MINISTERO DELL'UNIVERSITÀ E DELLA RICERCA

Segretariato Generale
Direzione generale per la ricerca
Ufficio III

Relazione Scientifica finale
PRIN 2020 - protocollo: 20202FCJMH

Coordinatore Scientifico

BERNARDO	Marco	
(cognome)	**(nome)**	
Professore Ordinario (L. 240/10)	12/02/1970	BRNMRC70B12A944M
(qualifica)	**(data di nascita)**	**(Codice Fiscale)**

Università degli Studi di Urbino Carlo Bo
(Università/Ente)

Dati Progetto

Titolo del progetto:	Noninterference and Reversibility Analysis in Private Blockchains (NiRvAna)
Finanziamento MUR:	Euro 395.354
Cofinanziamento:	Euro 227.457
Costo progetto:	Euro 622.811

Lista delle Unità di Ricerca (UR)

nº	Responsabile Scientifico	Qualifica	Istituzione
1.	BERNARDO Marco	Professore Ordinario (L. 240/10)	Università degli Studi di Urbino Carlo Bo
2.	ROSSI Sabina	Professore Ordinario (L. 240/10)	Università "Ca' Foscari" VENEZIA
3.	PIAZZA Carla	Professore Ordinario (L. 240/10)	Università degli Studi di UDINE

Costo complessivo rendicontato Euro: 656.522,25

Durata effettiva del progetto: 36 mesi

Obiettivo della ricerca eseguita

La ricerca svolta ha avuto come obiettivo lo sviluppo di tecniche formali di modellazione e analisi di proprietà di noninterferenza e caratteristiche di reversibilità per sistemi concorrenti, distribuiti e

decentralizzati, con riferimento non solo agli aspetti funzionali ma anche a quelli prestazionali.

I metodi formali considerati sono stati le algebre di processi, per diversi motivi. In primo luogo la loro natura composizionale, grazie a operatori di combinazione sequenziale, alternativa e parallela che agevolano lo sviluppo di modelli di sistemi complessi a partire da modelli di sistemi più semplici. In secondo luogo le relative equivalenze comportamentali, in primis la bisimilarità che ricorre spesso nella letteratura della noninterferenza e della reversibilità, tramite cui è possibile identificare sistemi strutturalmente diversi che esibiscono il medesimo comportamento osservabile, nonché ragionare sui modelli dei sistemi in modo composizionale. In terzo luogo la loro capacità di supportare aspetti quantitativi come tempo e probabilità per poi calcolare indici prestazionali, specialmente nel caso in cui i processi stocastici sottostanti sono catene di Markov dato lo stretto legame tra la semantica interleaving e le distribuzioni di probabilità prive di memoria come pure tra la bisimilarità e una nozione di aggregazione esatta per tali catene nota come lumping ordinario.

Il concetto di noninterferenza caratterizza l'assenza di flussi di informazione indesiderati in sistemi in cui gli agenti sono classificati in base a livelli di sicurezza diversi. La noninterferenza garantisce che il comportamento del sistema in cui le azioni degli agenti ad alto livello di sicurezza vengono rese invisibili agli agenti a basso livello di sicurezza è indistinguibile dal, cioè formalmente equivalente al, comportamento del sistema in cui le azioni degli agenti ad alto livello di sicurezza non hanno luogo. Ciò garantisce che non vi possano essere perdite di informazione dal livello alto al livello basso dovute ad azioni osservabili causate da quelle di alto livello. Il concetto può essere reso più fine nel caso in cui siano ammesse computazioni reversibili oppure vengano altresì considerate informazioni quantitative relative alla durata o alla probabilità delle azioni.

La nozione di reversibilità riguarda invece la possibilità di annullare gli effetti di una computazione a partire dall'ultima azione effettuata. Questo non è affatto banale in presenza di concorrenza perché, a causa del nondeterminismo, in generale non esiste un ordinamento totale delle azioni eseguite e pertanto l'ultima azione effettuata potrebbe non essere univocamente individuabile. La proprietà che si considera in questo contesto è quella di reversibilità causale, la quale stabilisce che un'azione può essere revocata solo se le eventuali azioni da essa causate sono già state revocate. Un'altra nozione di reversibilità è quella temporale, sviluppata nel campo delle catene di Markov, che vale quando il comportamento stocastico del sistema non cambia se si inverte la direzione del tempo. Tale proprietà è nota avere legami con diverse forme di lumping e, in caso di validità, consente di analizzare più efficientemente la catena considerata. È auspicabile una visione integrata dei vari tipi di reversibilità nei sistemi temporizzati o probabilistici.

L'ambito applicativo principale è stato quello delle blockchain, rispetto al corretto funzionamento del loro meccanismo di consenso, alla loro sicurezza e alle loro prestazioni. Oltre alle blockchain pubbliche, che sono completamente disintermediate e quindi consentono a chiunque lo voglia di entrare, operare e uscire in qualsiasi momento, sono state considerate anche quelle private, in cui l'accesso è regolato, con uno speciale interesse verso il loro impiego nelle central bank digital currency (CBDC).

