



Studio del Dust Attack: un attacco all'anonimato di Bitcoin

Candidato:

Jacopo Raffi

Relatori/Relatrici:

Prof.ssa Laura Emilia Maria Ricci

Prof. Damiano Di Francesco Maesa

Università di Pisa

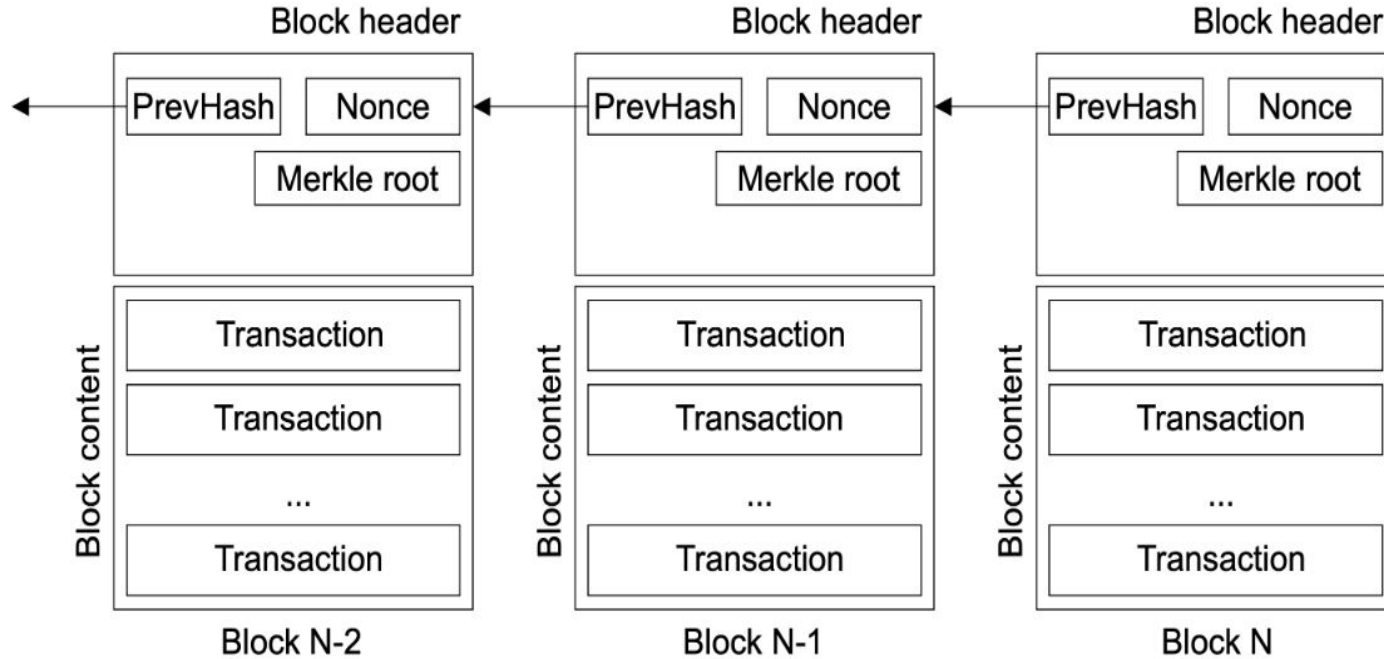
Dipartimento di Informatica

Corso di Laurea Triennale in Informatica

A.A. 2021/2022



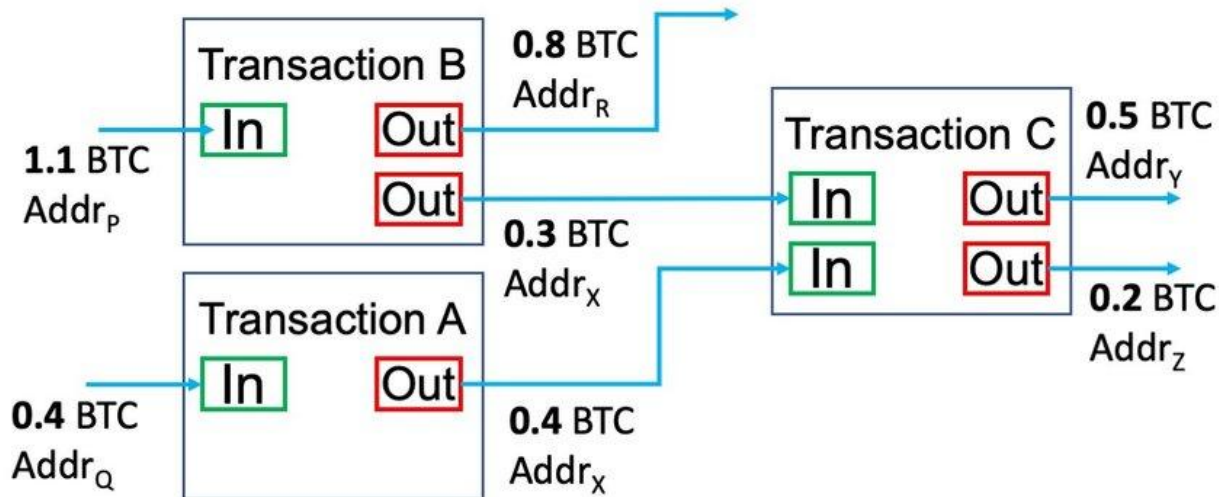
Blockchain di Bitcoin





Transazioni in Bitcoin

- Possono avere zero o più input, uno o più output;
- Gli output hanno associato uno script;
- Hanno una fee, la minima fee è denominata *minimum relay fee*.





Anonimato in Bitcoin

- Bitcoin è pseudo-anonimo:
 - Ogni utente utilizza un numero arbitrario di indirizzi.
- Esistono attacchi basati sull'analisi delle transazioni;
- Questi attacchi sfruttano determinate euristiche:
 - Per esempio l'euristica “multi-input”.

