

# Demystifying Bitcoin



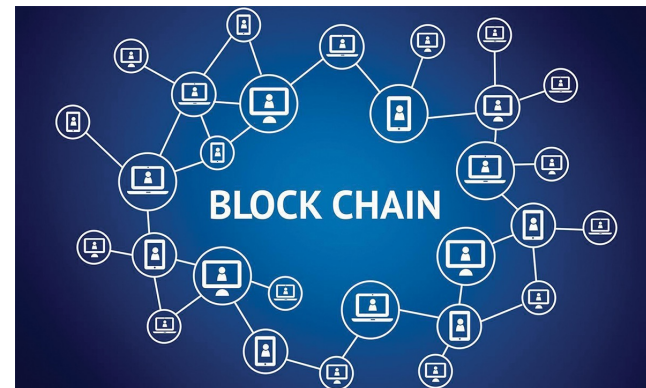
Prof R. Guerraoui EPFL

# Cryptocurrency

☛ Virtual currency



☛ Virtual bank (decentralized)





# Perspectives

☞ **(1) The journalist**

☞ **(2) The user / participant**

☞ **(3) The designer / scientist**



# 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

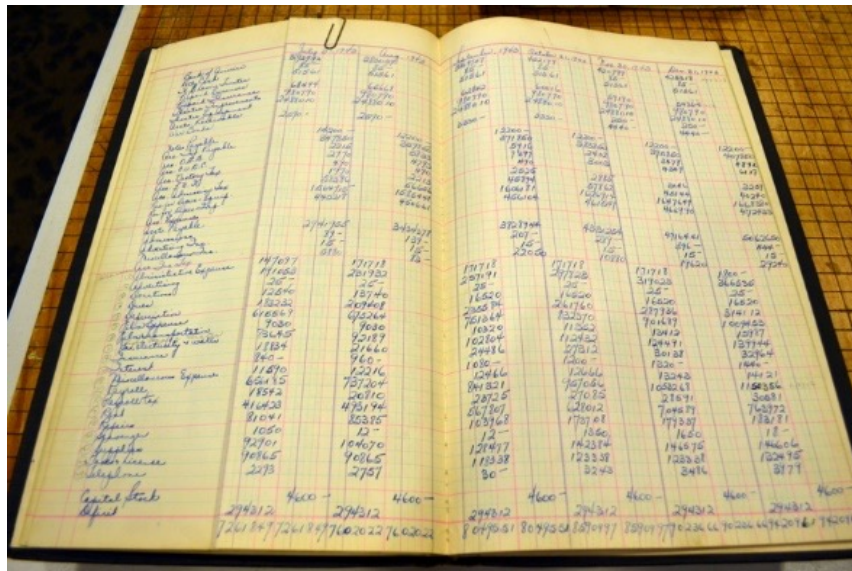
👉 **2008: Financial crisis – Nakamoto (1/21m)**

● **From 1c to 66000\$**

👉 **From trading hardware to general trading**



© Tous droits réservés



5	3			7					
6			1	9	5				
	9	8					6		
8				6					3
4			8		3				1
7				2					6
	6						2	8	
			4	1	9				5
			8				7	9	

# Perspectives

- ☛ **(1) The journalist**

- ☛ **(2) The user / participant**

- ☛ **(3) The designer / scientist**



# The User

BLOCKCHAIN

DASHBOARD

Transactions

BITCOIN

ETHER

New!

BUY & SELL

SECURITY CENTER

SETTINGS

FAQ

BE YOUR OWN BANK.®

ⓑ 0.00000546 BTC | Ⓢ 0.102338636803627092 ETH

\$23.08

Send

Request

ALL

SENT

RECEIVED

Export Private Key

Search

SENT

July 21 @ 10:10 AM

To: 0x9970b7e233555a037311be1f3261b59393d6981f

From: My Ethereum Wallet

Add a description

0.0001 ETH

Transaction Confirmed ✓

Transaction Fee:

SENT

July 18 @ 02:54 PM

To: 0x16a6920db1f14fc473325cf94a5e2d20c1fba868

From: My Ethereum Wallet

Add a description

0.0001416... ETH

RECEIVED

July 17 @ 11:44 AM

To: My Ethereum Wallet

From: 0x3b0bc51ab9de1e5b7b6e34e5b960285805c41736

Add a description

0.08380039 ETH

RECEIVED

July 13 @ 03:03 PM

To: My Ethereum Wallet

From: 0xeed16856d551569d134530ee3967ec79995e2051

test, hey jamie!

