



# Information Security and Blockchain

Andrea Vitaletti

Università degli studi di Roma "La Sapienza"

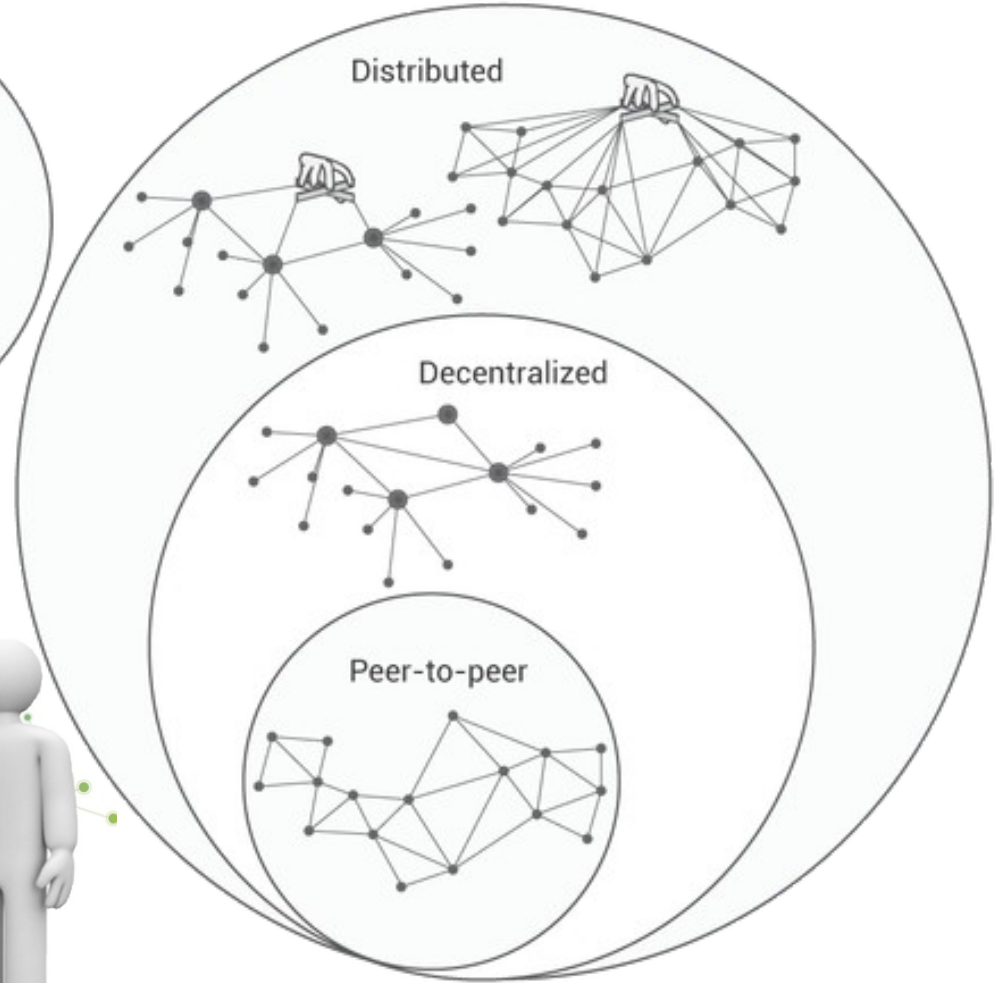
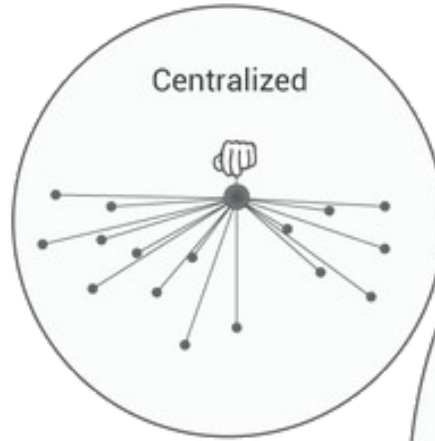
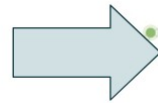
vitaletti@diag.uniroma1.it

