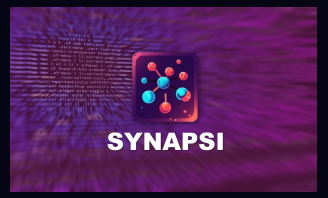
Riflessioni su Tecnologie della Liberazione per l'Arricchimento della Privacy, Crittografia e Comunicazione Sicura, un approccio pratico



A.Montillo

DV Cyber Security
PART OF DIGITAL VALUE GROUP

Crittografia e Comunicazione Sicura: un approccio pratico

Crittografia e Comunicazione Sicura: un approccio pratico

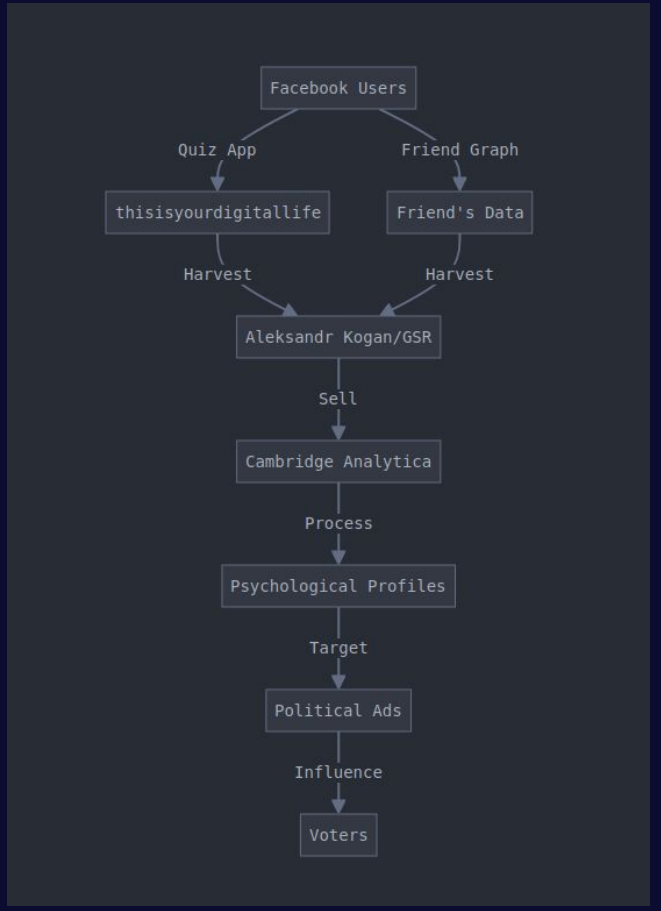
Iniziamo il Viaggio

Introduzione

Analisi del Contesto Attuale

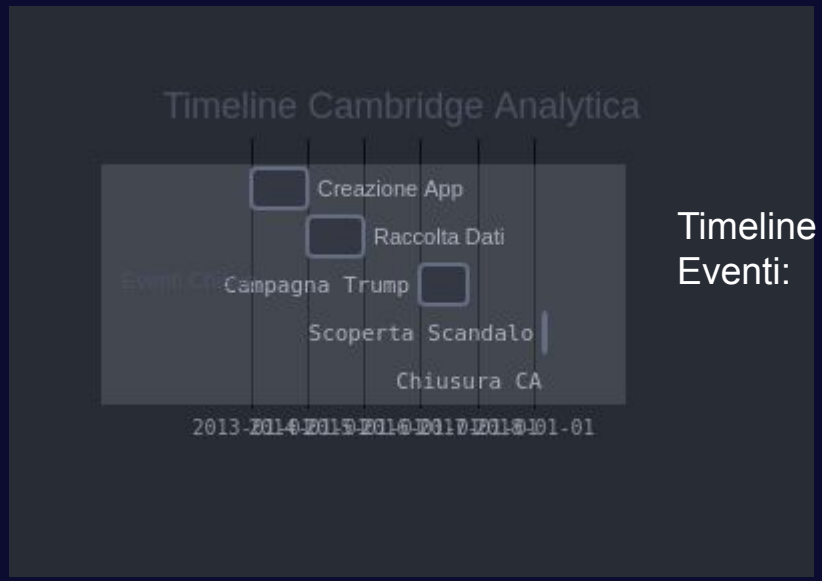
- **Caso Studio: Cambridge Analytica**
  - Impatto sulla democrazia
  - Manipolazione attraverso i dati personali
  - Lezioni apprese sulla protezione dei dati

La Monetizzazione della Privacy

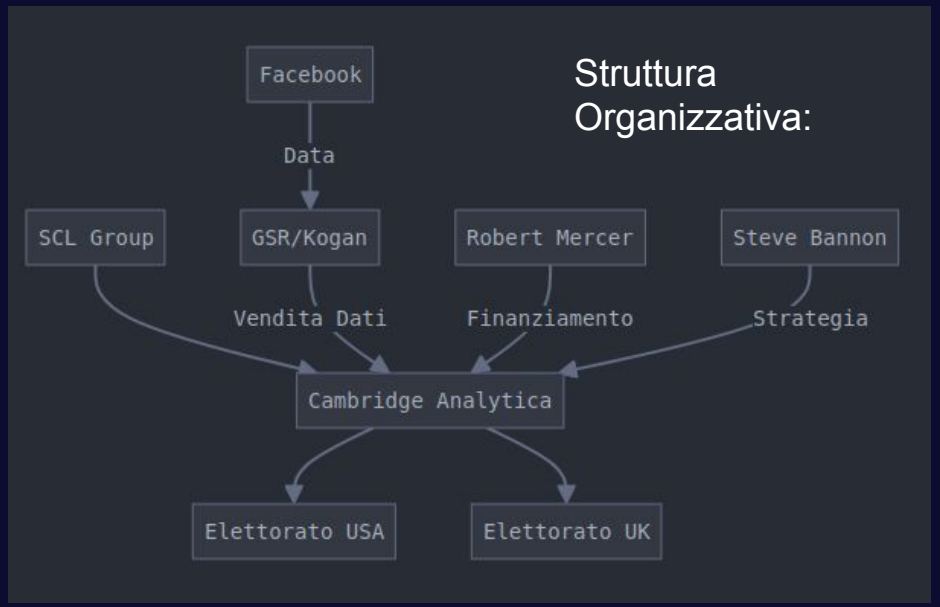


Flusso di Raccolta Dati:

Crittografia e Comunicazione Sicura: un approccio pratico

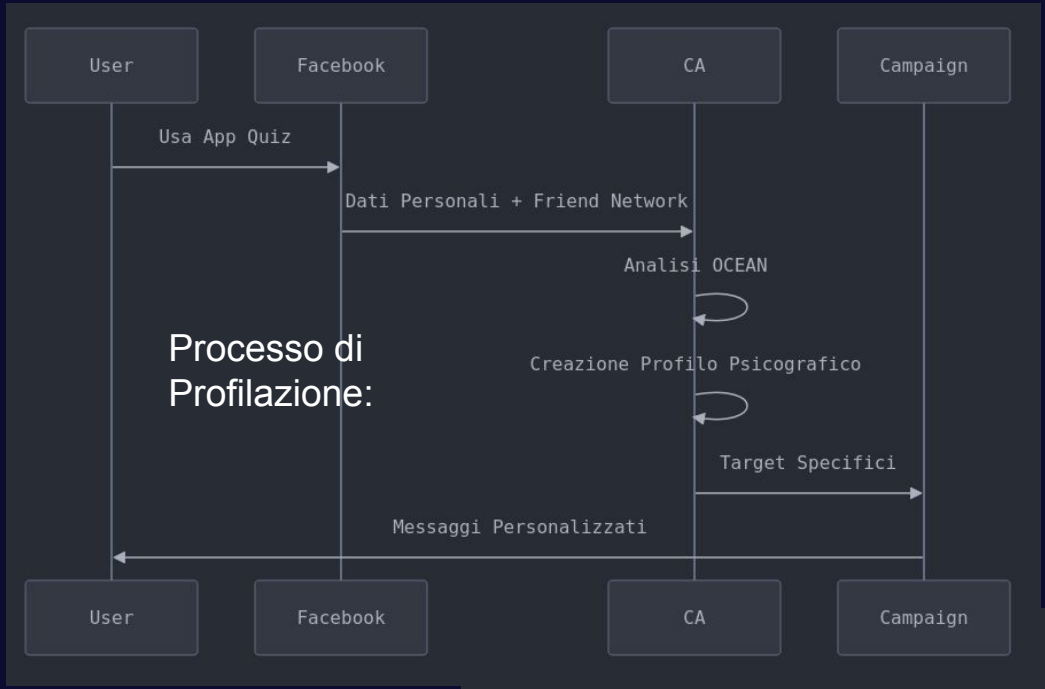


Timeline degli Eventi:



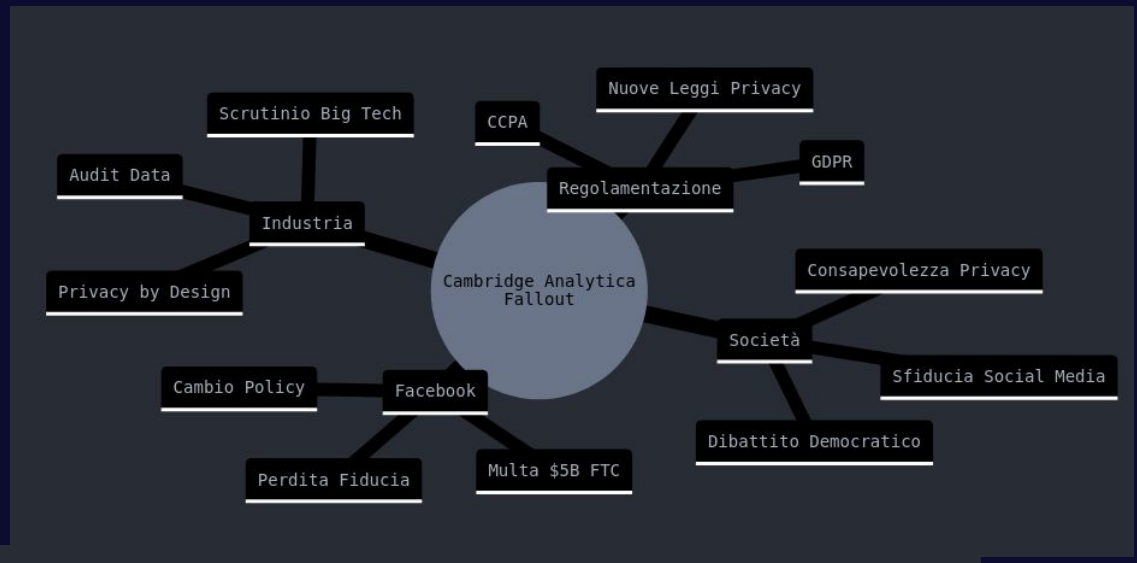
Struttura Organizzativa:

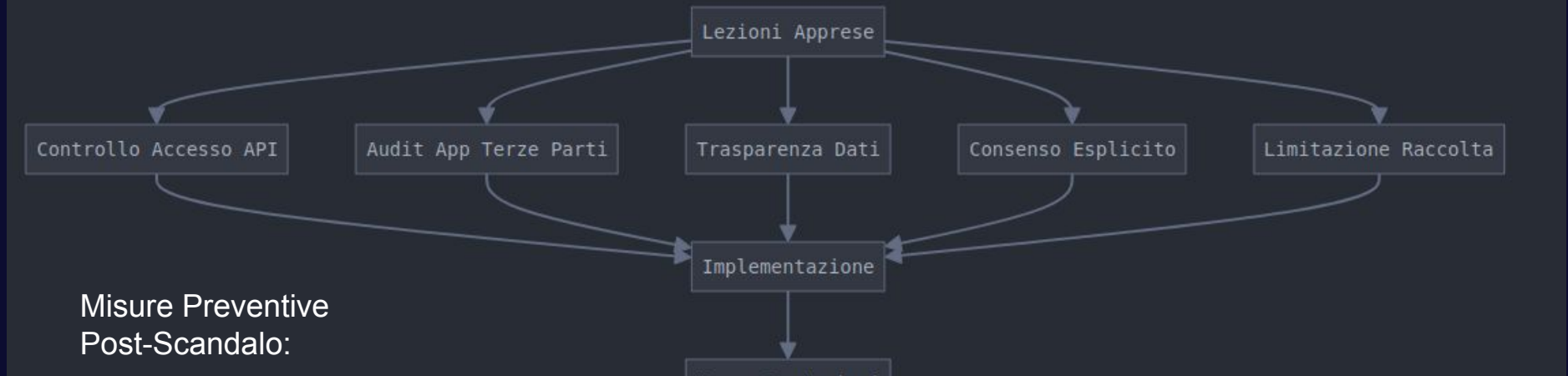
Crittografia e Comunicazione Sicura: un approccio pratico