0.01966193 ETH

👉 The wallet: 1 private key + several public keys

# Payment

- Joining (a P2P network)

- Signing (a transaction)

- Gossiping (the transaction)

- Gathering (a block)

- Mining (proof of work - nonce)

- Chaining (hash)

- Gossiping (the block)

- Committing/Aborting





# The User (Participant)

*Honey, I'm home!*  
*I found a block today!*

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9



✦...Miner Jack...✦

# The User (Participant)

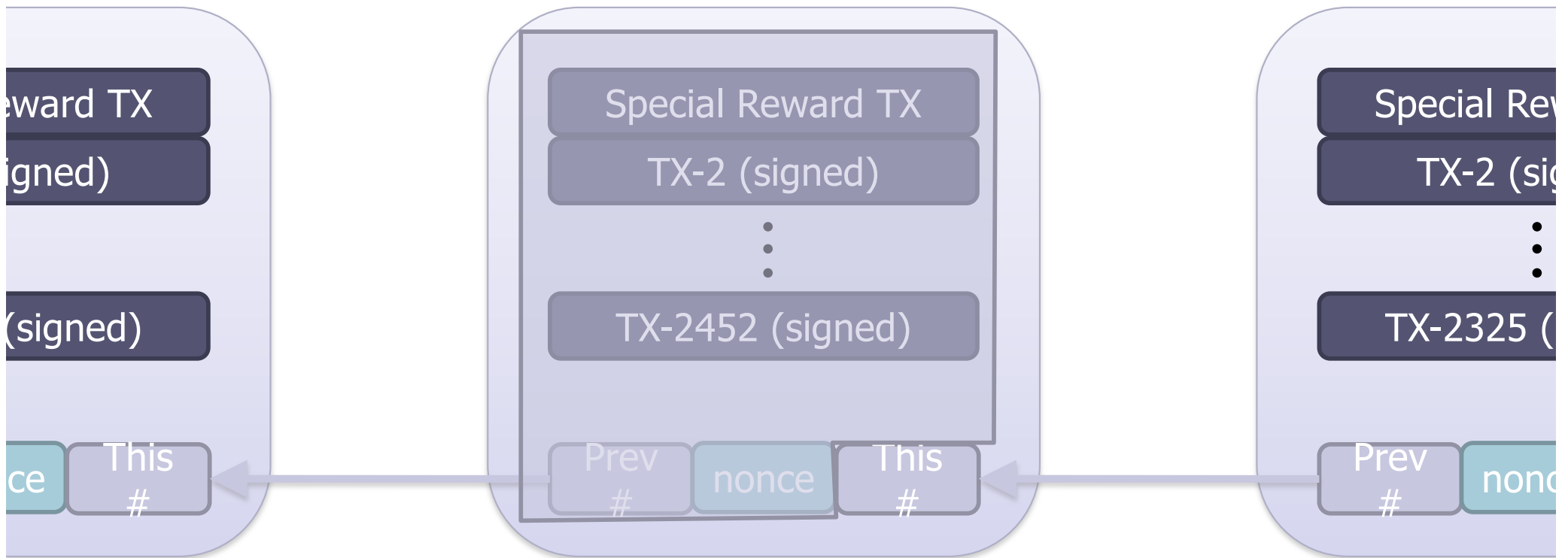
- ☞ **To validate a transaction, a miner has to solve a puzzle including it**
  - **Fairness and cooperation**
- ☞ **Incentive: 6.25 bitcoins / puzzle**
  - **Halved every 4 years**
- ☞ **Total: 21 millions bitcoins**
  - **Now: 19 millions already mined**

# The User (Participant)

Block:	<input type="text" value="0"/> <input type="text" value="1"/>
Nonce:	<input type="text" value="2790"/>
Data:	<input type="text" value="NCore"/>
Hash:	<input type="text" value="0000c5f693ac77a18ae73ace5df932457fc62e8dfa23c2f3c6d8ebb125ba7843"/>
<input type="button" value="Mine"/>	

