



Zero-knowledge protocols, blockchains, e-cash: a history

Jean-Jacques Quisquater

UCL, Louvain-la-Neuve, jjq@uclouvain.be

MIT : research affiliate CSAIL, jjq@mit.edu

Math Ri**ZK**, director

Played by Claude Crépeau (Thanks!)

Jean-Jacques Quisquater

- Ingénieur en math appliquées (UCL)
- PhD in computer science (Orsay, LRI)
- Philips Research: durant 20 ans
- UCL, professeur en cryptographie: durant 20 ans après
- 20 brevets dont GQ
- Introduction crypto forte (DES, RSA) dans la carte à puce
- ISO : éditeur principal de la première norme de signature digitale
- Projet initial sur les blockchains (voir plus loin) : 1996
- Enseignant ENS, rue d'Ulm, en cryptographie (1991-2002)
- 250 publications en cryptographie, sécurité, ...
- Actuellement formateur, conseiller pour start-up et consultant
- Impliqué en ce moment dans 4 ICO avec blockchains (pas académique)

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

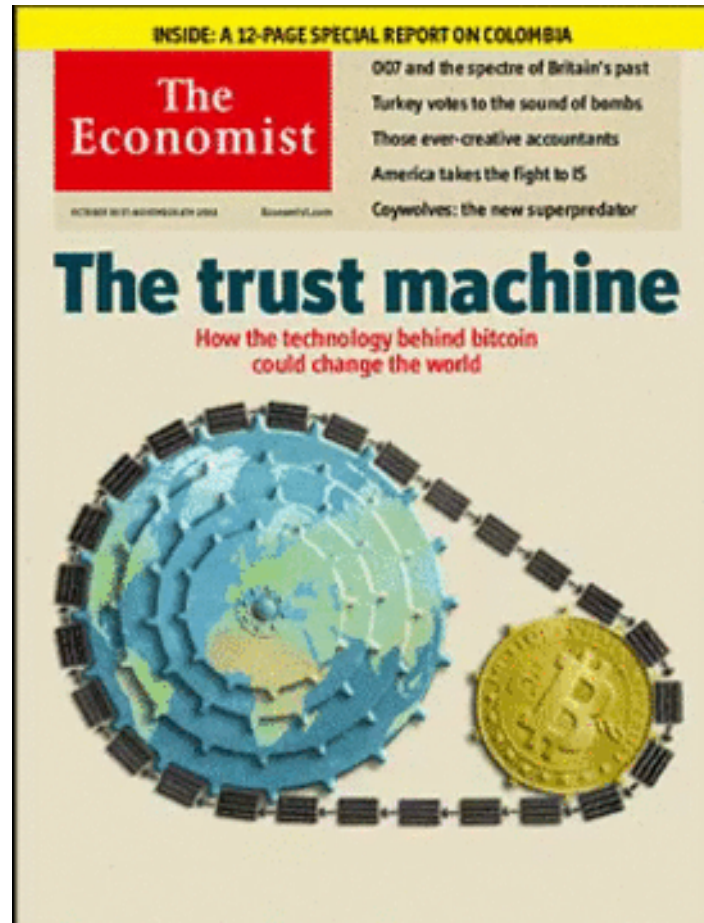
Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible 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.

Blockchain?

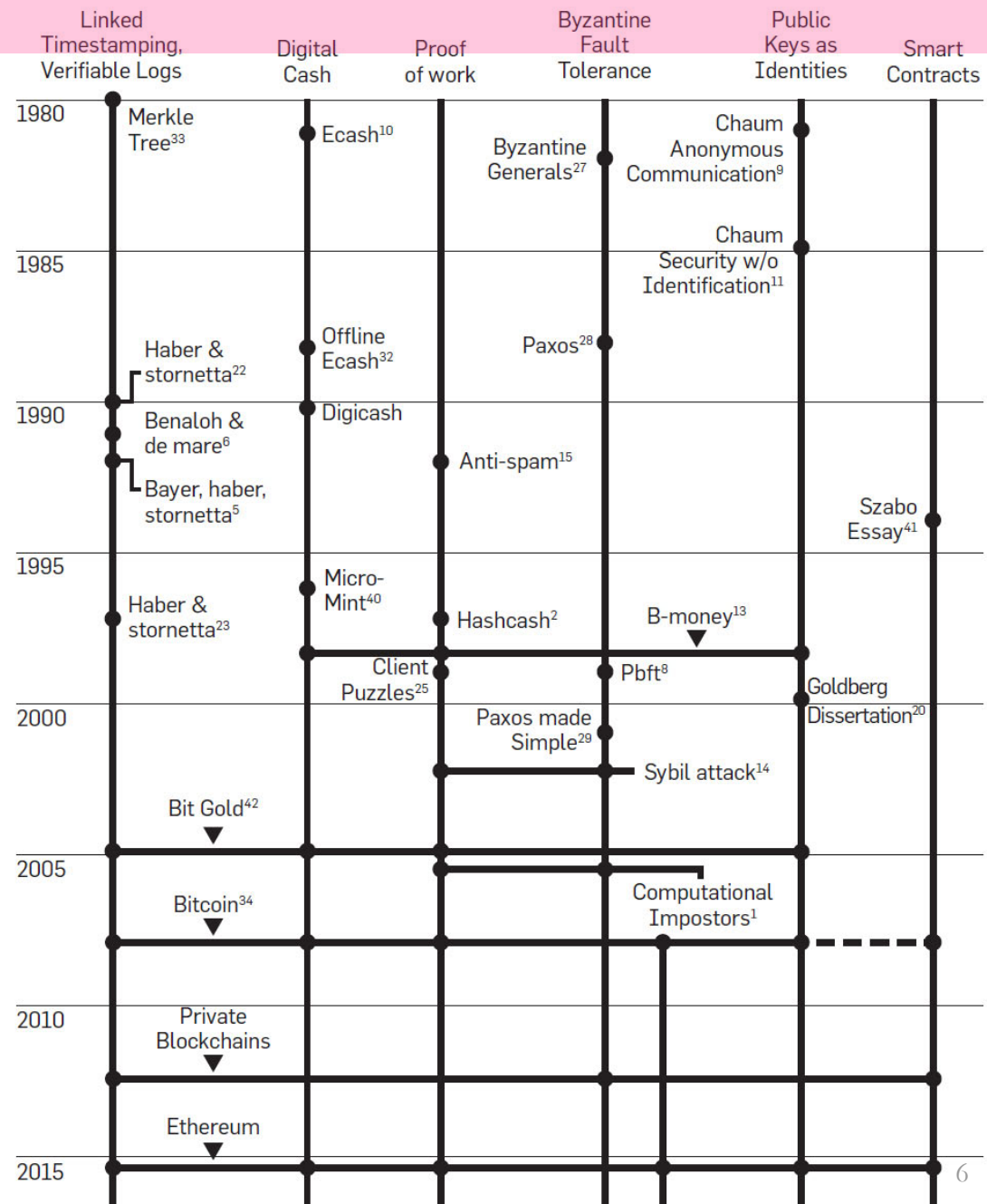
- Satoshi Nakamoto is not using at all the word « blockchain »: only one time chain of blocks ...
- Who was the first to use it? I don't know ...

The beginning of blockchains: this cover!



The story to bitcoin is long, unknown, incomplete

...



Identity of a file (Merkle)

- Use of a function (algorithm, recipe, ...) with very special properties,
- Function of cryptographic hash (one-way function),
- Known long time ago (Jevons, 1874), and first based on factorisation! It is easy to multiply two integer numbers but it is complicated knowing only the result to recover the two initial numbers (in general).

