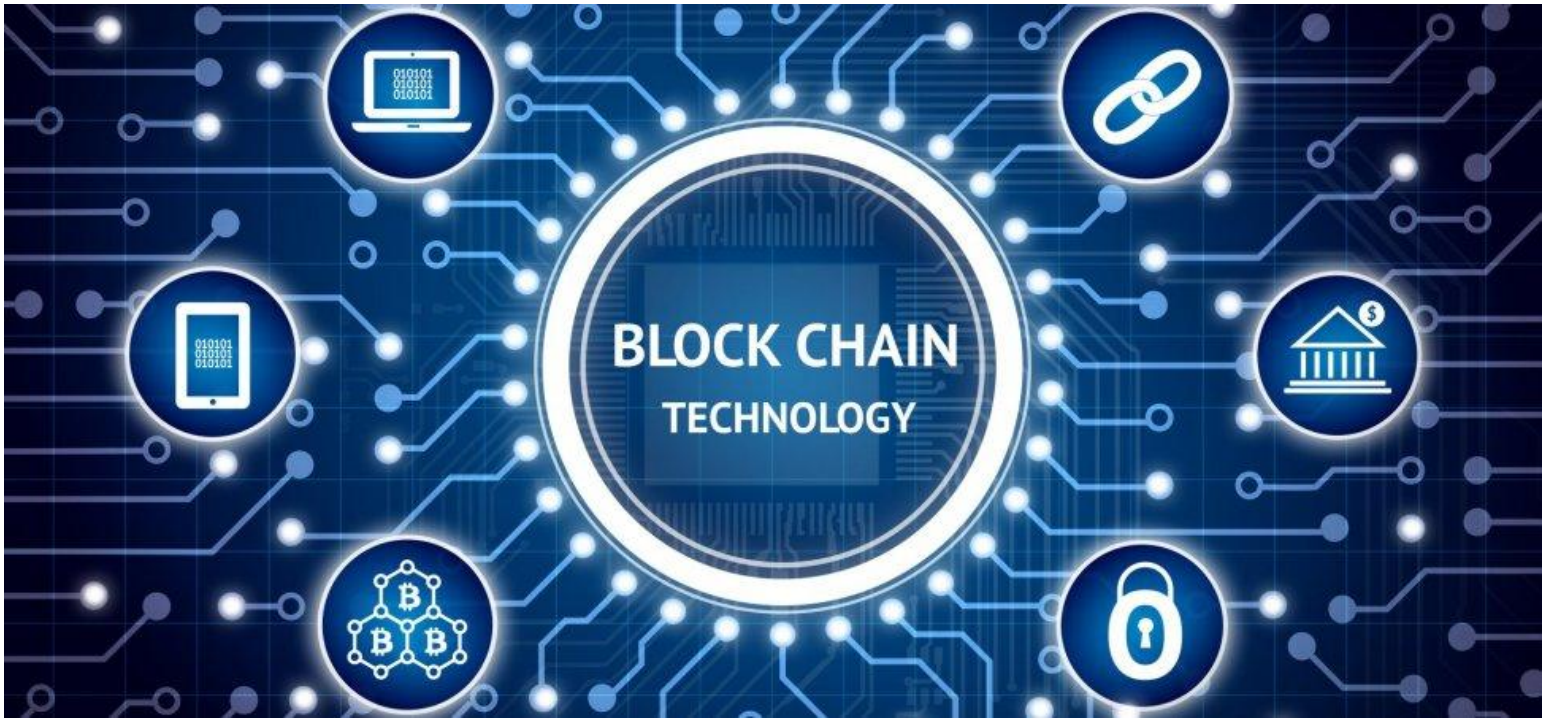
Blockchain: The New Technology of Trust

DECEMBER, 18 2017



Agenda

1. Context
2. Learning
3. Definitions
4. Use cases
5. Best practices

CONTEXT

Context


7:06
100%
Dashboard
BTC ETH LTC
€4.852,42
Prezzo bitcoin
€765,27
da ieri
1H 1G 1S 1M 1A TUTTO
€4.787,50
€4.499,12
€4.210,74
10:28 13:52 17:16 20:40 00:04 03:28


1h 12h 1d 1w 1m 3m 1y All
Jul 18, 2010 to Oct 15, 2017
16/10/2016: 639 $
16/10/2017: 5.580 $
13/12/2017:14.600 $
$5000
$4000
$3000
$2000
$1000
$0
coindesk
CoinDesk BPI in effect
2012
2014
2016

Context

Satoshi Nakamoto

It is the name of the person, or people, who designed the **bitcoin** and developed the first implementation. Within that deployment, they also created the first distributed database based on the model called **Blockchain**.
At present his identity is still **unknown**. It is believed to possess about one million bitcoins.

Satoshi Nakamoto publishes **his white paper**, explaining his idea of money virtual peer-to-peer solution by solving the problem of double-spend

The beginnings

2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014

Bad reputation

Relationship with Regulators

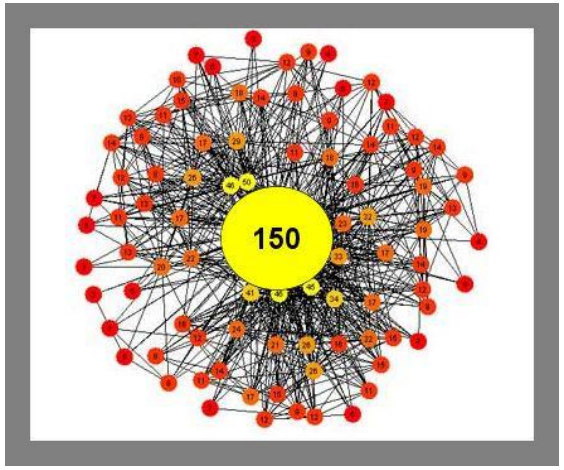
Not only Bitcoin

Context

Byzantine Generals' Problem (1980)

- Generals can communicate using messengers, cannot have a summit
- There are traitors amongst them
- Must decide unanimously whether to attack
- Success is achieved if the loyal general can agree on their strategy, whatever it might be

(Used in fault-tolerant computer systems, and in particular distributed computing systems)



Dunbar's number (anthropologist, 1990)

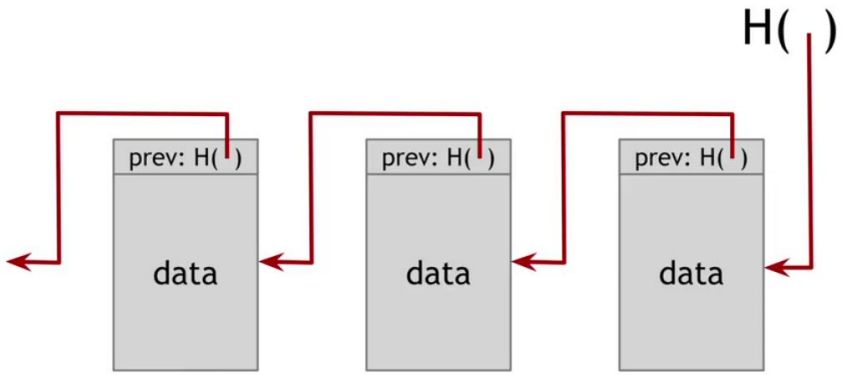
- 150 is the number of people with whom one can maintain stable social relationships.
- Numbers larger than this generally require more restrictive rules, laws, and enforced norms to maintain a stable, cohesive group.