# The Chain of Blocks

## Bitcoin block



Mining: find **nonce** such that **This #**  $< d$

How? By trying different nonces (brute force)

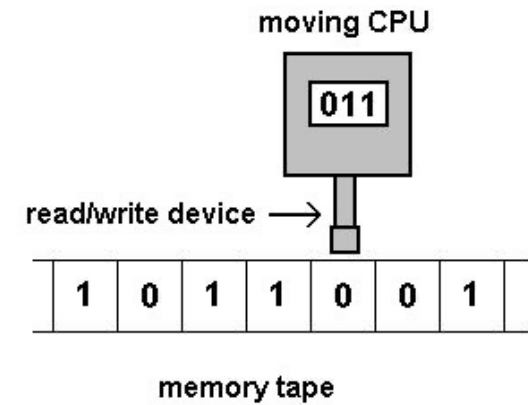
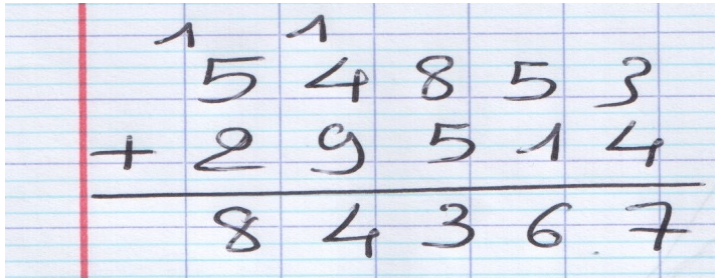
# Perspectives

