UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
Scuola Politecnica e delle Scienze di Base
Corso di Laurea in Ingegneria Informatica

tesi di laurea triennale

Analysis of blockchain technologies and benchmarking of NXT and Ethereum in emulated network environment

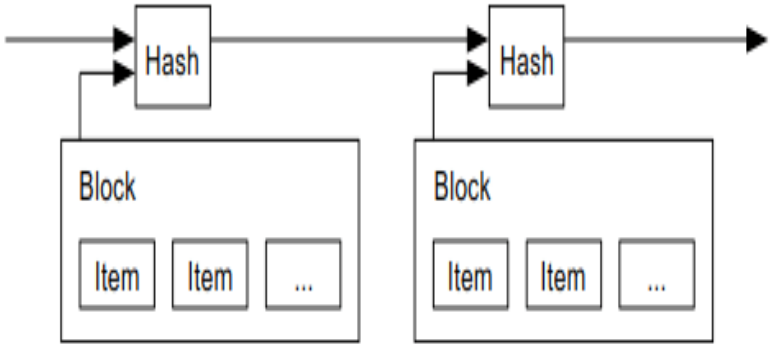
2019/2020

relatore
prof. Giuseppe Aceto

candidato
Marco Carlo Feliciano
Matr. N46003714

Contesto e contributo

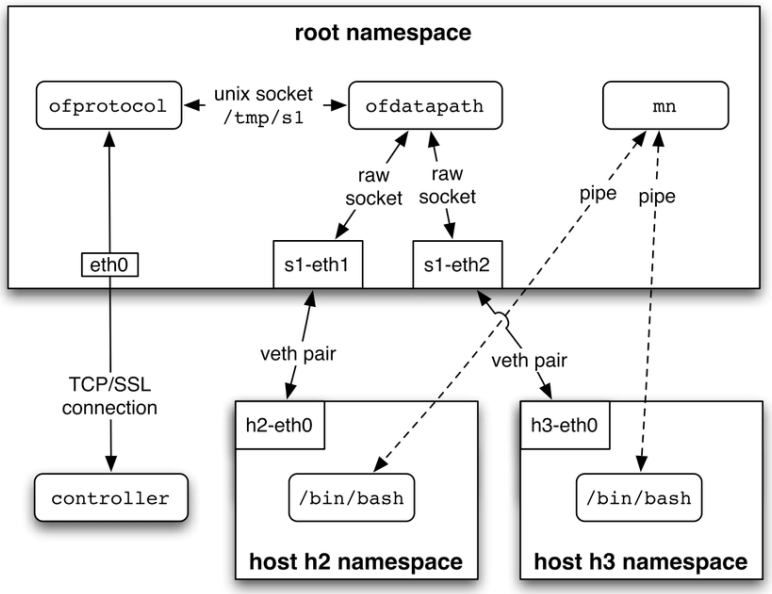
- **Contesto: discussione generale sulle tecnologie blockchain**
  - Introduzione
  - Cenno ai meccanismi di consenso di NXT ed Ethereum
  - Cenno alle metriche di performance
- **Contributo: confronto con Caliper, parte sperimentale**
  - Testbed di emulazione di rete
  - Cenno all'implementazione dei test
  - Definizione della test suite
  - Risultati sperimentali
- **Conclusioni**
- **Bibliografia**



Cos'è una blockchain, e a cosa serve?

Elementi che caratterizzano una blockchain:

- **Blocchi**
- Account
- **Meccanismi di consenso**
  - NXT: **Proof of Stake**
  - Ethereum: **Proof of Authority**
- Comportamento dei **client**, in relazione al CAP Theorem
- Transazioni
  - **Transaction throughput**

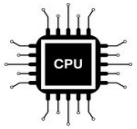


Testbed di emulazione di rete: Mininet

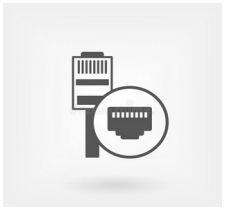
- Permette di creare **topologie custom**
- **Host e switch** sono dei processi shell, ciascuno con il suo **network namespace**: scalabilità
- C'è una pipe dal parent process, cioè "**mn**", alla shell di ogni host
- Supporto nativo ad SDN con gli OpenFlow datapath
- Portabilità degli esperimenti: VM Ubuntu con tutte le dipendenze di Mininet pre-installate

