A Distributed Ledger based infrastructure for Intelligent Transportation Systems

Mirko Zichichi

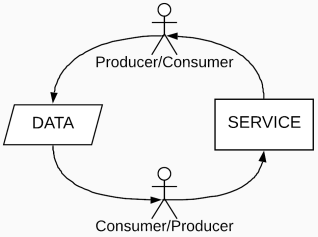
Relatore: Prof. Stefano Ferretti

Sommario

Introduzione

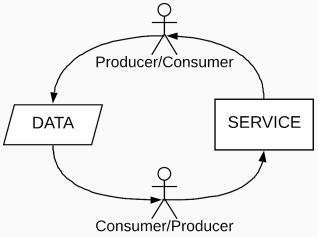
Infrastruttura [1/2]

Lo scopo principale di questa infrastruttura è quello di fornire il controllo assoluto sui propri **dati** prodotti e sulle **transazioni** effettuate agli utenti che si muovono all'interno di Sistemi di Trasporto Intelligenti (ITS).



Infrastruttura [1/2]

Lo scopo principale di questa infrastruttura è quello di fornire il controllo assoluto sui propri **dati** prodotti e sulle **transazioni** effettuate agli utenti che si muovono all'interno di Sistemi di Trasporto Intelligenti (ITS).



La **decentralizzazione** fornita dall'uso di Distributed Ledger Technologies (DLTs) permette a chiunque di poter operare all'interno dell'infrastruttura, senza dipendere da un'entità centrale.

Infrastruttura [2/2]

Data Sharing

Marketplace nel quale gli utenti **pubblicano** i dati prodotti a bordo dei veicoli ed altri utenti possono **accedervi** in seguito ad un accordo

Infrastruttura [2/2]

Data Sharing

Marketplace nel quale gli utenti **pubblicano** i dati prodotti a bordo dei veicoli ed altri utenti possono **accedervi** in seguito ad un accordo

Smart Services

Sfruttano appieno l'utilizzo di **Smart Contracts** per fornire servizi di trasporto agli utenti

Infrastruttura [2/2]

Data Sharing

Marketplace nel quale gli utenti **pubblicano** i dati prodotti a bordo dei veicoli ed altri utenti possono **accedervi** in seguito ad un accordo

Smart Services

Sfruttano appieno l'utilizzo di **Smart Contracts** per fornire servizi di trasporto agli utenti

- **Servizi di trasporto peer-to-peer** (p2p ridesharing)

Infrastruttura [2/2]

Data Sharing

Marketplace nel quale gli utenti **pubblicano** i dati prodotti a bordo dei veicoli ed altri utenti possono **accedervi** in seguito ad un accordo

Smart Services

Sfruttano appieno l'utilizzo di **Smart Contracts** per fornire servizi di trasporto agli utenti

- **Servizi di trasporto peer-to-peer** (p2p ridesharing)
- **Manutenzione e sicurezza del veicolo** tramite un servizio in remoto

Infrastruttura [2/2]

Data Sharing

Marketplace nel quale gli utenti **pubblicano** i dati prodotti a bordo dei veicoli ed altri utenti possono **accedervi** in seguito ad un accordo

Smart Services

Sfruttano appieno l'utilizzo di **Smart Contracts** per fornire servizi di trasporto agli utenti

- **Servizi di trasporto peer-to-peer** (p2p ridesharing)
- **Manutenzione e sicurezza del veicolo** tramite un servizio in remoto
- Servizi basati sull'aggregazione di **dati ambientali** forniti dai singoli utenti

Infrastruttura [2/2]

Data Sharing

Marketplace nel quale gli utenti **pubblicano** i dati prodotti a bordo dei veicoli ed altri utenti possono **accedervi** in seguito ad un accordo

Smart Services

Sfruttano appieno l'utilizzo di **Smart Contracts** per fornire servizi di trasporto agli utenti

- **Servizi di trasporto peer-to-peer** (p2p ridesharing)
- **Manutenzione e sicurezza del veicolo** tramite un servizio in remoto
- Servizi basati sull'aggregazione di **dati ambientali** forniti dai singoli utenti
- Integrazione dei **servizi di trasporto pubblico** con i dati forniti dagli utenti e con l'utilizzo di Smart Contracts per le transazioni

Distributed Technologies

- **Ethereum** - Fornisce una blockchain con un linguaggio quasi-Turing-completo che può essere usato per creare "**Contratti**" che codificano transazioni tra parti.

