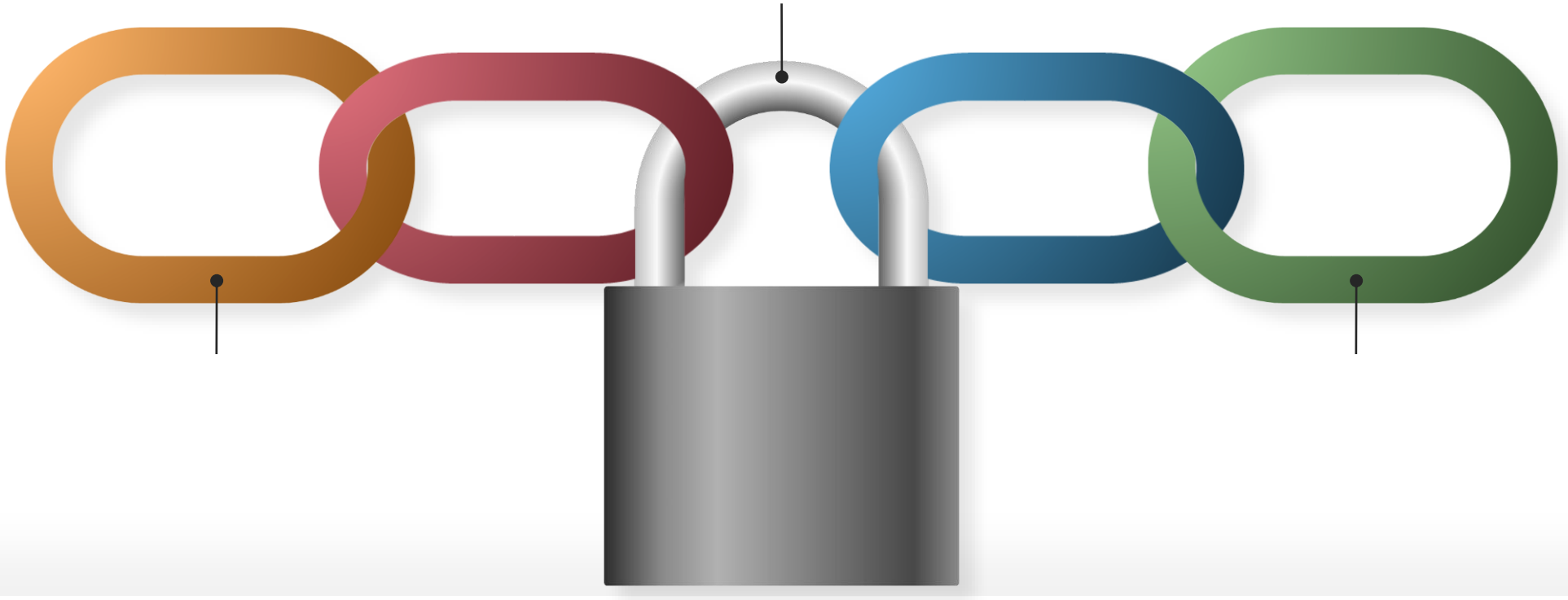
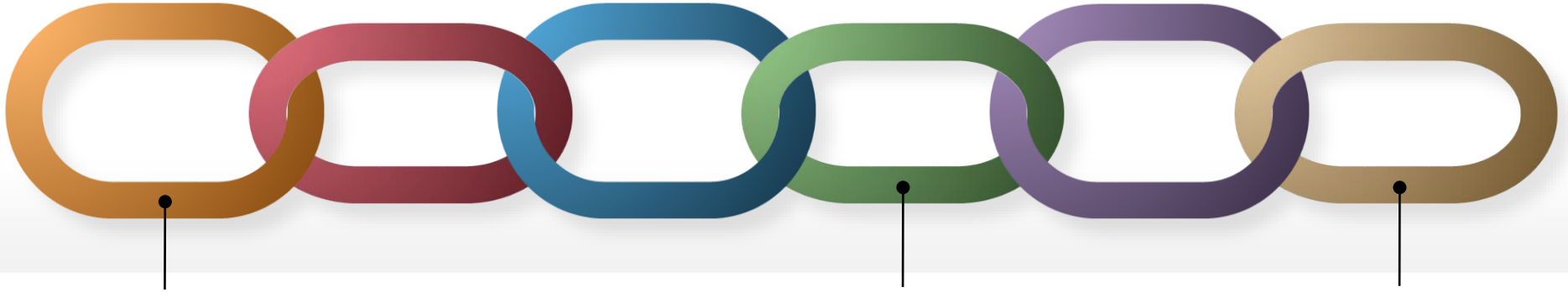


L’iniziativa CifrisChain

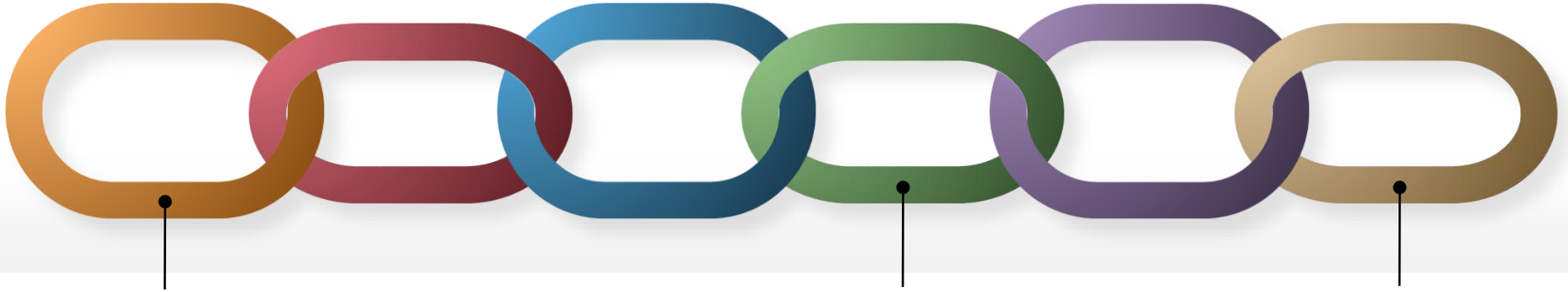
Ivan Visconti, Università di Salerno
Coordinatore dell’iniziativa CifrisChain



De Componendis Cifris

La De Componendis Cifris è un'iniziativa nazionale di Crittografia, che si sta costituendo da circa un anno, al cui interno trovano spazio varie anime e componenti.

