Nitin Awathare

Mumbai (India)

nitina@cse.iitb.ac.in +91 9503884632 IIT Bombay, Mumbai
linkedin profile github profile `https://www.cse.iitb.ac.in/~nitina/`

Education

Ph.D. **IIT Bombay** (Jul 2016 – Feb 2022)
Department of Computer Science and Engineering
Thesis title : **On the Scalability of Blockchains**
Advisor: **Prof. Umesh Bellur** and **Prof. Vinay Ribeiro**

M.Tech **IIT Kharagpur** (Jul 2013 – May 2015)
Department of Computer Science and Engineering
Advisor: **Prof. Arobinda Gupta**

B.Tech **WCE Sangli** (Jul 2007 – May 2011)
Department of Computer Science and Engineering

Professional Experience

Jun 2022 - May 2023 **National University of Singapore, Singapore**

- Worked as a postdoctoral researcher. During my tenure, I worked on the distributed cross-chain commit problem and explored the use of TLA+ model checker to ensure the correctness of the designed protocol.

Jun 2015 - Jul 2016 **Capillary Technologies, Bangalore, India**

- Worked on API development using Django-Python.

Jun 2011 - Jul 2013 **Persistent System Ltd., Pune, India**

- Worked on ERP application using AX-Dynamics.

Jun 2019 - Aug 2019 **IBM Research Lab, Bangalore, India (Research Internship)**

- Worked on empirical evaluation of different permissioned blockchain protocols such as Quorum, Hyperledger Fabric, and Corda.

Research Interests

Distributed Systems, Blockchain, Payment Channel Network.

Publications

2022

1. Das, S., **Awathare, N.**, Ren, L., Ribeiro, V. J. & Bellur, U. Tuxedo: Maximizing Smart Contract computation in PoW Blockchains. **ACM SIGMETRICS** (2022).

2021

2. **Awathare, N.**, Das, S., Ribeiro, V. J. & Bellur, U. RENOIR: Accelerating Blockchain Validation using State Caching. *International Conference on Performance Engineering (***ICPE***)* (2021).
3. **Awathare, N.**, Suraj, Akash, Ribeiro, V. & Bellur, U. REBAL : Channel Balancing for Payment Channel Networks. *IEEE International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (***MASCOTS***)* (2021).

Patent Application

Jun 2020 | **Method for scaling computation in blockchain by delaying transaction execution**
`https://patents.google.com/patent/US20200409941A1/en`
US Patent App. 16/912,389

Professional Activities

- Reviewer for **Transactions on Management Information Systems(TMIS)** and **COMSNETS**- Blockchain workshop.
- Technical advisor for an e-learning company **TalentServe**.
- Organized a **C3** workshop at NUS.

Academic Activities

- TA for course Introduction to Blockchains, Cryptocurrencies and Smart Contracts (CS765, CS653, CS620) and Advance Blockchain technologies (CS762). I am awarded an excellent TA award for CS762 during Autumn 2021.
- Mentored 3 UG and 6 PG students.
- Delivered a talk at Dr. B. R. Ambedkar Technological University, Lonere, on my Ph.D. research.
- Delivered a talk on Computation Scalability in the Blockchain at the University of Warsaw, Poland.

Skills

- Languages: C/C++, Java, Python, Shell Script, Solidity, Golang.
- Technologies: Ethereum, Bitcoin, Quorum.
- Tools: Omnet++, LaTeX, gnuplot.

Projects of Interest

- **Enable Decentralized Exchange that mitigate a Bribery attack:** This study introduces an attack strategy targeting decentralized exchange protocols, specifically MAD-HTLC and He-HTLC. Additionally, we present a novel decentralized exchange protocol that effectively prevents miners from seizing any funds belonging to users engaged in the exchange. This new protocol addresses the vulnerabilities highlighted in the attack we proposed, thereby offering enhanced security measures compared to existing approaches. (**Transcript under submission and work done at NUS**)
  Tools & Technologies - Ethereum, Golang

- **Consensus based node joining in the Lightning Network:** The lower transaction success ratio observed in the lightning network can be primarily attributed to the inherent nature of its topology. The current topology exhibits a power-law distribution in terms of node degree, where a few highly connected nodes, known as hubs, serve as frequent intermediaries for transactions. This often leads to the development of unidirectional channels. The prevalence of power-law distribution among nodes is driven by users' preference to join nodes with better connectivity for efficient transactions. In our research, we have decentralized the node joining decision-making process by shifting it from the user level to the consensus layer, specifically the blockchain. (**Transcript under submission and work done at NUS**) ***Tools & Technologies -*** Omnet++, C++, Lightning Network, and Python

- **Enable computationally-intensive transactions on the Blockchain without compromising security:** We have reduced the block validation time by prior state caching with and without changing the block structure. We have implemented both approaches after a major edit in the Ethereum-1.9.3 code. Further, we developed the experimental test-bed from scratch and demonstrated that the First approach increases the computation to 74% the block inter-arrival time, while the second increases it to 25% from the current value of 1%.
  Tools & Technologies - Ethereum, Golang, Python, and Shell script

- **Improved the transaction success ratio in the Payment Channel Network:** We have simulated the Lightning Network (LN) using Omnet++ (Discrete event simulator). Our simulator reflects the production LN topology, which we have collected by instrumenting Golang implementation of LN. We have demonstrated an increase in the transaction success from 30.18% to 79.54% and transaction success volume from 3.98% to 29.99%.
  Tools & Technologies - Omnet++, C++, Lightning Network, and Python

- **Scale the throughput and bandwidth utilization in Bitcoin:** We have modified the block to include only the transaction's hash, which is off the track from the current Bitcoin that includes complete transactions. It is implemented by non-trivial changes in the Bitcoin-C++ code and demonstrated the improvement of ≃7x in throughput and bandwidth utilization.
  Tools & Technologies - Bitcoin (C++ implementation) and Shell script

- **Measuring and improving the quality of barrier coverage in the wireless sensor network (M.Tech thesis):** We propose a distributed approach to improve the quality of k-barrier coverage with the objective of minimizing the number of sensors required.
  Tools & Technologies - C++

- **Edge-based attack on the time-varying network:** The edge-based attack is the more constrained case of the node-based attack where the attacker targets the link between the nodes. We found that the node-based attack is more severe than the edge-based attack for different attacking behavior that prioritizes the attacking edge based on betweenness centrality, eigenvector centrality, degree centrality, etc.
  Tools & Technologies - Python