

e-privacy 2025 (21-22/10), Firenze
Misurare l'Umano? Dal Vitruviano all'Algoritmo

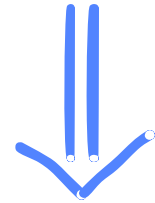
Blockchain tra privacy e regolamentazioni:
un nuovo paradigma di compliance

Andrea Rizzini - andrea.rizzini@polimi.it

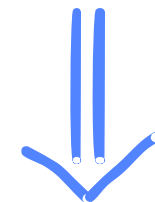


Roadmap

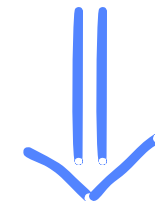
1) Concetti base sulla tecnologia blockchain



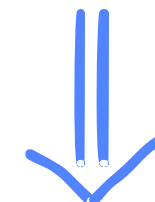
2) Concetto di pseudo-anonimato
e perchè non è sufficiente



3) Privacy tools... e problemi

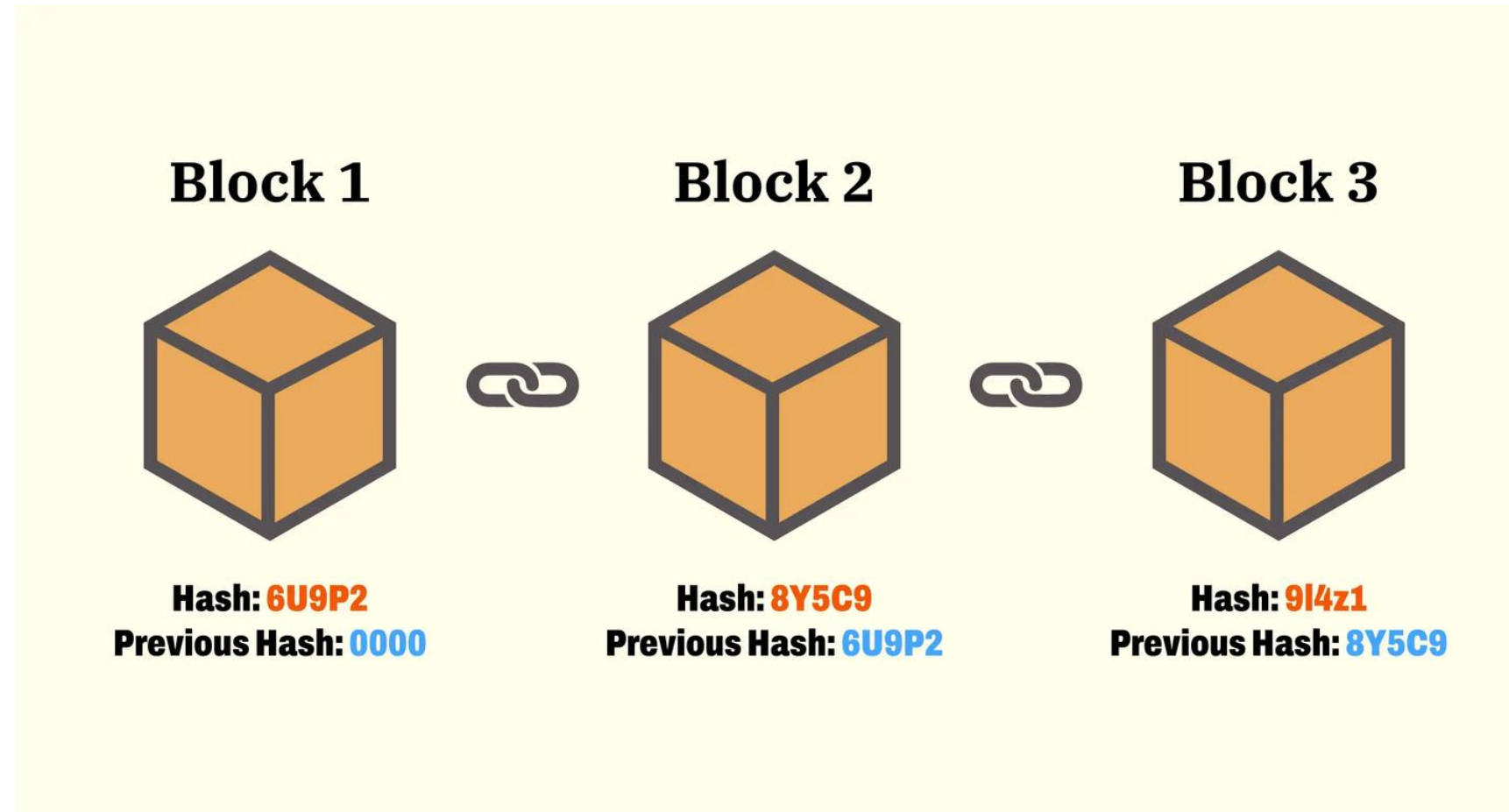


4) Compliance tools... e problemi



5) Il nostro contributo:
Ancestral Commitment Compliance

Blokchain - concetti di base



- Registro distribuito di transazioni digitali
- Le transazioni vengono raccolte in blocchi
- Ogni blocco è collegato crittograficamente con il precedente