Context

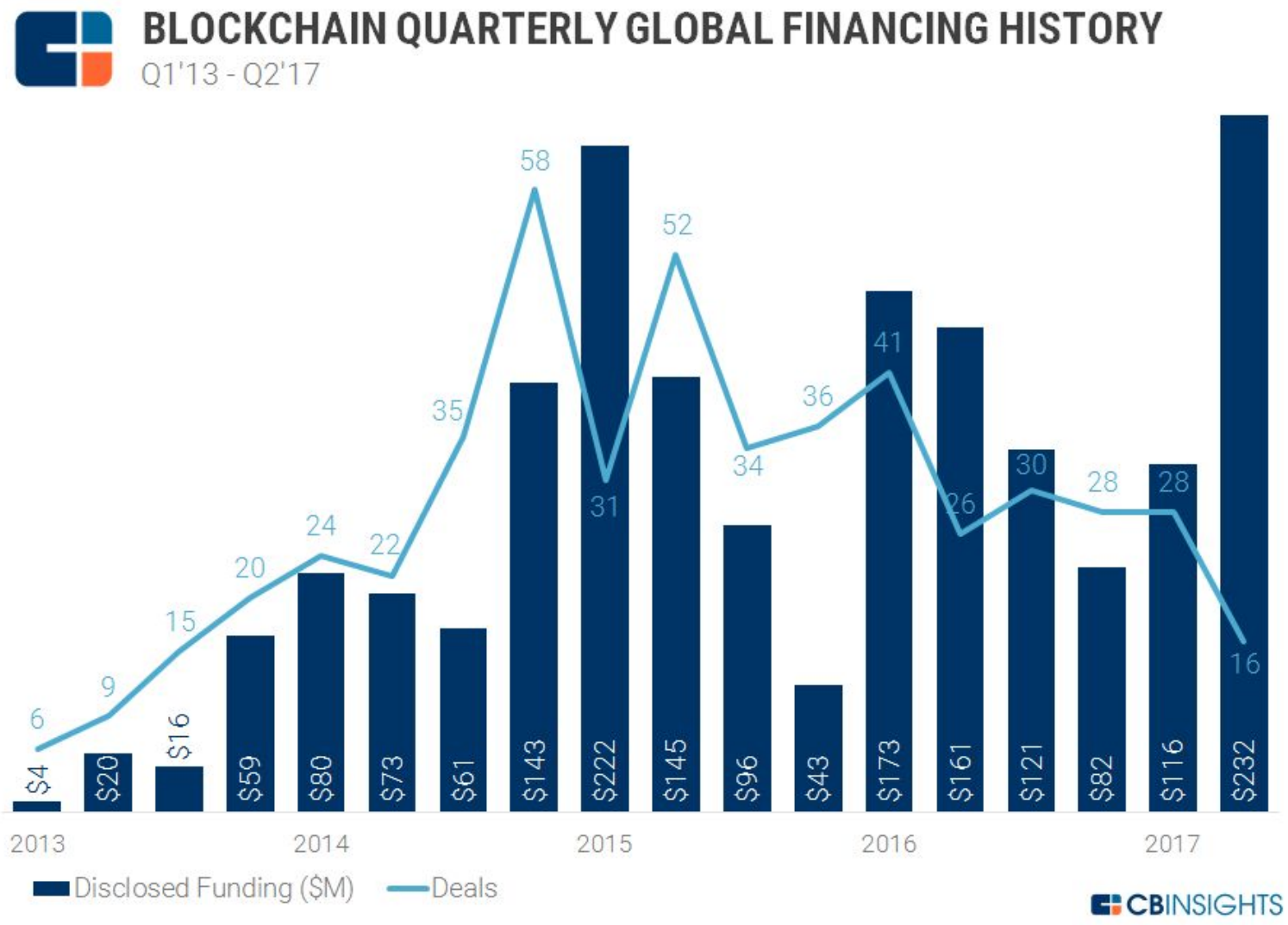
BLOCKCHAIN

A **Blockchain** is a continuously growing list of **records**, called *blocks*, which are linked and secured using **cryptography**. Each block typically contains a **hash** pointer as a link to a previous block, a **timestamp** and transaction data. By design, Blockchains are inherently resistant to modification of the data. A Blockchain can serve as "*an open, **distributed ledger** that can record transactions between two parties efficiently and in a verifiable and permanent way.*"