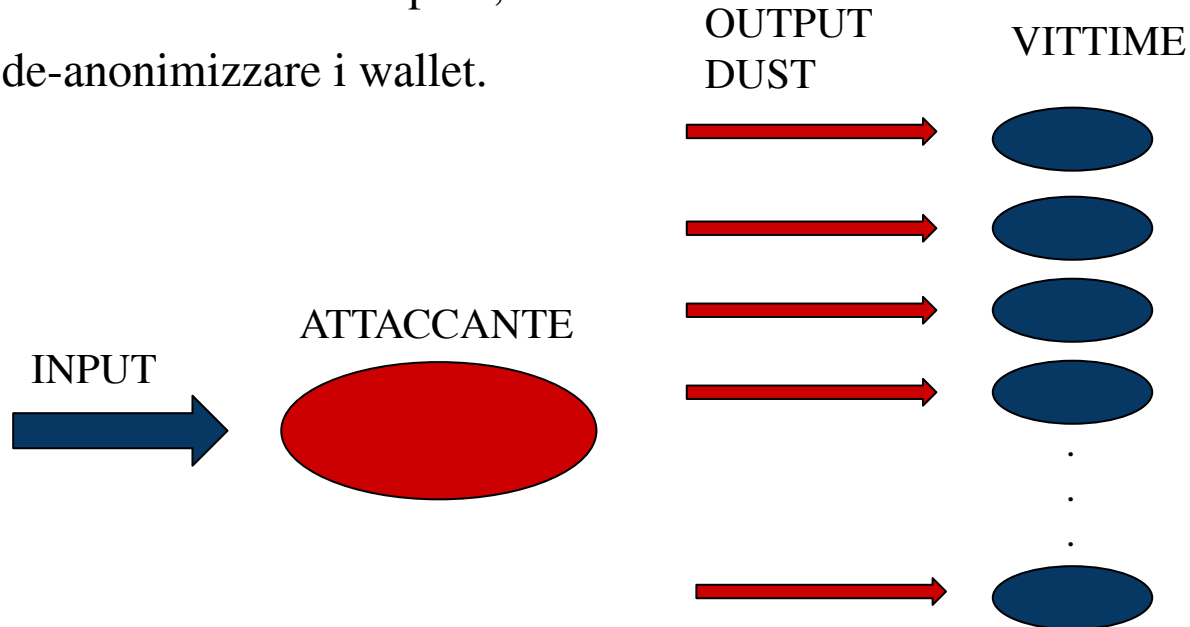


Bitcoin Dust

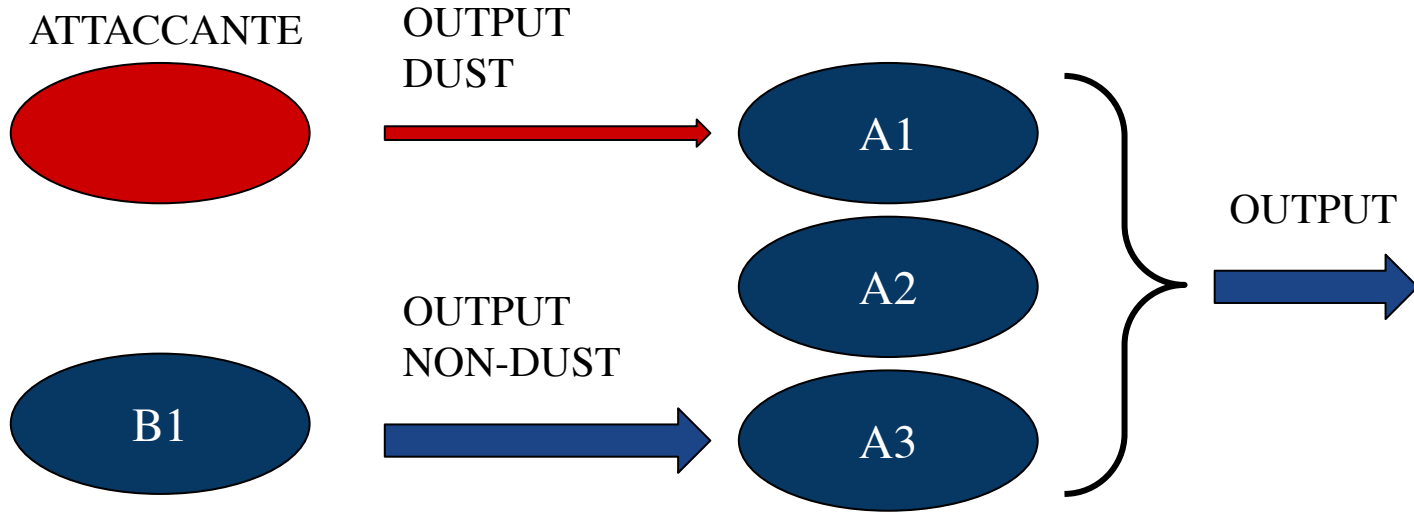
- Piccola quantità di criptovaluta inferiore alla *minimum relay fee*;
- Gli importi minori di 546 satoshi sono considerati *dust*:
 - 1 satoshi = 10^{-8} BTC;
 - 1 satoshi = 0.00016 € (27/11/2022).