Descrizione della ricerca eseguita

La ricerca svolta, articolata nei work package e task previsti in fase di presentazione del progetto ampliando a volte la portata degli stessi, ha dato luogo a numerosi risultati che vengono descritti nel seguito suddivisi per comodità nelle cinque aree equivalenze, noninterferenza, reversibilità, strumenti software e blockchain.

EQUIVALENZE

Rispetto a quanto previsto nel WP1 - MARKOVIAN BEHAVIORAL EQUIVALENCES, in [J5, C25] è stata approfondita la nozione di lumping proporzionale, che è una variante del lumping ordinario ottenuta perturbando opportunamente i tassi delle transizioni della catena di Markov, in maniera da affrontare il problema dell'esplosione dello spazio degli stati quando si calcolano indici prestazionali in modelli stocastici grandi, con applicazioni anche nel campo delle reti neurali [C3, J10]. Inoltre sono state sviluppate varianti stocastiche della back-and-forth bisimilarity di De Nicola, Montanari e Vaandrager, mostrando quale tra queste coincide con la bisimilarità stocastica di Hillston [J2], insieme a varianti reverse-only e forward-reverse della bisimilarità stocastica anzidetta su processi sequenziali, riportando risultati di congruenza, caratterizzazione equazionale e coincidenza con lumping esatto e lumping stretto rispettivamente [C4].

In aggiunta a quanto sopra, a partire da [C4] è stata sviluppata una teoria algebrica per sistemi concorrenti reversibili [C9, C10, C21, C26]. È stata messa a punto l'algebra di processi PRPC - Proved Reversible Process Calculus basata sui proved labeled transition system di Degano e Priami, che evita la decorazione con chiavi e il relativo branching infinito di CCSK di Phillips e Ulidowski come pure il ricorso a

memorie esterne ai processi di RCCS di Danos e Krivine. In PRPC sono state studiate sia la forward-reverse bisimilarity alla Phillips e Ulidowski che la forward-only bisimilarity alla Milner e la reverse-only bisimilarity, fornendo risultati di congruenza, caratterizzazione logica e caratterizzazione equazionale tanto per le varianti forti quanto per quelle deboli. Grazie alla semantica proved, le assiomatizzazioni sono state ricavate in modo uniforme per la forward-only bisimilarity, che è interleaving, e per la forward-reverse bisimilarity e la reverse-only bisimilarity, che sono truly concurrent, dopo aver individuato per queste ultime due nei backward ready set le informazioni discriminanti necessarie da aggiungere ai prefissi di azione. È stato inoltre scoperto che l'aggiunta alla forward-reverse bisimilarity di una condizione sull'uguaglianza dei backward ready multiset fa coincidere tale equivalenza con la hereditary history-preserving bisimilarity di Bednardick in assenza di conflitti non locali. Tutti questi risultati si trovano nella prima parte di [T1].

NONINTERFERENZA

Rispetto a quanto previsto nel WP2 - STOCHASTIC NONINTERFERENCE ANALYSIS, in [C16, C30] sono state introdotte nuove proprietà di sicurezza attraverso un rilassamento della noninterferenza ed equivalenze comportamentali approssimate, con l'obiettivo di descrivere in modo più accurato i sistemi reali, in particolare le blockchain. Tali proprietà sono state utilizzate per individuare vulnerabilità specifiche come gli attacchi MEV - Maximal Extractable Value, finalizzati a ottenere il massimo valore nell'interazione con uno smart contract, e la reentrancy, che si manifesta quando uno smart contract viene ripetutamente invocato prima che le esecuzioni precedenti siano state completate. Le proprietà sono state ulteriormente generalizzate introducendo il concetto di downgrading, ossia ammettendo determinati flussi di informazione considerati non pericolosi rispetto al tipo di garanzia di sicurezza che si intende catturare. In [R4] è stata introdotta una variante debole del lumping esatto e, a partire da essa, una nozione di noninterferenza stocastica denominata EPSNI, di cui sono stati analizzati gli aspetti di composizionalità ed è stata fornita una caratterizzazione che ne consente la verifica efficiente.

In aggiunta a quanto sopra, è stato effettuato uno studio di varie proprietà di noninterferenza per sistemi reversibili, comprensivo delle caratteristiche di composizionalità e preservazione. Il risultato fondamentale è stata la scoperta che la bisimilarità branching di Van Glabbeek e Weijland riesce in questo contesto reversibile a catturare canali coperti che la bisimilarità debole di Milner non rileva. Pertanto la tassonomia delle proprietà di noninterferenza per sistemi nondeterministici irreversibili sviluppata da Focardi e Gorrieri è stata estesa a quelli reversibili [C5, J13] e poi ulteriormente applicata a sistemi reversibili e irreversibili che, oltre al nondeterminismo, comprendono probabilità [C19], tempo stocastico [C32] o tempo deterministico [C33]. Tutti questi risultati si trovano nella seconda parte di [T1].

