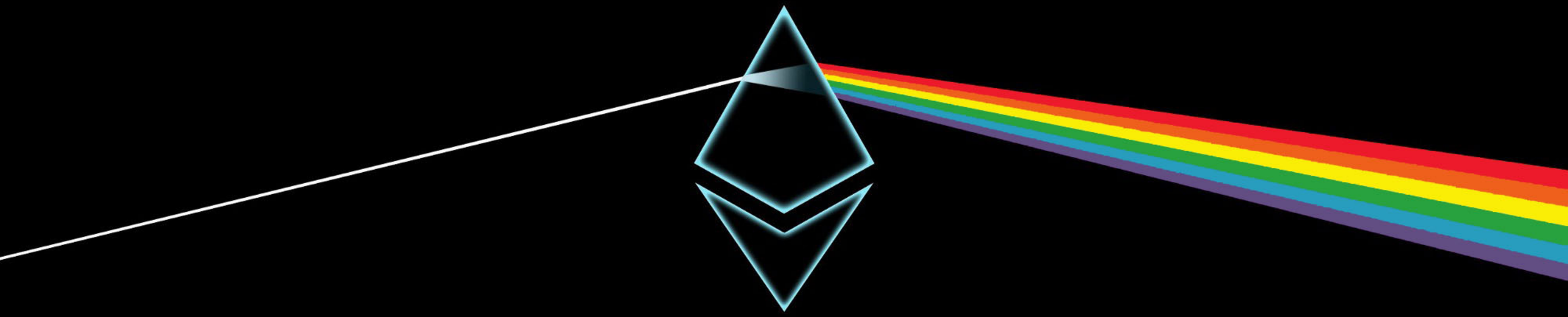
# COSTRUZIONE ED ANALISI DEL GRAFO DELLE TRANSAZIONI DI ETHEREUM

Università degli studi di Pisa - Dipartimento di Informatica - Anno Accademico 2017/18




Relatori:

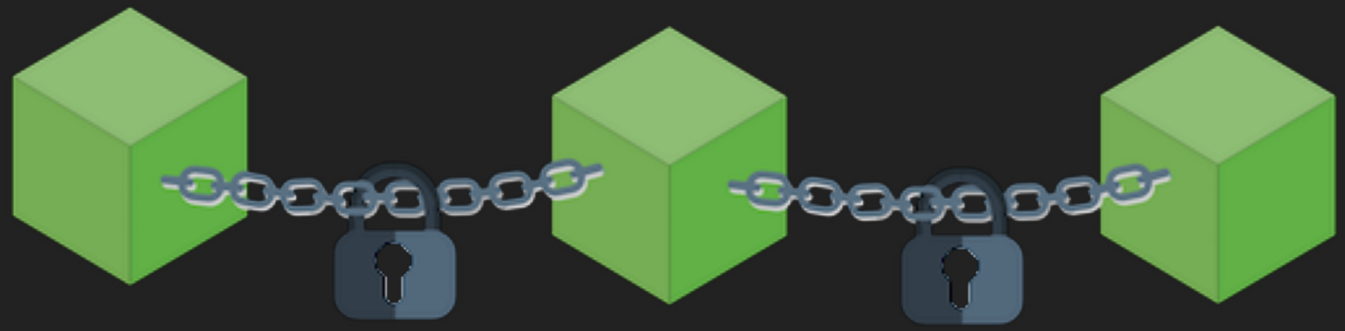
Laura Ricci
Damiano Di Francesco Maesa

Candidato:

Luca Corbucci

# OBIETTIVI DEL TIROCINIO

# LA BLOCKCHAIN



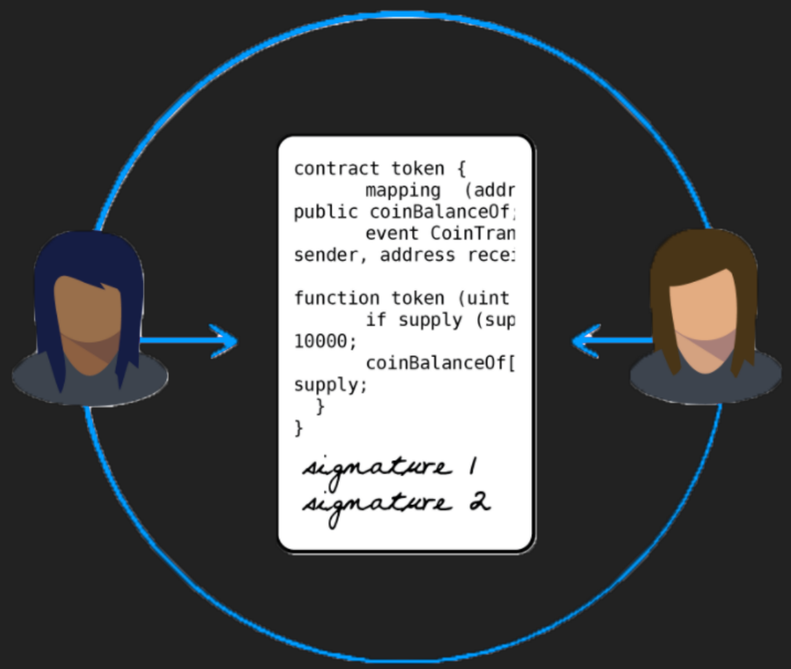
La blockchain è una struttura dati decentralizzata e pubblica. I dati vengono memorizzati in blocchi. A differenza dei normali database è possibile solamente inserire nuovi dati o leggere quelli già presenti.

# DUE APPLICAZIONI DELLA BLOCKCHAIN

- I nodi della rete Bitcoin si scambiano valuta digitale, le transazioni vengono registrate nella blockchain.

