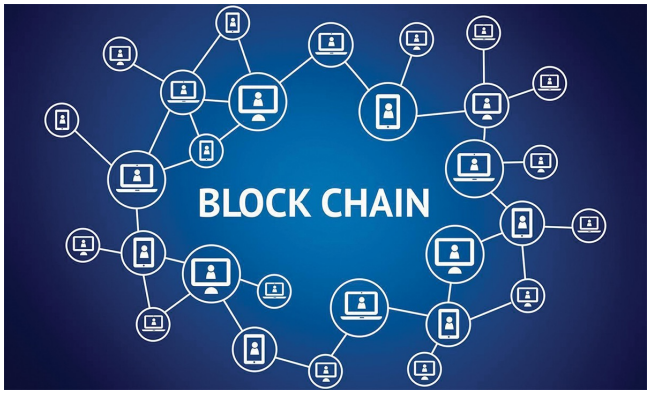
Demystifying Bitcoin

Prof R. Guerraoui EPFL

Cryptocurrency

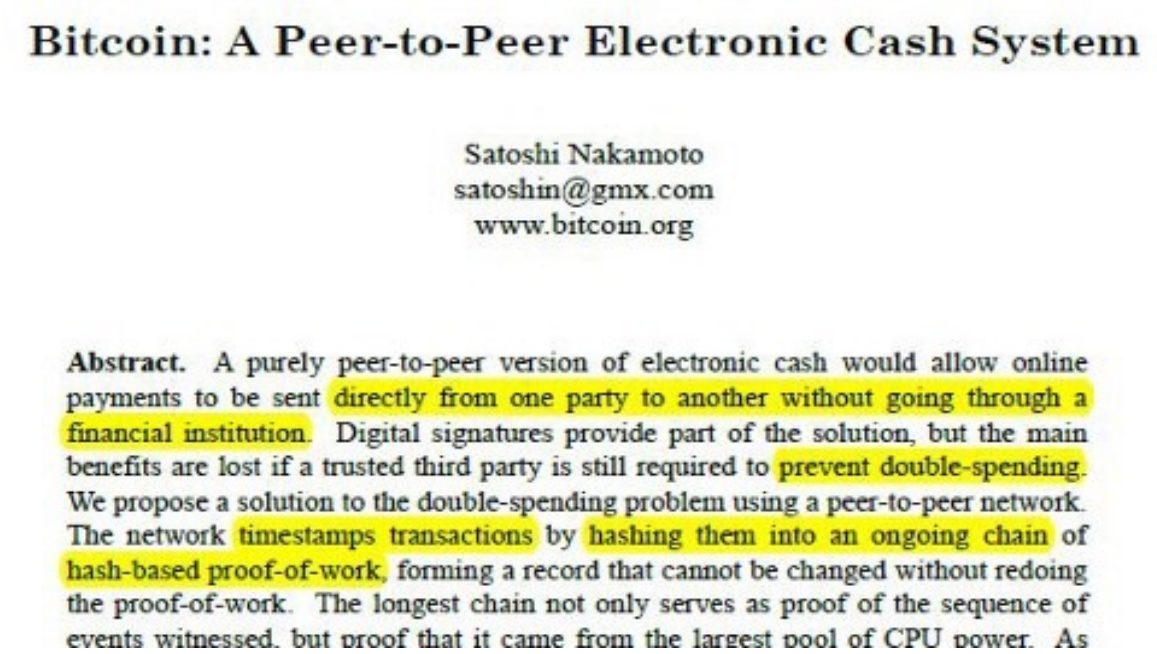
- Virtual currency

- Virtual bank (decentralized)