REVERSIBILITÀ

Rispetto a quanto previsto nel WP3 - INTEGRATED REVERSIBILITY ANALYSIS, da un lato in [J2] per le algebre di processi stocasticamente temporizzate è stata verificata l'applicabilità dell'approccio di Phillips e Ulidowski per ottenere reversibilità causale per costruzione, mostrando poi che è invece necessario modificare l'approccio stesso per le algebre di processi con nondeterminismo e tempo deterministico, sia nel caso di ritardi unitari [C1, J4] che nel caso di ritardi arbitrari soggetti a determinismo e additività temporali [C11], oppure probabilità [C23]. Dall'altro lato, sempre in [J2] è stato messo a punto un approccio per ottenere reversibilità temporale per costruzione, studiando successivamente le condizioni sotto le quali la reversibilità causale implica quella temporale [C12].

In aggiunta a quanto sopra, in [C6, J9] sono state studiate le relazioni esistenti tra le reti di Petri reversibili e le strutture di eventi reversibili. In [J11] è stata sviluppata una semantica concorrente basata su reti di Petri per l'algebra di processi reversibile RCCS. In [C7, J12] sono stati proposti meccanismi di reversibilità in linguaggi di programmazione basati su sessioni, così da liberarsi dall'onere di garantire la correttezza di eventuali rollback a seguito di circostanze impreviste o errori. In [C20] è stato infine investigato il model checking di sistemi reversibili basato sulla logica temporale LTL estesa con operatori relativi al passato.

STRUMENTI SOFTWARE

Rispetto a quanto previsto nel WP4 - SOFTWARE TOOL IMPLEMENTATION, il PEPA Eclipse plug-in è stato esteso (https://github.com/RiccardoRomanello/PEPA_Update) arricchendo la sintassi dell'algebra di processi stocastica PEPA di Hillston da un lato col livello di sicurezza di ogni azione, al fine di abilitare l'analisi delle proprietà di noninterferenza stocastica precedentemente menzionate, e dall'altro con l'indicazione di reversibilità o meno per ciascuna azione, con relativo impatto sulla semantica operazionale e conseguente supporto alla verifica di reversibilità temporale. Inoltre, nel suddetto plug-in sono state implementate le equivalenze stocastiche prima indicate insieme ai lumping corrispondenti nella catena di Markov.

In aggiunta a quanto sopra, nello strumento CADP per l'algebra di processi LNT (https://cadp.inria.fr/) sono state implementate le proprietà di noninterferenza basate sulla bisimilarità branching per sistemi nondeterministici eventualmente arricchiti con probabilità o tempo stocastico [R3].

BLOCKCHAIN

Rispetto a quanto previsto nel WP5 - APPLICATIONS TO PRIVATE BLOCKCHAINS, sono stati sviluppati e verificati con gli strumenti sopra menzionati i modelli in algebra di processi dell'algoritmo di consenso di Algorand in presenza di eventuali utenti malevoli [R3], degli aspetti prestazionali del protocollo di consenso di Cosmos [C18, C22], dell'attacco selfish mining che si verifica con biforcazioni della blockchain tali per cui la ricompensa è maggiore dell'energia impiegata [C8] e del verifier dilemma derivante dal fatto che la verifica dei blocchi non è soggetta a ricompensa diversamente dalla loro inclusione nella blockchain [C15, J15].

In aggiunta a quanto sopra:

- In [C14] è stato trattato il tema dei costrutti linguistici adeguati per blockchain e smart contract al fine di superare le loro vulnerabilità, proponendo l'adozione del linguaggio Move in Algorand, mentre in [J14] è stata condotta un'analisi comparativa dei linguaggi per smart contract.

- In [C24] è stato valutato l'impiego di tecniche di machine learning e di reti neurali per addestrare un rilevatore di vulnerabilità all'interno di smart contract, mentre in [J6] è stata presentata una panoramica dell'applicazione di tecniche di intelligenza artificiale in generale nel mondo blockchain.

- In [C27, C29] è stata studiata la variabilità dell'efficienza prestazionale ed energetica di alcune blockchain sotto carichi di lavoro diversi in funzione delle topologie di rete, mentre l'efficienza economica delle stesse blockchain misurata attraverso un indicatore generale basato sulla formula dell'entropia di Shannon è stata affrontata in [C31].

- Le stablecoin algoritmiche sono state oggetto di studio in [C17, J16, C28] sia in termini di come aumentarne la stabilità, partendo dal caso Terra-Luna, che di simularne il funzionamento tanto in condizioni normali quanto di panico.

- Mediante reti di code, per la blockchain di Bitcoin in [J3] è stato analizzato il rapporto ottimale tra il tempo di conferma di una transazione e il costo della transazione stessa, mentre in [J8] è stata analizzata la probabilità di perdita di una transazione in attesa di conferma quando la mempool è in un certo stato di riempimento.

- [R1, R2] sono lavori di rassegna rispettivamente su redactability, cioè la forma limitata di reversibilità talvolta ammessa nelle blockchain per conformità alla normativa vigente (p.e. diritto all'oblio) o semplicemente per rimediare a errori contenuti nelle transazioni o nella piattaforma, e l'uso dei metodi formali per garantire la resilienza operativa delle CBDC.

Problemi riscontrati nel corso della ricerca

Al momento non è ancora stata trovata una soluzione al problema di mantenere finito lo spazio degli stati in ambito reversibile in presenza di ricorsione in quelle situazioni in cui lo spazio sarebbe stato finito in un'algebra di processi senza reversibilità, né si è dimostrata l'inesistenza di tale soluzione (T3.2). Sono state comunque acquisite competenze nella modellazione di sistemi a stati infiniti [C13] che potranno essere sfruttate in futuro.