- Nella blockchain di Ethereum non vengono memorizzate solamente le transazioni tra gli utenti ma anche le chiamate ai contratti

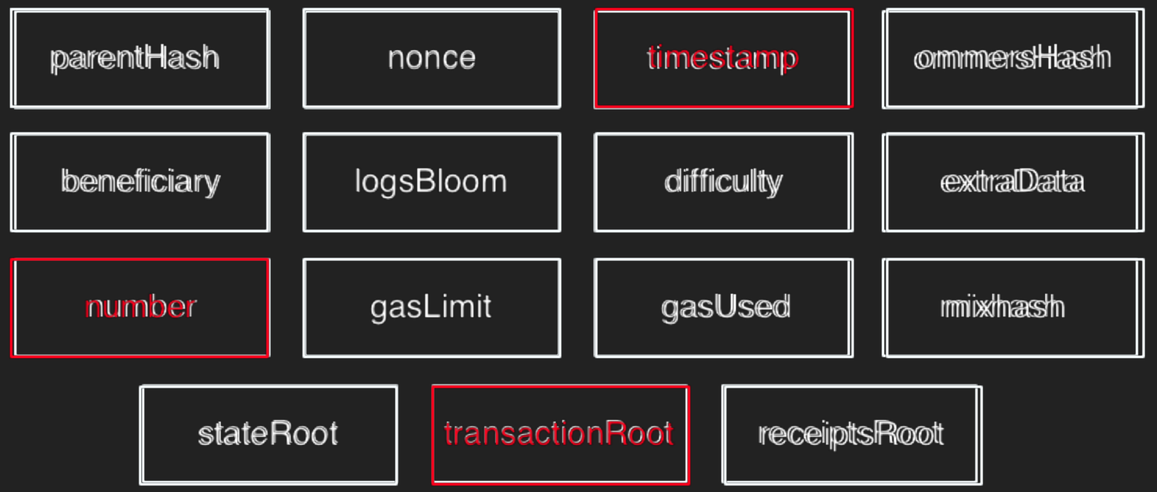
# ETHEREUM




- Presentato nel 2013 e lanciato nel 2015. Ethereum innalza la blockchain ad un livello più alto introducendo gli smart contract.
- Uno smart contract include del codice di una complessità arbitraria, viene eseguito nel momento in cui un utente invia una transazione verso l'indirizzo del contratto.
- Il codice del contratto viene eseguito su tutti i nodi della rete. Per questo motivo Ethereum è anche chiamato "The World Computer"

