



Lauro Grippa Neto

Blockchain

MAGRATHEA LABS

www.magrathealabs.com

SUMMARY

1. Introduction
2. Concepts and Components
3. Vulnerabilities
4. Applications
5. Challenges
6. Conclusions

<https://gist.github.com/laurogripa/>

What's a market?



The need for a currency

- Medium of exchange
- Unit of account
- Store of value





The "Double-spending" problem

"**Double-spending** is the result of successfully spending some money more than once."

Combating Double-Spending Using Cooperative P2P Systems

[Sign In or Purchase
to View Full Text](#)**5**
Paper
Citations**225**
Full
Text Views

Related Articles

[Dictionary design algorithms for vector map compression](#)[Jini meets embedded control networking: a case study in portability failure](#)[View All](#)**4**
Author(s)[Ivan Osipkov](#) ; [Eugene Y. Vasserman](#) ; [Nicholas Hopper](#) ; [Yongdae Kim](#)[View All Authors](#)[Abstract](#)[Authors](#)[Figures](#)[References](#)[Citations](#)[Keywords](#)[Metrics](#)[Media](#)

Abstract:

An electronic cash system allows users to withdraw coins, represented as bit strings, from a bank or broker, and spend those coins anonymously at participating merchants, so that the broker cannot link spent coins to the user who withdraws them. A variety of schemes with various security properties have been proposed for this purpose, but because strings of bits are inherently copyable, they must all deal with the problem of double-spending. In this paper, we present an electronic cash scheme that introduces a new peer-to-peer system architecture to prevent double-spending without requiring an on-line trusted party or tamper-resistant software or hardware. The scheme is easy to implement, computationally efficient, and provably secure. To demonstrate this, we report on a proof-of-concept implementation for Internet vendors along with a detailed complexity analysis and selected security proofs.

Published in: [Distributed Computing Systems, 2007. ICDCS '07. 27th International Conference on](#)

Date of Conference: 25-27 June 2007

INSPEC Accession Number: 10290180

Date Added to IEEE Xplore: 09 July 2007

DOI: [10.1109/ICDCS.2007.91](#)

CD-ROM ISBN: 0-7695-2837-3

Publisher: IEEE

Print ISSN: 1063-6927

Conference Location: Toronto, ON, Canada

Distributed Double Spending Prevention*

Jaap-Henk Hoepman

TNO Information and Communication Technology
P.O. Box 1416, 9701 BK Groningen, The Netherlands
jaap-henk.hoepman@tno.nl
and
Institute for Computing and Information Sciences
Radboud University Nijmegen
P.O. Box 9010, 6500 GL Nijmegen, the Netherlands
jhh@cs.ru.nl

Abstract. We study the problem of *preventing* double spending in electronic payment schemes in a *distributed* fashion. This problem occurs, for instance, when the spending of electronic coins needs to be controlled by a large collection of nodes (e.g., in a peer-to-peer (P2P) system) instead of one central bank. Contrary to the commonly held belief that this is fundamentally impossible, we propose several solutions that do achieve a reasonable level of double spending prevention, and analyse their efficiency under varying assumptions.

1 Introduction

Many electronic payment schemes exist. For an overview, we refer to Asokan *et al.* [AJSW97] or O'Mahony *et al.* [OPT97]. Some of those are coin based, where some bitstring locally stored by a user represents a certain fixed value.

Coin based systems run the risk that many copies of the same bitstring are spent at different merchants. Therefore, these systems need to incorporate *double spending* prevention or detection techniques. To *prevent* double spending, a central bank is usually assumed which is involved in each and every transaction. In off-line scenarios (where such a connection to a central bank is not available), double spending *detection* techniques are used that will discover double spending at some later time, and that allow one to find the perpetrator of this illegal activity. A major drawback of double spending detection techniques is the risk that a dishonest user spends a single coin a million times in a short period of time before being detected. This is especially a problem if such a user cannot be punished for such behaviour afterwards, e.g., fined, penalised judicially, or being kicked from the system permanently.

