamic Conjecture

- The protocol running Bitcoin's blockchsin establishes a chronology.

Strong Thermodynamic Conjecture

- The protocol running Bitcoin's blockchsin establishes a chronology.

Incompatible changes of the same data must be resolved by prioritizing one of the changes.

Strong Thermodynamic Conjecture

- The protocol running Bitcoin's blockchsin establishes a chronology.

Incompatible changes of the same data must be resolved by prioritizing one of the changes. This cannot rely on an external clock or decentralization would be lost.

Strong Thermodynamic Conjecture

- The protocol running Bitcoin's blockchsin establishes a chronology.

Incompatible changes of the same data must be resolved by prioritizing one of the changes. This cannot rely on an external clock or decentralization would be lost. Therefore there is an internal chronology of modifications of the database.

Strong Thermodynamic Conjecture

- The protocol running Bitcoin's blockchsin establishes a chronology.

Incompatible changes of the same data must be resolved by prioritizing one of the changes. This cannot rely on an external clock or decentralization would be lost. Therefore there is an internal chronology of modifications of the database.

Strong Thermodynamical Conjecture: There is no protocol establishing an internal chronology of a system without external input of energy.

Uncertainty principles formulations

Uncertainty principles formulations

Uncertainty principles formulations

Heisenberg formulation

Uncertainty principles formulations

Heisenberg formulation

If we want to measure the position x and the momentum p of a particle with precisions Δx and Δp, then we have

$$\Delta x \cdot \Delta p \geq \hbar \, .$$

$\hbar = h/2\pi \approx 1.0545718 \cdot 10^{-34}$ $J.s$ reduced Planck constant.

Uncertainty principles formulations

Heisenberg formulation

If we want to measure the position x and the momentum p of a particle with precisions Δx and Δp, then we have

$$\Delta x \cdot \Delta p \geq \hbar \, .$$

$\hbar = h/2\pi \approx 1.0545718 \cdot 10^{-34}$ $J.s$ reduced Planck constant.

Von Neumann formulation

Uncertainty principles formulations

Heisenberg formulation

If we want to measure the position x and the momentum p of a particle with precisions Δx and Δp, then we have

$$\Delta x \cdot \Delta p \geq \hbar \, .$$

$\hbar = h/2\pi \approx 1.0545718 \cdot 10^{-34}$ $J.s$ reduced Planck constant.

Von Neumann formulation

If we want to measure the energy of a system with a precision ΔE, we need a minimal time Δt and

$$\Delta E \cdot \Delta t \geq \hbar \, .$$

Uncertainty principles formulations

Heisenberg formulation

If we want to measure the position x and the momentum p of a particle with precisions Δx and Δp, then we have

$$\Delta x \cdot \Delta p \geq \hbar \, .$$

$\hbar = h/2\pi \approx 1.0545718 \cdot 10^{-34}$ $J.s$ reduced Planck constant.

Von Neumann formulation

If we want to measure the energy of a system with a precision ΔE, we need a minimal time Δt and

$$\Delta E \cdot \Delta t \geq \hbar \, .$$

Blockchain time and energy

Blockchain time and energy

Blockchain time and energy

- Blockchain time t has a precision $\Delta t \approx 10$ min.

Blockchain time and energy

- Blockchain time t has a precision $\Delta t \approx 10$ min.

This is so because we adjust the difficulty.

Blockchain time and energy

- Blockchain time t has a precision $\Delta t \approx 10$ min.

This is so because we adjust the difficulty.

- Without difficulty adjustment, the precision of blockchain time will be $\Delta t \sim 1/H$, where H is the hashrate of the network.

Blockchain time and energy

- Blockchain time t has a precision $\Delta t \approx 10$ min.

This is so because we adjust the difficulty.

- Without difficulty adjustment, the precision of blockchain time will be $\Delta t \sim 1/H$, where H is the hashrate of the network.
- The Blockchain needs an energy E to be build up.

Blockchain time and energy

- Blockchain time t has a precision $\Delta t \approx 10$ min.

This is so because we adjust the difficulty.

- Without difficulty adjustment, the precision of blockchain time will be $\Delta t \sim 1/H$, where H is the hashrate of the network.
- The Blockchain needs an energy E to be build up.
- The precision ΔE is the energy needed to validate a block.

Blockchain time and energy

- Blockchain time t has a precision $\Delta t \approx 10$ min.

This is so because we adjust the difficulty.

- Without difficulty adjustment, the precision of blockchain time will be $\Delta t \sim 1/H$, where H is the hashrate of the network.
- The Blockchain needs an energy E to be build up.
- The precision ΔE is the energy needed to validate a block.
- H is proportional to the external input of energy, $H = k \,.\, \Delta E$

Blockchain time and energy

- Blockchain time t has a precision $\Delta t \approx 10$ min.

This is so because we adjust the difficulty.

- Without difficulty adjustment, the precision of blockchain time will be $\Delta t \sim 1/H$, where H is the hashrate of the network.
- The Blockchain needs an energy E to be build up.
- The precision ΔE is the energy needed to validate a block.
- H is proportional to the external input of energy, $H = k \,.\, \Delta E$
- *The constant k depends on the hardware used.*

Blockchain Heisenberg Uncertainty Principle

Blockchain Heisenberg Uncertainty Principle

Blockchain Heisenberg Uncertainty Principle

Theorem (Blockchain Heisenberg Uncertainty Principle)

$$\Delta E \,.\, \Delta t \sim 1/k \,.$$

Blockchain Heisenberg Uncertainty Principle

Theorem (Blockchain Heisenberg Uncertainty Principle)

$$\Delta E \,.\, \Delta t \sim 1/k \,.$$

Blockchain Heisenberg Uncertainty Principle

Theorem (Blockchain Heisenberg Uncertainty Principle)

$$\Delta E \,.\, \Delta t \sim 1/k \ .$$

Observation: Heisenberg Uncertainty Principle indicates that a theoretical upper bound on k exists

$$1/k \geq \hbar.$$

Nakamoto, Heisenberg, Kolmogorov, Bennett

Nakamoto, Heisenberg, Kolmogorov, Bennett

Nakamoto, Heisenberg, Kolmogorov, Bennett

- The blockchain is hard to counterfeit because its Kolmogorov complexity is high (assuming standard assumptions on hash function).

Nakamoto, Heisenberg, Kolmogorov, Bennett

- The blockchain is hard to counterfeit because its Kolmogorov complexity is high (assuming standard assumptions on hash function).
- More precisely, its Bennett logical depth is high.

Nakamoto, Heisenberg, Kolmogorov, Bennett

- The blockchain is hard to counterfeit because its Kolmogorov complexity is high (assuming standard assumptions on hash function).
- More precisely, its Bennett logical depth is high.

Physical complexity principle: The amount of energy E necessary for the construction of information with a Bennett logical depth τ_0 is universally bounded from below

$$E \geq \kappa \tau_0$$

where κ is a universal physical constant.

Thank you for your attention!!