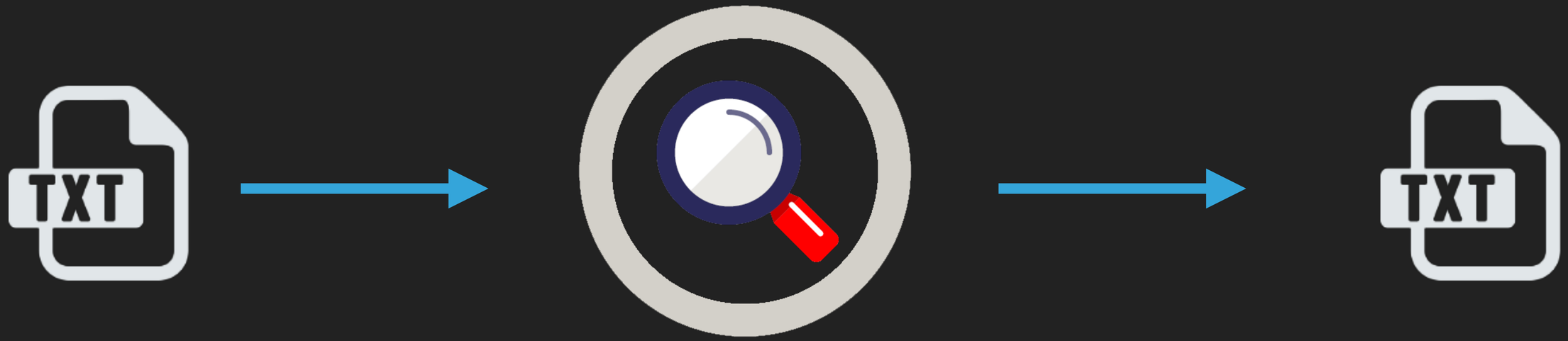
# STRUTTURA DI BLOCCHI E TRANSAZIONI

## Struttura di un blocco




## Struttura di una transazione

# PARSING DELLE TRANSAZIONI: UNA PRIMA SOLUZIONE




Lettura dei blocchi dal file

Parsing dei blocchi

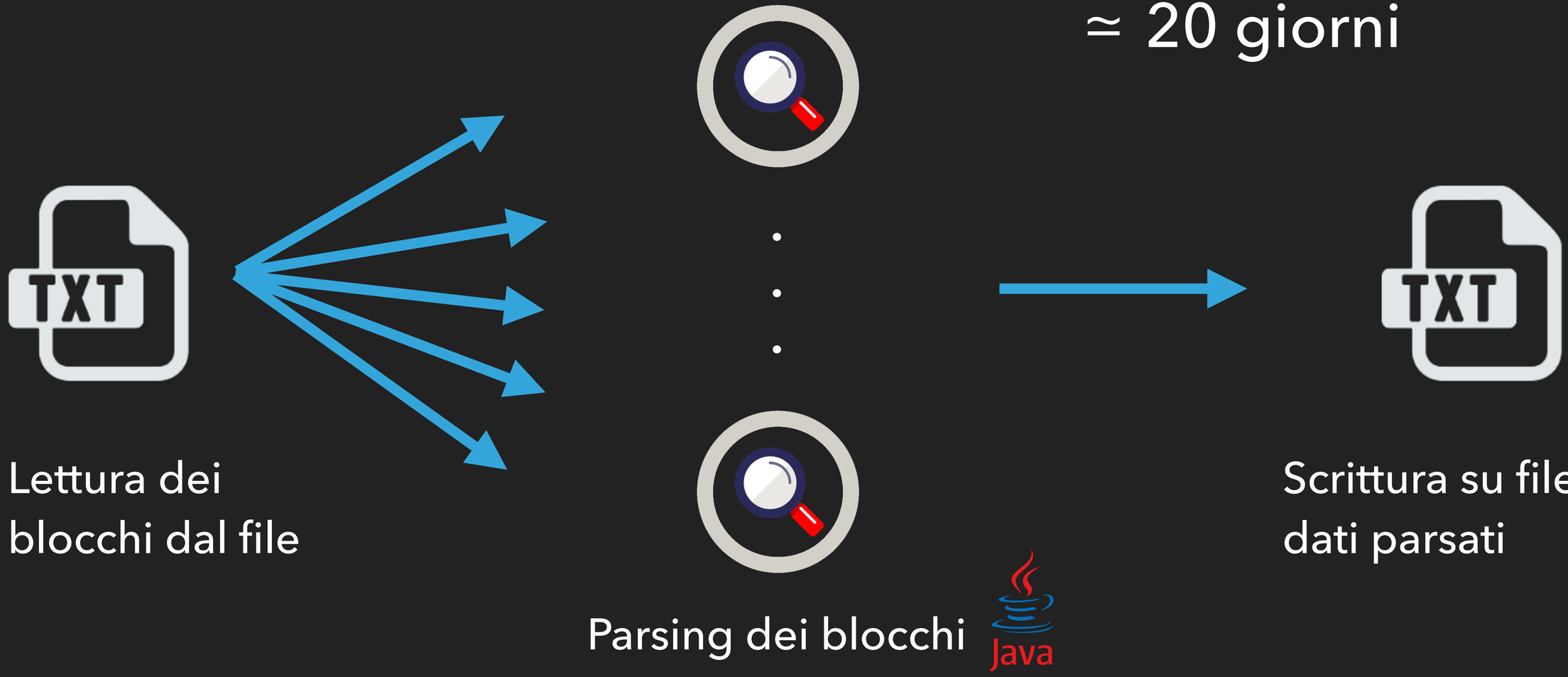
Java

Scrittura su file dei dati parsati

≃ 150 giorni

# PARSING DELLE TRANSAZIONI: UNA PRIMA SOLUZIONE

≃ 20 giorni

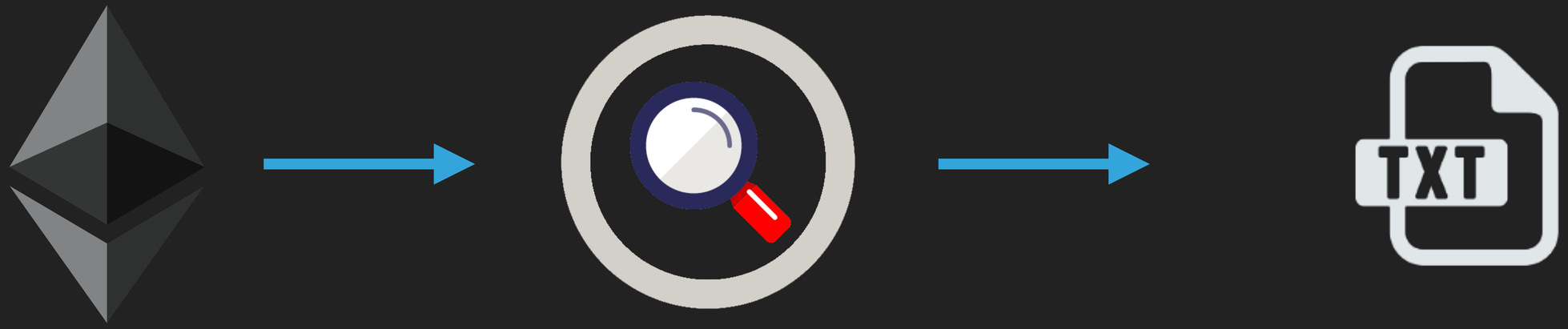



Lettura dei blocchi dal file

Parsing dei blocchi

Scrittura su file dei dati parsati

# PARSING DELLE TRANSAZIONI: SECONDA SOLUZIONE




Sincronizzazione della blockchain con Geth

Estrazione dai dati tramite la console di Geth

Scrittura su file dei dati parsati

≃ 30 giorni

# CONFRONTO TRA I DUE METODI

| | Parser in Java | Geth e Javascript |
|---|---|---|
| Pro | Velocità accettabile per l'estrazione dei dati dal file passato come parametro. | Possibilità di ottenere lo status per ogni transazione presente nella blockchain |
| Contro | Impossibile recuperare lo status delle transazioni. | Minore velocità nell'estrazione dei dati rispetto al parser in Java. |

# DIVISIONE DEL DATASET

- I dati ottenuti dopo la fase di parsing sono stati analizzati creando vari grafi:

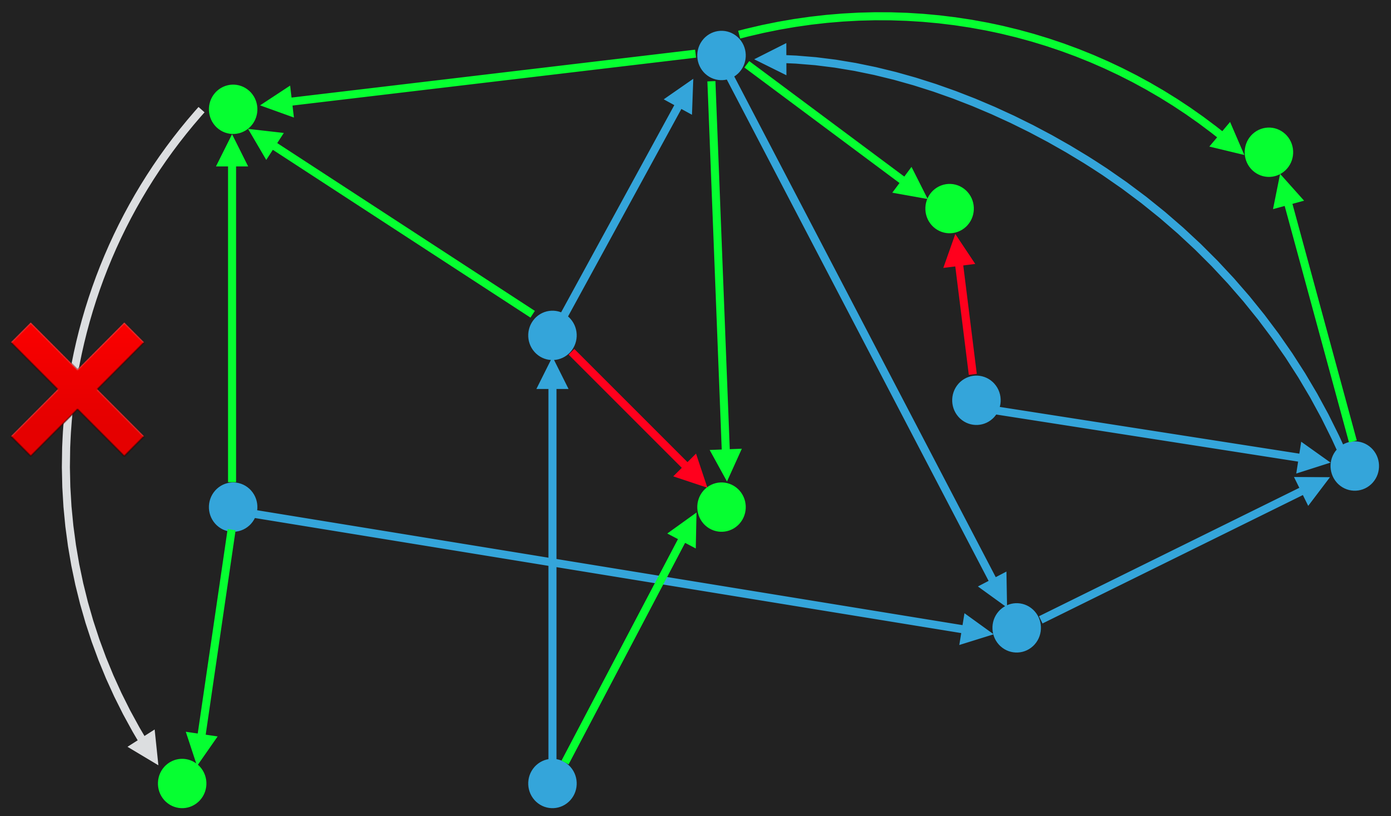

File ottenuto dal parsing della blockchain

Grafo che rappresenta tutte le transazioni

Grafi costruiti suddividendo il dataset in base al timestamp dei blocchi

Grafi costruiti dividendo le transazioni in base al tipo

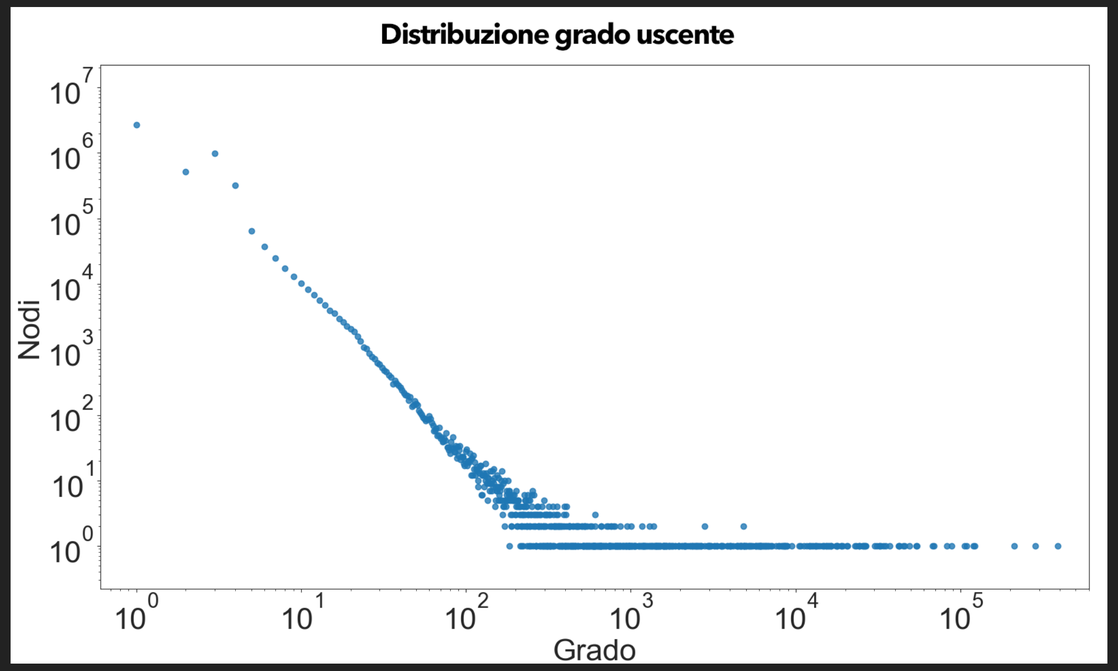
# CREAZIONE DEL GRAFO DELLE TRANSAZIONI

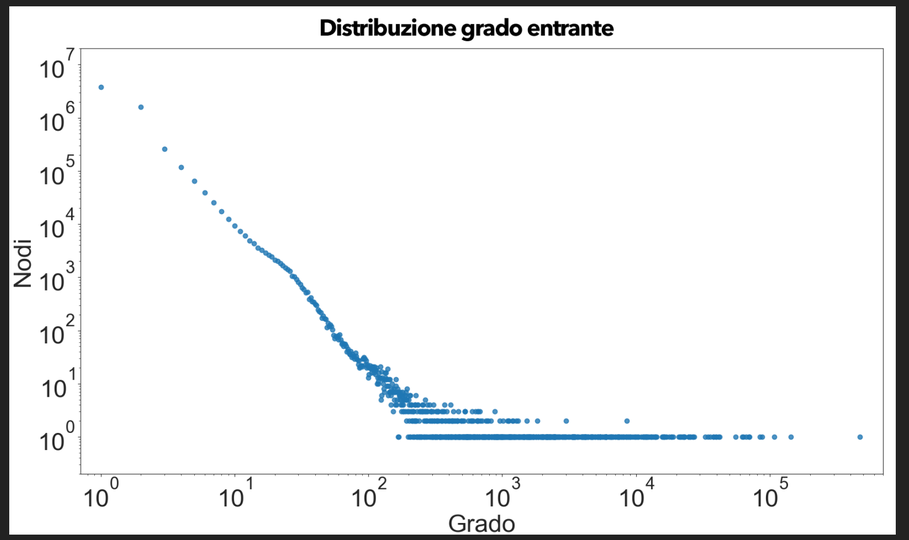


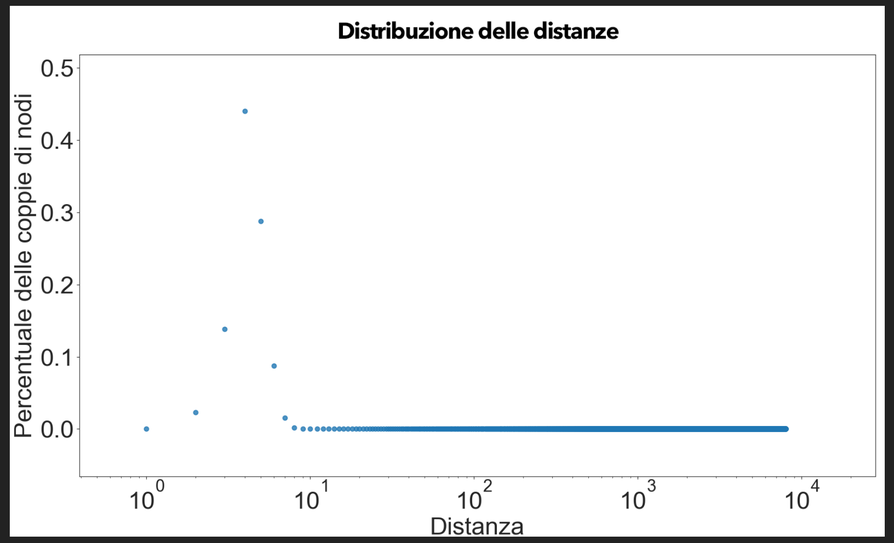
- Nel nostro grafo i nodi rappresentano gli indirizzi degli account della rete Ethereum.
- Gli archi rappresentano le transazioni tra utenti, le chiamate verso un contratto o la creazione di un nuovo contratto.