Proof of work (PoW), and others

- Dwork and Naor (1993) :

Pricing via Processing or Combatting Junk Mail*

Cynthia Dwork * Moni Naor †

Abstract

We present a computational technique for combatting junk mail, in particular, and controlling access to a shared resource, in general. The main idea is to require a user to compute a moderately hard, but not intractable, function in order to gain access to the resource, thus preventing frivolous use. To this end we suggest several *pricing functions*, based on, respectively, extracting square roots modulo a prime, the Fiat-Shamir signature scheme, and the Ong-Schnorr-Shamir (cracked) signature scheme.

*A Preliminary version of this paper was presented at Crypto'92.

*IBM Research Division, Almaden Research Center, 650 Harry Road, San Jose, CA 95120. E-mail: dwork@almaden.ibm.com.

†Incumbent of the Morris and Rose Goldman Career Development Chair, Dept. of Applied Mathematics and Computer Science, Weizmann Institute of Science, Rehovot 76100, Israel. Most of this work performed while at the IBM Almaden Research Center. Research supported by an Alon Fellowship and a grant from the Israel Science Foundation administered by the Israeli Academy of Sciences. E-mail: naor@wisdom.weizmann.ac.il.

E-cash: the idea is first in sci-fi book(s)

- "La nuit des temps" : René Barjavel (1968) ...
 - See also "La sphère d'or" by Erle Cox (1919-1925),
- Used by Roland Moreno, etc (1973) for the first "smart" cards,



E-cash: David Chaum: 1981 (CACM)

Fundamental paper:

- "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms"
 - Tor, e-cash, privacy, ... using cryptography,
 - Set the right problem: avoiding the double spending,
- Found a solution (if you use twice a token you're giving your secret key and you lost everything),
- European project CAFÉ (1989 ...) : used a secure smart card with cryptographic processor (I did the design) as a trusted-third-party,
- Digicash : a long story in Amsterdam.

The ESPRIT Project CAFÉ

ESORICS 94 (Third European Symposium on Research in Computer Security), LNCS 875, Springer-Verlag, Berlin 1994, 217-230

The ESPRIT Project CAFÉ — High Security Digital Payment Systems —[†]

Jean-Paul Boly¹, Antoon Bosselaers², Ronald Cramer³, Rolf Michelsen⁴,
Stig Mjølhusnes⁴, Frank Müller¹, Torben Pedersen⁵, Birgit Pfizmann⁶,
Peter de Rooij¹, Berry Schoenmakers³, Matthias Schunter⁶, Luc Vallée⁷,
Michael Waidner^{6,8}

Abstract. CAFÉ ("Conditional Access for Europe") is an ongoing project in the European Community's ESPRIT program. The goal of CAFÉ is to develop innovative systems for conditional access, and in particular, digital payment systems. An important aspect of CAFÉ is high security of all parties concerned, with the least possible requirements that they are forced to trust other parties (so-called multi-party security). This should give legal certainty to everybody at all times. Moreover, both the electronic money issuer and the individual users are less dependent on the tamper-resistance of devices than in usual digital payment systems. Since CAFÉ aims at the market of small everyday payments that is currently dominated by cash, payments are offline, and privacy is an important issue.

The basic devices used in CAFÉ are so-called electronic wallets, whose outlook is quite similar to pocket calculators or PDAs (Personal Digital Assistant). Particular advantages of the electronic wallets are that PINs can be entered directly, so that fake-terminal attacks are prevented. Other features are:

- Loss tolerance: If a user loses an electronic wallet, or the wallet breaks or is stolen, the user can be given the money back, although it is a prepaid payment system.
- Different currencies.
- Open architecture and system.

The aim is to demonstrate a set of the systems developed in one or more field trials at the end of the project. Note that these will be real hardware systems, suitable for mass production.

This paper concentrates on the basic techniques used in the CAFÉ protocols.

Keywords: Security in Applications (Financial); Security Versus other Requirements (Performance, Fault Tolerance).

[†] A preliminary version of this paper was presented at Securicom '94, Paris, June 1994 [BBCM 94].

¹ PTT Research, P.O. Box 421, NL-2260 AK Leidschendam, the Netherlands

² Katholieke Universiteit Leuven, Dept. Elektrotechniek E.S.A.T., Kardinaal Mercierlaan 94, B-3001 Heverlee, Belgium

³ CWI, Krusslaan 413, NL-1098 SJ Amsterdam, the Netherlands

⁴ SINTEF-DELAB, O.S. Bragstads Plass, N-7034 Trondheim, Norway

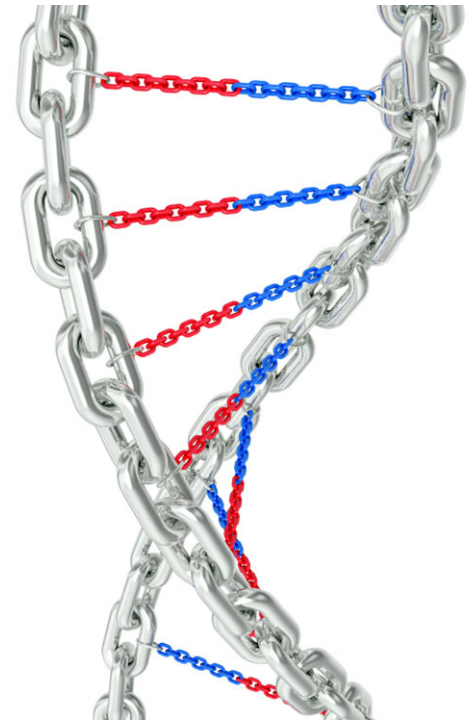
⁵ Aarhus Universitet, Matematisk Institut, Ny Munkegade, DK-8000 Aarhus C, Denmark

⁶ Universität Hildesheim, Institut für Informatik, Postfach 101363, D-31113 Hildesheim, Germany

⁷ SEPT, 42 rue des Coutures, BP 6243, F-14066 Caen Cedex, France

⁸ Universität Karlsruhe, Institut für Rechnerentwurf und Fehlertoleranz, Postfach, D-76128 Karlsruhe, Germany

The early history of blockchains



Derivative work. Original by Scott Adams. www.dilbert.com



Original © 2003 United Feature Syndicate, Inc.



Timestamping ("horodatage", "estampillage" in french)

- Old problems
- *"le cachet de la poste faisant foi" !!!*
 - No law or rule about that!
 - See <https://www.arcep.fr/index.php?id=12335> and this citation ...
 - « en France, aucune disposition juridique n'impose aux prestataires de services postaux l'obligation d'apposer un cachet postal sur les plis qu'ils acheminent. De même, aucun texte ne définit la notion de « cachet de la poste », ni ne précise les mentions qu'il doit comporter pour apporter une sécurité juridique suffisante. »,
 - the concept of hour and date is not simple ☺ see https://fr.wikipedia.org/wiki/ISO_8601
- Synchronisation of schedules of trains (stations = local solar hour at the beginning): Einstein, was thinking about that (really!) and it was restricted relativity, and then ... the GPS !