Distributed Technologies

- **Ethereum** - Fornisce una blockchain con un linguaggio quasi-Turing-completo che può essere usato per creare "**Contratti**" che codificano transazioni tra parti.
- **IOTA** - Technologia specificatamente progettata per l'industria dell'IoT, dove il registro distribuito prende la forma di un **Grafo Diretto Aciclico (DAG)**.

Distributed Technologies

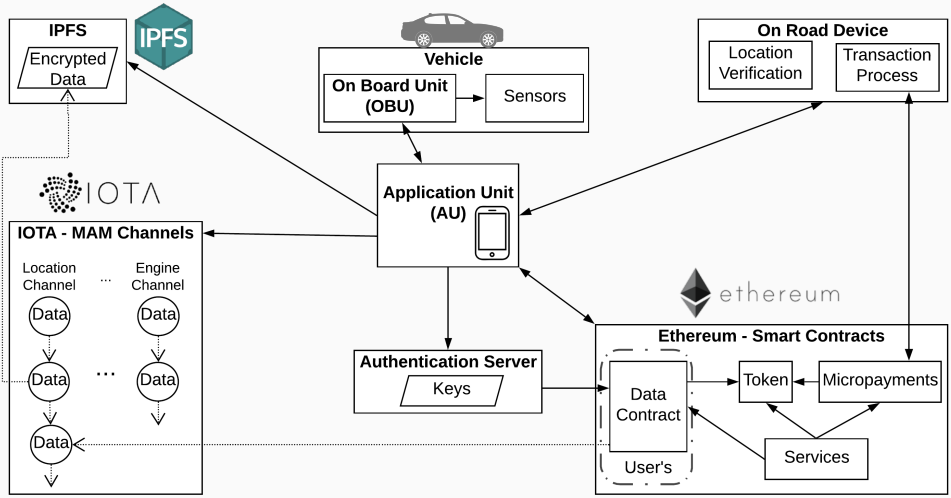
- **Ethereum** - Fornisce una blockchain con un linguaggio quasi-Turing-completo che può essere usato per creare "**Contratti**" che codificano transazioni tra parti.
- **IOTA** - Technologia specificatamente progettata per l'industria dell'IoT, dove il registro distribuito prende la forma di un **Grafo Diretto Aciclico (DAG)**.
- **IPFS** - Protocollo che permette di connettere tutti i nodi di una rete p2p tramite un **unico file system distribuito**.

Distributed Technologies

- **Ethereum** - Fornisce una blockchain con un linguaggio quasi-Turing-completo che può essere usato per creare "**Contratti**" che codificano transazioni tra parti.
- **IOTA** - Technologia specificatamente progettata per l'industria dell'IoT, dove il registro distribuito prende la forma di un **Grafo Diretto Aciclico (DAG)**.
- **IPFS** - Protocollo che permette di connettere tutti i nodi di una rete p2p tramite un **unico file system distribuito**.
- **Zero Knowledge Proof** - Metodo crittografico che permette ad un Prover di provare ad un Verifier di conoscere un **segreto** senza rivelarlo.