- Sono escluse dal grafo le transazioni da contratto a contratto
- Per ogni coppia di nodi inseriamo un solo arco anche se sono presenti più transazioni

# RISULTATI DELL'ANALISI SUL GRAFO COMPLETO

- 4237648  blocchi analizzati
- 6081755 nodi
- 7224840 archi



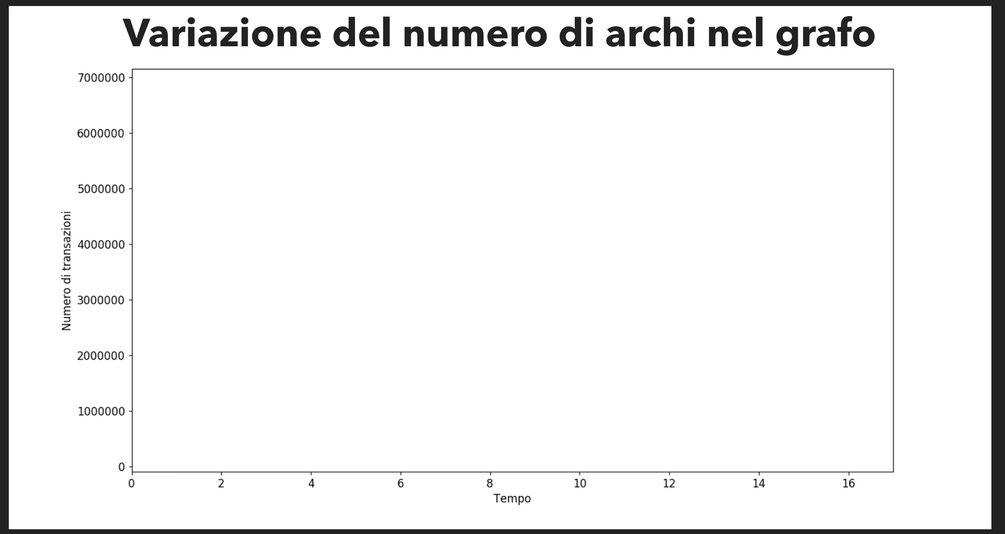
# ANALISI DELLA CENTRALITÀ NEL GRAFO COMPLETO

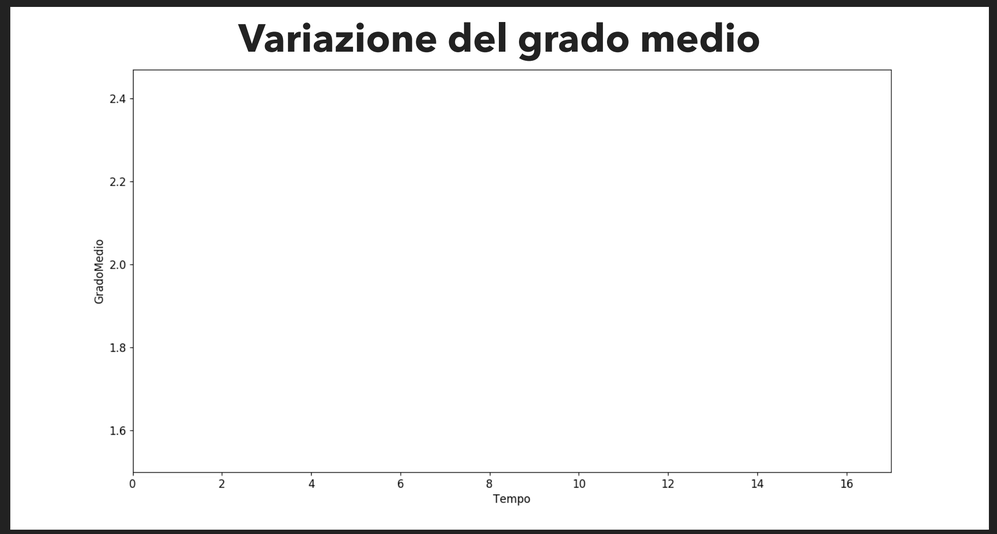
| Nome account | Archi entranti |
|---|---|
| Bittrex_1 | 390346 |
| Poloniex_1 | 285307 |
| 0xb42b20ddbeabdc2a288be7ff847ff94fb48d2579 | 210984 |
| Ethermine | 122359 |
| Kraken_4 | 119312 |
| ShapeShift | 108719 |
| Yunbi_2 | 105605 |
| Nanopool | 88463 |
| Yunbi_1 | 82843 |
| Freewallet | 69055 |