Time: synchronization (schedules of trains)

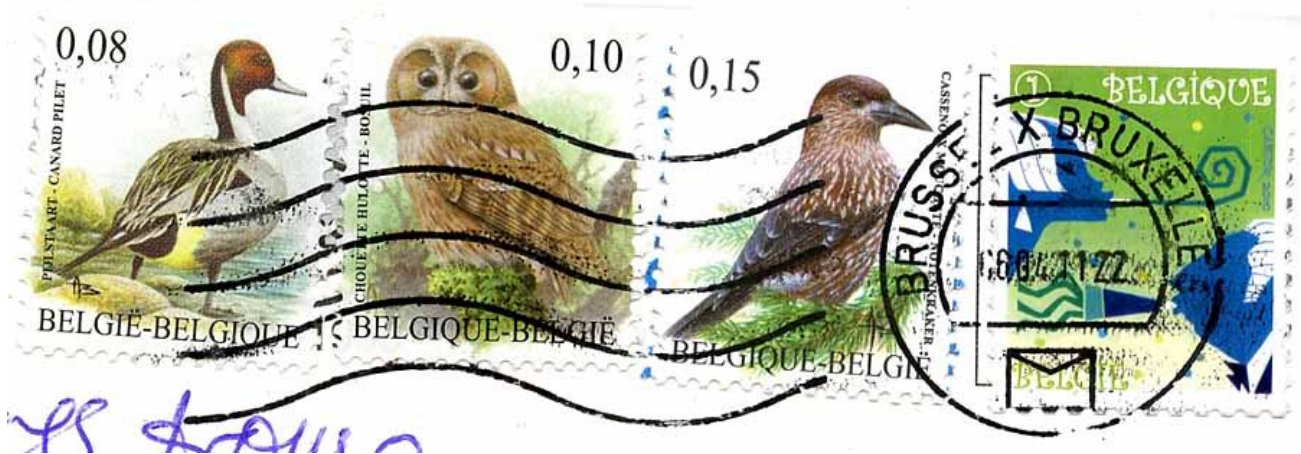
Peter Galison
**L'empire
du temps**

Les horloges d'Einstein
et les cartes de Poincaré

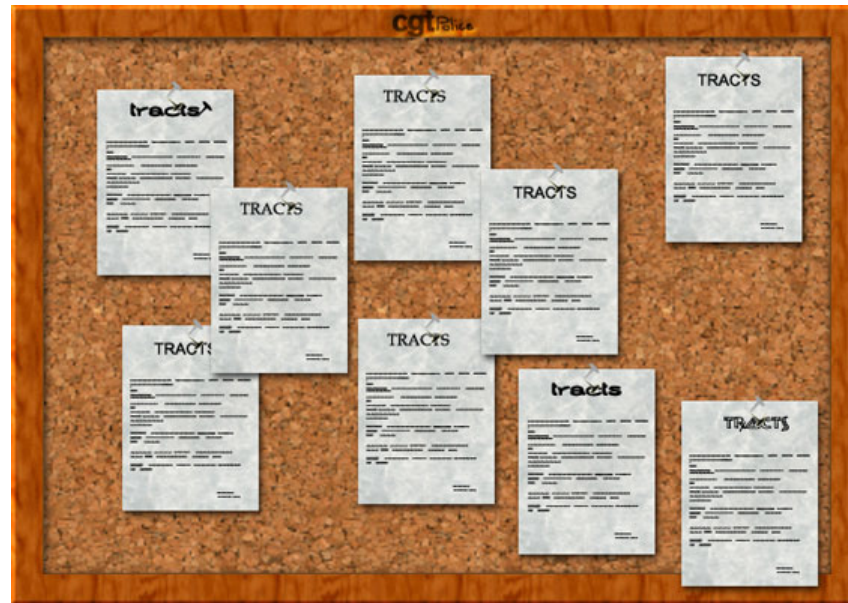


folio **essais**

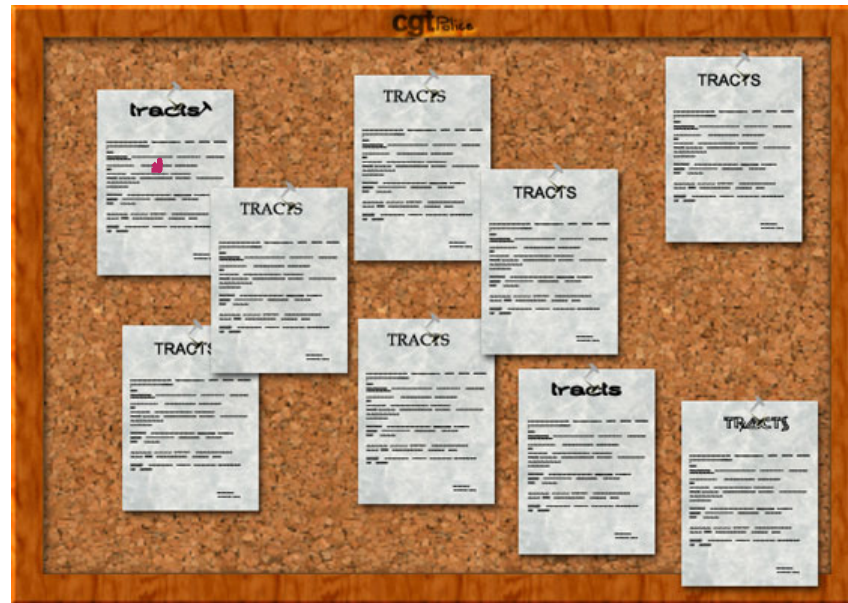
« Cachet de la poste faisant foi »
(illisible is not a problem for the post
office because there is no rule!)



Example of a (public): ledger how to know the order of operations?



Example of a (public): ledger
how to know the order of
operations? Add a chain.



A more secure one (order?)



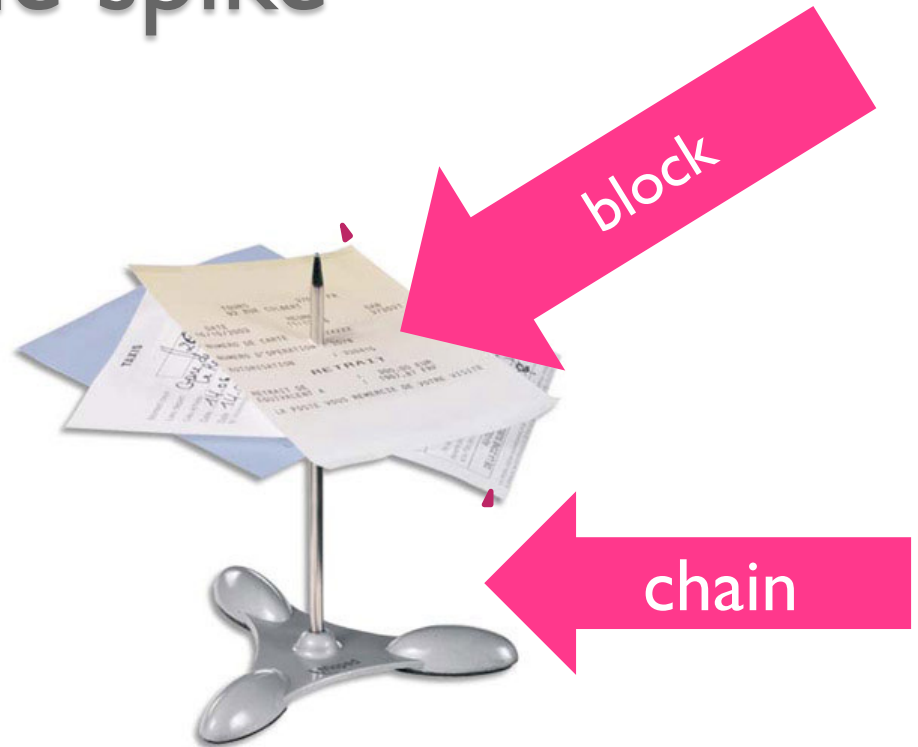
digitalisation

- How to name a file (binary) ? Associate the hash of the content,
- Use of a hash function (cryptographic)
- Special function easy to compute, very complicated to inverse.

