Blockchain per l'analisi di dati aggregati nel rispetto della privacy

Guglielmo Morgari

Blockchain e servizi: il ruolo dell'Italia tra PA e imprese
Roma, 25 settembre 2018

Telsy

Telsy: profilo dell’azienda

Fondata nel 1971

Oggi 100% gruppo TIM

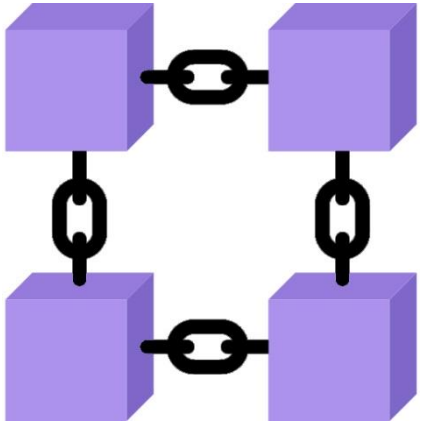
Sotto Golden Power

Specializzata in cybersecurity e crittografia

Applicazioni in ambito governativo e civile

Fortemente attiva nella ricerca

Blockchain



Implementata per la prima volta nel 2009 (Bitcoin)

Acquista notorietà dal 2015

Permette applicazioni rivoluzionarie

Oggi è alla base di soluzioni concrete e innovative

I concetti di base sono tuttora validi

Tuttavia richiede ancora molta ricerca

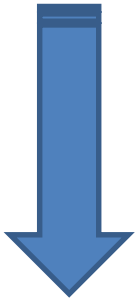
Telsy

Scenario applicativo: data analysis

Big Data

- Grandi quantità di **dati individuali**
  - **sanitari**
  - **economici**
  - **finanziari**
  - **…**
- Relativi ai singoli *individui*
- Spesso raccolti e gestiti in banche dati specializzate
- Tramite tecniche di elaborazione e aggregazione è possibile estrarre informazioni utili per la *data analysis*

Big Data



Data mining
Artificial intelligence
Machine learning
Analytics technologies

Dati aggregati

- Marketing
- Ricerca medica
- Analisi del crimine
- Valutazione del credito
- Assicurazioni
- …

Telsy

Scenario applicativo: data analysis

Dati individuali

- Spesso sono **dati sensibili**
- Gli *individui*
  - non li vogliono condividere (privacy)
  - non hanno interesse a farlo
- Sono soggetti a stringenti vincoli normativi (GDPR)
- Di conseguenza non sempre sono disponibili ai *data analyst*

Requisiti innovazione

- Esigenza di schemi di utilizzo delle informazioni che
  - incentivino la condivisione dei dati
  - ne garantiscano la riservatezza

Telsy

Dati aggregati nel rispetto della privacy

In collaborazione con il Politecnico di Torino (A. Di Nenno, Prof. D. Bazzanella)

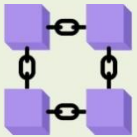
Blockchain

Struttura che implementa un database

- distribuito
- sicuro
- verificabile
- permanente

Tiene traccia indelebile delle operazioni nelle diverse fasi per risolvere eventuali contenziosi

Implementa gli smart contract



Smart contract

Programmi che implementano (tramite blockchain) **contratti** tra *individui* e *data analyst*

- ne definiscono i termini
- ne garantiscono il rispetto

Generano **automaticamente** ricompense (**incentivi**) agli *individui* quando i loro dati vengono usati

Multi party Computation

Servizio crittografico esterno alla blockchain ma ad essa agganciato

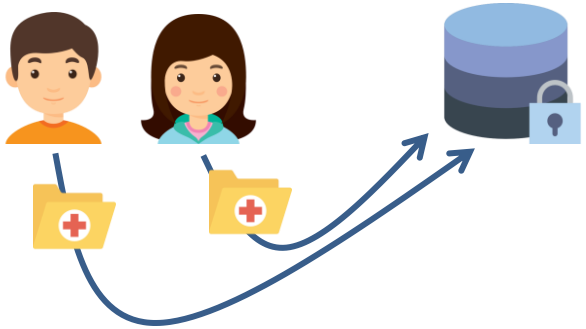
Interagisce con smart contract

Elabora dati individuali *in forma protetta* e fornisce ai *data analyst* i dati aggregati