| Nome account | Centralità armonica |
|---|---|
| Poloniex_1 | 2037051.1 |
| Bittrex_1 | 1967112.5 |
| Freewallet | 1764614.1 |
| Kraken_4 | 1729339.6 |
| ShapeShift | 1725644.1 |
| Bitfinex_1 | 1671783.1 |
| 0x563b377a956c80d77a7c613a9343699ad6123911 | 1611149.1 |
| Ethermine | 1590653.1 |
| DwarfPool_1 | 1590188.2 |
| 0x22b84d5ffea8b801c0422afe752377a64aa738c2 | 1580784.5 |

# RISULTATI DELLE ANALISI TEMPORALI (1)

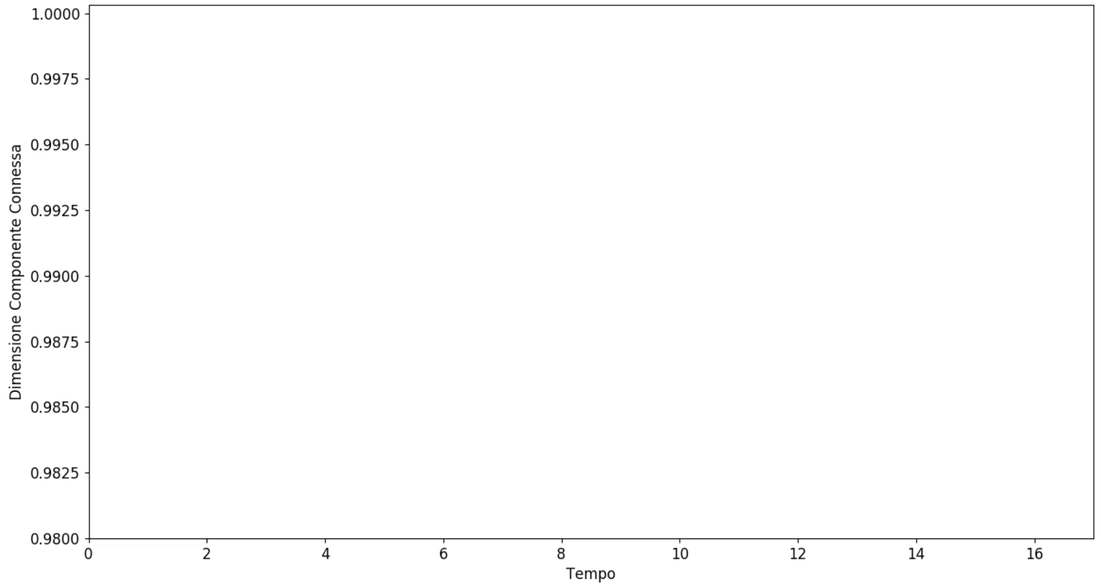
- 17 Snapshot temporali
- Ogni snapshot ≃ 44 giorni

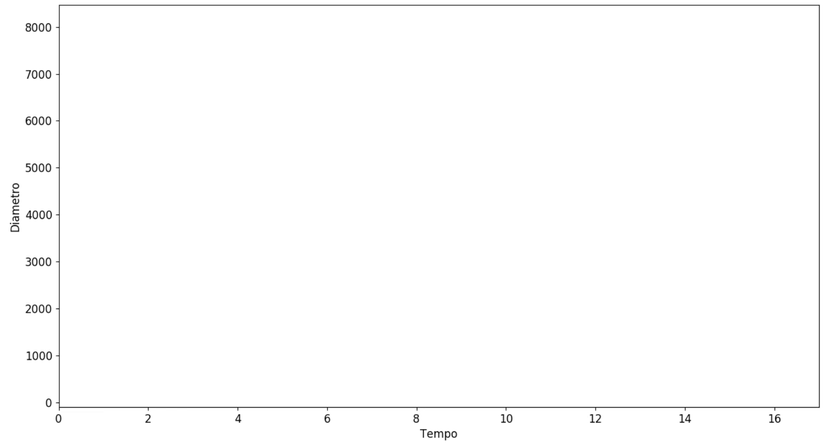



# RISULTATI DELLE ANALISI TEMPORALI (2)

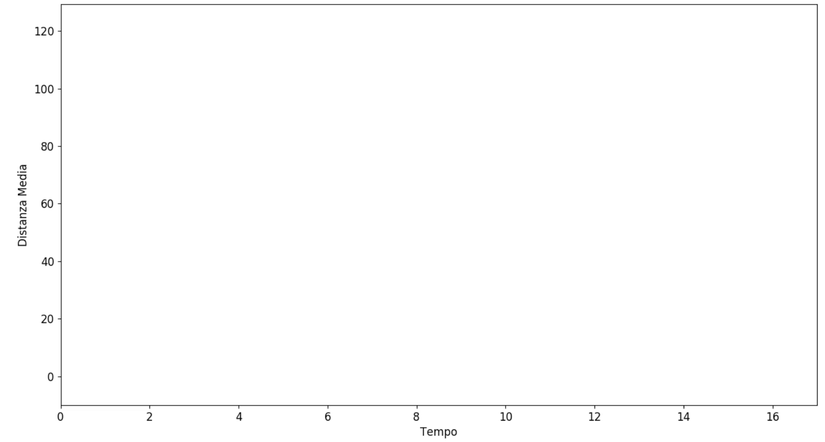
## Frazione di nodi nella componente connessa più grande