Perspectives

- (1) The journalist
- (2) The user / participant
- (3) The designer / scientist

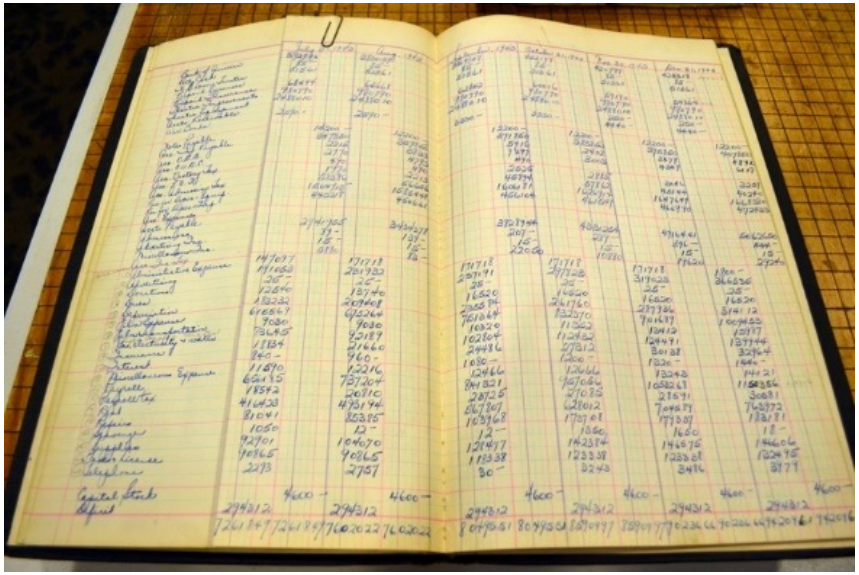


Bitcoin: A Peer-to-Peer Electronic Cash System

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**

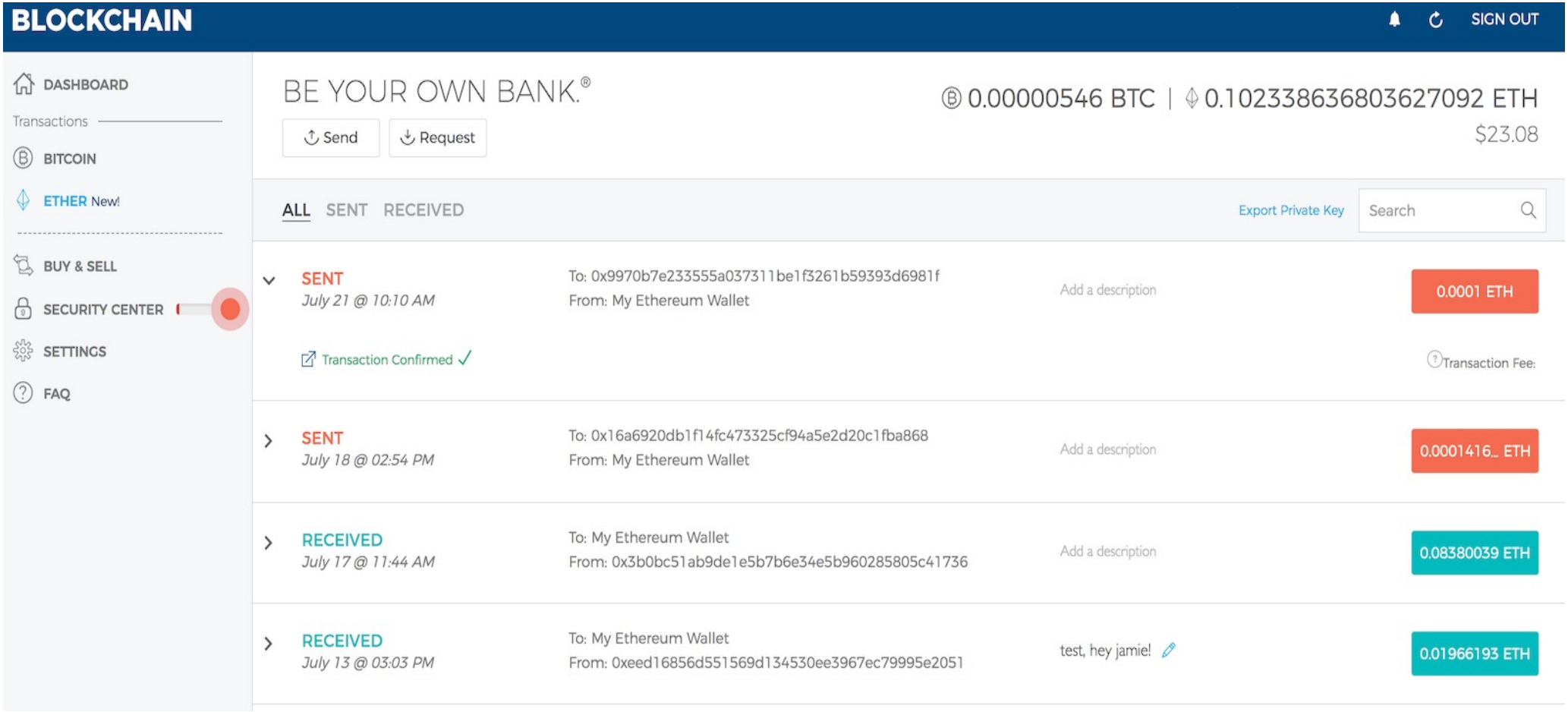


5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

Perspectives

- (1) The journalist
  - (2) The user / participant
    - (3) The designer / scientist