Processo di Profilazione:

Conseguenze e Impatto:





Misure Preventive Post-Scandalo:

Processo di Profilazione:

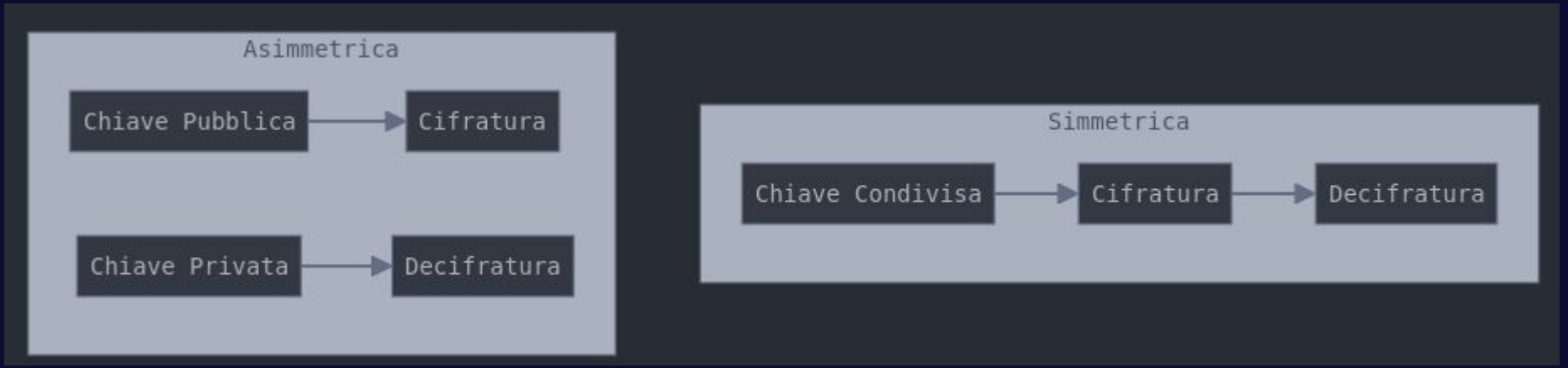
Fondamenti della Crittografia Moderna

La Monetizzazione
della Privacy

Processo di Profilazione:

Fondamenti della Crittografia Moderna

Crittografia Simmetrica vs Asimmetrica



Punti Critici:

- La crittografia simmetrica è veloce ma ha problemi di distribuzione delle chiavi
- La crittografia asimmetrica è sicura ma computazionalmente intensiva
- Vulnerabilità del quantum computing sugli algoritmi attuali

Processo di Profilazione:

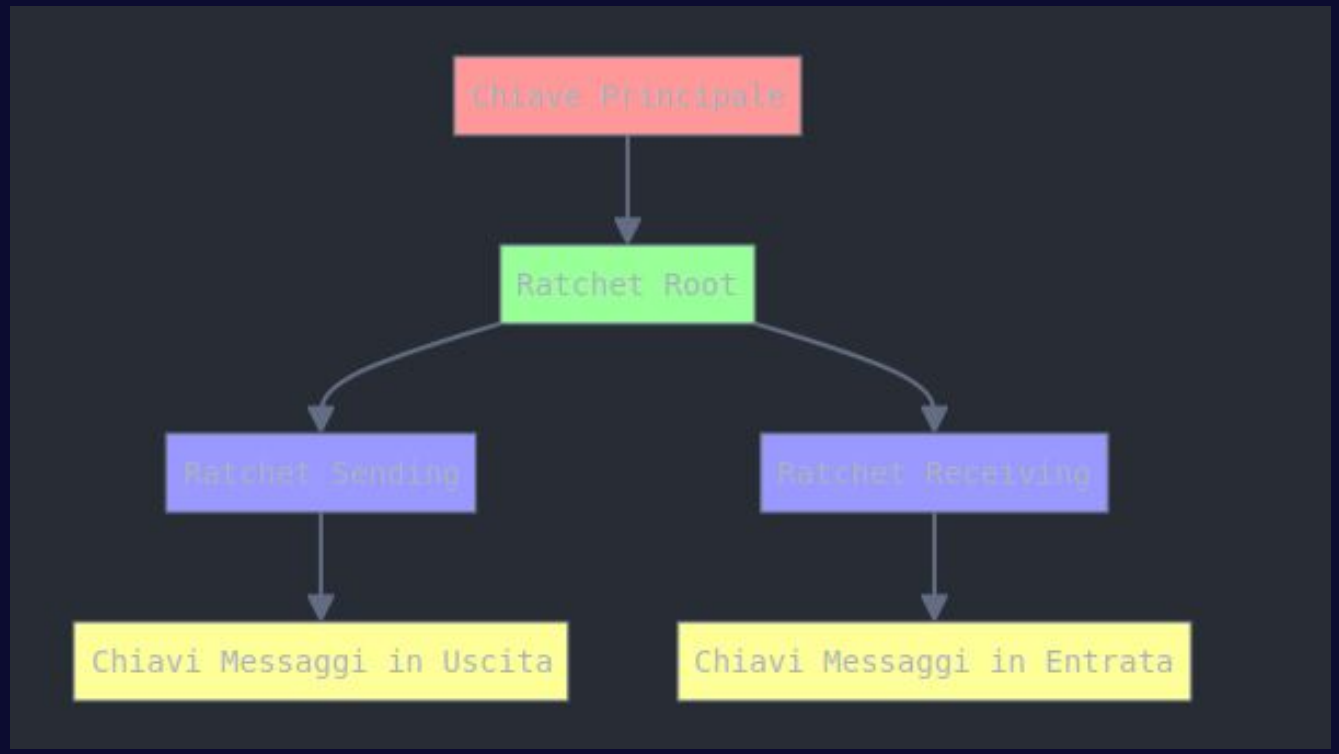
Fondamenti della Crittografia Moderna

Signal Protocol: Analisi Approfondita

- **Ratchet di Doppio** per Perfect Forward Secrecy
- **Problemi di Metadata** nonostante la cifratura E2E
- **Centralizzazione** del server Signal

Double Ratchet - Concetto Base

- È un protocollo che combina due "ratchet" (cricchetti):
  1. Ratchet Diffie-Hellman (DH)
  2. Ratchet di Catena di Chiavi



Processo di Profilazione:

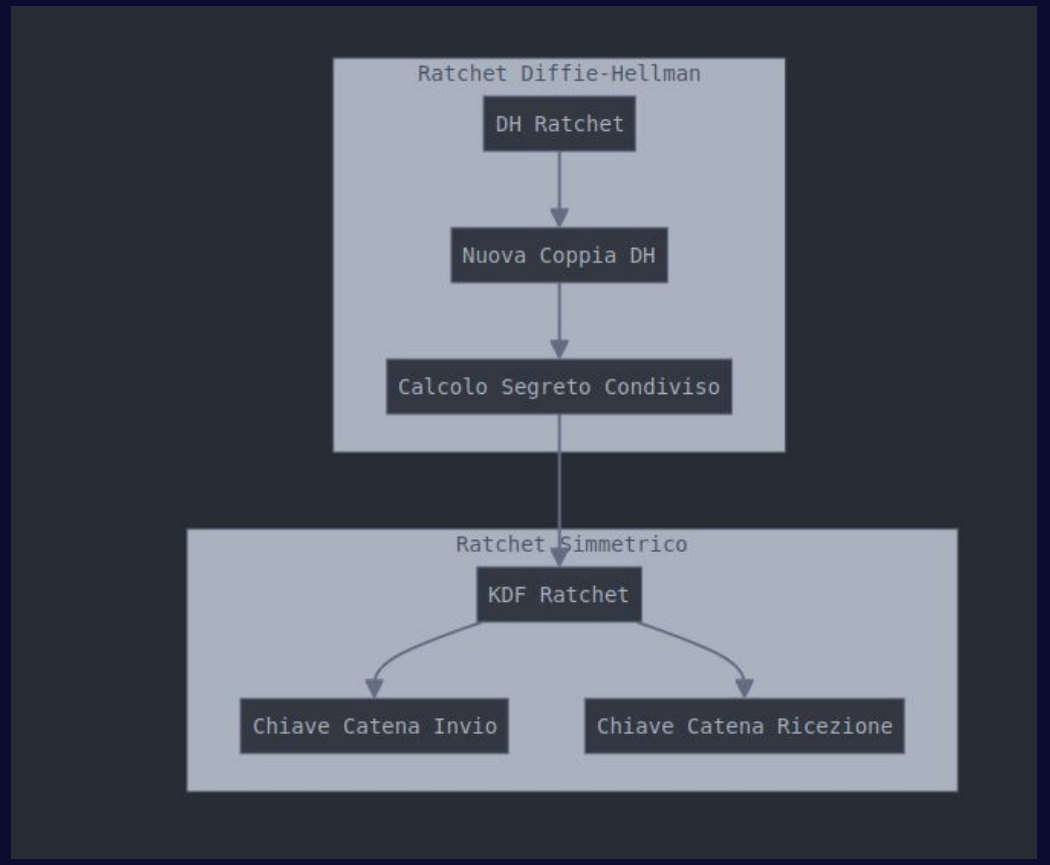
Fondamenti della Crittografia Moderna

Signal Protocol: Analisi Approfondita

- **Ratchet di Doppio** per Perfect Forward Secrecy
- **Problemi di Metadata** nonostante la cifratura E2E
- **Centralizzazione** del server Signal

Come Funziona

- **Ratchet DH**:
  - Genera nuove coppie di chiavi DH periodicamente
  - Calcola nuovi segreti condivisi
  - Fornisce proprietà di sicurezza come la "post-compromise security"
- **Ratchet di Catena di Chiavi**:
  - Deriva nuove chiavi per ogni messaggio
  - Utilizza funzioni KDF (Key Derivation Function)
  - Mantiene catene separate per invio e ricezione



Processo di Profilazione:

Fondamenti della Crittografia Moderna

Signal Protocol: Analisi Approfondita

- **Ratchet di Doppio** per Perfect Forward Secrecy
- **Problemi di Metadata** nonostante la cifratura E2E
- **Centralizzazione** del server Signal

Perfect Forward Secrecy (PFS)

- **Definizione**: Garantisce che la compromissione di una chiave non comprometta i messaggi passati
- **Implementazione**:
  - Chiavi di sessione temporanee
  - Eliminazione immediata delle chiavi usate
  - Rotazione continua delle chiavi
  -

Processo di Profilazione:

Fondamenti della Crittografia Moderna

Signal Protocol: Analisi Approfondita

- **Ratchet di Doppio** per Perfect Forward Secrecy
- **Problemi di Metadata** nonostante la cifratura E2E
- **Centralizzazione** del server Signal

Perfect Forward Secrecy (PFS)

- **Definizione**: Garantisce che la compromissione di una chiave non comprometta i messaggi passati
- **Implementazione**:
  - Chiavi di sessione temporanee
  - Eliminazione immediata delle chiavi usate
  - Rotazione continua delle chiavi
  -

Processo di Profilazione:

Fondamenti della Crittografia Moderna

Signal Protocol: Analisi Approfondita

- **Ratchet di Doppio** per Perfect Forward Secrecy
- **Problemi di Metaata** nonostante la cifratura E2E
- **Centralizzazione** del server Signal

1. **Vantaggi Chiave**
   - Compromissione limitata: Se una chiave viene compromessa, solo i messaggi futuri sono a rischio
   - Auto-guarigione: Il sistema si ripristina automaticamente dopo una compromissione
   - Gestione automatica delle chiavi: Non richiede intervento manuale
2. **Proprietà di Sicurezza**
   - **Forward Secrecy**: Protezione messaggi passati
   - **Future Secrecy**: Ripristino dopo compromissione
   - **Break-in Recovery**: Capacità di recupero dopo attacchi
   - **Post-compromise Security**: Protezione dopo compromissione temporanea
3. **Implementazione nel Signal Protocol**
   - Integrazione con X3DH per setup iniziale
   - Gestione automatica delle rotazioni chiave
   - Supporto per messaggi fuori ordine
   - Gestione efficiente della memoria