Inoltre, lo studio effettuato sulle blockchain esistenti insieme alla disponibilità di dati reali per esse, oltre alle difficoltà incontrate dall'Unità di Ricerca di UniUrb a reclutare personale specifico, hanno indotto a preferire la realizzazione e l'analisi di modelli in algebra di processi di blockchain consolidate di varia natura come Bitcoin, Algorand e Cosmos rispetto allo sviluppo del prototipo di una nuova blockchain (T5.3).

Risultati scientifici conseguiti

Tipologia del risultato	Si/No	Descrizione
Realizzazione di nuova strumentazione scientifica e/o di dispositivi avanzati	NO	
Messa in opera di metodologie scientifiche avanzate	NO	
Altro	NO	Avanzamento e integrazione dello stato delle conoscenze nell'ambito delle tecniche di noninterferenza e reversibilità applicate a sistemi concorrenti, distribuiti e decentralizzati, di cui vengono considerati non solo gli aspetti qualitativi come il nondeterminismo ma anche quelli quantitativi come tempo e probabilità. Implementazione delle estensioni di tali tecniche in due dei principali strumenti software per la modellazione e la verifica dei suddetti sistemi tramite algebre di processi e relative equivalenze: PEPA Eclipse plug-in e CADP.

Prodotti realizzati

Tipologia del risultato	Si/No	Descrizione
Pubblicazioni scientifiche: (indicare pubblicazione con autori, titolo, tipo di pubblicazione -monografia, libro di testo, capitolo di libro, rivista, atti di congressi, corpora, relazioni su invito, - e se soggetta a processo di revisione)	SI	Articoli su rivista: [J16] F. Calandra, F.P. Rossi, F. Fabris, M. Bernardo. Learning from Terra-Luna: A Simulation-Based Study on Stabilizing Algorithmic Stablecoins. Blockchain: Research and Applications. 2025. (to appear) [J15] D. Smuseva, A. Marin, S. Rossi, A. Van Moorsel. Verifier's Dilemma in Proof-of-Work Public Blockchains: A Quantitative Analysis. ACM Trans. on Modeling and Computer Simulation 35(2):12:1–12:24. April 2025. [J14] M. Bartoletti, L. Benetollo, M. Bugliesi, S. Crafa, G. Dal Sasso, R. Pettinau, A. Pinna, M. Piras, S. Rossi, S. Salis, A. Spanò, V. Tkachenko, R. Tonelli, R. Zunino. Smart Contract Languages: A Comparative Analysis. Future Generation Computer Systems 164:107563. March 2025. [J13] A. Esposito, A. Aldini, M. Bernardo, S. Rossi. Noninterference Analysis of Reversible Systems: An Approach Based on Branching Bisimilarity. Logical Methods in Computer Science 21(1):6:1–6:28. January 2025. [J12] C.A. Mezzina, F. Tiezzi, N. Yoshida. Checkpoint-Based Rollback Recovery in Session Programming. Logical Methods in Computer Science 21(1):2:1–2:36. January 2025. [J11] H.C. Melgratti, C.A. Mezzina, G.M. Pinna. A Truly Concurrent Semantics for Reversible CCS. Logical Methods in Computer Science 20(4):20:3–20:37. December 2024. [J10] D. Ressi, R. Romanello, S. Rossi, C. Piazza. Compressing Neural Networks via Formal Methods. Neural Networks 178:106411. October 2024. [J9] H.C. Melgratti, C.A. Mezzina, G.M. Pinna. A Reversible Perspective on Petri Nets and Event Structures. ACM Trans. on Computational Logic 25(4):23:1–23:38. October 2024. [J8] I. Malakhov, A. Marin, S. Rossi, D. Sadoc Menasché. Confirmed or Dropped? Reliability Analysis of Transactions in PoW Blockchains. IEEE Trans. on Network Science and Engineering 11(4):3276–3288. August 2024. [J7] D. Olliaro, G. Casale, A. Marin, S. Rossi. A Product-Form Network for Systems with Job Stealing Policies. ACM Trans. on Modeling and Performance Evaluation of Computing Systems 9(2):6:1–6:26. June 2024.