Parametri d'ambiente

- **Hardware allocato alla VM:**
  - un core da 2.3 GHz con due thread
  - 2 GB di RAM DDR4
  - hard disk SSD con throughput misurato di 3.1 GB/s



- **Congestione assegnata alle interfacce virtuali di rete degli host:**
  - Ritardo: media di 50 ms, jitter di 10 ms con distribuzione gaussiana, 25% di correlazione tra pacchetti consecutivi
  - Perdita di pacchetti: 10% di probabilità, 65% di probabilità di burst in caso di perdita
  - Corruzione di un bit: 0.01% di probabilità
  - Riordinamento di pacchetti: 10% di probabilità
  - Duplicazione di pacchetti: 5% di probabilità



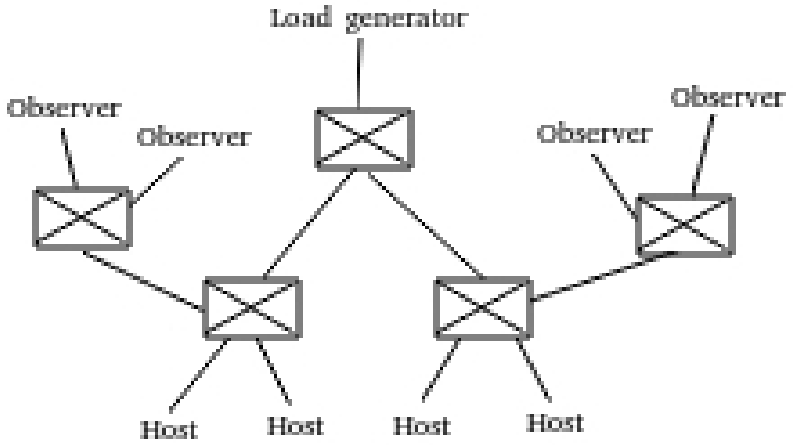
Implementazione dei client

- **Load-Generating Client:** invia transazioni ai nodi in maniera round-robin con burst uniformi di 50 transazioni e sleep uniformi tra un burst e l'altro

- **Observing Client:** fa polling dell'altezza della blockchain e conta in modo cumulativo le transazioni incluse nei nuovi blocchi

Topologie di test suite

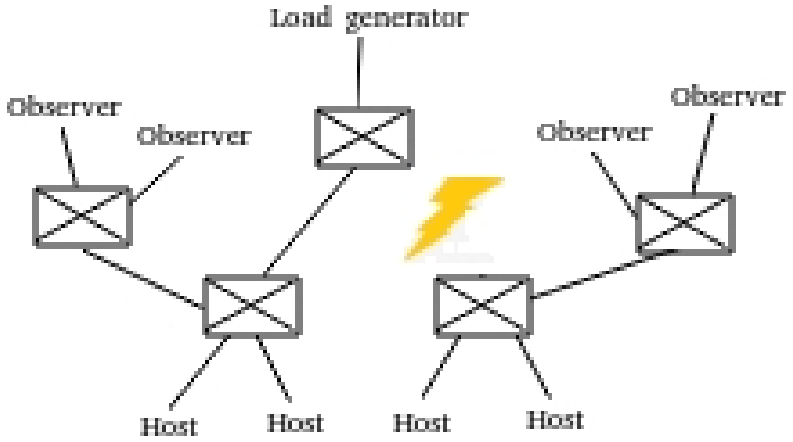
- **A stella** con crescente numero di host, senza transazioni
- **Ad albero** con profondità crescente e numero di transazioni crescente
- **Ad albero** con profondità crescente, numero di transazioni crescente e **partizione della rete** a metà per un certo intervallo di tempo



