IJTCS 2022 CSIAM Forum

**Title:**

DAMYSUS: Streamlined BFT Consensus Leveraging Trusted Components

**Abstract:**

Recently, streamlined BFT consensus protocols, such as HotStuff, have been proposed as a means to circumvent the inefficient view-changes of traditional BFT protocols, such as PBFT. Several works have detailed trusted components, and BFT protocols that leverage them to tolerate a minority of faulty nodes and use a reduced number of communication rounds. Inspired by these works we identify two basic trusted services, respectively called the Checker and Accumulator services, which can be leveraged by streamlined protocols. Based on these services, we design Damysus, a streamlined protocol that improves upon HotStuff’s resilience and uses less communication rounds. In addition, we show how the Checker and Accumulator services can be adapted to develop Chained-Damysus, a chained version of Damysus where operations are pipelined for efficiency. We prove the correctness of Damysus and Chained-Damysus, and evaluate their performance showcasing their superiority compared to previous protocols.

**Bio:** Dr. Jiangshan Yu is a 2021 ARC DECRA Fellow and Senior Lecturer (~US Associate Professor) at Monash University. He also serves as Associate Director (Research) at Monash Blockchain Technology Centre. He is a member of the Scientific Advisory Board for Austrian Blockchain Center (Austria), and an elected member of the IFIP 10.4 Working Group on Dependable Computing and Fault Tolerance. His research interests are in the broad area of cybersecurity and applied cryptography, with a current focus on blockchain systems. The impact of his research includes identified critical vulnerabilities and recommended (and adopted) fixes in several deployed blockchains and their applications (with a total market cap of over AU$30 billion). The importance and impact of his research have been recognised by the Australian Government’s National Blockchain Roadmap as an example of the world-leading blockchain research activities in Australia. He is also a recipient of several competitive awards, such as ARC DECRA (2021-2023) and the IBM Academic Award (2020), and Dean’s Research Impact Award at Monash (2019).

**Email:** jiangshan.yu@monash.edu

**Title:**

Blockchain-Based Private Provable Data Possession

**Abstract:**

In order to check remote data integrity, an important paradigm PDP is proposed. All the existing PDP schemes make use of RSA or bilinear pairings. The huge computation cost and communication cost incurs the inefficient PDP implementation. In other words, they are not practical. In order to solve the problem, we propose a new PDP model: blockchain-based private PDP. The new concept makes use of blockchain which is the core of cryptocurrency. For the new concept, the paper formalizes its system model and security model. Then, a concrete blockchain-based private PDP scheme is designed by making use of blockchain and RSA. The proposed blockchain-based private PDP scheme is provably secure, efficient and practical.

**Bio:** Huaqun Wang received the BS degree in mathematics education from Shandong Normal University, in China, in 1997, the MS degree in applied mathematics from East China Normal University, in China, in 2000, and the PhD degree in cryptography from the Nanjing University of Posts and Telecommunications, in 2006. Now, he is a full professor in Nanjing University of Posts and Telecommunications. His research interests include applied cryptography, blockchain, network security, and cloud computing security.

**Email:** whq@njupt.edu.cn