Spike file and blockchain



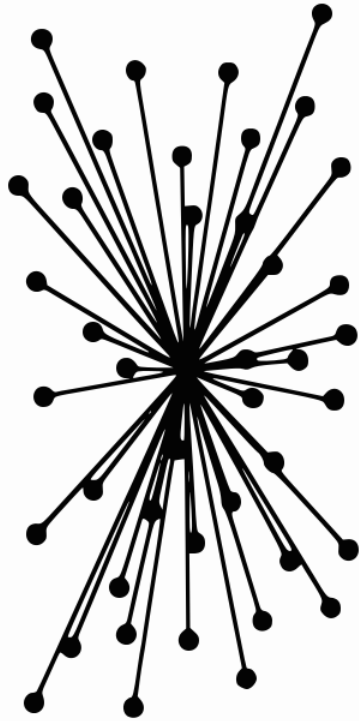
message or file spike



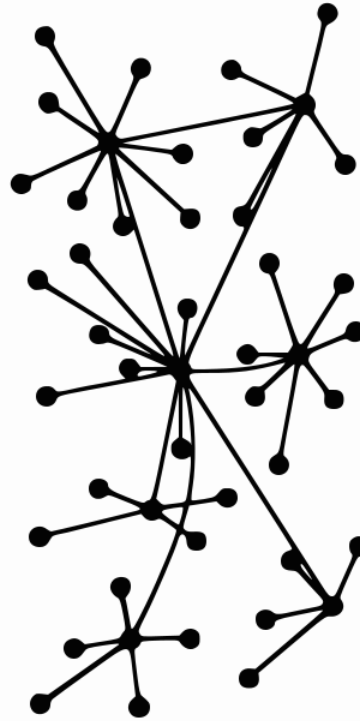
More secure ones



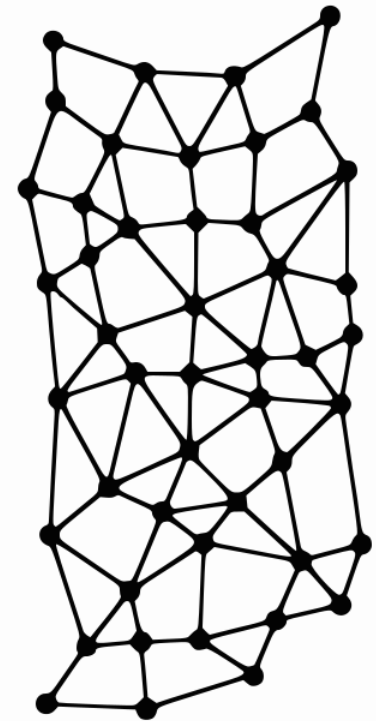
Choice for internet (1963: Baran)



Centralized

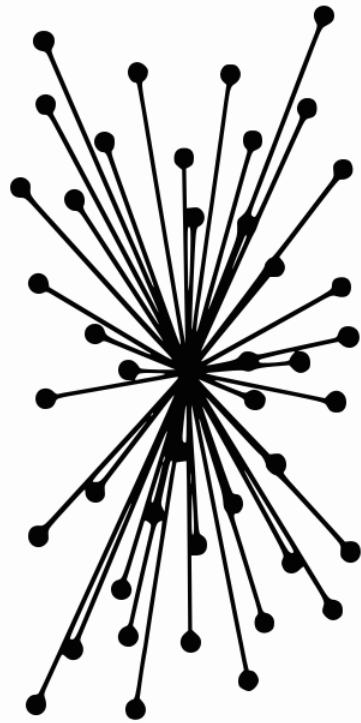


Decentralized

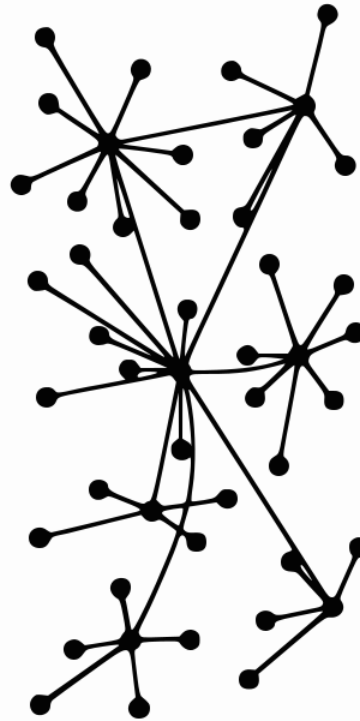


Distributed

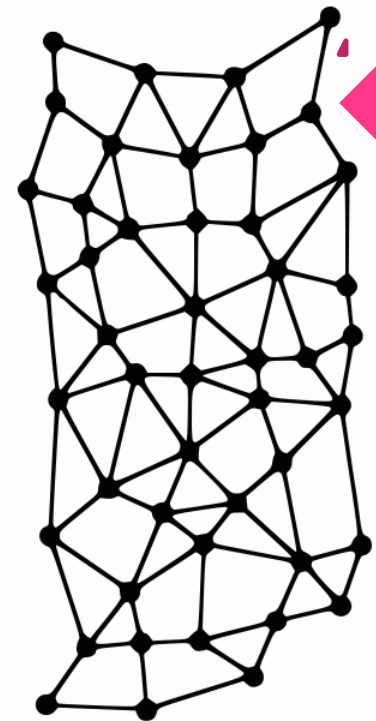
Choice for internet (1963: Baran)



Centralized



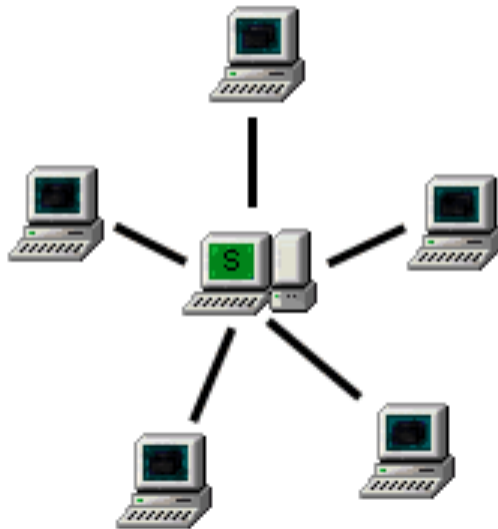
Decentralized



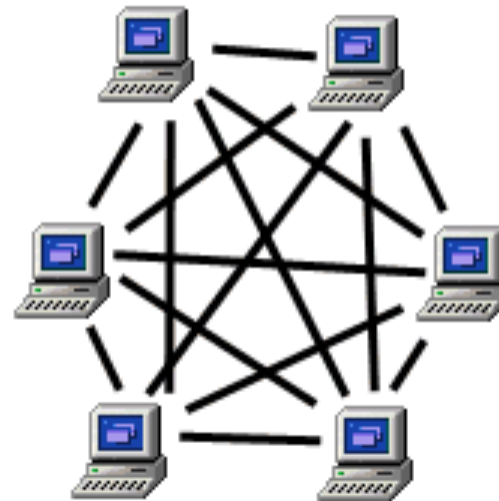
Distributed

Peer to peer ("virtual")

Server Based Network



Peer to Peer Network



The inventors: Haber and Stornetta

[1] S. Haber, W. S. Stornetta: “*How to time-stamp a digital document*”, Journal of Cryptology, January 1991, Vol. 3, Issue 2, pp 99–111 (first presented at CRYPTO '90). (see also patent US 5136647 A).