Esempio di topologia ad albero, di profondità 2

Topologie di test suite

- **A stella** con crescente numero di host, senza transazioni
- **Ad albero** con profondità crescente e numero di transazioni crescente
- **Ad albero** con profondità crescente, numero di transazioni crescente e **partizione della rete** a metà per un certo intervallo di tempo



Esempio di topologia ad albero con link down, di profondità 2

Risultati sperimentali ottenuti per NXT ed Ethereum nelle diverse topologie:

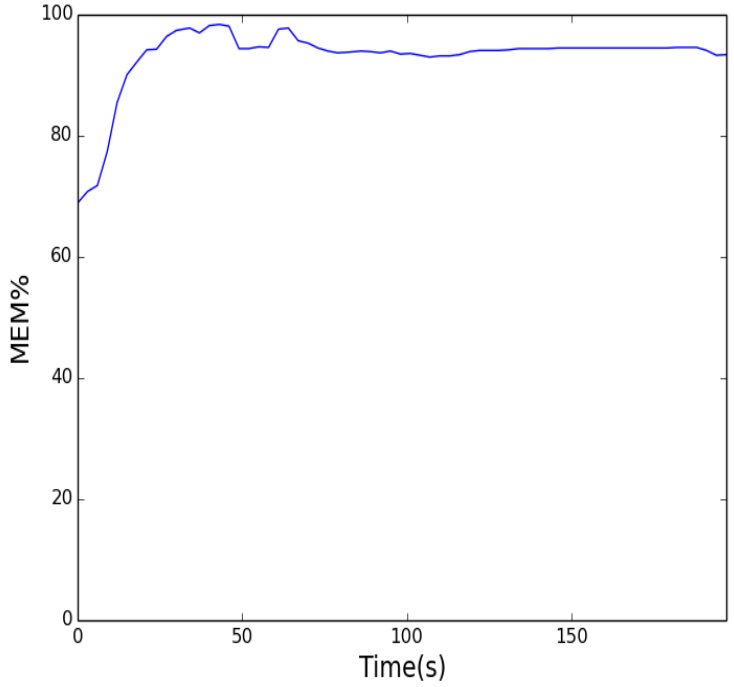
- Stella:
  - Utilizzo memoria centrale e CPU
  - Volume di traffico sulle interfacce di rete
- Albero:
  - Utilizzo memoria centrale e CPU
  - Volume di traffico sulle interfacce di rete
  - Transaction throughput
- Albero, con partizione di rete:
  - Utilizzo memoria centrale e CPU
  - Volume di traffico sulle interfacce di rete
  - Transaction throughput
  - Verifica dello switch da una fork all'altra analizzando i log dei nodi

Risultati sperimentali mostrati per NXT ed Ethereum nelle diverse topologie:

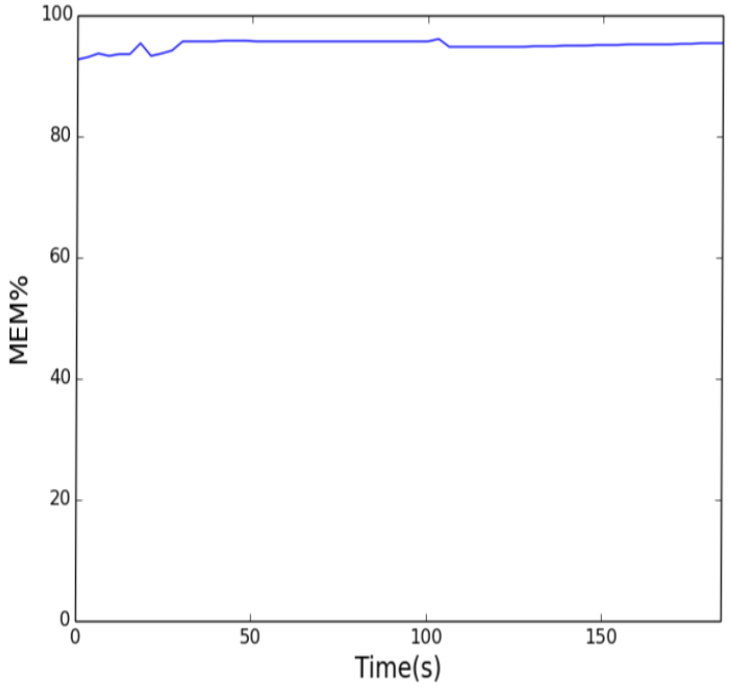
- Stella:
  - **Utilizzo memoria centrale** e CPU
  - Volume di traffico sulle interfacce di rete
- Albero:
  - Utilizzo memoria centrale e CPU
  - **Volume di traffico sulle interfacce di rete**
  - **Transaction throughput**
- Albero, con partizione di rete:
  - Utilizzo memoria centrale e CPU
  - Volume di traffico sulle interfacce di rete
  - **Transaction throughput**
  - Verifica dello switch da una fork all'altra analizzando i log dei nodi