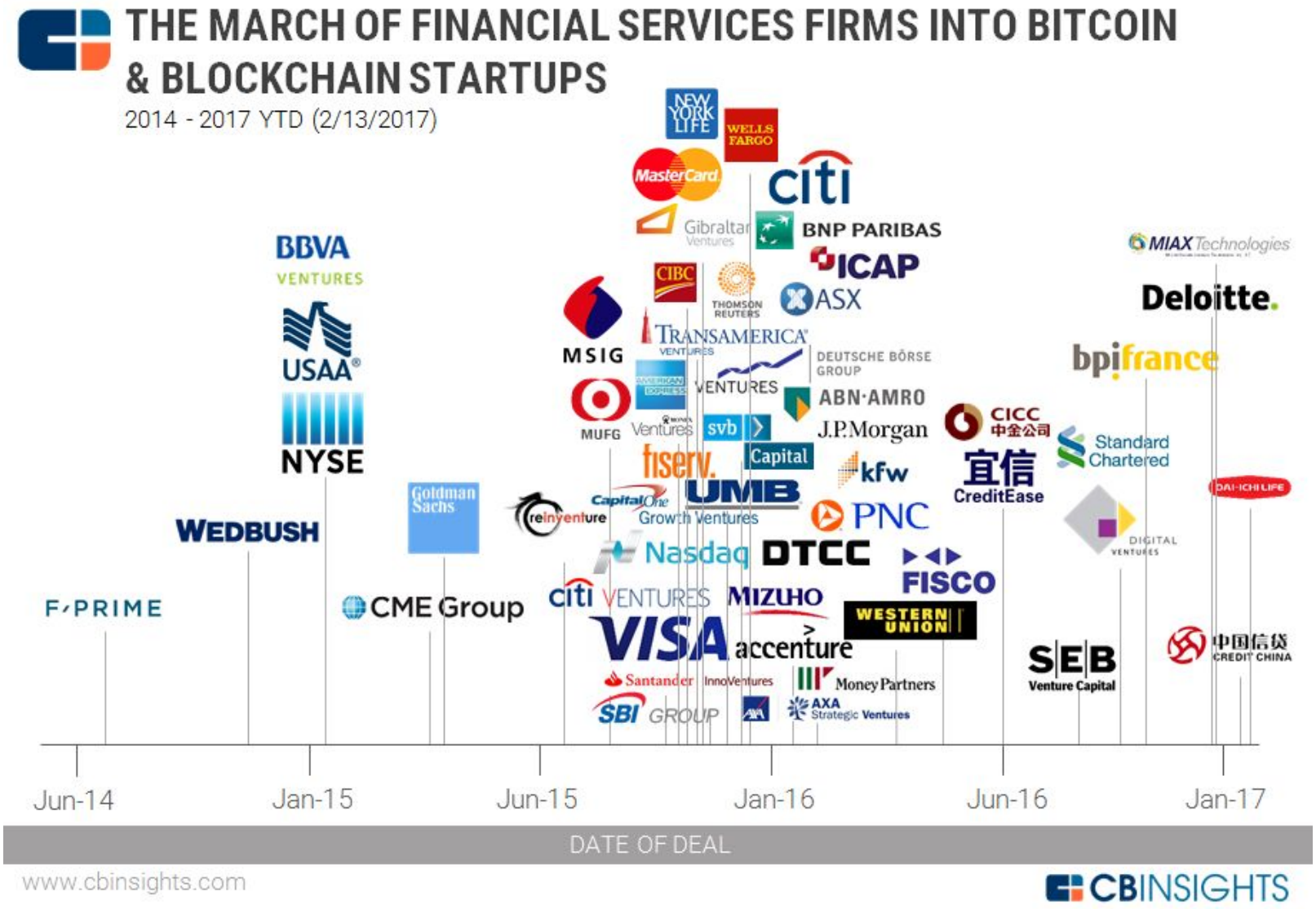
For use as a distributed ledger, a Blockchain is typically managed by a **peer-to-peer** network collectively adhering to a protocol for validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which needs a collusion of the network majority.



Context


BLOCKCHAIN QUARTERLY GLOBAL FINANCING HISTORY
Q1'13 - Q2'17
$4
$20
$16
$59
$80
$73
$61
$143
$222
$145
$96
$43
$173
$161
$121
$82
$116
$232
6
9
15
20
24
22
35
58
31
52
34
36
41
26
30
28
28
16
2013
2014
2015
2016
2017
Disclosed Funding ($M)
Deals
CBINSIGHTS

Context


THE MARCH OF FINANCIAL SERVICES FIRMS INTO BITCOIN & BLOCKCHAIN STARTUPS
2014 - 2017 YTD (2/13/2017)
NEW YORK LIFE
WELLS FARGO
MasterCard
citi
Gibraltar Ventures
BNP PARIBAS
MIAX Technologies
BBVA VENTURES
ICAP
CIBC
THOMSON REUTERS
ASX
Deloitte.
USAA
NYSE
MSIG
TRANSAMERICA VENTURES
DEUTSCHE BÖRSE GROUP
bpifrance
AMERICAN EXPRESS
VENTURES
ABN·AMRO
MUFG
Ventures
svb
J.P.Morgan
CICC 中金公司
Standard Chartered
fiserv.
Capital
kfw
宜信 CreditEase
DAI-ICHI LIFE
Goldman Sachs
reinventure
Capital One Growth Ventures
UMB
PNC
DIGITAL VENTURES
WEDBUSH
Nasdaq
DTCC
FISCO
F/PRIME
CME Group
citi VENTURES
MIZUHO
WESTERN UNION
VISA
accenture
SEB Venture Capital
中国信贷 CREDIT CHINA
Santander InnoVentures
Money Partners
SBI GROUP
AXA Strategic Ventures
Jun-14
Jan-15
Jun-15
Jan-16
Jun-16
Jan-17
DATE OF DEAL
www.cbinsights.com
CBINSIGHTS

Context

Walmart
Maersk
everledger

Eternity Wall

Check out process
Traceability and Supply Chain (GS1)
Wallet and exchange integration
SPID authentication

Ownership
Online voting
Ticketing / Couponing
Secure gateways
Authentication
Insurance
IoT messaging platform

Context

TechCrunch

IBM unveils Blockchain as a Service based on open source Hyperledger Fabric technology

Posted Mar 19, 2017 by Ron Miller (@ron_miller)

FT FINANCIAL TIMES

Banks team up with IBM in trade finance blockchain

System will track goods and release payments as they move around the world

Microsoft announces the Coco Framework to improve performance, confidentiality and governance characteristics of enterprise blockchain networks

August 10, 2017 | Microsoft News Center

BUSINESS INSIDER

Oracle launches blockchain service

Laurie Beaver

Oct. 3, 2017, 7:15 PM 278

LEARNING

Learning

POLITECNICO MILANO 1863
SCHOOL OF MANAGEMENT

OSSERVATORI.NET digital innovation

Workshop: "*Blockchain and Distributed Ledger*" (5 meetings)

Event: "*Il fenomeno Blockchain: oltre le cripto-valute, verso una internet dei valori*"

ASE Associazione Utilizzatori Sistemi E tecnologie Dell'informazione

UNIVERSITÀ DEGLI STUDI DI TRENTO
Dipartimento di Matematica

Laboratorio di Matematica Industriale e Crittografia

Course: "*Bitcoin, Blockchain and their new Frontiers*" (1 day)

MOOC course: "*Blockchain for Business - An Introduction to Hyperledger Technologies*" (2 months)