- Possibili utilizzi:
 - Satoshi Dice;
 - Scrittura di dati arbitrari (script OP_RETURN);
 - Dust Attack.

Dust Attack

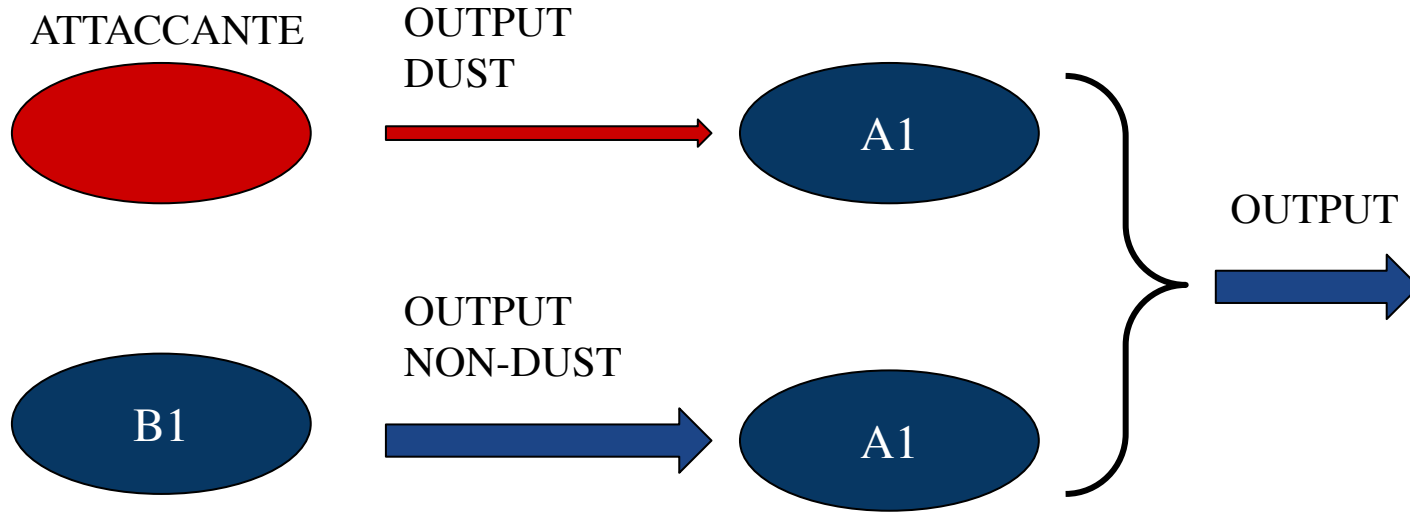
- È basato sull'invio del dust;
- Utilizza l'euristica “multi-input”;
- Mira a de-anonimizzare i wallet.