Sistema distribuito → I nodi devono acconsentire in maniera distribuita ai nuovi blocchi che verranno aggiunti

↳ Meccanismi di consenso: PoW, PoS

Il concetto di identità nelle blockchain

Le blockchain sono trasparenti

↳ Grazie agli explorer, chiunque può ispezionare blocchi e transazioni

Transaction Hash:	0x4c94dd8a3bfaf2c5bdc6a3754f0161851bfaa18d870c1c2990149211f22104b3
Status:	Success
Block:	23518682 3 Block Confirmations
Timestamp:	34 secs ago (Oct-06-2025 12:18:47 PM UTC) Confirmed within 30 secs
Sponsored:	
From:	0x185e4e5C1AfE6B5177FBb81647949f1e1Bf3790B
To:	0x98d88F379218a334C142Ea96166eA8bFd47e7578
Value:	1.05 ETH (\$4,817.40)
Transaction Fee:	0.000008106480354 ETH (\$0.04)
Gas Price:	0.386022874 Gwei (0.000000000386022874 ETH)

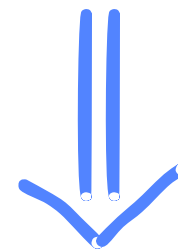
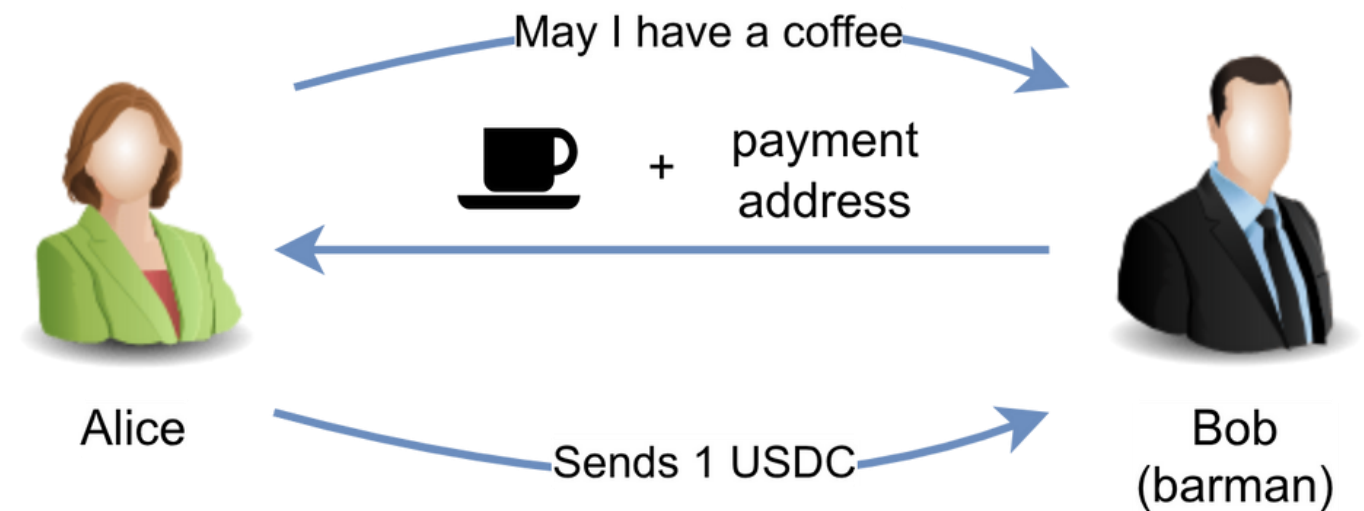
Pseudo-anonimato