- ☛ **(1) The journalist**

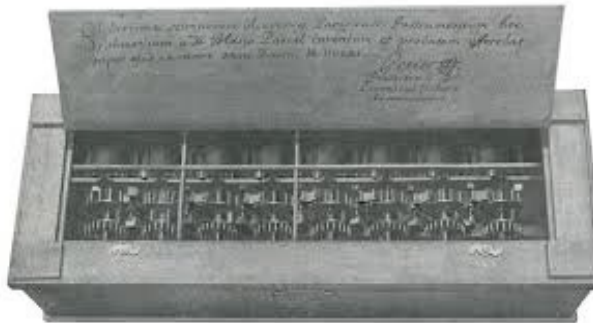
- ☛ **(2) The user / participant**

- ☛ **(3) The designer / scientist**

# (3) The Computer Scientist (Centralized- Universality 1936)

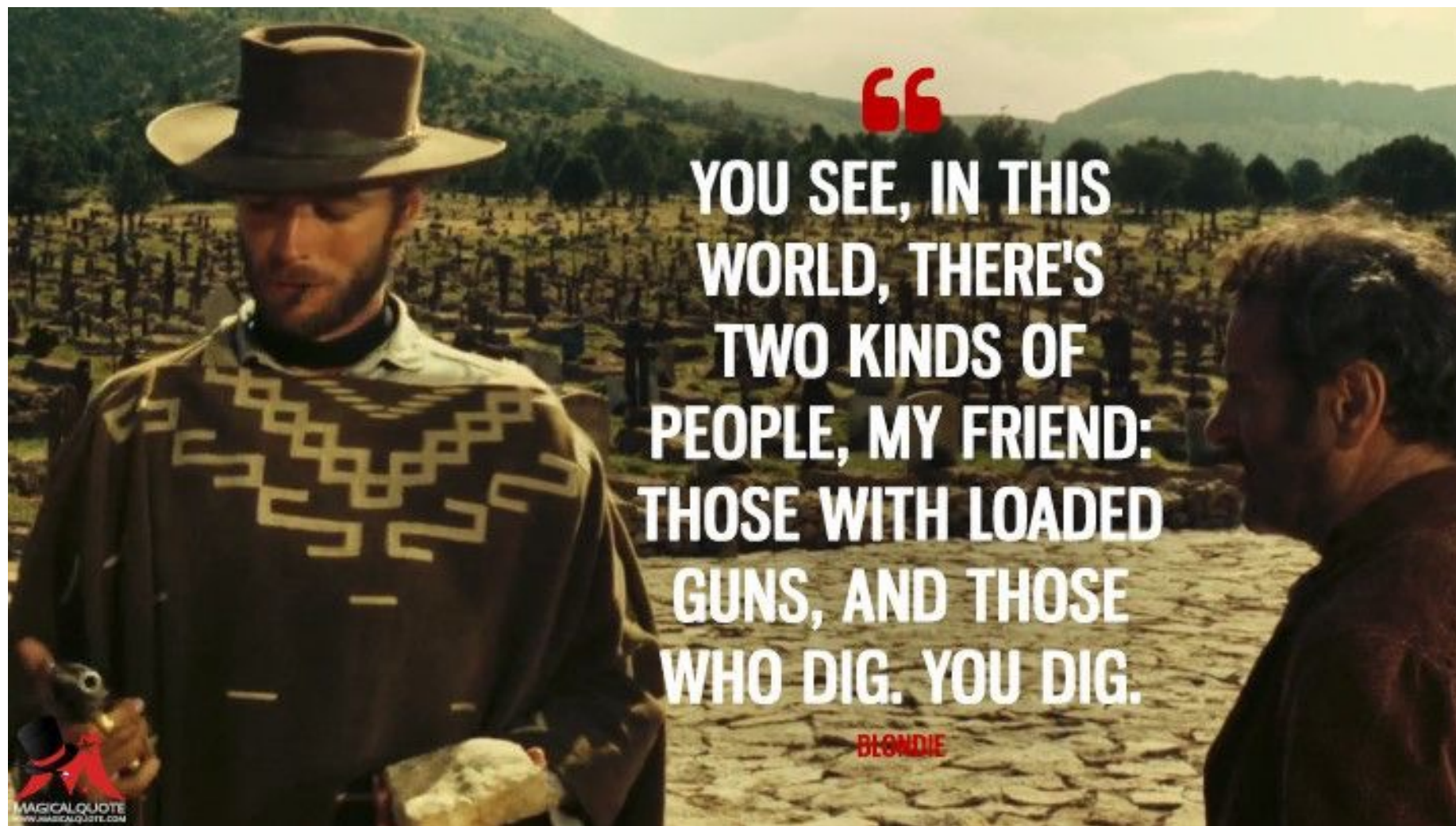


Algorithmi



Turing





“

YOU SEE, IN THIS  
WORLD, THERE'S  
TWO KINDS OF  
PEOPLE, MY FRIEND:  
THOSE WITH LOADED  
GUNS, AND THOSE  
WHO DIG. YOU DIG.