The User



- **The wallet: 1 private key + several public keys**

Payment

- Joinning (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

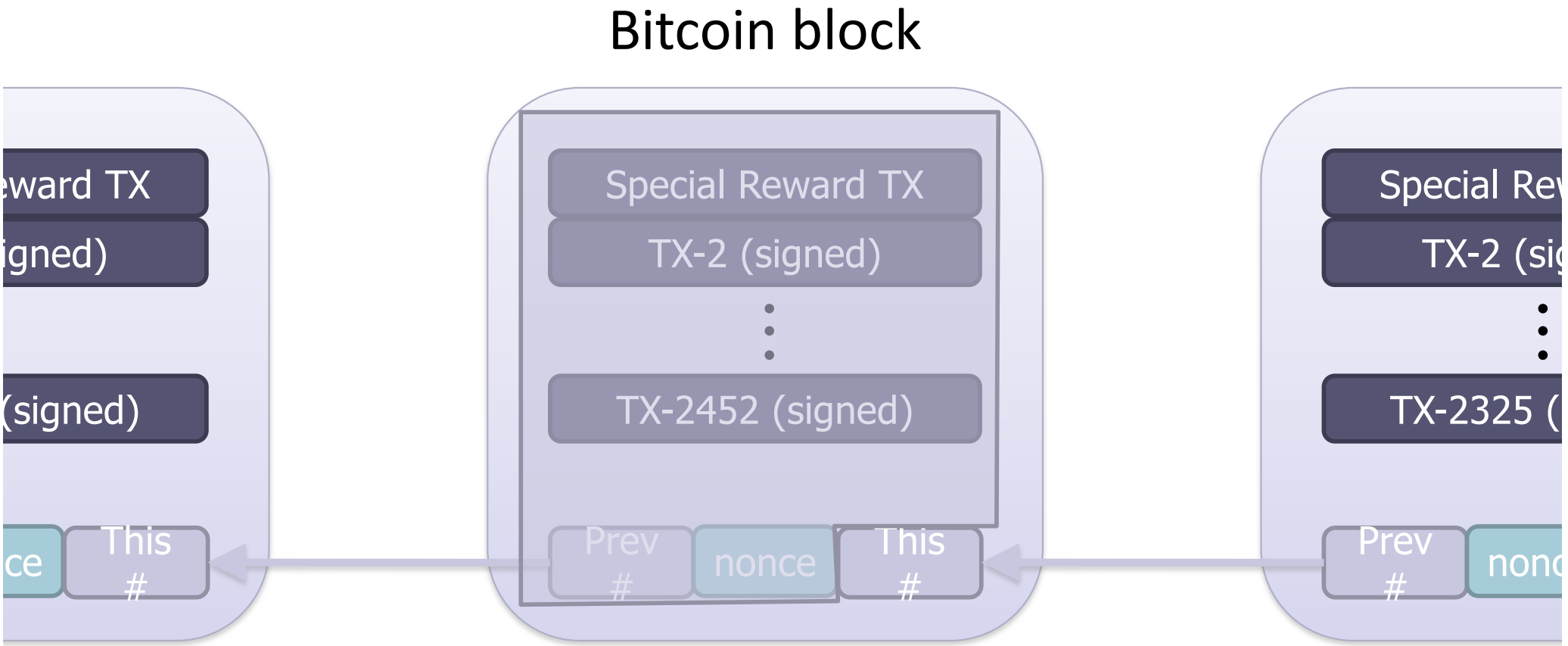
Miner Jack

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)

The Chain of Blocks



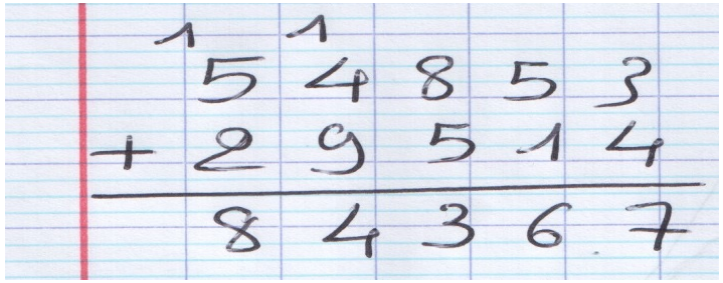
Mining: find nonce such that This # $< d$

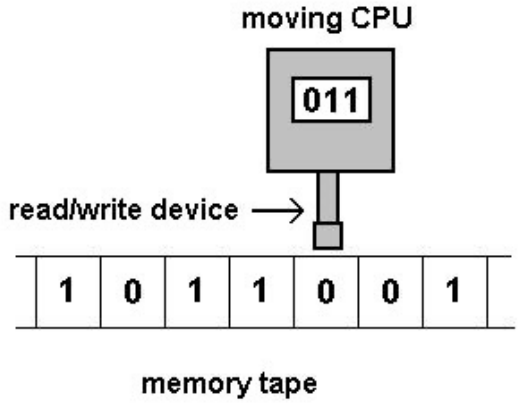
How? By trying different nonces (brute force)

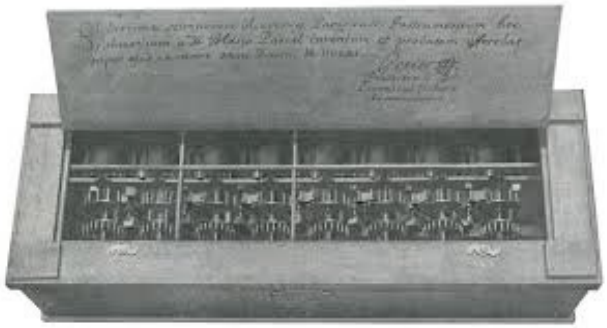
Perspectives

- (1) The journalist
  - (2) The user / participant
    - (3) The designer / scientist

