CONVEGNO

# Blockchain tra opportunità e timori

Scuola di Perfezionamento per le Forze di Polizia

Aula Magna

Roma, mercoledì 5 dicembre 2018 - ore 9.00

## Blockchain: stato dell'arte, prospettive e *cybersecurity*

**Elisabetta Zuanelli**

Presidente CReSEC

Università degli Studi di Roma «Tor Vergata»

Coordinatore del Piano di formazione nazionale in *cybersecurity, cyberthreat, privacy*

# Il contesto della blockchain: la Rete e le nuove tecnologie

**Trasformazione digitale e *abracadabra* digitali: le transazioni *on line***

- *cloud*, *IoT*, *mobile*, *big data analytics*, *AI*, **blockchain**
- soluzioni innovative di servizi pre-digitali e digitali
- *data economy*
- sicurezza informatica e *cyber*, protezione dei dati

# La tecnologia *blockchain*

La tecnologia *blockchain* **non è una singola tecnica** o un *tool*

Contiene **crittografia, matematica, modelli algoritmici ed economici**

Combina reti *peer-to-peer e usa* **l'algoritmo di consenso distribuito per risolvere il problema della sincronizzazione del database distribuito tradizionale**

E' una costruzione di **infrastruttura multipla integrata**

# La tecnologia blockchain



- All'origine: **catena di transazioni/blocchi di dati**, con *data base/ registro digitale* ***aperto*** e **distribuito**, condiviso e pubblico, OVVERO accessibile come registro/*ledger* di transazioni, accettato/approvato dai nodi/ *miner* della catena (51%), applicato a **crittovalute**
- **I dati in un blocco/transazioni sono trasferiti ad altro blocco e considerati incorruttibili**, immodificabili senza alterare tutta la catena
- Basata sull'**affidabilità** dei *miner*
- **Senza controlli** di un'istituzione/ente centrale
- Con l'utilizzo di **sistemi di crittazione dei dati** per il trasferimento di dati/ transazioni da un nodo a un altro
- Con l'utilizzo di una funzione di *hash (*puntatore *hash al blocco precedente)* che consente **identificazione certa della transazione**, immodificabilità del dato e ***timestamp*** **per la serializzazione delle modifiche**
- Parzialmente **anonimo**
- Utilizzo per **scambi monetari e attività finanziarie** attraverso crittovalute (*bitcoin*, Ethereum, ecc.)

# La struttura

1) The **sending node** records new data and broadcasts to the network.

2) The **receiving node checks the message**/data received. If the message is correct then it will be stored in a block.

3) **All receiving nodes in the network execute proof of work (PoW) or proof of stake (PoS) algorithm** to the block.

4) The block will be stored into the chain **after executing consensus algorithm**, every node in the network admits this block and will continuously extend the chain base on this block.