Utilizzo memoria centrale in topologia a stella

NXT, 40 nodi



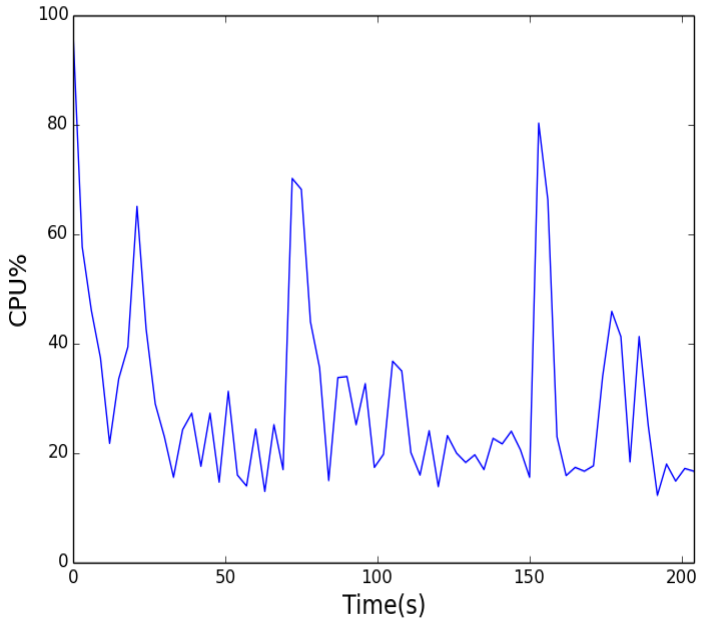
Ethereum, 10 nodi



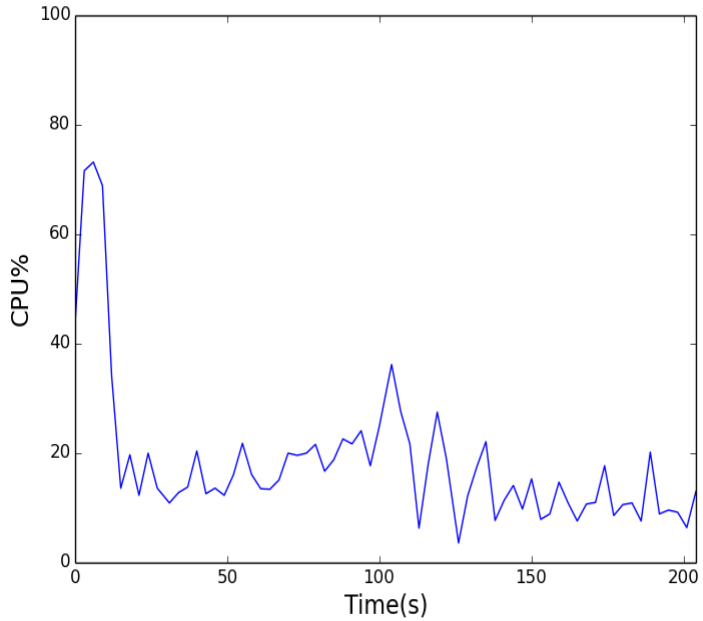
Ethereum richiede una maggiore quantità di memoria centrale