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

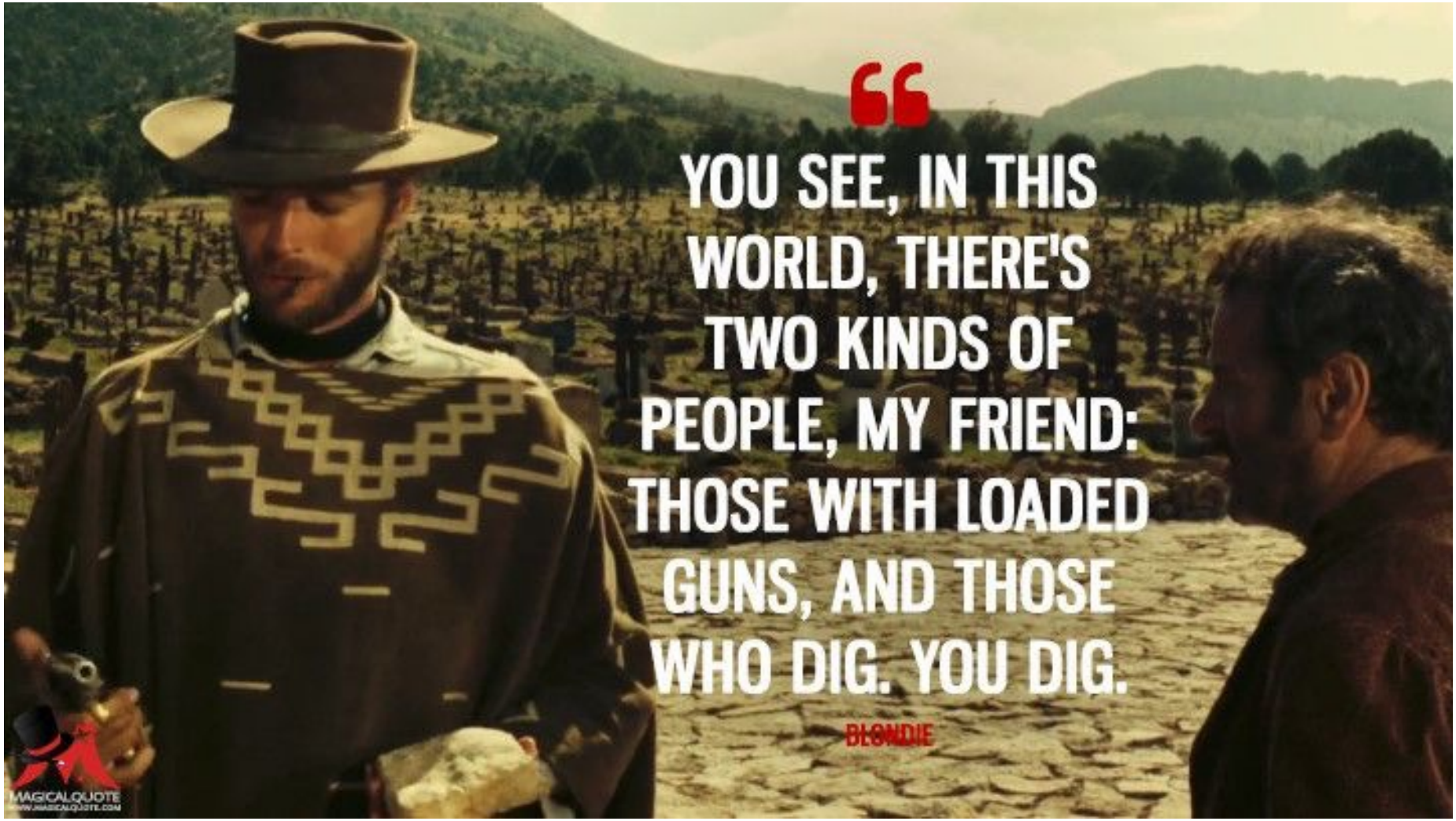






Algorithmi

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
MAGICALQUOTE

(3) The Computer Scientist (Centralized)

P vs NP (Nash/GV 50 – Ford 70)