# La struttura a blocchi

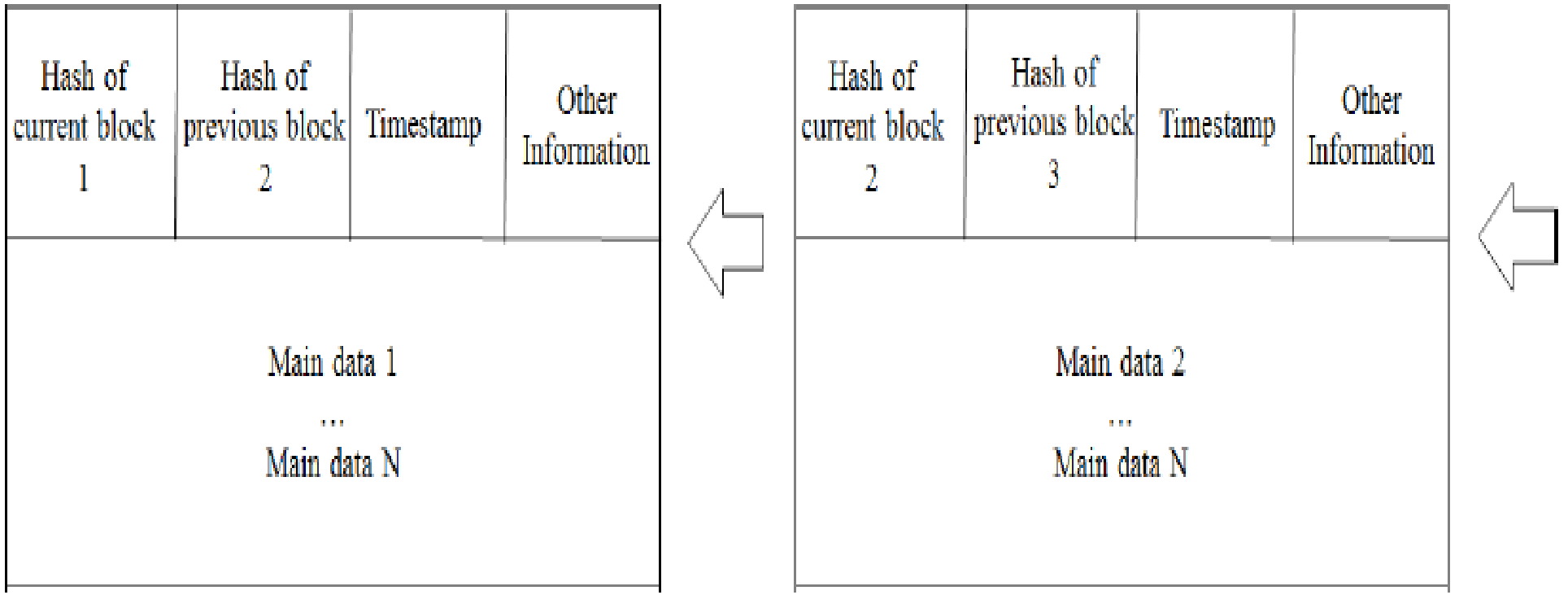



Figure 1: The structure of block chain

# La funzione di consenso

La **funzione di consenso** è un meccanismo che rende tutti i nodi della *blockchain* concordi sullo stesso messaggio. Assicura che l'ultimo blocco sia stato aggiunto correttamente alla catena

## PoW

Affinché un blocco possa essere accettato dai partecipanti alla rete, i minatori devono completare una *PoW* che copra tutti i dati nel blocco. La difficoltà di questo 'lavoro' è regolata in modo da limitare la velocità con cui i nuovi blocchi possono essere generati dalla rete a uno ogni 10 minuti (molto costoso, energia elettrica / potenza di elaborazione)

## PoS

Il *Proof of Stake* non ha bisogno di una potenza di calcolo costosa. Un metodo Proof of Stake potrebbe fornire una maggiore protezione da un attacco dannoso sulla rete

# Tipologie: *blockchain* aperte  e private

- Accessi controllati o meno: non necessitano di controllo quelli aperti
- Controllati quelli privati con un *ledger* database centralizzato: enti, istituzioni, aziende, sottoposti potenzialmente ad attacchi sui server aziendali e/o istituzionali

1) **Public blockchain**: Everyone can check the transaction and verify it, and can also participate the process of getting consensus, like Bitcoin and Ethereum.
2) **Consortium blockchains**: It means that the node that has authority can be chosen in advance. Usually in partnerships like business to business. Partly Decentralized. Hyperledger and R3CEV are both consortium blockchains.
3) **Private blockchain**: Node is restricted, not every node can participate this blockchain. It  has strict authority management on data access.

# Smart Contracts/ Contratti intelligenti

Contratti intelligenti/ programmi per computer eseguiti sul registro generale.

Questo tipo di programmi può essere utilizzato per **facilitare**, **verificare o imporre regole** tra le parti, consentendo l'elaborazione diretta e le interazioni con altri contratti intelligenti.

Tale software fornisce **un'ampia area di superficie per l'attacco**, quindi un attacco a un contratto intelligente potrebbe avere un effetto domino su altre parti della piattaforma.

# Cosa sono

**Protocolli informatici** utilizzati per facilitare, verificare o imporre la negoziazione di un contratto legale.

Un contratto intelligente è una frase per descrivere il **codice del computer.**

Oggi, i contratti intelligenti di Ethereum sono progettati per funzionare su tutti i nodi della rete Ethereum.