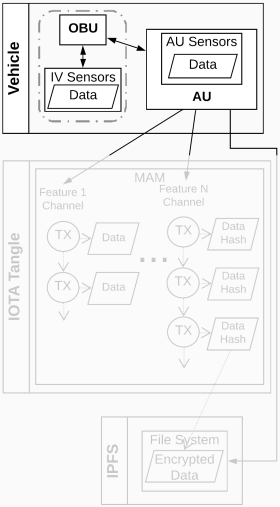
Architettura

Punto di vista dell'utente



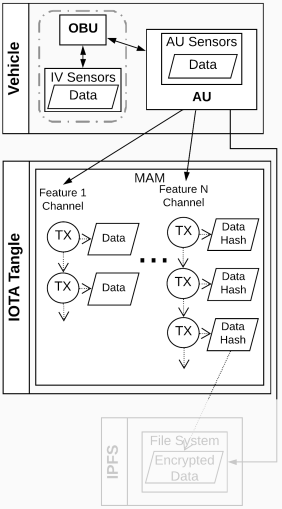
Data Sharing

- **Acquisizione dei dati**
  I dati relativi ad un utente vengono acquisiti dai **sensori** del veicolo o dell'AU (smartphone).



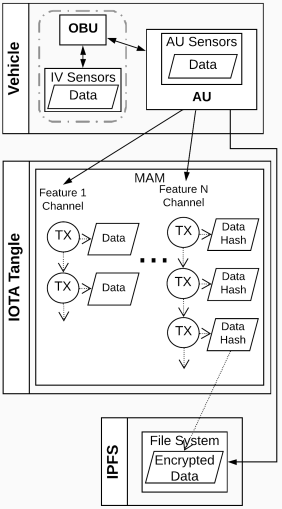
Data Sharing

- **Acquisizione dei dati**
  I dati relativi ad un utente vengono acquisiti dai **sensori** del veicolo o dell'AU (smartphone).
- **IOTA Masked Authenticated Messaging (MAM)**
  Protocollo che permette di creare **canali di transazioni** cifrati per conservare e condividere dati.
  I dati acquisiti vengono raggruppati in **feature** e caricati nel canale associato come transazioni.



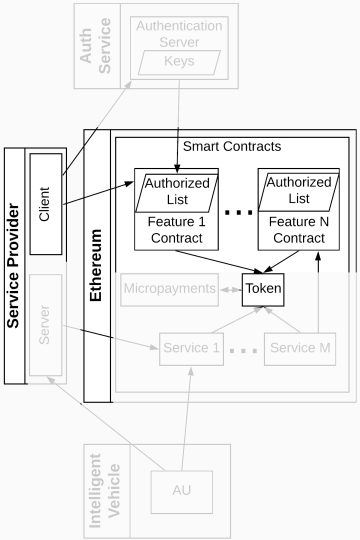
Data Sharing

- **Acquisizione dei dati**
  I dati relativi ad un utente vengono acquisiti dai **sensori** del veicolo o dell'AU (smartphone).
- **IOTA Masked Authenticated Messaging (MAM)**
  Protocollo che permette di creare **canali di transazioni** cifrati per conservare e condividere dati. I dati acquisiti vengono raggruppati in **feature** e caricati nel canale associato come transazioni.
- **IPFS Objects**
  I dati che consumano più spazio vengono salvati come IPFS Objects e poi referenziati sui canali MAM



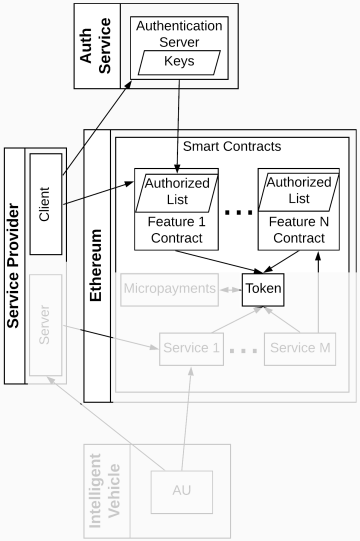
Accesso ai dati e Smart Services

- **Acquisizione dati**
  Il diritto di accesso ai dati di un utente può essere acquisito tramite uno Smart Contract che mantiene una **Lista di Autorizzati**.



