

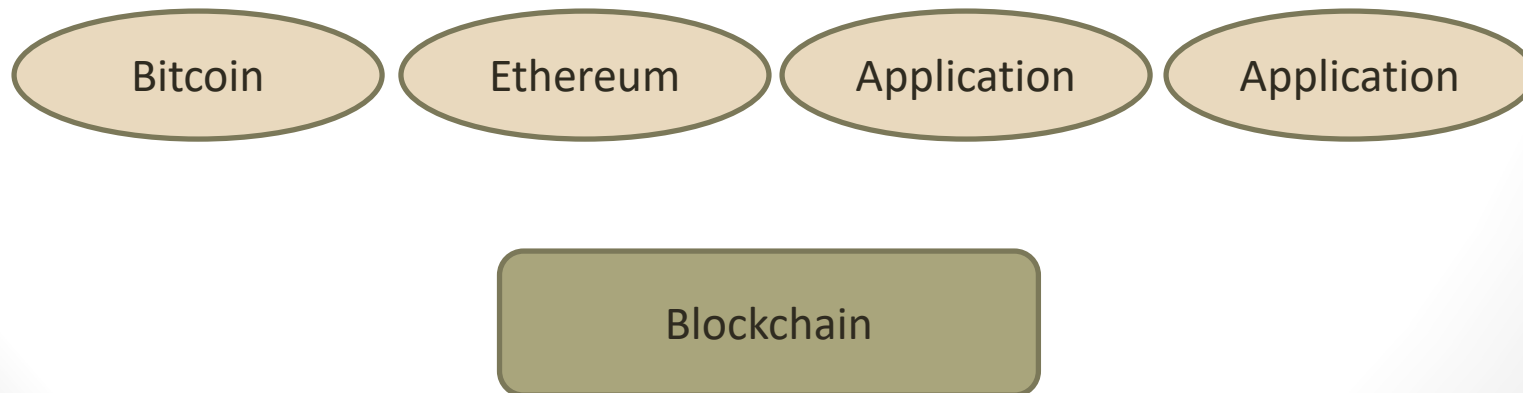
# Introduction to blockchains and the opportunities ahead

Sofoklis Efremidis, Ph.D.

Athens Information Technology

# Fundamental Technology

- Bitcoin  $\neq$  blockchain
- Is fundamental technology
  - Compared to the Internet
- Blockchain  $\Rightarrow$  Ethereum
- Blockchain  $\Rightarrow$  Applications



# New Technology

- 31 October 2008, a link to a paper

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

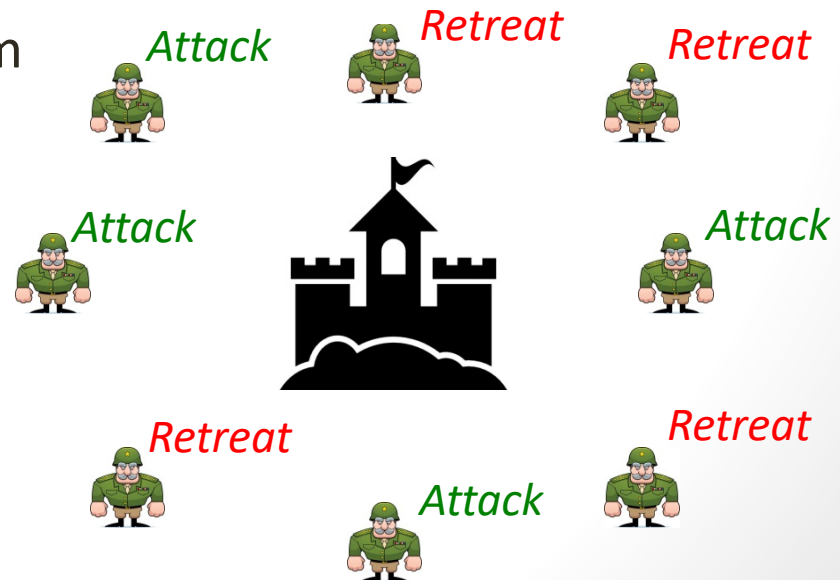
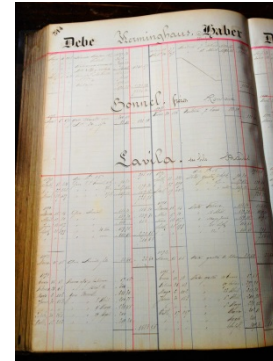
Satoshi Nakamoto  
satoshin@gmx.com  
www.bitcoin.org

was posted to a cryptography mailing list

- detailed methods of using a peer-to-peer network to generate what was described as “a system for electronic transactions without relying on trust”
- Several attempts for digital currency appeared before