I dati individuali non sono mai portati in chiaro

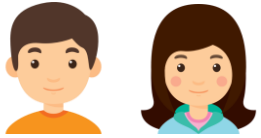
Telsy

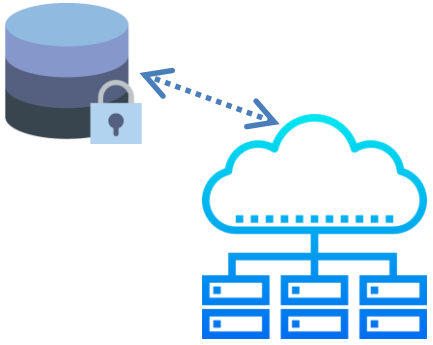
Dati aggregati nel rispetto della privacy

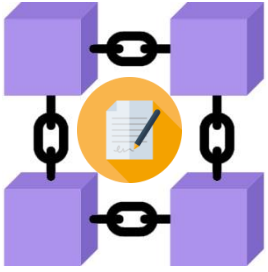


Telsy

Dati aggregati nel rispetto della privacy

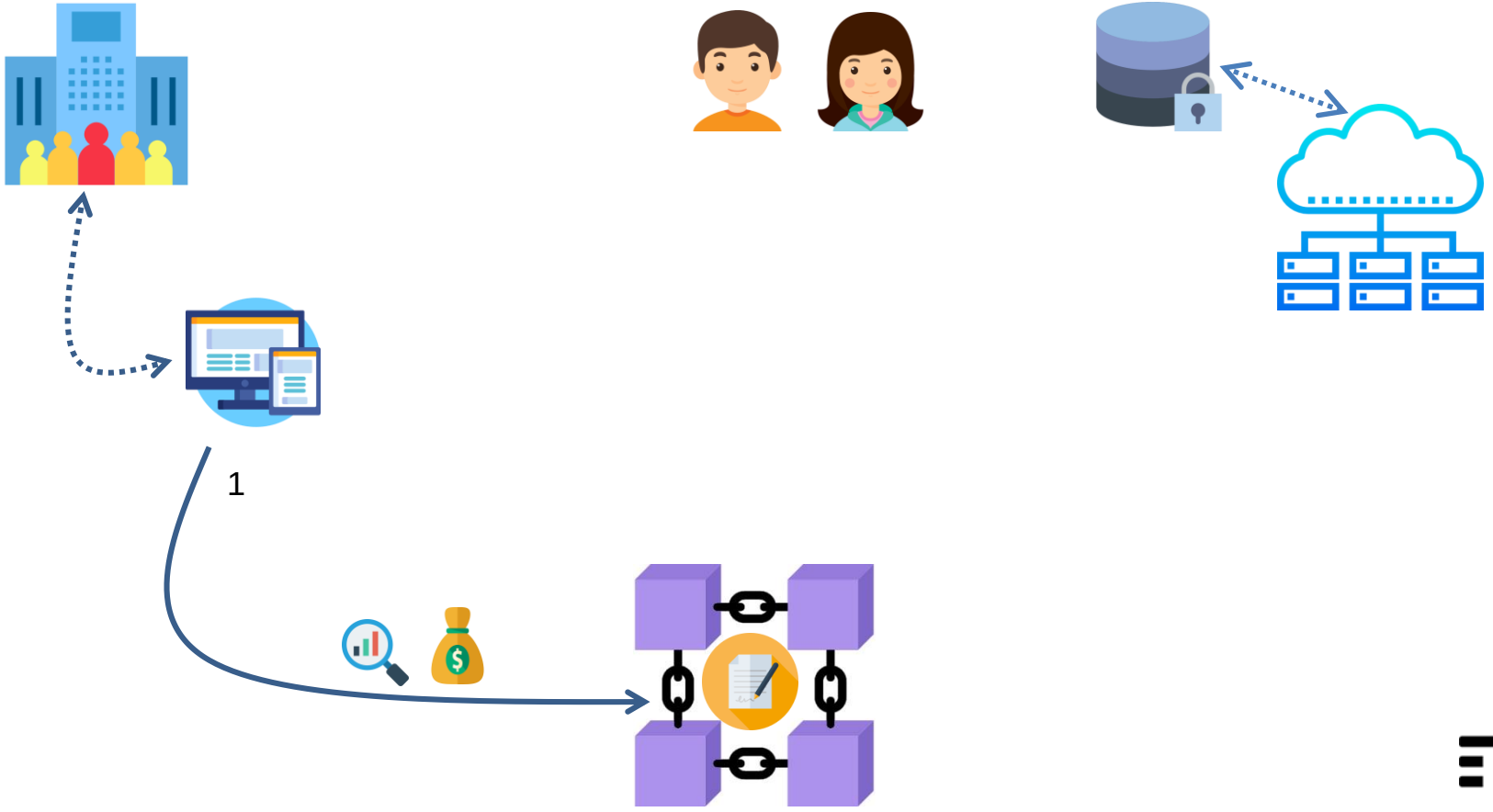






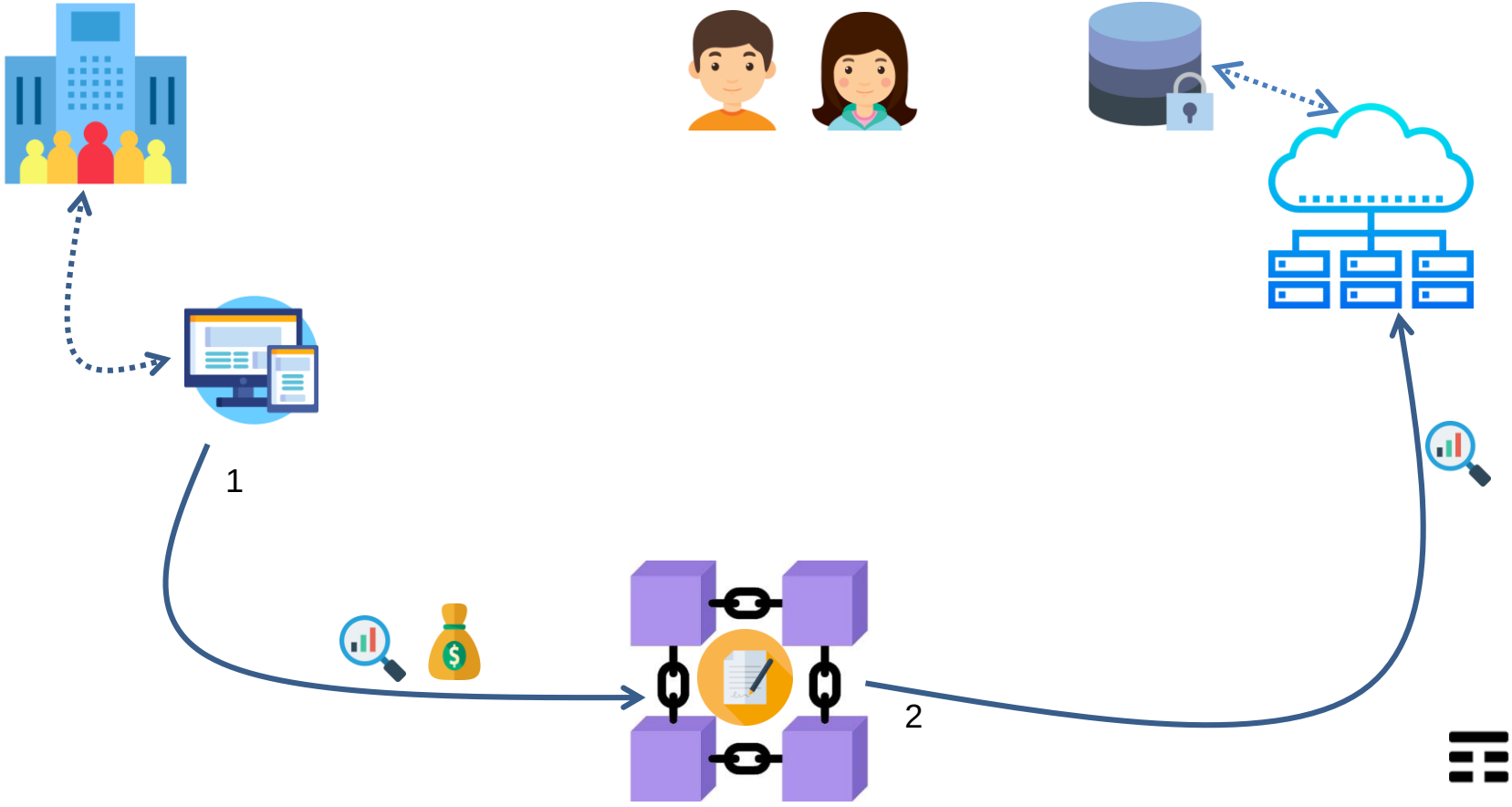
Telsy

Dati aggregati nel rispetto della privacy



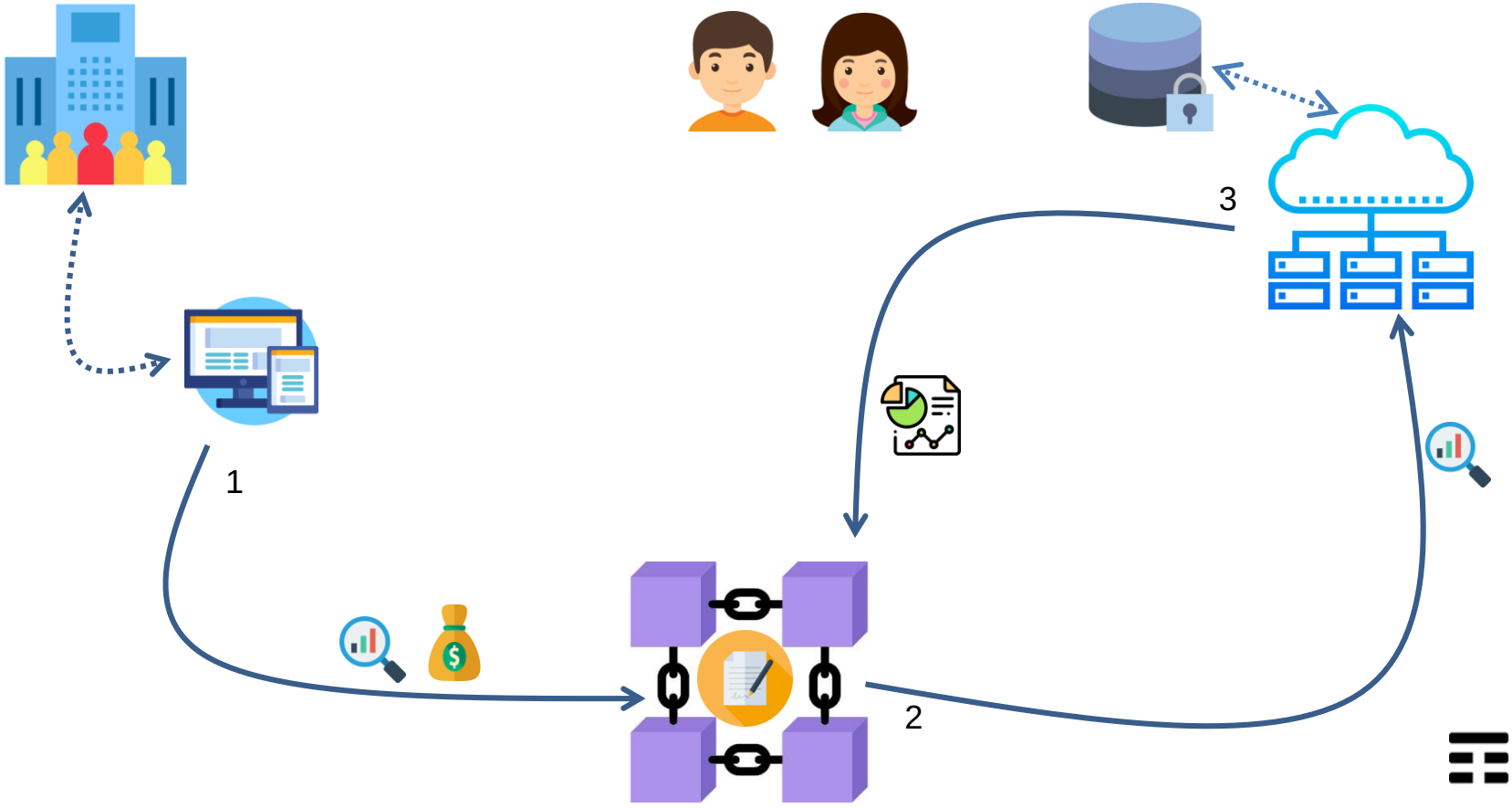
Telsy

Dati aggregati nel rispetto della privacy