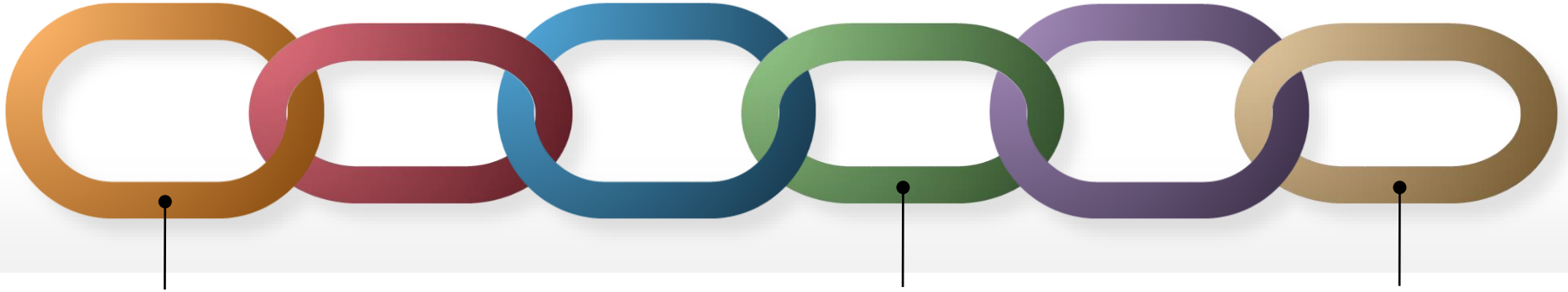
Per info:
http://www.decifris.it
http://www.decifris.it/membri.html"



CifrisChain: primo gruppo tematico della costituenda associazione De Cifris

«CifrisChain include i membri della De Cifris interessati agli aspetti crittografici della tecnologia blockchain e del concetto di cryptocurrency; l'obiettivo è creare una sinergia tra le diverse competenze presenti nell'associazione per contribuire sia agli aspetti di divulgazione e formazione, sia agli aspetti di ricerca e trasferimento tecnologico»

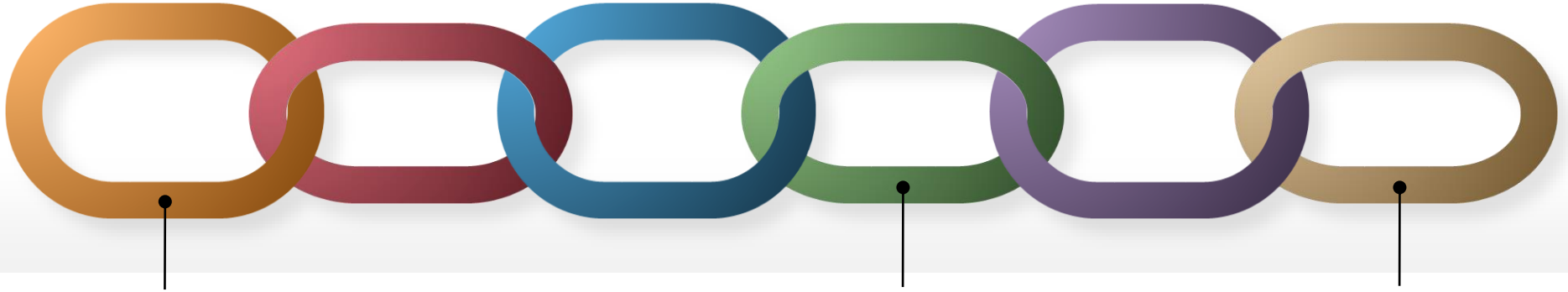
17 Dicembre 2018 Ivan Visconti Roma, CifrisChain



CifrisChain: Genesis Block

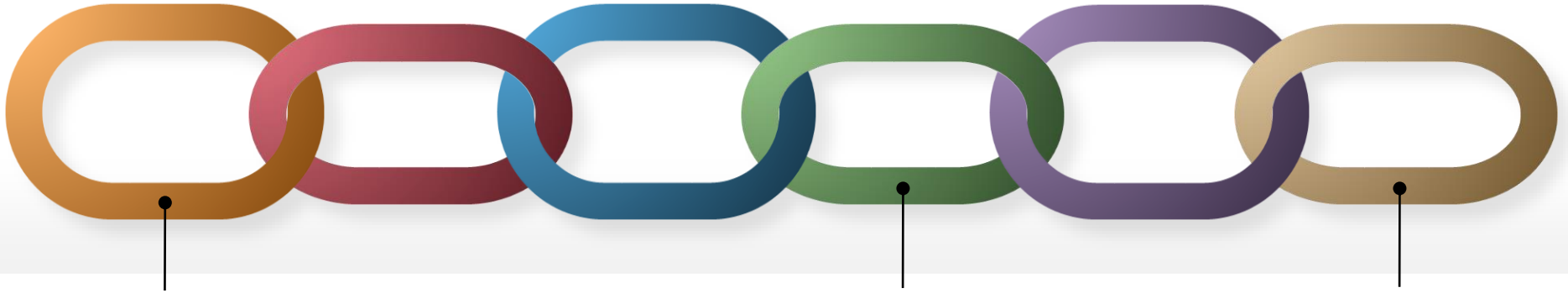
nasce a Giugno del 2018

come si diventa membri: email a cifrischain@decifris.it
(per iscriversi specificare "PARTECIPO" oppure "INTERESSE")



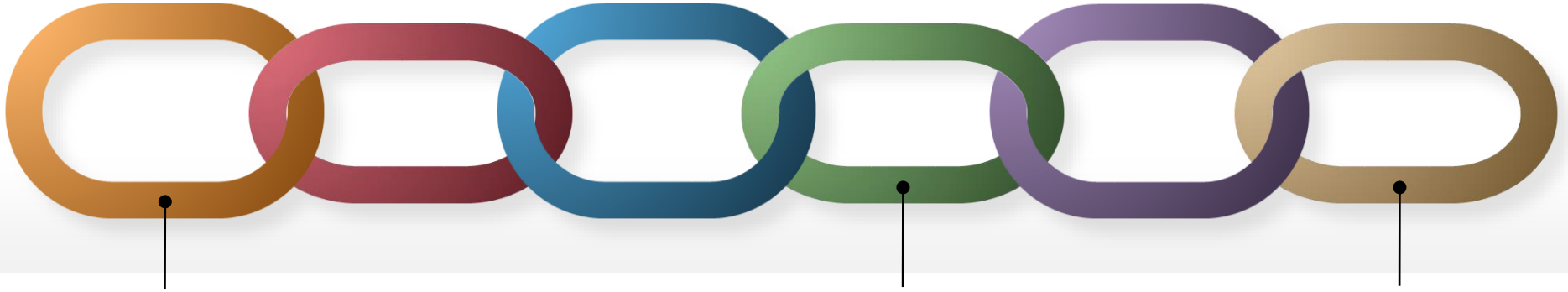
CifrisChain: primi 2 obiettivi

1) nomina di un coordinatore
2) un primo evento entro il 2018



Ivan Visconti, coordinatore di CifrisChain

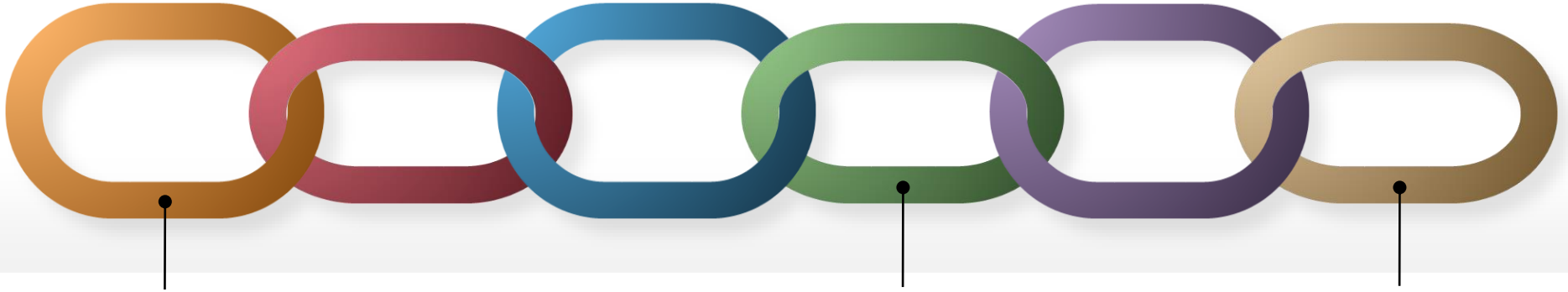
- Prof. Associato di Informatica, Università di Salerno (DIEM)
- Ricerca su strumenti avanzati di crittografia per la privacy dei dati nelle transazioni digitali (ZK proofs, secure MPC)
- Responsabile locale di un progetto EU-H2020 (PRIViLEDGE) su privacy e sicurezza della tecnologia blockchain con altri 9 partner internazionali (IBM Zurich, Edinburgh, IOHK, TUE, Guardtime,…)