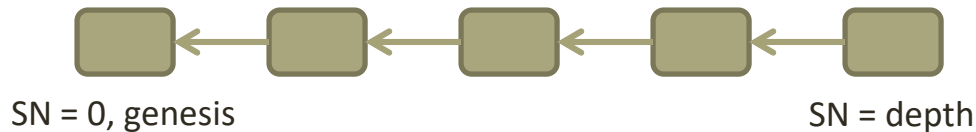
# Overview

- A public ledger
- Distributed
- Everybody agrees on it
- Solves a well known problem



# What is it

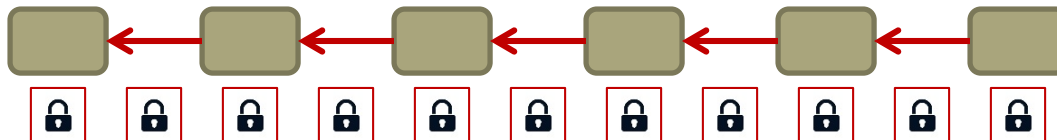
- A data structure: linked list of blocks



- Can only append data

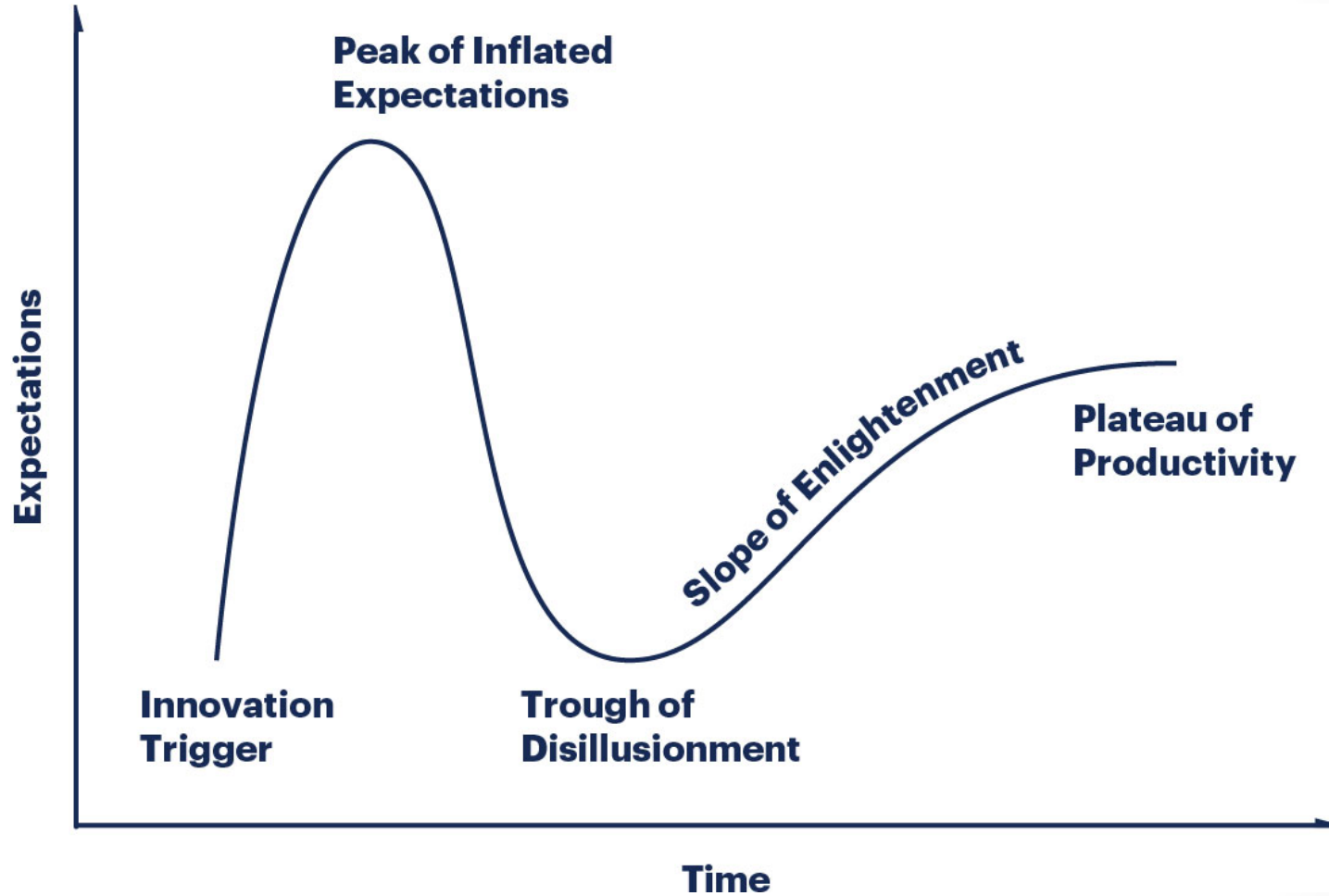


- Once an append is locked into place it can not be undone