THE LINUX FOUNDATION
edX

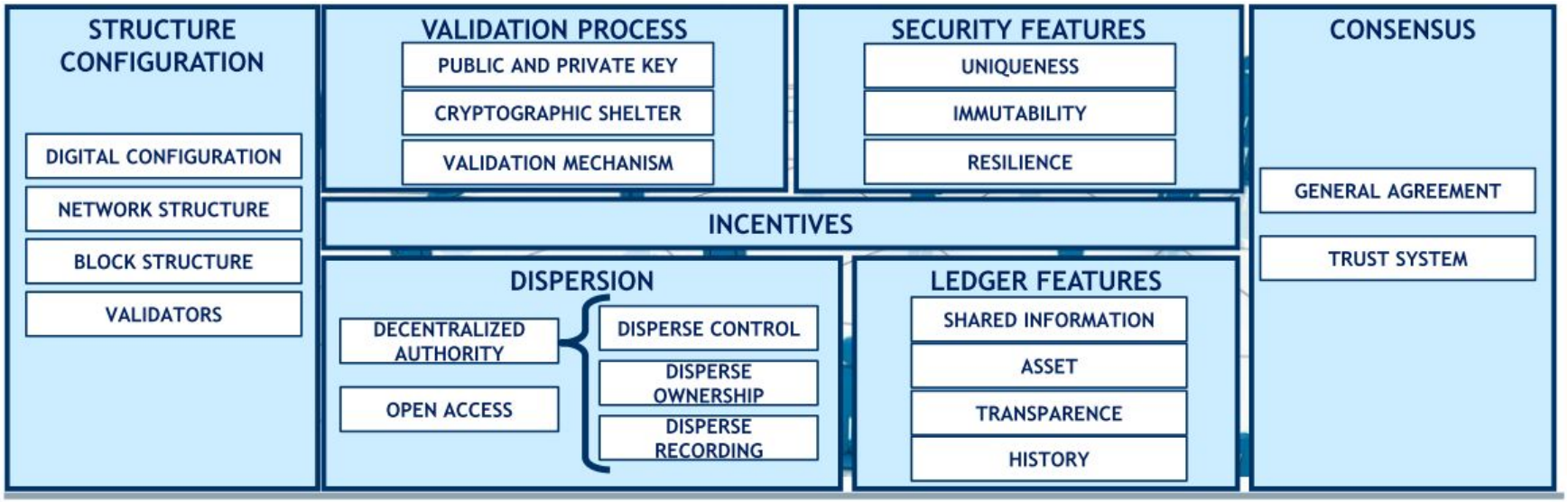
DEFINITIONS

Definitions

Blockchain is a technology which contains a shared ledger of transactions between **multiple nodes of a network**, **validated by the same network** and **block structured** (a chain of blocks that contains multiple transactions).

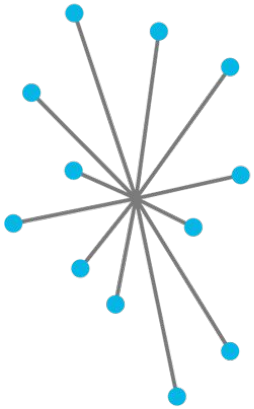
The main features are:

- **traceability** by all network participants
- **immutability**
- **security** through cryptographic systems

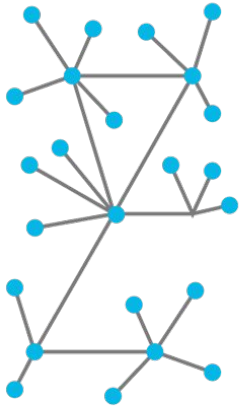


Definitions

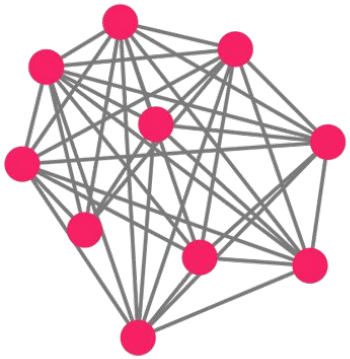
Centralized

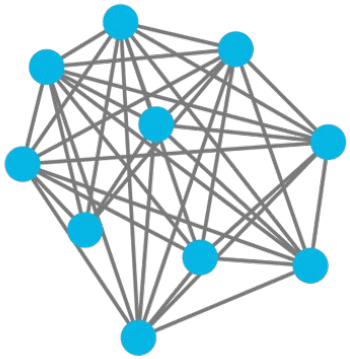


Decentralized



Distributed Ledgers





The New Networks

Distributed ledgers can be public or private and vary in their structure and size.

Public blockchains

Require computer processing power to confirm transactions (”mining”)

- Users (●) are anonymous

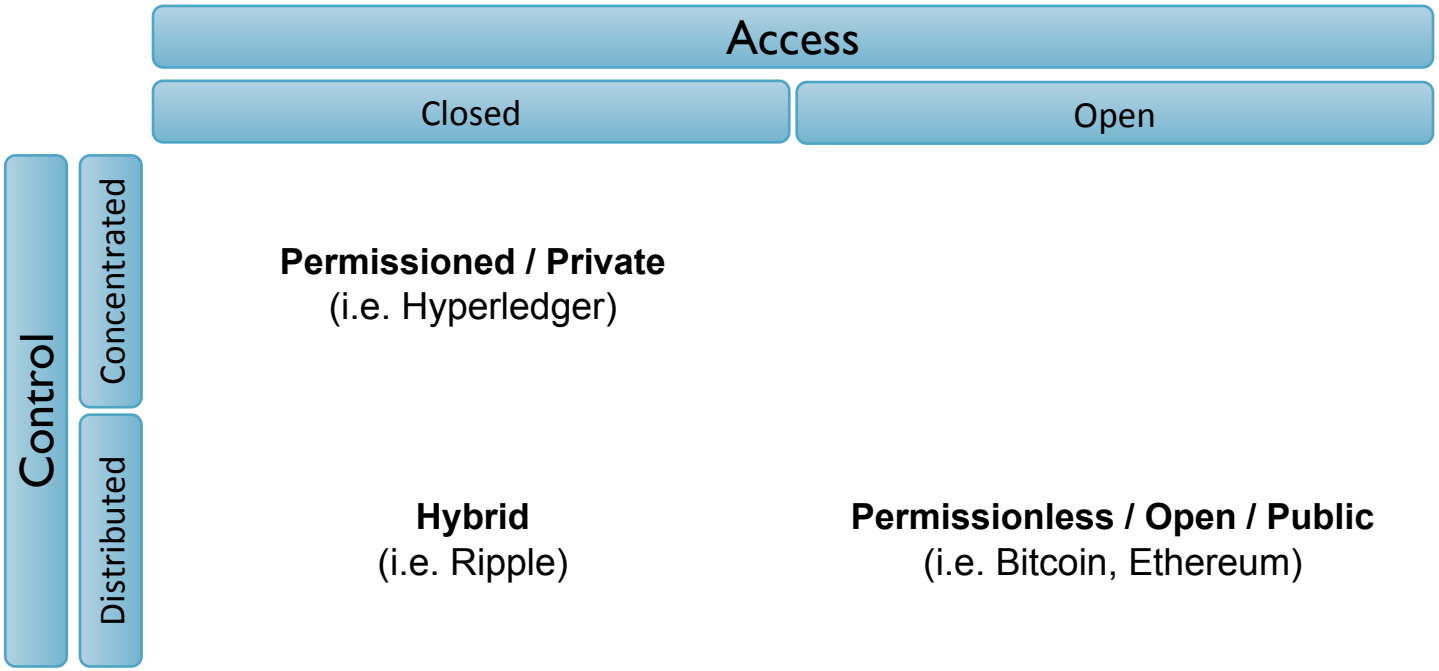
- Each user has a copy of the legder and partipates in confirming transactions independently