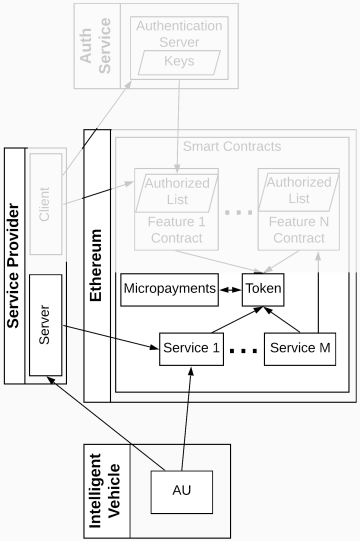
Accesso ai dati e Smart Services

- **Acquisizione dati**
  Il diritto di accesso ai dati di un utente può essere acquisito tramite uno Smart Contract che mantiene una **Lista di Autorizzati**.
- **Accesso ai dati**
  Gli aventi diritto richiedono le chiavi di accesso dei canali MAM ad un **Servizio di Autenticazione**



Accesso ai dati e Smart Services

- **Acquisizione dati**
  Il diritto di accesso ai dati di un utente può essere acquisito tramite uno Smart Contract che mantiene una **Lista di Autorizzati**.
- **Accesso ai dati**
  Gli aventi diritto richiedono le chiavi di accesso dei canali MAM ad un **Servizio di Autenticazione**
- **Smart Services**
  I dati acquisiti possono essere usati da un Provider per fornire servizi basati sull'utilizzo degli **Smart Contracts** come Business Logic.
  Le transazioni possono avvenire **on-chain** oppure **off-chain**.



Second Layer Trust

La validazione dei dati e delle transazioni nelle DLTs si basa sulla **fiducia** nell'algoritmo di consenso. La fiducia nella **veridicità dei dati** può essere costruita su un secondo layer

Second Layer Trust

La validazione dei dati e delle transazioni nelle DLTs si basa sulla **fiducia** nell'algoritmo di consenso. La fiducia nella **veridicità dei dati** può essere costruita su un secondo layer

- **Public Key Infrastructure (PKI)**
  Dei trusted devices all'interno di una PKI possono rilasciare **certificati** che validano la correttezza dei dati dell'utente.

Second Layer Trust

La validazione dei dati e delle transazioni nelle DLTs si basa sulla **fiducia** nell'algoritmo di consenso. La fiducia nella **veridicità dei dati** può essere costruita su un secondo layer

- **Public Key Infrastructure (PKI)**
  Dei trusted devices all'interno di una PKI possono rilasciare **certificati** che validano la correttezza dei dati dell'utente.
- **Zero Knowledge Proof of Location**
  Permette di **verificare** la presenza di un utente in una determinata **area geografica**, senza che questo comunichi le sue coordinate spaziali

Validazione

Scalabilità

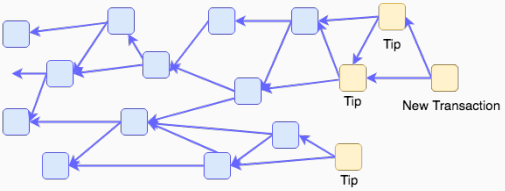
- **Numero di Nodi**
  Nuovi nodi possono facilmente aggiungersi alle reti **Ethereum**, **IOTA** e **IPFS**, perché queste sono **Permissionless**

Scalabilità

- **Numero di Nodi**
  Nuovi nodi possono facilmente aggiungersi alle reti **Ethereum**, **IOTA** e **IPFS**, perché queste sono **Permissionless**
- **Ethereum State Channels**
  Per i Micropagamenti vengono utilizzati gli State Channels, un design pattern per **transazioni istantanee off-chain**