* This research is/was partially supported by the research program Sentinels (www.sentinels.nl), project JASON (NIT.6677). Sentinels is being financed by Technology Foundation STW, the Netherlands Organization for Scientific Research (NWO), and the Dutch Ministry of Economic Affairs.
Id: double-spending.tex 18 2008-02-06 14:01:34Z jhh

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

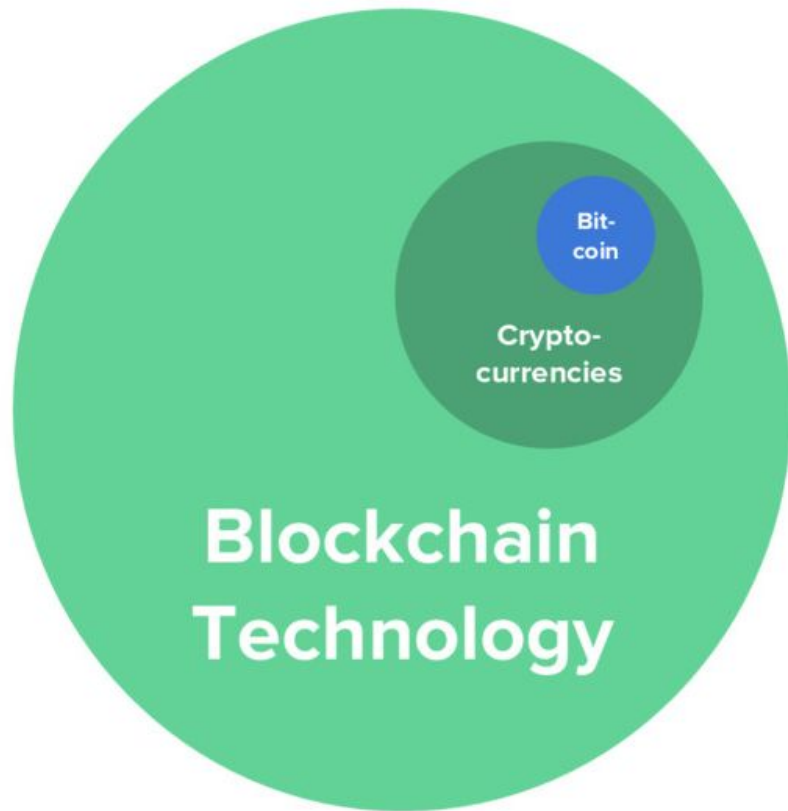
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required 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.