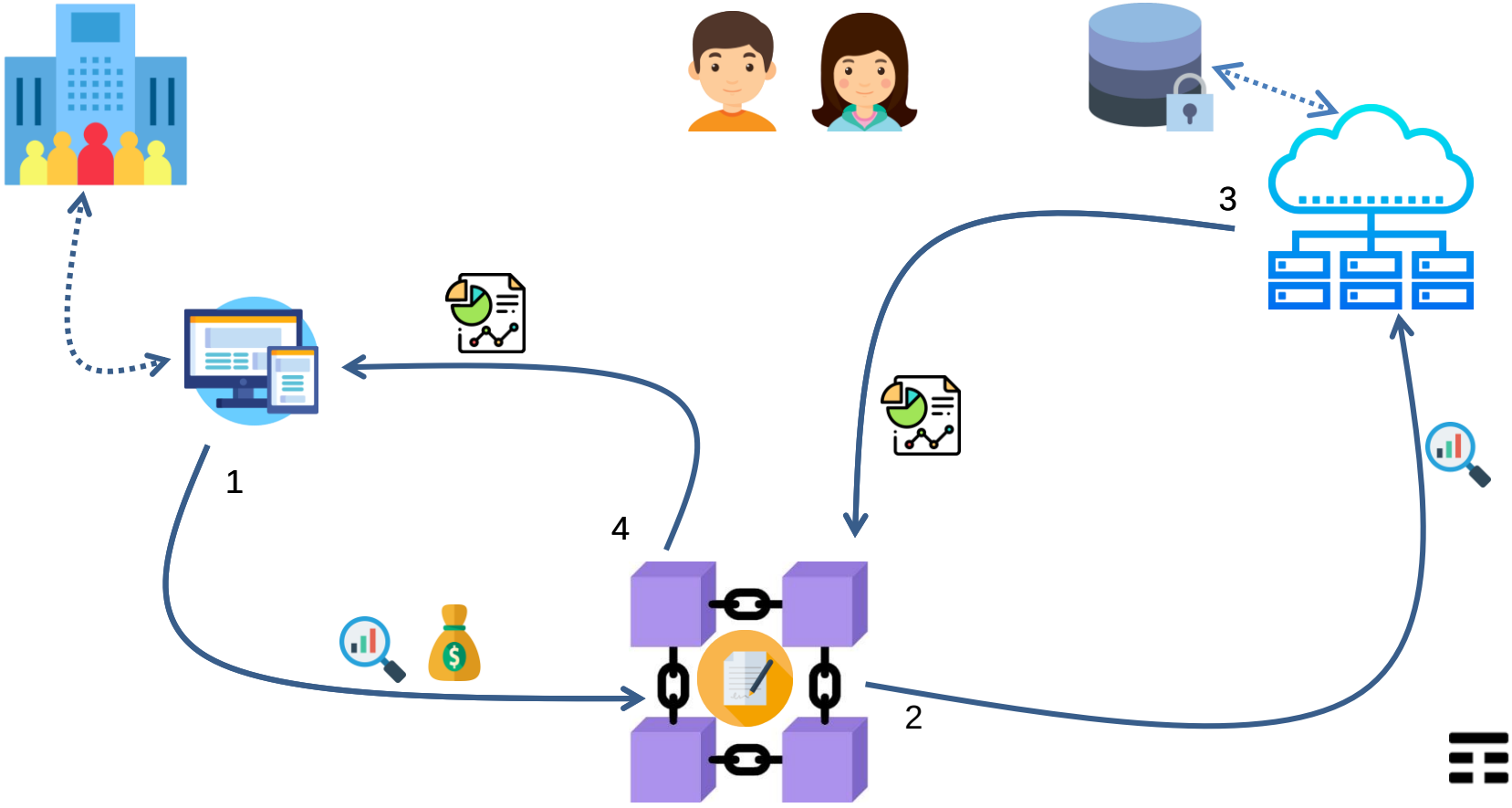
Telsy

Dati aggregati nel rispetto della privacy



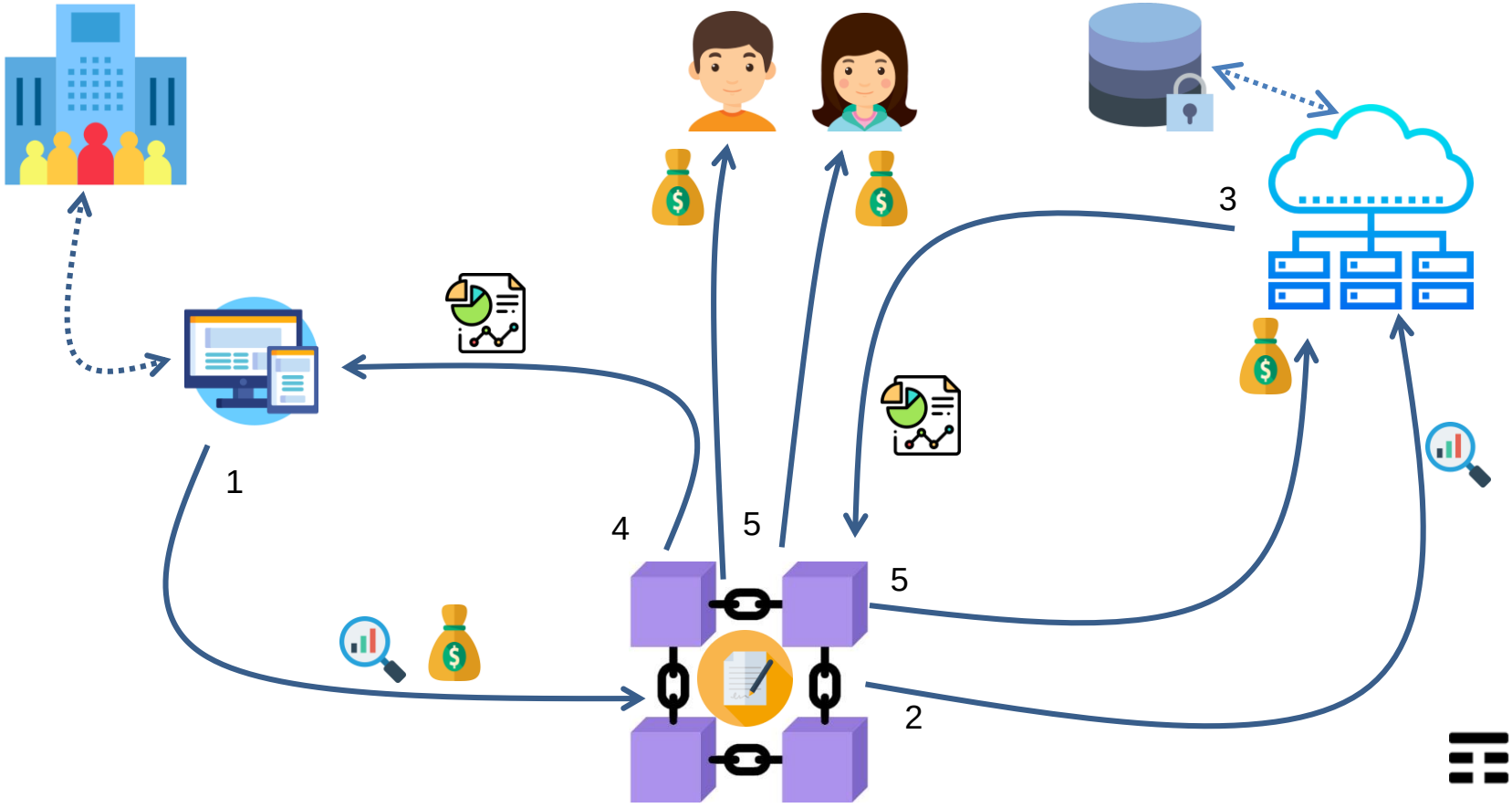
Telsy

Dati aggregati nel rispetto della privacy



Telsy

Dati aggregati nel rispetto della privacy



Telsy

Note conclusive

- Evoluzione del progetto
  - Scelta blockchain ottimale
  - Valutazione alternative crittografiche
  - Ottimizzazione dell'implementazione
  - Test di scalabilità

- Applicazioni delle stesse tecniche a scenari differenti
  - es. Match-making: incontro domanda e offerta con anonimizzazione dei dati

- Necessità di **ricerca continua** su blockchain e tecnologie collegate
  - Straordinario potenziale applicativo
  - Blockchain attuale come punto di partenza e non di arrivo

Telsy