CifrisChain: primi 2 obiettivi

1) nomina di un coordinatore ✓

2) un primo evento entro il 2018



CifrisChain 2018

Comitato Organizzativo

Dott. Massimo Bernaschi	IAC-CNR
Prof. Marco Pedicini	Università di Roma Tre
Dott. Giovanni Schmid	ICAR-CNR
Prof. Daniele Venturi	Università La Sapienza
Prof. Vincenzo Vespri	Università di Firenze
Prof. Andrea Visconti	Università di Milano
Prof. Ivan Visconti	Università di Salerno

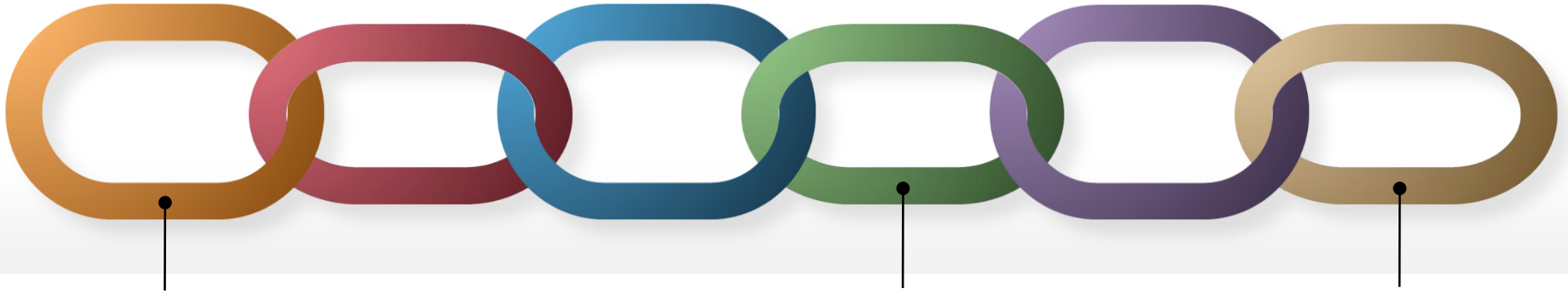
CifrisChain 2018

Siamo qui senza costi di iscrizione grazie ai ***contributi organizzativi*** di

ROMA TRE
UNIVERSITÀ DEGLI STUDI

Telsy

Consiglio Nazionale delle Ricerche



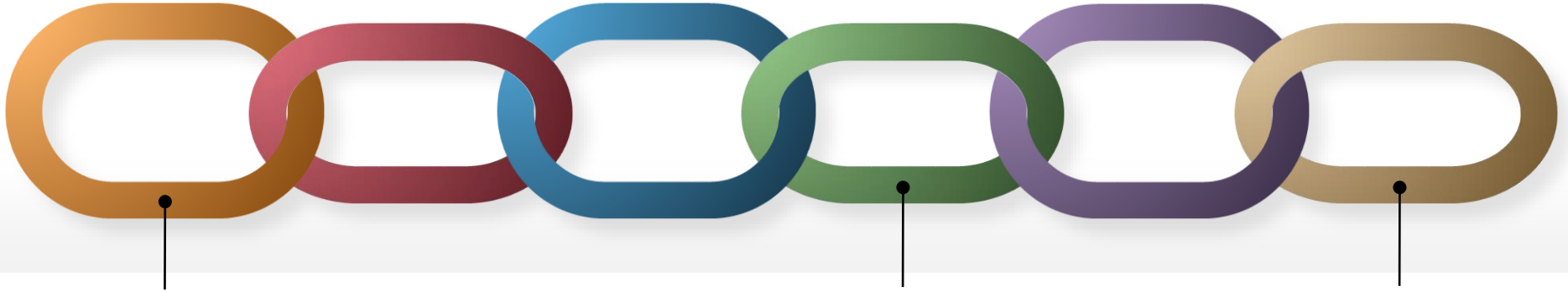
CifrisChain 2018

Visione del comitato organizzativo

tante presentazioni di pochi minuti renderebbero l'evento frammentato e non ci sarebbe «colla» che tenga

meglio raccogliere contributi dai membri ed organizzare delle panoramiche tematiche sulle principali attività svolte (si… abbiamo deciso di lavorare di più…)

complementate da un intervento istituzionale su cryptocurrency



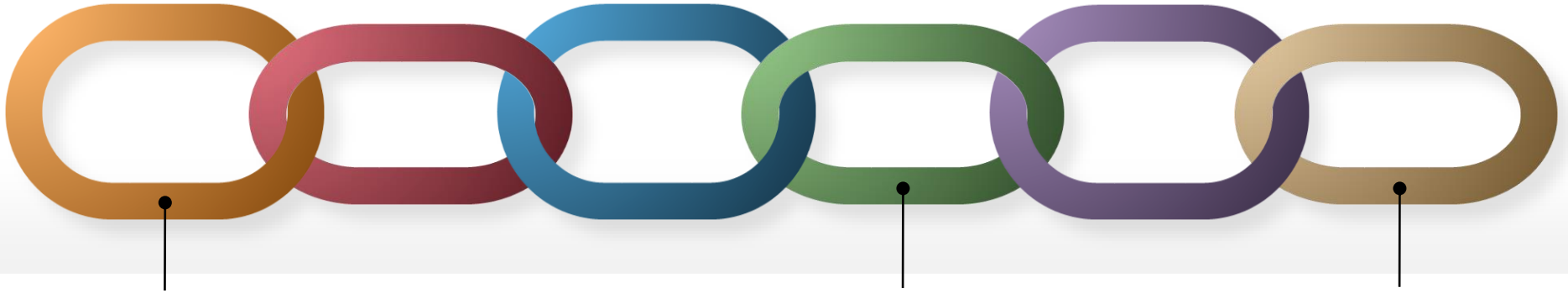
CifrisChain 2018

Sessione II (11.45-13.00)

11:45 Dott. Marco Benedetti, Banca d'Italia
Lightning Network: Cryptography to the rescue of Cryptography?

12:10 Prof. Daniele Venturi, La Sapienza
Panoramica su alcune attività didattiche e di ricerca svolte in CifrisChain

12:35 Prof. Andrea Visconti, Università di Milano
Panoramica su alcuni progetti industriali in CifrisChain

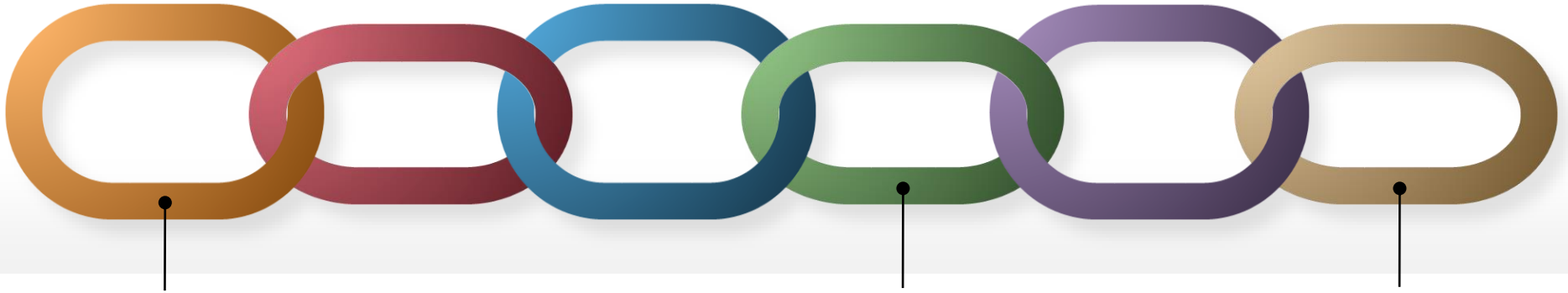


CifrisChain 2018

Altro obiettivo del comitato organizzativo

invitare contributi nelle seguenti 4 interessanti direzioni

- *ricerca*
- *attività industriali*
- *trasferimento tecnologico università-industria*
- *collaborazioni tra industrie e studenti*