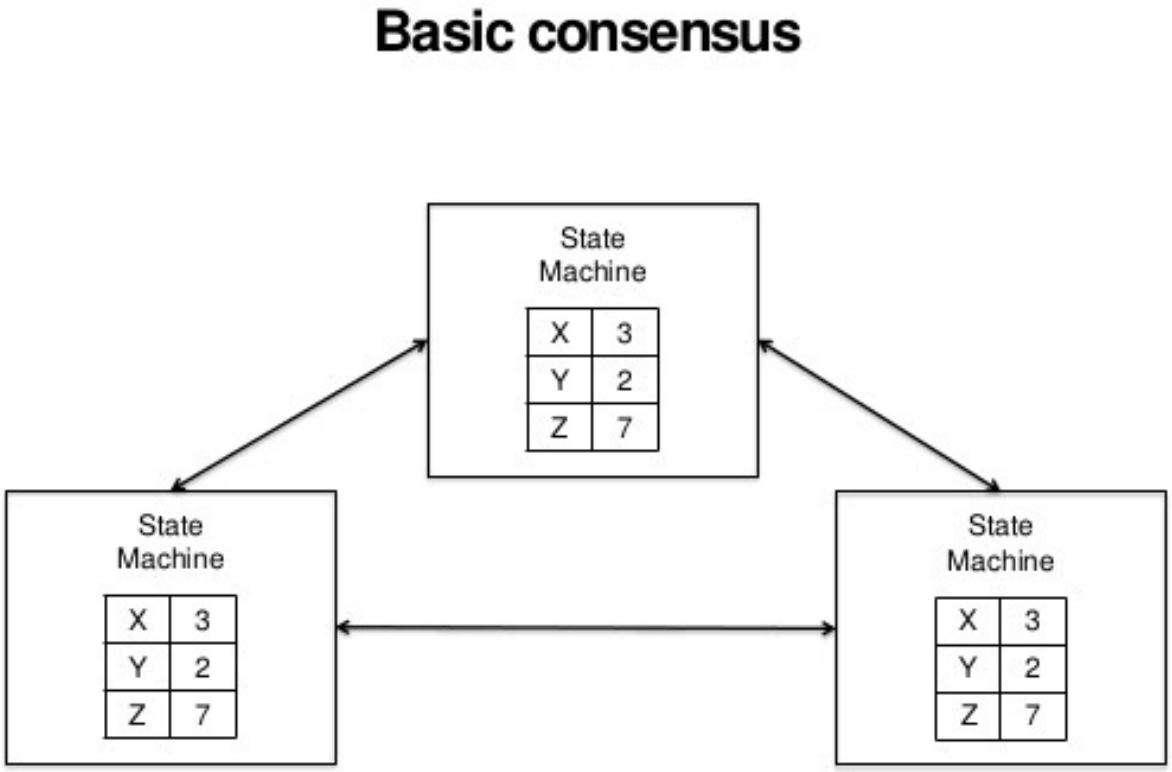
$? * ? = 91$

$7 * 13 = ?$

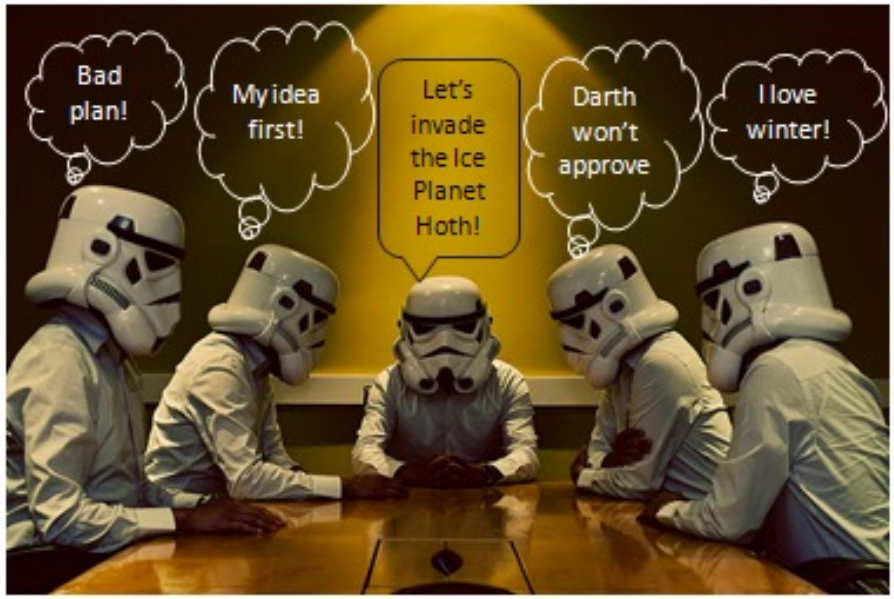
5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

(3) The Computer Scientist (Distributed)

Lamport Universality (78)

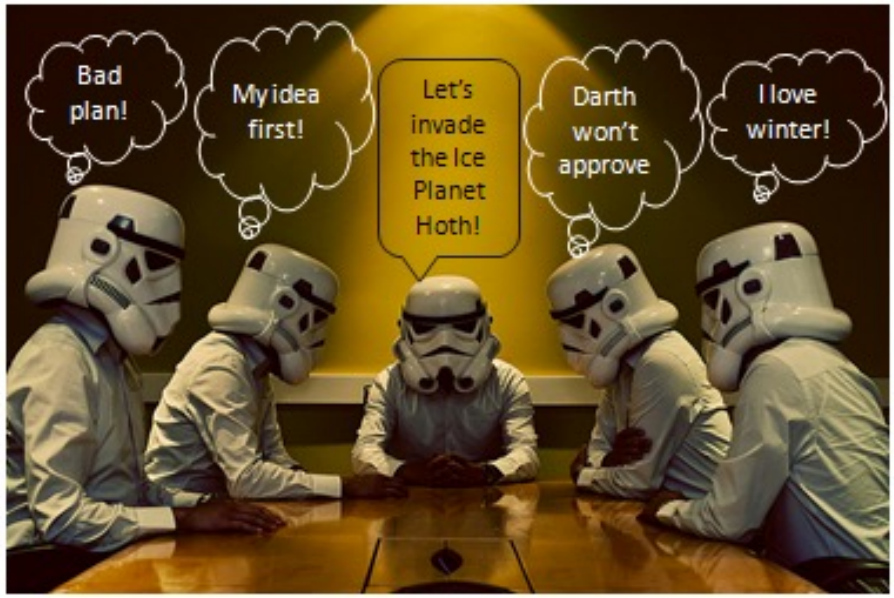


Consensus Universality (78)