Questi contratti intelligenti **facilitano lo scambio di valore, compresi denaro, contenuto, proprietà o azioni tra un numero fisso di parti.**

# I tratti distintivi delle tecnologie *blockchain*

- **Decentralizzazione**: non c'è più un nodo centralizzato su cui appoggiarsi
- **Trasparenza**: ad ogni nodo
- **Open source**: aperto a tutti e utilizzabile da chiunque per diverse applicazioni
- **Autonomia**: fondato sul consenso della catena
- **Immutabilità:** record dei dati memorizzato per sempre a meno che qualcuno possa controllare allo stesso tempo un nodo al 51%
- **Anonimato**: solo l'indirizzo blockchain

# Tratti positivi

## Immutabilità

La tecnologia blockchain può essere considerata una tecnologia sicura, dal punto di vista del fatto che consente agli utenti di **confidare che le transazioni archiviate nel registro siano valide.** La combinazione di ***hashing* sequenziale e crittografia con la struttura decentralizzata** rende molto difficile per qualsiasi parte manometterla in contrasto con un database standard

## Diritto all'oblio

L'immutabilità dei dati **si adatta alle leggi sulla *privacy***. Come implementare il diritto all'oblio in una tecnologia che garantisce che nulla sarà cancellato è una sfida interessante

# Tracciabilità

Ogni transazione aggiunta a una blockchain pubblica o privata **è firmata digitalmente con data e ora**

Le organizzazioni possono **risalire a un periodo di tempo specifico per ogni transazione e identificare la parte corrispondente** (tramite il loro indirizzo pubblico) sulla blockchain.

# Non ripudiabilità

Questa funzionalità si riferisce a **un'importante proprietà di sicurezza delle informazioni ovvero la non ripudiabilità**, che è l'assicurazione che **qualcuno non può duplicare l'autenticità della propria firma su un file o la paternità di una transazione da loro originata.** Questa funzionalità out of the box della blockchain aumenta l'affidabilità del sistema (rilevamento di tentativi di manomissione o transazioni fraudolente), poiché ogni transazione è associata crittograficamente a un utente

# Qualità dei dati

La tecnologia blockchain **non garantisce o migliora la qualità dei dati**.

I *blockchain* privati e pubblici possono solo assumersi la responsabilità dell'accuratezza e della qualità delle informazioni una volta che sono state immesse nella *blockchain*.

Il che significa che è necessario confidare che i dati estratti dalle organizzazioni nei sistemi esistenti siano di buona qualità, come nel caso di tutti gli altri sistemi tecnologici.