Special Thanks to prof. Hervé Debar



# PART I

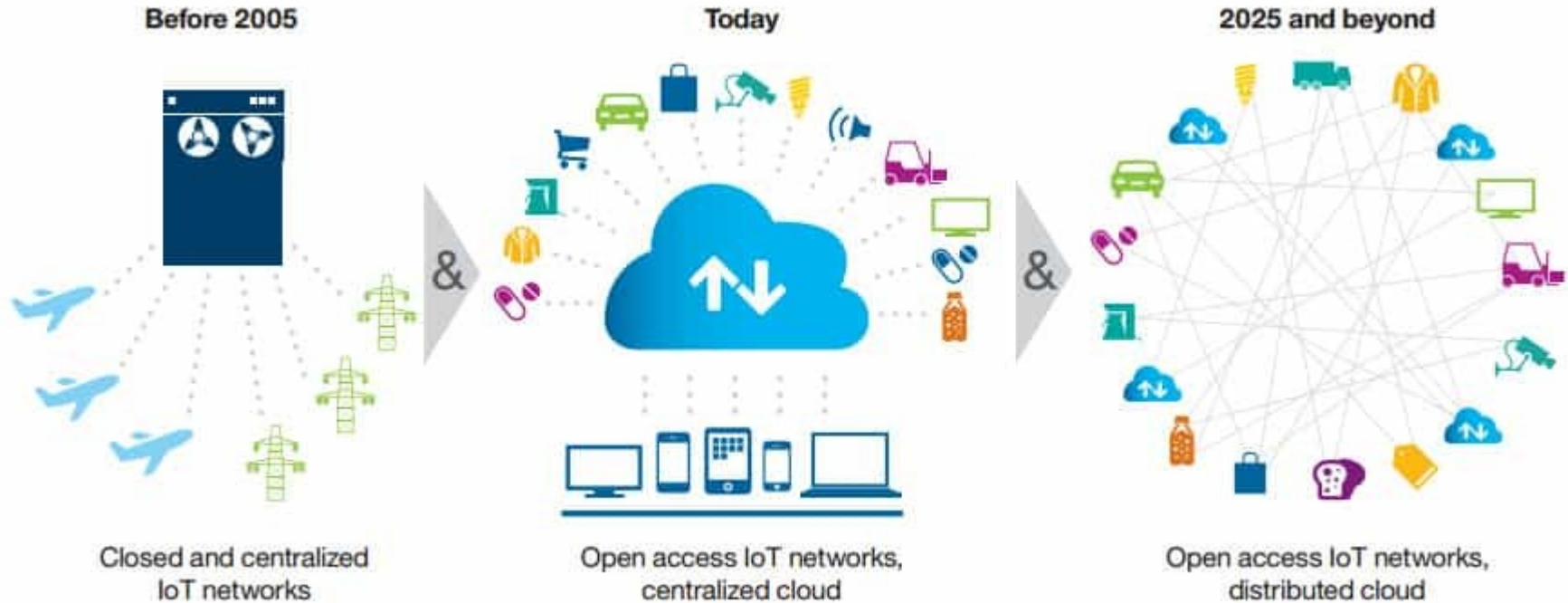
## Blockchain in about 10 slides



La sicurezza informatica dei dispositivi medici



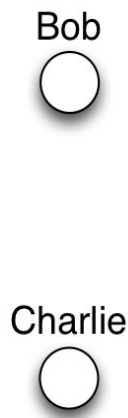
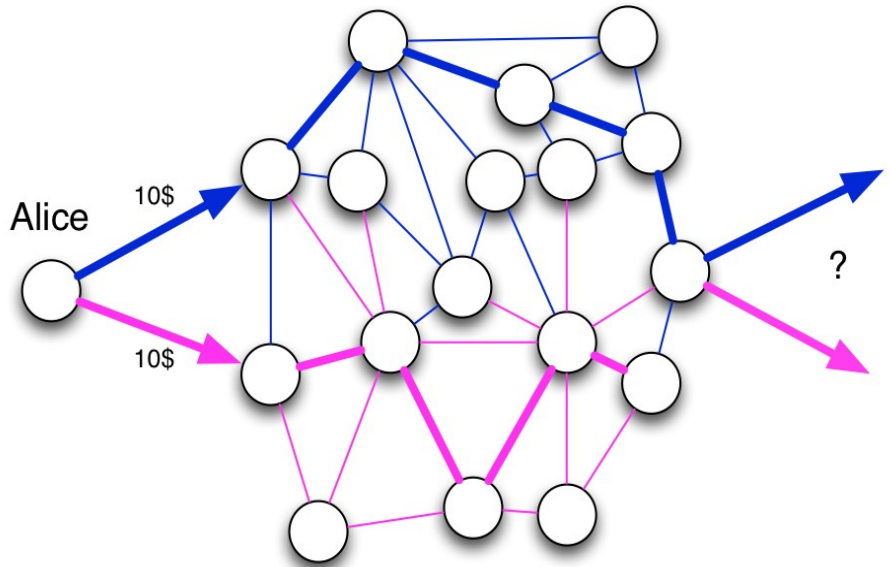
# Evolution of computing



Source: IBM



# Consensus in P2P



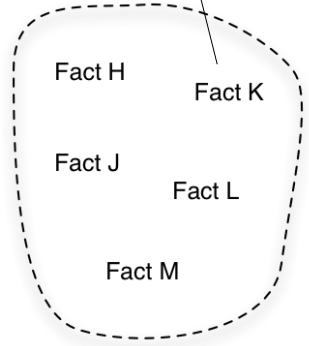
Alice → Bob(10\$)

Alice → Charlie(10\$)

