



Blockchain and Research

June 6, 2017

Jean-Jacques Quisquater
jjq@uclouvain.be --- jjq@mit.edu

UCL – Louvain-la-Neuve, Belgique (emeritus professor)
MIT-CSAIL, Cambridge, USA (research associate)
Académie Royale de Belgique

Nice properties of blockchains

- Decentralisation,
- Consensus,
- Validity,
- Unicity,
- Authenticity,
- Immuable past,
- Sure (security),
- Trust,
- Non-repudiation.

• Too nice?
A long story ...



THE BOOK OF SATOSHI




The Collected Writings of Bitcoin Creator

Satoshi Nakamoto

PHIL CHAMPAGNE

FOREWORD BY JEFF BERWICK

1991



How to Time-Stamp a Digital Document*

Stuart Haber
stuart@bellcore.com

W. Scott Stornetta
stornetta@bellcore.com

Bellcore
445 South Street
Morristown, N.J. 07960-1910

Abstract

The prospect of a world in which all text, audio, picture, and video documents are in digital form on easily modifiable media raises the issue of how to certify when a document was created or last changed. The problem is to time-stamp the data, not the medium. We propose computationally practical procedures for digital time-stamping of such documents so that it is infeasible for a user either to back-date or to forward-date his document, even with the collusion of a time-stamping service. Our procedures maintain complete privacy of the documents themselves, and require no record-keeping by the time-stamping service.

*Appeared, with minor editorial changes, in *Journal of Cryptology*, Vol. 3, No. 2, pp. 99-111, 1991.



certify when a document was created or last modified? Methods of certification, or time-stamping, must satisfy two criteria. First, they must time-stamp the actual bits of the document, making no assumptions about the physical medium on which the document is recorded. Second, the date and time of the time-stamp must not be forgeable.

We have proposed two solutions to this problem. Both involve the use of one-way hash functions, whose outputs are processed in lieu of the actual documents, and of digital signatures. The solutions differ only in the way that the date and time are made unforgeable. In the first, the hashes of documents submitted to a TSS are linked together, and certificates recording the linking of a given document are distributed to other clients both upstream and downstream from that document. In the second solution, several members of the client pool must time-stamp the hash. The members are chosen by means of a pseudorandom generator that uses the hash of the document itself as seed. This makes it infeasible to deliberately choose which clients should and should not time-stamp a given hash. The second method could be implemented without the need for a centralized TSS at all.

Finally, we have considered whether time-stamping could be extended to enhance the authenticity of documents for which the time of creation itself is not the critical issue. This is the case for a large class of documents which we call “tamper-unpredictable.” We further conjecture that no purely algorithmic scheme can add any more credibility to a document than time-stamping provides.

Acknowledgements

We gratefully acknowledge helpful discussions with Donald Beaver, Shimon Even, George Furnas, Burt Kaliski, Ralph Merkle, Jeff Shrager, Peter Winkler, Yacov Yacobi, and Moti Yung.

References

- [1] J. Alter. When photographs lie. *Newsweek*, pp. 44-45, July 30, 1990.
- [2] M. Blum and S. Micali. How to generate cryptographically strong sequences of pseudo-random bits. *SIAM Journal on Computing*, 13(4):850-864, Nov. 1984.
- [3] G. Brassard and M. Yung. One-way group actions. In *Advances in Cryptology—Crypto ’90*. Springer-Verlag, LNCS, to appear.
- [4] I. Damgård. Collision-free hash functions and public-key signature schemes. In *Advances in Cryptology—Eurocrypt ’87*, pp. 203-217. Springer-Verlag, LNCS, vol. 304, 1988.
- [5] I. Damgård. A design principle for hash functions. In *Advances in Cryptology—Crypto ’89* (ed. G. Brassard), pp. 416-427. Springer-Verlag, LNCS, vol. 435, 1990.
- [6] A. DeSantis and M. Yung. On the design of provably secure cryptographic hash functions. In *Advances in Cryptology—Eurocrypt ’90*. Springer-Verlag, LNCS, to appear.
- [7] W. Diffie and M.E. Hellman. New directions in cryptography. *IEEE Trans. on Inform. Theory*, vol. IT-22, Nov. 1976, pp. 644-654.



