DELTA

“Migliorare efficacia e disponibilità della base di conoscenza dell’AM”

AS-IS

Non è sempre possibile avere le condizioni ideali per il training

(meteo, disponibilità mezzi e apparati, tempo a disposizione, costi logistici, efficacia dei formatori, alti costi connessi all'uso di determinate strumentazioni…)

Fare interventi di manutenzione comporta difficoltà legate al trasporto di risorse specifiche

(identificazione della persona giusta per quel determinato problema, reperibilità, sicurezza, tempistiche e costi)

ADDESTRAMENTO

Maggior Realismo
Immersione
Condizioni ideali
Fruibilità e portabilità
Plug&Play

Cost saving
Modulare
Scalabile
Replicabile
Ammortizzabile

Certificazione
Auto update CV
Accesso autorizzato

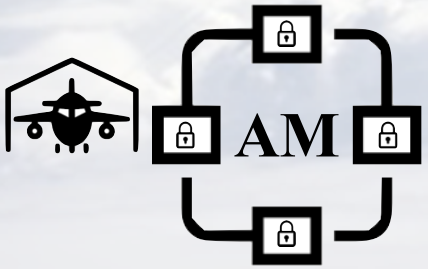
MANUTENZIONE

Accesso a contenuti per personale fuori base

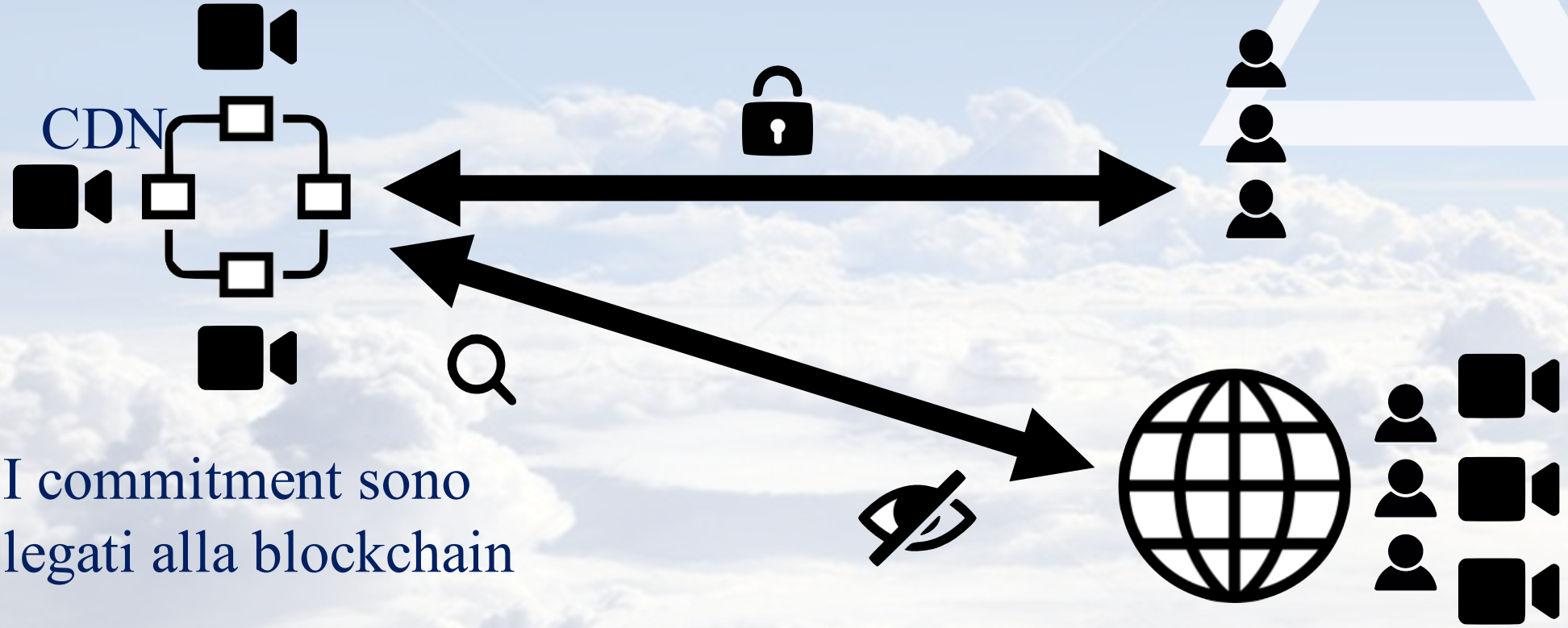
- Materiale Locale
- Autenticazione Richieste