**Block 20**  
Fact B  
Fact D  
Fact A

**Block 21**  
Fact C  
Fact F  
Fact H

**Block 22**  
Fact E  
Fact G  
Fact I



Confirmed facts

Pending facts

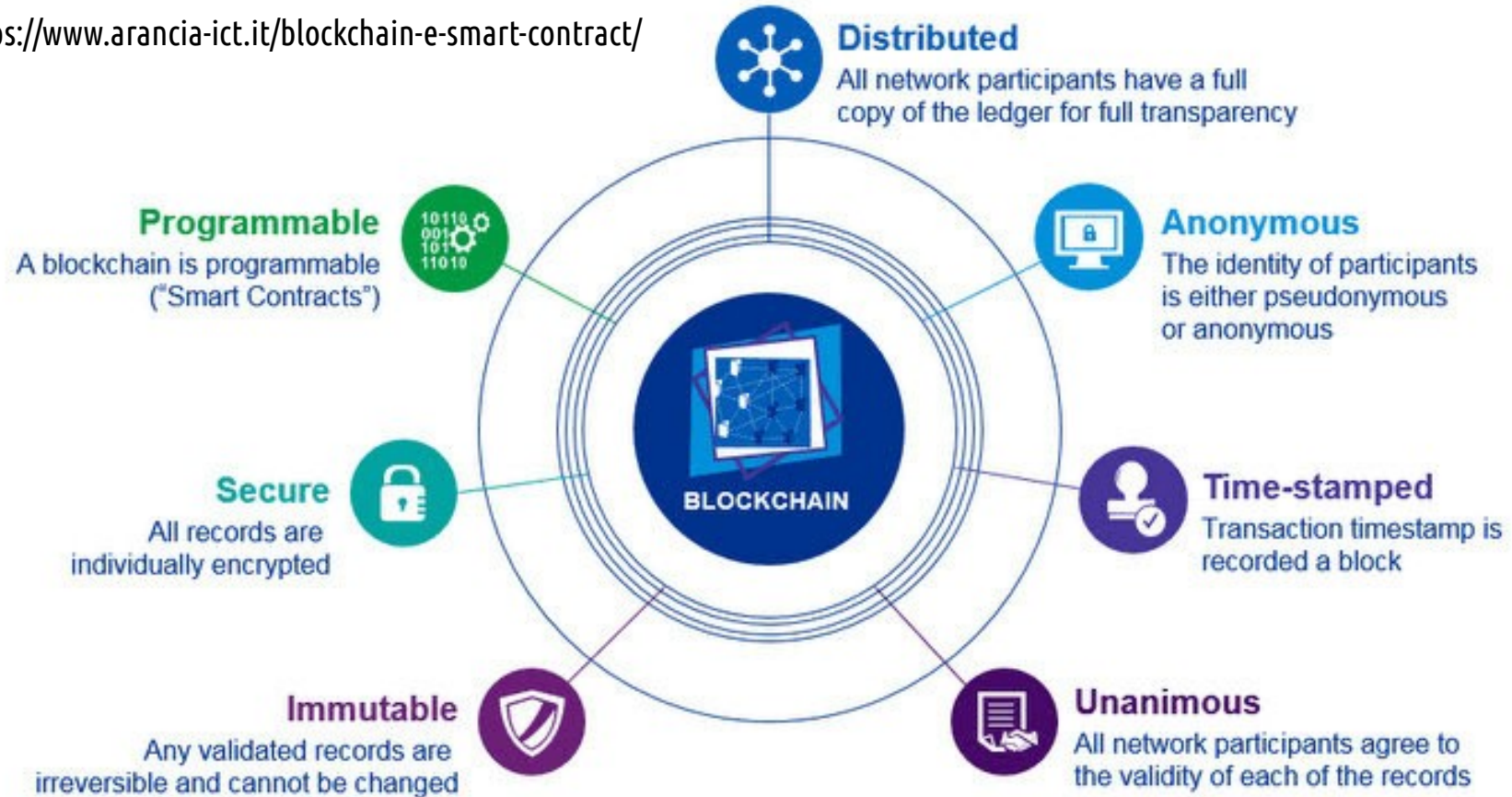
“If two **incompatible** facts arrive in the network, the first one to be recorded wins.”

Source: <https://marmelab.com/>



# Blockchain Properties

Source: <https://www.arancia-ict.it/blockchain-e-smart-contract/>

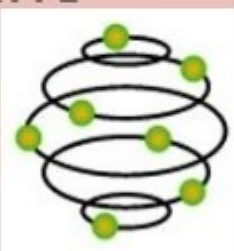





# Types of Blockchain

Source: blockchainappfactory.com


	<b>PUBLIC</b>	<b>PRIVATE/CONSORTIUM</b>
<b>ACCESS</b>	OPEN READ/WRITE	PERMISSIONED READ AND/OR WRITE
<b>SPEED</b>	SLOWER	FASTER
<b>SECURITY</b>	PROOF OF WORK PROOF OF STAKE OTHER MECHANISMS	PRE-APPROVED PARTICIPANTS
<b>IDENTITY</b>	ANONYMOUS PSEUDONYMOUS	KNOWN IDENTITIES