Tipologia del risultato	Si/No	Descrizione
		[J6] D. Ressi, R. Romanello, C. Piazza, S. Rossi. AI-Enhanced Blockchain Technology: A Review of Advancements and Opportunities. Journal of Network and Computer Applications 225:103858. May 2024. [J5] C. Piazza, S. Rossi, & D. Smuseva. Efficient Algorithm for Proportional Lumpability and Its Application to Selfish Mining in Public Blockchains. Algorithms 17(4):159. April 2024. [J4] L. Bocchi, I. Lanese, C.A. Mezzina, S. Yuen. revTPL: The Reversible Temporal Process Language. Logical Methods in Computer Science 20(1):11:1–11:35. January 2024. [J3] I. Malakhov, A. Marin, S. Rossi. Analysis of the Confirmation Time in Proof-of-Work Blockchains. Future Generation Computer Systems 147:275–291. October 2023. [J2] M. Bernardo, C.A. Mezzina. Bridging Causal Reversibility and Time Reversibility: A Stochastic Process Algebraic Approach. Logical Methods in Computer Science 19(2):6:1–6:27. April 2023. [J1] A. Marin, S. Rossi, D. Olliaro. A Product-Form Network for Systems with Job Stealing Policies. SIGMETRICS Performance Evaluation Review 50(4):2–4. March 2023. Articoli su atti di convegni: [C33] A. Esposito, A. Aldini, M. Bernardo. Noninterference Analysis of Deterministically Timed Reversible Systems. In Proc. of QEST/FORMATS 2025, Springer, LNCS, Aarhus (Denmark), August 2025. (to appear) [C32] A. Esposito, A. Aldini, M. Bernardo. Noninterference Analysis of Stochastically Timed Reversible Systems. In Proc. of FORTE 2025, Springer, LNCS 15732:75–95, Lille (France), June 2025. [C31] V.P. Di Perna, M. Foderaro, F. Fabris, M. Bernardo. An Entropy-Based Approach to Evaluating the Economic Efficiency of Cryptocurrencies. In Proc. of DLT 2025, CEUR-WS, Pizzo (Italy), June 2025. (to appear) [C30] L. Benetollo, S. Guesmi, C. Piazza, D. Ressi, S. Rossi, A. Spanò. Modeling Reentrancy in Smart Contracts through Noninterference. In Proc. of DLT 2025, CEUR-WS, Pizzo (Italy), June 2025. (to appear, winner of the best paper award) [C29] V.P. Di Perna, M. Bernardo, F. Fabris, S. Amaro, M. Matos, V. Schiavoni. Impact of Network Topologies on Blockchain Performance. In Proc. of DEBS 2025, ACM Press, pages 122–133, Gothenburg (Sweden), June 2025. (winner of the best student paper award) [C28] F. Calandra, F.P. Rossi, F. Fabris, M. Bernardo. Algorithmic Stablecoins: A Simulator for the Dual-Token Model in Normal and Panic Scenarios. In Proc. of ICBC 2025, IEEE-CS Press, pages 177–185, Pisa (Italy), June 2025. [C27] V.P. Di Perna, V. Schiavoni, F. Fabris, M. Bernardo. Blockchain Energy Consumption: Unveiling the Impact of Network Topologies. In Proc. of ICBC 2025, IEEE-CS Press, pages 67–76, Pisa (Italy), June 2025. [C26] M. Bernardo, A. Esposito, C.A. Mezzina. Alternative Characterizations of Hereditary History-Preserving Bisimilarity via Backward Ready Multisets. In Proc. of FOSSACS 2025, Springer, LNCS 15691:67–87, Hamilton (Canada), May 2025. [C25] C. Piazza, S. Rossi. Generalized Proportional Lumpability. In Proc. of VALUETOOLS 2024, Springer, LNICST, Milan (Italy), December 2024. (to appear) [C24] M. Rizzo, D. Ressi, A. Gasparetto, S. Rossi. A Comparison of