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

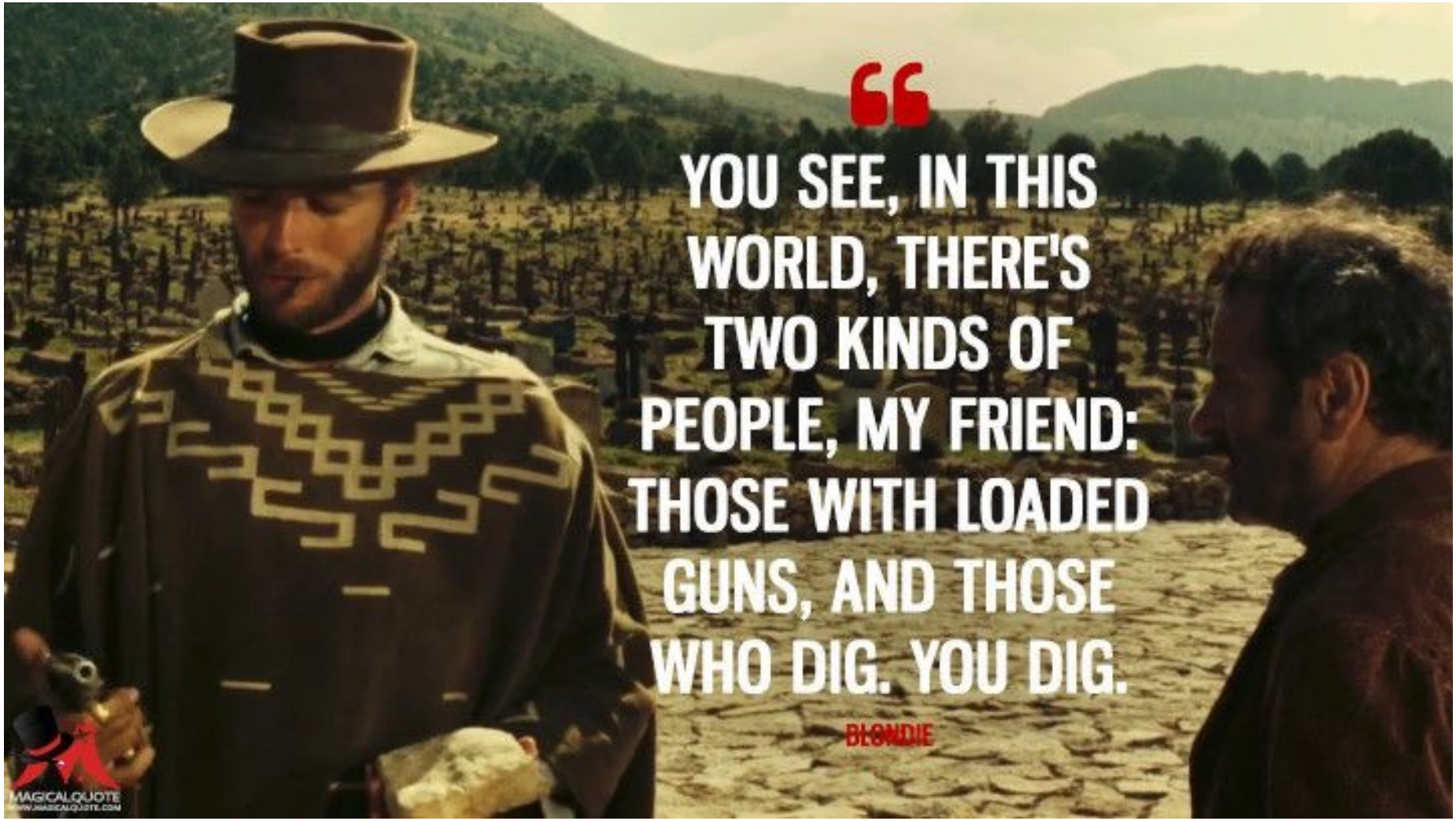
Consensus Impossibility (84)



Consensus is impossible in an asynchronous system

Cryptocurrency: X000 implementations

Can we implement a cryptocurrency asynchronously?