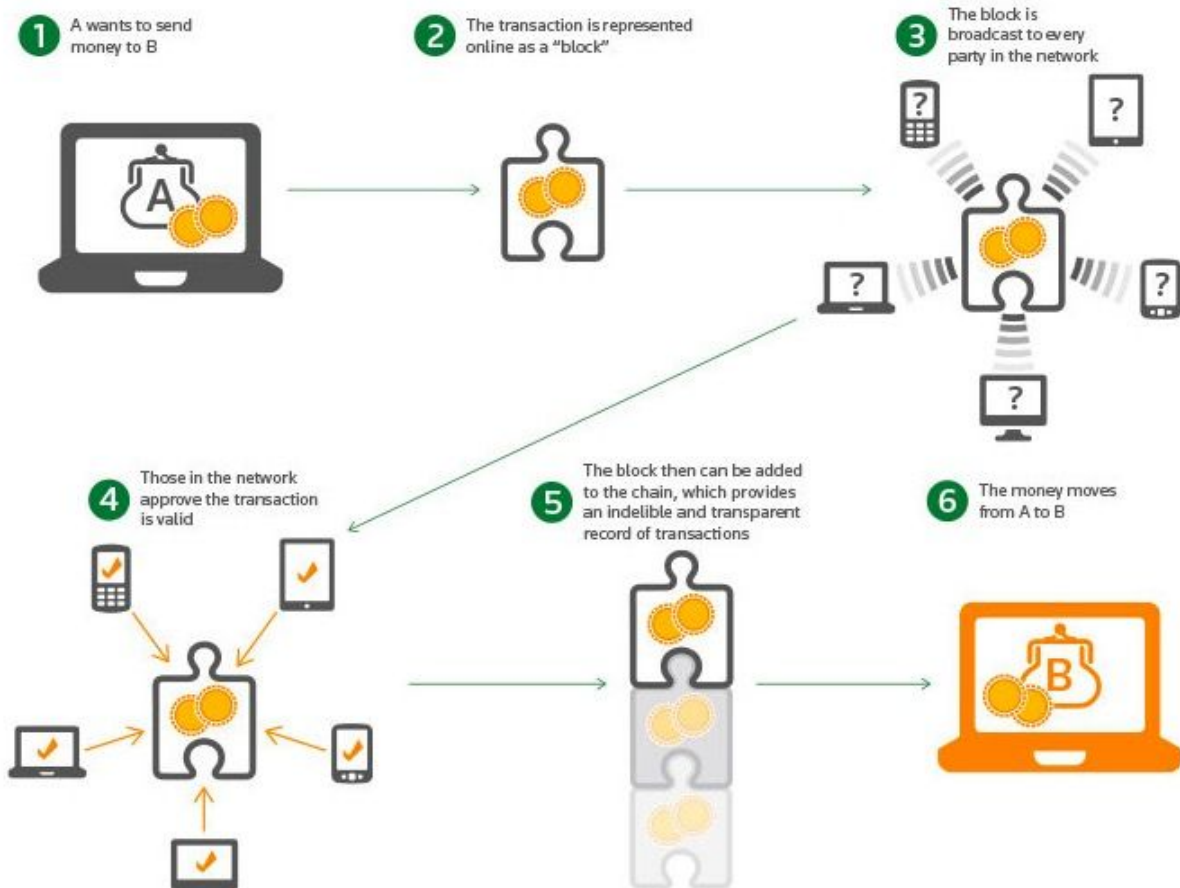
1. Introduction

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.

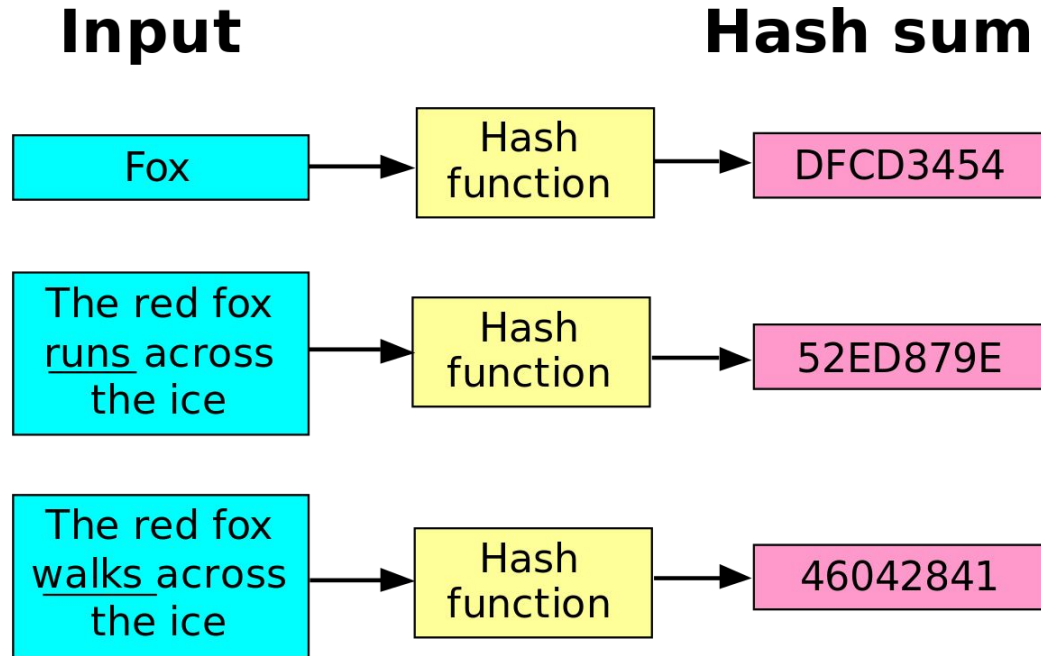
What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

BITCOIN ≠ BLOCKCHAIN





THE MAIN INGREDIENT: HASHES!



