ISCAS 中国科学院软件研究所学术年会'2022 暨计算机科学国家重点实验室开放周
学术论文

Dumbo-NG: Fast Asynchronous BFT Consensus with Throughput-Oblivious Latency

Yingzi Gao*, Yuan Lu*, Zhenliang Lu§, Qiang Tang§, Jing Xu*, Zhenfeng Zhang*

* Institute of Software, Chinese Academy of Sciences
§ School of Computer Science, The University of Sydney

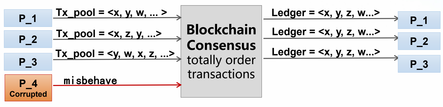
Contact: email {yingzi2019, luyuan, xujing, zhenfeng}@iscas.ac.cn, or call Yuan 13802125404
to appear in the 29th ACM Conference on Computer and Communications Security (**ACM CCS 2022**)

What is blockchain consensus?

Parties: a set of nodes (e.g., P_1, ...), some of which can be corrupted (e.g., P_4, ...);

Input: each party has a queue of transactions to process (called *Transaction pool*);

Output: an ever-growing sequence of linearized transactions (called *Ledger*).



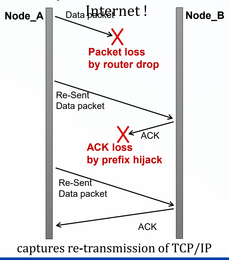
Security properties:

- ***Safety*:** the honest nodes would output the same ledger;
- ***Liveness*:** valid transactions eventually appear in the ledger.

Fault Tolerance: both properties are preserved despite attacks of corrupted parties.

In need of asynchronous consensus

Async. Network Model: messages can be *arbitrarily* delayed due to adversarial



captures re-transmission of TCP/IP

Asynchronous Consensus: aim to preserve all security realize in an asynchronous network

	In adversarial network	
	Safety	***Liveness***
Sync. Consensus (e.g. Bitcoin, Ethereum)	×	×
Partial-sync. Consensus (e.g. PBFT, HotStuff)	✓	×
Async. Consensus (e.g., Dumbo & this paper)	✓	✓

Robustness*:** async. consensus has both ***Safty and ***Liveness*** in an async. network;

***Responsiveness*:** async. consensus closely tracks the actual network speed instead of network delay's upper bound.

Progress & remaining efficiency hurdles

Timeline of asynchronous consensus:

[FLP83]: "**Impossible**"-- ***no*** deterministic async. consensus

[Rabin83][BenOr83] [CKPS01] etc. : "***theoretical* possibility**" -- possibile via randomization though with ***prohibitive cost***

2016

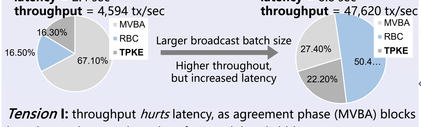
HoneyBadger [MXC+16]: first to realize ***linear*** communication complexity; ***but*** with slow **O(logN)** rounds

2020 2022

Dumbo [GLT+20][GLL+22]: both **O(1)** round and linear communication complexities; **an order of magnitude faster!**

Meta, VMware etc. also commit to build their own async. consensus

***Bottlenecks*: Latency breakdown of Dumbo** (16 nodes)

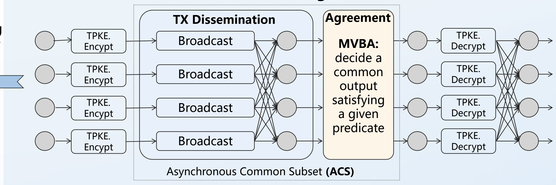


***Tension* I:** throughput *hurts* latency, as agreement phase (MVBA) blocks broadcasts, thus wasting a lot of network bandwidth

***Tension* II:** liveness needs *extra cost*, e.g. threshold encryption (TPKE) spends about 20% of whole latency

remaining efficiency hurdles

Execution flows of **Dumbo** [GLT+20] & **Speeding Dumbo** [GLL+22]: ***broadcast-then-agreement***



Dumbo-NG: our novel asynchronous blockchain consensus

Fundamental question solved by Dumbo-NG:

Can we push asynchronous consensus further to realize minimum latency, maximum throughput, and guaranteed liveness, simultaneously?