CPU in topologia ad albero con carico elevato e 8 nodi

Utilizzo CPU dei nodi NXT



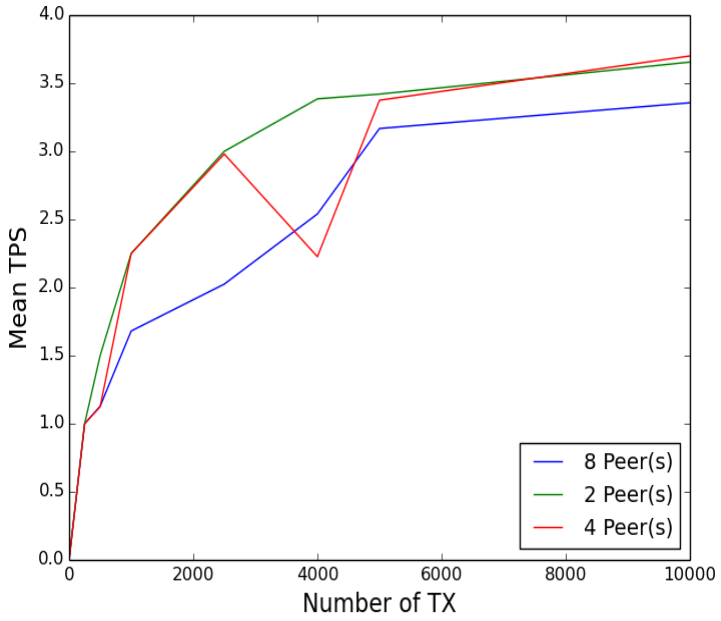
Utilizzo CPU dei nodi Ethereum



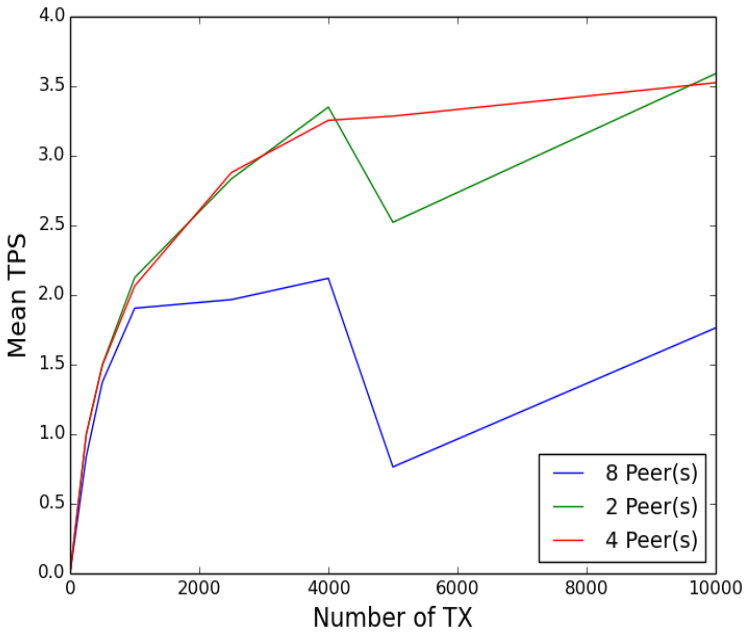
NXT utilizza maggiormente la CPU a parità di carico e di topologia a causa del meccanismo di consenso