BLONDIE

# (3) The Computer Scientist (Centralized)

## P vs NP (Nash/GV 50 – Ford 70)

$$? * ? = 91$$

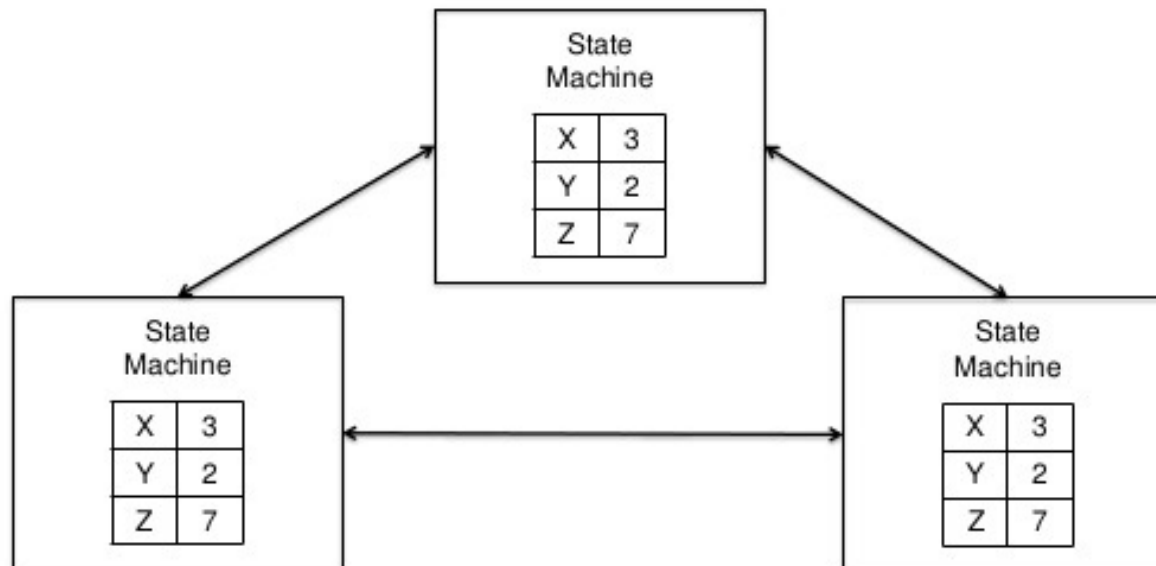
$$7 * 13 = ?$$

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

# (3) The Computer Scientist (Distributed)

## Lamport Universality (78)

Basic consensus



# Consensus Universality (78)



Every algorithm can be implemented across a network of machines iff these can solve consensus

