Smart contracts, Lightning network and new developments in cryptofinance

Ricardo Pérez-Marco (CNRS, IMJ-PRG, Labex Réfi)

Blockchain and lightning networks:
Coming closer to european values
Lieu d'Europe, Strasbourg

November 21, 2016

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

A brief introduction to Bitcoin

1 Electronic gold

2 The blockchain

3 The Bitcoin Network

4 Smart Money

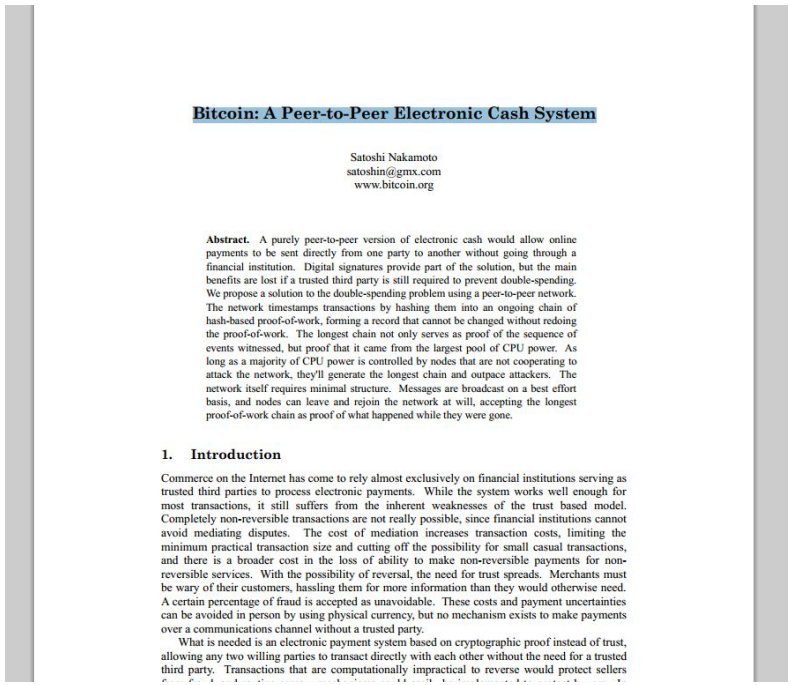
5 Bitcoin scaling

6 Lightning Network

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) is necessary.

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) is necessary.

New functionalities

- Bitcoin is programable money: Smart Money.

New functionalities

- Bitcoin is programable money: Smart Money.
- Each transaction contains a “scrypt field” where are set the conditions to spend the bitcoins in the target address.

New functionalities

- Bitcoin is programable money: Smart Money.
- Each transaction contains a “scrypt field” where are set the conditions to spend the bitcoins in the target address.

Examples:

New functionalities

- Bitcoin is programable money: Smart Money.
- Each transaction contains a “scrypt field” where are set the conditions to spend the bitcoins in the target address.

Examples:

- No condition. Then anyone can spend the bitcoins (and they will disappear in seconds).

New functionalities

- Bitcoin is programable money: Smart Money.
- Each transaction contains a “scrypt field” where are set the conditions to spend the bitcoins in the target address.

Examples:

- No condition. Then anyone can spend the bitcoins (and they will disappear in seconds).
- The receiver must sign with his private key to spend the output (most common condition).

New functionalities

- Bitcoin is programable money: Smart Money.
- Each transaction contains a “scrypt field” where are set the conditions to spend the bitcoins in the target address.

Examples:

- No condition. Then anyone can spend the bitcoins (and they will disappear in seconds).
- The receiver must sign with his private key to spend the output (most common condition).
- Several signatures are required to spend the output ($m - n$ multisignature means that m out of n need to sign).

New functionalities

- Bitcoin is programable money: Smart Money.
- Each transaction contains a “scrypt field” where are set the conditions to spend the bitcoins in the target address.

Examples:

- No condition. Then anyone can spend the bitcoins (and they will disappear in seconds).
- The receiver must sign with his private key to spend the output (most common condition).
- Several signatures are required to spend the output ($m - n$ multisignature means that m out of n need to sign).
- Delayed output: The output cannot be spend before some time.

New functionalities

- Bitcoin is programable money: Smart Money.
- Each transaction contains a “scrypt field” where are set the conditions to spend the bitcoins in the target address.

Examples:

- No condition. Then anyone can spend the bitcoins (and they will disappear in seconds).
- The receiver must sign with his private key to spend the output (most common condition).
- Several signatures are required to spend the output ($m - n$ multisignature means that m out of n need to sign).
- Delayed output: The output cannot be spend before some time.

Smart Contracts

The above are examples of simple “smart contracts”.

Smart Contracts

The above are examples of simple “smart contracts”.

- In Bitcoin, the scrypt functionalities have been limited because of concerns of bugs.

Smart Contracts

The above are examples of simple “smart contracts”.

- In Bitcoin, the scrypt functionalities have been limited because of concerns of bugs.
- Other cryptocurrencies implement richer scrypt languages (for example Ethereum with a Turing complete language).

Smart Contracts

The above are examples of simple “smart contracts”.

- In Bitcoin, the scrypt functionalities have been limited because of concerns of bugs.
- Other cryptocurrencies implement richer scrypt languages (for example Ethereum with a Turing complete language).
- More powerful but more insecure (example: DAO hacking).

