IIT MADRAS
Indian Institute of Technology Madras

Technology Transfer Office
TTO – IPM Cell

Industrial Consultancy & Sponsored Research (IC&SR)

COLOSSEUM, A SCALABLE AND BYZANTINE-FAULT TOLERANT CONSENSUS MECHANISM FOR PERMISSIONED SYSTEMS

IITM Technology Available for Licensing

Problem Statement

- **Byzantine failures in blockchain** complicate system reliability and security, especially in financial, healthcare, and supply chain domains.
- **Traditional permissioned blockchains** rely on voting-based consensus, which **assumes constant adversaries and suffers from high message complexity**, leading **to scalability issues** and limited applications in high-demand scenarios.
- Further, **conventional methods** face challenges like **network congestion**, **double-spending risks**, **high computational costs**, and **inefficient handling of adversaries**, making them unsuitable for large-scale applications demanding high throughput.
- There is a **need for a novel consensus mechanism to address Byzantine failures** and improve system reliability and security for industries requiring **secure, scalable, and efficient blockchain solutions**.

Intellectual Property

- IITM IDF Ref 1869
- **IN 564032 Patent Granted**
- **US 12,107,959 B2 Patent Granted**

TRL (Technology Readiness Level)

TRL 6 Technology demonstrated in relevant environment

Technology Category/ Market

Category- Blockchain

Industry Classification:

Financial Services; Healthcare; Supply Chain and Logistics; Government and Public Sector

Applications:

Secure and scalable transactions for banking and stock exchanges; Managing sensitive patient data across distributed networks; Ensuring fault tolerance in distributed IoT ecosystems and Verifiable and tamper-proof transaction records

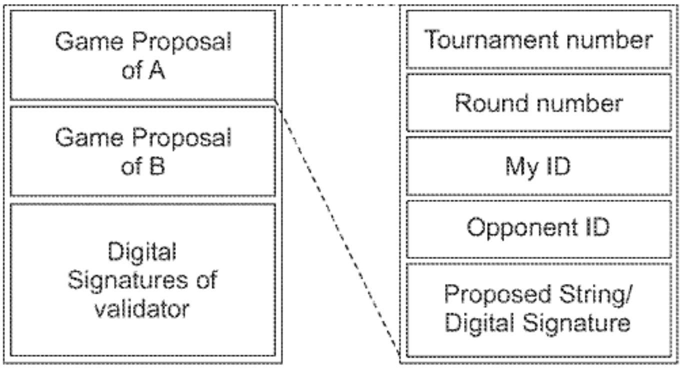
Market report:

The global blockchain market was valued at USD 42.29 billion in 2024 and is projected to grow to $2346.01 billion by 2032 with a CAGR of 65.2%

Research Lab

Prof. Janakiram D

Dept.of Computer Science and Engineering



Game Proposal of A

Game Proposal of B

Digital Signatures of validator

Tournament number

Round number

My ID

Opponent ID

Proposed String/ Digital Signature

Figure: Colosseum (a Byzantine fault tolerant scalable method to achieve consensus) proposes a novel two-player game-like approach which uses Proof-of-Win to eliminate nodes in each round of a tournament resulting in the selection of a subset of nodes after α (α <log 2N,where N is the number of nodes in then network) number of rounds. It allows multiple block proposers for a tournament and tries to commit a maximum of their blocks using Converging Directed Acyclic Graph (CDAG) as the ledger to increase the throughput of the transactions.

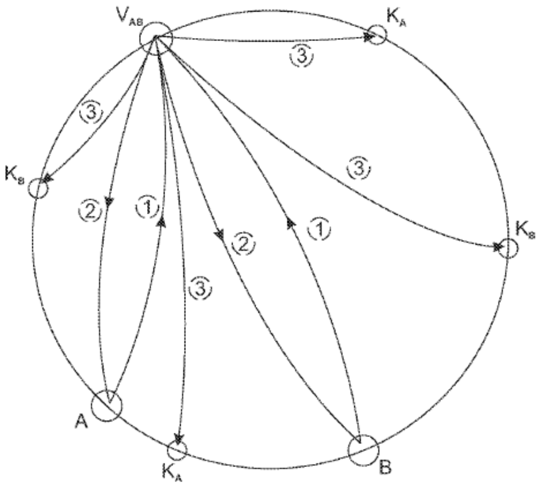


Figure: Depicts message flow of a match in Colosseum. A, B are the players, V_{AB} is the validator, and K_A, K_B are the keepers