- Users (●) are not anonymous

- Permision is required for users to have a copy of the legder and participate in confirming transactions

Blockgeeks

Definitions



	Public	Private
Access	Open read/write access to database	Permissioned read and/or write access to database
Speed	Slower	Faster
Security	Proof-of-Work/ Proof-of-Stake	Pre-approved participants
Identity	Anonymous/ pseudonymous	Known identities
Asset	Native assets	Any asset

What people say?

Bitcoin purists: any control makes the Blockchain vulnerable and less efficient.
Hybrids: use Bitcoin to periodically validate a private Blockchain.
Blockchain fans: Blockchains can be applied to every area.

Definitions

Consensus: process of achieving agreement among the network participants as to the correct state of data on the system. Consensus leads to all nodes sharing the exact same data.

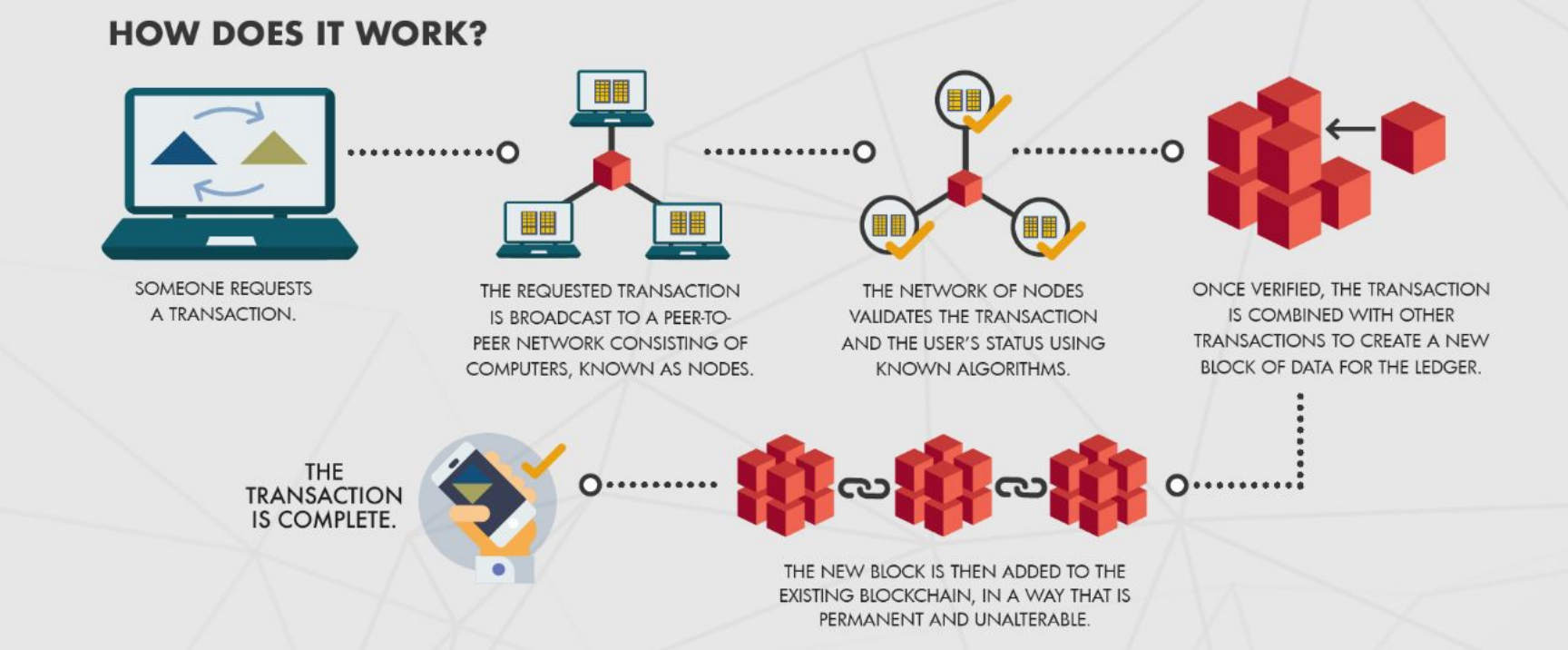
A **consensus algorithm** does two things:

- it ensures that **the data on the ledger is the same for all the nodes**
- **prevents malicious actors from manipulating the data**.

Examples of consensus algorithms are:

- **Proof of Work:** requires computation power (i.e. Bitcoin)
- **Proof of Stake:** depends on the amount owned by the miner and its age
- **Proof of Burn:** some coins are burnt (sent to unspendable address)
- **Proof of Elapsed Time:** each validator is given a random wait time (HyperLedger)
- **Proof of Authority:** the majority of authorities must agree on block insertion (permissioned ledgers)

Definitions

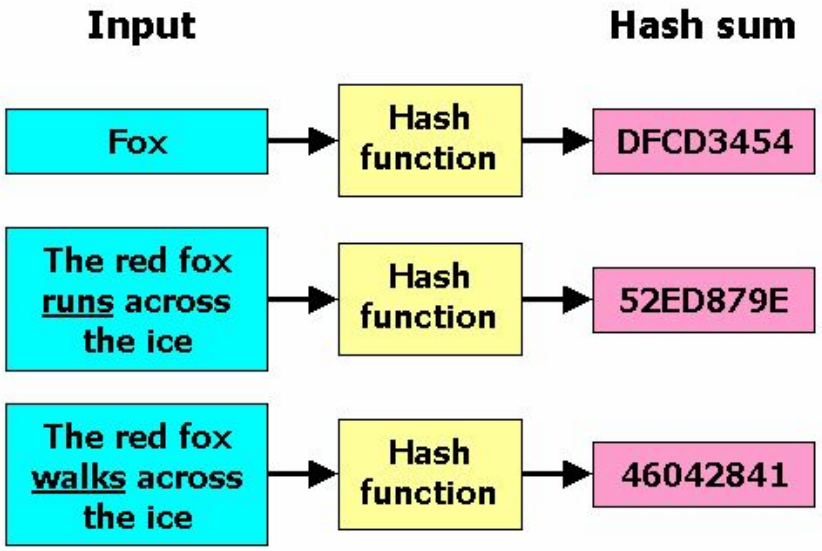


When people say that Blockchains are immutable, they don't mean that the data can't be changed, they mean it is extremely hard to change without collusion, and if you try, it's extremely easy to detect the attempt.