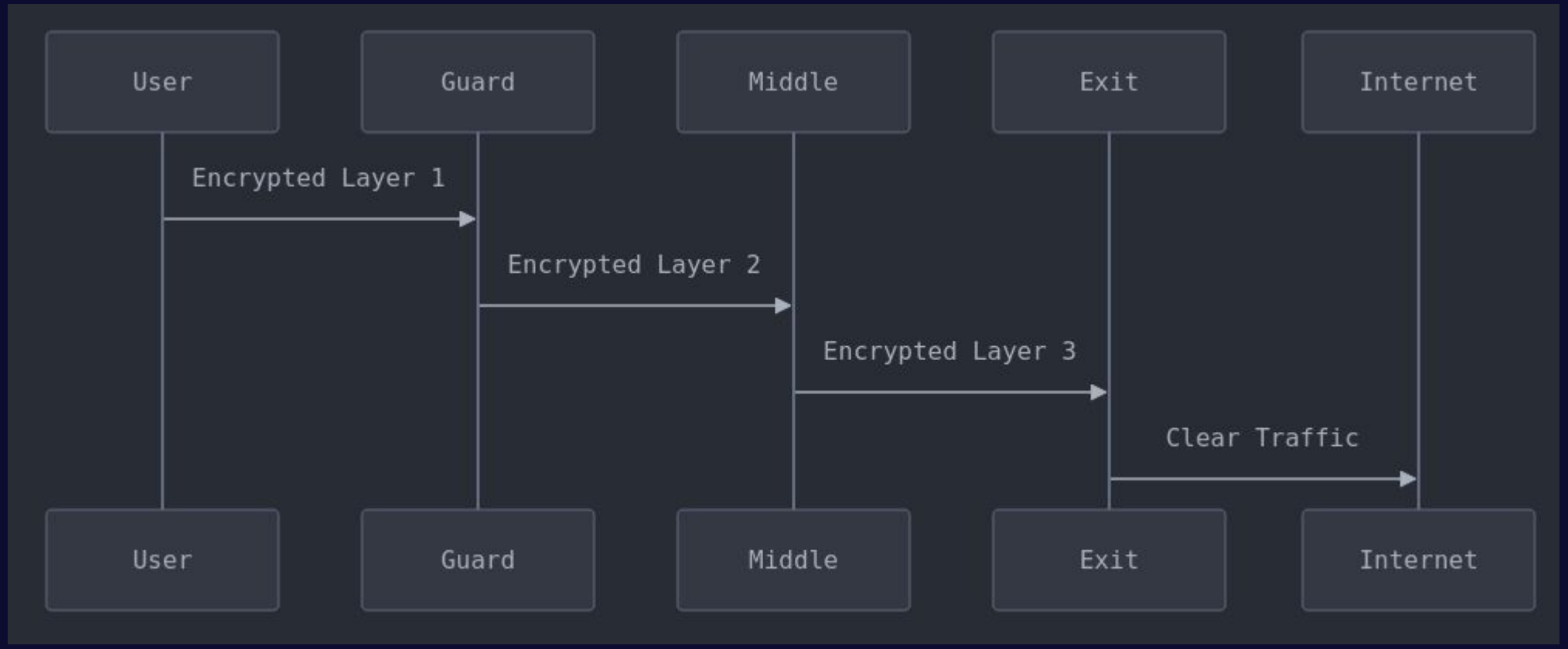
Il Double Ratchet è fondamentale per la sicurezza moderna delle comunicazioni perché:

1. Fornisce protezione automatica e continua
2. Non richiede intervento utente
3. Si adatta a scenari di comunicazione reali
4. Offre garanzie di sicurezza molto forti

Processo di Profilazione:

Tecnologie Decentralizzate

Architettura Tor



Processo di Profilazione:

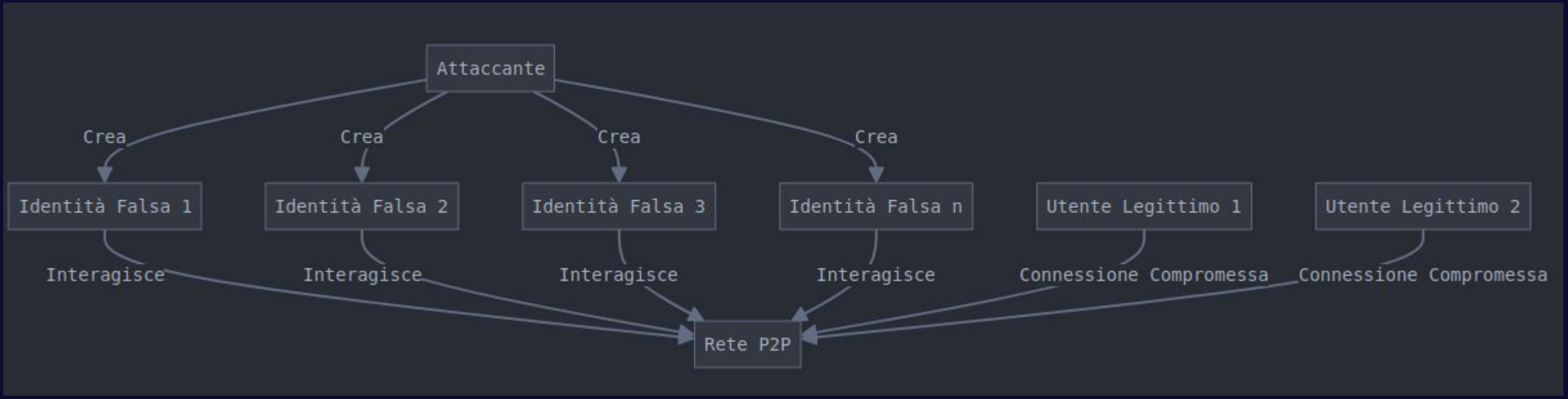
Tecnologie Decentralizzate

Architettura Tor

Meccanismo Base dell'Attacco Sybil

Vulnerabilità Note:

- Attacchi di correlazione temporale
- Nodi di uscita malevoli
- Attacchi Sybil



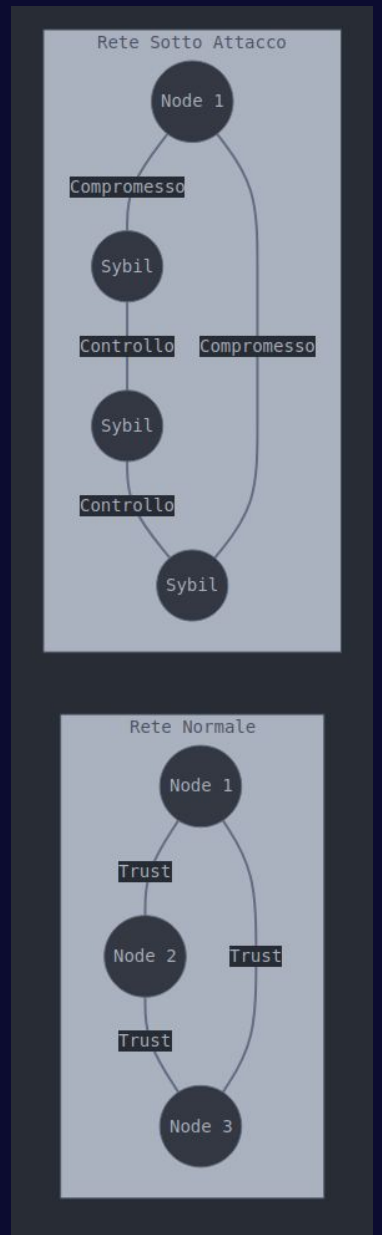
Processo di Profilazione:

Tecnologie Decentralizzate

Architettura Tor

Vulnerabilità Note:

- Attacchi di correlazione temporale
- Nodi di uscita malevoli
- Attacchi Sybil



Impatto sulla Rete:

Processo di Profilazione:

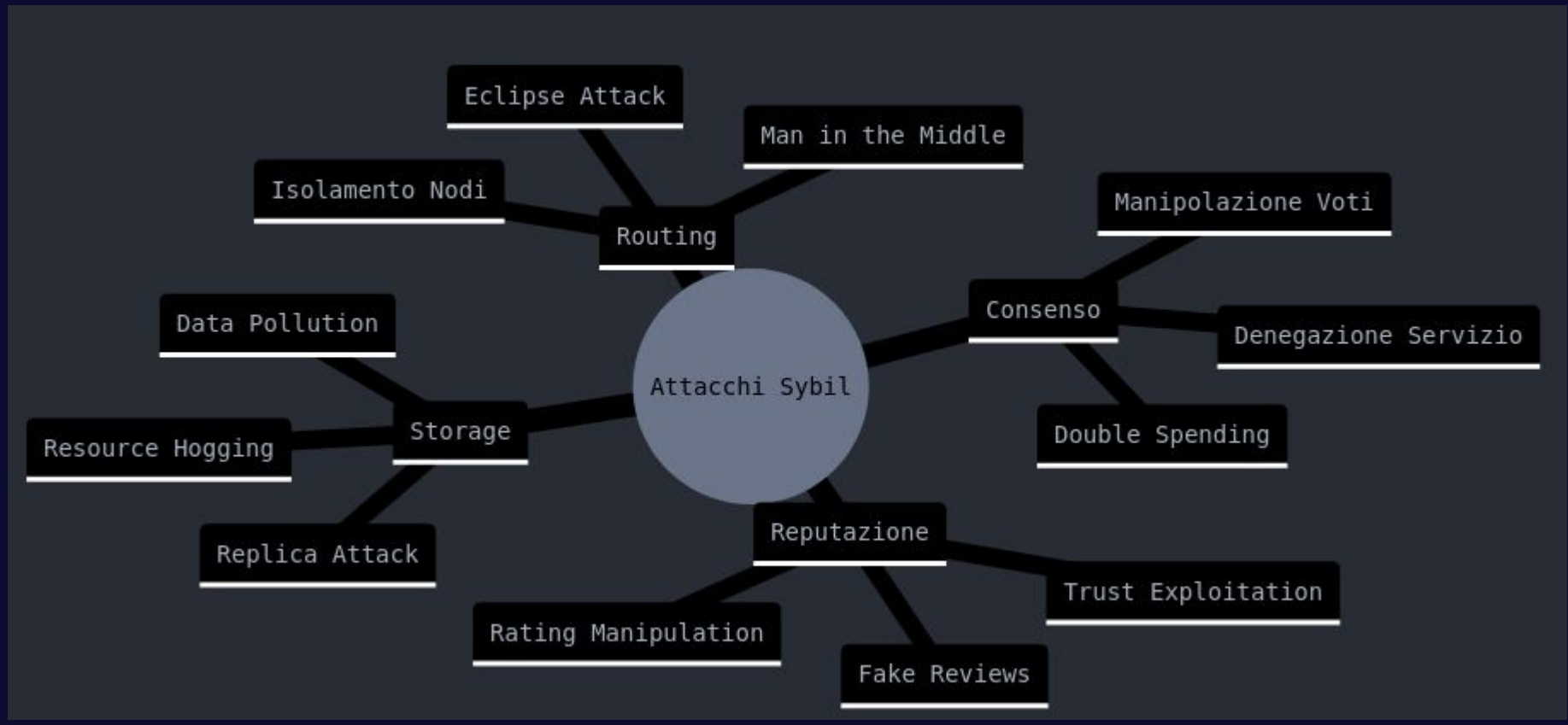
Tecnologie Decentralizzate

Architettura Tor

Vulnerabilità Note:

- Attacchi di correlazione temporale
- Nodi di uscita malevoli
- Attacchi Sybil

Vettori di Attacco:



Processo di Profilazione:

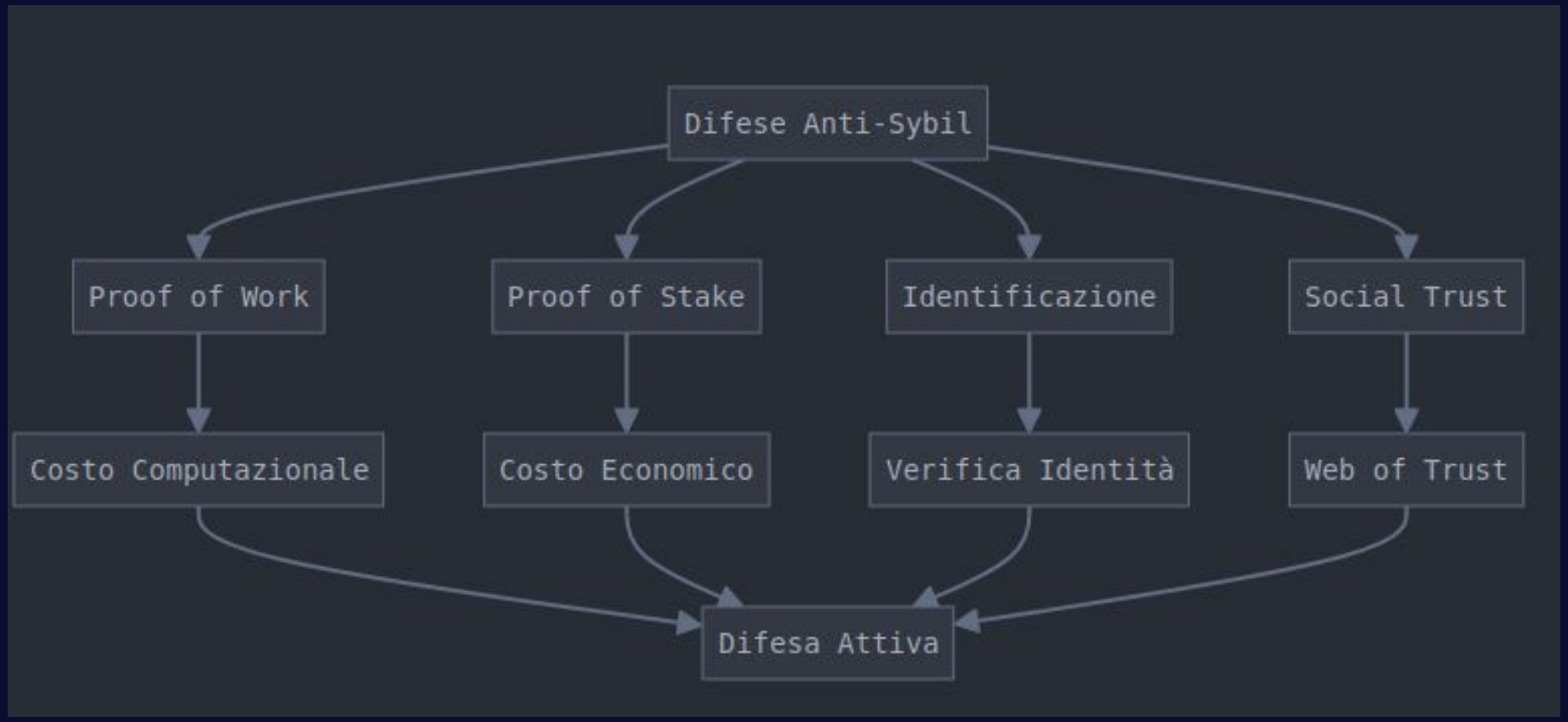
Tecnologie Decentralizzate

Architettura Tor

Vulnerabilità Note:

- Attacchi di correlazione temporale
- Nodi di uscita malevoli
- Attacchi Sybil

Contromisure di Difesa:



Processo di Profilazione:

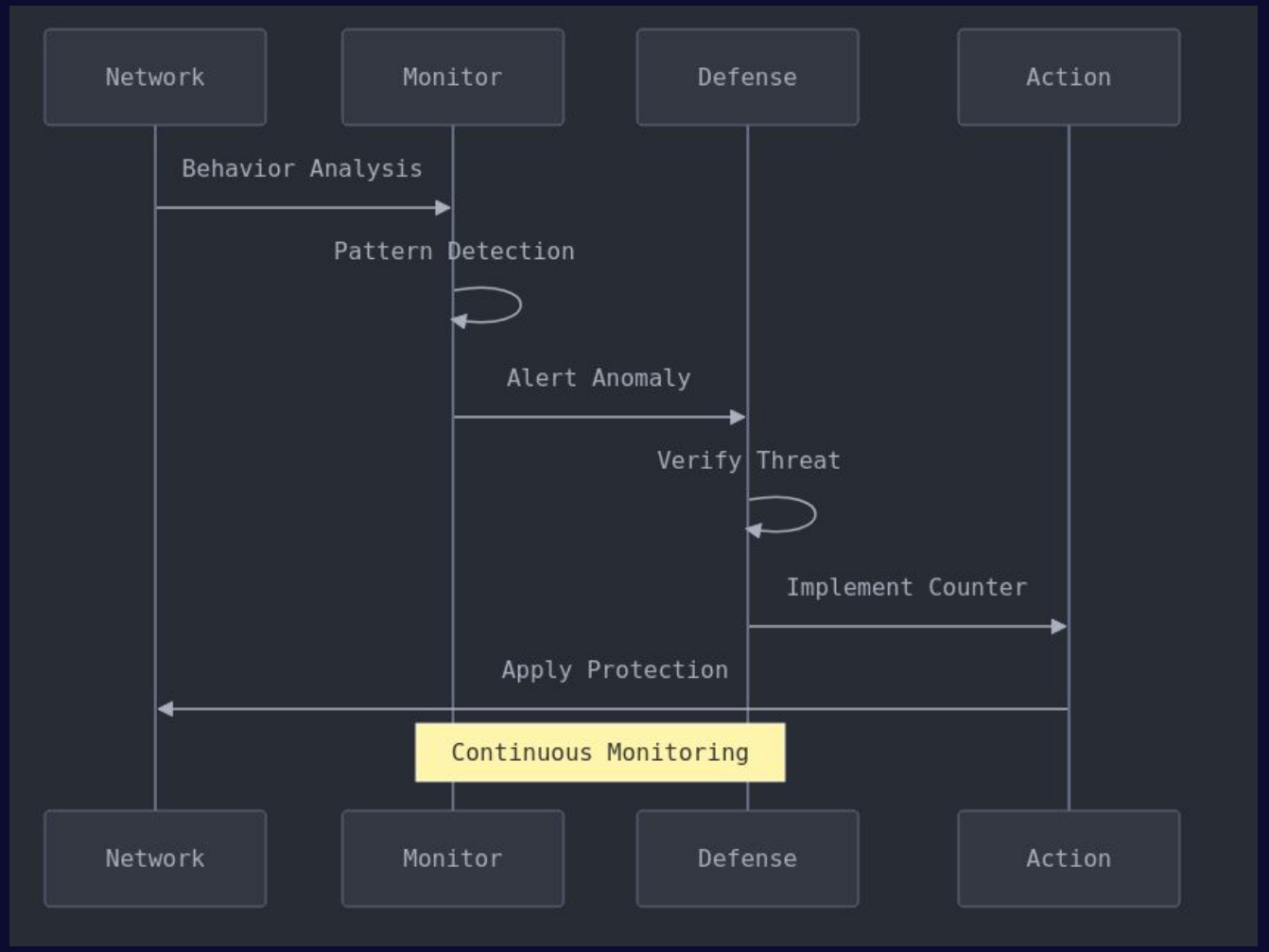
Tecnologie Decentralizzate

Architettura Tor

Vulnerabilità Note:

- Attacchi di correlazione temporale
- Nodi di uscita malevoli
- Attacchi Sybil

Processo di Rilevamento:



Processo di Profilazione:

Tecnologie Decentralizzate

1. **Cosa sono gli Attacchi Sybil**
- Definizione: Un attacco Sybil avviene quando un singolo malintenzionato crea multiple identità false per acquisire influenza sproporzionata in una rete decentralizzata
- Origine: Il nome viene dal caso clinico "Sybil" (1973), che trattava di un disturbo di personalità multipla
2. **Come Funzionano**
- Creazione di multiple identità false
- Infiltrazione nella rete P2P
- Manipolazione del comportamento della rete
- Controllo di una porzione significativa dei nodi
3. **Impatti Principali**
- Manipolazione del consenso
- Controllo del routing
- Alterazione dei sistemi di reputazione
- Denial of Service distribuito
- Double spending in cryptocurrencies

4. **Contromisure Comuni**
- **Proof of Work (PoW)**:
  - Richiede risorse computazionali
  - Rende costosa la creazione di identità multiple
- **Proof of Stake (PoS)**:
  - Richiede investimento economico
  - Lega l'influenza al capitale investito
- **Identificazione**:
  - Verifica dell'identità
  - KYC (Know Your Customer)
  - Certificati digitali
- **Social Trust**:
  - Web of Trust
  - Reputation systems
  - Social graph analysis
5. **Best Practices di Prevenzione**
- Implementazione di sistemi di identificazione robusti
- Monitoraggio continuo del comportamento della rete
- Utilizzo di algoritmi di consenso resistenti agli attacchi Sybil
- Implementazione di sistemi di reputazione distribuiti

Processo di Profilazione:

Blockchain e Privacy: Miti e Realtà

Monero:

- Ring signatures e stealth addresses
- Scalabilità vs Privacy
- Problemi di adoption

ZCash:

- zk-SNARKs: potenzialità e limiti
- Trusted setup controverso
- Bassa percentuale di transazioni private

Struttura Base Blockchain:

Processo di Profilazione:

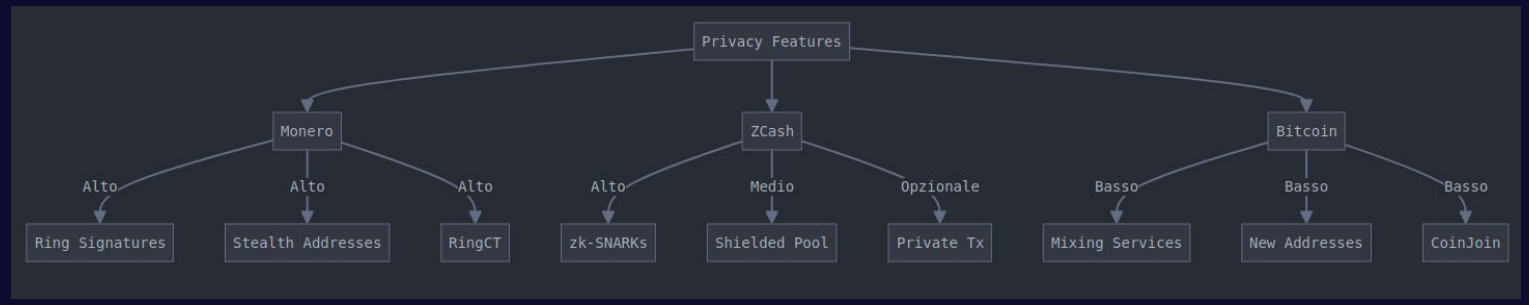
Blockchain e Privacy: Miti e Realtà

Monero:

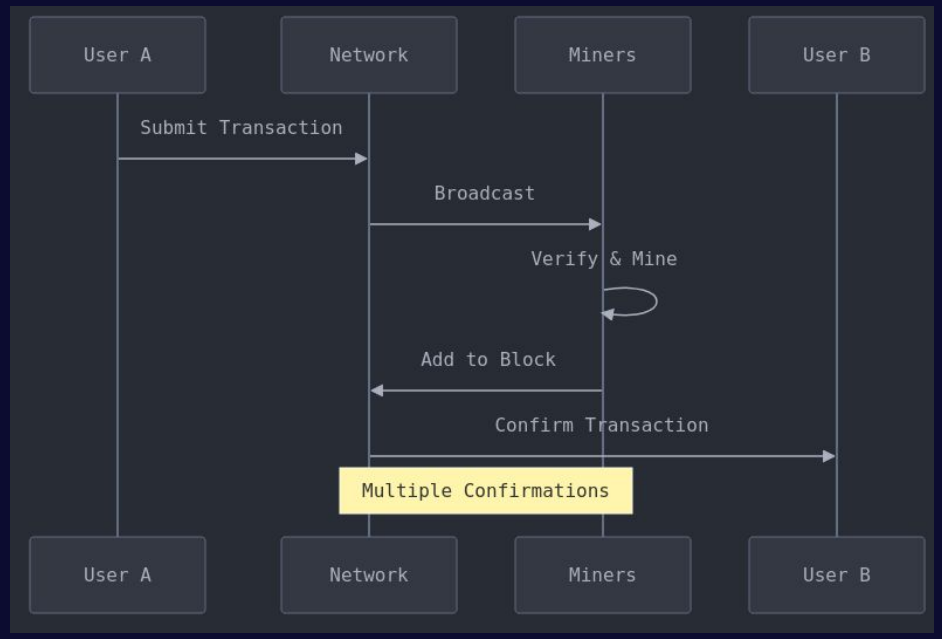
- Ring signatures e stealth addresses
- Scalabilità vs Privacy
- Problemi di adoption

ZCash:

- zk-SNARKs: potenzialità e limiti
- Trusted setup controverso
- Bassa percentuale di transazioni private



Privacy Features nelle Cryptocurrencies:



Processo di :Transazione

Processo di Profilazione:

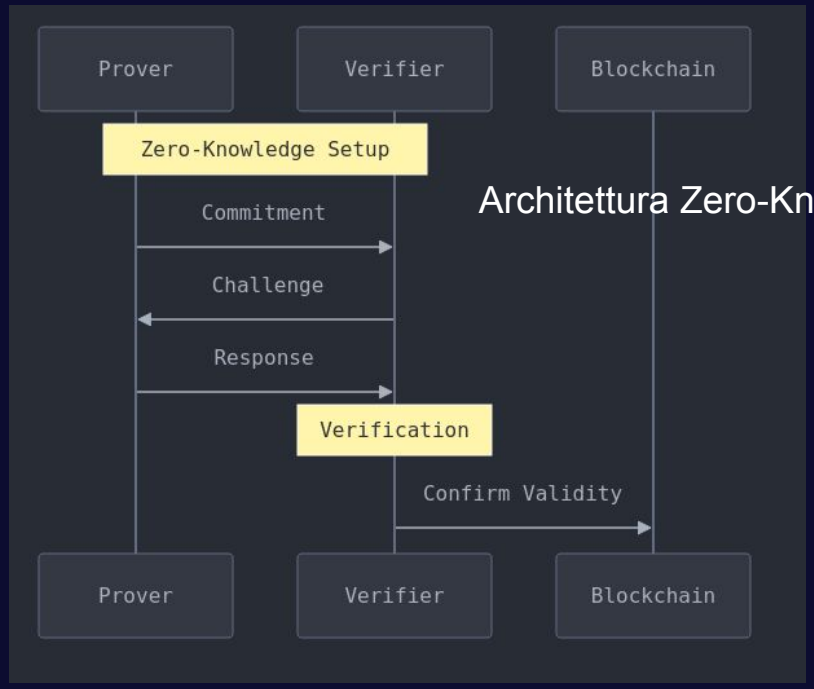
Blockchain e Privacy: Miti e Realtà

Monero:

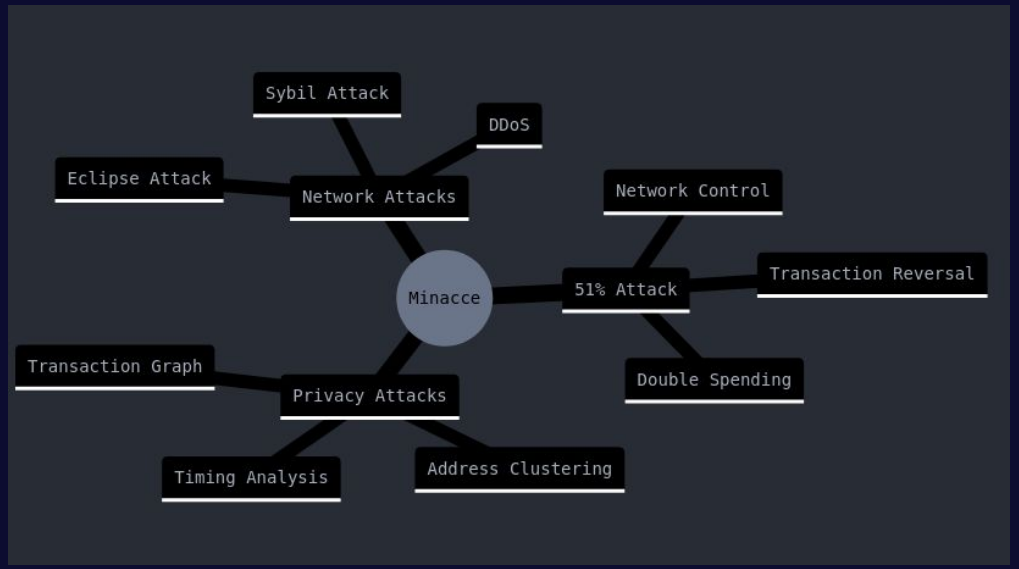
- Ring signatures e stealth addresses
- Scalabilità vs Privacy
- Problemi di adoption

ZCash:

- zk-SNARKs: potenzialità e limiti
- Trusted setup controverso
- Bassa percentuale di transazioni private



Architettura Zero-Knowledge Proof:



Attacchi e Vulnerabilità:

Processo di Profilazione:

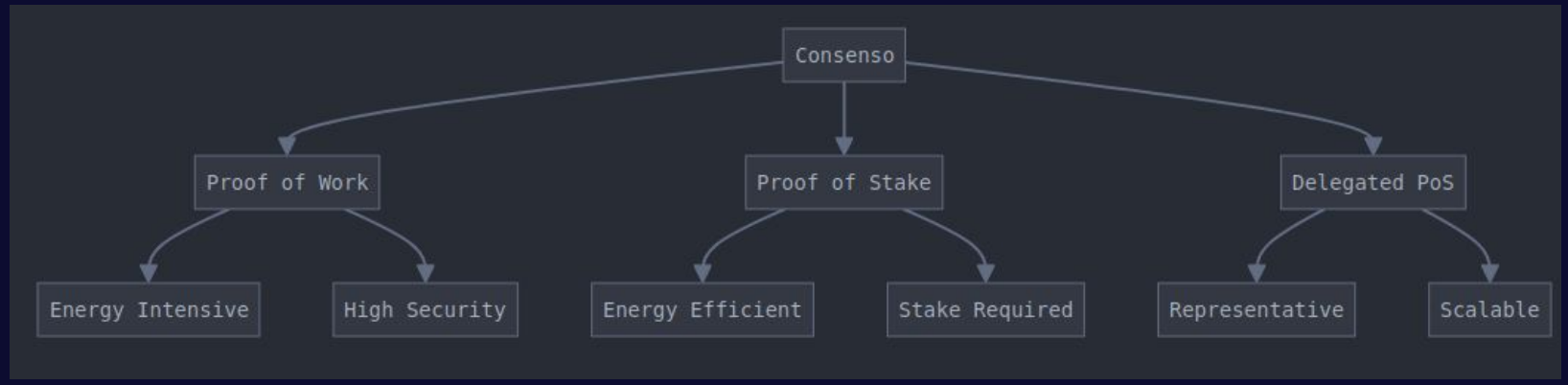
Blockchain e Privacy: Miti e Realtà

Monero:

- Ring signatures e stealth addresses
- Scalabilità vs Privacy
- Problemi di adoption

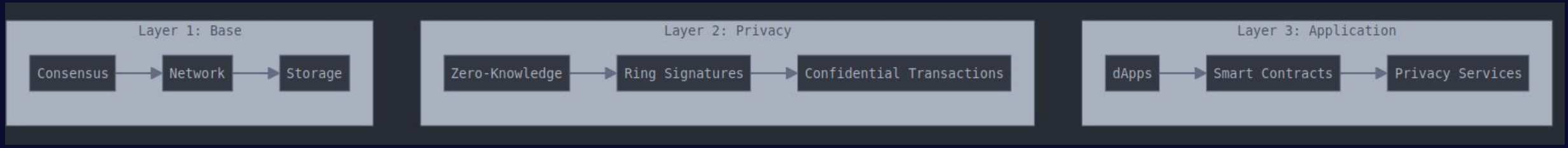
ZCash:

- zk-SNARKs: potenzialità e limiti
- Trusted setup controverso
- Bassa percentuale di transazioni private



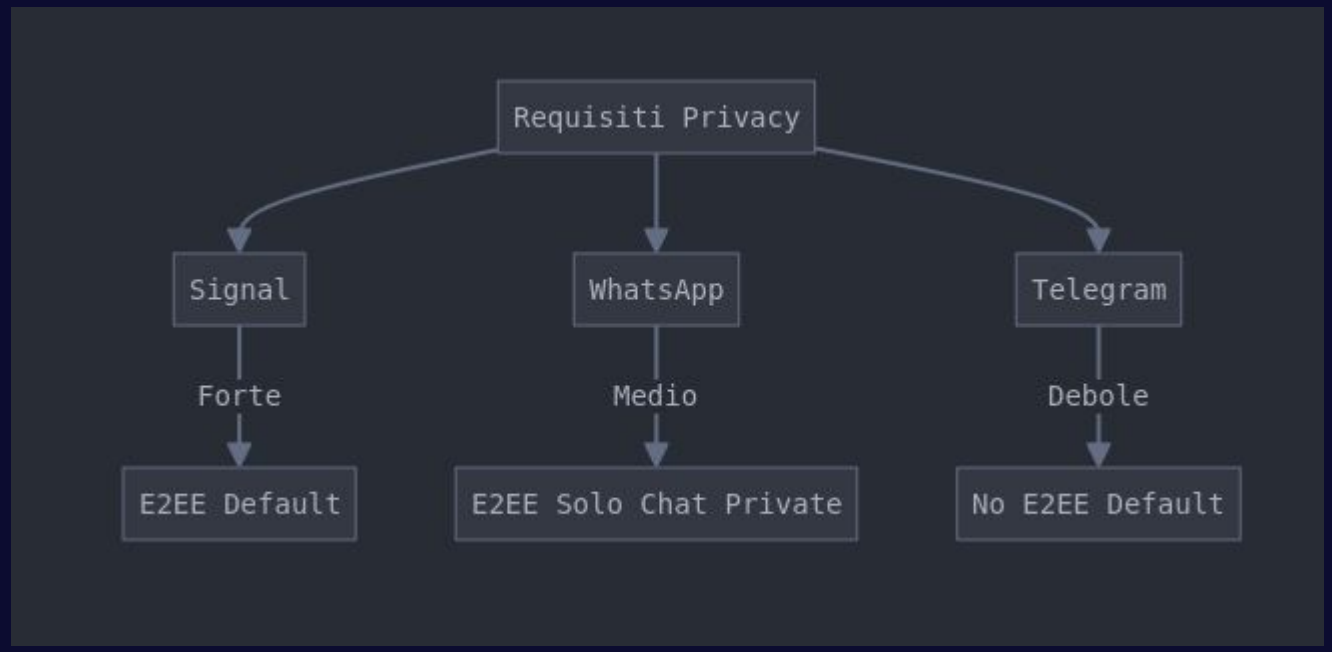
Consenso e Validazione:

Privacy Stack Completo:



Processo di Profilazione:

Comunicazione Sicura Analisi Comparativa delle Soluzioni



Messaggistica Sicura:

Processo di Profilazione:

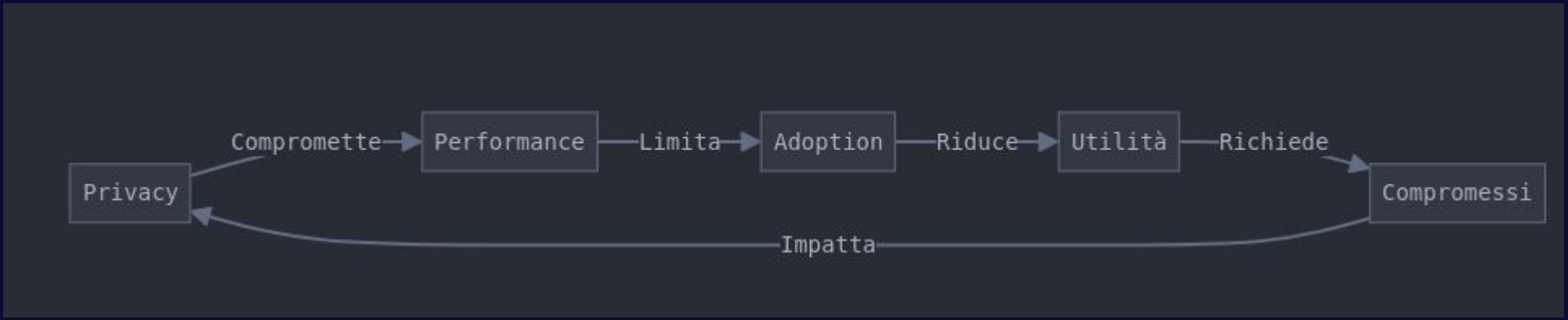
Comunicazione Sicura Analisi Comparativa delle Soluzioni

Problematiche:

- **Signal:**
  - Numero di telefono richiesto
  - Centralizzazione
  - Metadati esposti
- **Matrix:**
  - Complessità di deployment
  - Frammentazione dell'ecosistema
  - Problemi di scalabilità

Processo di Profilazione:

Sfide e Limitazioni Analisi Tecnica delle Barriere



Criticità:

- Overhead computazionale delle soluzioni privacy-preserving
- Latenza nelle reti anonime
- Complessità di UX nelle soluzioni sicure