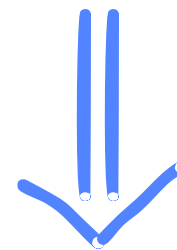
Perchè lo pseudo-anonimato non è sufficiente

Consideriamo il seguente scenario:

- ↳ Bob è un barista che accetta pagamenti crypto
- ↳ Alice vuole pagare un caffè in USDC



- Alice conosce l'indirizzo di Bob (il barista)
- Bob conosce l'indirizzo di Alice



Grazie alla proprietà di trasparenza

- Alice può vedere tutti gli introiti del bar
- Bob può vedere tutte le spese di Alice

Soluzioni privacy-preserving negli anni

Soluzioni native



Zcash



Diverse
modalità per
le transazioni

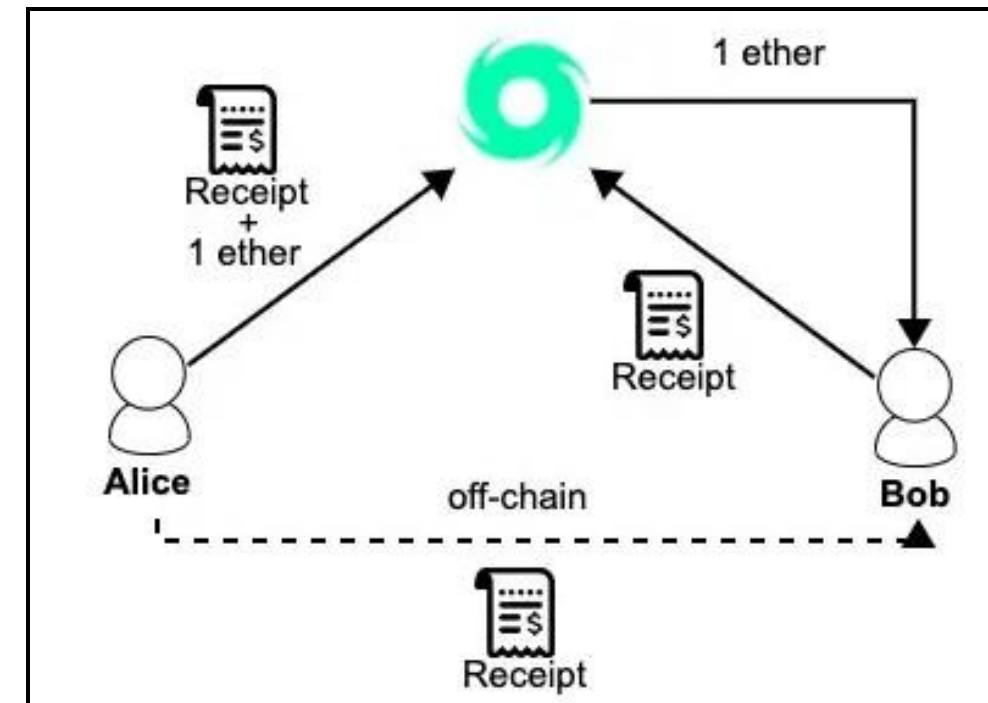
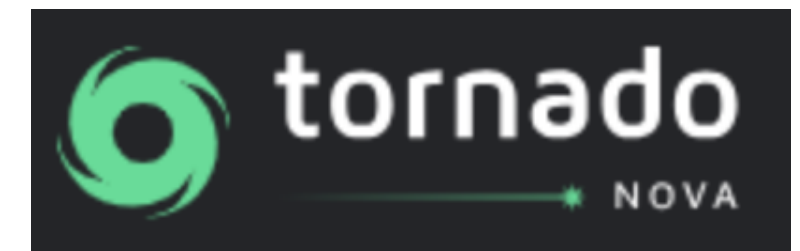
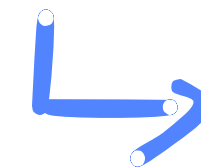