# Consensus Impossibility (84)



Consensus is impossible in an asynchronous system

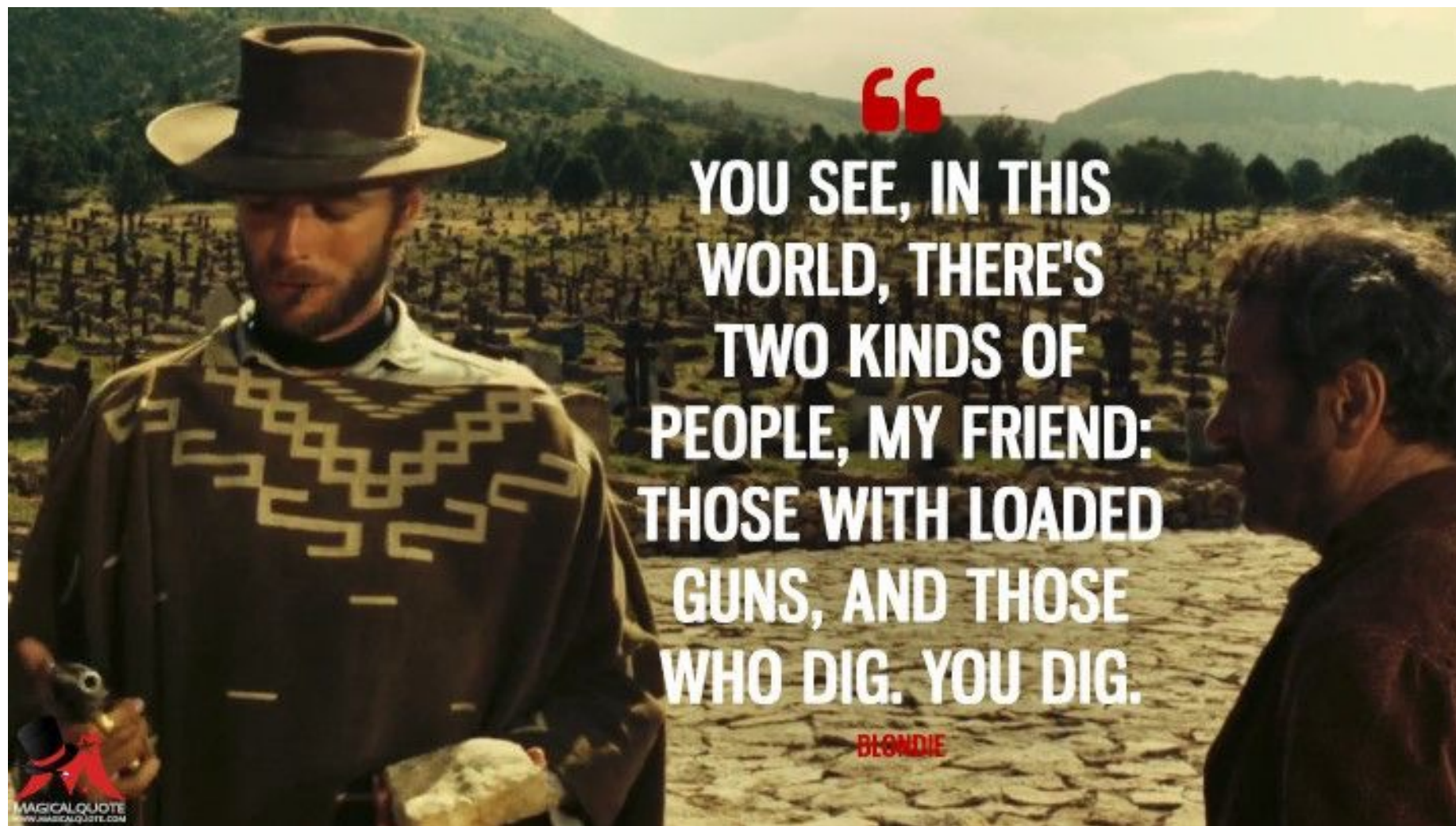


# Cryptocurrency: X000 implementations



Can we implement a  
cryptocurrency asynchronously?





“

YOU SEE, IN THIS  
WORLD, THERE'S  
TWO KINDS OF  
PEOPLE, MY FRIEND:  
THOSE WITH LOADED  
GUNS, AND THOSE  
WHO DIG. YOU DIG.

BLONDIE



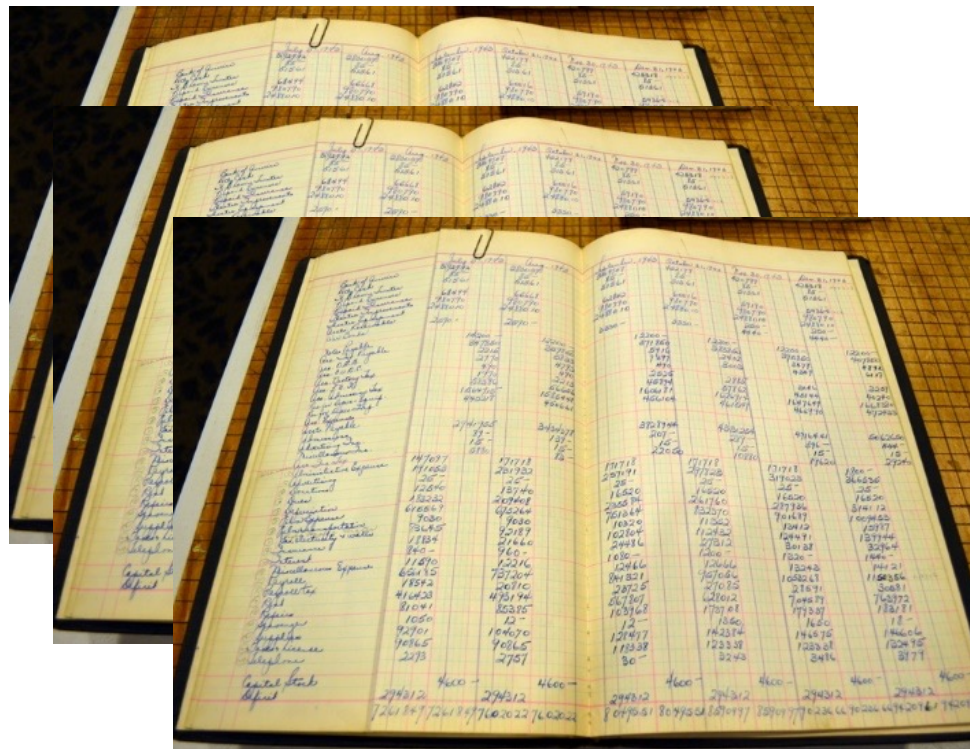


## Bitcoin: A Peer-to-Peer Electronic Cash System

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





# **PO can be implemented Asynchronously**

Consensus number of PO is 1

Consensus number of  $PO(k)$  is  $k$

- The **consensus number** of an object is the maximum number of processes that can solve consensus with it