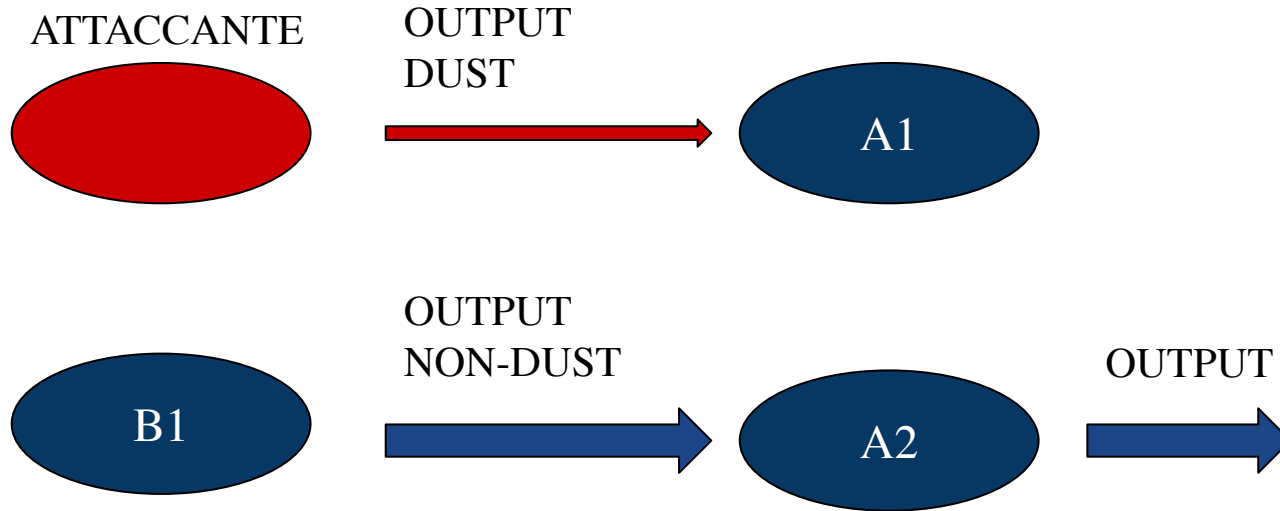
Attacco di Successo



Attacco Fallito - Caso 1



Attacco Fallito - Caso 2





Conseguenze e Contromisure

Conseguenze:

- Maggior tracciabilità;
- È necessario de-anonimizzare solo un indirizzo (tramite gli *exchange*).

Contromisure:

- Non spendere il dust;
- Utilizzare servizi di “Dust Collecting”.