Monero



Transazioni
private di
default

Tools



Mixers: agiscono da
intermediario
rompendo il link
mittente / destinatario

... e problemi

Tornado Cash Founder, Roman Storm, Faces Trial for Money Laundering Charges

Published Jul 14, 2025, 11:34 PM

Source



Fatti rilevanti

- \$7 miliardi riciclati tramite Tornado Cash dalla sua creazione nel 2019
- \$455 milioni provenienti da furti attribuiti al gruppo Lazarus
- \$96 milioni provenienti dall'attacco a Harmony Bridge (giugno 2022)
- \$7,8 milioni provenienti dall'attacco a Nomad Bridge (agosto 2022)

Fonte: <https://home.treasury.gov/news/press-releases/jy0916>

Soluzioni di compliance - regolamentazioni

Recentemente, molte regolamentazioni sono state proposte, solo per citarne

alcune:

- └ Raccomandazioni FATF (Rec. 15 - new technologies, Rec. 16 - travel rule)
 - └ MiCA - Market in Crypto-Assets Regulation - (EU)
 - └ Regolazioni FinCEN (US), FCA crypto policies (UK), AMLD5/AMLD6 (UE) e molte altre in base alla giurisdizione
-

Problemi

- └ Mancanza di un quadro realmente uniforme a livello globale
- └ Gli obblighi colpiscono soprattutto VASP/CASP (exchange, custodial wallet, banche)
 - └ L'utente con wallet non-custodial (es. Metamask) non è direttamente soggetto alle regolamentazioni

Soluzioni di compliance - tools

Project	Arbitrary Denominations	Internal Transfers	Due Diligence	Optional Inclusion Delay	State Propagation	Updatable State
Tornado Cash (compliance tool)	✗	✗	✗	✓	✗	✗
Privacy Pools	✓	✗	✓	✓	✗	✓
Railgun	✓	✓	✓	✗	✗	✗

- └─ Tornado Cash (Compliance Tool): meccanismo di reporting opzionale
- └─ Privacy Pools: basato su association sets e Proof of Innocence [BIN+24]
- └─ Railgun: Proof of Innocence

Problema

- └─ Cosa succede se un indirizzo diventa sanzionato in un secondo momento?
 - └─ Due sfide principali
 - └─ **Come aggiornare lo stato**
 - └─ **Come propagare il nuovo stato**

Il nostro contributo

A Private Smart Wallet with Probabilistic Compliance

Andrea Rizzini, Marco Esposito, Francesco Bruschi, Donatella Sciuto

Dipartimento di Elettronica, Informazione e Bioingegneria (DEIB),

Politecnico di Milano, Milano, Italy

Email: {andrea.rizzini, marco.esposito, francesco.bruschi, donatella.sciuto}@polimi.it

2025 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS), Tucson, AZ, USA, 2025, pp. 101-110, doi: 10.1109/DAPPS65174.2025.00021.