- Almost impossible to modify a block
  - The deeper, the harder

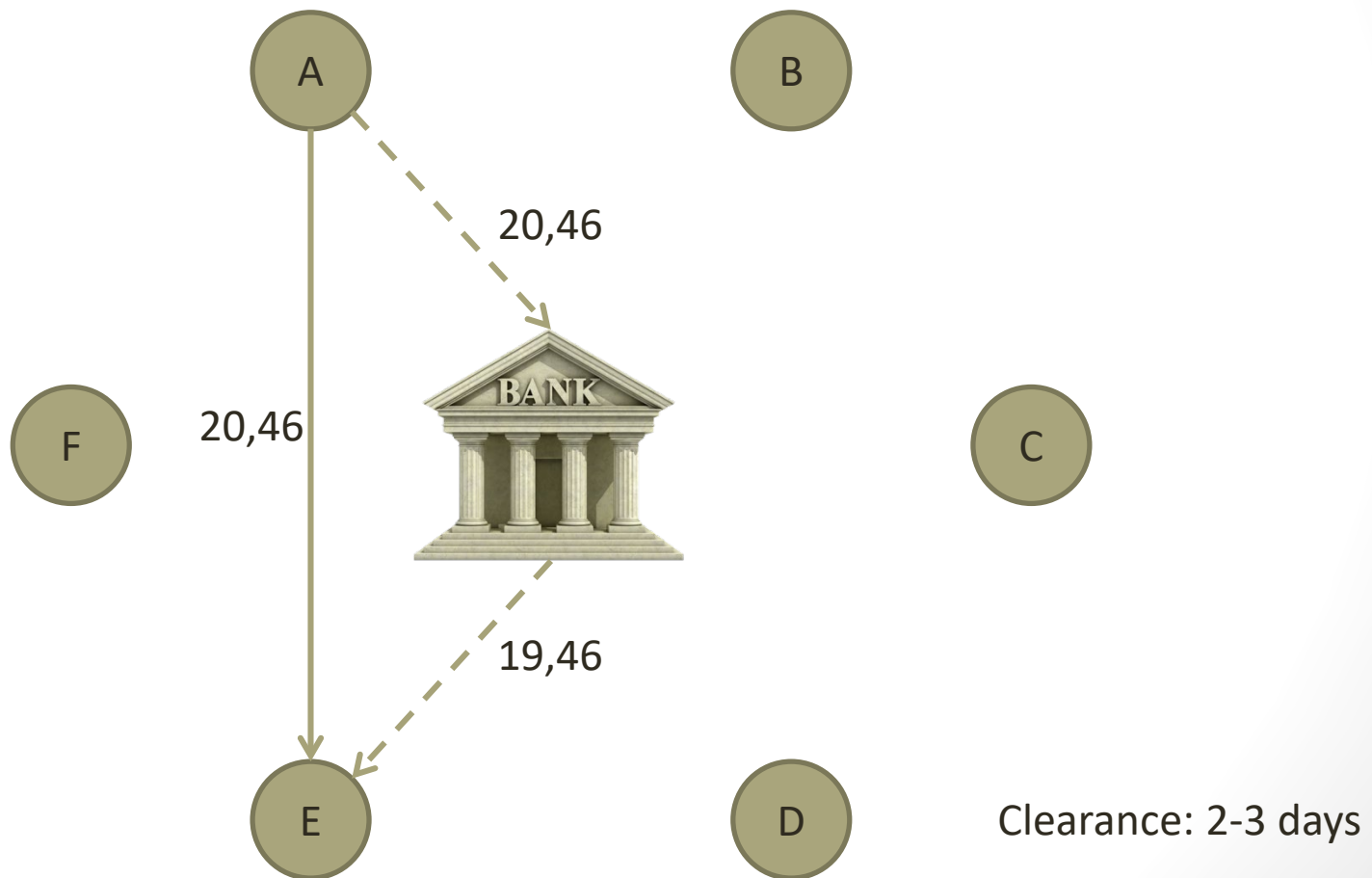
# Gartner Hype Cycle



<https://www.gartner.com/en/research/methodologies/gartner-hype-cycle>

# Money transfer

- Or any other type of transaction



# Account balances



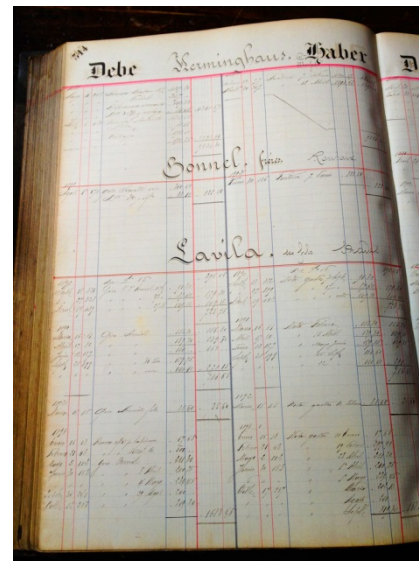
Name	Balance
A	120,53
B	394,72
C	172,88
D	251,90
E	401,57
F	332,55