Smart Contracts

The above are examples of simple “smart contracts”.

- In Bitcoin, the scrypt functionalities have been limited because of concerns of bugs.
- Other cryptocurrencies implement richer scrypt languages (for example Ethereum with a Turing complete language).
- More powerful but more insecure (example: DAO hacking).

DAO= Decentralized Autonomous Organization

Smart Contracts

The above are examples of simple “smart contracts”.

- In Bitcoin, the scrypt functionalities have been limited because of concerns of bugs.
- Other cryptocurrencies implement richer scrypt languages (for example Ethereum with a Turing complete language).
- More powerful but more insecure (example: DAO hacking).

DAO= Decentralized Autonomous Organization

Automatic rules are implemented. Rich field of applications in the Internet of Things.

Transactions per second

- Current Bitcoin network supports at most 5 to 7 transactions per second.

Transactions per second

- Current Bitcoin network supports at most 5 to 7 transactions per second.
- VISA runs on average about 600 transactions per second.

Transactions per second

- Current Bitcoin network supports at most 5 to 7 transactions per second.
- VISA runs on average about 600 transactions per second.

Several scaling proposals:

Transactions per second

- Current Bitcoin network supports at most 5 to 7 transactions per second.
- VISA runs on average about 600 transactions per second.

Several scaling proposals:

(1) Increase block size (currently 1 Mb).

Transactions per second

- Current Bitcoin network supports at most 5 to 7 transactions per second.
- VISA runs on average about 600 transactions per second.

Several scaling proposals:

(1) Increase block size (currently 1 Mb).

Problems with size of the blockchain (currently 90 Gb), problems with block propagation on the network.

Transactions per second

- Current Bitcoin network supports at most 5 to 7 transactions per second.
- VISA runs on average about 600 transactions per second.

Several scaling proposals:

(1) Increase block size (currently 1 Mb).

Problems with size of the blockchain (currently 90 Gb), problems with block propagation on the network.

(2) SegWit. “Segregated Witness”

Transactions per second

- Current Bitcoin network supports at most 5 to 7 transactions per second.
- VISA runs on average about 600 transactions per second.

Several scaling proposals:

(1) Increase block size (currently 1 Mb).

Problems with size of the blockchain (currently 90 Gb), problems with block propagation on the network.

(2) SegWit. “Segregated Witness”

Separates signatures from the rest of transaction messages. We may gain about 30-50% of block space, thus around 10 transactions per second.

Transactions per second

- Current Bitcoin network supports at most 5 to 7 transactions per second.
- VISA runs on average about 600 transactions per second.

Several scaling proposals:

(1) Increase block size (currently 1 Mb).

Problems with size of the blockchain (currently 90 Gb), problems with block propagation on the network.

(2) SegWit. “Segregated Witness”

Separates signatures from the rest of transaction messages. We may gain about 30-50% of block space, thus around 10 transactions per second.

(3) Lightning network.

Transactions per second

- Current Bitcoin network supports at most 5 to 7 transactions per second.
- VISA runs on average about 600 transactions per second.

Several scaling proposals:

(1) Increase block size (currently 1 Mb).

Problems with size of the blockchain (currently 90 Gb), problems with block propagation on the network.

(2) SegWit. “Segregated Witness”

Separates signatures from the rest of transaction messages. We may gain about 30-50% of block space, thus around 10 transactions per second.

(3) Lightning network.

Payment Channels

- The implementation of SegWit (in several month) solves the problem of transaction malleability and allows the opening of Payment Channels.

Payment Channels

- The implementation of SegWit (in several month) solves the problem of transaction malleability and allows the opening of Payment Channels.
- A Payment Channel allows arbitrary number of transactions between 2 parties at almost no cost.

Payment Channels

- The implementation of SegWit (in several month) solves the problem of transaction malleability and allows the opening of Payment Channels.
- A Payment Channel allows arbitrary number of transactions between 2 parties at almost no cost.
- Uses the security of bitcoin blockchain: One opening bitcoin transaction and one closing transaction.

Payment Channels

- The implementation of SegWit (in several month) solves the problem of transaction malleability and allows the opening of Payment Channels.
- A Payment Channel allows arbitrary number of transactions between 2 parties at almost no cost.
- Uses the security of bitcoin blockchain: One opening bitcoin transaction and one closing transaction.
- An open Payment Channels freezes a certain amount of bitcoins in the blockchain (that fixes the maximum of the final settlement).

Lightning network

Lightning network

• One can build a payment network: If we have an open channel $A \to B$ and another $B \to C$, then A can pay C.

Lightning network

- One can build a payment network: If we have an open channel $A \to B$ and another $B \to C$, then A can pay C.

- In a chain of payment $A \to B \to \ldots \to Z$ the maximum amount transacted is bounded from the minimum in all channels.

Lightning network

• One can build a payment network: If we have an open channel $A \to B$ and another $B \to C$, then A can pay C.

• In a chain of payment $A \to B \to \ldots \to Z$ the maximum amount transacted is bounded from the minimum in all channels.

• The Lightning Network operates on top of the Bitcoin network. Currently in development. Will be fast and more anonymous.

Thank you for your attention!