Ancestral Commitment Compliance

Project	Arbitrary Denominations	Internal Transfers	Due Diligence	Optional Inclusion Delay	State Propagation	Updatable State
Tornado Cash (compliance tool)	✗	✗	✗	✓	✗	✗
Privacy Pools	✓	✗	✓	✓	✗	✓
Railgun	✓	✓	✓	✗	✗	✗
Ancestral Commitments	✓	✓	✓	✓	✓	✓

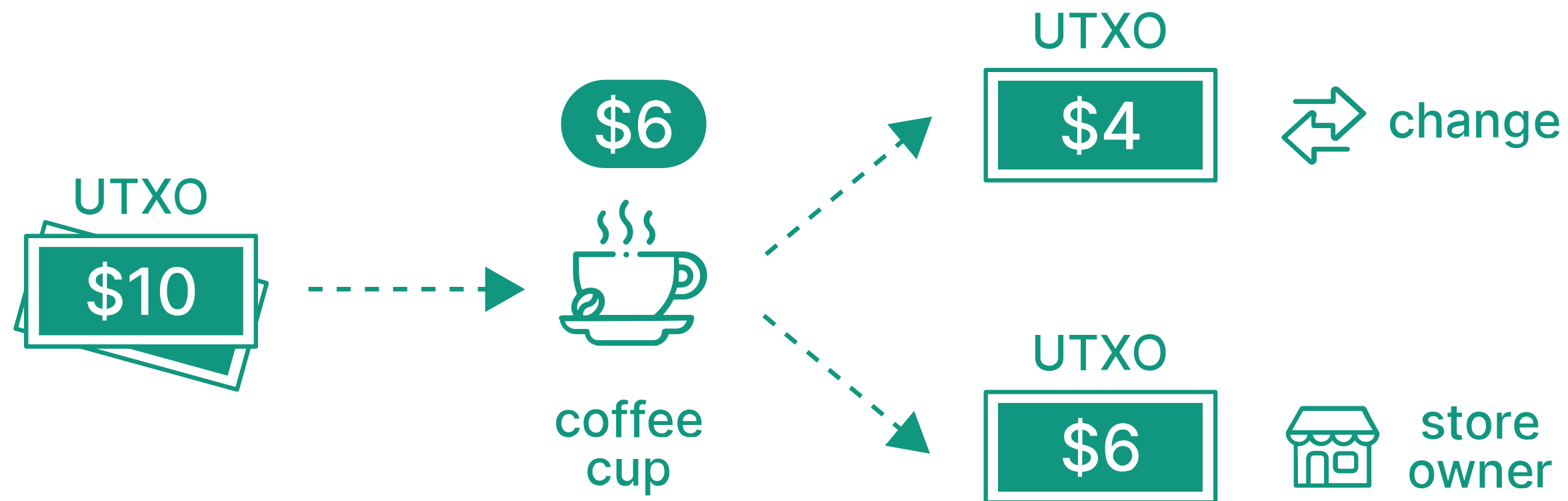
Features del
wallet

- EVM compatibile
- Usa ERC-4337 - account abstraction
- Layer di privacy integrato
- Transazioni e onboarding privatizzati**
- Ancestral Commitment Compliance**

ACC - background (1)

Concetti da tenere a mente:

- UTXO: rappresentazione di una quantità arbitraria di token spendibile
- Un utente sulla blockchain può possedere un certo numero di UTXO
- Transazioni basate su UTXO:



ACC - background (2)

Concetti da tenere a mente:

- Bloom filter

- └ Permette di memorizzare in maniera compatta dati arbitrari
- └ Ci servirà per memorizzare la struttura degli UTXO

- Zero-knowledge proofs

- └ “Voglio provarti che sono maggiorenne senza rivelare la mia età”
- └ Permette ad un prover, di provare la correttezza di un certo statement, che verrà verificato da un verifier
- └ Permette opzionalmente di tenere nascosti certi input della computazione

ACC - il protocollo (1)

Per ottenere transazioni private su Ethereum

↳ Modello UTXO + ZK-proofs

Computazione che voglio dimostrare con le ZK:

- ↳ Di avere il controllo sugli UTXO che voglio spendere
 - ↳ Che gli UTXO che voglio usare non siano già stati spesi (double-spending)
 - ↳ Che l'ammontare resti invariato
-

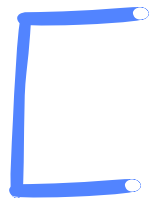
Per aggiungere il layer di compliance (ACC)