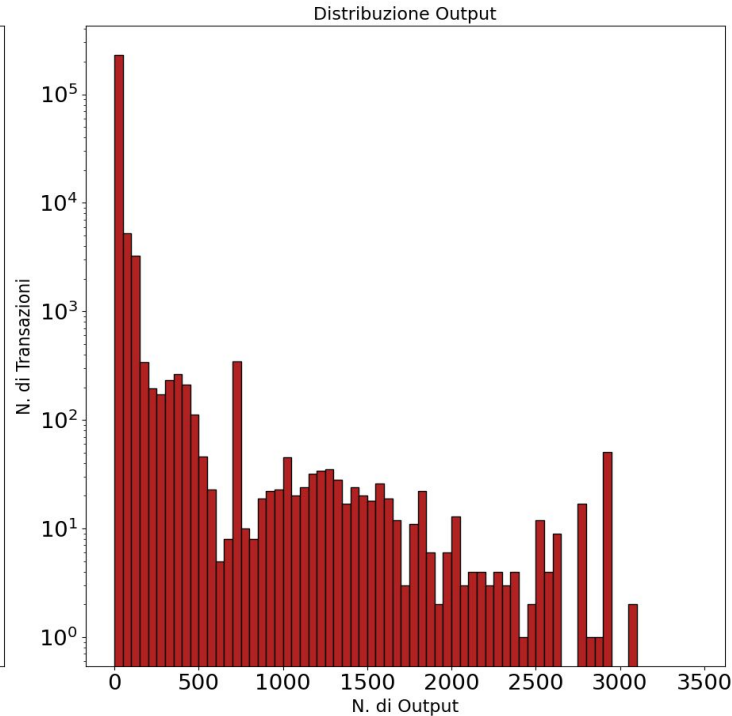
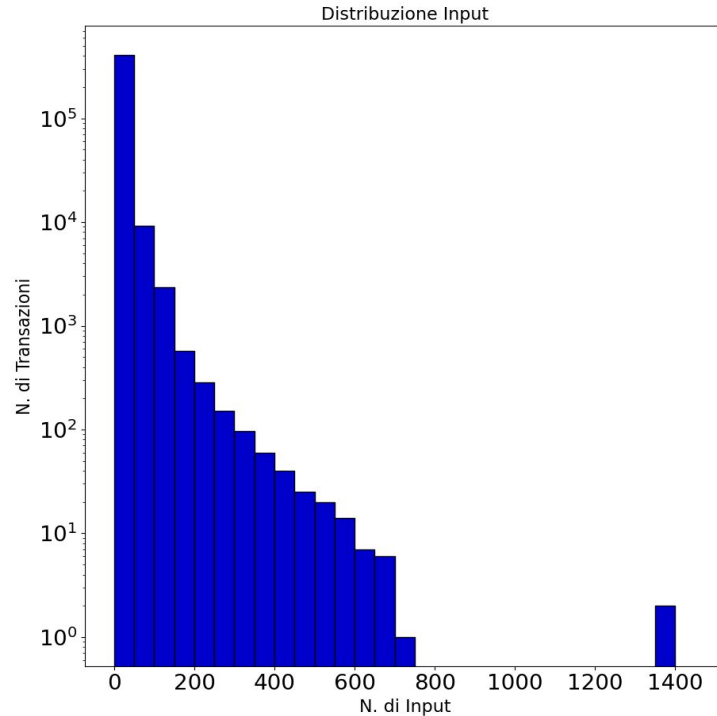
Analisi dei Dati

- Transazioni dal 3 Gennaio 2009 al 10 Agosto 2017:
 - Transazioni totali: 245 410 083.
- Considerate solo transazioni contenenti input e/o output dust:
 - Importo compreso nell'intervallo $[1, 545]$;
 - Transazioni dust: 2 114 335 (0.8% del totale).
- Filtraggio transazioni generate da Satoshi Dice:
 - Transazioni generate da Satoshi Dice: 1 465 295 (69% delle transazioni dust).



Distribuzione del Dust

- Intervalli di ampiezza 50;
- Primo intervallo $[1, 50]$.

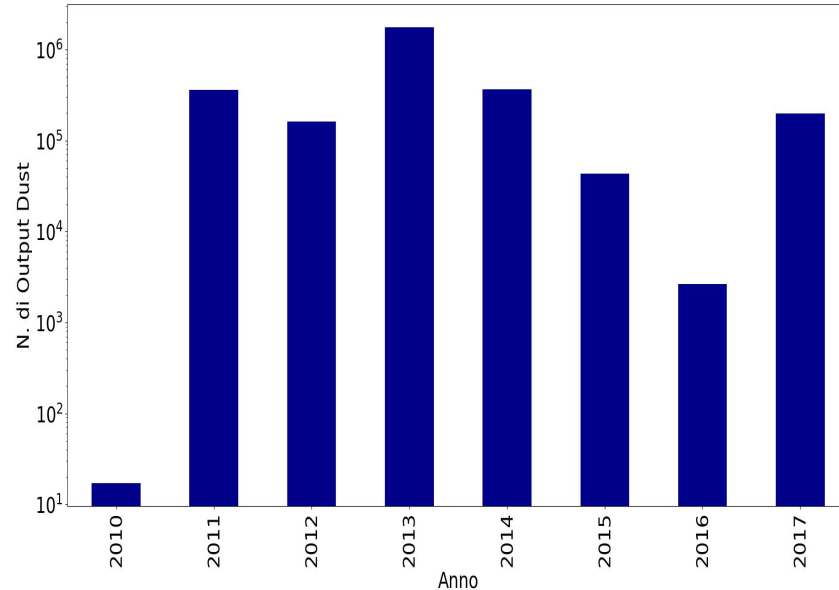




Dust negli anni

- Filtrati gli output con script
OP_RETURN;
- Totale output dust generati:
2 893 877.