Scambio dati su rete protetta limitato

- Fruizione contenuti offline
- Validazione richieste e contenuti



ARCHITETTURA EVOLUTA



I commitment sono legati alla blockchain

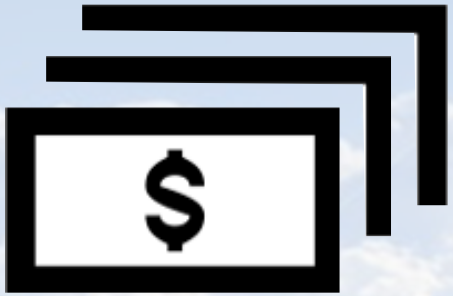
A parametri nascosti quando la rete non è controllata

DEMO

http://40.121.41.140/first.html

COMPONENTI

Video Immersivi



Soluzione plug&play ed economica

Sicurezza avanzata in fase di manutenzione

IMPERSIVE

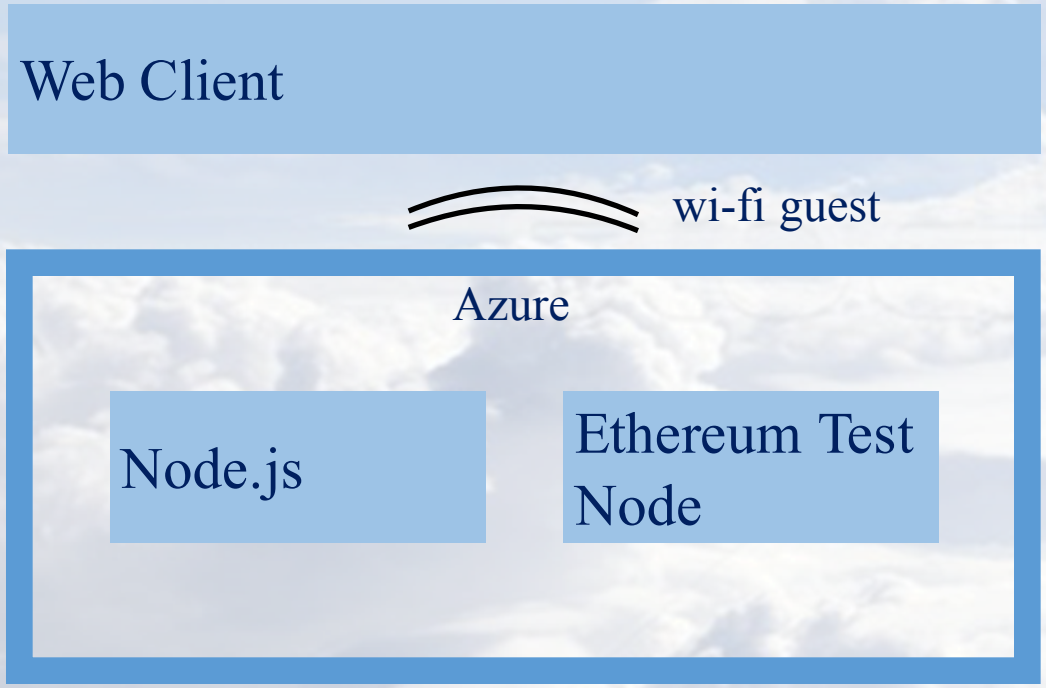
Con LEONARDO VITROCISET Microsoft ptc EY