TPS in topologia ad albero

Curve parametriche TPS per NXT



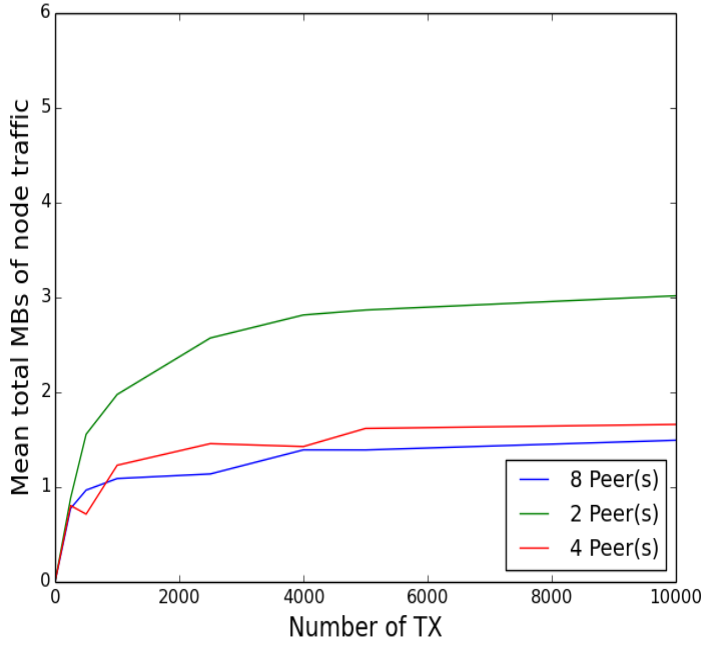
Curve parametriche TPS per Ethereum



Le performance sono simili, ma il TPS rate in Ethereum satura all'aumentare del numero di peer se non aumenta anche il numero di nodi autorizzati a validare blocchi

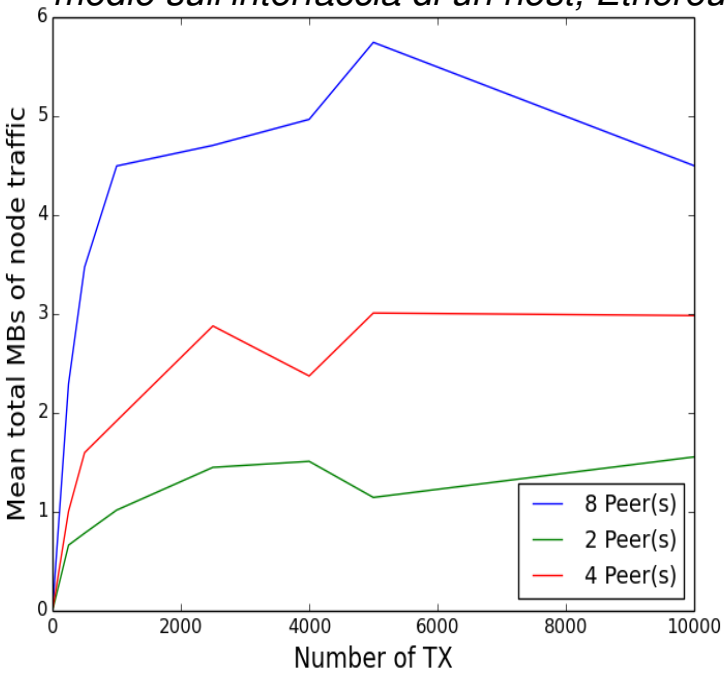
Volume di traffico in topologia ad albero

Curve parametriche volume di traffico medio sull'interfaccia di un host, NXT



*Nota: questo traffico tiene conto anche delle transazioni, perciò ad esempio per NXT il traffico con 2 peer è maggiore del traffico con 8 peer: meno **load balancing***

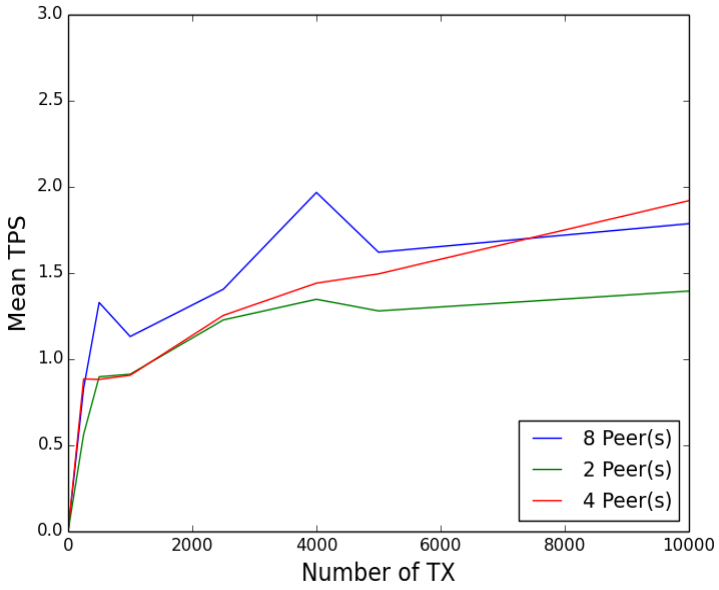
Curve parametriche volume di traffico medio sull'interfaccia di un host, Ethereum