## Variazione del diametro

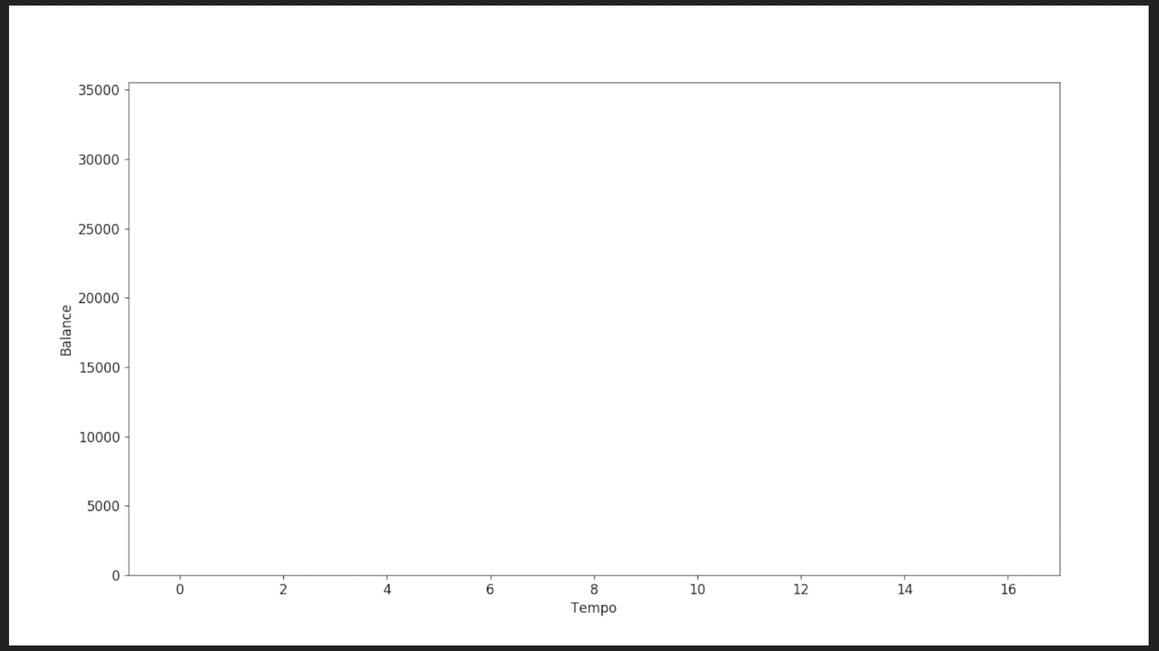



## Variazione della distanza media

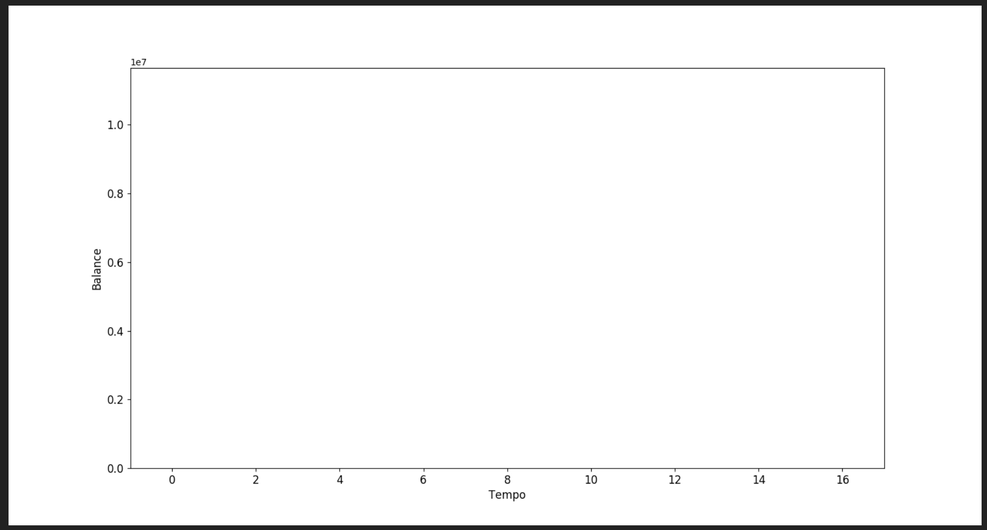


# ACCOUNT PIÙ ATTIVI NEGLI SNAPSHOT

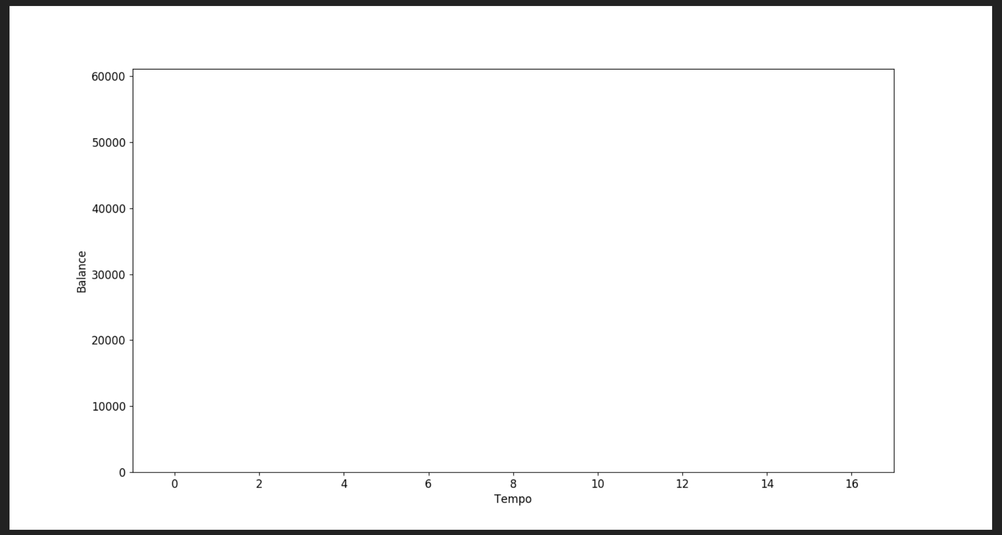
Evoluzione del balance degli account relativi a ShapeShift