TEAMΔ

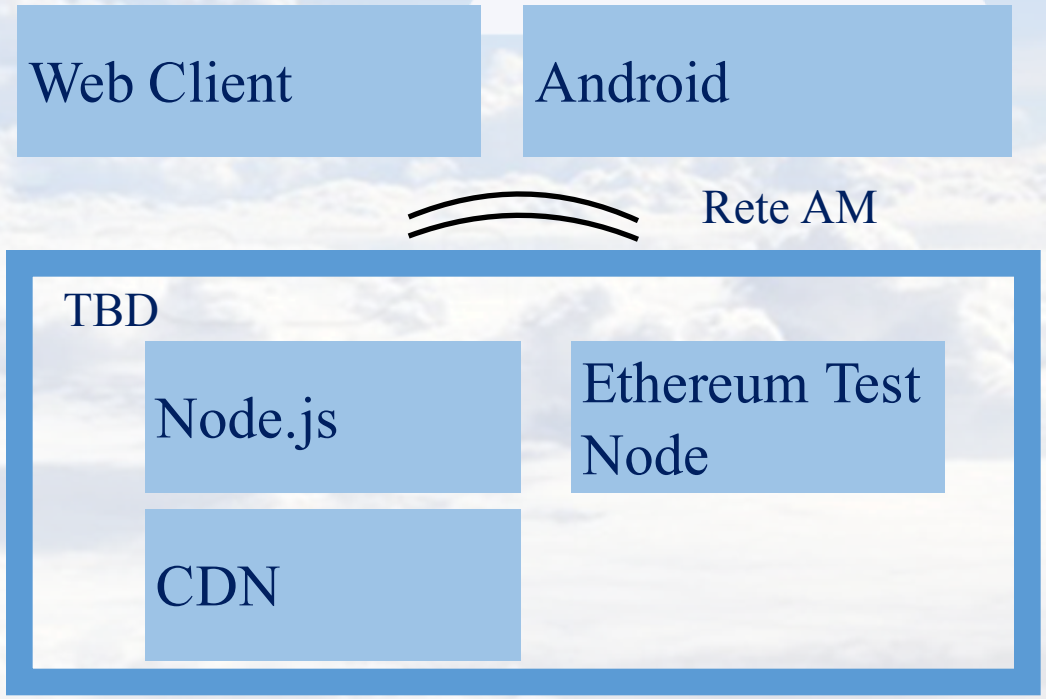
- ANNEX -

ARCHITETTURA

Airathon

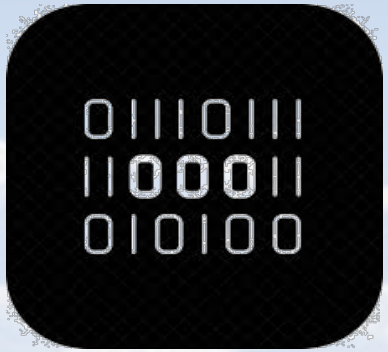


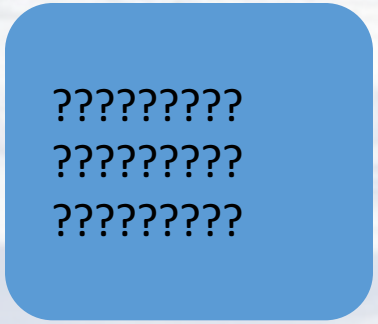
POC Fase 1



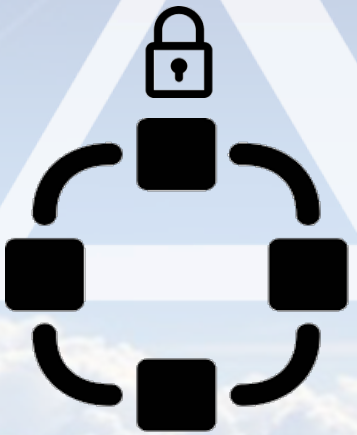
EVOLUTIVE

Video in Streaming, non più solo filmati preimpostati ma collaborazione real-time