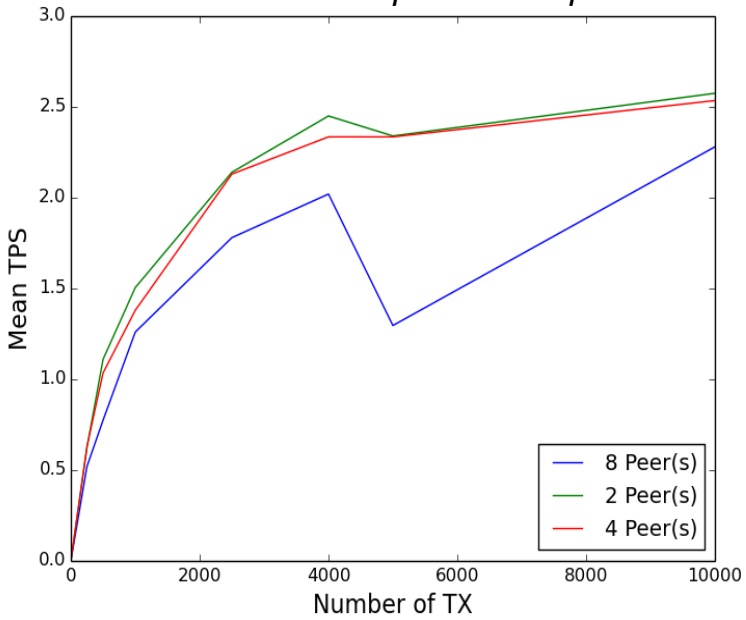
Questi dati possono essere interpretati come "*banda richiesta ad un peer*": **in Ethereum la banda richiesta è maggiore** a causa del meccanismo di consenso Proof of Authority

TPS in topologia ad albero con il link che cade

Curve parametriche TPS per NXT con link che cade e poi torna up



Curve parametriche TPS per Ethereum con link che cade e poi torna up



Ethereum ha prestazioni migliori in caso di partizione di rete perché il meccanismo PoA permette di accumulare transazioni ed il protocollo GHOST permette di non sprecare tutti i blocchi creati da una delle due partizioni quando si seleziona una catena valida a discapito dell'altra

Conclusioni

- **Riepilogo**
  - Analisi teorica del contesto, in particolare di NXT ed Ethereum
  - Confronto con Caliper
  - Setup di un testbed di emulazione di rete
  - Implementazione dei SUT e dei client specifici delle due tecnologie
  - **Confronto tra le due tecnologie:**
    - NXT scalabile su dispositivi che hanno poche risorse
    - Ethereum robusto alle partizioni di rete
  - Esperimento ripetibile: https://github.com/Shotokhan/blockchain-benchmarking-on-mininet
- **Possibili miglioramenti:**
  - Modello delle transazioni in input
  - Migliore ingegnerizzazione del setup, imitando il framework Caliper
  - Aggiunta di faultloads, ad esempio tentativi di double-spending attack
  - Observing client CP al posto di quello AP
- **Considerazioni: matching con altre tecnologie "disruptive"**
  - Caso di studio reale: Xbox game royalties (blockchain-as-a-service, big data analysis)

Bibliografia

[1] Neel Mehta, Adi Agashe, Parth Detroja, "Bubble or Revolution? The Present and Future of Blockchain and Cryptocurrencies", Paravane Ventures, 2020

[2] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", https://bitcoin.org/bitcoin.pdf

[3] Nxt community, "Nxt whitepaper", Revision 4 – Nxt v1.2.2 – July 12, 2014

[4] Thomas H. Cormen [et al.], "Introduction to Algorithms" (3 rd ed.), MIT Press, 2009

[5] SoluLab, answered on 23/12/2019: https://www.quora.com/What-kind-of-databases-are-used-by-Blockchain-platforms