Two solutions: one with TTP, the other one decentralized (= nearly the blockchain of bitcoin).

[2] J. Benaloh, M. de Mare: “Efficient Broadcast Time-Stamping”, TR from Clarkson University, 1991/1992.

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.

Patents (no longer valid)

JUSTIA Patents

[Log In](#)

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.

Then voting: 1991: Josh Benaloh-de Mare

- With reference to the work of Stuart Haber
- Then there was "The Chinese Lotto"
(also 1991: an early proof of work, by JJQ and Yvo Desmedt),
- Then the Belgian TIMESEC project ...

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

Banque de données projets FEDRA

[Présentation](#)[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

Belgian project TIMESEC: 1996-1998

- With the support of Stuart Haber,
- Implementing his ideas and improving it also by implementations and tests,
- Two servers, but in theory many ones,
- Also using 2 hash functions in parallel, Merkle trees, accumulators, aso,
- ISO: yes we proposed the use of blockchains to ISO-IEC WD 18104 (SC27)
- IETF ([Internet Engineering Task Force](#)): yes we proposed there the use of blockchains in 1997!


Some public references

- [MAQ99a] H. Massias, X. Serret Avila, and J.-J. Quisquater. Design of a secure timestamping service with minimal trust requirements. In A. Barbé, E.C. van der Meulen, and P. Vanroose, editors, *Twentieth Symposium on Information Theory in the Benelux*, pages 79–86, May 1999.
- [MAQ99b] H. Massias, X. Serret Avila, and J.-J. Quisquater. Timestamps: Main issues on their use and implementation. Accepted at Wet Ice '99, Stanford CA, June, 1999.
- [Mas98] H. Massias. A survey of accumulators. Technical report, UCL Crypto Group Technical Report, February 1998.
- [MQ97] H. Massias and J.-J. Quisquater. Time and cryptography. Technical report, TIMESEC Project (Federal Gouvernement Project, Belgium), 1997. Available at <http://www.dice.ucl.ac.be/crypto/TIMESEC.html>.
- [PRQ⁺98] B. Preneel, B. Van Rompay, J.-J. Quisquater, H. Massias, and X. Serret Avila. Design of a timestamping system. Technical report, TIMESEC Project (Federal Gouvernement Project, Belgium), 1998. To be available at <http://www.dice.ucl.ac.be/crypto/TIMESEC.html>.

Nothing really new! We proposed to study scalability, granularity ...

7 Conclusion

As we explained, the problem of securely timestamping documents is not as easy as it seems. The lifetime of the crypto-algorithms used to define a timestamping system must be carefully studied. A value associated with a time must be published somewhere in an unmodifiable media in order to be trusted by all the possible verifiers. The place and frequency of this published round value influences directly the trust and granularity provided by the timestamps. The dependency on this published value is the major brake for the scalability of the timestamping system, which must be further investigated.

- 
- In 2001 there was a report from the bank of Japan,
 - Study of 7 timestamping systems including TIMESEC,
 - Set the practical problem of distributed consensus, and, in some sense, it was a call for constructing something like bitcoin.

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

Blockchain here ...

completely and therefore find it hard to manipulate a time stamp. However, just as in the case of the linking scheme, a distributed scheme system is more complicated than a simple scheme. For example, the time signature distributed system (Takura et al. [1998]) belongs to this category, and Ansper et al. [2001] proposed a scheme possessing the characteristics of both the linking and distributed schemes. The main strengths and limitations of these schemes are summarized in Table 1.

Table 1 Main Strengths and Limitations of Three Schemes

Schemes	Strengths	Limitations
simple scheme	The system is relatively simple.	It is necessary to assume that the issuer is the trusted third party.
linking scheme	The assumption that the issuer is the trusted third party is rendered unnecessary, for example, by the periodical publication of a part of a chain of time stamps.	The system is relatively complicated because additional operations for linking all time stamps are needed.
distributed scheme	The assumption that the issuers are the trusted third parties is rendered unnecessary by sharing the secret data among multiple issuers.	The system is relatively complicated because multiple issuers generate a time stamp cooperatively.

The classification described above is also adopted in standardization activities relating to a time stamping service. A working draft of ISO/IEC 18014 (Time stamping services, ISO/IEC [2001]) includes the following two types of scheme: "mechanisms producing independent tokens" and "mechanisms producing linked tokens." These correspond to the simple and linking schemes, respectively. On the other hand, ISO/IEC 13888 (Non-repudiation, ISO/IEC [1997]) and IETF PKIX



Who are these authors?

- Une, Masshi, and Tsutomu Matsumoto,



- The author of bitcoin is:
 - Satshi Nakamoto,
- Curious coincidence!?
- Better, **Satoshi** is a reference:
 - Takura, Akira, Satoshi Ono and Shozo Naito

Who is Masashi UNE?

- Majored in *experimental economy*!
- Research subjects: *cryptography linked to financial services*,
- Related to cryptographic systems of distributed chaining and trusted!

Bitcoin: paper again

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshi@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.

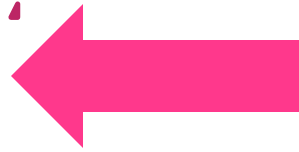
What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, 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.

- The inventor of bitcoin knows very well this story.
- Out of 8 references 5 references are Haber, Merkle, and ... JJQ.
- Thanks to him. Curiously Satoshi cites the less known paper from an unknown conference (40 participants) in Benelux ... Was he there?

References of the bitcoin paper:

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.



Question: why invented so early without use?

- People didn't think it was important,
- People didn't understand very well the concept of distributed computation (that is, peer-to-peer) and then waiting for bittorrent, gnutella and napster, ...
- Then bitcoin was coming! And people saw the blockchain inside.

More! We introduced
an ISO project going
to a

Standard ISO: 2004-
2009-2014 ...2019
Yes linked tokens is
blockchain (so
standard from 2004)



perspectives

- Be careful with smart contracts (language solidity too powerful!)
 - Models for contracts (limited)
 - Analyzers: not mature ...
 - Trust about a contract (notary again?)?
- Proof of work (aso): also proof of speed (ammbr.com)
- Avoid strong or fast standardization
 - Everybody is doing it: ENISA, IETF, NIST, ...
- Evolution of security: we don't know all the attacks
- Evolution of cryptography:
 - Strong enough primitives?
 - Quantum computers
 - NSA and NIST
- Research continues: Cryptology ePrint Archive: Report 2017/775 Proofs of Work for Blockchain Protocols

Marwa Chaieb, Souheib Yousfi, Pascal Lafourcade, Riadh Robbana
- Well-known solutions for blockchains exist, see ...