Public



Private



Consortium



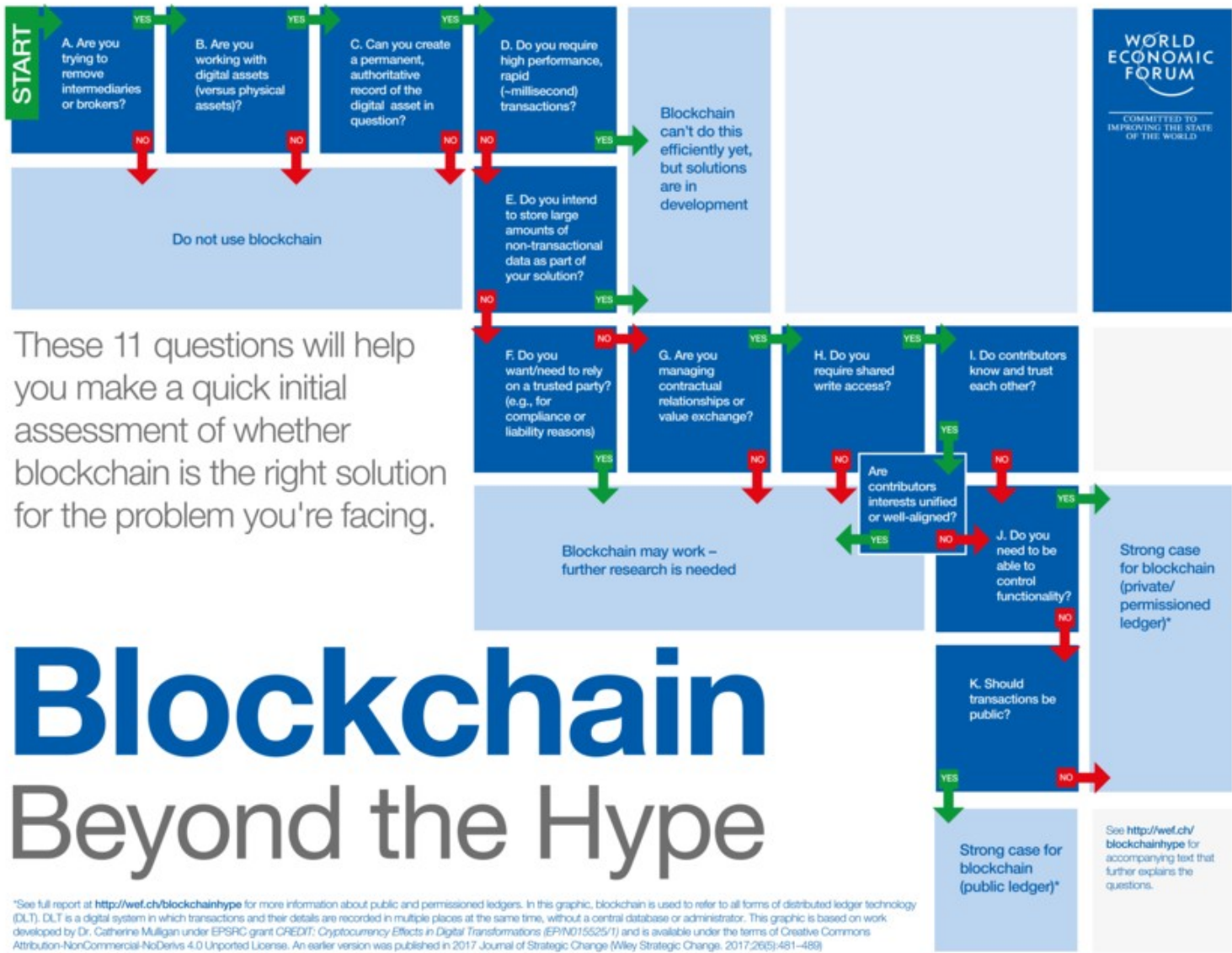
# Blockchain is not a DB

- CRUD vs **CRAB**
- Centralized vs **Decentralized**
- Permissioned vs **permissionless**
- However can guarantee some properties of a DB
  - **Integrity of data**
  - **Time stamp**





# Do We need the Blockchain?



These 11 questions will help you make a quick initial assessment of whether blockchain is the right solution for the problem you're facing.

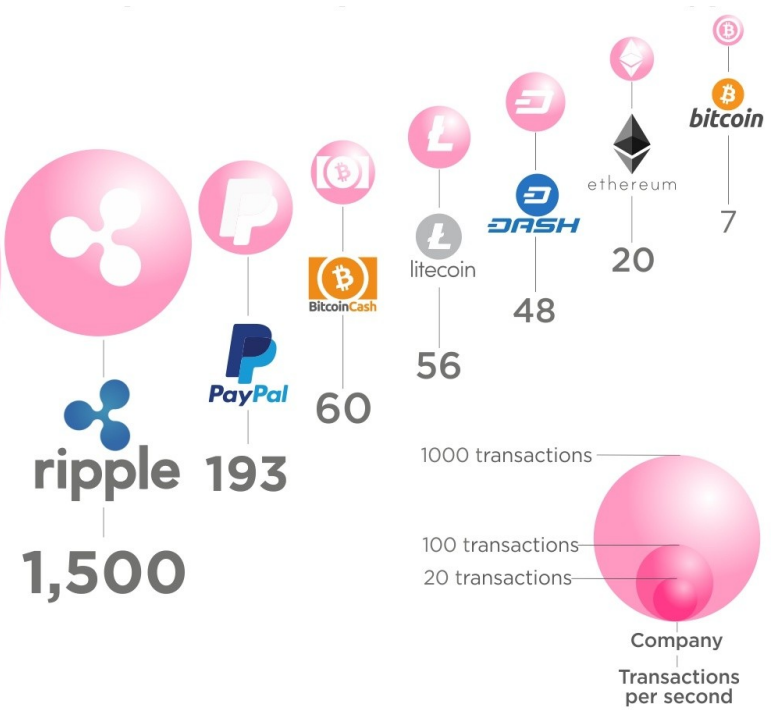
# Blockchain Beyond the Hype

\*See full report at <http://wef.ch/blockchainhype> for more information about public and permissioned ledgers. In this graphic, blockchain is used to refer to all forms of distributed ledger technology (DLT). DLT is a digital system in which transactions and their details are recorded in multiple places at the same time, without a central database or administrator. This graphic is based on work developed by Dr. Catherine Mulligan under EPSRC grant CREDIT: Cryptocurrency Effects in Digital Transformations (EP/R015525/1) and is available under the terms of Creative Commons Attribution-NonCommercial-NoDerivs 4.0 Unported License. An earlier version was published in 2017 Journal of Strategic Change (Wiley Strategic Change, 2017;26(5):481-488)