CONTACT US
Dr. Dara Ajay, Head TTO
Technology Transfer Office,
IPM Cell- IC&SR, IIT Madras

IITM TTO Website:
https://ipm.icsr.in/ipm/

Email: headtto-icsr@icsrpis.iitm.ac.in
ttooffice@icsrpis.iitm.ac.in
Phone: +91-44-2257 9756/ 9845

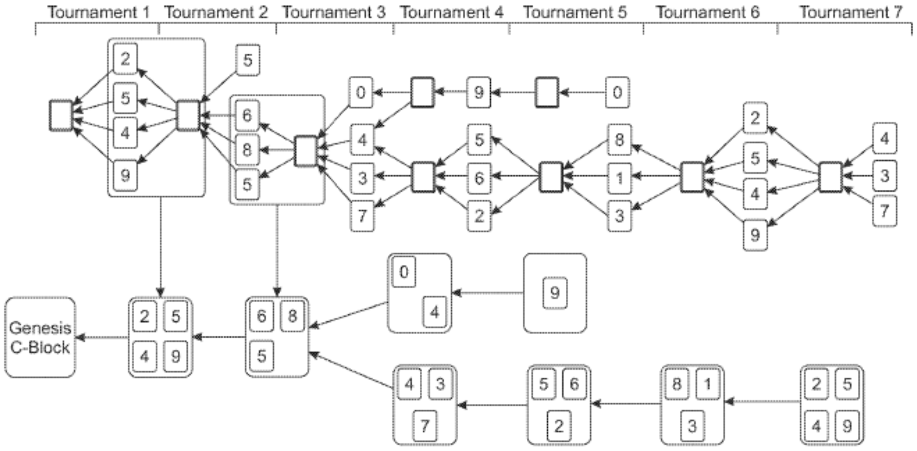


Figure: Depicts the progress of CDAG for the number of tournaments.

Technology

- Colosseum uses a novel knockout tournament to select block proposers, leveraging a cryptographic Proof-of-Win for transparency and fault tolerance.
- **Employs Converging Directed Acyclic Graph (CDAG) to enable simultaneous block additions, reducing conflicts and improving transaction finality.**
- Adaptable configurations allow the system to scale efficiently with network size, as demonstrated by throughput results under varying conditions.
- Random validator assignment and independent verification mechanisms prevent tampering and unauthorized actions, enhancing trust in the system.
- Features like distributed time barriers and transaction bucketing ensure operational efficiency, even in large, diverse networks.

Key Features / Value Proposition

- Colosseum utilizes a knockout tournament to select block proposers, reducing complexity and ensuring fairness without assuming constant adversarial presence.
- The introduction of CDAG allows simultaneous block additions, addressing the bottlenecks in traditional blockchain and blockDAG structures.
- Efficient transaction bucketing and distributed time barriers minimize conflicts and ensure ledger consistency, critical for large-scale deployment.
- By leveraging Proof-of-Win (PoWin) certificates, the system ensures tamper-proof validation and restricts unauthorized actions, improving security.
- Dynamic pairing, random validator selection, and C-Block integration make the system resilient to targeted attacks, enhancing usability in diverse environments.

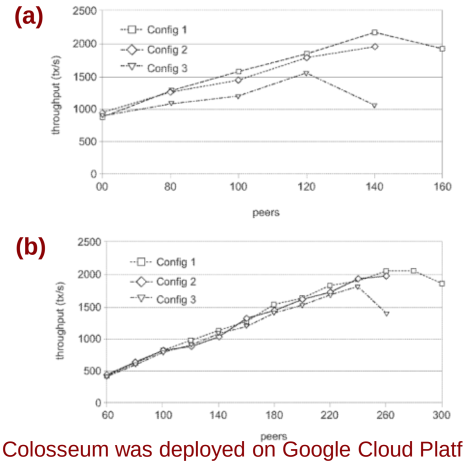


Figure: The Colosseum was deployed on Google Cloud Platform using Google Kubernetes Engine having n1-high-mem-16 instances, each with 16 cores and 104 GB memory. Figures **(a)** for **α** = 3 and **(b)** for **α** = 4; show that for a fixed value of **α** the throughput of the system increases initially with the number of nodes and then starts to decrease. The value of **α** can be manipulated to achieve the optimum throughput for a given configuration similar to setting the hardness of the cryptographic puzzle in Bitcoin.