[DEMO]

<https://anders.com/blockchain/>

CONCEPTS AND COMPONENTS

- **Hash:** address (public keys), wallet (private keys), transactions (signatures and receipts).
- **Block:** contain transactions/contracts
- **Blockchain:** “It’s just a database!”
- **Distributed:** P2P networks
- **Token:** Distributed Ledger
- **Coinbase:** incentives (mining and staking)

Game Theory

"The primary role of blockchains are to solve **coordination problems** among **multilateral agreements** between a **network of participants**."

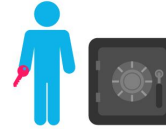
Reaching consensus

- Proof of Work
- Proof of Stake
- Delegated Proof of Stake

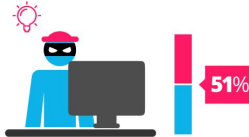
Proof of Work vs **Proof of Stake**



proof of work is a requirement to define an expensive computer calculation, also called mining



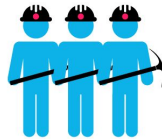
Proof of stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as stake.



A reward is given to the first miner who solves each blocks problem.



The PoS system there is no block reward, so, the miners take the transaction fees.



Network miners compete to be the first to find a solution for the mathematical problem



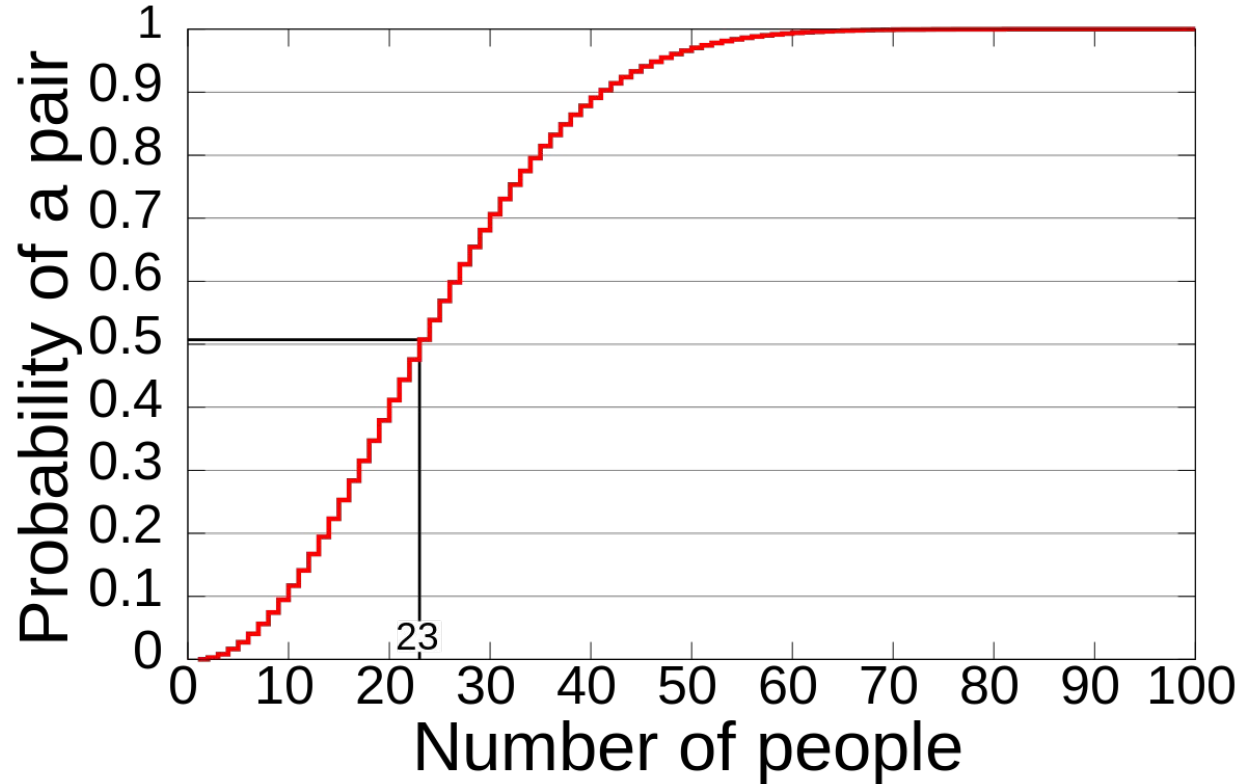
Proof of Stake currencies can be several thousand times more cost effective.