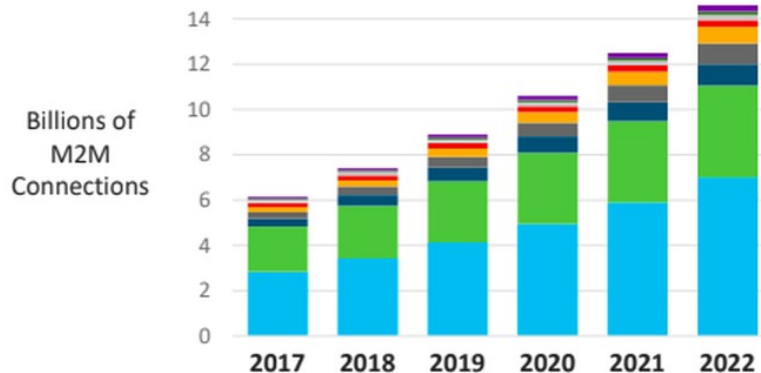
See <http://wef.ch/blockchainhype> for accompanying text that further explains the questions.



# Consensus and Verification at scale



howmuch.net



Article & Sources:  
<https://howmuch.net/articles/crypto-transaction-speeds-compared>  
<https://howmuch.net/sources/crypto-transaction-speeds-compared>



# From App to Dapp the "world computer"

## Apps

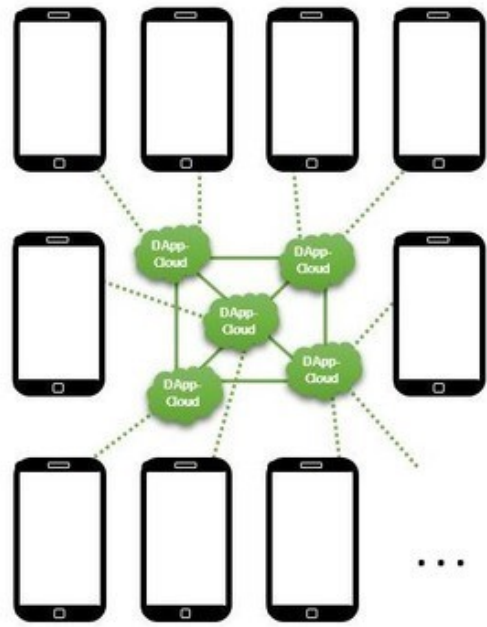
(classically centralized)



Source: Medium

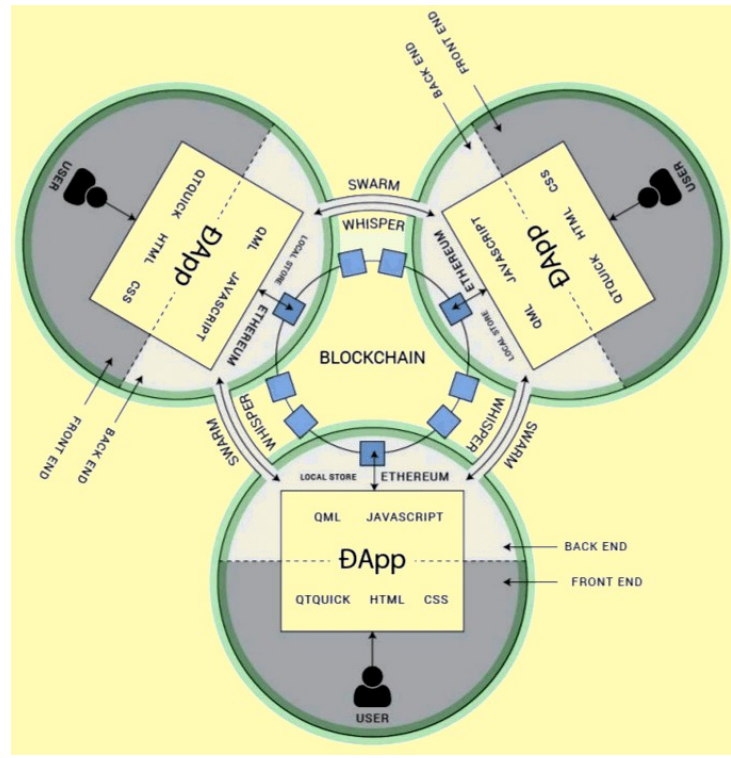
## DApps

(decentralized)