Definitions

Hash functions:

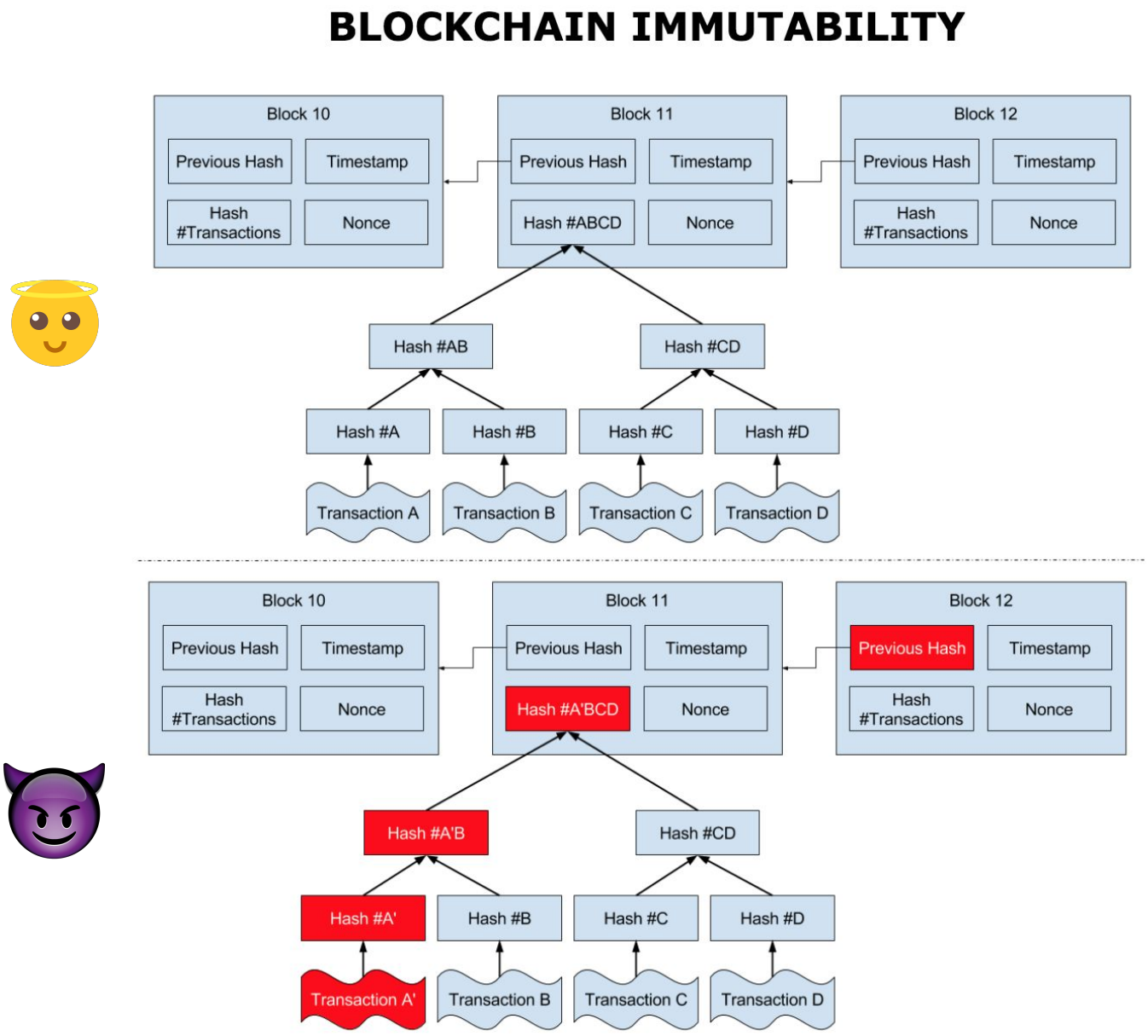
- **collision-free**: it's practically impossible to find x ≠ y, such that H(x)=H(y)
- **pre-image resistant**: if we know H(x), we can't retrieve x
- **second pre-image resistant**: given an output value y=H(x) it should be very difficult to find x' such that H(x')=y



Consequences:

- **Collision free:** we are almost sure that if H(x)=H(y) => x=y ('file fingerprint')
- **Pre-image resistant:** it's like sealing something into an envelope. We can publish the hash (closed envelope). We can prove that x was the envelope content.
- **Second pre-image resistant** -> grants the difficulty of the mathematical problem (proof-of-work) that miner's need to solve in order to insert new blocks. The only possible approach is brute force.