VULNERABILITIES

HASHES AND THE PIGEONHOLE



THE BIRTHDAY PROBLEM



THE BIRTHDAY ATTACK

Given y , find x such as $f(x) = y$

- Preimage resistance: 2^n
- Birthday attack: $\sqrt{2^n} = 2^{n/2}$
- Quantum birthday attack: $\sqrt[3]{2^n} = 2^{n/3}$

LARGE BITCOIN COLLIDER

“The “Large Bitcoin Collider” (LBC - a homage to LHC) is a distributed effort to find **at least one collision** of private Bitcoin keys”

OTHER VULNERABILITIES

- 51% attack (PoW)
- Nothing-at-Stake (PoS)
- Sybil attack (Both)
- Phishing/scamming

APPLICATIONS

QUANTUM RESISTANT LEDGER

The Quantum Resistant Ledger (QRL) is a first of its kind, **future-proof post quantum value store** and decentralized communication layer which tackles the threat Quantum Computing will pose to cryptocurrencies.



ETHEREUM

“Ethereum is a decentralized platform that runs smart contracts: **applications** that run exactly as programmed **without any possibility of downtime, censorship, fraud or third party interference.**”



GOLEM

“Golem is a global, open sourced, **decentralized supercomputer that anyone can access**. It’s made up of the combined power of user’s machines, from personal laptops to entire datacenters.”



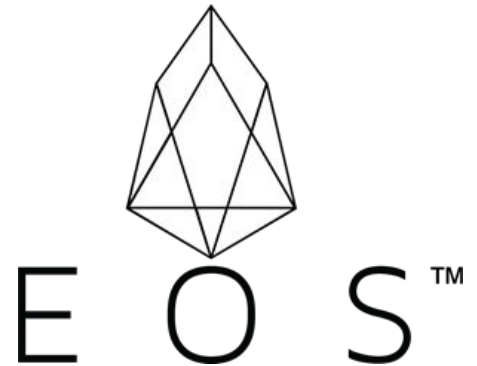
NUMERAI

“Machine learning competitions are susceptible to intentional overfitting. Numerai proposes Numeraire, a new cryptographic token that can be used in a novel auction mechanism to **make overfitting economically irrational.**”



EOS

“EOSIO is software that introduces a blockchain architecture designed to enable **vertical and horizontal scaling of decentralized applications** (the “EOSIO Software”)”



Challenges

- https://docs.google.com/presentation/d/1542_5OiH_KuXxE0x4w5F7M_ngLKuzWogSjBUQW-ZnxQ/edit#slide=id.p
- <https://gist.github.com/laurogripa/f568285bcd5fe6ca116ce5562ee9a37f>
- <https://www.ethereum.org/token>
- <http://remix.ethereum.org>
- <http://voting-dapp-testnet.herokuapp.com>
- https://hackattic.com/challenges/mini_miner



Questions?

MAGRATHEA LABS

www.magrathealabs.com

Blockchain Joinville

<https://www.meetup.com/Blockchain-Joinville/>



MAGRATHEA LABS

www.magrathealabs.com/careers

contact@magrathealabs.com



Thank you!

MAGRATHEA LABS

www.magrathealabs.com