Scalabilità vs Privacy

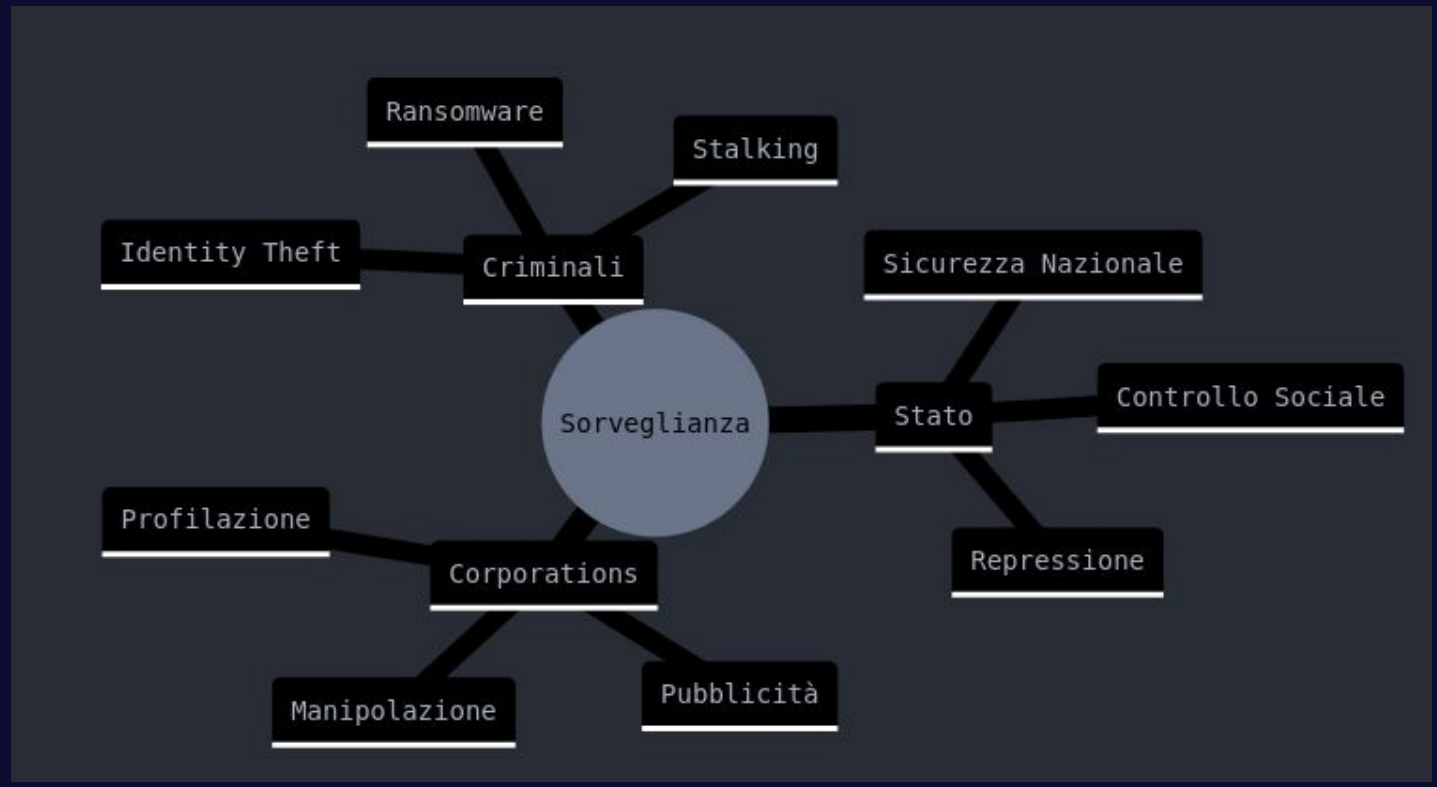
Processo di Profilazione:

Considerazioni Etiche

Sorveglianza di Massa

Impatti Sociali

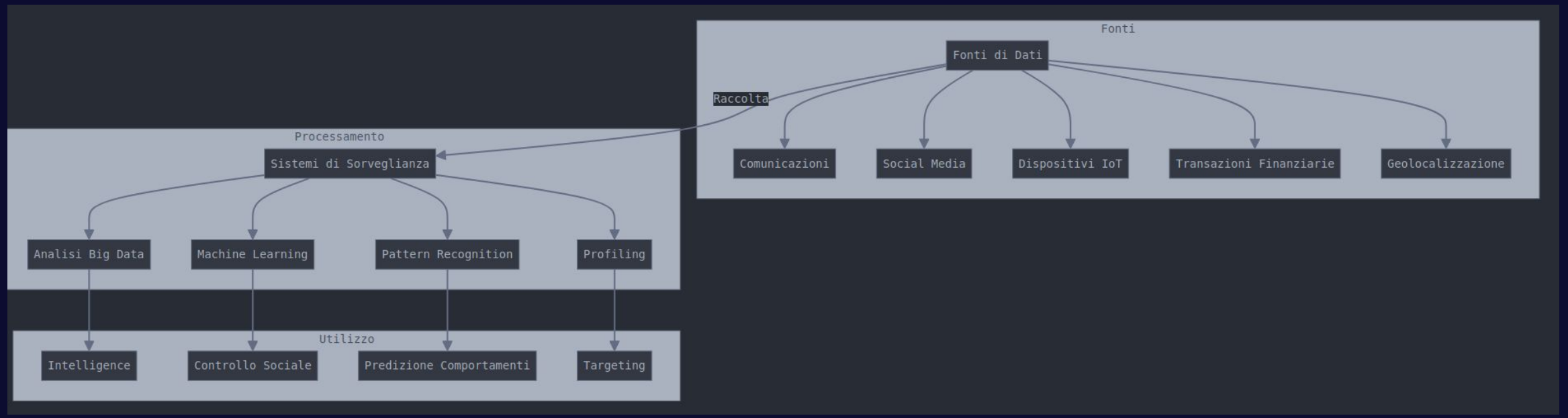
- **Caso Studio: Silk Road**
  - Privacy come strumento di libertà vs criminalità
  - Bilanciamento tra anonimato e responsabilità
  - Ruolo della regolamentazione



Processo di Profilazione:

Considerazioni Etiche

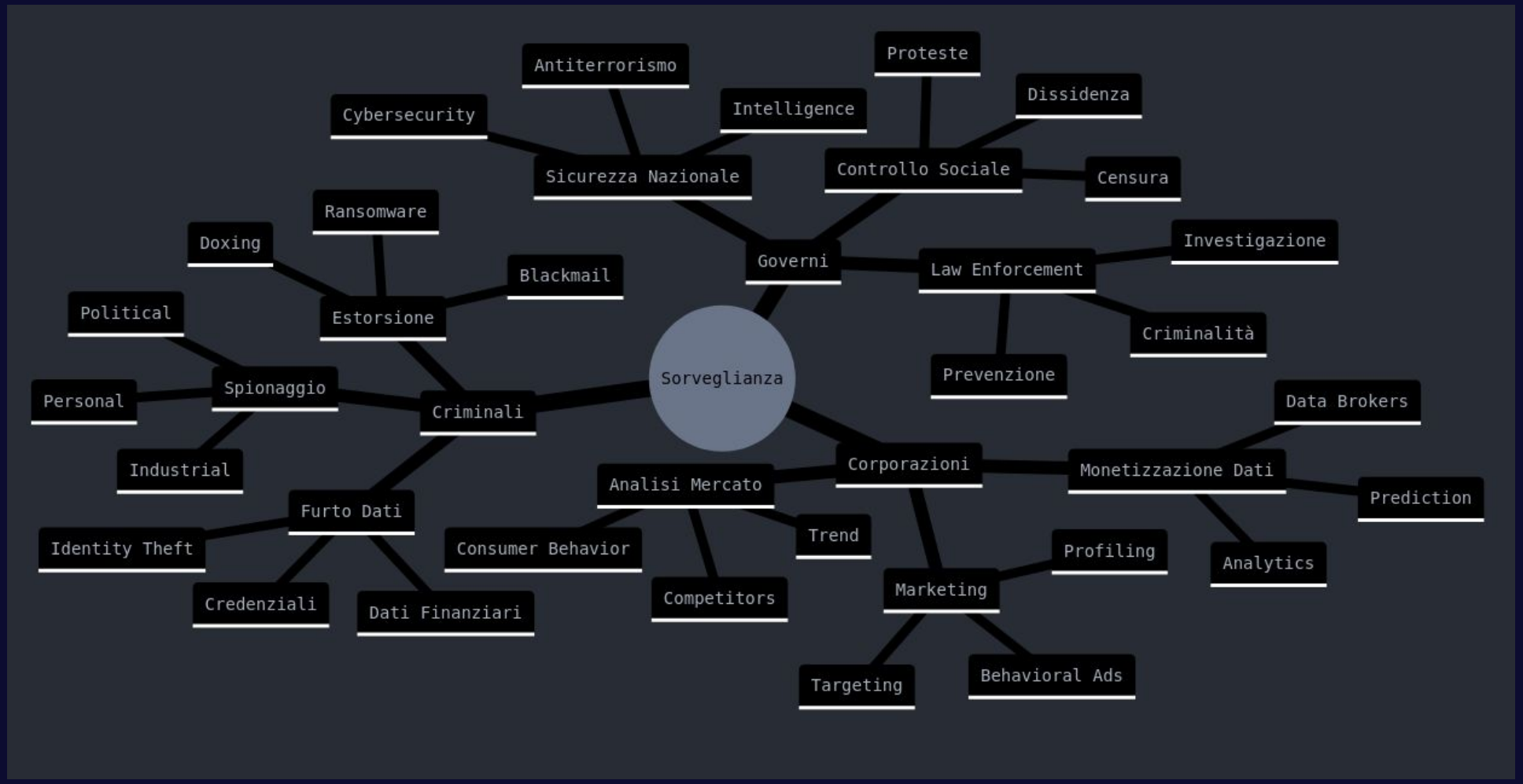
Sorveglianza di Massa



Processo di Profilazione:

Considerazioni Etiche

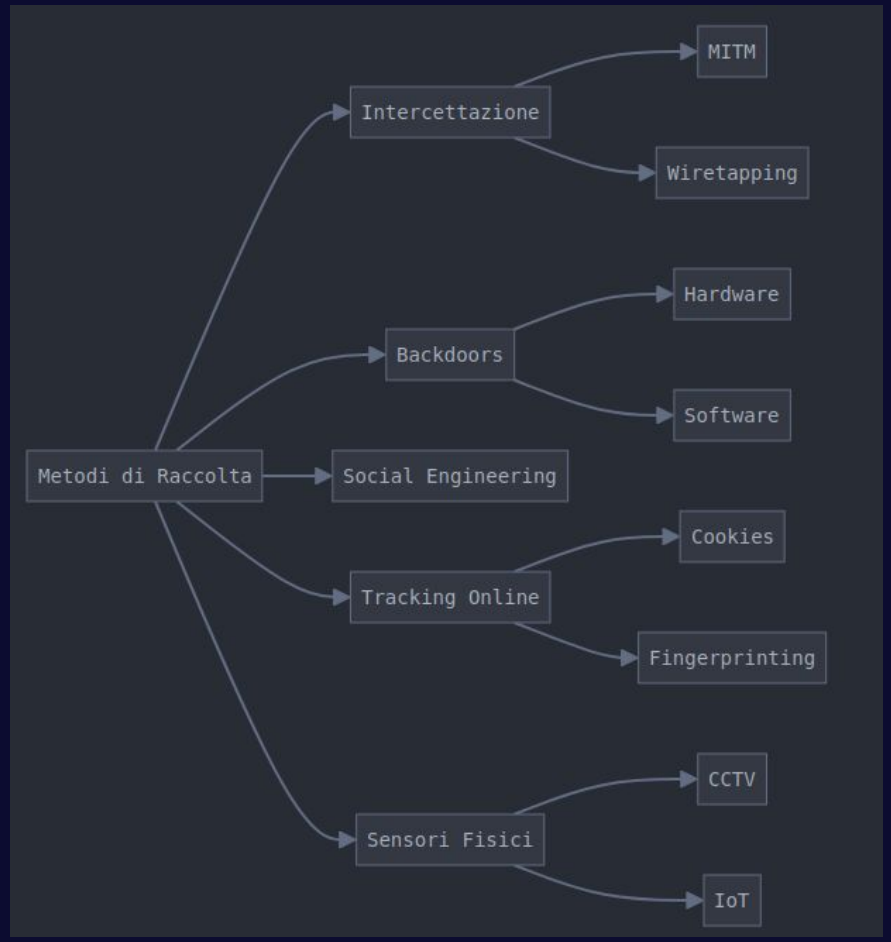
Gli attori



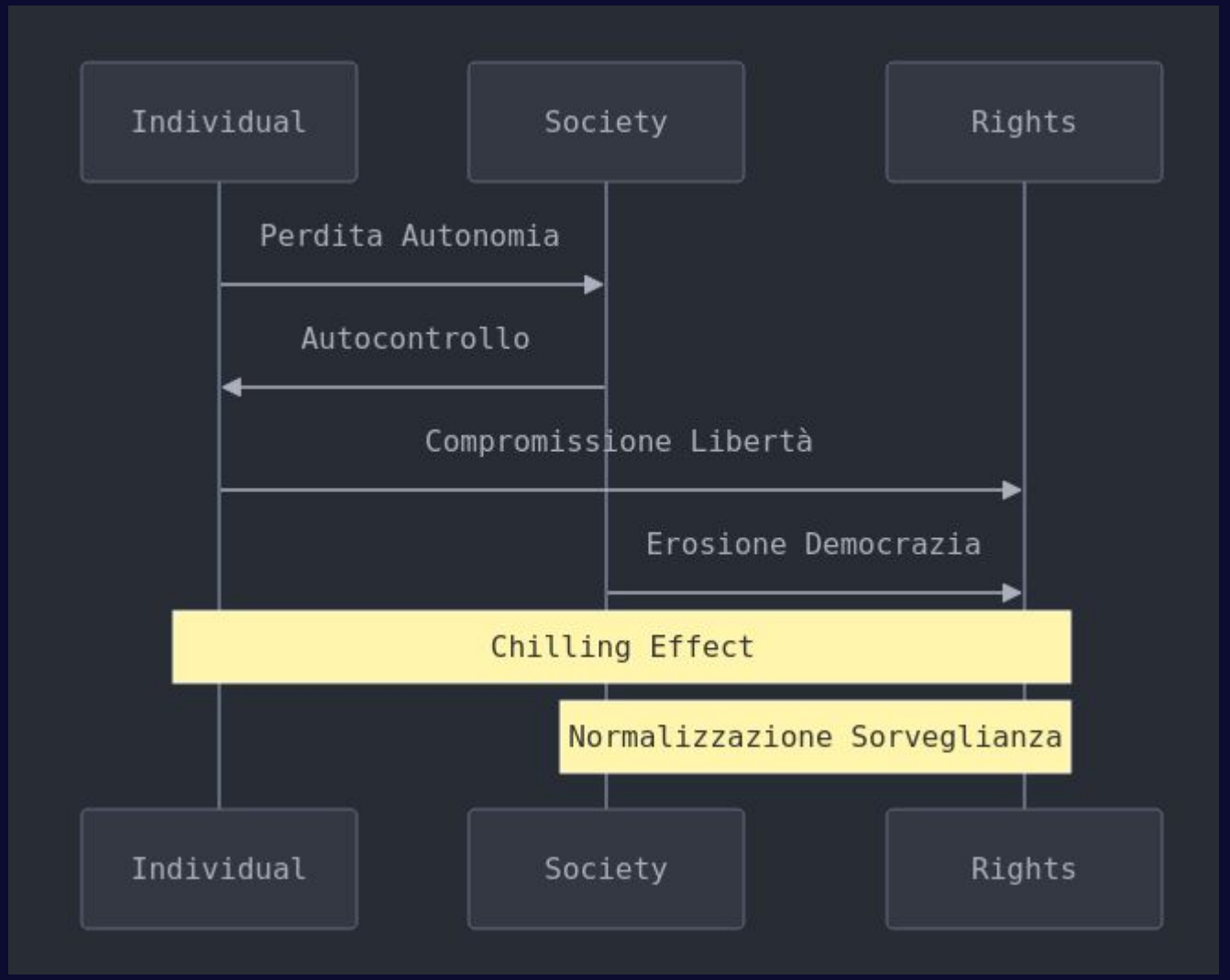
Processo di Profilazione:

Considerazioni Etiche

Tecniche di raccolta



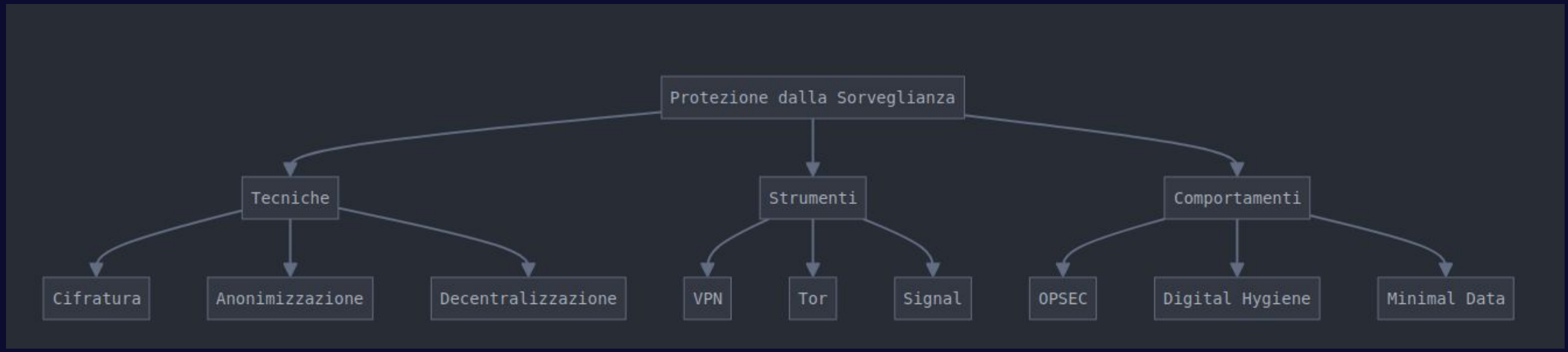
Impatti sulla privacy



Processo di Profilazione:

Considerazioni Etiche

Contromisure e Protezioni:



Processo di Profilazione:

Considerazioni Etiche

1. **Tipologie di Sorveglianza**
   - **Upstream**: Intercettazione diretta delle comunicazioni
   - **PRISM-like**: Accesso ai dati attraverso provider
   - **Passive**: Raccolta senza interazione
   - **Active**: Targeting specifico
2. **Meccanismi di Raccolta**
   - **Bulk Collection**: Raccolta massiva indiscriminata
   - **Targeted**: Sorveglianza mirata
   - **Metadata**: Dati sui dati
   - **Content**: Contenuto delle comunicazioni

Impatti Sociali

- **Chilling Effect**: Autocensura
- **Conformità Sociale**: Comportamento normativo
- **Erosione Privacy**: Perdita graduale
- **Discriminazione**: Profilazione e targeting

Framework Legali

- Leggi antiterrorismo
- Mandati di sorveglianza
- Accordi internazionali
- Data retention laws

Conseguenze

- Perdita di libertà civili
- Compromissione della democrazia
- Controllo sociale aumentato
- Vulnerabilità a abusi

Resistenza e Protezione

- **Tecnologica**:
  - Crittografia end-to-end
  - Reti anonime
  - Decentralizzazione
- **Sociale**:
  - Attivismo
  - Educazione
  - Policy making
- **Legale**:
  - Riforme legislative
  - Cause strategiche
  - Advocacy

Tendenze Future

- Intelligenza Artificiale nella sorveglianza
- Biometria e riconoscimento
- Internet of Things
- Quantum computing implications

La sorveglianza di massa è un problema complesso che richiede:

1. Consapevolezza delle tecniche utilizzate
2. Comprensione degli impatti
3. Implementazione di contromisure
4. Azione collettiva per il cambiamento

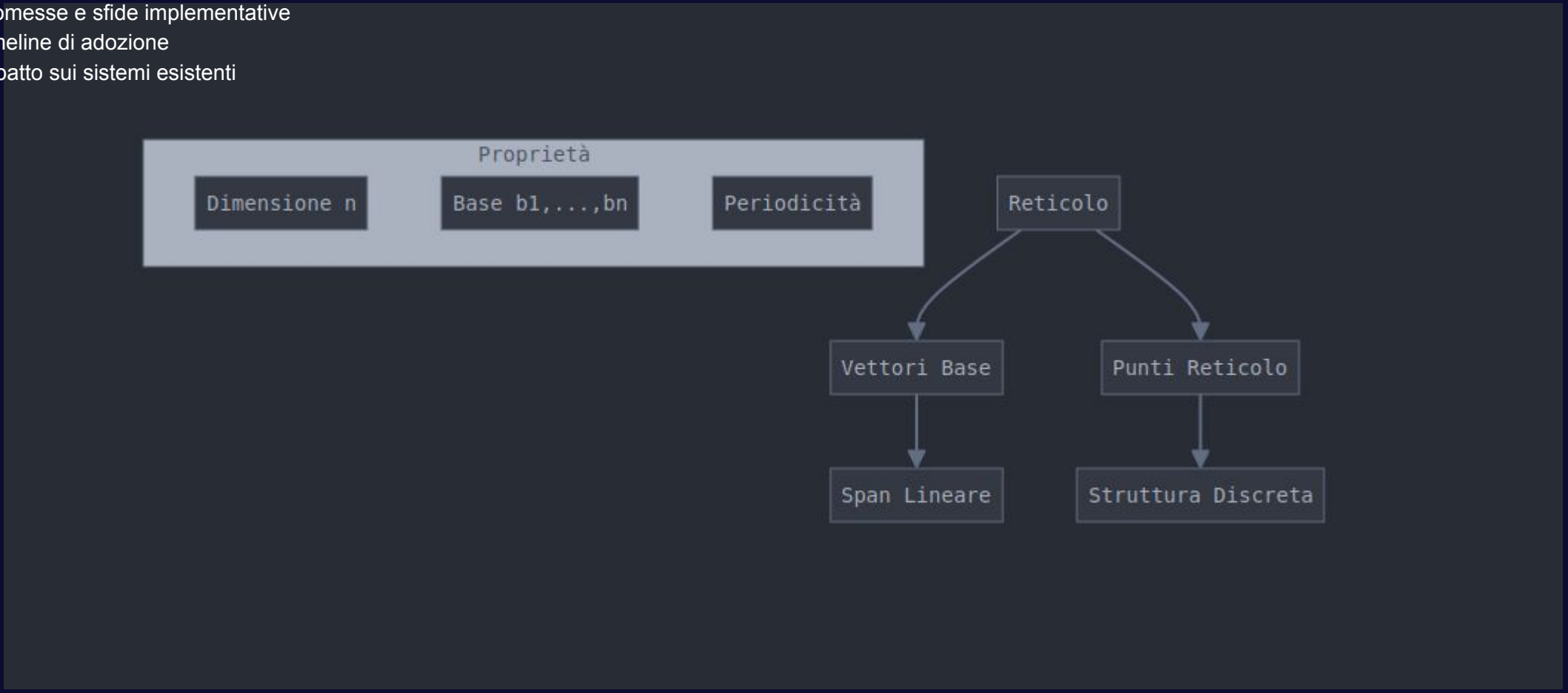
Processo di Profilazione:

Il Futuro delle Tecnologie Analisi delle Tendenze Emergenti

Post-Quantum Cryptography

- **Lattice-based cryptography**
  - Promesse e sfide implementative
  - Timeline di adozione
  - Impatto sui sistemi esistenti

Contromisure e Protezioni:



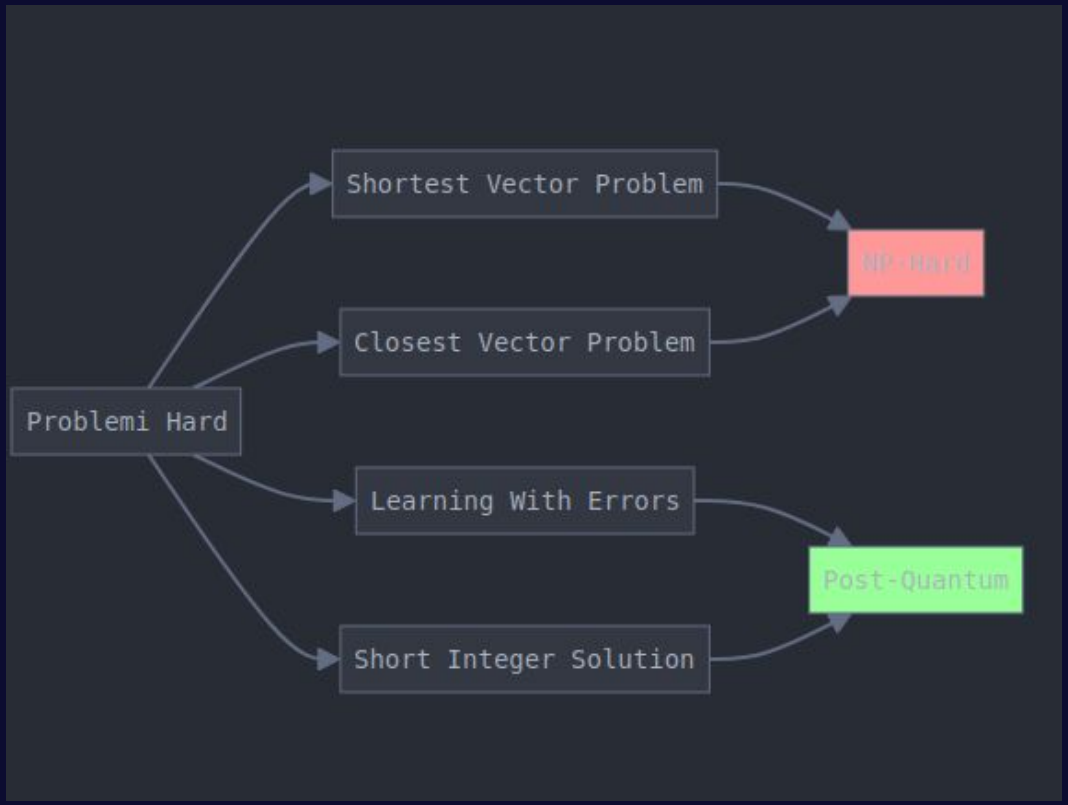
Processo di Profilazione:

Il Futuro delle Tecnologie Analisi delle Tendenze Emergenti

Post-Quantum Cryptography

- **Lattice-based cryptography**
  - Promesse e sfide implementative
  - Timeline di adozione
  - Impatto sui sistemi esistenti

Problemi Computazionali Hard:

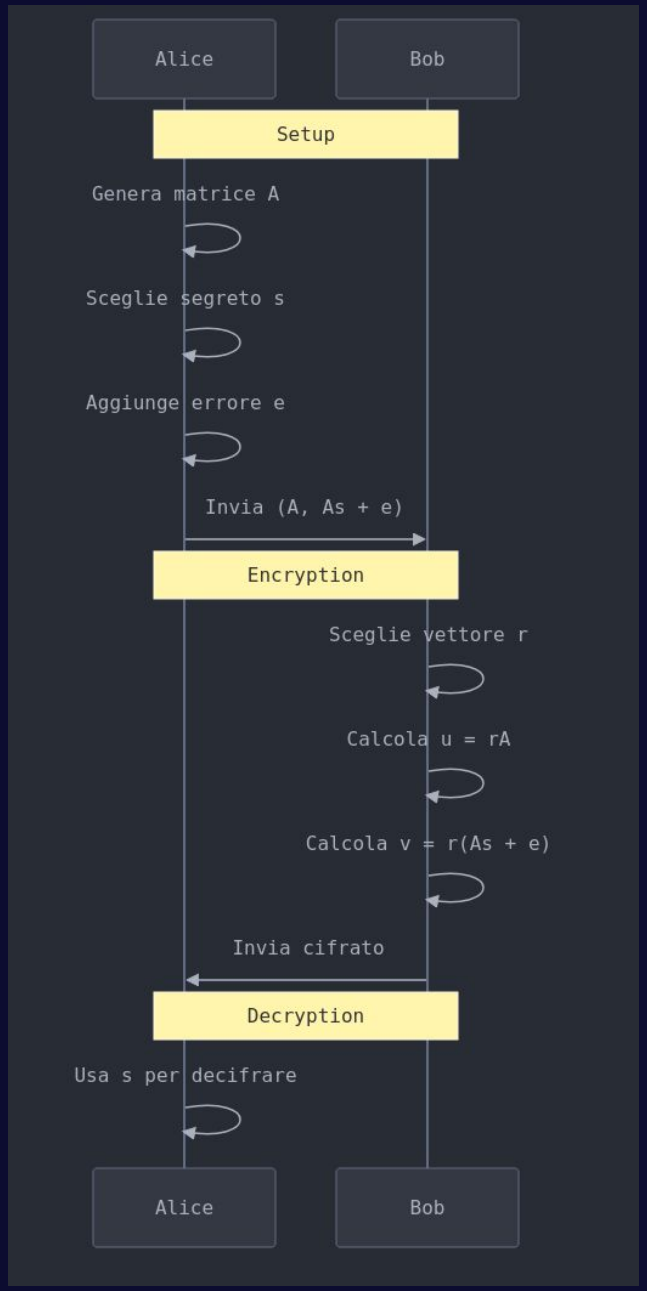


Processo di Profilazione:

Il Futuro delle Tecnologie Analisi delle Tendenze Emergenti

Post-Quantum Cryptography

- **Lattice-based cryptography**
  - Promesse e sfide implementative
  - Timeline di adozione
  - Impatto sui sistemi esistenti



Schema di Crittografia LWE (Learning With Errors):

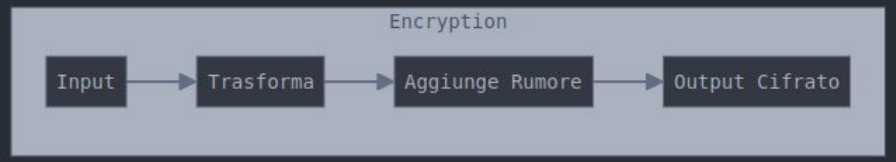
Processo di Profilazione:

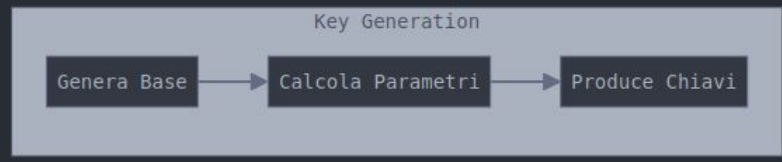
Il Futuro delle Tecnologie Analisi delle Tendenze Emergenti

Post-Quantum Cryptography

- **Lattice-based cryptography**
  - Promesse e sfide implementative
  - Timeline di adozione
  - Impatto sui sistemi esistenti

Componenti di un Sistema Lattice-based:





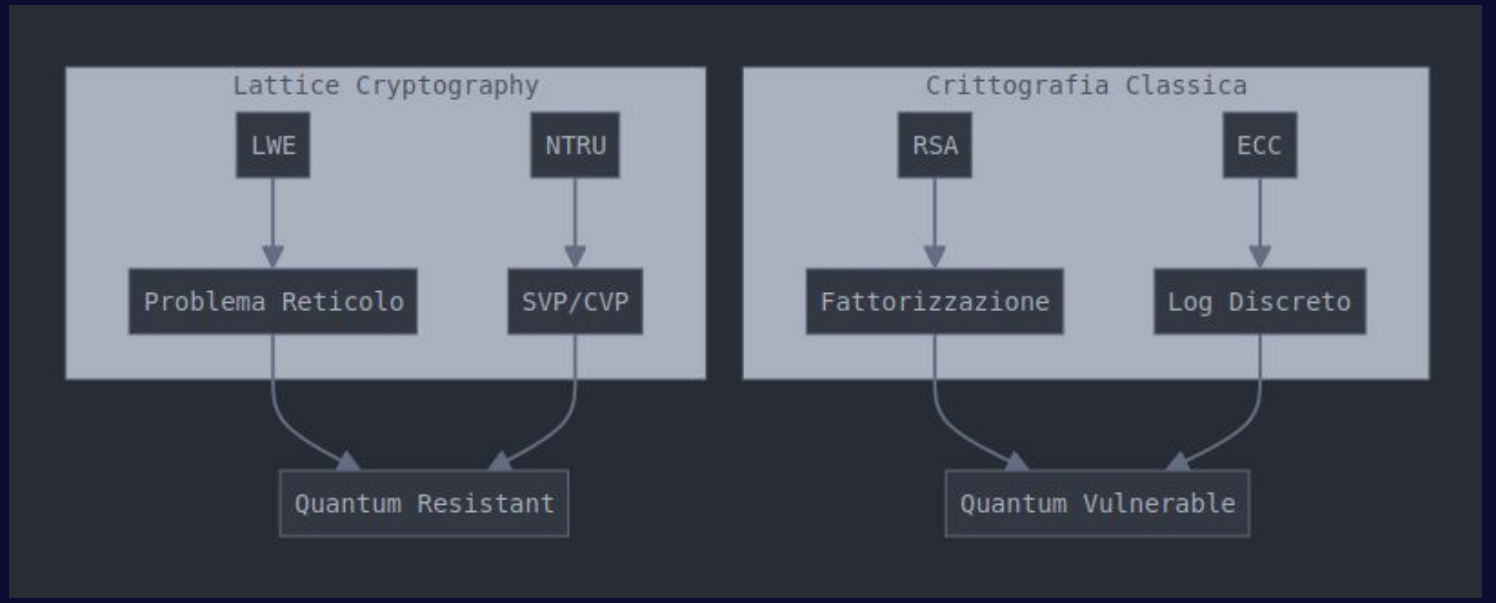
Processo di Profilazione:

Il Futuro delle Tecnologie Analisi delle Tendenze Emergenti

Post-Quantum Cryptography

- **Lattice-based cryptography**
  - Promesse e sfide implementative
  - Timeline di adozione
  - Impatto sui sistemi esistenti

Confronto con Crittografia Tradizionale:



Processo di Profilazione:

Il Futuro delle Tecnologie Analisi delle Tendenze Emergenti

Post-Quantum Cryptography

- **Lattice-based cryptography**
  - Promesse e sfide implementative
  - Timeline di adozione
  - Impatto sui sistemi esistenti

Concetti Fondamentali

- **Reticolo (Lattice)**:
  - Struttura matematica periodica in n dimensioni
  - Definito da vettori base lineari indipendenti
  - Proprietà di discretezza e periodicità

Problemi Computazionali

- **SVP (Shortest Vector Problem)**:
  - Trovare il vettore non nullo più corto nel reticolo
  - Computazionalmente difficile in alte dimensioni
- **LWE (Learning With Errors)**:
  - Problema di apprendimento con errori
  - Base per molti schemi crittografici
  - Resistente agli attacchi quantistici

Vantaggi Principali:

- Resistenza quantum
- Efficienza computazionale
- Flessibilità nelle applicazioni
- Sicurezza provabile

Applicazioni Pratiche:

- **Crittografia Asimmetrica**:
  - Cifratura di chiave pubblica
  - Firme digitali
  - Scambio di chiavi
- **Crittografia Omomorfa**:
  - Computazioni su dati cifrati
  - Privacy-preserving computing
  - Secure multiparty computation

Punti Chiave:

1. Base matematica solida
2. Resistenza quantum provata
3. Flessibilità applicativa
4. Standardizzazione in corso
5. Sfide implementative reali

Sfide Implementative:

- Dimensioni chiavi maggiori
- Complessità implementativa
- Overhead di comunicazione
- Ottimizzazione parametri

Standard e Implementazioni:

- NIST PQC competition
- Standardizzazione in corso
- Implementazioni di riferimento
- Ottimizzazioni hardware

Considerazioni di Sicurezza:

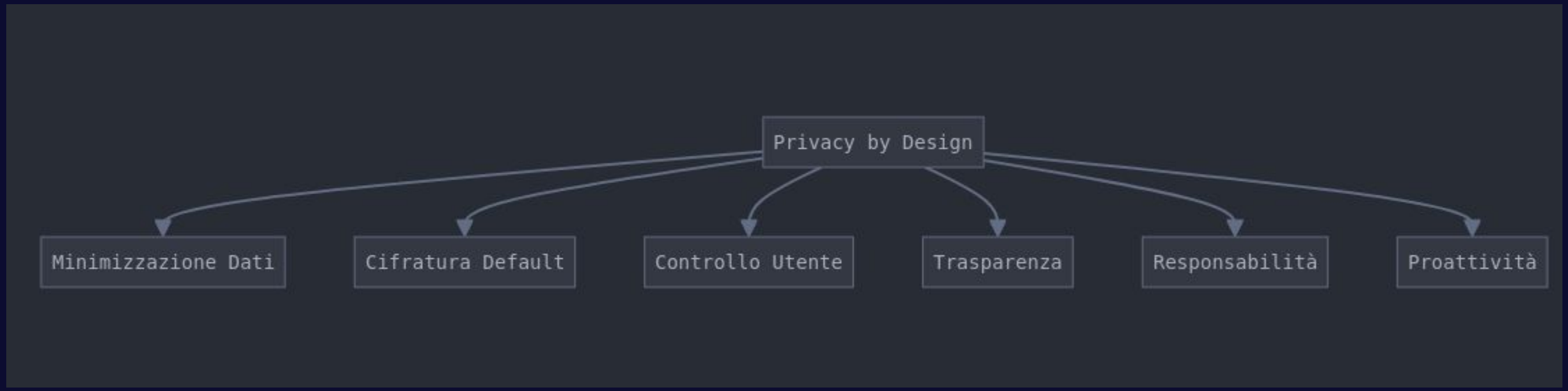
- **Sicurezza Matematica**:
  - Riduzione a problemi hard
  - Analisi worst-case
  - Resistenza attacchi noti
- **Parametri di Sicurezza**:
  - Dimensione reticolo
  - Distribuzione errori
  - Margini di sicurezza

Processo di Profilazione:

Il Futuro delle Tecnologie Analisi delle Tendenze Emergenti

Privacy by Design

L’UNICA SOLUZIONE



Processo di Profilazione:

Il Futuro delle Tecnologie Analisi delle Tendenze Emergenti

Conclusioni Pratiche

Roadmap per l'Implementazione

Azioni Immediate

1. **Individui:**
   - Adozione di password manager
   - Uso di 2FA
   - VPN affidabili
2. **Organizzazioni:**
   - Audit di privacy
   - Training del personale
   - Implementazione di E2EE
3. **Sviluppatori:**
   - Code review per privacy
   - Implementazione di zero-knowledge
   - Minimizzazione dei dati

Bibliografia

1. "The Age of Surveillance Capitalism" - Shoshana Zuboff
2. "Data and Goliath" - Bruce Schneier
3. "Privacy in the Age of Big Data" - Theresa Payton
4. "Networks of Control" - Wolfie Christl

Grazie per l’attenzione

Ready for the future