Evoluzione del balance dell'account "The Dao"

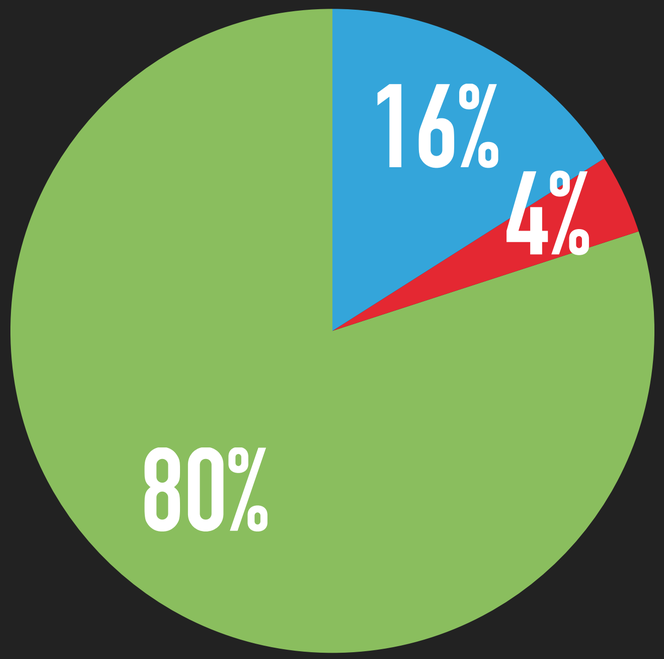


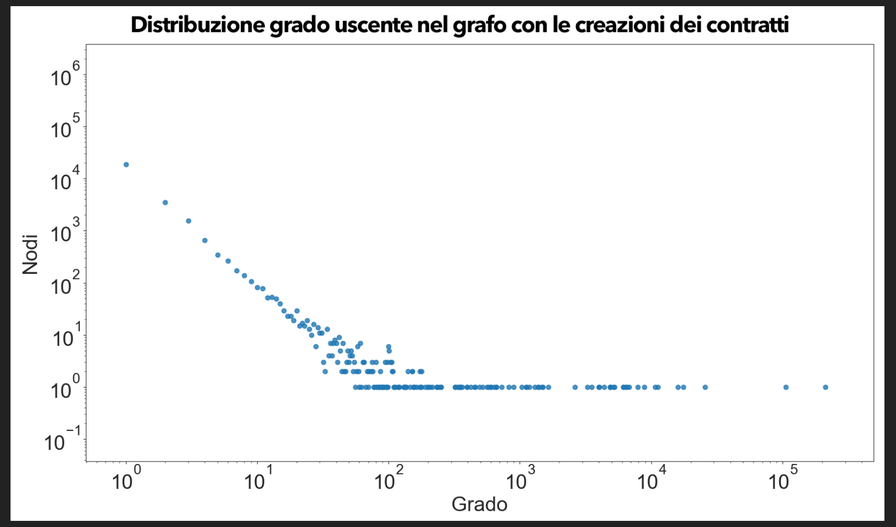

Evoluzione del balance dell'account "Cryptsy"

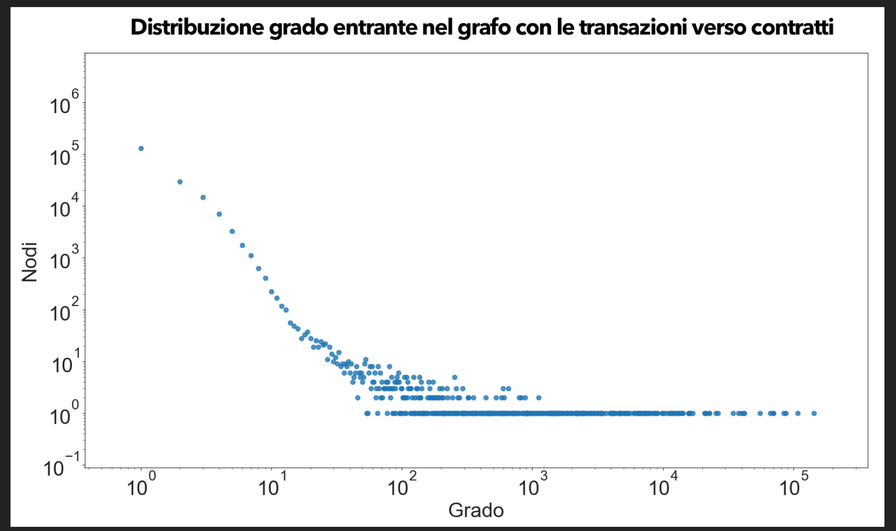


# RISULTATI DELL'ANALISI SUL GRAFO DIVISO IN BASE AL TIPO DELLE TRANSAZIONI

- Transazioni verso contratti
- Creazioni di contratti
- Transazioni tra utenti esterni



# ANALISI DELLE CHIAMATE AI CONTRATTI

| Nome Contratto | Chiamate |
|---|---|
| Bittrex_2 | 143738 |
| Kraken_5 | 107762 |
| Poloniex_3 | 87302 |
| EOSTokenContract | 84275 |
| Golem | 70277 |
| Bitfinex_2 | 69510 |
| ReplaySafeSplit | 66499 |
| 0x331d077518216c07c87f4f18ba64cd384c411f84 | 55276 |
| EtherDelta_2 | 41942 |
| TheDAO | 41469 |

- Nel grafo con le sole transazioni verso contratti, tramite lo studio della centralità in base agli archi entranti è stato possibile ottenere una lista degli smart contracts che hanno ricevuto più chiamate dagli utenti

# LAVORI FUTURI

- Estendere l’analisi ai blocchi non ancora estratti dalla blockchain
- Studiare altre proprietà del grafo tra cui "Rich get Richer” per il grafo delle transazioni di Ethereum

# Grazie per l'attenzione.

Domande?