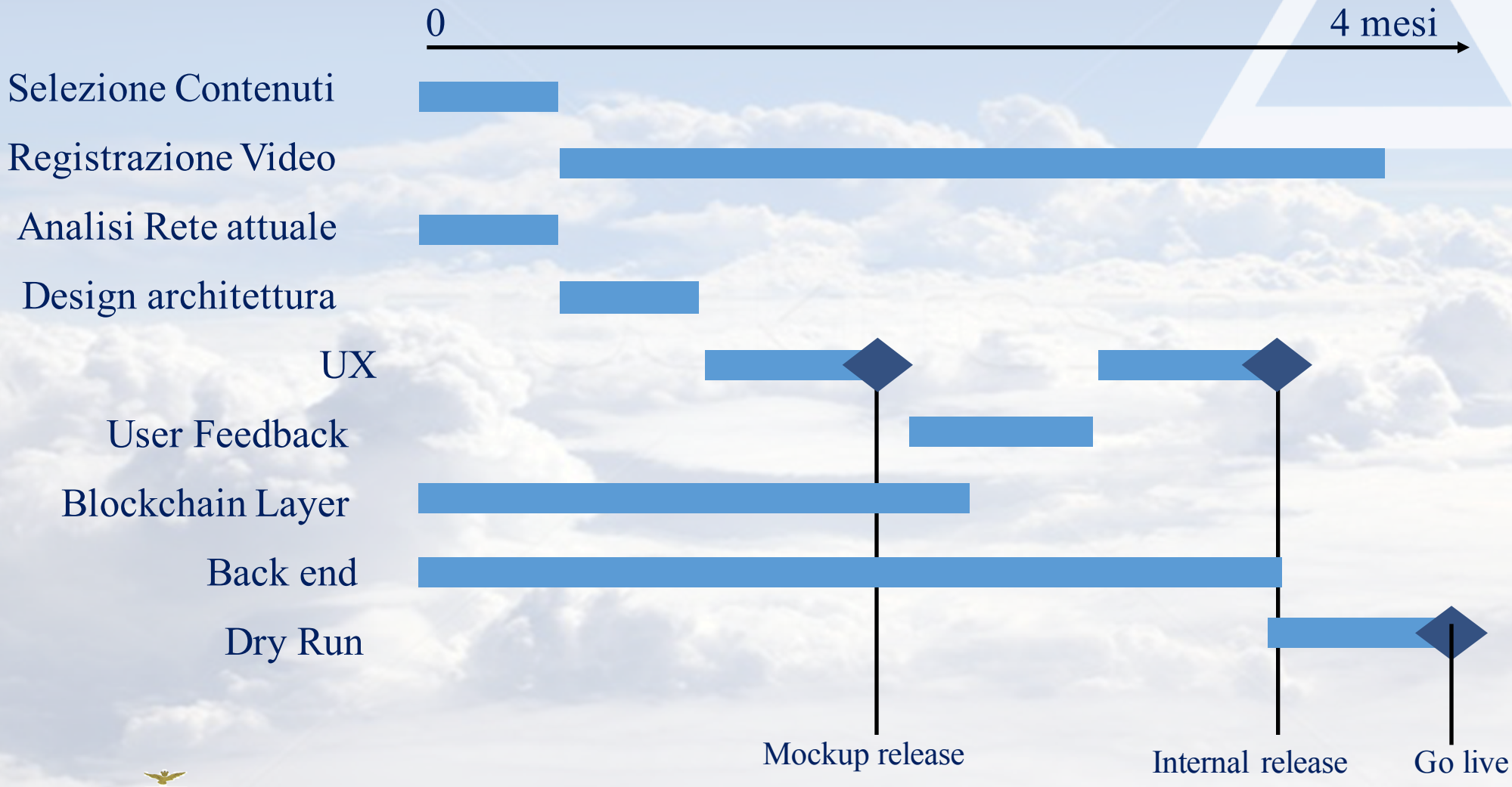
Crittografia hiding BIT PER BIT



Estensione dell'infrastruttura a rete non militare

TEMPISTICHE

PROTOTIPO FASE 1



PARAMETRI NASCOSTI

Setup iniziale, diverso missione per missione, utente per utente

Commitment

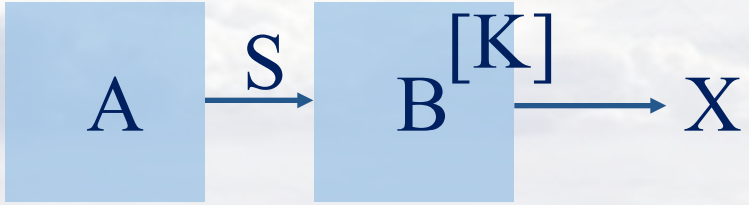
- ID personale
- Motivo Richiesta
- Libreria

Acknowledge

- Sblocco Video

PARAMETRI NASCOSTI

A dichiara un valore X e rivela in un secondo momento a B una chiave per controllare quale valore fosse