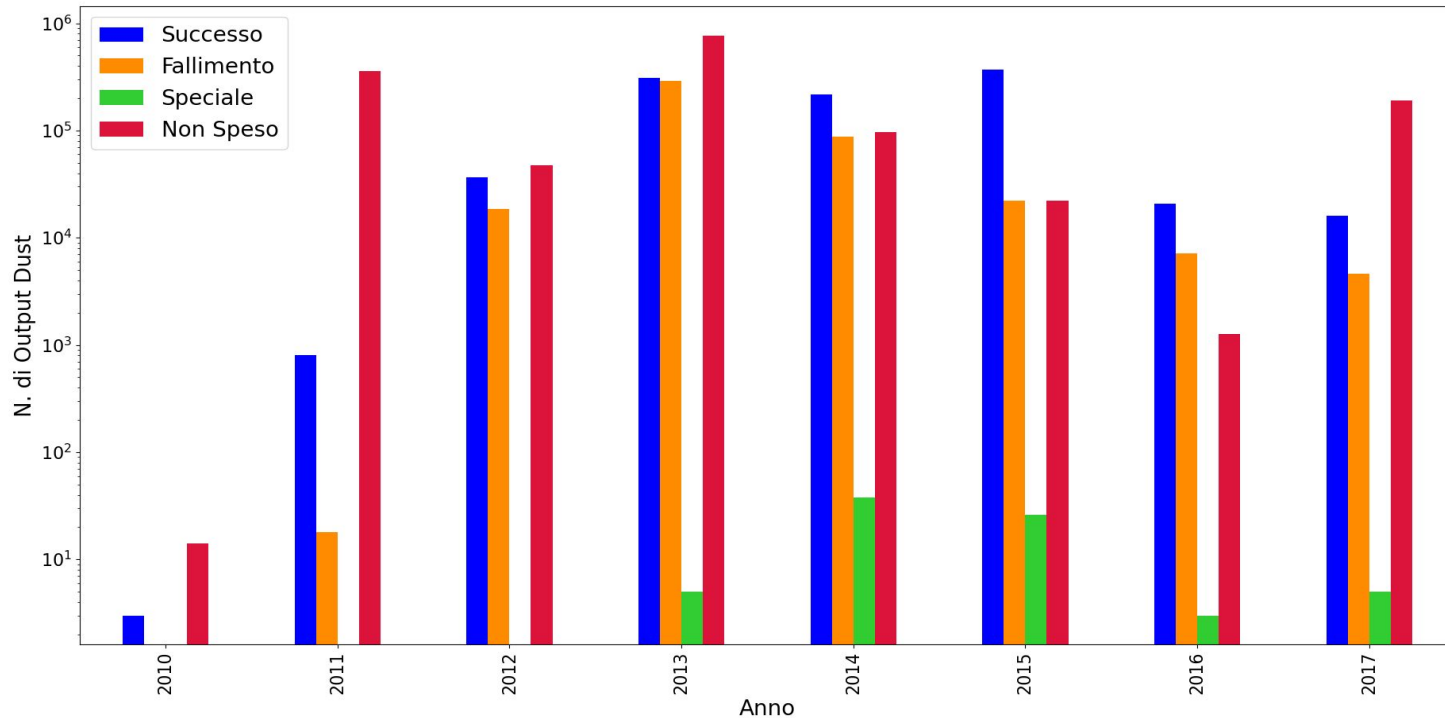
- Fenomeno “Enjoy Sochi”:
 - 2014: 48 750 output;
 - 2015: 17 250 output;
 - 2017: 189 495 output.



- *1Enjoy1C4bYBr3tN4sM KxvvJDqG8NkdR4Z;*
- *1SochiWwFFySPjQoi2biVftXn8NRPCSQC.*

Classificazione del Dust

- Dust non speso: 51.5 %;
- Dust speso: 48.5 %.





Classificazione delle transazioni

- Il dust è stato speso in 263 963 transazioni;
- Queste transazioni sono divise in tre categorie:
 - 2+ indirizzi;
 - 1 indirizzo;
 - Speciale.

2+ indirizzi	63.2 %
1 indirizzo	36.7%
Speciale	0.1 %



Categoria 1 indirizzo

- Transazioni totali: 97 040;
- Le transazioni sono divise in:
 - NOD: Not Only Dust;
 - OD: Only Dust.