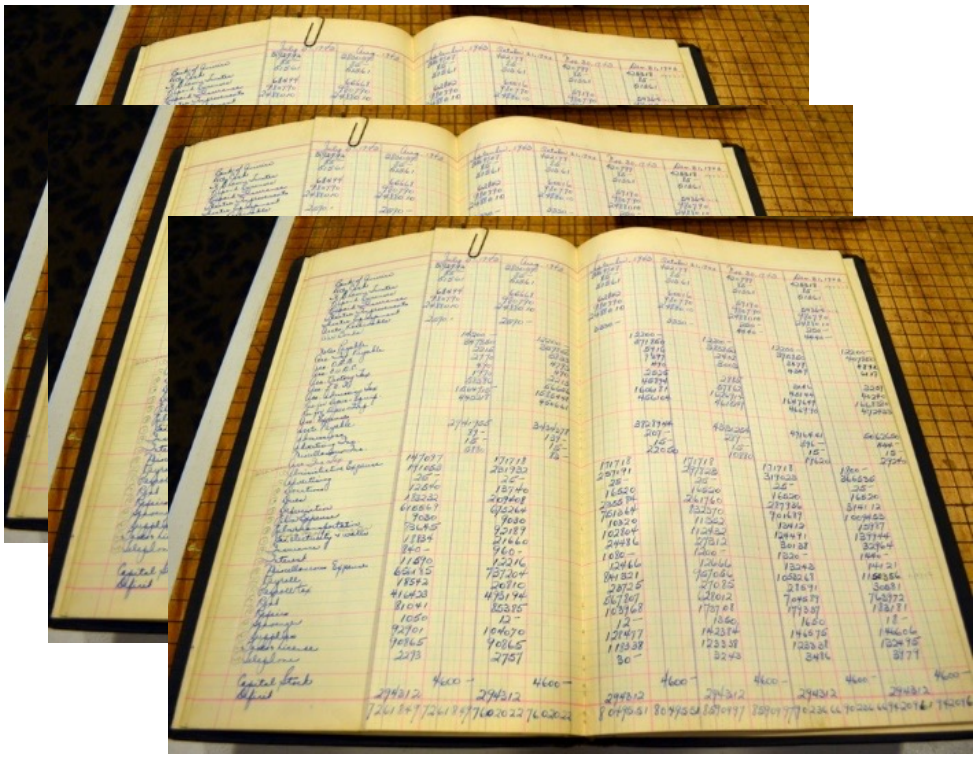

“
YOU SEE, IN THIS WORLD, THERE'S TWO KINDS OF PEOPLE, MY FRIEND: THOSE WITH LOADED GUNS, AND THOSE WHO DIG. YOU DIG.
BLONDIE
MAGICALQUOTE