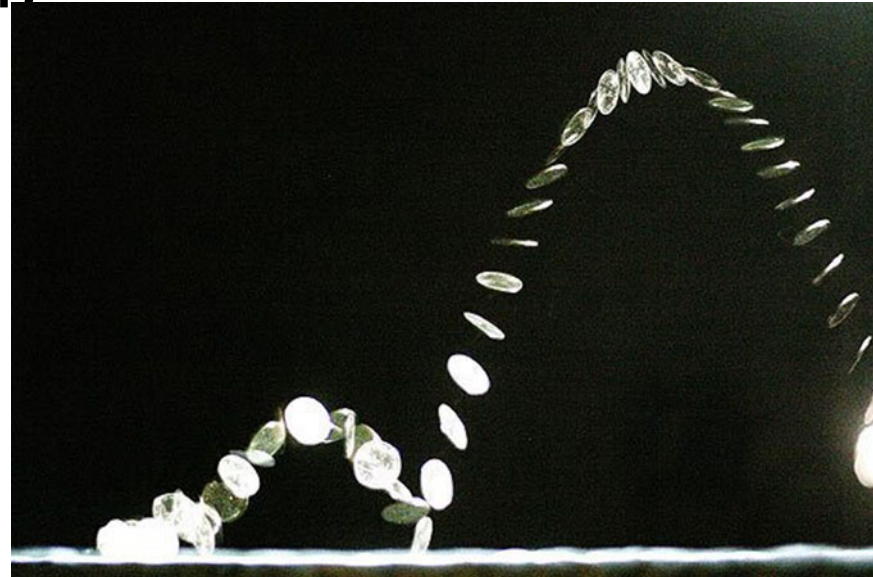
Juan A. Garay and Aggelos Kiayias and Giorgos Panagiotakos
- Snake oil (see other presentation)

standards

- IETF: <https://trac.ietf.org/trac/irtf/wiki/blockchain-federation> (DINRG)
- ENISA: <https://www.enisa.europa.eu/news/enisa-news/enisa-report-on-blockchain-technology-and-security>
- W3C: <https://www.w3.org/community/blockchain/>
- NIST: <https://github.com/usnistgov/Blockchain>
- NB: <https://www.internationalairportreview.com/news/33288/7-principles-blockchain-wave/>

ZK: What we need

- commitments (coin-flipping),
- zero-knowledge (general idea, proof of graph isomorphism)



Problem of identification

- How to do that?
 - How secure is it?
 - Better?
-
- Who is Alice, Peggy, ... and others?
 - Remotely.

Access control (login: Baran, 1963)

User (prover)
visitor
driver
card

Computer (verifier)
warden
car
terminal



- ☹ spy (on-line)
- ☹ fake prover (copy or false identity)
- ☹ fake verifier
- ☹ database of users and passwords (hash or ?)

Problems: prover side

- Copy of the password (stealing, coercion, radiations, ...), and use in another context,
- Spying during the communication, ...

Problems: verifier side

- Terminal side: (fake terminal, coercion, radiations, ...),
- Several terminals for verification,
- How to verify? Need of some initial reference!

Better?

- One-time password! Any copy is not useful anymore,
- Solution: don't use the password!
- Implementations!

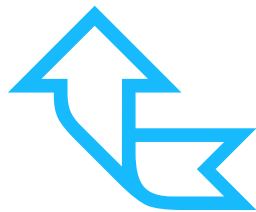
solutions

User (prover)
visitor
driver
card

Computer (verifier)
warden
car
terminal

PROVER

VERIFIER



solutions

User (prover)
visitor
driver
card

■

PROVER

CE *proof of
possession of
password*



Computer (verifier)
warden
car
terminal



solutions

User (prover)
visitor
driver
card

PROVER

Computer (verifier)
warden
car
terminal

VERIFIER

CE *proof of
possession of
password*

② *new proof for
each interaction*



solutions

User (prover)
visitor
driver
card

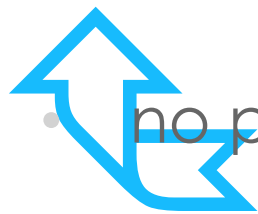
PROVER

Computer (verifier)
warden
car
terminal

VERIFIER

⌘ *proof of
possession of
password*

② *new proof for
each interaction*

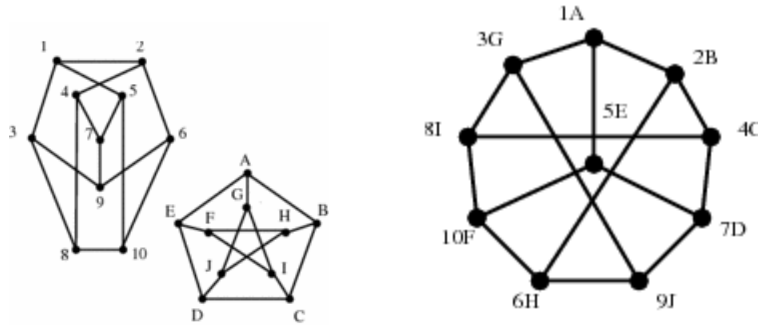


- no possible copy of password (always inside) and tamperresistant object

Smart cards

- Physically secure object (permanent memory, ...),
- Computing power for cryptography,
- Related to people (biometry?, possession, ...)

Graph isomorphism



a mapping f of the vertices of g to the vertices of h such that g and h are identical, i.e. (x,y) is an edge of g iff $(f(x),f(y))$ is an edge of h .

What is a Zero- Knowledge Proof?

A **zero-knowledge proof** is a way that a “**prover**” can prove possession of a certain piece of information (bits) to a “**verifier**” without revealing it.

This is done by manipulating data provided by the verifier in a way that would be impossible without the secret information in question.

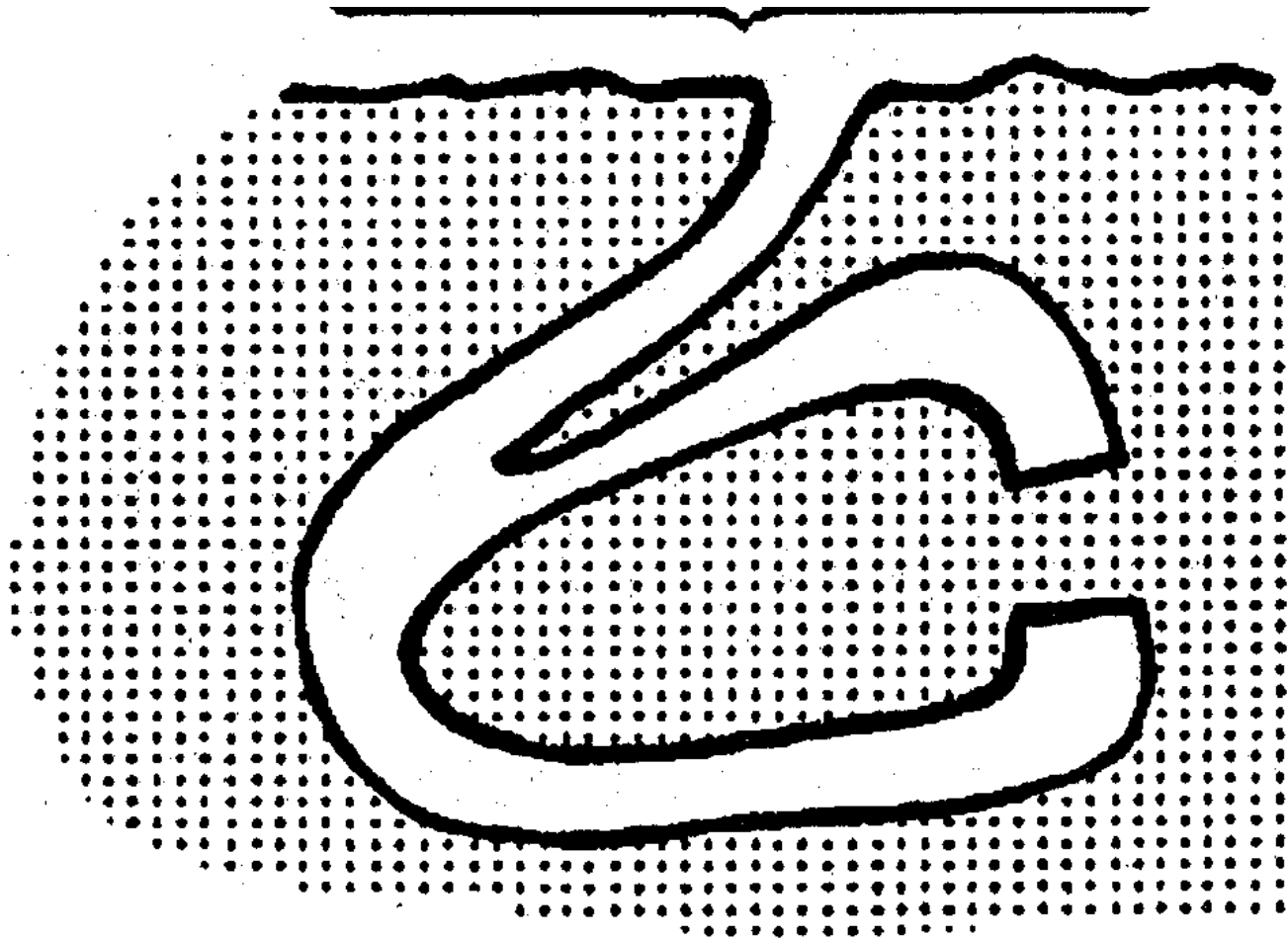
A third party, reviewing the transcript created, cannot be convinced that either prover or verifier knows the secret.