Digital document time-stamping with catenate certificate

Patent number: 5136646

Abstract: A system for time-stamping a digital document, for example any alphanumeric, video, audio, or pictorial data, protects the secrecy of the document text and provides a tamper-proof time seal establishing an author's claim to the temporal existence of the document. Initially, the document may be condensed to a single number by means of a one-way hash function, thereby fixing a unique representation of the document text. The document representation is transmitted to an outside agency where the current time is added to form a receipt. The agency then certifies the receipt by adding and hashing the receipt data with the current record catenate certificate which itself is a number obtained as a result of the sequential hashing of each prior receipt with the extant catenate certificate. The certified receipt bearing the time data and the catenate certificate number is then returned to the author as evidence of the document's existence.

Type: Grant

Filed: March 8, 1991

Date of Patent: August 4, 1992

Assignee: Bell Communications Research, Inc.

Inventors: Stuart A. Haber, Wakefield S. Stornetta, Jr.

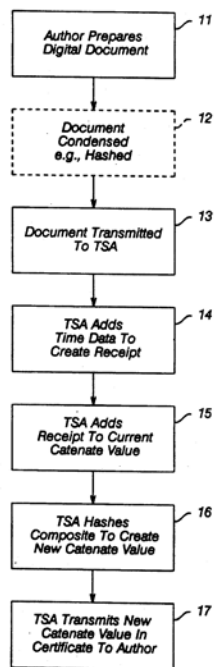


FIG. 1

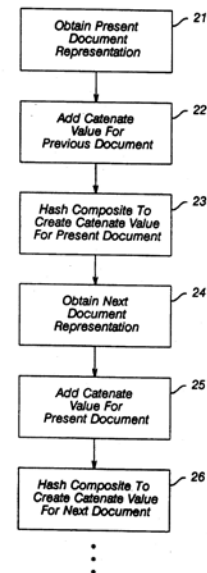
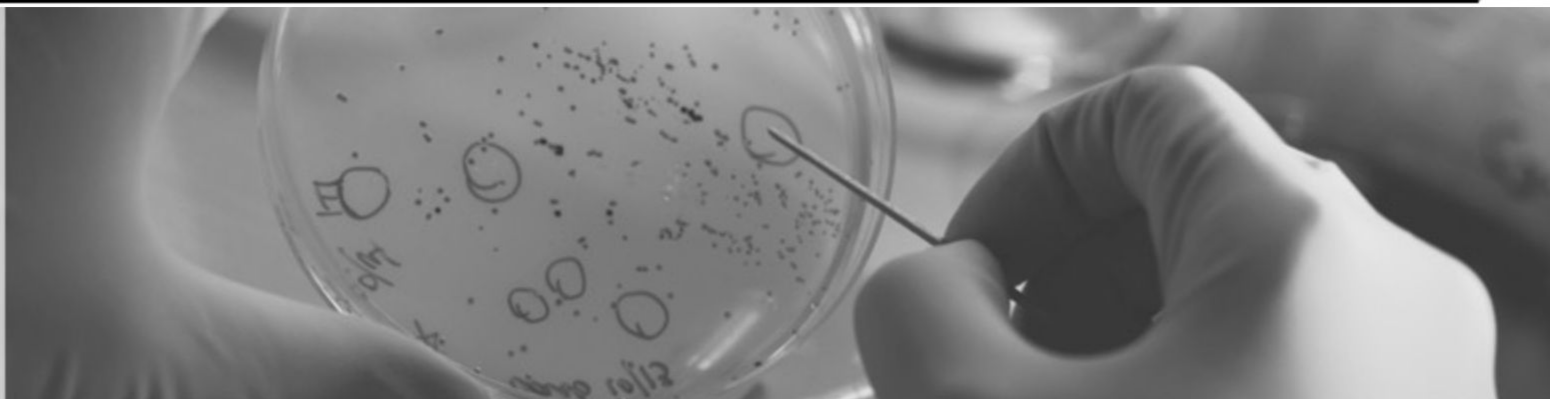