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


© Tous droits réservés



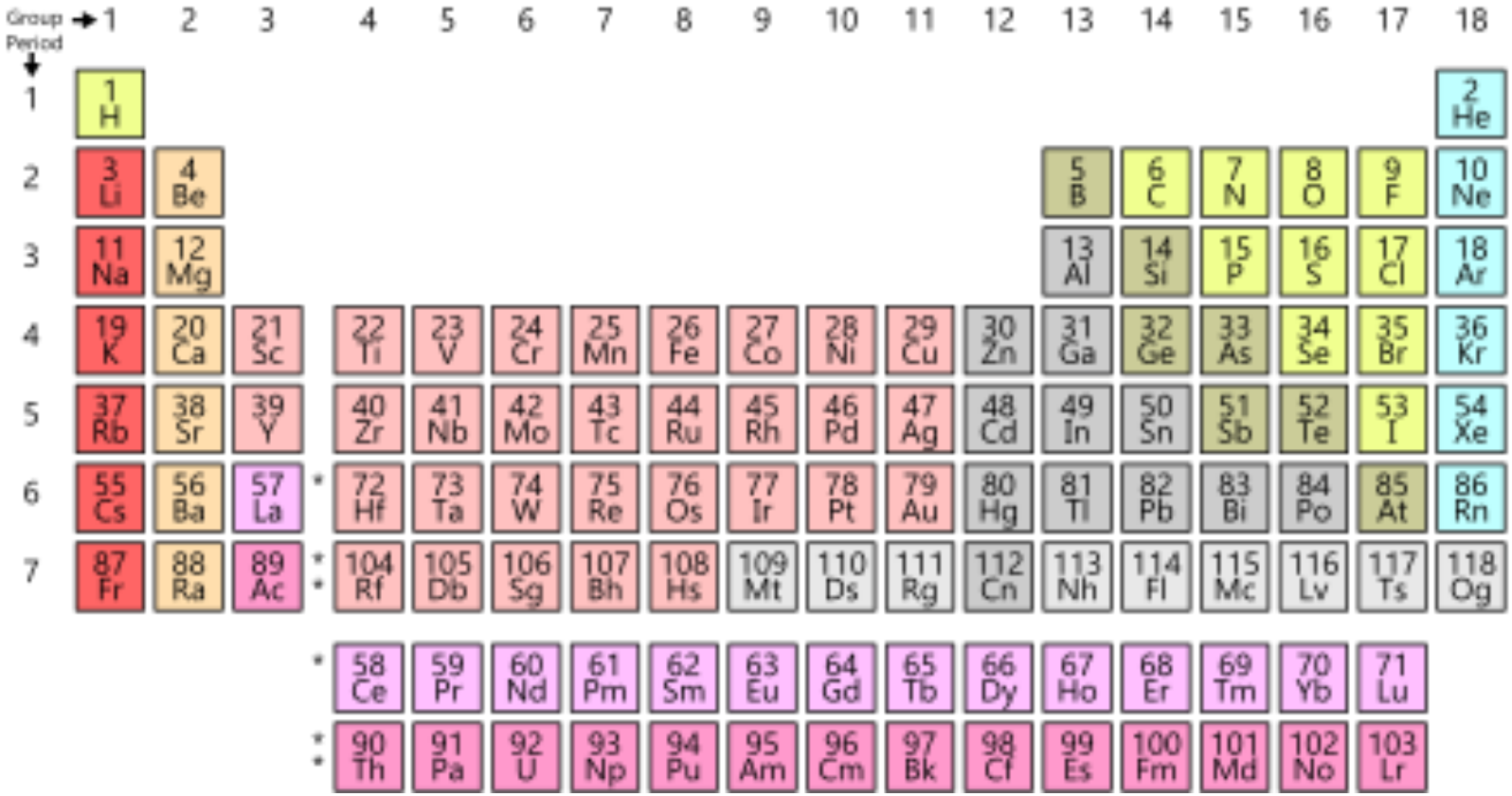

alamy stock photo
CXKJM6
www.alamy.com

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 than can solve consensus with it



AT2: Carbon Cryptocurrency

- **AT2_S**
- **AT2_D**
- **AT2_R**

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

References

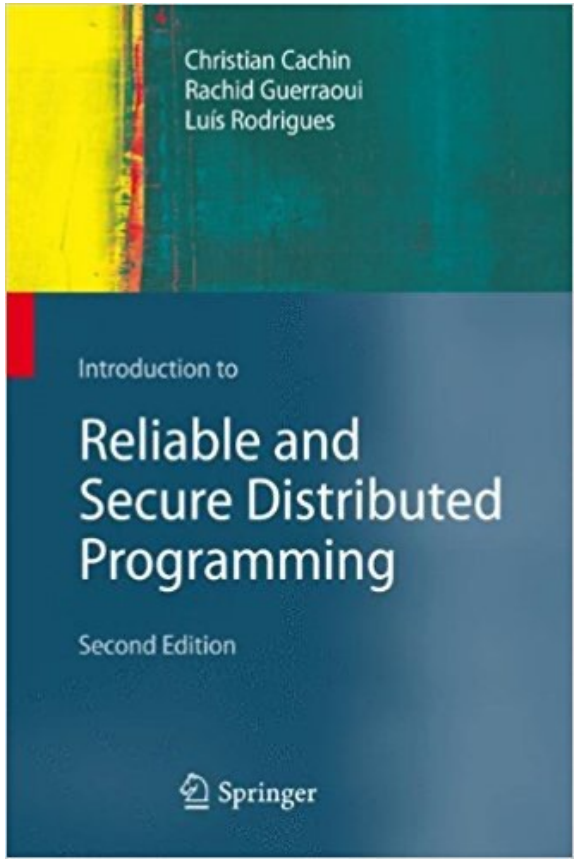
dcl.epfl.ch/site/cryptocurrencies

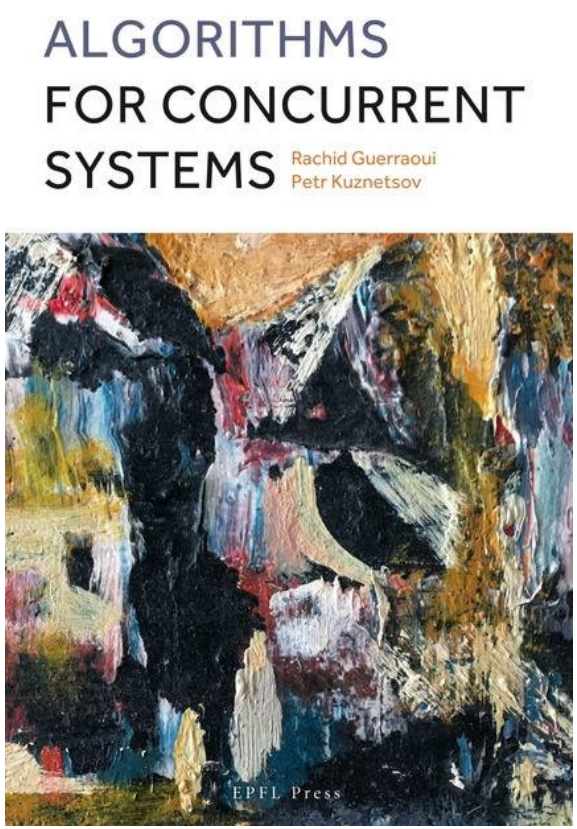
Rachid Guerraoui, Petr Kuznetsov, Matteo Monti, Matej Pavlovic, Dragos-Adrian Seredinschi: **The Consensus Number of a Cryptocurrency.** PODC 2019: 307-316

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


Christian Cachin
Rachid Guerraoui
Luís Rodrigues
Introduction to
Reliable and Secure Distributed Programming
Second Edition
Springer


ALGORITHMS FOR CONCURRENT SYSTEMS
Rachid Guerraoui
Petr Kuznetsov
EPFL Press