[6] Coordicide Team, IOTA Foundation, "The Coordicide", May 2019

[7] Dominique Guegan. Public Blockchain versus Private blockhain. 2017. ffhalshs-01524440f

[8] Jonathan Ore, "How a $64M hack changed the fate of Ethereum, Bitcoin's closest competitor", CBC News, Aug 2018

[9] Ekin Tuna, Gardener Oracle, "An unexpected but ideal union: Magic and Blockchain", Medium, Aug 2019

[10] Vitalik Buterin, "Ethereum: The Ultimate Smart Contract and Decentralized Application Platform", Bitcoin Magazine, Dec 2013

[11] The Coin Rise, https://thecoinrise.com/how-do-bitcoin-transactions-work/, Aug 2020

[12] Wenbo Wang [et al.], "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks", arXiv:1805.02707v4 [cs.CR], 19 Feb 2019

[13] Binance Academy, "What is Delegated Proof of Stake (D-PoS) – Explained For Beginners", https://www.youtube.com/watch?v=OVKAOwzAwHI, Feb 2019

[14] REST Bitcoin API, https://rest.bitcoin.com/, Aug 2020

[15] Julian Browne, "Brewer's CAP Theorem: The kool aid Amazon and Ebay have been drinking", http://www.julianbrowne.com/, written in Jan 2009, last access in Aug 2020

[16] Wikipedia, https://en.wikipedia.org/wiki/CAP_theorem, Aug 2020

[17] Yaron Y. Goland, "The block chain and the CAP Theorem", https://www.goland.org/, written in Mar 2017, last access in Aug 2020

[18] Nicola Atzei [et al.], "A survey of attacks on Ethereum smart contracts", Università degli Studi di Cagliari, Mar 2017

[19] Steemit, https://steemit.com/blockchain/@reverseacid/the-scalability-trilemma, Aug 2020

[20] Lee, Timothy B., "Bitcoin has a huge scaling problem – Lightning could be the solution", Ars Technica, Feb 2018

[21] Bitcointalk, https://bitcointalk.org/index.php?topic=303898.0, Aug 2020

[22] Github, https://github.com/ethereum/EIPs/issues/225, written in Mar 2017, last access in Aug 2020

[23] Cryptocompare, https://www.cryptocompare.com/coins/guides/what-is-the-ghost-protocol-for-ethereum/, written in Jul 2015, last access in Aug 2020

[24] Blocking, https://blocking.net/5392/analysis-of-ethereum-ghost-agreement/, Aug 2020

[25] Vitalik, http://web.archive.org/web/20131228111141/http://vitalik.ca/ethereum/dagger.html, Aug 2020

[26] Unhashed, https://unhashed.com/cryptocurrency-news/ethereum-sharding-update-expected-2020/, Aug 2020

[27] Hyperledger, https://www.hyperledger.org/learn/publications/blockchain-performance-metrics, Aug 2020

[28] Bob Lantz, Brandon Heller, and Nick McKeown, "A Network in a Laptop: Rapid Prototyping for Software-Defined Networks. 9th ACM Workshop on Hot Topics in Networks", October 20-21, 2010, Monterey, CA

[29] University of South Carolina, "Network tools and protocols: Lab 3: Emulating WAN with NETEM I: Latency, Jitter", 14 Jun 2019

[30] University of South Carolina, "Network tools and protocols: Lab 3: Emulating WAN with NETEM II: Packet Loss, Duplication, Reordering and Corruption", 14 Jun 2019

[31] Jelurida, https://www.jelurida.com/nxt/evaluation, Aug 2020

[32] Github, https://github.com/ethereum/go-ethereum, Aug 2020

[33] Ethereum Wiki, https://eth.wiki/json-rpc/API, Aug 2020

[34] Hyperledger, https://hyperledger.github.io/caliper/, Aug 2020

[35] LinuxFoundation, https://web.archive.org/web/20170717193806/https://www.linuxfoundation.org/news-media/announcements/2015/12/linux-foundation-unites-industry-leaders-advance-blockchain, written Dec 2015, last access in Aug 2020