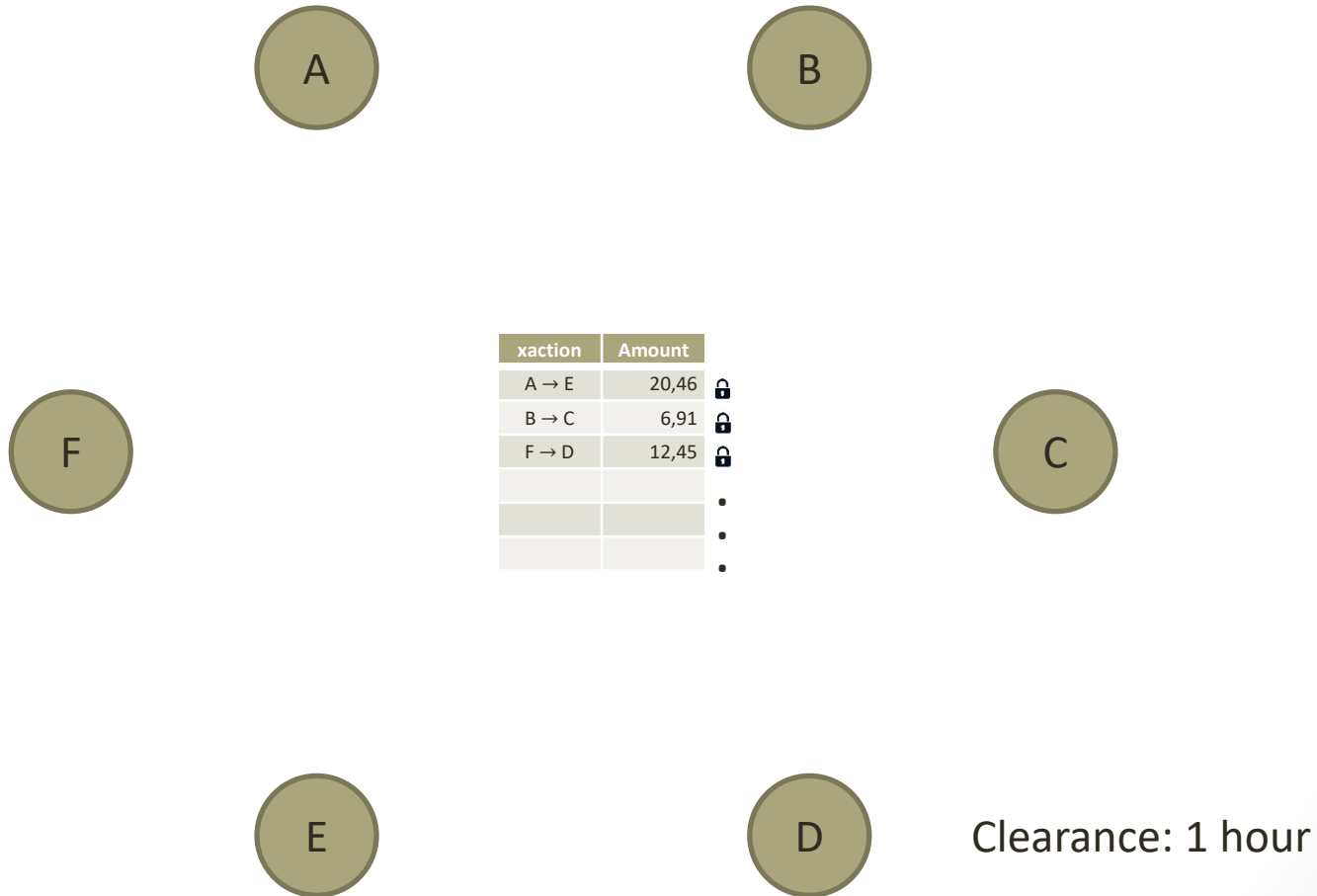
# Transactions and ledger

Name	Balance
A	120,53 100,07
B	394,72 387,81
C	172,88 179,79
D	251,90 264,35
E	401,57 422,03
F	332,55 310,10