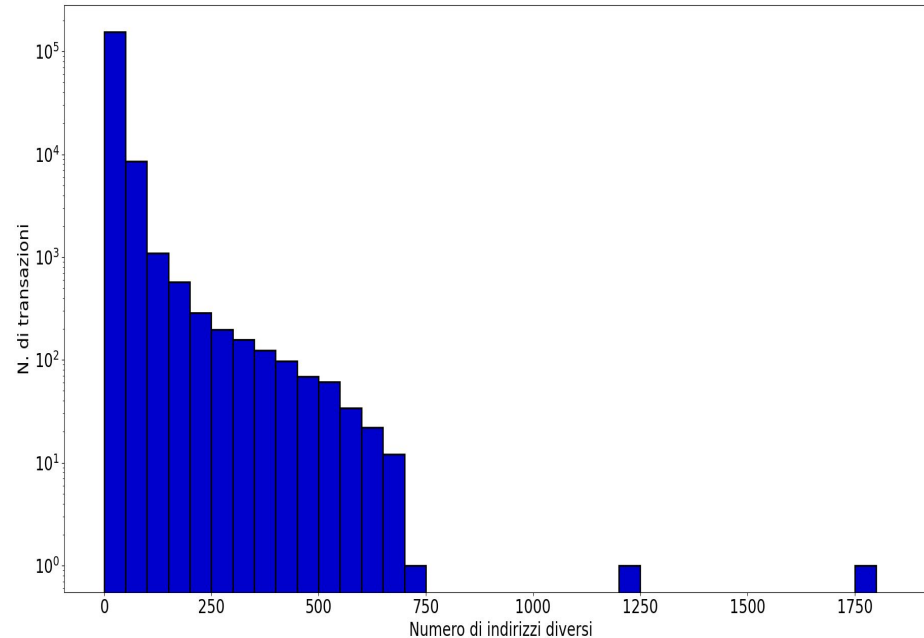
NOD	92 712	95,5 %
OD	4 328	4,5 %

- Categoria OD:
 - *1JwSSubhmg6iPtRjtyqhUYYH7bZg3Lfy1T*
(1 569 transazioni);
 - *1PEDJAibfNetJzM289oXsW1qLAgjYDjLgN*
(1 835 transazioni).



Categoria 2+ indirizzi

- 166 906 transazioni totali:
 - NOD: 99.9 %;
 - OD: 0.1 %.
- Media indirizzi diversi in una singola transazione: 13.