CifrisChain 2018

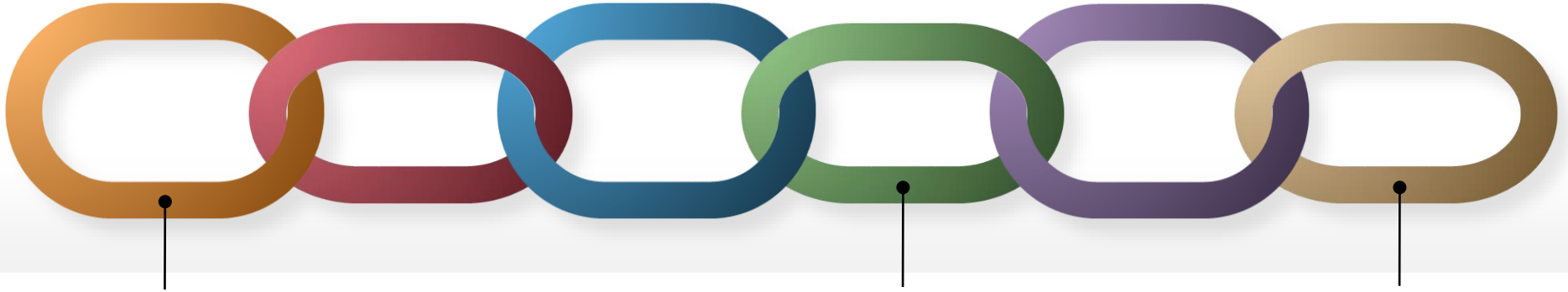
Sessione III (14.15-15.40)

14:15 Dott. Andrea Di Nenno, Telsy e Politecnico di Torino
Decentralized and Secure Analytics System

14:30 Dott. Alessio Meneghetti, Università di Trento
Blockchain per Processi Aziendali in una Grande Azienda

14:45 Dott. Paolo Campegiani, Bit4id
Le attività di standardizzazione su blockchain e distributed ledger in Italia, in Europe a nel mondo

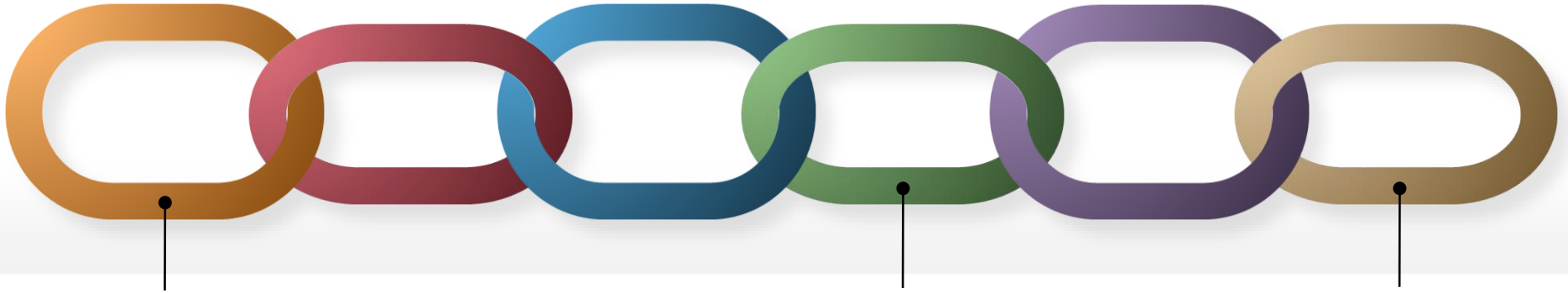
15:10 Prof. Massimo Bartoletti, Università di Cagliari
Modelling and Verifying Bitcoin Contracts



CifrisChain 2018

E’ inoltre emersa nel comitato organizzativo la sensazione che

i partecipanti siano già convinti del potenziale di tali tecnologie e sarebbe utile discuterne le criticità



CifrisChain 2018

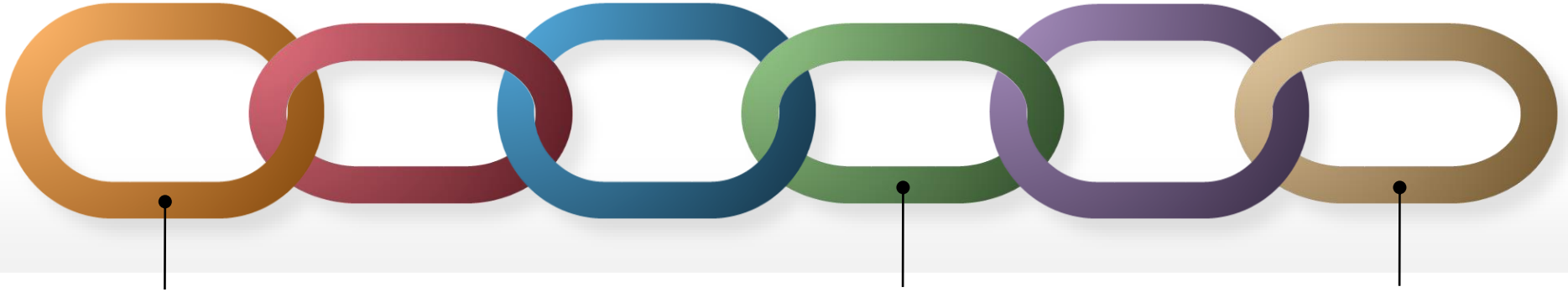
Sessione IV (16.10-17.00)

16:10 Panel: *Criticità in Blockchain e Cryptocurrency*

Prof. Massimo Bartoletti, Università di Cagliari
Dott. Paolo Campegiani, Bit4id
Prof. Alessandro Toscano, Università Roma Tre

(modera: Prof. Ivan Visconti, Università di Salerno)