Tipologia del risultato	Si/No	Descrizione
		Machine Learning Techniques for Ethereum Smart Contract Vulnerability Detection. In Proc. of OVERLAY 2024, CEUR-WS, 3904:119–126, Bolzano (Italy), November 2024. [C23] M. Bernardo, C.A. Mezzina. Reversibility in Process Calculi with Nondeterminism and Probabilities. In Proc. of ICTAC 2024, Springer, LNCS 15373:251–271, Bangkok (Thailand), November 2024. [C22] D. Smuseva, C. Piazza, I. Malakhov, A. Marin, S. Rossi. Cosmos Discovery: Quantitative Assessment of Cosmos Blockchain. In Proc. of MASCOTS 2024, IEEE-CS Press, pages 1–8, Krakow (Poland), October 2024. [C21] M. Bernardo, A. Esposito, C.A. Mezzina. Expansion Laws for Forward-Reverse, Forward, and Reverse Bisimilarities via Proved Encodings. In Proc. of EXPRESS/SOS 2024, Open Publishing Association, EPTCS 412:51–70, Calgary (Canada), September 2024. [C20] F. Dal Pio Luogo, C.A. Mezzina, G.M. Pinna. Model Checking Reversible Systems: Forwardly. In Proc. of RC 2024, Springer, LNCS 14680:218–237, Torun (Poland), July 2024. [C19] A. Esposito, A. Aldini, M. Bernardo. Noninterference Analysis of Reversible Probabilistic Systems. In Proc. of FORTE 2024, Springer, LNCS 14678:39–59, Groningen (The Netherlands), June 2024. [C18] D. Smuseva, I. Malakhov, A. Marin, C. Piazza, S. Rossi. Under the Space Threat: Quantitative Analysis of Cosmos Blockchain. In Proc. of EPEW 2024, Springer, LNCS 15454:91–105, Venice (Italy), June 2024. [C17] F. Calandra, F.P. Rossi, F. Fabris, M. Bernardo. Making Algorithmic Stablecoins More Stable: The Terra-Luna Case Study. In Proc. of DLT 2024, CEUR-WS, 3791:19:1–19:14, Torino (Italy), May 2024. [C16] S. Guesmi, C. Piazza, S. Rossi. Noninterference Analysis for Smart Contracts: Would You Bet on It?. In Proc. of DLT 2024, CEUR-WS, 3791:12:1–12:15, Torino (Italy), May 2024. [C15] D. Smuseva, I. Malakhov, A. Marin, S. Rossi. Crisis of Trust: Analyzing the Verifier's Dilemma in Ethereum's Proof-of-Stake Blockchain. In Proc. of BLOCKCHAIN 2023, IEEE-CS Press, pages 332–339, Danzhou (China), December 2023. [C14] L. Benetollo, M. Bugliesi, S. Crafa, S. Rossi, A. Spanò. ALGOMOVE – A Move Embedding for Algorand. In Proc. of BLOCKCHAIN 2023, IEEE-CS Press, pages 62–67, Danzhou (China), December 2023. [C13] A. Casagrande, C. Piazza. Adaptive Directions for Bernstein-Based Polynomial Set Evolution. In Proc. of RP 2023, Springer, LNCS 14235:113–126, Nice (France), October 2023. [C12] M. Bernardo, I. Lanese, A. Marin, C.A. Mezzina, S. Rossi, C. Sacerdoti Coen. Causal Reversibility Implies Time Reversibility. In Proc. of QEST 2023, Springer, LNCS 14287:270–287, Antwerp (Belgium), September 2023. [C11] M. Bernardo, C.A. Mezzina. Causal Reversibility for Timed Process Calculi with Lazy/Eager Durationless Actions and Time Additivity. In Proc. of FORMATS 2023, Springer, LNCS 14138:15–32, Antwerp (Belgium), September 2023. [C10] M. Bernardo, A. Esposito. Modal Logic Characterizations of Forward, Reverse, and Forward-Reverse Bisimilarities. In Proc. of GANDALF 2023, Open Publishing Association, EPTCS 390:67–81, Udine (Italy), September 2023. [C9] M. Bernardo, A. Esposito. On the Weak Continuation of Reverse Bisimilarity vs. Forward Bisimilarity. In Proc. of ICTCS 2023, CEUR-WS,

Tipologia del risultato	Si/No	Descrizione
		3587:44–58, Palermo (Italy), September 2023. [C8] D. Smuseva, A. Marin, S. Rossi. Selfish Mining in Public Blockchains: A Quantitative Analysis. In Proc. of VALUETOOLS 2023, Springer, LNICST 539:18–32, Crete (Greece), September 2023. [C7] C.A. Mezzina, F. Tiezzi, N. Yoshida. Rollback Recovery in Session-Based Programming. In Proc. of COORDINATION 2023, Springer, LNCS 13908:195–213, Lisbon (Portugal), June 2023. [C6] H.C. Melgratti, C.A. Mezzina, G.M. Pinna. Relating Reversible Petri Nets and Reversible Event Structures, Categorically. In Proc. of FORTE 2023, Springer, LNCS 13910:206–223, Lisbon (Portugal), June 2023. [C5] A. Esposito, A. Aldini, M. Bernardo. Branching Bisimulation Semantics Enables Noninterference Analysis of Reversible Systems. In Proc. of FORTE 2023, Springer, LNCS 13910:57–74, Lisbon (Portugal), June 2023. [C4] M. Bernardo, S. Rossi. Reverse Bisimilarity vs. Forward Bisimilarity. In Proc. of FOSSACS 2023, Springer, LNCS 13992:265–284, Paris (France), April 2023. [C3] D. Ressi, R. Romanello, C. Piazza, S. Rossi. Neural Networks Reduction via Lumping. In Proc. of AIxIA 2022, Springer, LNAI 13796:75–90, Udine (Italy), November 2022. [C2] C. Piazza, R. Romanello. Mirrors and Memory in Quantum Automata. In Proc. of QEST 2022, Springer, LNCS 13479:359–380, Warsaw (Poland), September 2022. [C1] L. Bocchi, I. Lanese, C.A. Mezzina, S. Yuen. The Reversible Temporal Process Language. In Proc. of FORTE 2022, Springer, LNCS 13273:31–49, Lucca (Italy), June 2022.
Tesi di dottorato collegate	SI	Tesi di dottorato: [T1] A. Esposito. A Process Algebraic Theory of Reversible Concurrent Systems with Applications to Noninterference Analysis. Ph.D. Thesis, University of Urbino (Italy), May 2025.
Realizzazione di prototipi	NO	
Brevetti realizzati nell'ambito del progetto	NO	
Sintesi di nuove molecole e/o di materiali artificiali	NO	
Sviluppo di software open source o commerciale (dare titolo del programma, numero di linee di codice, uso previsto, link al website dove il software si trova,...)	SI	Estensione del PEPA Eclipse plug-in con analisi di noninterferenza stocastica e supporto alla reversibilità temporale in ambito algebre di processi stocastiche (https://github.com/RiccardoRomanello/PEPA_Update). Implementazione nello strumento CADP per l'algebra di processi LNT (https://cadp.inria.fr/) delle proprietà di noninterferenza basate sulla bisimilarità branching per sistemi nondeterministici eventualmente reversibili e/o arricchiti con probabilità o tempo stocastico.
Altro	SI	Rapporti tecnici: [R4] C. Piazza, R. Romanello, S. Rossi. Exact Persistent Stochastic Non-Interference. Technical Report arXiv:2508.19110, August 2025. [R3] A. Esposito, F.P. Rossi, M. Bernardo, F. Fabris, H. Garavel. Formal Modeling and Verification of the Algorand Consensus Protocol in CADP. Technical Report arXiv:2508.19452, August 2025. [R2] F. Calandra, M. Bernardo, A. Esposito, F. Fabris. Redactable Blockchains: An Overview. Technical Report arXiv:2508.08898, August