Definitions

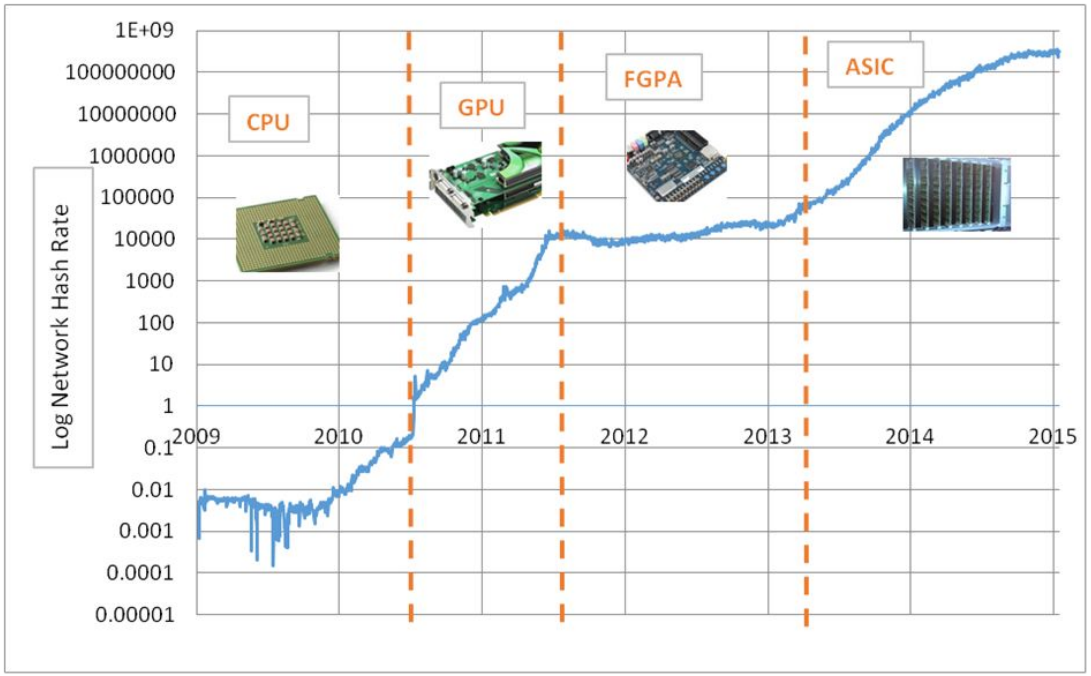


Definitions

Miners (Bitcoin):

- contribute to the system management in exchange for a reward
- have to solve a difficult problem in order to gain the right to insert a new block (i.e. hash starting with a certain number of 0)
- receive transactions fees plus minted Bitcoins

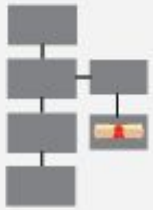
As the number of miners and overall computation power grow, mining is becoming more difficult.



Definitions

Smart Contracts

Option contract written as code into a blockchain.



Contract is part of the public blockchain.

Parties involved in the contract are anonymous.

Contract executes itself when the conditions are met.

Regulators use blockchain to keep an eye on contracts.

Happy Hustlin'

https://codebrahma.com

USE CASES

Use cases

Sectors	Processes								
	Data & Document management	Property transaction	Capital markets	Payment	Supply chain finance	Tracking & Supply chain	Identity	Voting	Marketing
Agri-food						8			
Automotive	2								
Finance	12		35	48	11	8	6	5	
Government	4	4					5		
Healthcare	4								
Insurance	2			1					
Logistic	1					8			
Luxury						1			
Media									2
Utility	1			1		6			
Other	6					1			3