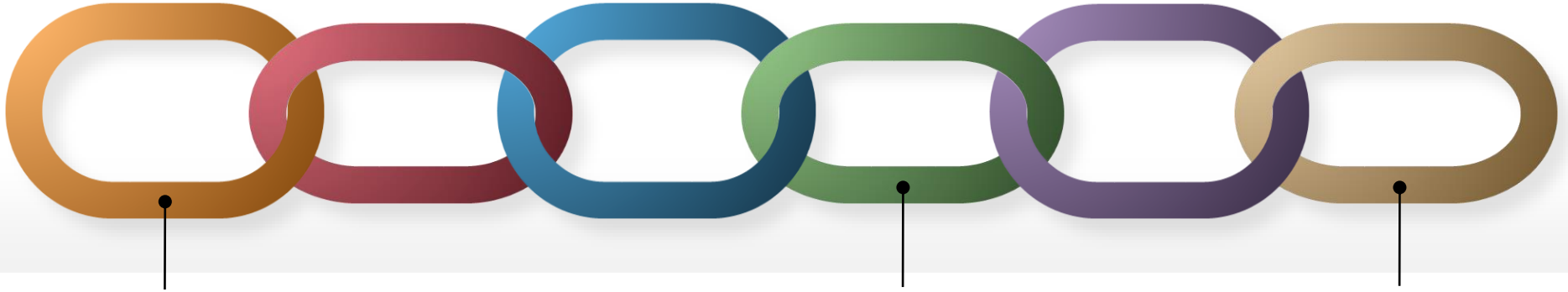
16.40 Conclusioni e Networking



CifrisChain: primi 2 obiettivi

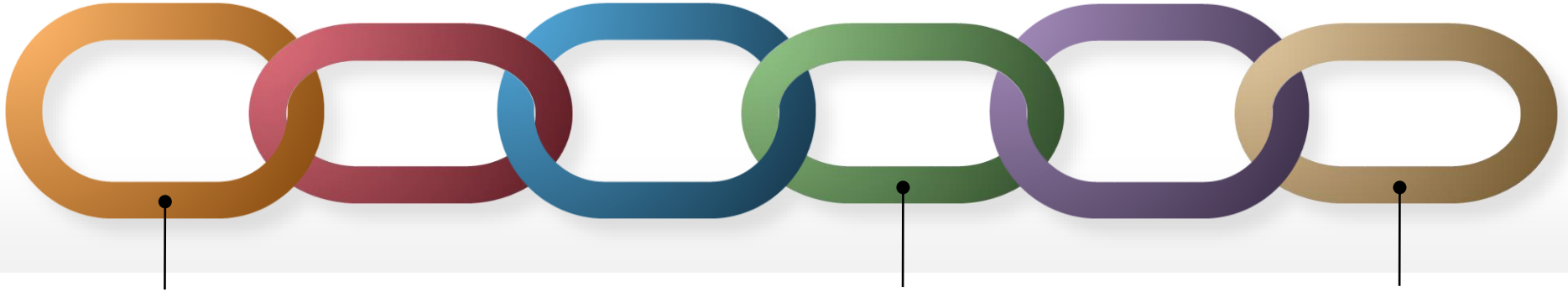
1) nomina di un coordinatore ✓

2) un primo evento entro il 2018 ✓



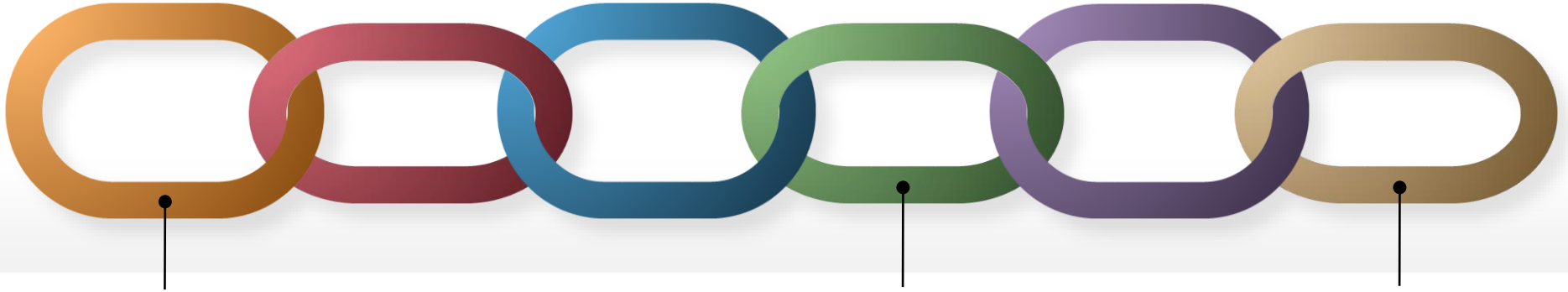
La keyword in questo momento storico:

Decentralizzare



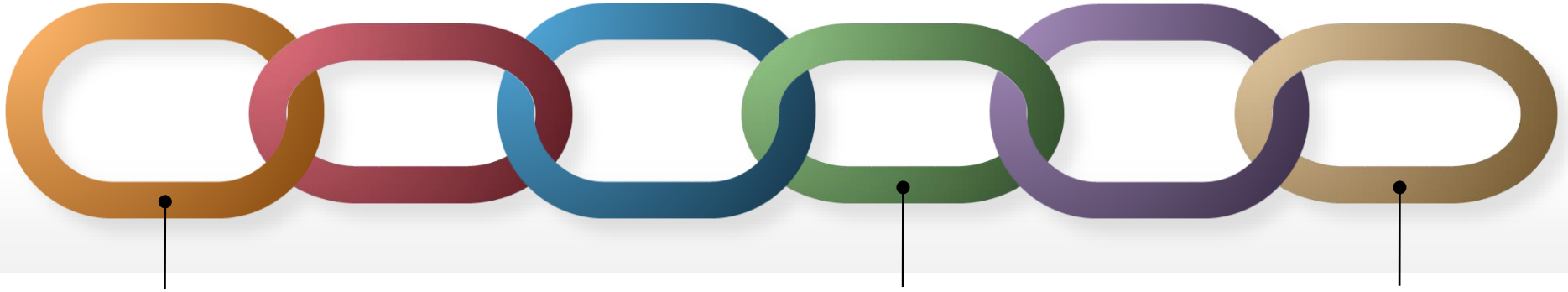
Decentralizzare

rendere un servizio, un processo, una transazione sicuri anche se c’è una (limitata) «corruzione» tra i gestori del servizio



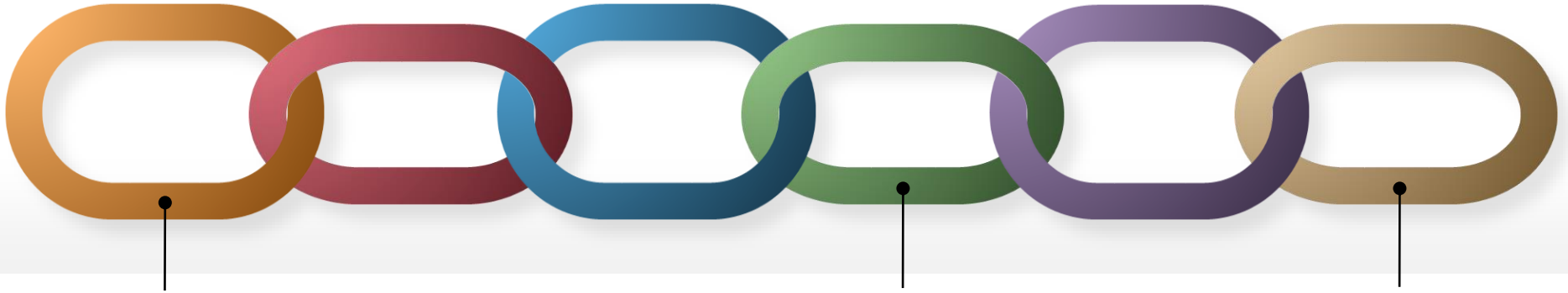
Decentralizzare

è un concetto noto da tempo nel mondo della crittografia. Perché si espande ed ha grande impatto solo negli ultimi anni?