Tipologia del risultato	Si/No	Descrizione
		2025. [R1] M. Bernardo, F. Calandra, A. Esposito, F. Fabris. On the Operational Resilience of CBDC: Threats and Prospects of Formal Validation for Offline Payments. Technical Report arXiv:2508.08064, August 2025.

Realizzazione di nuovi network e collaborazioni

Tipologia del risultato	Si/No	Descrizione
Accordi di collaborazione con organizzazioni scientifiche nazionali	NO	
Accordi di collaborazione con imprese nazionali	NO	
Accordi di collaborazione con organizzazioni scientifiche internazionali	NO	
Accordi di collaborazione con imprese internazionali	NO	
Altro	SI	Sono state rafforzate le collaborazioni scientifiche con l'Università di Edimburgo (UK) per l'estensione del PEPA Eclipse plug-in. Sono state instaurate nuove collaborazioni scientifiche con INRIA Grenoble Rhone-Alpes (Francia) per l'estensione di CADP, con l'Università di Neuchatel (Svizzera) per lo studio di variabilità dell'efficienza prestazionale ed energetica delle blockchain in funzione delle topologie di rete, con il Cambridge Center for Alternative Finance (UK) per lo studio dell'efficienza economica delle blockchain e con IRIF (Francia) per lo studio di protocolli di lending e borrowing. Sono in corso di definizione collaborazioni scientifiche con Banca d'Italia per investigare canali di pagamento e CBDC.

Note

DIFFUSIONE DEI DATI SCIENTIFICI

Informazione

Modalità	Si/No	Descrizione
Pubblicazioni (escluse quelle con referaggio)	NO	
Depliant	NO	
CD-Rom	NO	
Altro	SI	La riunione conclusiva del progetto, svoltasi a Urbino nei giorni 29-31/05/2025 con la possibilità di collegarsi da remoto, è stata pubblicizzata presso il GRIN - Società Informatica Italiana. Tutte le pubblicazioni contenenti i risultati del progetto sono

Modalità	Si/No	Descrizione
		disponibili nel sito web http://www.sti.uniurb.it/nirvana/ insieme a tutte le presentazioni effettuate nelle quattro riunioni di progetto.

Realizzazione/partecipazione a eventi

Modalità	Si/No	Descrizione
Organizzazione di congressi	SI	Pur non essendo stati organizzati congressi in senso stretto sui temi del progetto, le tre unità di ricerca si sono alternate nell'organizzazione di riunioni di progetto aperte al pubblico, l'ultima delle quali è stata anche pubblicizzata presso il GRIN - Società Informatica Italiana e si è svolta con la possibilità di collegarsi da remoto. In ciascuna riunione sono stati presentati i risultati man mano ottenuti; inoltre, in quella iniziale sono stati richiamati i problemi da affrontare e in quella finale sono stati riepilogati i principali risultati. La riunione di apertura è stata organizzata a Fano dall'Unità di Ricerca di UniUrb nei giorni 09-11/02/2022. La prima riunione intermedia è stata organizzata a Mestre dall'Unità di Ricerca di UniVe nei giorni 05-07/06/2023. La seconda riunione intermedia è stata organizzata a Udine dall'Unità di Ricerca di UniUd nei giorni 06-08/06/2024. La riunione conclusiva è stata organizzata a Urbino dall'Unità di Ricerca di UniUrb nei giorni 29-31/05/2025.
Comunicazioni a congressi nazionali	SI	4) 7th Distributed Ledger Technology Workshop (DLT 2025) [2 comunicazioni]. 3) 6th Distributed Ledger Technology Workshop (DLT 2024) [2 comunicazioni]. 2) 24th Italian Conf. on Theoretical Computer Science (ICTCS 2023). 1) 21st Int. Conf. of the Italian Association for Artificial Intelligence (AIxIA 2022).
Comunicazioni a congressi internazionali	SI	24) Joint 22nd Int. Conf. on the Quantitative Evaluation of Systems and 23rd Int. Conf. on Formal Modeling and Analysis of Timed Systems (QEST/FORMATS 2025). 23) 45th Int. Conf. on Formal Techniques for Distributed Objects, Components, and Systems (FORTE 2025). 22) 19th ACM Int. Conf. on Distributed and Event-Based Systems (DEBS 2025). 21) 7th IEEE Int. Conf. on Blockchain and Cryptocurrency (ICBC 2025) [2 comunicazioni]. 20) 28th Int. Conf. on Foundations of Software Science and Computation Structures (FOSSACS 2025). 19) 17th EAI Int. Conf. on Performance Evaluation Methodologies and Tools (VALUETOOLS 2024). 18) 6th Int. Workshop on Artificial Intelligence and Formal Verification, Logic, Automata, and Synthesis (OVERLAY 2024). 17) 21st Int. Coll. on Theoretical Aspects of Computing (ICTAC 2024). 16) 32nd Int. Conf. on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS 2024). 15) Combined 31st Int. Workshop on Expressiveness in Concurrency and 21st Workshop on Structural Operational Semantics (EXPRESS/SOS 2024). 14) 16th Int. Conf. on Reversible Computation (RC 2024). 13) 44th Int. Conf. on Formal Techniques for Distributed Objects, Components, and Systems (FORTE 2024). 12) 20th European Computer Performance Engineering Workshop (EPEW 2024). 11) 6th IEEE Int. Conf. on Blockchain (BLOCKCHAIN 2023) [2 comunicazioni]. 10) 17th Int. Conf. on Reachability Problems (RP 2023). 9) 20th Int. Conf. on the Quantitative Evaluation of Systems (QEST 2023). 8) 21st Int. Conf. on Formal Modeling and Analysis of Timed Systems (FORMATS 2023). 7) 14th Int. Symp. on Games, Automata, Logics, and Formal Verification (GANDALF 2023). 6) 16th EAI Int. Conf. on Performance Evaluation Methodologies and Tools (VALUETOOLS 2023). 5) 25th Int. Conf. on Coordination Models and Languages (COORDINATION 2023). 4) 43rd Int. Conf. on Formal Techniques for Distributed Objects, Components, and Systems (FORTE 2023) [2 comunicazioni]. 3) 26th Int. Conf. on Foundations of Software Science and Computation Structures (FOSSACS 2023). 2) 19th Int. Conf. on the Quantitative Evaluation of Systems (QEST 2022).