Transaction	Amount
A → E	20,46
B → C	6,91
F → D	12,45



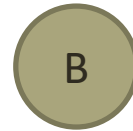
# Central ledger



# Distributed ledger



xaction	Amount	
A → E	20,46	🔒
B → C	6,91	🔒
F → D	12,45	🔒
		⋮
		⋮
		⋮



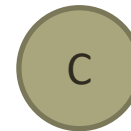
This is the next transaction  
This is the key to lock it

xaction	Amount	
A → E	20,46	🔒
B → C	6,91	🔒
F → D	12,45	🔒
		⋮
		⋮
		⋮



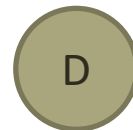
xaction	Amount	
A → E	20,46	🔒
B → C	6,91	🔒
F → D	12,45	🔒
		⋮
		⋮
		⋮

xaction	Amount	
A → E	20,46	🔒
B → C	6,91	🔒
F → D	12,45	🔒
		⋮
		⋮
		⋮



xaction	Amount	
A → E	20,46	🔒
B → C	6,91	🔒
F → D	12,45	🔒
		⋮
		⋮
		⋮

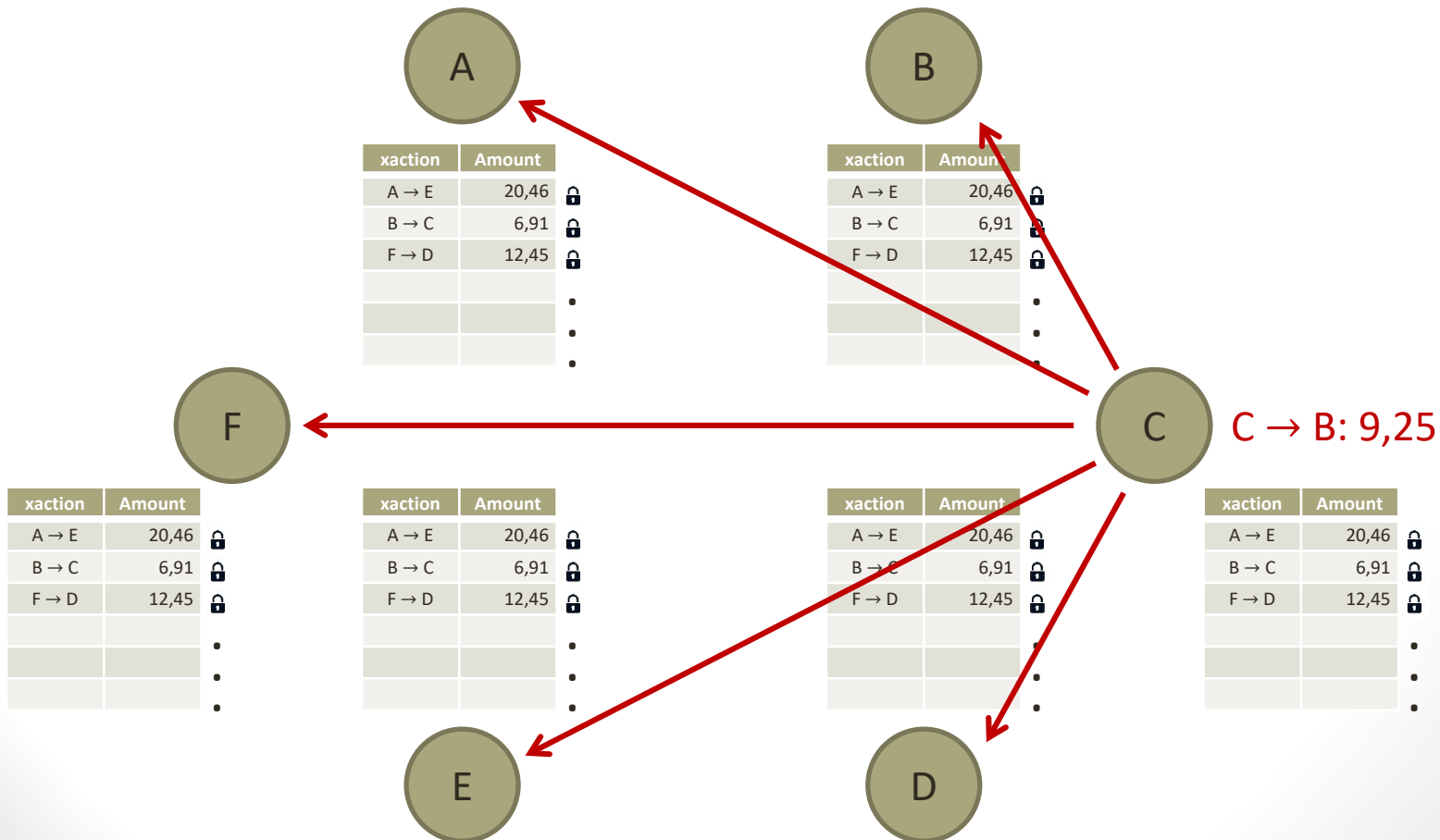
xaction	Amount	
A → E	20,46	🔒
B → C	6,91	🔒
F → D	12,45	🔒
		⋮
		⋮
		⋮