↳ Trusted entity

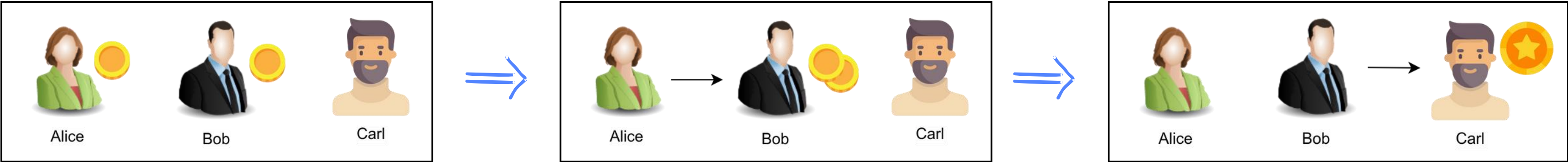
↳ ZK-proofs

↳ Bloom filter: ogni UTXO ora avrà una rispettiva rappresentazione in un Bloom Filter $\langle \text{UTXO}_i, \text{BF}_i \rangle$

ACC - il protocollo (2)

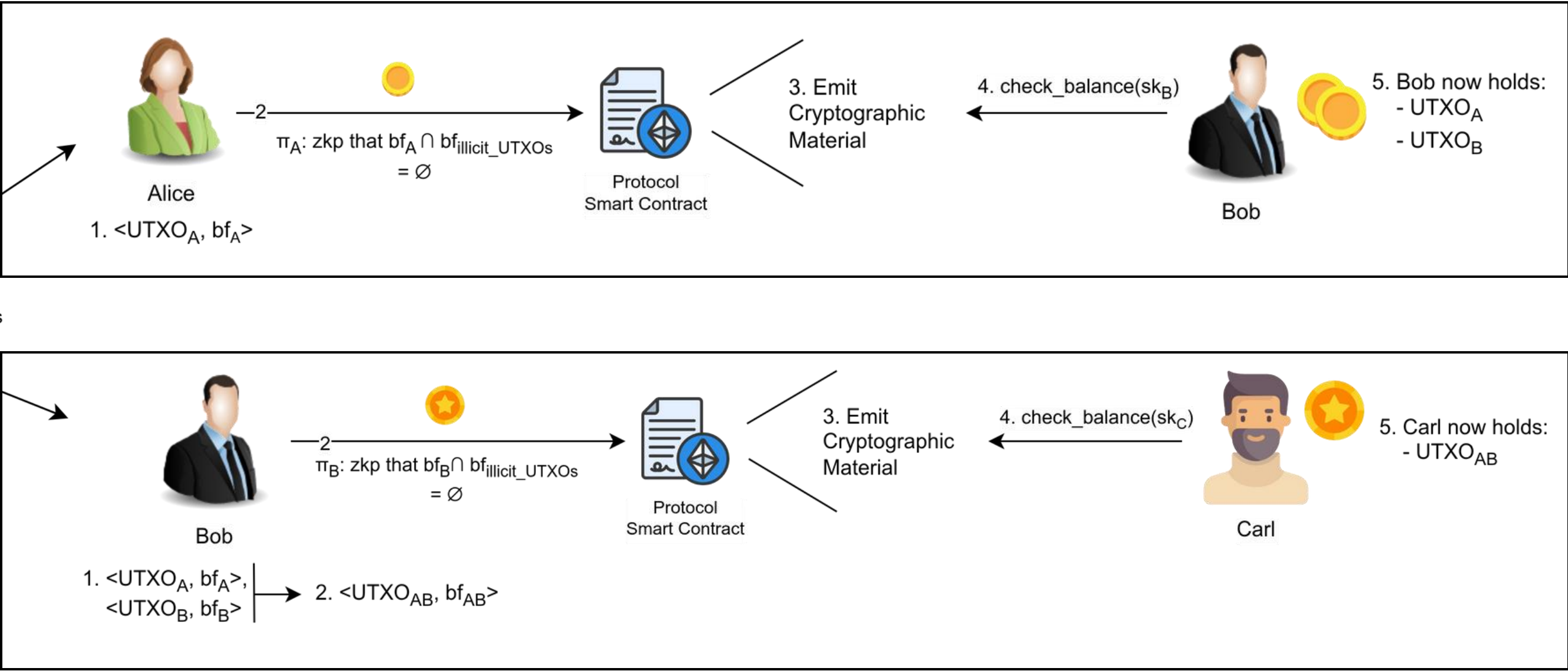
- 1) La Trusted Entity (TE) tiene traccia degli UTXO che circolano in questo protocollo
- 2) La TE monitora liste pubbliche di transazioni sospette/anomale sulla blockchain
- 3) Se uno UTXO risulta sospetto, la TE lo aggiunge ad una struttura dati apposita
- 4) Un utente che vuole effettuare una transazione privata userà  n UTXOs
 n bloom filters
- 5) L'utente creerà un bloom filter comprensivo di tutti gli UTXO che sta usando, chiamiamolo BF1
- 6) L'utente creerà un bloom filter comprensivo di tutti gli UTXO segnalati dalla nostra entità fidata, chiamiamolo BF2
- 7) L'utente creerà un zkp dimostrando che BF2 non è contenuto in BF1 ($BF1 \cap BF2 = \emptyset$)
 Gli UTXO che l'utente sta usando non sono nella lista di quelli segnalati