Modalità	Si/No	Descrizione
		1) 42nd Int. Conf. on Formal Techniques for Distributed Objects, Components, and Systems (FORTE 2022).
Altro	SI	3) Relazioni di Marco Bernardo e Andrea Esposito sui temi del progetto al 4th Int. Workshop on Recent Advances in Concurrency and Logic (RADICAL 2025). 2) Relazione invitata di Marco Bernardo sui temi del progetto al 12th IFIP WG 1.8 Workshop on Trends in Concurrency Theory (TRENDS 2023). 1) Relazioni di Marco Bernardo, Andrea Esposito, Claudio A. Mezzina e Sabina Rossi sui temi del progetto al 4th Research Seminar on Open Problems in Concurrency Theory (OPCT 2023).

Divulgazione scientifica on-line

Modalità	Si/No	Descrizione
Creazione di siti	SI	L'Unità di Ricerca di UniUrb ha sviluppato e popolato di contributi il sito web http://www.sti.uniurb.it/nirvana/ in lingua inglese, articolato nelle sezioni Description, Research Units, Work Packages, Meetings, Publications e Documentation. In particolare, la sezione Meetings contiene il pdf delle presentazioni avvenute nelle quattro riunioni di progetto e in appositi seminari tenuti da relatori invitati, mentre la sezione Publications contiene il pdf di tutte le pubblicazioni apparse su riviste scientifiche e in atti di convegni, nonché di tesi di dottorato e rapporti tecnici, che riportano risultati del progetto e contengono un riferimento esplicito al finanziamento del progetto. Quest'ultima sezione verrà aggiornata nei prossimi mesi con tutti gli ulteriori lavori, attualmente in corso di revisione o preparazione, che verranno pubblicati.
Creazione di pagine web	NO	
Altro	SI	Per la riunione conclusiva del progetto, che si è tenuta a Urbino nei giorni 29-31/05/2025, è stata attivata la possibilità di collegarsi da remoto e di ciò è stata data notizia presso il GRIN - Società Informatica Italiana.

Note

Tabella riassuntiva delle spese sostenute per Unità Operativa

nº	Responsabile Scientifico	Spesa A.1	Spesa A.2.1	Spesa B	Spesa C	Spesa D	Spesa E	TOTALE
1.	**BERNARDO Marco**	106.268,16	23.890,04	78.094,92	0	0	37.543,78	**245.796,9**
2.	**ROSSI Sabina**	83.166,6	51.761,75	80.957,01	0	625,44	6.687,16	**223.197,96**
3.	**PIAZZA Carla**	68.017,65	47.778,75	69.477,84	0	0	2.253,15	**187.527,39**
	Totale	257.452,41	123.430,54	228.529,77	0	625,44	46.484,09	656.522,25

Risorse umane complessivamente ed effettivamente impegnate

	Mesi/persona TOTALE
A.1 – Personale dipendente a tempo indeterminato	28,571
A.2.1 - Personale non dipendente appositamente da reclutare solo se afferente all'Ateneo/ente sede dell'unità di ricerca	62
A.2.2 - Personale non dipendente: solo altro personale (acquisito con fondi liberi di ateneo)	19
Totale	109,571

28/08/2025 22:39