# Announcement





A new transaction is announced to the whole network

- $C \rightarrow B: 9,25$



# Validation

- The transaction must be checked for its validity before it gets locked into the ledger
  - $C \rightarrow B$ : 9,25
  - The amount has not been spent again
  - C must give consent the transaction
    - Sign the transaction

xaction	Amount	
A $\rightarrow$ E	20,46	
B $\rightarrow$ C	6,91	
F $\rightarrow$ D	12,45	
C $\rightarrow$ B	9,25	
		.
		.

# Miners

Special nodes that

- collect and validate transactions
- search for a lock to lock them to the ledger



Finding a lock is a difficult problem

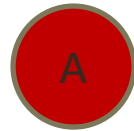
- Requires exhaustive search
- Requires resources

Incentive: miners are awarded

- New bitcoins
- Transaction fees

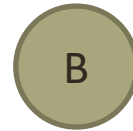


# Miners



C → B: 9,25

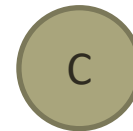
xaction	Amount
A → E	20,46
B → C	6,91
F → D	12,45
	•
	•
	•



xaction	Amount
A → E	20,46
B → C	6,91
F → D	12,45
	•
	•
	•

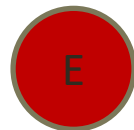


xaction	Amount
A → E	20,46
B → C	6,91
F → D	12,45
	•
	•
	•



xaction	Amount
A → E	20,46
B → C	6,91
F → D	12,45
	•
	•
	•

xaction	Amount
A → E	20,46
B → C	6,91
F → D	12,45
	•
	•
	•



C → B: 9,25



C → B: 9,25

# Discovery and validation

- Solving the problem  
finding the lock  
is a difficult problem
- Maybe several locks exists
- Checking if a lock is correct is an easy problem





# Competition

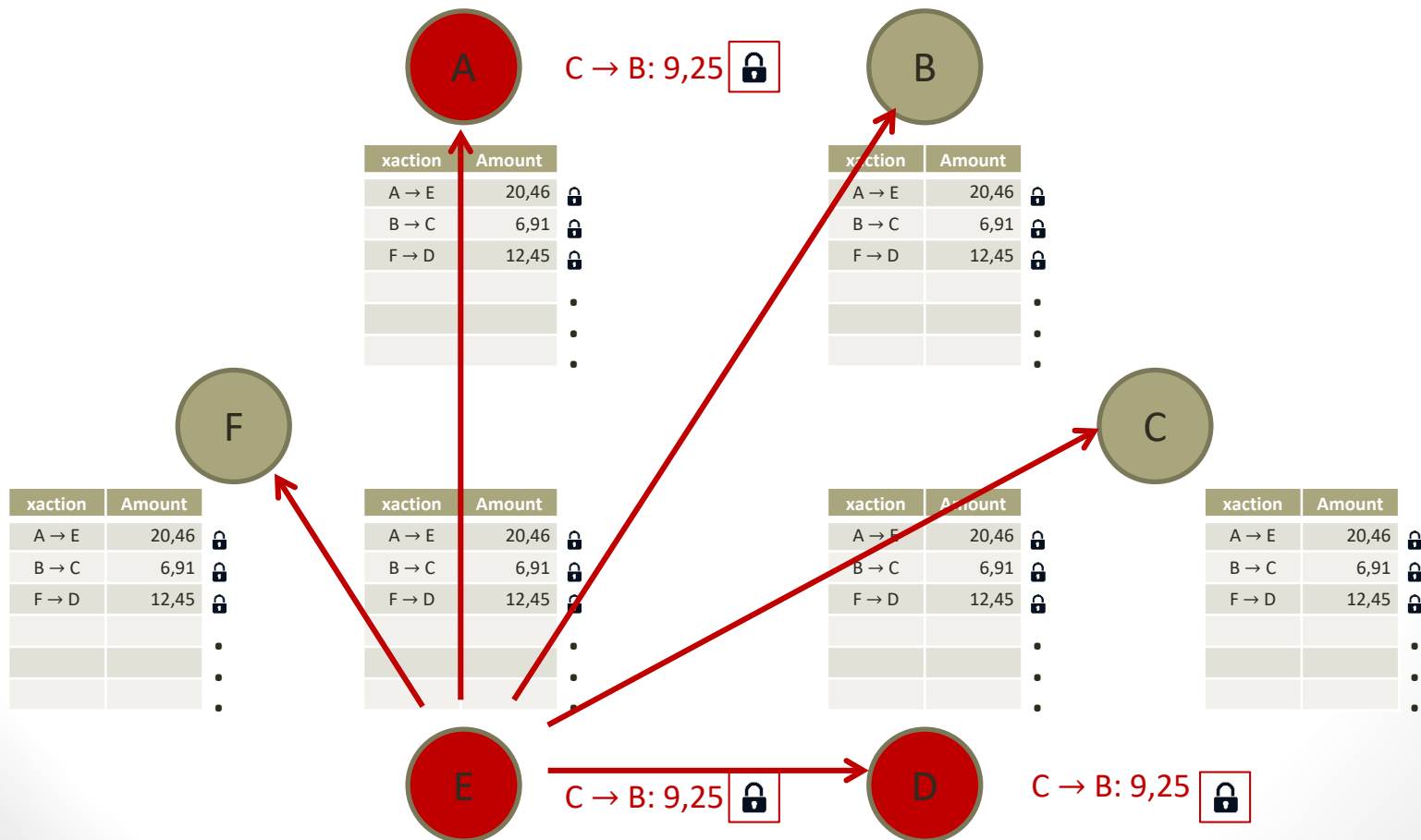
- Miners compete to solve the same problem
- Lock  $[C \rightarrow B: 9,25]$  to the chain



