Harmony

Open Consensus for 10B People

@ 10M tx/sec, 100ms latency, 0.1% fee

Let’s build an open marketplace at Google-scale.

To 1,000x the ***decentralized economy***.
By speed & incentives.

State of Research: 13,000 tx/sec @ 1,800 nodes

Google's UDP

Powers 35% of Google's traffic (or 7% of the Internet) with 50% latency improvement & *zero round-trip* latency

OmniLedger

Shard Practical Byzantine Fault Tolerance (PBFT) with collective signing in O(1) size to elect continuously

Mosaic Pull-Reduce

Process a trillion edge graph on a single 244-core machine using *Hilbert-ordered* tiling scheme for locality

A high-performance blockchain demands ***10x innovations*** in the transport network, consensus protocol & system tools.

We master innovations already *proven in practice*.

	tx/sec	latency	msg	member	committee	coins
ByzCoin 🔥🐝💰	1,000	10s	O(n)	PoW	144	CYPHER
Solidus 🙈🐝💰	-	-	$O(n^2)$	PoW	-	*
Algorand 🙈	0.025	40s	$O(n^2)$	Lottery	50,000	*
Hyperledger 🔥	110,000	<1s	-	Perm	4	-
RSCoin 🚀🔥	2,000	<1s	O(n)	Perm	3/10	*
Elastico 🚀🙈💰	0.15	16s	$O(n^2)$	PoW	100/16	-
OmniLedger 🚀💰	10,000	~1s	O(n)	PoW	72/25	ZIL
Chainspace 🚀🔥🐝💰	350	<1s	$O(n^2)$	-	4/15	-
Ouroboros 🙈🐝	(257.6)	(20s)	O(nc)	Lottery	40	ADA
Praos 🙈💰	-	-	O(1)	PoS	-	ADA
Snow-white 🚀🙈🐝	(150)	-	O(1)	PoS	40	Thunder
PermaCoin 🔥	-	-	O(1)	PoR	-	-
SpaceMint 🔥	-	(600s)	O(1)	PoS	-	-
Intel PoET 🚀🔥	1,000	-	O(1)	HW	-	-
REM 🚀	-	-	O(1)	HW	-	-
Bitcoin 🔥	7	600s	O(1)	PoW	-	BTC
Bitcoin-NG 🐝	(7)	(<1s)	O(1)	PoW	-	CYPHER
Ghost	-	-	O(1)	PoW	-	ETH
Decor+Hop	(30)	(60s)	O(1)	PoW	-	-
Spectre	-	-	O(1)	PoW	-	-

Consensus protocols in open research from SoK Consensus.

🚀 scalable to 100K nodes
🔥 source code available
🙈 vulnerable to tx censorship
🐝 vulnerable to DoS
💰 incentive to join committee

OmniLedger is the *most scalable* permissionless protocol, tested with 25 committees (each consists of 72 nodes).

Our Milestones in 2018

Optimal Languages

Rust/Go for backends, OCaml/Coq for algorithms + verification

Core Team

5 engineers, ex-Google, serial entrepreneurs, security Ph.D.

Open benchmark

Public testnet of 100k nodes at 100k tx/sec and 1s latency

Novel Architecture

Google UDP on 5G, unikernel servers, allocation-free multi-core streaming, memory-only database

Open source

Full code at Github for native X86-64 / JVM compiler, and open development community

Open Research

Published at IEEE Security & Privacy, ACM Transactions on Programming Languages & Systems

Location Oracles & Decentralized Maps

Community content

Long-tail features, incentivized games, #pokemom, augmented reality & IoT w/ GPS data

Smart cities

Autonomous vehicles, ~1,000 self-organizing **swarm robots** w/ driven mission

Privacy-preserving

Multiparty computation, #deletefacebook, homomorphic encryption

Harmony is a new ***public chain*** redesigned with top performance and physical locations.

For real-world decentralized applications.

Harmony scales *Decentralized Economy* to 10B People

*An extended team (part time) of **four Ph.D.**, 3 Ex-Google, 2 Ex-Apple, graduates from Berkeley, CMU, Waterloo, Penn and Harvard.*

See simple-rules.com/whitepaper.

- *Stephen Tse* UPenn PhD on compiler and **security protocols**
- Microsoft Research, Google Maps infrastructure engineer
- founder of mobile search Spotsetter **acquired by Apple**
- principal engineer at Apple Maps search ranking
- TGI-ML/Blockchain for ex-Google founders

OmniLedger: Principles & Optimizations for Scaling

Representative sharding

O(1)-size multi-signatures for 10k nodes vs 16-node PBFT. Crypto sortition via randoness from multi-party computation and commit-then-reveal step.

Gradual transition

Sybil-resistant identities to maintain liveness when swapping. A sliding window from a fixed permutation to ensure ⅔ honest majority.

Atomic shard-commit

Each shard uses O(log n) *multicast tree-based BFT* to unanimously accept cross-shard transactions with O(1)-size *coordination.*

Parallelizing blocks

Acyclic graphs to capture transaction *dependencies transitively*. Divide each shard into groups to replace faulty nodes with a view-change.

Pruning checkpoints

State blocks for storage and bootstrapping against Byzantine DoS. Multi-hop, collectively signed back -pointers, 100x space savings.

Optimistic confirms

Trust but verify low-value transactions with shard deposits. Guarantee finality in ~1s with *penalty linear to loss* and detection in minutes.