Group Period	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	1 H																	2 He
2	3 Li	4 Be											5 B	6 C	7 N	8 O	9 F	10 Ne
3	11 Na	12 Mg											13 Al	14 Si	15 P	16 S	17 Cl	18 Ar
4	19 K	20 Ca	21 Sc	22 Ti	23 V	24 Cr	25 Mn	26 Fe	27 Co	28 Ni	29 Cu	30 Zn	31 Ga	32 Ge	33 As	34 Se	35 Br	36 Kr
5	37 Rb	38 Sr	39 Y	40 Zr	41 Nb	42 Mo	43 Tc	44 Ru	45 Rh	46 Pd	47 Ag	48 Cd	49 In	50 Sn	51 Sb	52 Te	53 I	54 Xe
6	55 Cs	56 Ba	57 La *	72 Hf	73 Ta	74 W	75 Re	76 Os	77 Ir	78 Pt	79 Au	80 Hg	81 Tl	82 Pb	83 Bi	84 Po	85 At	86 Rn
7	87 Fr	88 Ra	89 Ac *	104 Rf	105 Db	106 Sg	107 Bh	108 Hs	109 Mt	110 Ds	111 Rg	112 Cn	113 Nh	114 Fl	115 Mc	116 Lv	117 Ts	118 Og
				* 58 Ce	59 Pr	60 Nd	61 Pm	62 Sm	63 Eu	64 Gd	65 Tb	66 Dy	67 Ho	68 Er	69 Tm	70 Yb	71 Lu	
				* 90 Th	91 Pa	92 U	93 Np	94 Pu	95 Am	96 Cm	97 Bk	98 Cf	99 Es	100 Fm	101 Md	102 No	103 Lr	

# AT2: Carbon Cryptocurrency

☞ **AT2\_S**

☞ **AT2\_D**

☞ **AT2\_R**

- ☞ Number of lines of code: one order of magnitude less
- ☞ Latency: seconds (at most)



# References

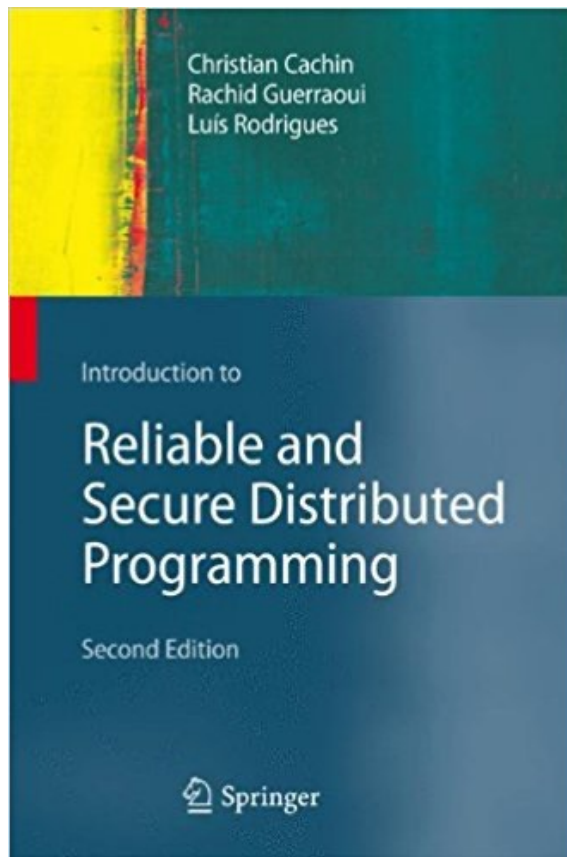
[dcl.epfl.ch/site/cryptocurrencies](https://dcl.epfl.ch/site/cryptocurrencies)

Rachid Guerraoui, [Petr Kuznetsov](#), [Matteo Monti](#), [Matej Pavlovic](#), [Dragos-Adrian Seredinschi](#): **The Consensus Number of a Cryptocurrency**. PODC [2019](#): 307-316

Rachid Guerraoui, [Petr Kuznetsov](#), [Matteo Monti](#), [Matej Pavlovic](#), [Dragos-Adrian Seredinschi](#): **Scalable Byzantine Reliable Broadcast**. DISC [2019](#): 1-16 (**Best Paper Award**)

[Daniel Collins](#), Rachid Guerraoui, [Jovan Komatovic](#), [Petr Kuznetsov](#), [Matteo Monti](#), [Matej Pavlovic](#), [Yvonne Anne Pignolet](#), [Dragos-Adrian Seredinschi](#), [Andrei Tonkikh](#), [Athanasios Xygkis](#): **Online Payments by Merely Broadcasting Messages**. DSN [2020](#): 26-38 (**Runner for the Best Paper Award**)

# References



## ALGORITHMS FOR CONCURRENT SYSTEMS

Rachid Guerraoui  
Petr Kuznetsov