- One winner, many losers
  - The winners gets it all
  - All attempt to solve a new problem

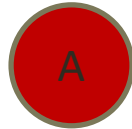
# Lock announcement

- Once a lock is found it is announced to the network

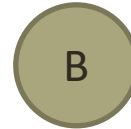


# State update

- Once a miner receives a lock
  - Checks its validity
  - Updates its list
  - Starts over



xaction	Amount	
A → E	20,46	🔒
B → C	6,91	🔒
F → D	12,45	🔒
C → B	9,25	🔒
		•
		•

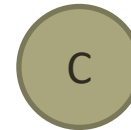


xaction	Amount	
A → E	20,46	🔒
B → C	6,91	🔒
F → D	12,45	🔒
C → B	9,25	🔒
		•
		•



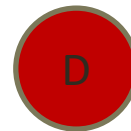
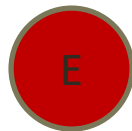
xaction	Amount	
A → E	20,46	🔒
B → C	6,91	🔒
F → D	12,45	🔒
C → B	9,25	🔒
		•
		•

xaction	Amount	
A → E	20,46	🔒
B → C	6,91	🔒
F → D	12,45	🔒
C → B	9,25	🔒
		•
		•



xaction	Amount	
A → E	20,46	🔒
B → C	6,91	🔒
F → D	12,45	🔒
C → B	9,25	🔒
		•
		•

xaction	Amount	
A → E	20,46	🔒
B → C	6,91	🔒
F → D	12,45	🔒
C → B	9,25	🔒
		•
		•



# Distributed agreement

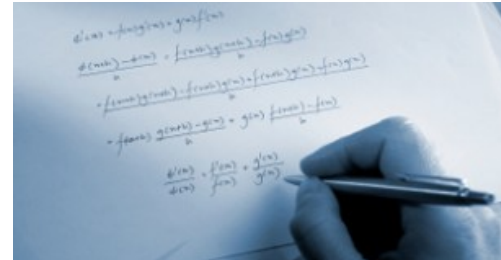
- A number of unknown parties
- All parties agree on the same state of the blockchain
- Once an agreement has been made
  - It is recorded and locked
  - Can not be undone



Blockchain: a technology that allows  
a number of distributed parties  
that do not share trust relationships  
to reach agreement

# Proving a solution

- Miners must solve a difficult mathematical problem
- Exhaustive search
  - Prove that work has been done to solve it to avoid attacks



- Process requires CPU power (POW)
  - Energy consuming
  - 1 CPU  $\Rightarrow$  1 vote

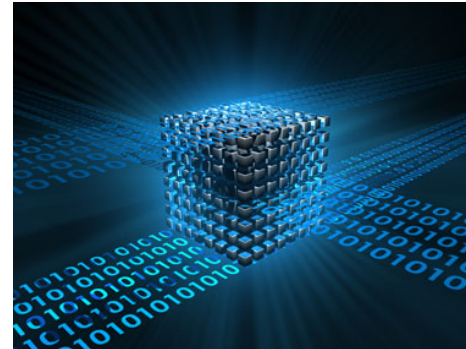


- Alternative: space (POS)
  - 1 PC  $\Rightarrow$  1 vote
  - Memory demanding



# Data and processing

- Bitcoin blockchain data: transactions
  - $C \rightarrow B: 9,25$
- Transaction validation
  - Set of criteria
- Transaction execution
  - Result of a primitive program
  - For a stack machine