Scalabilità

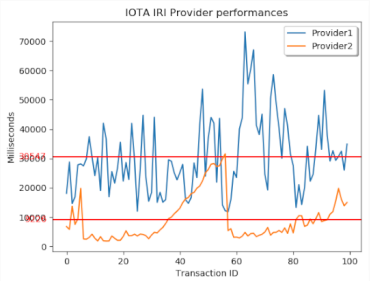
- **Numero di Nodi**
  Nuovi nodi possono facilmente aggiungersi alle reti **Ethereum**, **IOTA** e **IPFS**, perché queste sono **Permissionless**
- **Ethereum State Channels**
  Per i Micropagamenti vengono utilizzati gli State Channels, un design pattern per **transazioni istantanee off-chain**
- **IOTA Tangle**

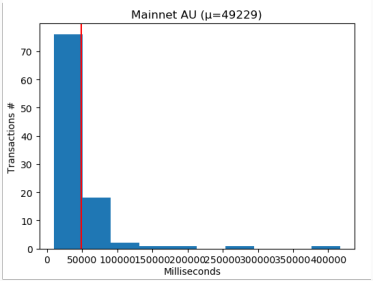


Inserimento di una transazione:
- **Tips Selection**
- **Proof of Work**

All'aumentare del numero di nuove transazioni, diminuisce il tempo di attaccamento alla Tangle

Tempo di latenza inserimento transazione IOTA





Differenza di tempo di inserimento nella Tangle

Provider1 poco utilizzato, Provider2 molto utilizzato

Canali MAM

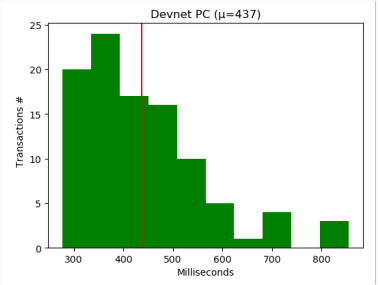
Richiedono circa 20 secondi in più

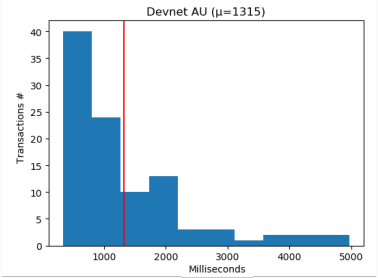
Tempo di latenza inserimento transazione IOTA

Canali MAM

Differenza di difficoltà del PoW

Tempo di latenza inserimento transazione IOTA





Differenza di tempo di inserimento su Canali MAM

PC e Smartphone

Conclusione

Conclusione

- L'**infrastruttura decentralizzata** presentata si basa sull'interazione di diverse tecnologie per fornire due funzionalità agli utenti all'interno di ITS: Data Sharing e Smart Services

Conclusione

- L'**infrastruttura decentralizzata** presentata si basa sull'interazione di diverse tecnologie per fornire due funzionalità agli utenti all'interno di ITS: Data Sharing e Smart Services
- Le soluzioni adottate in questo lavoro si focalizzano sulla **privacy** dell'utente riguardo i suoi dati e sul **controllo** che può avere su di questi, oltre alla possibilità di eseguire **transazioni** in maniera decentralizzata

Conclusione

- L'**infrastruttura decentralizzata** presentata si basa sull'interazione di diverse tecnologie per fornire due funzionalità agli utenti all'interno di ITS: Data Sharing e Smart Services
- Le soluzioni adottate in questo lavoro si focalizzano sulla **privacy** dell'utente riguardo i suoi dati e sul **controllo** che può avere su di questi, oltre alla possibilità di eseguire **transazioni** in maniera decentralizzata
- Sviluppi futuri:
  - Lo **sharding** consiste nel dividere il registro in più parti, aumentando il throughput delle transazioni
  - Un **content-centric networking** potrebbe consentire di accedere ai dati in maniera più veloce rispetto all'IP networking