Proof of possession of password

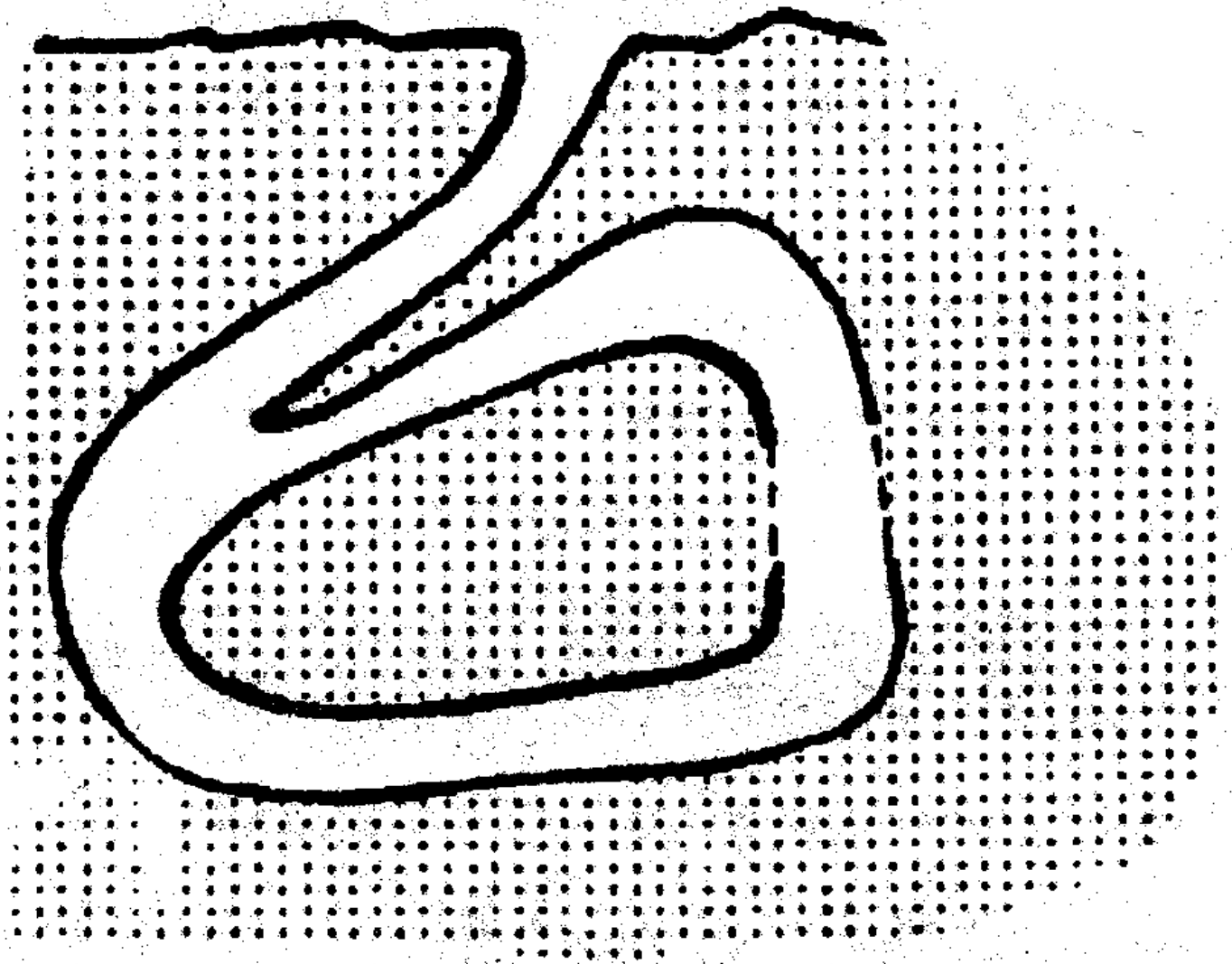
- Protocols zero-knowledge (Fiat-Shamir, GQ, ...)
- Only using the password in an internal computation
- Verification of the proof is very specific