# Blockchain data

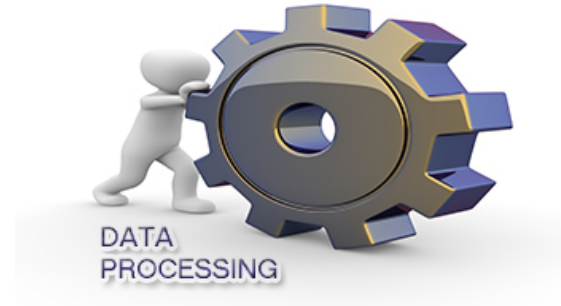
Anything worth recording

- Property registrations
  - Ids
  - Goods tracking
  - Health records
  - Financial data
  - Insurance data
  - Supply chain data
  - Digital rights
- 
- Each one gives rise to a new set of applications



# Blockchain data processing

- Data validation
  - Set of criteria



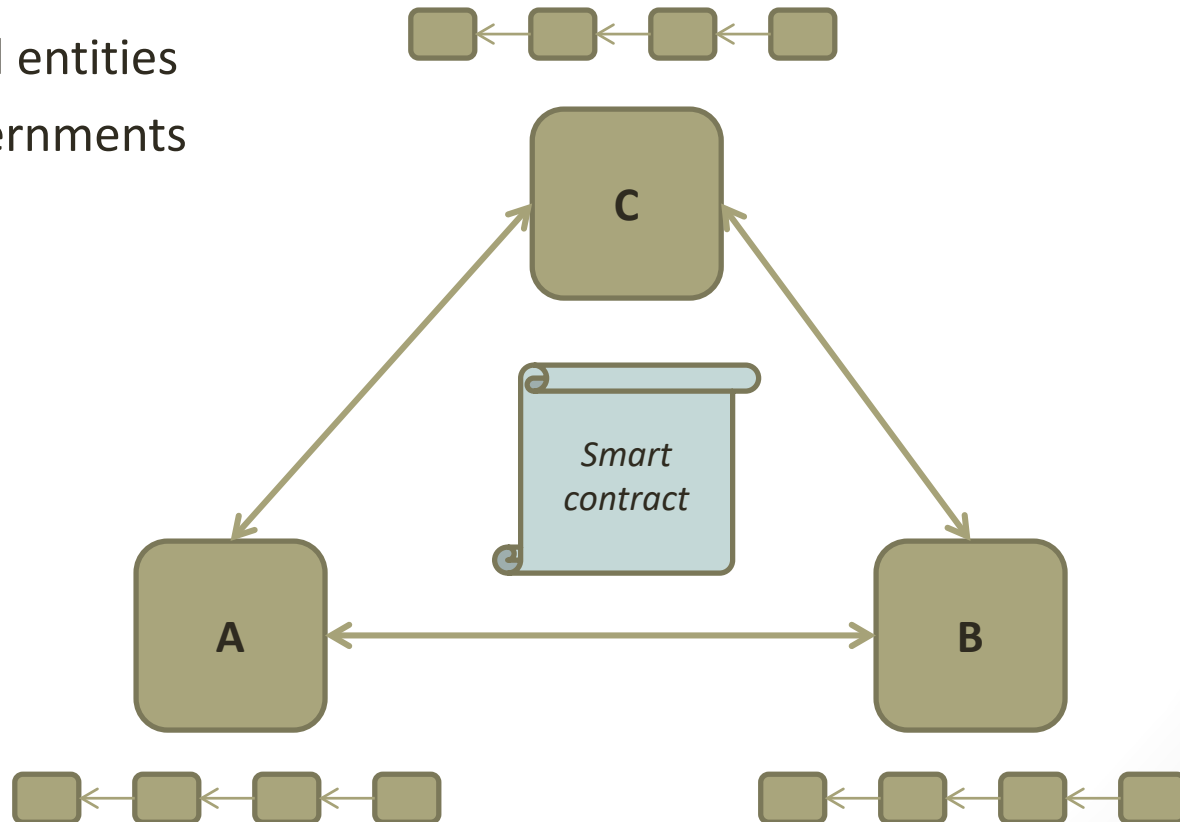
- Execution of more complex programs on chain data
  - Turing complete language
  - Smart Contracts
  - Self regulating stakeholders
  - A whole new set of applications





# Blockchain applications

- Smart contracts: a new way of self governance
- Can encode legal agreements between
  - Individuals
  - Legal entities
  - Governments



*Thank you*