Blockchain Decentralizzata

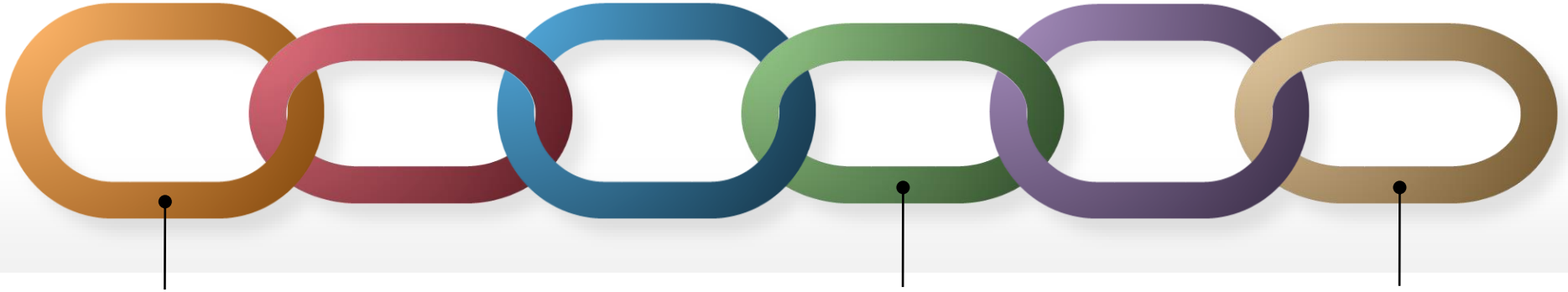
l’importanza della decentralizzazione si amplifica quando è associata al concetto di Blockchain



Blockchain

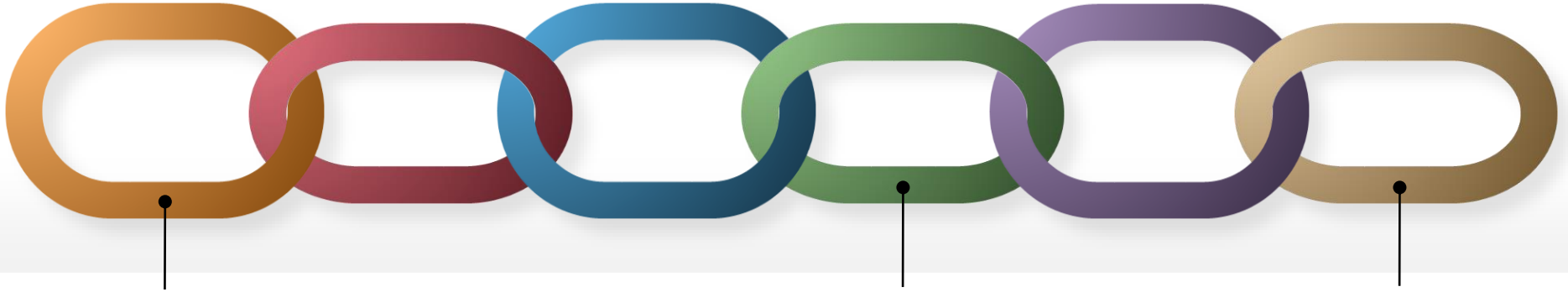
una blockchain è un piattaforma che attraverso la validazione di transazioni permette di aggiornare lo stato di processi e di eseguire programmi (smart contract)

gli aggiornamenti sono irreversibili (da cui la proprietà di immutabilità)



Decentralizzare una Blockchain: Cryptocurrency

la decentralizzazione di una blockchain in cui le transazioni generano e trasferiscono token (cryptocurrency) costituisce l'innovazione (o meglio rivoluzione) introdotta recentemente da Satoshi Nakamoto

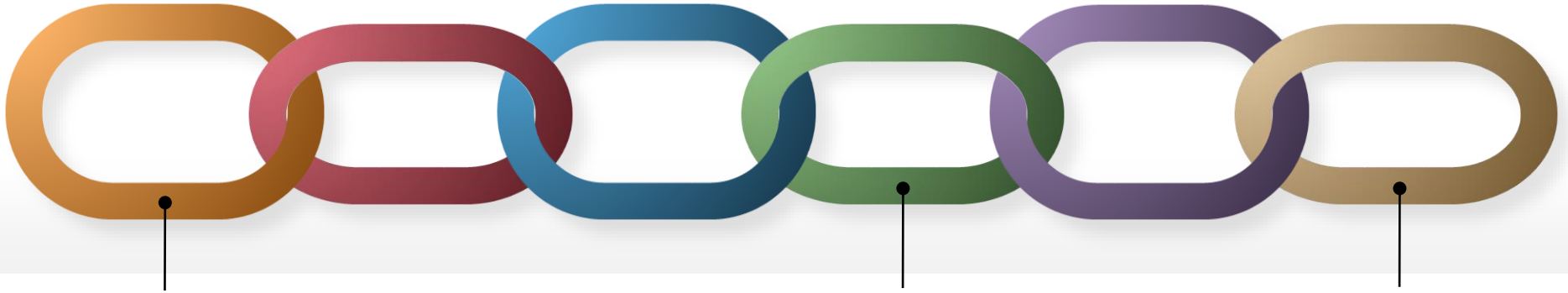


Blockchain Decentralizzata: Public Verifiability

la decentralizzazione combinata al concetto di Blockchain ci regala una funzionalità di grande impatto:

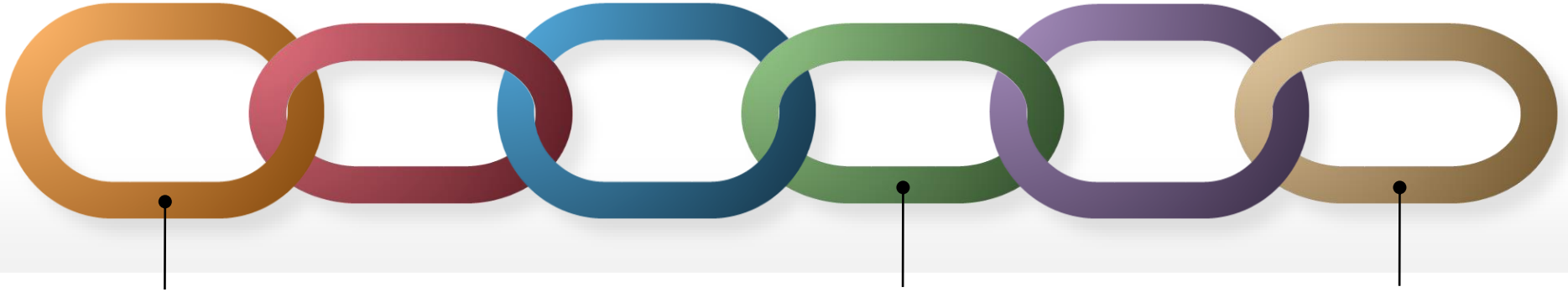
la Public Verifiability

:



Blockchain Decentralizzata – Public Verifiability

poter verificare in qualunque momento la correttezza di un processo dalle sue origini fino allo stato attuale anche quando alcuni dei gestori/controlli del processo sono «corrotti» è «disruptive» (dirompente)