FIG. 2

[Home](#)[Nouveau](#)[Calendrier](#)[Contact](#)[Plan du site](#)

Banque de données projets FEDRA

[Presentation](#)[Actions de recherche](#)[Personnes](#)[Chercher](#)[Recherche et applications](#) > [Banque de données projets](#) > Banque de données projets FEDRA

TIMESEC - Time-Stamping Digital et l'évaluation des primitifs de protection

Projet de recherche NO/B/007 (Action de recherche [NO](#))

- [Description](#)
- [Documentation](#)

Personnes :

- [Prof. dr. PRENEEL Bart](#) - Katholieke Universiteit Leuven (K.U.Leuven)
Partenaire financé belge
Durée: 1/8/1996-31/7/1998
- [Prof. dr. QUISQUATER Jean-Jacques](#) - Université Catholique de Louvain (UCL)
Partenaire financé belge
Durée: 1/8/1996-31/7/1998

Description :

Contexte

Les services de Time-stamping sont un composant important pour la protection des services de télécommunication modernes, par exemple pour la conclusion de contrats électroniques, EDI (Electronic Data Interchange), la protection de IPR (Intellectual Property Rights), les services multimédia interactifs, etc. Les instances pour la standardisation travaillent actuellement à des solutions à cette problématique.

IMES DISCUSSION PAPER SERIES

**The Security Evaluation of Time
Stamping Schemes:
The Present Situation and Studies**

Masashi UNE

Discussion Paper No. 2001-E-18

IMES

**INSTITUTE FOR MONETARY AND ECONOMIC
STUDIES**

BANK OF JAPAN

C.P.O BOX 203 TOKYO
100-8630 JAPAN

Bitcoin: paper

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.

references:

References

- [1] W. Dai, "b-money," <http://www.weidai.com/bmoney.txt>, 1998.
- [2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In *20th Symposium on Information Theory in the Benelux*, May 1999.
- [3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of Cryptology*, vol 3, no 2, pages 99-111, 1991.
- [4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In *Sequences II: Methods in Communication, Security and Computer Science*, pages 329-334, 1993.
- [5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pages 28-35, April 1997.
- [6] A. Back, "Hashcash - a denial of service counter-measure," <http://www.hashcash.org/papers/hashcash.pdf>, 2002.
- [7] R.C. Merkle, "Protocols for public key cryptosystems," In *Proc. 1980 Symposium on Security and Privacy*, IEEE Computer Society, pages 122-133, April 1980.
- [8] W. Feller, "An introduction to probability theory and its applications," 1957.

ethereum.org



openzeppelin



[Sign in](#) / [Sign up](#)



Manuel Aráoz

[Follow](#)

Aug 16, 2016 · 12 min read

Onward with Ethereum Smart Contract Security



Never miss a story from **OpenZeppelin**, when you sign up for Medium. [Learn more](#)

[GET UPDATES](#)

Redo!

- Voting: was one of the first example of use of blockchains (Benaloh, 1991)
- Now:
bitcoin+blockchain+ethereum+openzeppelin!
- aso

research

- Network (latency, ...)
- Cryptography (quantum computers?)
- Protocols
- Hardware
- Software
- Proofs of security (dynamic, long-term)
- Scalability
- Variants
- Combined blockchains
- Flexibility
- Proofs of work, ressources, ...
- resilience
- ...



Let's play it!

- Nous pouvons vous aider ...