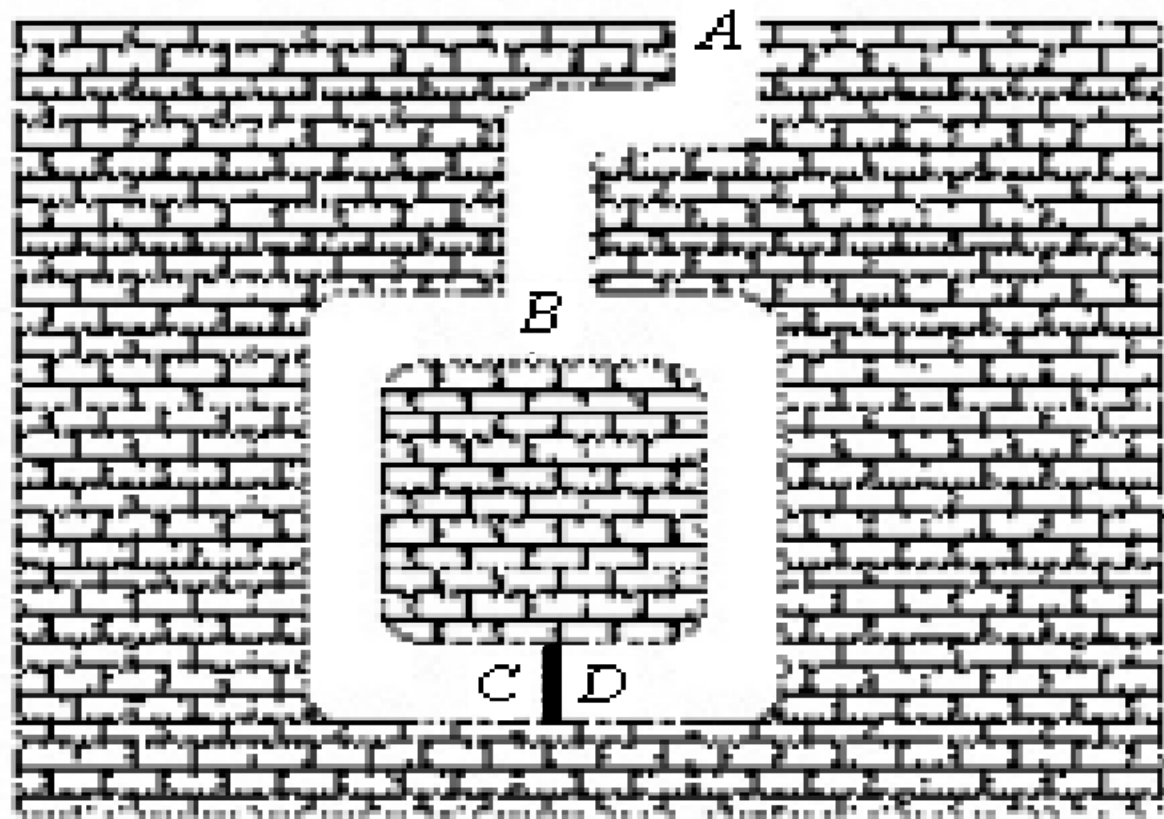


The Cave of the Forty Thieves (Ali-Baba)



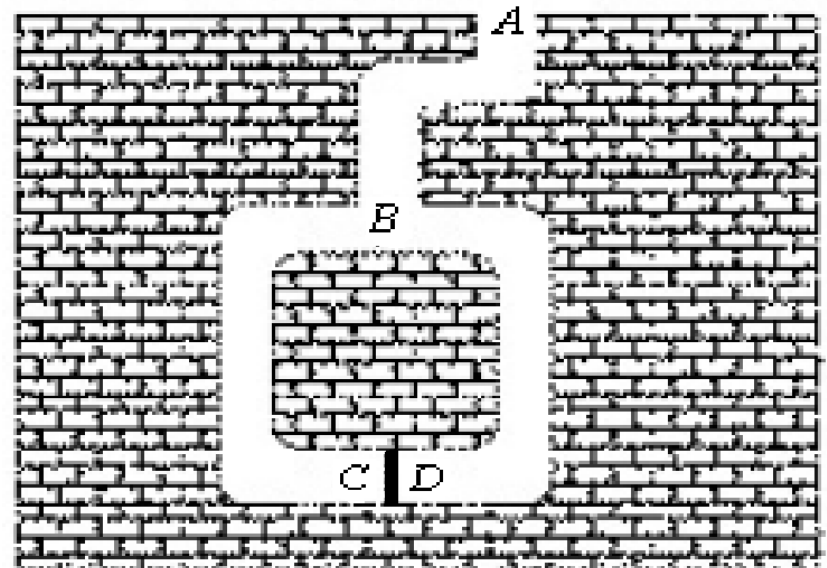
The Cave of the Forty Thieves





Peggy knows the secret of the cave. She wants to prove her knowledge to Victor, but she doesn't want to reveal the magic words. Here's how she convinces him:

- (1) Victor stands at point *A*.
- (2) Peggy walks all the way into the cave, either to point *C* or point *D*.
- (3) After Peggy has disappeared into the cave, Victor walks to point *B*.





(4) Victor shouts to Peggy, asking her either to:

(4.1) come out of the left passage or

(4.2) come out of the right passage.

(5) Peggy complies, using the magic words to open the secret door if she has to.

(6) Peggy and Victor repeat steps (1) through (5) n times.

Comment.

The technique used in this protocol is called cut and choose, because of its similarity to the classic protocol for dividing anything fairly:

- (1) Peggy cuts the thing in half.
- (2) Victor chooses one of the halves for himself.
- (3) Peggy takes the remaining half.

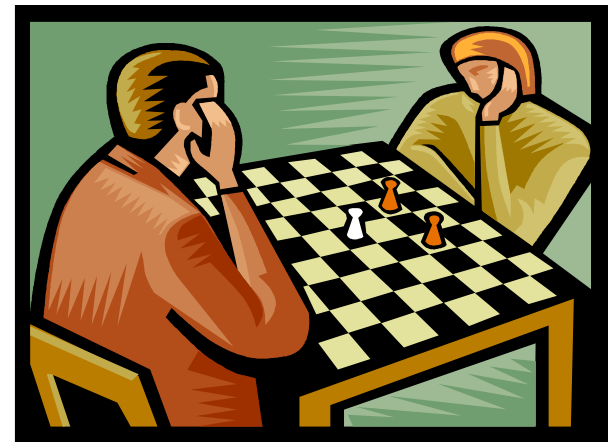
It is in Peggy's best interest to divide fairly in step (1), because Victor will choose whichever half he wants in step (2).

Applications

- Zero-knowledge proofs can be applied where secret knowledge too sensitive to reveal needs to be verified
- Key authentication
- PIN numbers
- Smart cards

Limitations

- A zero-knowledge proof is only as good as the secret it is trying to conceal
- Zero-knowledge proofs of identities in particular are problematic
- The Grandmaster Problem
- The Mafia Problem
- etc.



GQ protocol (1988)

- **System Parameters**

- Private: $p, q, s = v^{-1} \bmod \phi(n)$
- $n = pq, v > 2$

- **User Parameters**

- The secret of A with $J_A = f(I_A)$ is $J_A^{-s} \bmod n$

- **Protocol Messages** (*Repeat t times*)

- A sends to B(Commit): $I_A, x = r^v \bmod n$ for a random r
- B sends to A(Challenge): a random e with $1 \leq e \leq v$
- A sends to B(Response): $y = r s_A^e \bmod n$

- **Verify**

- B computes $z = J_A^e y^v \bmod n$
- Accept A's proof of identity if $z = x$ and $z \neq 0$

References

- Blum, M., “How to Prove a Theorem So No One Else Can Claim It”, Proceedings of the International Congress of Mathematicians, Berkeley, California, 1986, pp. 1444-1451
- Camenisch, J., M. Michels, “Proving in Zero-Knowledge that a Number is the Product of Two Safe Primes”, Eurocrypt '99, J. Stern, ed., Lecture Notes in Computer Science 1592, pp. 107-122, Springer-Verlag 1999
- Cramer, R., I. Dămgård, B. Schoenmakers, “Proofs of Partial Hiding and Simplified Design of Witness Hiding Protocols”, Advances in Cryptology – CRYPTO '94, Lecture Notes in Computer Science 839, pp. 174-187, Springer-Verlag, 1994
- De Santis, A., G. di Crescenzo, G. Persiano, M. Yung, “On Monotone Formula Closure of SZK”, Proceedings of the 35th Symposium on the Foundations of Computer Science, pp. 454-465, IEEE, 1994
- Feigenbaum, J., “Overview of Interactive Proof Systems and Zero-Knowledge”, Contemporary Cryptology, G.J. Simmons, ed., pp. 423-440, IEEE Press 1992
- Quisquater, J.J., L. Guillou, T. Berson, “How to Explain Zero-Knowledge Protocols to Your Children”, Advances in Cryptology - CRYPTO '99, Lecture Notes in Computer Science 435, pp. 628-631, 1990
- Stinson, D.R., Cryptography: Theory and Practice, CRC, 1995