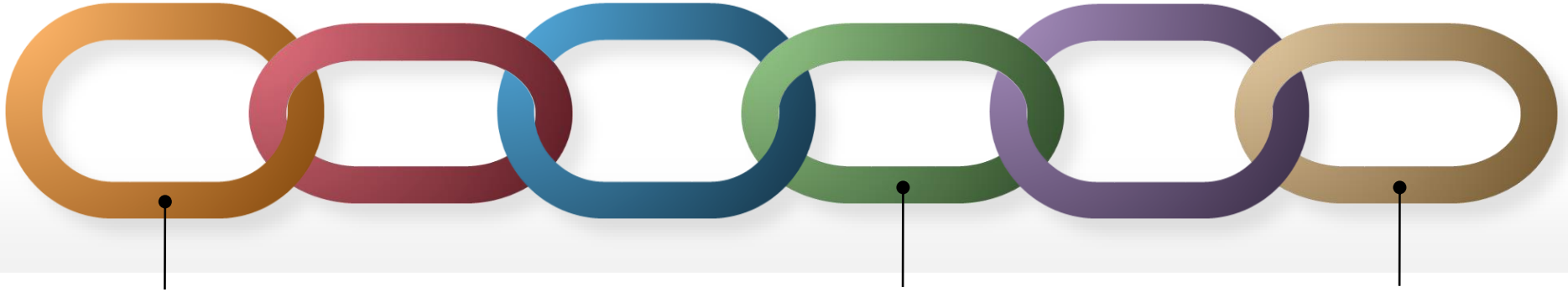


Blockchain Decentralizzata – Applicazioni

Bitcoin ci insegna che questa tecnologia induce fiducia verso l'uso di cryptocurrency

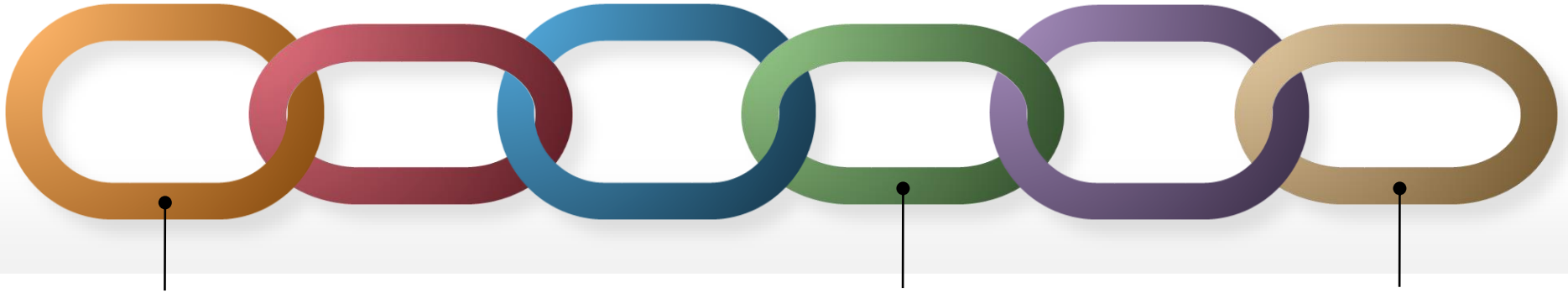
Ethereum ha già ampiamente confermato l'importanza della public verifiability con il successo di nuovi meccanismi di crowdfunding (ICO)

e poi?



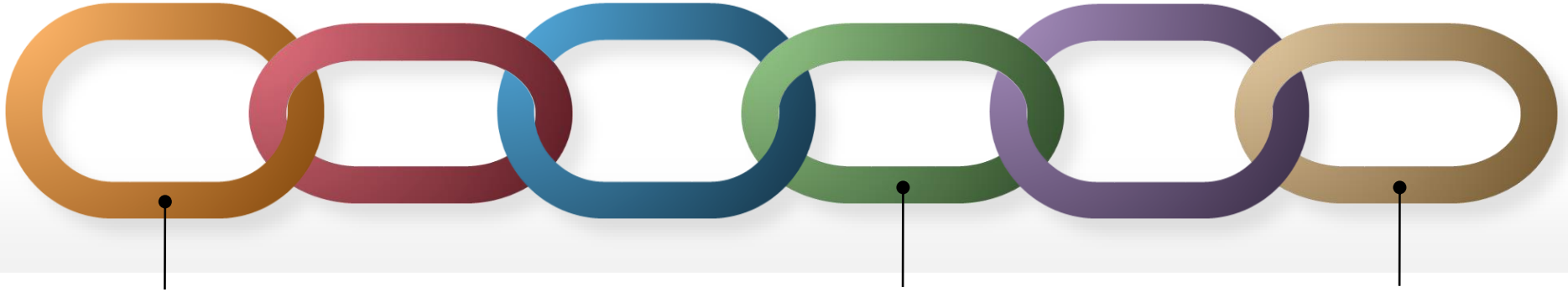
Blockchain Decentralizzata – Dati Privati o Pubblici?

è facile pensare a tante utili applicazioni (trasparenza di atti amministrativi, delle catene di distribuzione, del voto elettronico, etc...) coinvolgendo tuttavia svariati tipi di dati che diventano di pubblico dominio



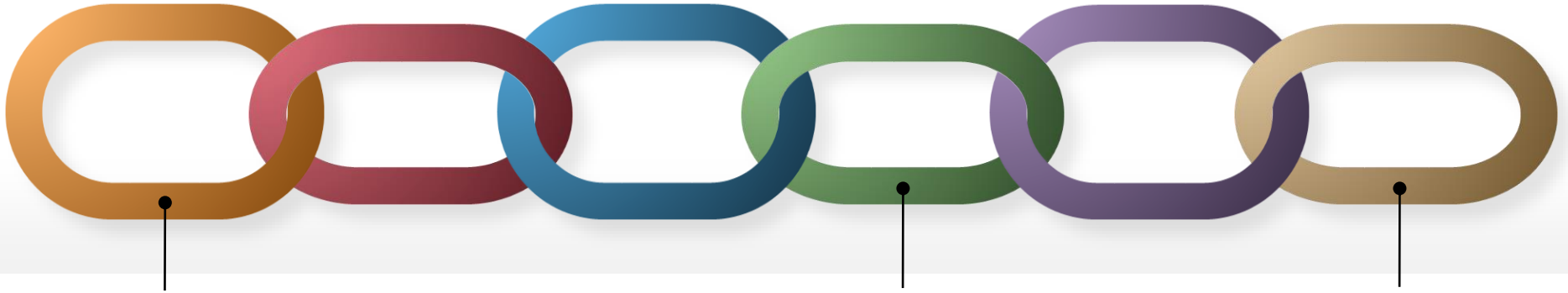
Blockchain Decentralizzata – Paradosso

è possibile mitigare la tensione tra Public Verifiability e privacy dei dati?



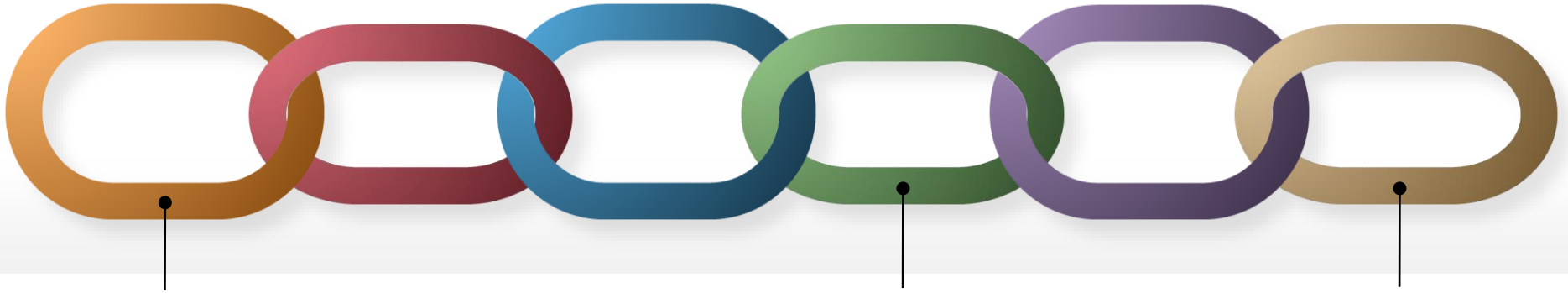
Blockchain Decentralizzata – GDPR

può l'immutabilità di una blockchain essere compatibile con il GDPR?