La sicurezza informatica dei dispositivi medici

Source: Héctor Ugarte on ResearchGate





# Smart Contracts

```
pragma solidity ^0.4.16;

contract MyToken {
    // This creates an array with all balances
    mapping (address => uint256) public balanceOf;

    // Initializes contract with initial supply tokens to the creator of the contract
    function MyToken(
        uint256 initialSupply
    ) {
        balanceOf[msg.sender] = initialSupply; // Give the creator all initial tokens
    }

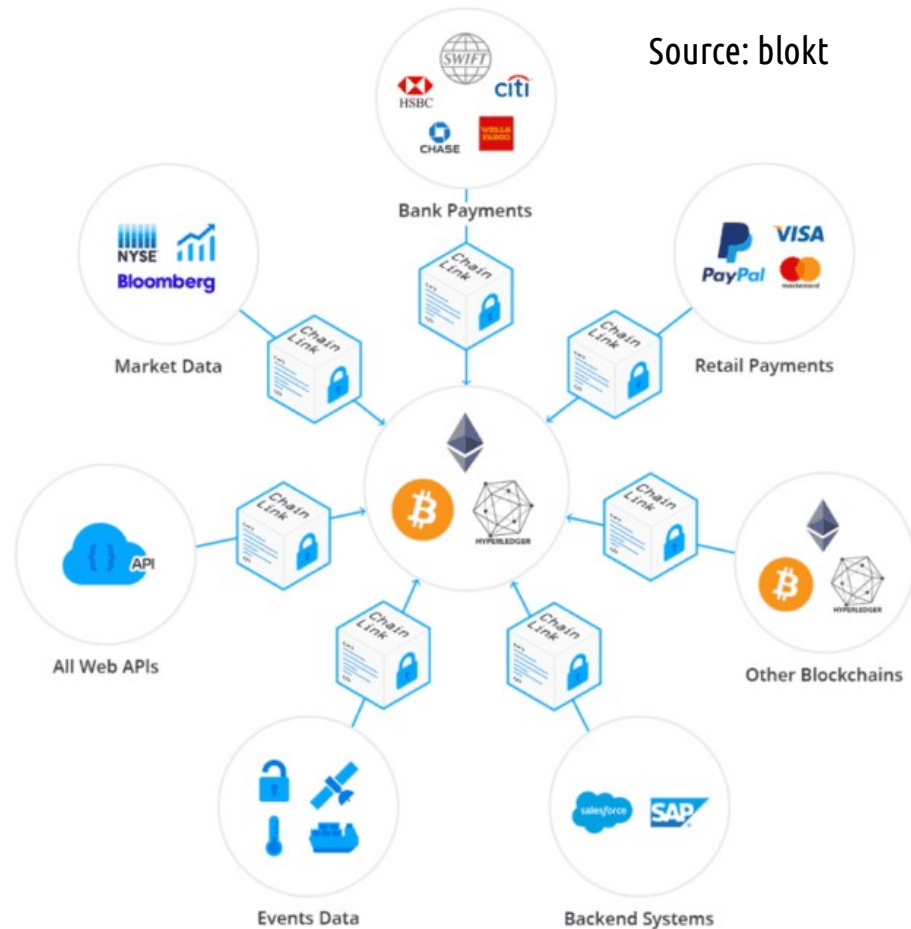
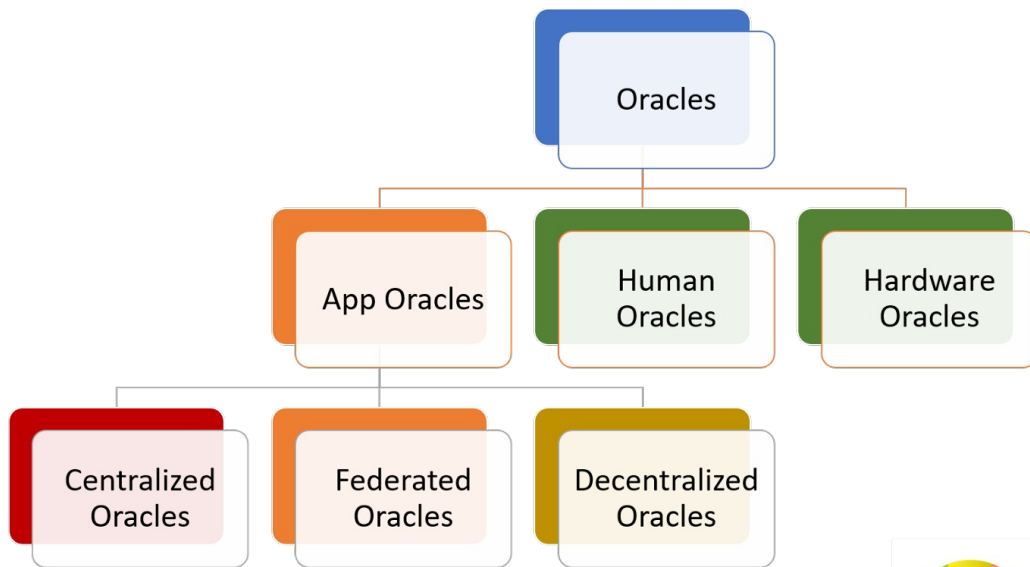
    // Send coins
    function transfer(address _to, uint256 _value) {
        require(balanceOf[msg.sender] >= _value); // Check if the sender has enough
        require(balanceOf[_to] + _value >= balanceOf[_to]); // Check for overflows
        balanceOf[msg.sender] -= _value; // Subtract from the sender
        balanceOf[_to] += _value; // Add the same to the recipient
    }
}
```

- Computer programs that may encode agreements, policies, rules and penalties that can not be arbitrarily altered once agreed and autonomously run on the blockchain.
- Transfer digital assets between parties