ACC - esempio completo



Trusted
Entity

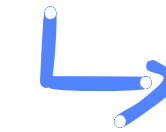
$bf_{illicit_UTXOs}$



Quanto costa usare la nostra soluzione

Operation	Gas π_{acc}	GWei	USD
insertIntoUsersPool	836405	41k	<0.12
callDeposit	2528502	126k	<0.33
callTransact	2842161	142k	<0.36
callWithdraw	2957810	148k	<0.38

Transazioni per 10 USDC
Accettabili comparati alle altre soluzioni



Railgun:

- 0.25% dell'amount per lo shielding (deposito)
- 10% del gas cost totale per le transazioni private

Action	SNARK transaction proof (ms)	SNARK compliance proof (ms)	Overall time (ms)
Onboard someone	2097.78	22340	24437.78
Onboard via link	X	X	14486.89
Fund the wallet	2064.56	X	X
Transfer privately	1999.40	20500	31292.36
Withdraw	2076.77	20650	22726.77

Overhead:

- tempo aggiunto dal tool di compliance: ~20 seconds

Direzioni future

- Siamo in grado di tracciare gli UTXO illeciti. Come dovremmo trattarli?
 - └ Burning? Rispedirli al mittente? Metterli in un deposito (sequestro)?
- Provare a ridurre ulteriormente i costi
 - └ Possiamo considerare soluzioni come i Layer-3 (Horizen roadmap)
- Considerazioni sull'open source
 - └ Fork e modifiche del codice potrebbero introdurre comportamenti indesiderati
 - └ Forzare la corretta costruzione del bloom filter
- Aumentare la decentralizzazione nel nostro sistema
 - └ Ridurre la dipendenza dall'entità fidata

Bibliografia

- S Goldwasser, S Micali, and C Rackoff. 1985. The knowledge complexity of interactive proof-systems. In Proceedings of the seventeenth annual ACM symposium on Theory of computing (STOC '85). Association for Computing Machinery, New York, NY, USA, 291–304.
<https://doi.org/10.1145/22145.22178>
- Jens Groth. On the Size of Pairing-Based Non-Interactive Arguments. IACR Cryptology ePrint Archive, Report 2016/260, 2016. Available at: <https://eprint.iacr.org/2016/260>
- Buterin, Vitalik & Illum, Jacob & Nadler, Matthias & Schär, Fabian & Soleimani, Ameen. (2024). Blockchain privacy and regulatory compliance: Towards a practical equilibrium. Blockchain: Research and Applications, 5(1), 100176. <https://doi.org/10.1016/j.bcra.2023.100176>.
- Burton H. Bloom. 1970. Space/time trade-offs in hash coding with allowable errors. Commun. ACM 13, 7 (July 1970), 422–426. <https://doi.org/10.1145/362686.362692>

Grazie