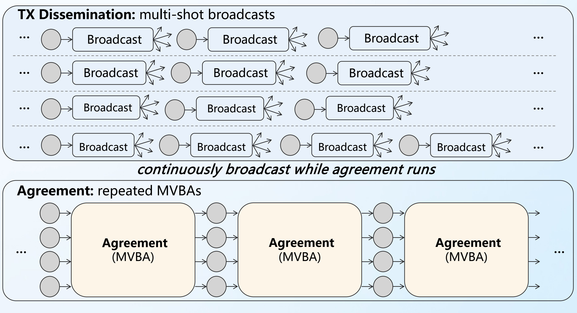
Core of Dumbo-NG (next generation of Dumbo):

- Parallelize broadcast and agreement
- Use MVBAs to ensure all broadcasts to totally order

broadcast -then- agreement → *broadcast -aside- agreement*

Execution flow of **Dumbo-NG** (***broadcast at full speed as agreement goes***):

1. each party starts an ever-growing broadcast to diffuse transactions (with fully utilizing bandwidth);
2. a sequence of MVBAs concurrently run to solicit all completed broadcasts into the final output.

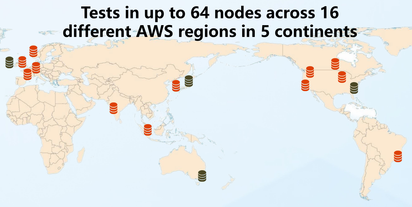


Evaluations in the wide-area global Internet

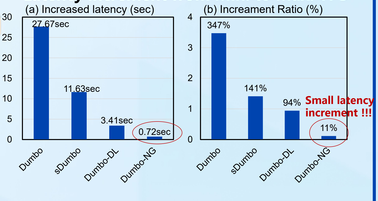
Highlights of experiments:

- ***throughput more than 100k tx/sec for all scales***: 4-8x over Dumbo, 2-4x over Speeding Dumbo, and 2-3x over another very recent study DispersedLedger (NSDI 2022) from Stanford and MIT;
- ***nearly stable latency despite throughput***, about only 10% increment in latency from least to peak throughputs.

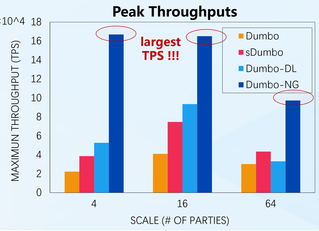
Tests in up to 64 nodes across 16 different AWS regions in 5 continents



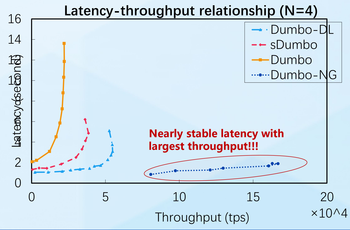
Latency increment from Min. to Max. TPS



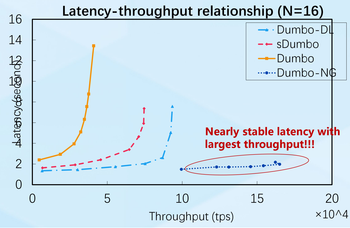
Peak Throughputs



Latency-throughput relationship (N=4)



Latency-throughput relationship (N=16)



Reference:
[**BenOr83**] M. Ben-Or, "*Another advantage of free choice: completely asynchronous agreement protocols*." **PODC** 1983
[**CKPS01**] C. Cachin, K. Kursawe, F. Petzold, and V. Shoup. "*Secure and efficient asynchronous broadcast protocols*." **CRYPTO** 2001
[**FLP83**] M. Fischer, N. Lynch, and M. Paterson, "*Impossibility of distributed consensus with one faulty process*." **PODS** 1983 / **JACM** 1985
[**GLL+22**] B. Guo, et al. "*Speeding Dumbo: Pushing asynchronous BFT closer to practice*."**NDSS** 2022
[**GLT+20**] B. Guo, et al. "*Dumbo: Faster asynchronous BFT protocols*."**CCS** 2020
[**MXC+16**] A. Miller, et al. "*The honey badger of BFT protocols*." **CCS** 2016
[**Rabin83**] M. Rabin, "*Randomized byzantine generals*." **FOCS** 1983