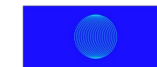


# Oracles: in-chani vs off-chain data

Source: blokt



Oracle Paradox Index



Source: [Hackernoon](#)

La sicurezza informatica dei dispositivi medici



# Blockchain and GDPR

- Data Controller vs Decentralized
- Right to erasure (art 17) and rectification (16) vs immutability
- Minimization vs Append-Only
- Blockchain and the General Data Protection Regulation – A study by EU\*

\* [https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS\\_STU\(2019\)634445\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf)



# PART II

## Blockchain in Healthcare

### A case study on medical device traceability



# Plenty of possibilities

<p><b>FINANCIAL</b></p>	<p><b>SUPPLY CHAIN</b></p>	<p><b>SPECIALTY</b></p>	<p><b>DNA</b></p>	<p><b>ELECTRONIC HEALTH RECORDS</b></p>
<p><b>MARKETPLACE</b></p> <p>MEDICAL PROVIDER</p> <p>SERVICES</p> <p>GOODS</p> <p>DATA</p>		<p><b>INCENTIVIZED PREVENTION</b></p>		<p><b>PREVENTION</b></p>
		<p>EST 2018</p> <p><b>THE BLOCKCHAIN HEALTHCARE ECOSYSTEM 2018</b></p> <p>SHERPAPROTOCOL.CO</p>		<p><b>INFORMATIONAL</b></p>
		<p><b>TELEMEDICINE</b></p>		

Source: The Blockchain Healthcare Ecosystem by SHERPA PROTOCOL

La sicurezza informatica dei dispositivi medici





# Medical Device Traceability

- EU Medical Device Regulation MDR (EU) 2017/745
- All medical devices covered by the EU MDR must carry a Unique Device Identifier (UDI) to ensure identification and allow for traceability.
- EU “Database” of all medical devices
- May 2020: MDR date of application

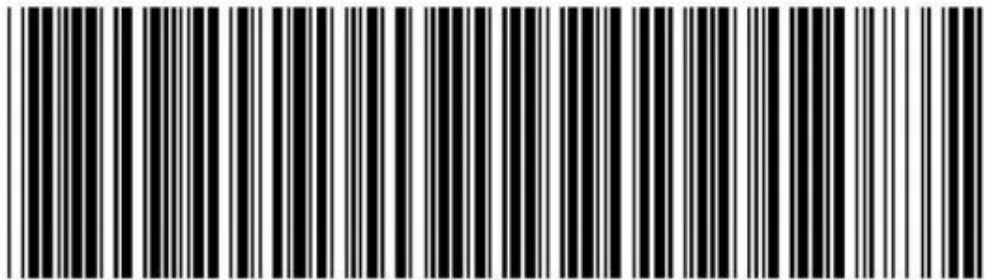


# Unique Device Identification (UDI)

Source: <https://easymedicaldevice.com/udi/>



Machine Readable

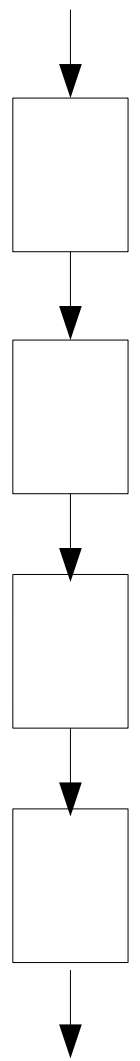


Human Readable

(01)00827002005112(17)000004(10)1234(21)8234

(01)	(17)	(10)	(21)
Device Identifier	Expiration date	Lot Number	Serial Number

Source: <https://www.nist.gov/cyberframework/new-framework>





# Classification of Vulnerabilities

	CVE	CWE	CVSS
Full Name	Common Vulnerabilities and Exposures	Common Weaknesses Enumeration	Common Vulnerabilities Scoring System
What is it?	A dictionary of publicly known security vulnerabilities and exposures.	A community-developed dictionary of software weakness types.	A vendor-agnostic industry open-standard designed to convey vulnerability severity.
Main Benefit	Easier to share vulnerability data across different databases and tools. Different security tools can now “talk” to each other using a common language.	Provides a standard measuring stick for software security.	Helps determine urgency and priority of response when vulnerabilities are detected.
Solution	Provides a baseline for evaluating the coverage of an organization’s security tools.	Provides a common baseline for weaknesses identification, mitigation and prevention efforts.	Solves the problem of multiple incompatible scoring systems.
More information	<a href="http://cve.mitre.org/index.html">http://cve.mitre.org/index.html</a>	<a href="https://cwe.mitre.org">https://cwe.mitre.org</a>	<a href="http://www.first.org/cvss">http://www.first.org/cvss</a>