PARAMETRI NASCOSTI

Setup condiviso prima del periodo offline

p,q interi primi

g: generatore del setup, < q

a: segreto del setup, < p

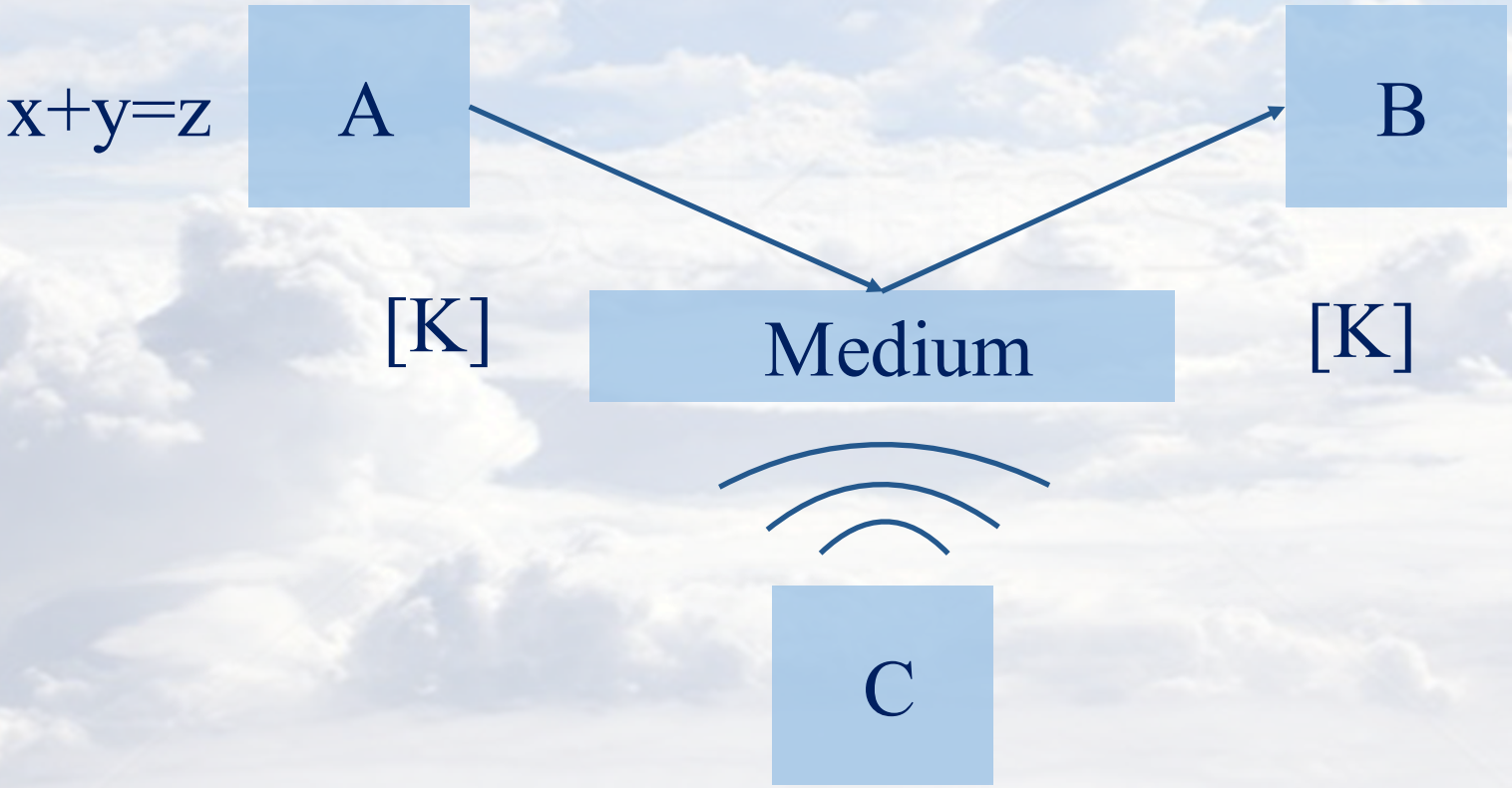
h=g^a mod(p)

Nascondo il valore x usando un numero random r:

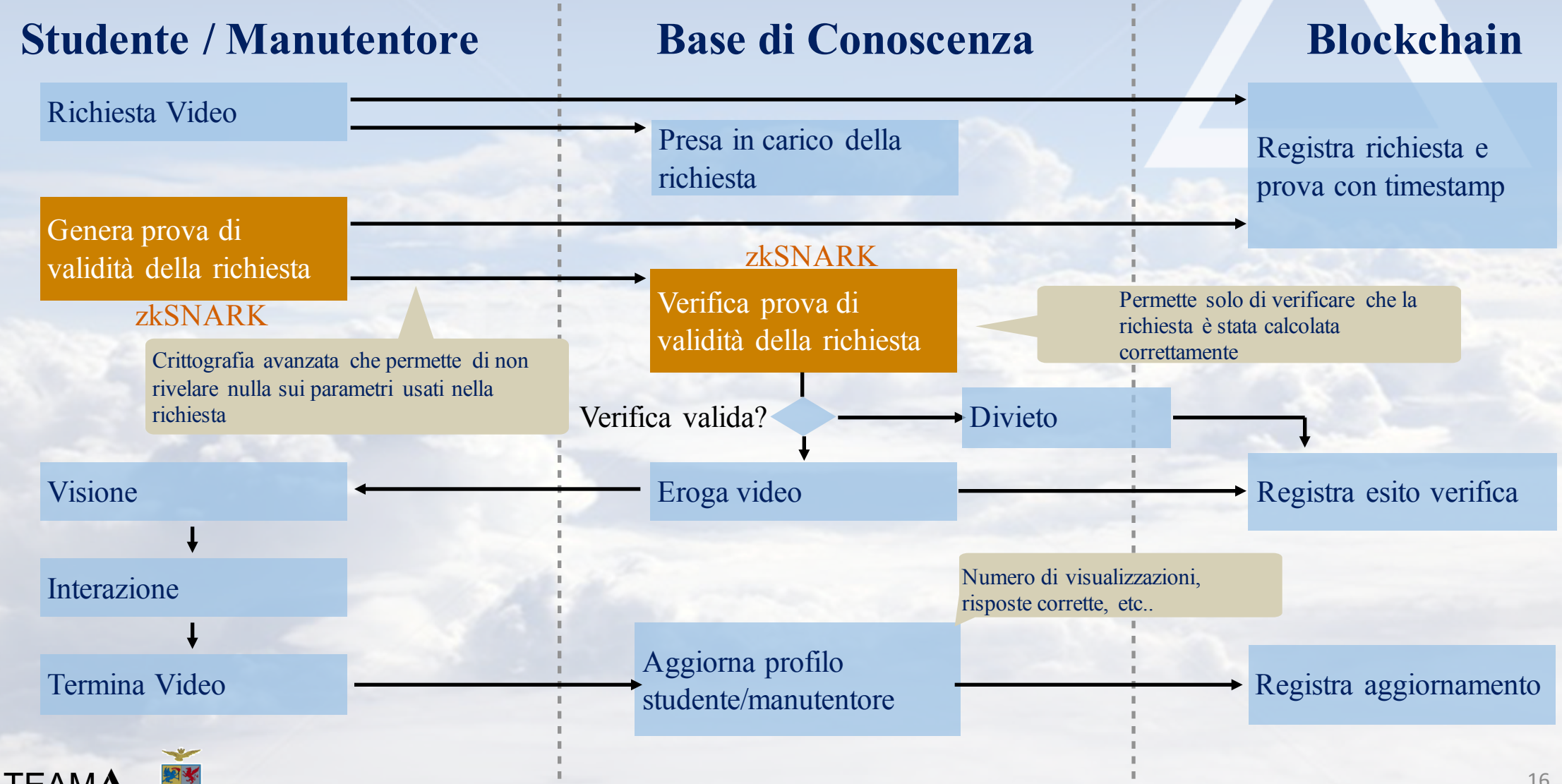
$$\text{commitment} = g^{x} h^{r} \bmod(p)$$