# Hyperledger: the Linux Foundation project

Hyperledger è una **piattaforma** di *blockchain open source*

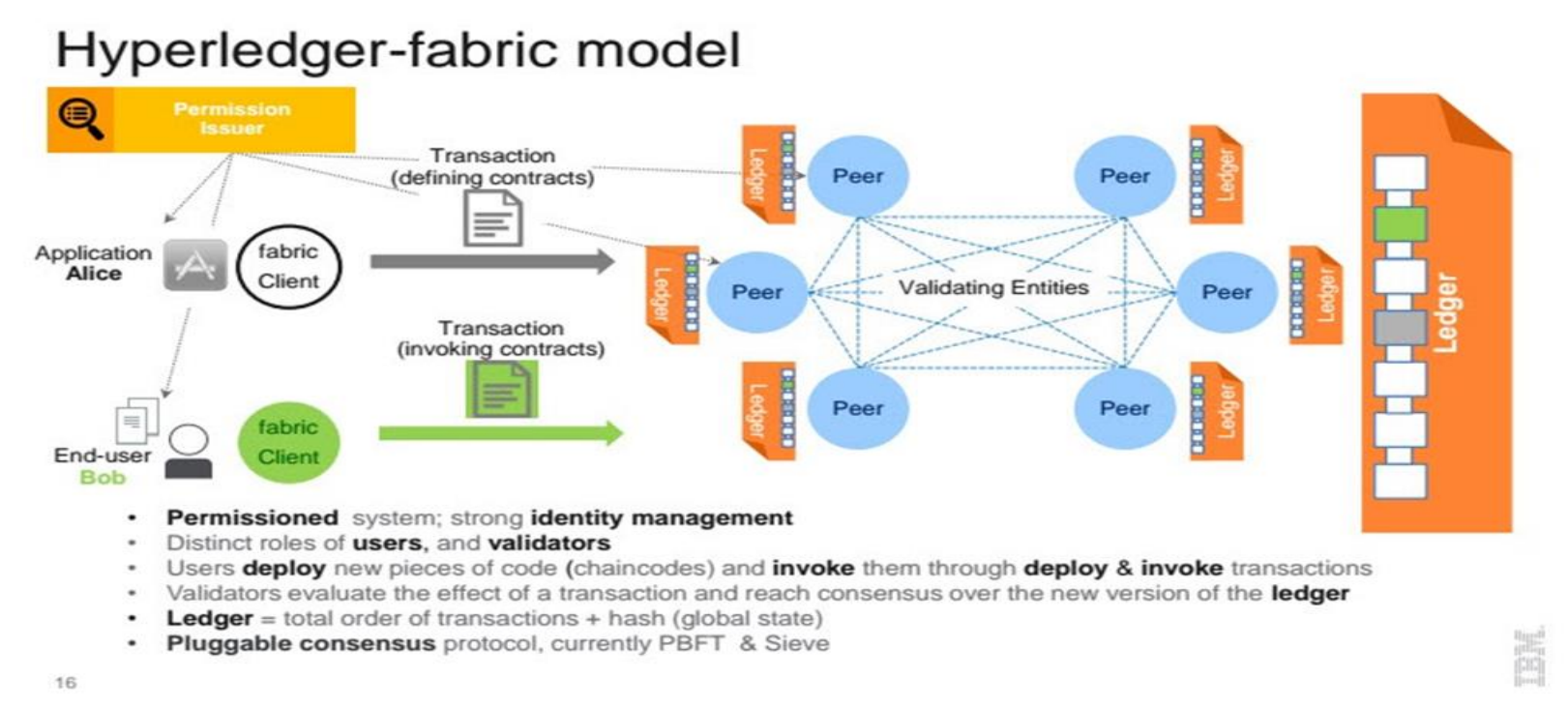
Avviata nel dicembre 2015 dalla Linux Foundation per supportare registri distribuiti basati su *blockchain*

Si concentra sui libri mastri progettati per supportare transazioni globali di business, incluse

- le principali società tecnologiche
- il business finanziario
- e società della catena di fornitura

con l'obiettivo di migliorare molti aspetti delle  prestazioni e affidabilità

# Versione 1.0 2017
# Applicazioni: manifatturiero, salute, agricultura, mercati di capitali, …



# Il progetto

**Sviluppo di**

- protocolli aperti e standard
- un *framework* modulare che supporti diverse component per diversi usi
- include una varietà di *blockchain* con il loro consenso
- modelli di *storage* e servizi per l'identità, il controllo degli accessi e i contratti

# Problemi

- Assenza di regolazione: es. crittovalute e banche centrali
- Soluzioni non pronte e direttamente applicabili
- La *blockchain* non garantisce la qualità del contenuto del messaggio/transazione
- Sicurezza cibernetica

# La cybersecurity nella *blockchain*

Deloitte 2017

*"Some of the early use cases were deploying blockchain* ***for the sake of it****,*

***without sufficiently focusing on the core attributes of the technology****, which*

*indeed has the* ***potential*** *to generate substantial process efficiencies across*

*many industries and is likely to contribute to entirely* ***new business models.*****"**

# Data Access

*"People want and need to be connected to their data at*

***all times** from **any location** and **any device** which bring about*

***new cyber risks** which makes* network access

*management in enterprise and global organizations inherently challenging"*

# Cillian Leonowicz, Senior Manager at Deloitte Ireland opines

*"blockchain's characteristics* ***do not provide an impenetrable panacea to all cyber ills****,*

*to* ***think the same would be naïve at best****,*

*instead as with other technologies blockchain implementations and roll outs* ***must include typical system and network cyber security controls, due diligence, practice and procedures"***

# I tratti di sicurezza

Autenticazione,  autorizzazione, audit (AAA) e non ripudio:

**aspetti fondamentali di sicurezza per la protezione delle informazioni e la progettazione e la gestione di nuovi sistemi e reti**

# Il sentiero

conoscenza, progettazione di soluzioni, applicazioni: il percorso al quale connettersi senza fughe in avanti

# Per concludere: attenzione agli *abracadabra* digitali…

Grazie!