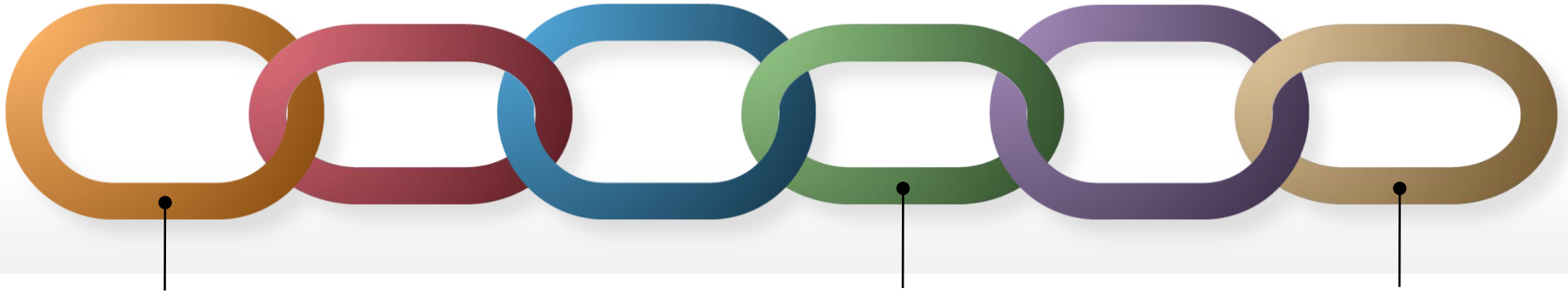
Blockchain Decentralizzata: Governance e Scalabilità

fino a che punto possiamo affidarci alle dispendiose proof of work? chi governa Bitcoin ed Ethereum? Potrebbe una gran parte dei gestori delle blockchain coalizzarsi a danno degli utenti dei servizi erogati dalle piattaforme?



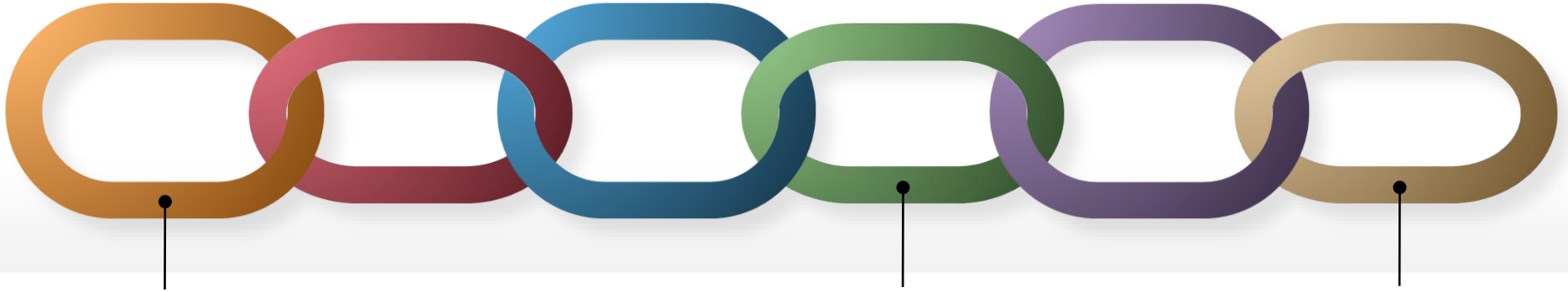
Blockchain Decentralizzata – Permissioned

i problemi di governance, di scalabilità e di sostenibilità sono in gran parte risolti scegliendo blockchain «permissioned» ossia gestite da un consorzio di organizzazioni che si conoscono ad hanno un comune interesse nella gestione della piattaforma



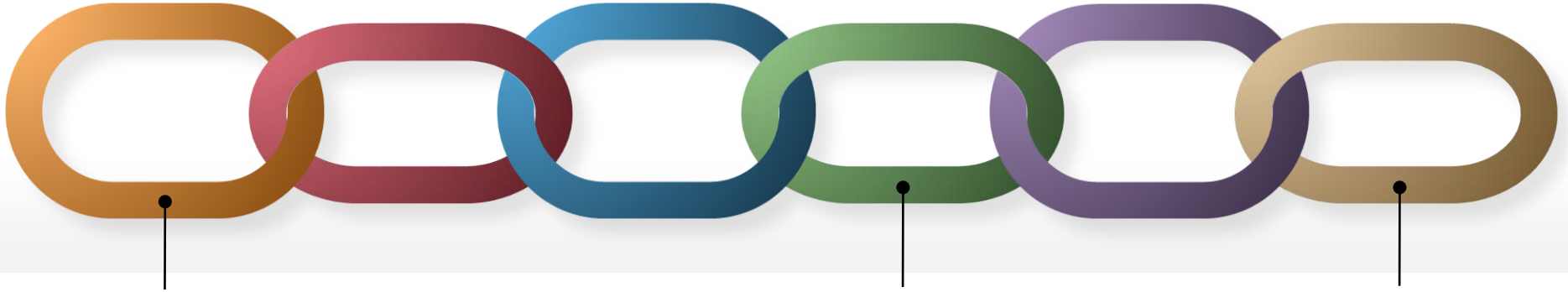
Blockchain Decentralizzata – Il Gioco si fa duro

i problemi legati alla privacy dei dati coinvolti nelle transazioni sono la sfida più ardua per l'utilizzo pervasivo di questa tecnologia



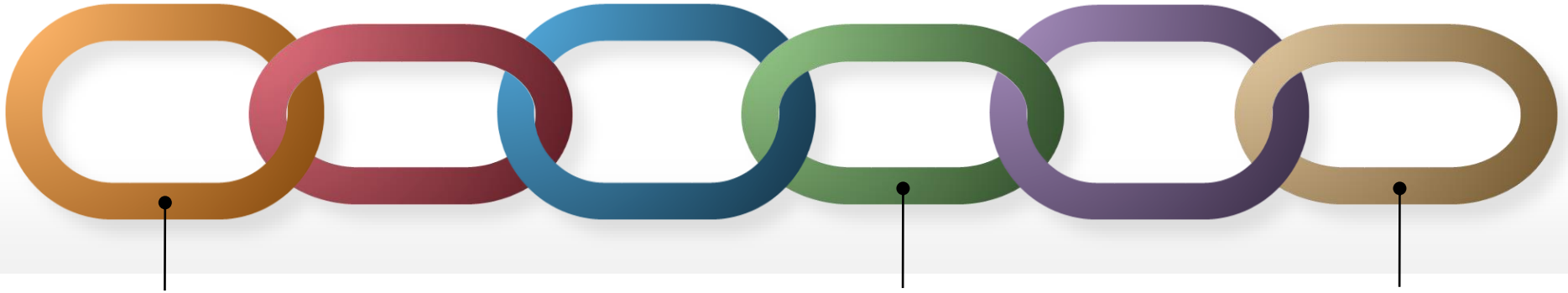
Blockchain Decentralizzata
Dove vai se il crittografo non ce l'hai?

la protezione dei dati privati, la garanzia della loro immutabilità e l'esecuzione di transazioni con dati privati sono pane per i denti dei crittografi, ed oggi siamo qui per parlarne



Blockchain in Italia
Industria, Università e Istituzioni che fanno?

CifrisChain 2018 ci permette di affrontare questi temi



Blockchain e Cryptocurrency

ci diranno di più i prossimi speaker e ne parleremo insieme durante il panel,

a più tardi!