OSSERVATORI.NET digital innovation

Use cases

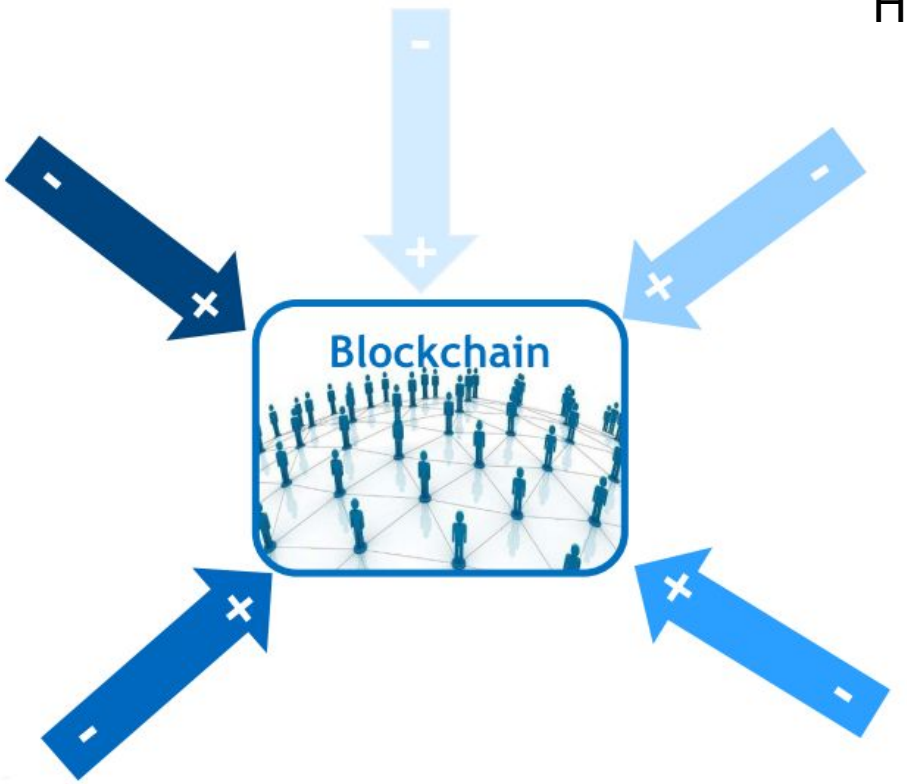
REPLY

Use cases

Confusion among participants

Importance of transparency and security

Heterogeneity among the actors



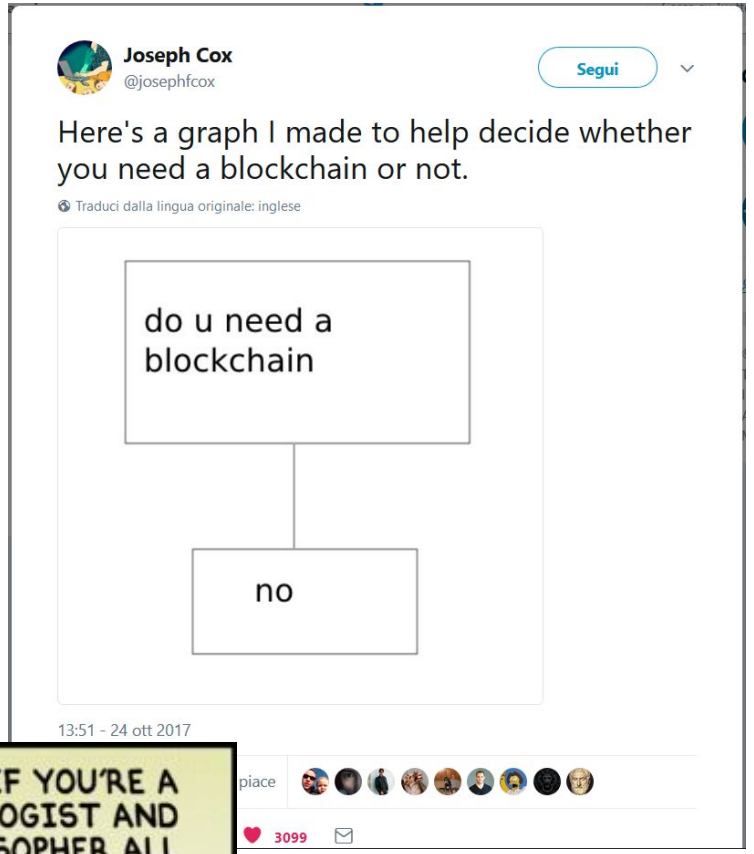
Need to share information

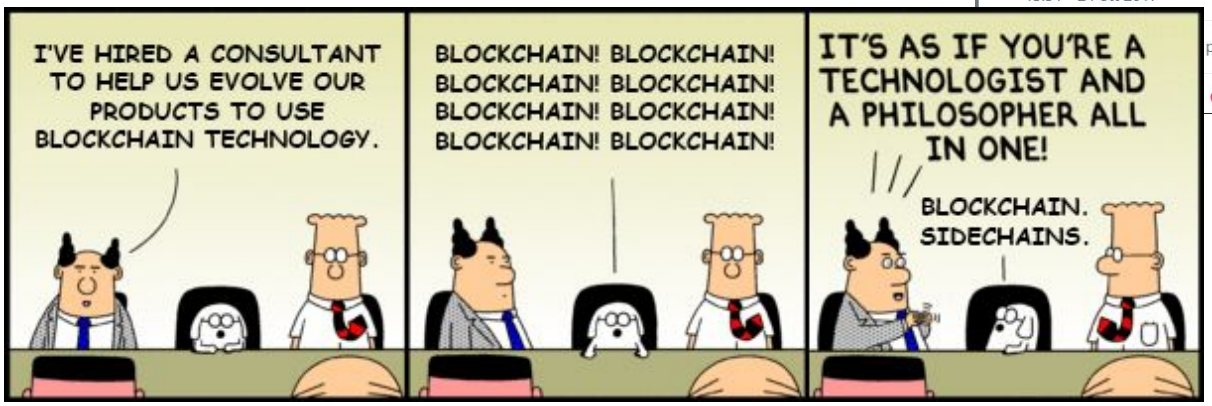
Numerous actors

Use cases

Do we **REALLY** need Blockchain?

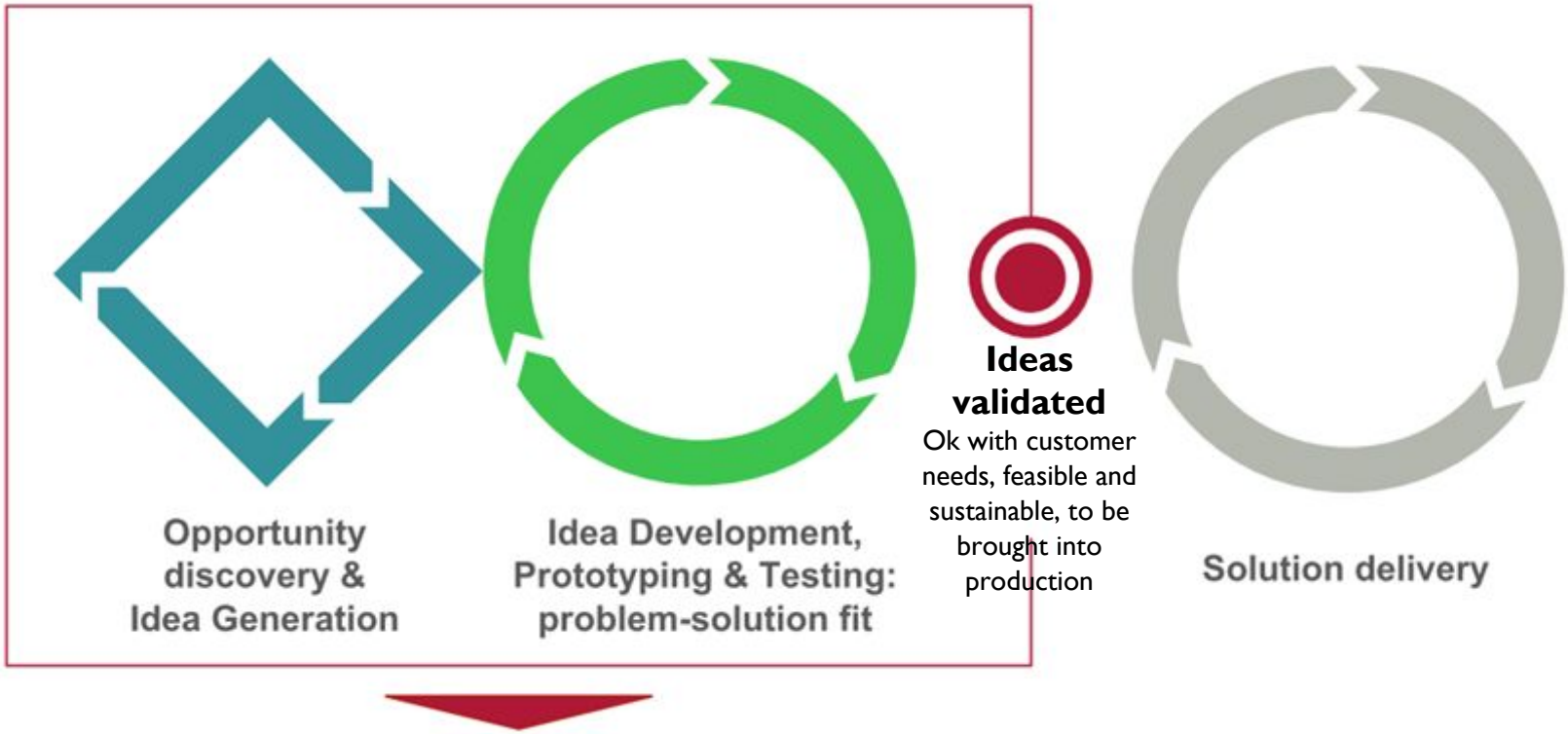
(80% no…)





BEST PRACTICES

Best practices



- Small cross-functional teams
- Free from constraints (hierarchical, legislative, etc.)
- Working "like a start-up"
- Open to collaboration (open-source all that you will do!)

:)


John McAfee
@officialmcafee
Segui
We have to go back, Marty!
Save the world?
No, buy bitcoins!
12:58 - 10 dic 2017
819 Retweet 2.198 Mi piace

Marco Segato

Project Manager

https://www.linkedin.com/in/marcosegato/

@machms

Passionate with **#linux #opensource #innovation**
My interests: **#rock #reading #photo #cinema #theatre**