CRITTOGRAFIA ZK

B controlla che A ha calcolato
x+y=z in modo corretto, SENZA rivelare x, y, z

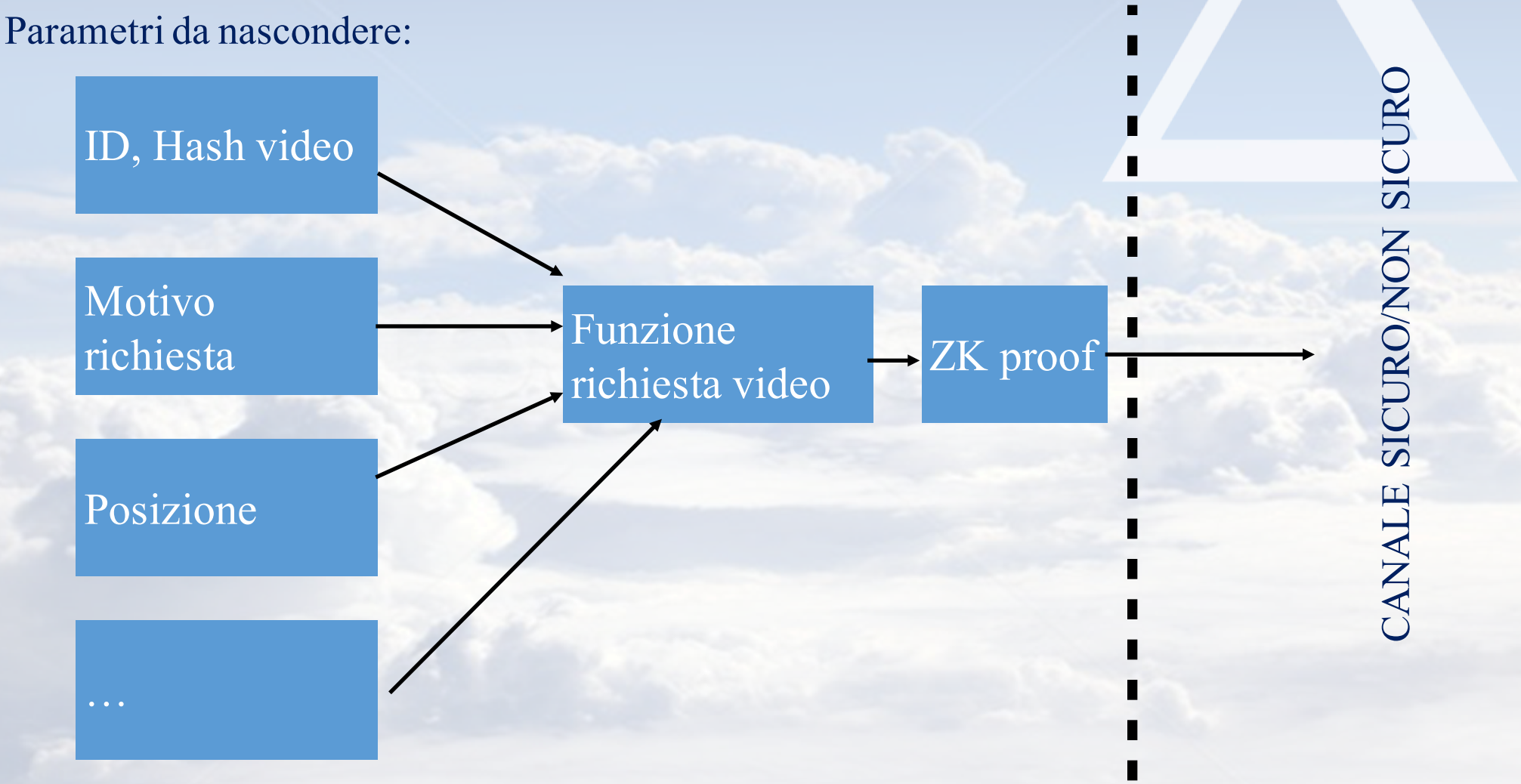


CRITTOGRAFIA ZK



COMUNICAZIONE ZK

Parametri da nascondere:



ONLINE

Missione **Lezione**

Setup iniziale, emissione public keys:
Vk verifying key
Pk proving key

Classic zkSNARK scenario

Verifier

Gestore libreria

Communication Bridge

Witness string:
Dati di una certa missione (quale elicottero, quale componente, etc..) che devono essere detti per formulare una richiesta ma non devono essere rivelati