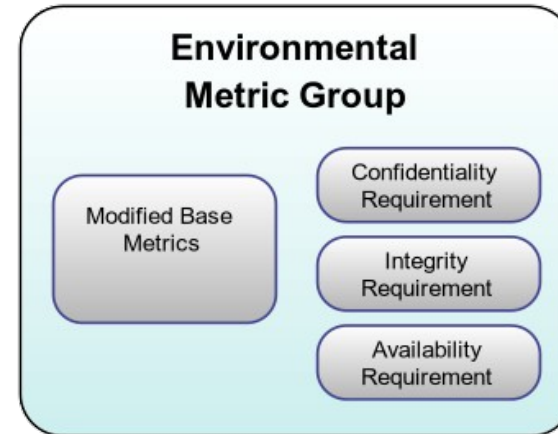
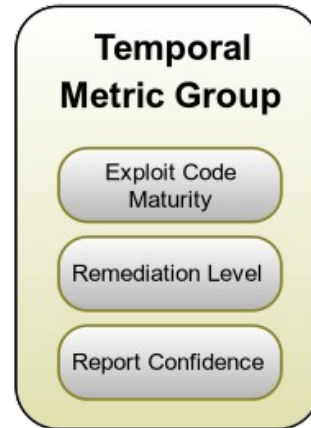
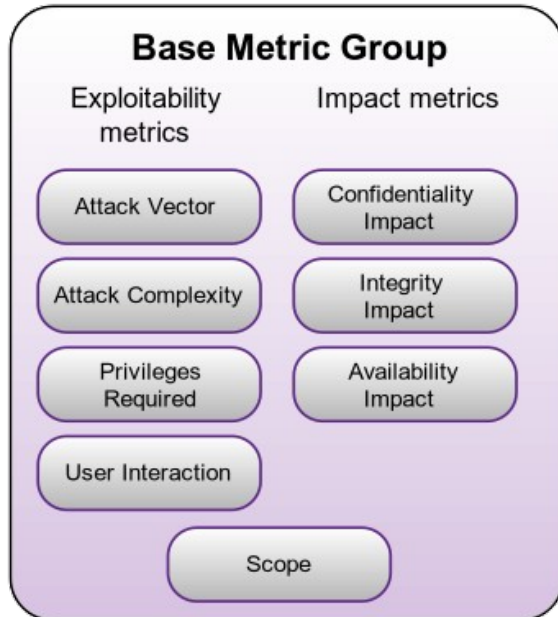
# CVE: Common Vulnerabilities and Exposures

- Dictionary of vulnerabilities found in software
  - Over 120000 entries since 1999
- Specific (product, version)
- Identifier: CVE-<year>-<number>
- Maintained by MITRE
  - <https://cve.mitre.org/>
  - [https://cve.mitre.org/cve/search\\_cve\\_list.html](https://cve.mitre.org/cve/search_cve_list.html)
- Nowadays, about 15000 new entries assigned per year



# CVSS: Common Vulnerabilities Scoring System (version 3)

- Standardized representation of the impact of a vulnerability



See: <https://www.recordedfuture.com/cvss-scores-guide/>  
Source: prof. Hervé Debar



# CVSS: Common Vulnerabilities Scoring System (version 3)

Scoring: <https://www.first.org/cvss/calculator/3.0>

**CVSS v3.0 Calculator** [?]

Attack Vector [?]  
 Network  Adjacent  Local  Physical

Attack Complexity [?]  
 Low  High

Privileges Required [?]  
 None  Low  High

User Interaction [?]  
 None  Required

Scope [?]  
 Unchanged  Changed

Confidentiality [?]  
 None  Low  High

Integrity [?]  
 None  Low  High

Availability [?]  
 None  Low  High

Medium **4.3**



# CWE: Common Weakness Enumeration

- Taxonomy of vulnerabilities
  - About 1000 entries
- Different abstraction levels
  - Base/variant: « fundamental » concepts
  - Composite: realization of vulnerability requires multiple steps
  - Graph/view: aggregates over the dataset
- Maintained by MITRE
  - <https://cwe.mitre.org/>
- Aggregate organization in views
  - Partial coverage of structure



# 2019 CWE Top 25 (excerpt)

Rank	ID	Name	Score
[1]	<a href="#">CWE-119</a>	Improper Restriction of Operations within the Bounds of a Memory Buffer	75.56
[2]	<a href="#">CWE-79</a>	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	45.69
[3]	<a href="#">CWE-20</a>	Improper Input Validation	43.61
[4]	<a href="#">CWE-200</a>	Information Exposure	32.12
[5]	<a href="#">CWE-125</a>	Out-of-bounds Read	26.53
[6]	<a href="#">CWE-89</a>	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24.54
[7]	<a href="#">CWE-416</a>	Use After Free	17.94
[8]	<a href="#">CWE-190</a>	Integer Overflow or Wraparound	17.35
[9]	<a href="#">CWE-352</a>	Cross-Site Request Forgery (CSRF)	15.54
[10]	<a href="#">CWE-22</a>	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14.10
[11]	<a href="#">CWE-78</a>	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11.47
[12]	<a href="#">CWE-787</a>	Out-of-bounds Write	11.08
[13]	<a href="#">CWE-287</a>	Improper Authentication	10.78
[14]	<a href="#">CWE-476</a>	NULL Pointer Dereference	9.74
[15]	<a href="#">CWE-732</a>	Incorrect Permission Assignment for Critical Resource	6.33
[16]	<a href="#">CWE-434</a>	Unrestricted Upload of File with Dangerous Type	5.50
[17]	<a href="#">CWE-611</a>	Improper Restriction of XML External Entity Reference	5.48





# Conclusions

- Blockchain is a unique and disruptive opportunity
- Blockchain is not a panacea
- Blockchain requires specific expertise
- Still some technical problems: scalability, bandwidth, oracles, smart contracts
- Applicability to medical device traceability appears promising