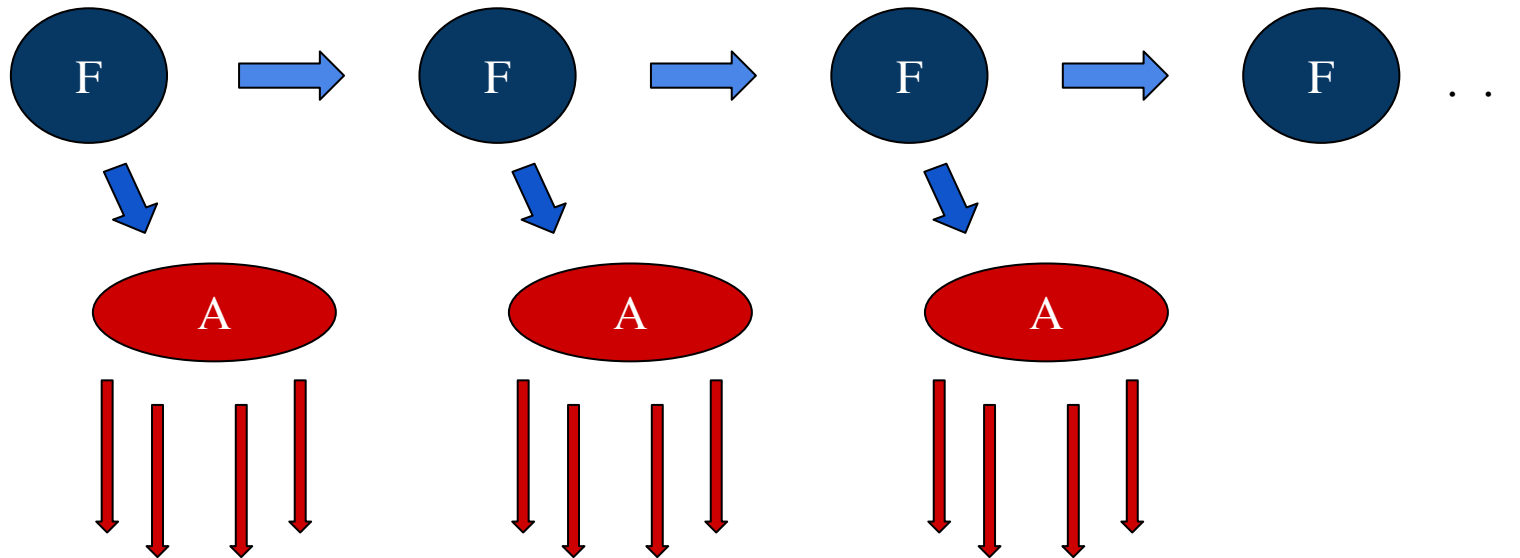
Analisi Indirizzi

- Output dust generati: 2 893 877;
- Gli indirizzi destinatari sono 1 059 836:
 - 312 114 indirizzi (29 % dei destinatari) hanno speso il dust;
 - 259 252 indirizzi (83 % di chi ha speso il dust) lo hanno speso nella categoria “2+ Indirizzi”.
- Transazioni che generano almeno un dust della categoria “Successo” sono 98 198:
 - 58 146 transazioni (59 %) non presentano indirizzi nuovi tra gli output.



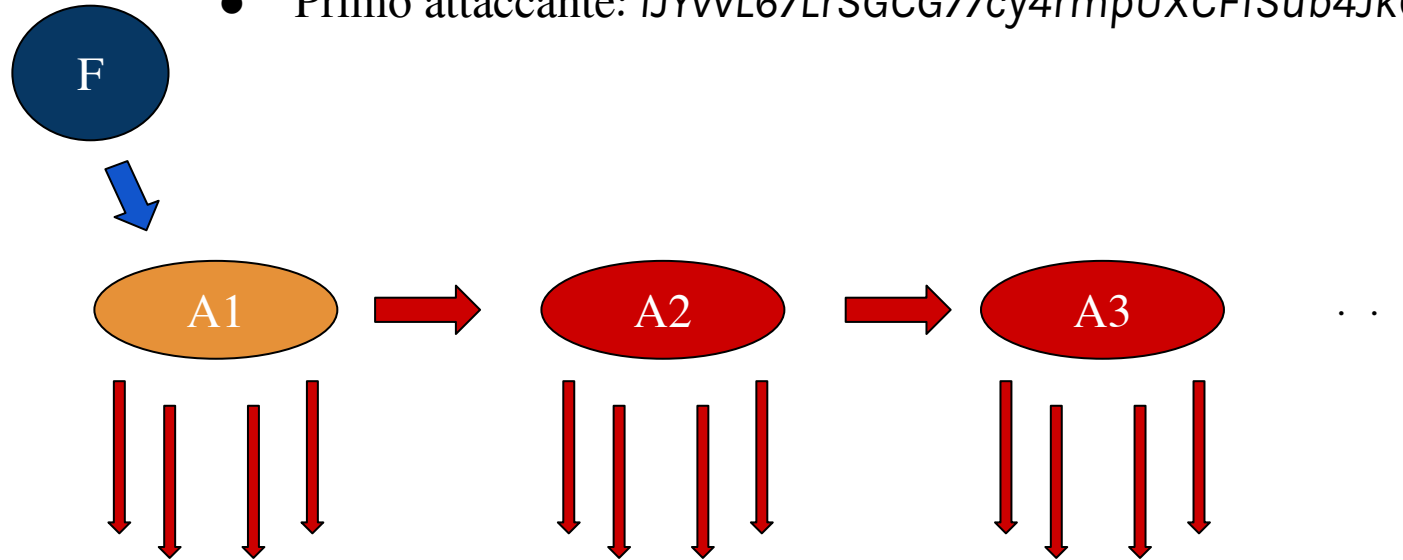
Pattern: Un finanziatore - un attaccante

- Attaccante: *1DiRy9Giiq1GCkAD7VMSrXoKVe2dimnovm;*
- Finanziatore: *1Nj3AsYfhHC4zVv1HHH4FzsYWeZSeVC8vj.*



Pattern: Un finanziatore - più attaccanti

- Primo attaccante: 1JYvvL67LrSGCG77cy4rmpUXCFfSub4JkG.





**Grazie a tutti per
l'attenzione.**

Ringrazio inoltre
la Prof.ssa Ricci,
il Prof Di Francesco e
Il Dott. Loporchio
per tutta la disponibilità che
hanno avuto nei miei confronti.