Video

Video

Video

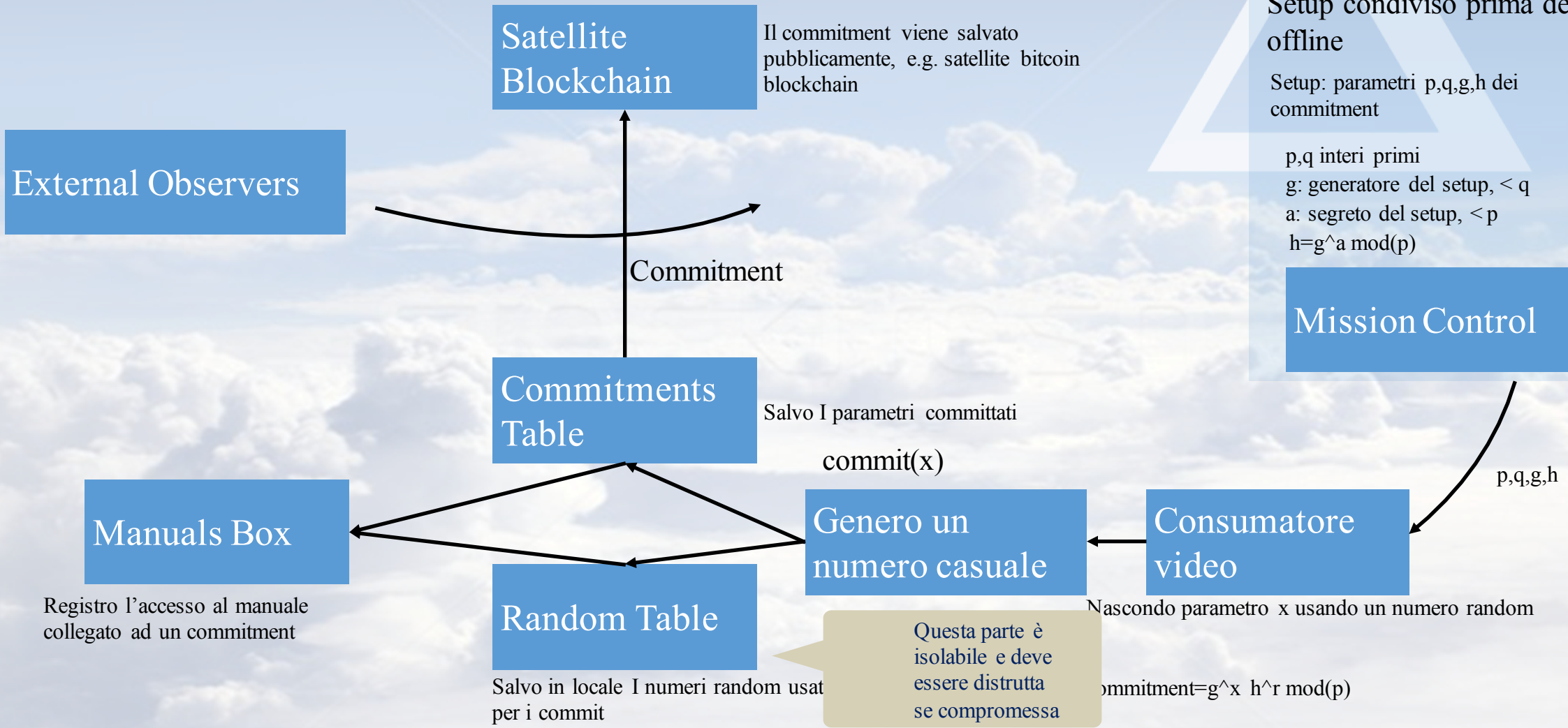
Il verifier e chiunque nel mezzo verifica che il prover ha fatto un'operazione calcolata correttamente. Nel nostro caso la composizione di una richiesta di accesso ad un certo video

Consumatore video

Prover

Manutentore **Studente**

OFFLINE


Satellite Blockchain
Il commitment viene salvato pubblicamente, e.g. satellite bitcoin blockchain
External Observers
Commitment
Commitments Table
Salvo I parametri committati
commit(x)
Manuals Box
Registro l'accesso al manuale collegato ad un commitment
Genero un numero casuale
Consumatore video
Nascondo parametro x usando un numero random
Random Table
Salvo in locale I numeri random usat per i commit
Questa parte è isolabile e deve essere distrutta se compromessa
ommitment=g^x h^r mod(p)
Setup condiviso prima del periodo offline
Setup: parametri p,q,g,h dei commitment
p,q interi primi
g: generatore del setup, < q
a: segreto del setup, < p
h=g^a mod(p)
Mission Control
p,q,g,h

RITORNO ONLINE

Satellite Blockchain

Il commitment viene salvato pubblicamente, e.g. satellite bitcoin blockchain

Mission Control

Tabella dove viene salvata ogni richiesta di manuale e il suo commitment

Commitments Table

Mission Control controlla la coerenza dei committent fatti (timestamp, valori committati, dati di richiesta accessi al manuale)

open(x, r)

Manuals Box

Random Table

Consumatore video

Tabella dove vengono salvati i random per i commitments

Questa parte è isolabile e deve essere distrutta se compromessa

TEAMΔ